Technical Guideline TR-03105

Conformity Tests for Official Electronic ID Documents

Part 3.2: Test plan for eMRTDs with Advanced Security Mechanisms – EAC 1

Version 1.5.1
April 30th 2020
### Version history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>17-04-2007</td>
<td>AFNOR</td>
<td>Proposal for harmonized document</td>
</tr>
<tr>
<td>0.5</td>
<td>24-04-2007</td>
<td>BSI/Secunet</td>
<td>EAC conformity tests – Harmonization document</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Working Draft</td>
</tr>
<tr>
<td>0.6</td>
<td>15-05-2007</td>
<td>AFNOR</td>
<td>EAC conformity tests – Harmonization document</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Working Draft -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- AFNOR tests addition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Test cases EAC.CV.E.13, EAC.CV.E.14 and EAC.CV.E.15 have been deleted</td>
</tr>
<tr>
<td>0.7</td>
<td>24-05-2007</td>
<td>BSI/Secunet</td>
<td>- Editorial changes, - renumbered test case IDs - Add test for migration policy</td>
</tr>
<tr>
<td>0.72</td>
<td>01-06-2007</td>
<td>AFNOR</td>
<td>- Editorial changes</td>
</tr>
<tr>
<td>0.73</td>
<td>01-06-2007</td>
<td>BSI/Secunet</td>
<td>- Editorial change in certificate definition</td>
</tr>
<tr>
<td>0.8</td>
<td>09-07-2007</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 0.73</td>
</tr>
<tr>
<td>0.81</td>
<td>10-07-2007</td>
<td>AFNOR</td>
<td>- Resolved comments on 0.73 (suite)</td>
</tr>
<tr>
<td>0.82</td>
<td>10-07-2007</td>
<td>BSI/Secunet</td>
<td>- Minor editorial changes</td>
</tr>
<tr>
<td>0.83</td>
<td>13-07-2007</td>
<td>AFNOR</td>
<td>- Resolved comments on 0.73 (suite)</td>
</tr>
<tr>
<td>0.84</td>
<td>16-07-2007</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 0.73 (suite)</td>
</tr>
<tr>
<td>0.85</td>
<td>16-07-2007</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 0.73 (suite)</td>
</tr>
<tr>
<td>0.86</td>
<td>16-07-2007</td>
<td>AFNOR</td>
<td>- Minor editorial changes</td>
</tr>
<tr>
<td>0.87</td>
<td>18-07-2007</td>
<td>BSI/Secunet</td>
<td>- Fix expected results for ISO7816_I_8, ISO7816_J_14, ISO7816_J_16, ISO7816_K_8</td>
</tr>
<tr>
<td>0.88</td>
<td>19-07-2007</td>
<td>AFNOR</td>
<td>- Fix expected results for ISO7816_I_6</td>
</tr>
<tr>
<td>1.0</td>
<td>23-07-2007</td>
<td>BSI/Secunet</td>
<td>- Minor fix ISO7816_H_2 - Add clarification to ISO7816_I_8</td>
</tr>
<tr>
<td>1.1 RC1</td>
<td>13-11-2007</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 1.0 - Additional tests for EAC 1.1</td>
</tr>
<tr>
<td>1.1</td>
<td>23-11-2007</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 1.1 RC1</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Editor</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.11RC1</td>
<td>12-03-2008</td>
<td>BSI/Secunet</td>
<td>- Changes based on EAC 1.11</td>
</tr>
<tr>
<td>1.11RC2</td>
<td>15-04-2008</td>
<td>BSI/Secunet</td>
<td>- Changes based on EAC 1.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Paris testing</td>
</tr>
<tr>
<td>1.11RC3</td>
<td>25-04-2008</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 1.1 RC2</td>
</tr>
<tr>
<td>1.11</td>
<td>30-04-2008</td>
<td>BSI/Secunet</td>
<td>- Resolved comments on 1.1 RC3</td>
</tr>
<tr>
<td>1.12 RC1</td>
<td>03-07-2008</td>
<td>AFNOR/Soliatis</td>
<td>- ISO7816_K_19 test case addition</td>
</tr>
<tr>
<td>1.12 RC2</td>
<td>07-08-2008</td>
<td>BSI/Secunet</td>
<td>- Resolved comments from Ispra testing</td>
</tr>
<tr>
<td>1.12 RC3</td>
<td>25-09-2008</td>
<td>BSI/Secunet</td>
<td>- Resolved comments from Prague testing</td>
</tr>
<tr>
<td>1.12</td>
<td>03-10-2008</td>
<td>BSI/Secunet</td>
<td>- Released without changes</td>
</tr>
<tr>
<td>1.2 RC1</td>
<td>16-04-2012</td>
<td>BSI</td>
<td>- Added test cases for PACE/TA binding and Chip Authentication with MSE:Set AT &amp; General Authenticate commands</td>
</tr>
<tr>
<td>1.2 RC2</td>
<td>13-06-2012</td>
<td>BSI/AFNOR</td>
<td>- Resolved comments from AFNOR</td>
</tr>
<tr>
<td>1.2 RC3</td>
<td>21-06-2012</td>
<td>BSI/AFNOR</td>
<td>- Minor corrections</td>
</tr>
<tr>
<td>1.2 RC4</td>
<td>08-11-2012</td>
<td>BSI</td>
<td>- Resolved comments on V1.2RC3 from Article 6 Technical Subgroup meeting</td>
</tr>
<tr>
<td>1.2 RC5</td>
<td>23-11-2012</td>
<td>BSI</td>
<td>- Minor clarifications on test case ISO7816_J_12 and ISO7816_L_13</td>
</tr>
<tr>
<td>1.2 RC6</td>
<td>30-11-2012</td>
<td>BSI/AFNOR</td>
<td>- Resolved comments from AFNOR</td>
</tr>
<tr>
<td>1.2</td>
<td>05-12-2012</td>
<td>BSI/AFNOR</td>
<td>- Released finalized version 1.2</td>
</tr>
<tr>
<td>1.3</td>
<td>25-02-2013</td>
<td>BSI</td>
<td>- Minor corrections</td>
</tr>
<tr>
<td>1.4</td>
<td>13-03-2014</td>
<td>BSI/AFNOR</td>
<td>- Minor clarifications on test case ISO7816_II_4, ISO7816_L_13 and ISO7816_L_14</td>
</tr>
<tr>
<td>1.4.1</td>
<td>06-04-2014</td>
<td>BSI/AFNOR</td>
<td>- Minor corrections</td>
</tr>
<tr>
<td>1.5 RC1</td>
<td>19-01-2018</td>
<td>BSI/secunet</td>
<td>- Editorial changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Resolved comments</td>
</tr>
<tr>
<td>1.5 RC2</td>
<td>30-04-2018</td>
<td>BSI/secunet</td>
<td>- Resolved comments of DIF AG Chip</td>
</tr>
<tr>
<td>1.5 RC3</td>
<td>17-09-2018</td>
<td>BSI/secunet</td>
<td>- Resolved comments of DIF AG Chip</td>
</tr>
<tr>
<td>1.5 RC4</td>
<td>13-11-2018</td>
<td>BSI/secunet</td>
<td>- Resolved comments of DIF AG Chip</td>
</tr>
<tr>
<td>1.5</td>
<td>14-12-2018</td>
<td>BSI</td>
<td>Resolved DIF AG CHIP comments on RC 4</td>
</tr>
</tbody>
</table>
## Test plan for eMRTDs with EACv1

### Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5.1</td>
<td>30-04-2020</td>
<td>BSI/secunet</td>
<td>Added AFNOR logo on cover page</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Resolved comments of AFNOR</td>
</tr>
</tbody>
</table>
# Content

<table>
<thead>
<tr>
<th>1</th>
<th>Introduction</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Abbreviations</td>
<td>9</td>
</tr>
<tr>
<td>1.2</td>
<td>Reference documentation</td>
<td>10</td>
</tr>
<tr>
<td>1.3</td>
<td>Terminology</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>General test requirements</td>
<td>11</td>
</tr>
<tr>
<td>2.1</td>
<td>Test setup</td>
<td>11</td>
</tr>
<tr>
<td>2.2</td>
<td>Test profiles</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Key pair definition</td>
<td>13</td>
</tr>
<tr>
<td>2.4</td>
<td>Certificate specification</td>
<td>14</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Certificate Set 1</td>
<td>15</td>
</tr>
<tr>
<td>2.4.2</td>
<td>Certificate Set 2</td>
<td>25</td>
</tr>
<tr>
<td>2.4.3</td>
<td>Certificate Set 3</td>
<td>28</td>
</tr>
<tr>
<td>2.4.4</td>
<td>Certificate Set 4</td>
<td>30</td>
</tr>
<tr>
<td>2.4.5</td>
<td>Certificate Set 5</td>
<td>32</td>
</tr>
<tr>
<td>2.4.6</td>
<td>Certificate Set 6</td>
<td>34</td>
</tr>
<tr>
<td>2.4.7</td>
<td>Certificate Set 7</td>
<td>37</td>
</tr>
<tr>
<td>2.4.8</td>
<td>Certificate Set 8</td>
<td>40</td>
</tr>
<tr>
<td>2.4.9</td>
<td>Certificate Set 9</td>
<td>41</td>
</tr>
<tr>
<td>2.4.10</td>
<td>Certificate Set 10</td>
<td>42</td>
</tr>
<tr>
<td>2.4.11</td>
<td>Certificate Set 11</td>
<td>47</td>
</tr>
<tr>
<td>2.4.12</td>
<td>Certificate Set 12</td>
<td>54</td>
</tr>
<tr>
<td>2.4.13</td>
<td>Certificate Set 13</td>
<td>68</td>
</tr>
<tr>
<td>2.4.14</td>
<td>Certificate Set 14</td>
<td>70</td>
</tr>
<tr>
<td>3</td>
<td>Tests for layer 6 (ISO 7816)</td>
<td>75</td>
</tr>
<tr>
<td>3.1</td>
<td>Test case notation</td>
<td>75</td>
</tr>
<tr>
<td>3.2</td>
<td>General requirements</td>
<td>75</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Security Status</td>
<td>75</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Extended length APDUs</td>
<td>76</td>
</tr>
<tr>
<td>3.3</td>
<td>Unit ISO7816_H – Security Conditions for EAC protected MRTDs</td>
<td>76</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Test case ISO7816_H_1</td>
<td>76</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Test case ISO7816_H_2</td>
<td>77</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Test case ISO7816_H_3</td>
<td>77</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Test case ISO7816_H_4</td>
<td>77</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Test case ISO7816_H_5</td>
<td>78</td>
</tr>
<tr>
<td>3.3.6</td>
<td>Test case ISO7816_H_6</td>
<td>78</td>
</tr>
<tr>
<td>3.3.7</td>
<td>Test case ISO7816_H_7</td>
<td>79</td>
</tr>
<tr>
<td>3.3.8</td>
<td>Test case ISO7816_H_8</td>
<td>79</td>
</tr>
<tr>
<td>3.3.9</td>
<td>Test case ISO7816_H_9</td>
<td>80</td>
</tr>
<tr>
<td>3.3.10</td>
<td>Test case ISO7816_H_10</td>
<td>80</td>
</tr>
<tr>
<td>3.3.11</td>
<td>Test case ISO7816_H_11</td>
<td>81</td>
</tr>
<tr>
<td>3.3.12</td>
<td>Test case ISO7816_H_12</td>
<td>81</td>
</tr>
<tr>
<td>3.3.13</td>
<td>Test case ISO7816_H_13</td>
<td>81</td>
</tr>
<tr>
<td>Section</td>
<td>Test Case Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>3.3.14</td>
<td>Test case ISO7816_H_14</td>
<td></td>
</tr>
<tr>
<td>3.3.15</td>
<td>Test case ISO7816_H_15</td>
<td></td>
</tr>
<tr>
<td>3.3.16</td>
<td>Test case ISO7816_H_16</td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Unit ISO7816_I – Chip Authentication (MSE:Set KAT)</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>Unit ISO7816_II – Chip Authentication (MSE:Set AT &amp; GA)</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Unit ISO7816_J – Certificate verification</td>
<td></td>
</tr>
<tr>
<td>3.6.1</td>
<td>Test case ISO7816_J_1</td>
<td></td>
</tr>
<tr>
<td>3.6.2</td>
<td>Test case ISO7816_J_2</td>
<td></td>
</tr>
<tr>
<td>3.6.3</td>
<td>Test case ISO7816_J_3</td>
<td></td>
</tr>
<tr>
<td>3.6.4</td>
<td>Test case ISO7816_J_4</td>
<td></td>
</tr>
<tr>
<td>3.6.5</td>
<td>Test case ISO7816_J_5</td>
<td></td>
</tr>
<tr>
<td>3.6.6</td>
<td>Test case ISO7816_J_6</td>
<td></td>
</tr>
<tr>
<td>3.6.7</td>
<td>Test case ISO7816_J_7</td>
<td></td>
</tr>
<tr>
<td>3.6.8</td>
<td>Test case ISO7816_J_8</td>
<td></td>
</tr>
<tr>
<td>3.6.9</td>
<td>Test case ISO7816_J_9</td>
<td></td>
</tr>
<tr>
<td>3.6.10</td>
<td>Test case ISO7816_J_10</td>
<td></td>
</tr>
<tr>
<td>3.6.11</td>
<td>Test case ISO7816_J_11</td>
<td></td>
</tr>
<tr>
<td>3.6.12</td>
<td>Test case ISO7816_J_12</td>
<td></td>
</tr>
<tr>
<td>3.6.13</td>
<td>Test case ISO7816_J_13</td>
<td></td>
</tr>
<tr>
<td>3.6.14</td>
<td>Test case ISO7816_J_14</td>
<td></td>
</tr>
<tr>
<td>3.6.15</td>
<td>Test case ISO7816_J_15</td>
<td></td>
</tr>
<tr>
<td>3.6.16</td>
<td>Test case ISO7816_J_16</td>
<td></td>
</tr>
<tr>
<td>3.6.17</td>
<td>Test case ISO7816_J_17</td>
<td></td>
</tr>
<tr>
<td>3.6.18</td>
<td>Test case ISO7816_J_18</td>
<td></td>
</tr>
<tr>
<td>3.6.19</td>
<td>Test case ISO7816_J_19</td>
<td></td>
</tr>
<tr>
<td>3.6.20</td>
<td>Test case ISO7816_J_20</td>
<td></td>
</tr>
<tr>
<td>3.6.21</td>
<td>Test case ISO7816_J_21</td>
<td></td>
</tr>
<tr>
<td>3.6.22</td>
<td>Test case ISO7816_J_22</td>
<td></td>
</tr>
<tr>
<td>3.6.23</td>
<td>Test case ISO7816_J_23</td>
<td></td>
</tr>
<tr>
<td>3.6.24</td>
<td>Test case ISO7816_J_24</td>
<td></td>
</tr>
<tr>
<td>3.6.25</td>
<td>Test case ISO7816_J_25</td>
<td></td>
</tr>
<tr>
<td>3.6.26</td>
<td>Test case ISO7816_J_26</td>
<td></td>
</tr>
<tr>
<td>3.6.27</td>
<td>Test case ISO7816_J_27</td>
<td></td>
</tr>
<tr>
<td>3.6.28</td>
<td>Test case ISO7816_J_28</td>
<td></td>
</tr>
<tr>
<td>3.6.29</td>
<td>Test case ISO7816_J_29</td>
<td></td>
</tr>
<tr>
<td>3.6.30</td>
<td>Test case ISO7816_J_30</td>
<td></td>
</tr>
<tr>
<td>3.6.31</td>
<td>Test case ISO7816_J_31</td>
<td></td>
</tr>
<tr>
<td>3.6.32</td>
<td>Test case ISO7816_J_32</td>
<td></td>
</tr>
<tr>
<td>3.6.33</td>
<td>Test case ISO7816_J_33</td>
<td></td>
</tr>
<tr>
<td>3.6.34</td>
<td>Test case ISO7816_J_34</td>
<td></td>
</tr>
<tr>
<td>3.6.35</td>
<td>Test case ISO7816_J_35</td>
<td></td>
</tr>
<tr>
<td>3.6.36</td>
<td>Test case ISO7816_J_36</td>
<td></td>
</tr>
<tr>
<td>3.6.37</td>
<td>Test case ISO7816_J_37</td>
<td></td>
</tr>
<tr>
<td>3.6.38</td>
<td>Test case ISO7816_J_38</td>
<td></td>
</tr>
</tbody>
</table>
3.6.39 Test case ISO7816_J_39 123
3.6.40 Test case ISO7816_J_40 124
3.6.41 Test case ISO7816_J_41 125
3.6.42 Test case ISO7816_J_42 126
3.6.43 Test case ISO7816_J_43 126
3.6.44 Test case ISO7816_J_44 127
3.6.45 Test case ISO7816_J_45 128
3.6.46 Test case ISO7816_J_46 129
3.6.47 Test case ISO7816_J_47 130
3.6.48 Test case ISO7816_J_48 131
3.6.49 Test case ISO7816_J_49 132
3.6.50 Test case ISO7816_J_50 133
3.6.51 Test case ISO7816_J_51 134
3.6.52 Test case ISO7816_J_52 135
3.6.53 Test case ISO7816_J_53 136
3.6.54 Test case ISO7816_J_54 138
3.6.55 Test case ISO7816_J_55 138
3.6.56 Test case ISO7816_J_56 139
3.7 Unit ISO7816_K – Terminal Authentication 140
  3.7.1 Test case ISO7816_K_1 140
  3.7.2 Test case ISO7816_K_2 142
  3.7.3 Test case ISO7816_K_3 143
  3.7.4 Test case ISO7816_K_4 143
  3.7.5 Test case ISO7816_K_5 145
  3.7.6 Test case ISO7816_K_6 146
  3.7.7 Test case ISO7816_K_7 146
  3.7.8 Test case ISO7816_K_8 148
  3.7.9 Test case ISO7816_K_9 148
  3.7.10 Test case ISO7816_K_10 148
  3.7.11 Test case ISO7816_K_11 150
  3.7.12 Test case ISO7816_K_12 150
  3.7.13 Test case ISO7816_K_13 151
  3.7.14 Test case ISO7816_K_14 151
  3.7.15 Test case ISO7816_K_15 152
  3.7.16 Test case ISO7816_K_16 154
  3.7.17 Test case ISO7816_K_17 154
  3.7.18 Test case ISO7816_K_18 156
  3.7.19 Test case ISO7816_K_19 157
  3.7.20 Test case ISO7816_K_20 159
3.8 Unit ISO7816_L – Effective Access Conditions 160
  3.8.1 Test case ISO7816_L_1 160
  3.8.2 Test case ISO7816_L_2 162
  3.8.3 Test case ISO7816_L_3 163
  3.8.4 Test case ISO7816_L_4 165
Test plan for eMRTDs with EACv1

3.8.5 Test case ISO7816_L_5 166
3.8.6 Test case ISO7816_L_6 167
3.8.7 Test case ISO7816_L_7 169
3.8.8 Test case ISO7816_L_8 170
3.8.9 Test case ISO7816_L_9 172
3.8.10 Test case ISO7816_L_10 173
3.8.11 Test case ISO7816_L_11 174
3.8.12 Test case ISO7816_L_12 176
3.8.13 Test case ISO7816_L_13 177
3.8.14 Test case ISO7816_L_14 179
3.8.15 Test case ISO7816_L_15 180
3.8.16 Test case ISO7816_L_16 182
3.9 Unit ISO7816_M – Update mechanism 184
3.9.1 Test case ISO7816_M_1 184
3.9.2 Test case ISO7816_M_2 185
3.9.3 Test case ISO7816_M_3 187
3.9.4 Test case ISO7816_M_4 189
3.9.5 Test case ISO7816_M_5 190
3.9.6 Test case ISO7816_M_6 191
3.10 Unit ISO7816_N – Migration policies 192
3.10.1 Test case ISO7816_N_1 192
4 Tests for layer 7 (LDS) 194
4.1 Unit LDS_E – Data Group 14 194
4.1.1 Test case LDS_E_1 194
4.1.2 Test case LDS_E_2 194
4.1.3 Test case LDS_E_3 194
4.1.4 Test case LDS_E_4 194
4.1.5 Test case LDS_E_5 194
4.2 Unit LDS_F – EF.CVCA 195
4.2.1 Test case LDS_F_1 195
4.3 Unit LDS_G – Data Group 3 196
4.3.1 Test case LDS_G_1 196
4.3.2 Test case LDS_G_2 196
4.3.3 Test case LDS_G_3 196
4.3.4 Test case LDS_G_4 197
4.3.5 Test case LDS_G_5 197
4.3.6 Test case LDS_G_6 197
4.3.7 Test case LDS_G_7 198
4.3.8 Test case LDS_G_8 198
4.3.9 Test case LDS_G_9 199
4.3.10 Test case LDS_G_10 199
4.3.11 Test case LDS_G_11 199
4.4 Unit LDS_H – Data Group 4 200
4.4.1 Test case LDS_H_1 200
1 Introduction

The TR-03105 defines a RF protocol and application test standard for electronic machine readable travel documents (eMRTDs).

This document enhances this test plan for eMRTDs with advanced security mechanisms. These mechanisms are used to protect the additional and more sensitive biometric data like fingerprints introduced with the second generation of eMRTDs.

As the original test plan, this specification has a layer based structure. The layers 1 - 4 refer the RF protocol according to the ISO/IEC 14443 1-4 standard. Since the advanced security mechanisms have no direct influence on this abstraction layer, this amendment does not contain any additional tests for these layers. In the future it may be useful to define an EAC specific test command sequence for the tests of layer 1-4.

However, this document concentrates on the additional tests for the layer 6 (ISO/IEC 7816) and 7 (LDS encoding). For a full conformance test for EAC protected MRTDs, the tests specified in this document MUST be performed in addition to the original tests as described in [R7].

Former version 2.10 of BSI TR-03110 Part 1, which is referred by international standards, is also covered by this test specification.

1.1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>AT</td>
<td>Authentication Template</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
</tr>
<tr>
<td>CA</td>
<td>Chip Authentication</td>
</tr>
</tbody>
</table>
Abbreviation | Full Name
--- | ---
CAN | Card Access Number
CAR | Certification Authority Reference
CHR | Certificate Holder Reference
CVCA | Country Verifying Certification Authority
DG | Data Group
EAC | Extended Access Control
ECDH | Elliptic Curve Diffie-Hellman
ECDSA | Elliptic Curve Digital Signature Algorithm
FID | File Identifier
DH | Diffie-Hellman
DO | Data Object
DST | Digital Signature Template
DV | Document Verifier
ICS | Implementation Conformance Statement
IS | Inspection System
LDS | Logical Data Structure
KAEG | Key Agreement ElGamal-type
KAT | Key Agreement Template
MF | Master File
MSE | Manage Security Environment
OID | Object Identifier
PACE | Password Authenticated Connection Establishment
PSO | Perform Security Operation
RSA | Rivest Shamir Adleman
SFI | Short File Identifier
TA | Terminal Authentication

1.2 Reference documentation

The following documents serve as a reference for this specification:

[R5] PKCS #3: Diffie-Hellman Key-Agreement Standard
[R9] BSI, AFNOR: ADVANCED SECURITY MECHANISMS FOR MACHINE READABLE TRAVEL DOCUMENTS – EXTENDED ACCESS CONTROL (EACv1)
Complementary test methods for MRTDs using static binding
1.3 Terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in [R8].

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUST</td>
<td>This word, or the terms &quot;REQUIRED&quot; or &quot;SHALL&quot;, mean that the definition is an absolute requirement of the specification.</td>
</tr>
<tr>
<td>MUST NOT</td>
<td>This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.</td>
</tr>
<tr>
<td>SHOULD</td>
<td>This word, or the adjective &quot;RECOMMENDED&quot;, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.</td>
</tr>
<tr>
<td>SHOULD NOT</td>
<td>This phrase, or the phrase &quot;NOT RECOMMENDED&quot; mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.</td>
</tr>
<tr>
<td>MAY</td>
<td>This word, or the adjective „OPTIONAL„, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)</td>
</tr>
</tbody>
</table>

2 General test requirements

2.1 Test setup

For setting up these tests, any contactless reader supporting type A and type B protocols can be used. However, this reader has to support extended length APDUs required for Terminal Authentication. One personalized eMRTD sample is needed for executing the tests.

Some of the tests specified for layer 6 (ISO7816) rely on the proper coding of the logical data structure stored in the chip (esp. Data Group 14 and the EF.CVCA file). Therefore it is RECOMMENDED that the layer 7 tests (LDS) are performed before the layer 6 tests to detect coding related issues beforehand.
IMPORTANT NOTE: This test plan contains certain test cases which verify the MRTDs behavior with expired certificates. During these tests, the effective date stored inside the chip is changed. For these tests a set of certificates can be used only once with a single eMRTD sample. After these tests have been performed, another sample or a new set of certificates is needed to repeat the tests. Therefore it is recommended to perform these tests as the last one in a test sequence.

As already mentioned in the introduction of this document, the test cases specified herein have to be performed in addition to the test defined in [R7].

Some of the original test cases will fail with an EAC enabled eMRTD. This is because of the restricted access conditions to the Data Group 3 and Data Group 4. This concerns the following test cases:

ISO7816_B_41
ISO7816_B_42
ISO7816_D_9
ISO7816_D_10
ISO7816_E_9
ISO7816_E_10
LDS_D_06

All these test cases have an established BAC session as a test requirement. For eMRTDs with EAC these tests MUST be performed with an established EAC session. It is RECOMMENDED to perform the BAC tests before the EAC related test cases and to use the DV_CERT_1 and IS_CERT_1 as defined in this document to establish an EAC session when needed.

Most of the test cases in this document require an established PACE or BAC session and a selected ePassport Application as described in [R3] and [R11]. In the preconditions or in the test scenario this procedure is called “Open ePassport Application”. If the Open ePassport Application procedure is performed with PACE the MRZ SHALL be used.

Throughout this document, the term PACE refers to PACEv2.

### 2.2 Test profiles

This test plan refers to the EACv1 specification as described in [R10] and [R11]. The test objects MUST fully comply with this version.

In addition to the profiles already specified in the original test plan this amendment defines the following additional profiles.

<table>
<thead>
<tr>
<th>Profile-ID</th>
<th>Profile</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH</td>
<td>Diffie-Hellman</td>
<td>According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the DH profile are only applicable if the DH algorithm is used.</td>
</tr>
<tr>
<td>ECDH</td>
<td>Elliptic Curve Diffie-Hellman</td>
<td>According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the ECDH profile are only applicable if the elliptic curve based DH algorithm is used.</td>
</tr>
<tr>
<td>TA</td>
<td>Terminal Authentication</td>
<td>In addition to the Chip Authentication mechanism the Terminal Authentication profile is used by MRTDs with sensitive biometric data to protect the file access for the Data Group 3 and/or 4.</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic curve algorithm</td>
<td>According to the EAC specification a chip is free to</td>
</tr>
</tbody>
</table>
### Table: Test Plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Profile-ID</th>
<th>Profile Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>RSA algorithm</td>
<td>According to the EAC specification a chip is free to support either elliptic curve or RSA based keys. All tests which belong to the RSA profile MUST only be processed if the test object is personalized with RSA based keys.</td>
</tr>
<tr>
<td>MIG</td>
<td>Migration</td>
<td>According to the EAC specification the algorithm used for the Terminal Authentication process can be changed with an appropriate link certificate if the chip supports more than one algorithm. The tests for this Migration profile MUST only be performed, if the chip supports the migration from one cryptosystem to another. This must be stated in the ICS.</td>
</tr>
<tr>
<td>DATE</td>
<td>Date validation</td>
<td>Since the validation of the certificates effective and expiration date is not explicitly required by the EAC specification, the optional tests which belong to the Date validation profile must only be performed if this is supported by the chip. This must be stated in the ICS.</td>
</tr>
<tr>
<td>PACE</td>
<td>Password Authenticated Connection Establishment</td>
<td>In some test cases the binding between PACE and Terminal Authentication is tested. In these cases the eMRTD must support the PACE protocol.</td>
</tr>
<tr>
<td>DG3</td>
<td>Data Group 3</td>
<td>According to ICAO Doc 9303 [R2] Data Group 3 is optional. If chip contains encoded fingerprints in DG3 this optional test cases have to be performed.</td>
</tr>
<tr>
<td>DG4</td>
<td>Data Group 4</td>
<td>According to ICAO Doc 9303 [R2] Data Group 4 is optional. If chip contains encoded iris scans in DG4 this optional test cases have to be performed.</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
<td>According to ICAO Doc 9303 [R3] starting on January 1st 2018 eMRTDs may support PACE only.</td>
</tr>
<tr>
<td>EFATR</td>
<td>EF.ATR/INFO</td>
<td>According to ICAO Doc 9303 [R2] file EF.ATR/INFO is optional. If chip supports Extended Length this information and the maximum buffer sizes can be stored in EF.ATR/INFO.</td>
</tr>
<tr>
<td>MF</td>
<td>Master File</td>
<td>According to ICAO Doc 9303 [R2] a Master File is optional. If chip contains MF this must be stated in ICS.</td>
</tr>
</tbody>
</table>

### 2.3 Key pair definition

The certificate sets defined in chapter 2.4 are based on several asymmetric key pairs. In preparation to the tests, these key pairs have to be generated. The parameters used for these keys depend on the initial CVCA private key.

The initial CVCA root private key SHOULD be provided by the eMRTD vendor. It is also possible the eMRTD vendor generates all keys and certificates on its own and passes it to the test operator for the tests.
Test plan for eMRTDs with EACv1

For the key set 13 (CVCA_KEY_13, DV_KEY_13, IS_KEY_13) the algorithm for the cryptosystem migration MUST be used as defined in the ICS. All key pairs MUST be generated independently; therefore it is not permitted to use the same key pair for all sets.

<table>
<thead>
<tr>
<th>Key pair</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVCA_KEY_00</td>
<td>The key pair CV_KEY_00 is the public/private key for the initial CVCA root.</td>
</tr>
<tr>
<td>DV_KEY_01</td>
<td>Key pair of the test DV 01</td>
</tr>
<tr>
<td>IS_KEY_01</td>
<td>Key pair of the test IS 01</td>
</tr>
<tr>
<td>DV_KEY_02</td>
<td>Key pair of the test DV 02</td>
</tr>
<tr>
<td>IS_KEY_02</td>
<td>Key pair of the test IS 02</td>
</tr>
<tr>
<td>DV_KEY_03</td>
<td>Key pair of the test DV 03</td>
</tr>
<tr>
<td>IS_KEY_03</td>
<td>Key pair of the test IS 03</td>
</tr>
<tr>
<td>DV_KEY_04</td>
<td>Key pair of the test DV 04</td>
</tr>
<tr>
<td>IS_KEY_04</td>
<td>Key pair of the test IS 04</td>
</tr>
<tr>
<td>DV_KEY_05</td>
<td>Key pair of the test DV 05</td>
</tr>
<tr>
<td>IS_KEY_05</td>
<td>Key pair of the test IS 05</td>
</tr>
<tr>
<td>DV_KEY_06</td>
<td>Key pair of the test DV 06</td>
</tr>
<tr>
<td>IS_KEY_06</td>
<td>Key pair of the test IS 06</td>
</tr>
<tr>
<td>CVCA_KEY_07</td>
<td>Key pair of the test CVCA 07</td>
</tr>
<tr>
<td>DV_KEY_07</td>
<td>Key pair of the test DV 07</td>
</tr>
<tr>
<td>IS_KEY_07</td>
<td>Key pair of the test IS 07</td>
</tr>
<tr>
<td>CVCA_KEY_08</td>
<td>Key pair of the test CVCA 08</td>
</tr>
<tr>
<td>CVCA_KEY_09</td>
<td>Key pair of the test CVCA 09</td>
</tr>
<tr>
<td>DV_KEY_09</td>
<td>Key pair of the test DV 09</td>
</tr>
<tr>
<td>CVCA_KEY_10</td>
<td>Key pair of the test CVCA 10</td>
</tr>
<tr>
<td>DV_KEY_10</td>
<td>Key pair of the test DV 10</td>
</tr>
<tr>
<td>IS_KEY_10</td>
<td>Key pair of the test IS 10</td>
</tr>
<tr>
<td>CVCA_KEY_11</td>
<td>Key pair of the test CVCA 11</td>
</tr>
<tr>
<td>DV_KEY_11</td>
<td>Key pair of the test DV 11</td>
</tr>
<tr>
<td>IS_KEY_11</td>
<td>Key pair of the test IS 11</td>
</tr>
<tr>
<td>DV_KEY_12</td>
<td>Key pair of the test DV 12</td>
</tr>
<tr>
<td>CVCA_KEY_13</td>
<td>Key pair of the test CVCA 13</td>
</tr>
<tr>
<td>DV_KEY_13</td>
<td>Key pair of the test DV 13</td>
</tr>
<tr>
<td>IS_KEY_13</td>
<td>Key pair of the test IS 13</td>
</tr>
<tr>
<td>DV_KEY_14a</td>
<td>Key pair of the test DV 14 (length equal to CVCA Key length)</td>
</tr>
<tr>
<td>DV_KEY_14b</td>
<td>Key pair of the test DV 14 (MUST be shorter than CVCA Key length)</td>
</tr>
<tr>
<td>IS_KEY_14a</td>
<td>Key pair of the test IS 14 (length equal to CVCA Key length)</td>
</tr>
<tr>
<td>IS_KEY_14b</td>
<td>Key pair of the test IS 14 (MUST be shorter than CVCA Key length)</td>
</tr>
</tbody>
</table>

2.4 Certificate specification

Since the advanced security mechanisms are using a certificate based authentication schema it is necessary to provide a set of well prepared certificates in order to perform all tests.
This chapter defines the exact set of certificates referred in the tests. Besides the regular certificate chain there is also the need for special encoded certificates.

The certificates are specified in two different ways. For providers of personalized eMRTD samples, which do already have a preconfigured trust point based on their own CVCA key pair, the chapters below define a set of certificates relative to the effective date (CVCA\text{eff}) and expiration date (CVCA\text{exp}) of the given the CVCA. The time span between CVCA\text{eff} and CVCA\text{exp} MUST be at least two month to allow proper adoption of the certificate time scheme defined below. The “current date” of the provided sample MUST be set to CVCA\text{eff} before the tests are started. The provider of the sample or the test laboratory has to generate the corresponding certificate according to this specification based on the CVCA data.

If no preconfigured key pair is available or if the production process allows the use of an externally defined CVCA, a certificate set can be used which is defined as a “worked example” by this specification. This set is provided for ECDSA, RSA and RSAPSS based certificates and is defined in a full binary form with fixed keys and dates. It also includes a definition for an initial CVCA key pair and its effective and expiry dates.

### 2.4.1 Certificate Set 1

The certificate set consist of a regular certificate chain (DV -> IS) which is used for the positive tests regarding the certificate verification. Furthermore it contains variants of the original DV certificate to simulate a variety of certificate coding issues (missing elements, badly encoded dates …).

#### 2.4.1.1 DV\_CERT\_1

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
</tbody>
</table>

The DV\_CERT\_1 SHOULD also be used for all other test cases that rely on a established EAC session to access DG3 and DG4 (like the LDS unit G and H, or the BAC test cases mentioned in 2.1).

<table>
<thead>
<tr>
<th>Content definition</th>
<th>7F 21 aa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td></td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

aa is the encoded combined length of certificate body and signature objects

bb is the encoded length the certificate body object
**cc** is the encoded length of the Certification Authority Reference  
**dd** is the placeholder for the Certification Authority Reference (cc bytes)  
**ee** is the encoded length of the certificates public key,  
**ff** is the placeholder for the certificates public key bytes (ee bytes),  
**xx** is the encoded length of the Certificate Holder Reference  
**yy** is the placeholder for the Certificate Holder Reference (xx bytes)  
**gg** is the placeholder for the BCD encoded effective date of the certificate  
**hh** is the placeholder for the BCD encoded expiration date of the certificate  
**ii** is the encoded length of the certificates signature object,  
**jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td>DETESTDVDDE001</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate Holder Authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td></td>
<td>CVCAeff</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td></td>
<td>CVCAeff + 1 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td></td>
<td>Public key of key pair DV_KEY_01</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td></td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

### 2.4.1.2 DV_CERT_1a

**ID**  
DV_CERT_1a

**Purpose**  
This certificate is similar to DV_CERT_1, but does not contain a Certificate Holder Authorization

**Version**  
1.11

**Referred by**  
ISO7816 J 6

**Content definition**

```
7F 21 aa
  7F 4E bb
  5F 29 01 00
  42 cc dd
  7F 49 ee ff
  5F 20 xx yy
  5F 25 06 gg
  5F 24 06 hh
  5F 37 ii jj
```

**aa** is the encoded combined length of certificate body and signature objects  
**bb** is the encoded length the certificate body object  
**cc** is the encoded length of the Certification Authority Reference  
**dd** is the placeholder for the Certification Authority Reference (cc bytes)  
**ee** is the encoded length of the certificates public key,  
**ff** is the placeholder for the certificates public key bytes (ee bytes),  
**xx** is the encoded length of the Certificate Holder Reference  
**yy** is the placeholder for the Certificate Holder Reference (xx bytes)  
**gg** is the placeholder for the BCD encoded effective date of the certificate  
**hh** is the placeholder for the BCD encoded expiration date of the certificate  
**ii** is the encoded length of the certificates signature object,  
**jj** is the placeholder for the certificates signature (ii bytes)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorization</td>
<td>absent</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.3 DV_CERT_1b

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but does not contain a Certificate Effective Date</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_7</td>
</tr>
</tbody>
</table>
| Content definition | 7F 21 aa  
  7F 4E bb  
  5F 29 01 00  
  42 cc dd  
  7F 49 ee ff  
  5F 20 xx yy  
  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83  
  5F 24 06 hh  
  5F 37 ii jj |

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)
### 2.4.1.4 DV_CERT_1c

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but does not contain a Certificate Expiration Date</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_8</td>
</tr>
<tr>
<td>Content</td>
<td>7F 21 (aa)</td>
</tr>
<tr>
<td></td>
<td>7F 4E (bb)</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 (cc) (dd)</td>
</tr>
<tr>
<td></td>
<td>7F 49 (ee) (ff)</td>
</tr>
<tr>
<td></td>
<td>5F 20 (xx) (yy)</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00</td>
</tr>
<tr>
<td></td>
<td>7F 00 07 03 01 02 01 53</td>
</tr>
<tr>
<td></td>
<td>01 83</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 (gg)</td>
</tr>
<tr>
<td></td>
<td>5F 37 (ii) (jj)</td>
</tr>
</tbody>
</table>

\(aa\) is the encoded combined length of certificate body and signature objects
\(bb\) is the encoded length the certificate body object
\(cc\) is the encoded length of the Certification Authority Reference
\(dd\) is the placeholder for the Certification Authority Reference (cc bytes)
\(ee\) is the encoded length of the certificates public key,
\(ff\) is the placeholder for the certificates public key bytes (ee bytes),
\(xx\) is the encoded length of the Certificate Holder Reference
\(yy\) is the placeholder for the Certificate Holder Reference (xx bytes)
\(gg\) is the placeholder for the BCD encoded effective date of the certificate
\(ii\) is the encoded length of the certificates signature object,
\(jj\) is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorization</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>absent</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.5 DV_CERT_1d

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1d</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid BCD encoding)</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_9</td>
</tr>
<tr>
<td>Content</td>
<td>7F 21 (aa)</td>
</tr>
<tr>
<td></td>
<td>7F 4E (bb)</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 (cc) (dd)</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>7F 49 ee ff</th>
</tr>
</thead>
<tbody>
<tr>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
</tr>
<tr>
<td>5F 25 06 0A 0B 0C 0D 0E 0F</td>
</tr>
<tr>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

**Parameter**
| Certification Authority Reference | As defined by the CVCA |
| Certificate Holder Reference | DETESTDVDE001 |
| Certificate Holder Authorisation | domestic DV, DG 3, DG 4 |
| Certificate effective date | 0A 0B 0C 0D 0E 0F (invalid BCD encoding) |
| Certificate expiration date | CVCA_{eff} + 1 month |
| Public Key reference | Public key of key pair DV_KEY_01 |
| Signing Key reference | Signed with the private key of key pair CVCA_KEY_00 |

### 2.4.1.6 DV_CERT_1e

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date (Invalid BCD encoding)</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_10</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa</td>
</tr>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 0A 0B 0C 0D 0E 0F</td>
</tr>
<tr>
<td></td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{\text{eff}}</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>0A 0B 0C 0D 0E 0F (invalid BCD encoding)</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

### 2.4.1.7 DV_CERT_1f

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1f</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid Gregorian date)</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816_J_19</td>
</tr>
</tbody>
</table>
| **Content definition** | 7F 21 \(aa\)  
7F 4E \(bb\)  
5F 29 01 00  
42 \(cc\) \(dd\)  
7F 49 \(ee \(ff\)\)  
5F 20 \(xx \(yy\)\)  
7F 4C 0E 09 04 00 7F 00 07 03 01 02 01 53 01 83  
5F 25 06 \(gg\)  
5F 24 06 \(hh\)  
5F 37 \(ii \(jj\)\)  |

\(aa\) is the encoded combined length of certificate body and signature objects  
\(bb\) is the encoded length the certificate body object  
\(cc\) is the encoded length of the Certification Authority Reference  
\(dd\) is the placeholder for the Certification Authority Reference (cc bytes)  
\(ee\) is the encoded length of the certificates public key,  
\(ff\) is the placeholder for the certificates public key bytes (ee bytes),  
\(xx\) is the encoded length of the Certificate Holder Reference  
\(yy\) is the placeholder for the Certificate Holder Reference (xx bytes)  
\(gg\) is the placeholder for the BCD encoded effective date of the certificate  
\(hh\) is the placeholder for the BCD encoded expiration date of the certificate  
\(ii\) is the encoded length of the certificates signature object,  
\(jj\) is the placeholder for the certificates signature (ii bytes)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>The month and the year used as defined by the CVCAeff and the day is always set to the 32nd so that it becomes an invalid Gregorian date.</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAexp</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.8 DV_CERT_1g

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date (Invalid Gregorian date)</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_20</td>
</tr>
<tr>
<td>Content definition</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7F 21 aa</th>
<th>7F 4E bb</th>
</tr>
</thead>
<tbody>
<tr>
<td>5F 29 01 00</td>
<td>42 cc dd</td>
</tr>
<tr>
<td>7F 49 ee ff</td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td>5F 24 06 hh</td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

**Content definition**

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)
<table>
<thead>
<tr>
<th>Certificate expiration date</th>
<th>The month and the year used as defined by the CVCA\text{\textsubscript{eff}} and the day is always set to the 32\textsuperscript{nd} so that it becomes an invalid Gregorian date.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

### 2.4.1.9 DV\_CERT\_1h

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a Certificate Expiration Date BEFORE the Certificate Effective Date</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_21</td>
</tr>
</tbody>
</table>

#### Content definition

- \text{7F 21 aa}
- \text{7F 4E bb}
- \text{5F 29 01 00}
- \text{42 cc dd}
- \text{7F 49 ee ff}
- \text{5F 20 xx yy}
- \text{7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83}
- \text{5F 25 06 gg}
- \text{5F 24 06 hh}
- \text{5F 37 ii jj}

\text{aa} is the encoded combined length of certificate body and signature objects  
\text{bb} is the encoded length the certificate body object  
\text{cc} is the encoded length of the Certification Authority Reference  
\text{dd} is the placeholder for the Certification Authority Reference (cc bytes)  
\text{ee} is the encoded length of the certificates public key,  
\text{ff} is the placeholder for the certificates public key bytes (ee bytes),  
\text{xx} is the encoded length of the Certificate Holder Reference  
\text{yy} is the placeholder for the Certificate Holder Reference (xx bytes)  
\text{gg} is the placeholder for the BCD encoded effective date of the certificate  
\text{hh} is the placeholder for the BCD encoded expiration date of the certificate  
\text{ii} is the encoded length of the certificates signature object,  
\text{jj} is the placeholder for the certificates signature (ii bytes)

#### Parameter

<table>
<thead>
<tr>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA\text{\textsubscript{eff}} + 1 day</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA\text{\textsubscript{eff}}</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>
### 2.4.1.10 DV_CERT_1i

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a Certificate Holder Authorization with an invalid OID</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>7F 21 aa</code></td>
</tr>
<tr>
<td><code>7F 4E bb</code></td>
</tr>
<tr>
<td><code>5F 29 01 00</code></td>
</tr>
<tr>
<td><code>42 cc dd</code></td>
</tr>
<tr>
<td><code>7F 49 ee ff</code></td>
</tr>
<tr>
<td><code>5F 20 xx yy</code></td>
</tr>
<tr>
<td><code>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 01 83</code></td>
</tr>
<tr>
<td><code>5F 25 06 gg</code></td>
</tr>
<tr>
<td><code>5F 24 06 hh</code></td>
</tr>
<tr>
<td><code>5F 37 ii jj</code></td>
</tr>
</tbody>
</table>

- `aa` is the encoded combined length of certificate body and signature objects
- `bb` is the encoded length the certificate body object
- `cc` is the encoded length of the Certification Authority Reference
- `dd` is the placeholder for the Certification Authority Reference (cc bytes)
- `ee` is the encoded length of the certificates public key,
- `ff` is the placeholder for the certificates public key bytes (ee bytes),
- `xx` is the encoded length of the Certificate Holder Reference
- `yy` is the placeholder for the Certificate Holder Reference (xx bytes)
- `gg` is the placeholder for the BCD encoded effective date of the certificate
- `hh` is the placeholder for the BCD encoded expiration date of the certificate
- `ii` is the encoded length of the certificates signature object,
- `jj` is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff+1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.11 DV_CERT_1j

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_1j</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is similar to DV_CERT_1, but contains a Public Key with an invalid OID</td>
</tr>
<tr>
<td>Version</td>
<td>1.12</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>7F 21 aa</code></td>
</tr>
<tr>
<td><code>7F 4E bb</code></td>
</tr>
</tbody>
</table>
aa is the encoded combined length of certificate body and signature objects  
b b is the encoded length the certificate body object  
cc is the encoded length of the Certification Authority Reference  
d d is the placeholder for the Certification Authority Reference (cc bytes)  
ee is the encoded length of the certificates public key,  
ff is the placeholder for the certificates public key bytes (ee bytes),  
xx is the encoded length of the Certificate Holder Reference  
yy is the placeholder for the Certificate Holder Reference (xx bytes)  
ii is the placeholder for the BCD encoded effective date of the certificate  
jj is the placeholder for the BCD encoded expiration date of the certificate  
ij is the encoded length of the certificates signature object,  
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE001</td>
<td></td>
</tr>
<tr>
<td>Certificate Public Key</td>
<td>Bad OID (Use 0.4.0.127.0.7.2.2.5.1)</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_01</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.12 IS_CERT_1

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_1</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
</tbody>
</table>
| Referred by | ISO7816_J_1, ISO7816_J_2, ISO7816_J_3, ISO7816_J_4, ISO7816_J_5,  
ISO7816_J_6, ISO7816_J_7, ISO7816_J_8, ISO7816_J_9, ISO7816_J_10,  
ISO7816_J_17, ISO7816_J_18, ISO7816_J_19, ISO7816_J_20, ISO7816_J_21,  
ISO7816_J_22, ISO7816_J_23, ISO7816_J_24, ISO7816_K, ISO7816_L_9,  
ISO7816_L_10, ISO7816_L_11, ISO7816_L_12, ISO7816_L_13 |
| Content definition | 7F 21  aa  
7F 4E  bb  
5F 29 01 00  
42  cc  dd  
7F 49  ee  ff  
5F 20  xx  yy |
### 2.4.2 Certificate Set 2

This certificate set contains certificates which are used to verify the behavior of ePassports in respect to foreign IS certificates.

#### 2.4.2.1 DV_CERT_2

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_11</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa</td>
</tr>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00</td>
</tr>
<tr>
<td></td>
<td>7F 00 07 03 01 02 01 53 01 03</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 hh</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE002</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorization</td>
<td>foreign DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_eff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_eff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_02</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

#### 2.4.2.2 IS_CERT_2a

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_2a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an advanced effective date. (Beyond the expiration date of IS_CERT_2b).</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_11</td>
</tr>
</tbody>
</table>

| Content definition| 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj |

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)
**2.4.2.3 IS_CERT_2b**

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_2b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an expiration date BEFORE the effective date of IS_CERT_2a.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>7F 21 aa 7F 4E bb</td>
</tr>
<tr>
<td>5F 29 01 00</td>
</tr>
<tr>
<td>42 cc dd</td>
</tr>
<tr>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03</td>
</tr>
<tr>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE002</td>
</tr>
</tbody>
</table>
2.4.3 Certificate Set 3

The certificate set follows a certification scheme where the DV permits full access to Data Group 3 and Data Group 4 while the IS certificate restricts the access to specific Data Group.

2.4.3.1 DV_CERT_3

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular DV certificate, with access rights for Data Group 3 AND 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_L_1, ISO7816_L_2, ISO7816_L_3, ISO7816_L_4</td>
</tr>
</tbody>
</table>
| Content definition | 7F 21 aa  
7F 4E bb  
5F 29 01 00  
42 cc dd  
7F 49 ee ff  
5F 20 xx yy  
7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83  
5F 25 06 gg  
5F 24 06 hh  
5F 37 ii jj |

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
iis the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE003</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_03</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>IS_CERT_3a</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for Data Group 3 only.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816_L_1, ISO7816_L_2</td>
</tr>
<tr>
<td><strong>Content definition</strong></td>
<td>7F 21  aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 01 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
<tr>
<td><strong>aa</strong></td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td><strong>bb</strong></td>
<td>is the encoded length the certificate body object</td>
</tr>
<tr>
<td><strong>cc</strong></td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td><strong>dd</strong></td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td><strong>ee</strong></td>
<td>is the encoded length of the certificates public key</td>
</tr>
<tr>
<td><strong>ff</strong></td>
<td>is the placeholder for the certificates public key bytes (ee bytes)</td>
</tr>
<tr>
<td><strong>xx</strong></td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td><strong>yy</strong></td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes)</td>
</tr>
<tr>
<td><strong>gg</strong></td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td><strong>hh</strong></td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td><strong>ii</strong></td>
<td>is the encoded length of the certificates signature object</td>
</tr>
<tr>
<td><strong>jj</strong></td>
<td>is the placeholder for the certificates signature (ii bytes)</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td>Certification Authority Reference  DETESTDVDE003</td>
</tr>
<tr>
<td><strong>Certificate Holder Reference</strong></td>
<td>DETESTISDE003</td>
</tr>
<tr>
<td><strong>Certificate Holder Authorisation</strong></td>
<td>IS, DG 3</td>
</tr>
<tr>
<td><strong>Certificate effective date</strong></td>
<td>CVCA_{eff}</td>
</tr>
<tr>
<td><strong>Certificate expiration date</strong></td>
<td>CVCA_{eff} + 1 month</td>
</tr>
<tr>
<td><strong>Public Key reference</strong></td>
<td>Public key of key pair IS_KEY_03</td>
</tr>
<tr>
<td><strong>Signing Key reference</strong></td>
<td>Signed with the private key of key pair DV_KEY_03</td>
</tr>
</tbody>
</table>

### 2.4.3.3 IS_CERT_3b

<table>
<thead>
<tr>
<th><strong>ID</strong></th>
<th>IS_CERT_3b</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for Data Group 4 only.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

#### Referred by
ISO7816_L_3, ISO7816_L_4

<table>
<thead>
<tr>
<th>Content definition</th>
<th>7F 21 aa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 02</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td></td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

*aa* is the encoded combined length of certificate body and signature objects
*bb* is the encoded length the certificate body object
*cc* is the encoded length the Certification Authority Reference
*dd* is the placeholder for the Certification Authority Reference (cc bytes)
*ee* is the encoded length of the certificates public key,
*ff* is the placeholder for the certificates public key bytes (ee bytes),
*xx* is the encoded length of the Certificate Holder Reference
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)
*gg* is the placeholder for the BCD encoded effective date of the certificate
*hh* is the placeholder for the BCD encoded expiration date of the certificate
*ii* is the encoded length of the certificates signature object,
*jj* is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTDVDE003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE003</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_03</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV_KEY_03</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.4 Certificate Set 4

The certificate set follows a certification scheme where the DV permits only access to Data Group 3 while the IS certificate permits full access to Data Group 3 and Data Group 4.

#### 2.4.4.1 DV_CERT_4

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular DV certificate, with access rights for group 3 only.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_L_5, ISO7816_L_6</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa</td>
</tr>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
</tbody>
</table>
aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
c is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE004</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>Domestic DV, DG 3</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_04</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key pair</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.4.2 IS_CERT_4

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_4. It encodes access rights for Data Group 3 AND Data Group 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_L_5, ISO7816_L_6</td>
</tr>
</tbody>
</table>
| Content definition | 7F 21 aa

aa is the encoded combined length of certificate body and signature objects
2.4.5 Certificate Set 5

The certificate set follows a certification scheme where the DV permits only access to Data Group 4 while the IS certificate permits full access to Data Group 3 and Data Group 4.

2.4.5.1 DV_CERT_5

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular DV certificate, with access rights for group 4 only.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_L_7, ISO7816_L_8</td>
</tr>
</tbody>
</table>

**Content definition:**

```
7F 21 aa
  7F 4E bb
    5F 29 01 00
    42 cc dd
    7F 49 ee ff
    5F 20 xx yy
    7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 82
    5F 25 06 gg
    5F 24 06 hh
    5F 37 ii jj
```

*aa* is the encoded combined length of certificate body and signature objects
*bb* is the encoded length of certificate body object
*cc* is the encoded length of the Certification Authority Reference
*dd* is the placeholder for the Certification Authority Reference (cc bytes)
*ee* is the encoded length of the certificates public key,
*ff* is the placeholder for the certificates public key bytes (ee bytes),
*xx* is the encoded length of the Certificate Holder Reference
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)
*gg* is the placeholder for the BCD encoded effective date of the certificate
*hh* is the placeholder for the BCD encoded expiration date of the certificate
*ii* is the encoded length of the certificates signature object,
*jj* is the placeholder for the certificates signature (ii bytes)
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE005</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_05</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

2.4.5.2 **IS_CERT_5**

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_5. It encodes access rights for Data Group 3 AND Data Group 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_L_7, ISO7816_L_8</td>
</tr>
</tbody>
</table>

| Content definition | 7F 21 aa  |
|                   | 7F 4E bb  |
|                   | 5F 29 01 00 |
|                   | 42 cc dd  |
|                   | 7F 49 ee ff |
|                   | 5F 20 xx yy |
|                   | 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 |
|                   | 5F 25 06 gg |
|                   | 5F 24 06 hh |
|                   | 5F 37 ii jj |

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTDVDE005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE005</td>
<td></td>
</tr>
</tbody>
</table>
2.4.6 Certificate Set 6

This certificate set contains certificates which have different effective and expiration dates to test the ePassports behavior in respect to the update of the effective date and with expired certificates.

2.4.6.1 DV_CERT_6

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>DV_CERT_6</td>
</tr>
<tr>
<td>Purpose</td>
<td>This certificate is a domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_1, ISO7816_M_2</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

| aa                        | is the encoded combined length of certificate body and signature objects |
| bb                        | is the encoded length the certificate body object                      |
| cc                        | is the encoded length of the Certification Authority Reference         |
| dd                        | is the placeholder for the Certification Authority Reference (cc bytes) |
| ee                        | is the encoded length of the certificates public key                   |
| ff                        | is the placeholder for the certificates public key bytes (ee bytes)    |
| xx                        | is the encoded length of the Certificate Holder Reference              |
| yy                        | is the placeholder for the Certificate Holder Reference (xx bytes)     |
| gg                        | is the placeholder for the BCD encoded effective date of the certificate|
| hh                        | is the placeholder for the BCD encoded expiration date of the certificate|
| ii                        | is the encoded length of the certificates signature object             |
| jj                        | is the placeholder for the certificates signature (ii bytes)           |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE006</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff}</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff}+1 month</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_06</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

#### 2.4.6.2 DV_CERT_6a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_6a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This DV certificate is similar to DV_CERT_6, but the certificate effective date is beyond the DV_CERT_6 expiration date.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_2</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa</td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE006</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 1 day</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 2 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_06</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

#### 2.4.6.3 IS_CERT_6a

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_6a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an advanced effective date. (Beyond the expiration date of IS_CERT_6b)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Test plan for eMRTDs with EACv1**

<table>
<thead>
<tr>
<th>Version</th>
<th>1.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referred by</td>
<td>ISO7816_M_1</td>
</tr>
<tr>
<td>Content definition</td>
<td></td>
</tr>
</tbody>
</table>

```
7F 21  aa
  7F 4E  bb
  5F 29  01 00
  42  cc  dd
  7F 49  ee  ff
  5F 20  xx  yy
  7F 4C  0E 06 09 04 00 7F 00 07 03 01 02 01 03
  5F 25  06  gg
  5F 24  06  hh
  5F 37  ii  jj
```

(aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTDVDE006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE006</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 14 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_06</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV_KEY_06</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.6.4 IS_CERT_6b

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_6b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an expiration date BEFORE the effective date of IS_CERT_6a.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_1</td>
</tr>
<tr>
<td>Content definition</td>
<td></td>
</tr>
</tbody>
</table>

```
7F 21  aa
  7F 4E  bb
  5F 29  01 00
  42  cc  dd
  7F 49  ee  ff
  5F 20  xx  yy
```

36/207
### 2.4.7 Certificate Set 7

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

#### 2.4.7.1 LINK_CERT_7

Note for ECDSA profile: Since the crypto mechanism is not changed by this link certificate it must be stated by the vendor of the test sample if the domain parameter should be included in this certificate (see ICS Annex A).

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a link certificate, which validity period starts one day before the original CVCA certificate expires.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_3</td>
</tr>
</tbody>
</table>
| Content definition | 7F 21 aa  
7F 4E bb  
5F 29 01 00  
42 cc dd  
7F 49 ee ff  
5F 20 xx yy |
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETEST_LINKDE007</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>CVCA, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAexp - 1 day</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAexp + 2 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair CVCA_KEY_07</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

#### 2.4.7.2 DV_CERT_7a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_7a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a domestic DV certificate, which was issued by the original CVCA.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
<th>7F 21</th>
<th>aa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7F 4E</td>
<td>bb</td>
</tr>
<tr>
<td></td>
<td>5F 29</td>
<td>01 00</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49</td>
<td>ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20</td>
<td>xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C</td>
<td>0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
</tr>
<tr>
<td></td>
<td>5F 25</td>
<td>06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24</td>
<td>06 hh</td>
</tr>
<tr>
<td></td>
<td>5F 37</td>
<td>ii jj</td>
</tr>
</tbody>
</table>

`aa` is the encoded combined length of certificate body and signature objects  
`bb` is the encoded length the certificate body object  
`cc` is the encoded length of the Certification Authority Reference  
`dd` is the placeholder for the Certification Authority Reference (cc bytes)  
`ee` is the encoded length of the certificates public key,  
`ff` is the placeholder for the certificates public key bytes (ee bytes),  
`xx` is the encoded length of the Certificate Holder Reference  
`yy` is the placeholder for the Certificate Holder Reference (xx bytes)  
`gg` is the placeholder for the BCD encoded effective date of the certificate  
`hh` is the placeholder for the BCD encoded expiration date of the certificate  
`ii` is the encoded length of the certificates signature object,  
`jj` is the placeholder for the certificates signature (ii bytes)
**Test plan for eMRTDs with EACv1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE007</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCEff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCExp</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_07</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.7.3 DV_CERT_7b

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_7b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a domestic DV certificate, which was issued by the update CVCA (LINK_CERT_7).</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_3</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETEST_LINKDE007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE007</td>
<td></td>
</tr>
</tbody>
</table>
### Certificate Set 8

This certificate set defines a link certificate used for the trust point update mechanism tests. Note for ECDSA profile: Since the crypto mechanism is not changed by the link certificates defined in this certificate set, it must be stated by the vendor of the test sample if the domain parameter should be included (see ICS Annex A).

#### 2.4.8.1 LINK_CERT_8

This link certificate is used to update the trust point defined by LINK_CERT_7.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETEST_LINKDE007</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETEST_LINKDE008</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>CVCA, DG 3, DG 4</td>
</tr>
</tbody>
</table>

#### Table for Certificate Set 8

<table>
<thead>
<tr>
<th>Certificate Holder Authorisation</th>
<th>domestic DV, DG 3, DG 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{exp} + 1 day</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{exp} + 1 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_07</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_07</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a link certificate, based on the LINK_CERT_7</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_4</td>
</tr>
</tbody>
</table>

**Content definition**

```
01 00 42 cc dd
7F 49 ee ff
5F 20 xx yy
7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
5F 25 06 gg
5F 24 06 hh
5F 37 ii jj
```

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETEST_LINKDE008</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTCADE009</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>CVCA, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{exp} + 3 month</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{exp} + 6 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair CVCA_KEY_09</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_08</td>
</tr>
</tbody>
</table>

### 2.4.9 Certificate Set 9

#### 2.4.9.1 LINK_CERT_9

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a link certificate, based on the LINK_CERT_8</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_4</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)
### 2.4.9.2 DV_CERT_9

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a domestic DV certificate, which was issued by LINK_CERT_9.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_4</td>
</tr>
</tbody>
</table>

**Content definition**

```
7F 21 aa
  7F 4E bb
    5F 29 01 00
    42 cc dd
    7F 49 ee ff
    5F 20 xx yy
    7F 4C 0E 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
    5F 24 06 hh
  5F 37 ii jj
```

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)

**Parameter**

- Certification Authority Reference: DETESTCADE009  
- Certificate Holder Reference: DETESTDVDE009  
- Certificate Holder Authorisation: domestic DV, DG 3, DG 4  
- Certificate effective date: CVCA<sub>exp</sub> + 3 month  
- Certificate expiration date: CVCA<sub>exp</sub> + 4 month  
- Public Key reference: Public key of key pair DV_KEY_09  
- Signing Key reference: Signed with the private key of key pair CVCA_KEY_09

### 2.4.10 Certificate Set 10

#### 2.4.10.1 LINK_CERT_10

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular CVCA certificate. The signing key is a DV key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_44, ISO7816_J_45</td>
</tr>
<tr>
<td>Content</td>
<td>7F 21 aa</td>
</tr>
</tbody>
</table>
### 2.4.10.2 DV_CERT_10a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_10a</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816 J_44, ISO7816 J_46, ISO7816 J_47</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>7F 4E bb</strong></td>
</tr>
<tr>
<td></td>
<td><strong>5F 29 01 00</strong></td>
</tr>
<tr>
<td></td>
<td><strong>42 cc dd</strong></td>
</tr>
<tr>
<td></td>
<td><strong>7F 49 ee ff</strong></td>
</tr>
<tr>
<td></td>
<td><strong>5F 20 xx yy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3</strong></td>
</tr>
<tr>
<td></td>
<td><strong>5F 25 06 gg</strong></td>
</tr>
<tr>
<td></td>
<td><strong>5F 24 06 hh</strong></td>
</tr>
<tr>
<td></td>
<td><strong>5F 37 ii jj</strong></td>
</tr>
</tbody>
</table>

- aa is the encoded combined length of certificate body and signature objects
- bb is the encoded length the certificate body object
- cc is the encoded length of the Certification Authority Reference
- dd is the placeholder for the Certification Authority Reference (cc bytes)
- ee is the encoded length of the certificates public key,
- ff is the placeholder for the certificates public key bytes (ee bytes),
- xx is the encoded length of the Certificate Holder Reference
- yy is the placeholder for the Certificate Holder Reference (xx bytes)
- gg is the placeholder for the BCD encoded effective date of the certificate
- hh is the placeholder for the BCD encoded expiration date of the certificate
- ii is the encoded length of the certificates signature object,
- jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTDVDE010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td>As defined by the initial CVCA root</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td></td>
<td>CVCA, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td></td>
<td>CVCAeff</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td></td>
<td>CVCAexp</td>
</tr>
<tr>
<td>Public Key reference</td>
<td></td>
<td>Public key of key pair CVCA_KEY_00</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td></td>
<td>Signed with the private key of key pair DV_KEY_10</td>
</tr>
</tbody>
</table>
### 2.4.10.3 DV_CERT_10b

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Certification Authority Reference</strong></th>
<th><strong>Certificate Holder Reference</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
<td>DETESTDVDE010</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td></td>
<td>CVCAeff</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td></td>
<td>CVCAeff + 1 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td></td>
<td>Public key of key pair DV_KEY_10</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td></td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

#### Content definition

<p>| | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7F 21</td>
<td>aa</td>
<td></td>
<td>7F 4E</td>
<td>bb</td>
<td></td>
<td>5F 29</td>
<td>01 00</td>
<td></td>
<td>42</td>
<td>cc dd</td>
<td></td>
<td>7F 49</td>
<td>ee ff</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7F 4C</td>
<td>0E 06</td>
<td>09 04</td>
<td>00 7F</td>
<td>00 07</td>
<td>03 01</td>
<td>02 01</td>
<td>53 01</td>
<td>43</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5F 25</td>
<td>06 gg</td>
<td></td>
<td>5F 24</td>
<td>06 hh</td>
<td></td>
<td>5F 37</td>
<td>ii jj</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ID** DV_CERT_10b

**Purpose**

This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.

**Version**

1.11

**Referred by**

ISO7816_J_45, ISO7816_J_48, ISO7816_J_49

### Test plan for eMRTDs with EACv1

- **5F 24 06 hh**
- **5F 37 ii jj**

**aa** is the encoded combined length of certificate body and signature objects

**bb** is the encoded length the certificate body object

**cc** is the encoded length of the Certification Authority Reference

**dd** is the placeholder for the Certification Authority Reference (cc bytes)

**ee** is the encoded length of the certificates public key,

**ff** is the placeholder for the certificates public key bytes (ee bytes),

**xx** is the encoded length of the Certificate Holder Reference

**yy** is the placeholder for the Certificate Holder Reference (xx bytes)

**gg** is the placeholder for the BCD encoded effective date of the certificate

**hh** is the placeholder for the BCD encoded expiration date of the certificate

**ii** is the encoded length of the certificates signature object,

**jj** is the placeholder for the certificates signature (ii bytes)
2.4.10.4 DV_CERT_10c

**ID:** DV_CERT_10c

**Purpose:**
This certificate is an irregular DV domestic certificate. The signing key is a DV key.

**Version:** 1.11

**Referred by:**
ISO7816_J_46, ISO7816_J_48

**Content definition:**

```
7F 21 aa
   7F 4E bb
      5F 29 01 00
      42 cc dd
      7F 49 ee ff
      5F 20 xx yy
      7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
      5F 25 06 gg
      5F 24 06 hh
      5F 37 ii jj
```

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority</td>
<td>DETESTDVDE010</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>foreign DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_10</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

| Certificate Holder Authorisation | domestic DV, DG 3, DG 4 |
| Certificate effective date       | CVCA_{eff}              |
| Certificate expiration date      | CVCA_{eff} + 1 month    |
| Public Key reference             | Public key of key pair DV_KEY_10 |
| Signing Key reference            | Signed with the private key of key pair DV_KEY_10 |

### 2.4.10.5 DV_CERT_10d

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>DV_CERT_10d</td>
</tr>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular DV foreign certificate. The signing key is a DV key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_47, ISO7816_J_49</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

Parameter | Value
---|---
Certification Authority Reference | DETESTDVDE010
Certificate Holder Reference | DETESTDVDE110
Certificate Holder Authorisation | foreign DV, DG 3, DG 4
Certificate effective date | CVCA_{eff}
Certificate expiration date | CVCA_{eff} + 1 month
Public Key reference | Public key of key pair DV_KEY_10
Signing Key reference | Signed with the private key of key pair DV_KEY_10
2.4.10.6  IS_CERT_10

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_10</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>This certificate is an irregular domestic IS certificate. This IS certificate is signed by the CVCA key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_43</td>
</tr>
</tbody>
</table>

**Content definition**

- **aa**: the encoded combined length of certificate body and signature objects
- **bb**: the encoded length the certificate body object
- **cc**: the encoded length of the Certification Authority Reference
- **dd**: the placeholder for the Certification Authority Reference (cc bytes)
- **ee**: the encoded length of the certificates public key,
- **ff**: the placeholder for the certificates public key bytes (ee bytes),
- **xx**: the encoded length of the Certificate Holder Reference
- **yy**: the placeholder for the Certificate Holder Reference (xx bytes)
- **gg**: the placeholder for the BCD encoded effective date of the certificate
- **hh**: the placeholder for the BCD encoded expiration date of the certificate
- **ii**: the encoded length of the certificates signature object,
- **jj**: the placeholder for the certificates signature (ii bytes)

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE010</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 13 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_10</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

2.4.11  Certificate Set 11

2.4.11.1  LINK_CERT_11a

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_11a</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>This certificate is a link certificate. The signing key is an IS key.</th>
</tr>
</thead>
</table>
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Version</th>
<th>1.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referred by</td>
<td>ISO7816_J_53</td>
</tr>
</tbody>
</table>

### Content definition

\[ \text{7F 21 \text{ aa}} \]
\[ \text{7F 4E \text{ bb}} \]
\[ \text{5F 29 01 00} \]
\[ \text{42 \text{ cc dd}} \]
\[ \text{7F 49 \text{ ee ff}} \]
\[ \text{5F 20 \text{ xx yy}} \]
\[ \text{7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3} \]
\[ \text{5F 25 06 \text{ gg}} \]
\[ \text{5F 24 06 \text{ hh}} \]
\[ \text{5F 37 \text{ ii jj}} \]

- \text{aa} is the encoded combined length of certificate body and signature objects
- \text{bb} is the encoded length the certificate body object
- \text{cc} is the encoded length of the Certification Authority Reference
- \text{dd} is the placeholder for the Certification Authority Reference (\text{cc} bytes)
- \text{ee} is the encoded length of the certificates public key,
- \text{ff} is the placeholder for the certificates public key bytes (\text{ee} bytes)
- \text{xx} is the encoded length of the Certificate Holder Reference
- \text{yy} is the placeholder for the Certificate Holder Reference (\text{xx} bytes)
- \text{gg} is the placeholder for the BCD encoded effective date of the certificate
- \text{hh} is the placeholder for the BCD encoded expiration date of the certificate
- \text{ii} is the encoded length of the certificates signature object,
- \text{jj} is the placeholder for the certificates signature (\text{ii} bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETTESTISDE011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>As defined by the initial CVCA root</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>CVCA, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff}</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{exp}</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair IS_KEY_11</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.11.2 LINK_CERT_11b

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_11b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a valid link certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_5</td>
</tr>
</tbody>
</table>

### Content definition

\[ \text{7F 21 \text{ aa}} \]
\[ \text{7F 4E \text{ bb}} \]
\[ \text{5F 29 01 00} \]
\[ \text{42 \text{ cc dd}} \]
\[ \text{7F 49 \text{ ee ff}} \]
\[ \text{5F 20 \text{ xx yy}} \]
2.4.11.3 DV_CERT_11a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_50, ISO7816_J_51, ISO7816_J_52, ISO7816_J_53</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 (aa) 7F 4E (bb) 5F 29 01 00 42 (cc) (dd) 7F 49 (ee) (ff) 5F 20 (xx) (yy) 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 (gg) 5F 24 06 (hh) 5F 37 (ii) (jj)</td>
</tr>
</tbody>
</table>

\(aa\) is the encoded combined length of certificate body and signature objects
\(bb\) is the encoded length the certificate body object
\(cc\) is the encoded length of the Certification Authority Reference
\(dd\) is the placeholder for the Certification Authority Reference (\(cc\) bytes)
\(ee\) is the encoded length of the certificates public key,
\(ff\) is the placeholder for the certificates public key bytes (\(ee\) bytes),
\(xx\) is the encoded length of the Certificate Holder Reference
\(yy\) is the placeholder for the Certificate Holder Reference (\(xx\) bytes)
\(gg\) is the placeholder for the BCD encoded effective date of the certificate
\(hh\) is the placeholder for the BCD encoded expiration date of the certificate
\(ii\) is the encoded length of the certificates signature object,
\(jj\) is the placeholder for the certificates signature (\(ii\) bytes)
**Test plan for eMRTDs with EACv1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE011</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_11</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.11.4 DV_CERT_11b

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_11b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular foreign DV certificate. The signing key is an IS key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_50</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff is the placeholder for the certificates public key bytes (ee bytes),  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)
### 2.4.11.5 DV_CERT_11c

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>DV_CERT_11c</td>
</tr>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular domestic DV certificate. The signing key is an IS key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_51</td>
</tr>
</tbody>
</table>

#### Content definition

```
7F 21 aa
  7F 4E bb
  5F 29 01 00
  42 cc dd
  7F 49 ee ff
  5F 20 xx yy
  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
  5F 25 06 gg
  5F 24 06 hh
  5F 37 ii jj
```

- `aa` is the encoded combined length of certificate body and signature objects
- `bb` is the encoded length the certificate body object
- `cc` is the encoded length of the Certification Authority Reference
- `dd` is the placeholder for the Certification Authority Reference (cc bytes)
- `ee` is the encoded length of the certificates public key,
- `ff` is the placeholder for the certificates public key bytes (ee bytes),
- `xx` is the encoded length of the Certificate Holder Reference
- `yy` is the placeholder for the Certificate Holder Reference (xx bytes)
- `gg` is the placeholder for the BCD encoded effective date of the certificate
- `hh` is the placeholder for the BCD encoded expiration date of the certificate
- `ii` is the encoded length of the certificates signature object,
- `jj` is the placeholder for the certificates signature (ii bytes)

#### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTISDE011</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE011</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff}</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_11</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair IS_KEY_11</td>
</tr>
</tbody>
</table>

### 2.4.11.6 IS_CERT_11a

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>IS_CERT_11a</td>
</tr>
</tbody>
</table>
### Purpose
This certificate is a regular IS certificate.

### Version
1.11

### Referred by
ISO7816_J_50, ISO7816_J_51, ISO7816_J_52, ISO7816_J_53

### Content definition

<table>
<thead>
<tr>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( aa )</td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td>( bb )</td>
<td>is the encoded length of the certificate body object</td>
</tr>
<tr>
<td>( cc )</td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td>( dd )</td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td>( ee )</td>
<td>is the encoded length of the certificates public key,</td>
</tr>
<tr>
<td>( ff )</td>
<td>is the placeholder for the certificates public key bytes (ee bytes),</td>
</tr>
<tr>
<td>( xx )</td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td>( yy )</td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes)</td>
</tr>
<tr>
<td>( gg )</td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td>( hh )</td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td>( ii )</td>
<td>is the encoded length of the certificates signature object,</td>
</tr>
<tr>
<td>( jj )</td>
<td>is the placeholder for the certificates signature (ii bytes)</td>
</tr>
</tbody>
</table>

### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE011</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE011</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 13 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_11</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV_KEY_11</td>
</tr>
</tbody>
</table>

### 2.4.11.7 IS_CERT_11b

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_11b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular IS certificate. The signing key is an IS key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_52</td>
</tr>
</tbody>
</table>

### Content definition

<table>
<thead>
<tr>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( aa )</td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td>( bb )</td>
<td>is the encoded length of the certificate body object</td>
</tr>
<tr>
<td>( cc )</td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td>( dd )</td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td>( ee )</td>
<td>is the encoded length of the certificates public key,</td>
</tr>
<tr>
<td>( ff )</td>
<td>is the placeholder for the certificates public key bytes (ee bytes),</td>
</tr>
<tr>
<td>( xx )</td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td>( yy )</td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes)</td>
</tr>
<tr>
<td>( gg )</td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td>( hh )</td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td>( ii )</td>
<td>is the encoded length of the certificates signature object,</td>
</tr>
<tr>
<td>( jj )</td>
<td>is the placeholder for the certificates signature (ii bytes)</td>
</tr>
</tbody>
</table>
2.4.11.8 IS_CERT_11c

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_11c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is an irregular IS certificate. The signing key is a CVCA key.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_M_5</td>
</tr>
<tr>
<td>Content</td>
<td>7F 21 ( aa )</td>
</tr>
<tr>
<td>definition</td>
<td>7F 4E ( bb )</td>
</tr>
<tr>
<td></td>
<td>7F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00 07 03 01 02 01 53 01 03</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td></td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

\( aa \) is the encoded combined length of certificate body and signature objects
\( bb \) is the encoded length the certificate body object
\( cc \) is the encoded length of the Certification Authority Reference
\( dd \) is the placeholder for the Certification Authority Reference (\( cc \) bytes)
\( ee \) is the encoded length of the certificates public key,
\( ff \) is the placeholder for the certificates public key bytes (\( ee \) bytes),
\( xx \) is the encoded length of the Certificate Holder Reference
\( yy \) is the placeholder for the Certificate Holder Reference (\( xx \) bytes)
\( gg \) is the placeholder for the BCD encoded effective date of the certificate
\( hh \) is the placeholder for the BCD encoded expiration date of the certificate
\( ii \) is the encoded length of the certificates signature object,
\( jj \) is the placeholder for the certificates signature (\( ii \) bytes)
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DETESTCADE011</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE011</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{\text{exp}} + 5 months</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{\text{exp}} + 6 months</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_{\text{KEY}}_{11}</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair</td>
</tr>
<tr>
<td></td>
<td>CVCA_{\text{KEY}}_{11}</td>
</tr>
</tbody>
</table>

### 2.4.12 Certificate Set 12

This certificate set is used for the certificate structure tests.

#### 2.4.12.1 DV_CERT_12a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a domestic DV certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_25, ISO7816_J_35</td>
</tr>
</tbody>
</table>

**Content definition**

\[
\begin{array}{c}
7F\ 21\ \text{aa} \\
7F\ 4E\ \text{bb} \\
5F\ 29\ 01\ 00 \\
42\ \text{cc}\ \text{dd} \\
7F\ 49\ \text{ee}\ \text{ff} \\
5F\ 20\ \text{xx}\ \text{yy} \\
7F\ 4C\ 0E\ 06\ 09\ 04\ 00\ 07\ 00\ 07\ 03\ 01\ 02\ 01\ 53\ 01\ 83 \\
5F\ 25\ 06\ \text{gg} \\
5F\ 24\ 06\ \text{hh} \\
5F\ 37\ \text{ii}\ \text{jj} \\
\end{array}
\]

\text{aa} is the encoded combined length of certificate body and signature objects
\text{bb} is the encoded length the certificate body object
\text{cc} is the encoded length of the Certification Authority Reference
\text{dd} is the placeholder for the Certification Authority Reference (cc bytes)
\text{ee} is the encoded length of the certificates public key,
\text{ff} is the placeholder for the certificates public key bytes (ee bytes),
\text{xx} is the encoded length of the Certificate Holder Reference
\text{yy} is the placeholder for the Certificate Holder Reference (xx bytes)
\text{gg} is the placeholder for the BCD encoded effective date of the certificate
\text{hh} is the placeholder for the BCD encoded expiration date of the certificate
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 20 days</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month + 25 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

#### 2.4.12.2 DV_CERT_12b

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with a wrong “certificate body” tag</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_1_26</td>
</tr>
<tr>
<td>Content definition</td>
<td>7F 21 aa 7F 4F bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</td>
</tr>
</tbody>
</table>

*aa* is the encoded combined length of certificate body and signature objects,
*bb* is the encoded length the certificate body object,
*cc* is the encoded length of the Certification Authority Reference,
*dd* is the placeholder for the Certification Authority Reference (cc bytes),
*ee* is the encoded length of the certificates public key,
*ff* is the placeholder for the certificates public key bytes (ee bytes),
*xx* is the encoded length of the Certificate Holder Reference,
*yy* is the placeholder for the Certificate Holder Reference (xx bytes),
*gg* is the placeholder for the BCD encoded effective date of the certificate,
*hh* is the placeholder for the BCD encoded expiration date of the certificate,
*ii* is the encoded length of the certificates signature object,
*jj* is the placeholder for the certificates signature (ii bytes).
Test plan for eMRTDs with EACv1

| Signing Key reference | Signed with the private key of key pair CVCA_KEY_00 |

### 2.4.12.3 DV_CERT_12c

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with a wrong “certificate signature” tag</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_27</td>
</tr>
</tbody>
</table>

**Content definition**

- **aa**: the encoded combined length of certificate body and signature objects
- **bb**: the encoded length the certificate body object
- **cc**: the encoded length of the Certification Authority Reference
- **dd**: the placeholder for the Certification Authority Reference (cc bytes)
- **ee**: the encoded length of the certificates public key,
- **ff**: the placeholder for the certificates public key bytes (ee bytes),
- **xx**: the encoded length of the Certificate Holder Reference
- **yy**: the placeholder for the Certificate Holder Reference (xx bytes)
- **gg**: the placeholder for the BCD encoded effective date of the certificate
- **hh**: the placeholder for the BCD encoded expiration date of the certificate
- **ii**: the encoded length of the certificates signature object,
- **jj**: the placeholder for the certificates signature (ii bytes)

**Parameter**

| Certification Authority Reference | As defined by the CVCA |
| Certificate Holder Reference     | DETESTDVDE012 |
| Certificate Holder Authorisation | domestic DV, DG 3, DG 4 |
| Certificate effective date       | CVCA_{eff} + 1 month + 20 days |
| Certificate expiration date      | CVCA_{eff} + 1 month + 25 days |
| Public Key reference             | Public key of key pair DV_KEY_12 |
| Signing Key reference            | Signed with the private key of key pair CVCA_KEY_00 |

### 2.4.12.4 DV_CERT_12d

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12d</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with an inconsistent “certificate body” D.O. (wrong length)</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_28</td>
</tr>
</tbody>
</table>
### Content definition

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aa</strong></td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td><strong>bb</strong></td>
<td>is the encoded length the certificate body object <strong>decreased by one</strong></td>
</tr>
<tr>
<td><strong>cc</strong></td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td><strong>dd</strong></td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td><strong>ee</strong></td>
<td>is the encoded length of the certificates public key,</td>
</tr>
<tr>
<td><strong>ff</strong></td>
<td>is the placeholder for the certificates public key bytes (ee bytes),</td>
</tr>
<tr>
<td><strong>xx</strong></td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td><strong>yy</strong></td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes)</td>
</tr>
<tr>
<td><strong>gg</strong></td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td><strong>hh</strong></td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td><strong>ii</strong></td>
<td>is the encoded length of the certificates signature object,</td>
</tr>
<tr>
<td><strong>jj</strong></td>
<td>is the placeholder for the certificates signature (ii bytes)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

#### 2.4.12.5 DV_CERT_12e

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with an inconsistent “certificate signature” D.O. (The length byte specifies one byte less than the actual signature length)</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_1_29</td>
</tr>
</tbody>
</table>

Content definition

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aa</strong></td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td><strong>bb</strong></td>
<td>is the encoded length the certificate body object <strong>decreased by one</strong></td>
</tr>
<tr>
<td><strong>cc</strong></td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td><strong>dd</strong></td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td><strong>ee</strong></td>
<td>is the encoded length of the certificates public key,</td>
</tr>
<tr>
<td><strong>ff</strong></td>
<td>is the placeholder for the certificates public key bytes (ee bytes),</td>
</tr>
<tr>
<td><strong>xx</strong></td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td><strong>yy</strong></td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes)</td>
</tr>
<tr>
<td><strong>gg</strong></td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td><strong>hh</strong></td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td><strong>ii</strong></td>
<td>is the encoded length of the certificates signature object,</td>
</tr>
<tr>
<td><strong>jj</strong></td>
<td>is the placeholder for the certificates signature (ii bytes)</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

#### 2.4.12.6 DV_CERT_12f

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12f</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with a wrong signature</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
<th>7F 21 aa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7F 4E bb</td>
</tr>
<tr>
<td></td>
<td>5F 29 01 00</td>
</tr>
<tr>
<td></td>
<td>42 cc dd</td>
</tr>
<tr>
<td></td>
<td>7F 49 ee ff</td>
</tr>
<tr>
<td></td>
<td>5F 20 xx yy</td>
</tr>
<tr>
<td></td>
<td>7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83</td>
</tr>
<tr>
<td></td>
<td>5F 25 06 gg</td>
</tr>
<tr>
<td></td>
<td>5F 24 06 hh</td>
</tr>
<tr>
<td></td>
<td>5F 37 ii jj</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa</td>
<td>is the encoded combined length of certificate body and signature objects</td>
</tr>
<tr>
<td>bb</td>
<td>is the encoded length the certificate body object,</td>
</tr>
<tr>
<td>cc</td>
<td>is the encoded length of the Certification Authority Reference</td>
</tr>
<tr>
<td>dd</td>
<td>is the placeholder for the Certification Authority Reference (cc bytes)</td>
</tr>
<tr>
<td>ee</td>
<td>is the encoded length of the certificates public key,</td>
</tr>
<tr>
<td>ff</td>
<td>is the placeholder for the certificates public key bytes (ee bytes),</td>
</tr>
<tr>
<td>xx</td>
<td>is the encoded length of the Certificate Holder Reference</td>
</tr>
<tr>
<td>yy</td>
<td>is the placeholder for the Certificate Holder Reference (xx bytes),</td>
</tr>
<tr>
<td>gg</td>
<td>is the placeholder for the BCD encoded effective date of the certificate</td>
</tr>
<tr>
<td>hh</td>
<td>is the placeholder for the BCD encoded expiration date of the certificate</td>
</tr>
<tr>
<td>ii</td>
<td>is the encoded length of the certificates signature object decreased by one,</td>
</tr>
<tr>
<td>jj</td>
<td>is the placeholder for the certificates signature (ii+1 bytes)</td>
</tr>
</tbody>
</table>

58/207
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes) last byte is increased by one (mod 256)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

2.4.12.7 DV_CERT_12g

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with a wrong signature</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816 J_31</td>
</tr>
</tbody>
</table>
| Content definition | 7F 21 aa
  7F 4E bb
  5F 29 01 00
  42 cc dd
  7F 49 ee ff
  5F 20 xx yy
  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
  5F 25 06 gg
  5F 24 06 hh
  5F 37 ii jj |

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object,
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes) – last byte is dropped and ii is updated according to the new length

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

59/207
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff + 1 month + 20 days</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month + 25 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

### 2.4.12.8 DV_CERT_12h

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Modification in the certificate public key: OID is missing</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816 J_37</td>
</tr>
</tbody>
</table>

**Content definition**

```
7F 21   aa
  7F 4E   bb
       5F 29 01 00
       42 cc dd
       7F 49 ee ff
       5F 20 xx yy
       7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
       5F 25 06 gg
       5F 24 06 hh
      5F 37 ii jj
```

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes) – **It does not contain any O.I.D.D.O.,**
- **xx** is the encoded length of the Certificate Holder Reference
- yy is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff + 1 month + 20 days</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month + 25 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>
### 2.4.12.9 DV_CERT_12i

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Modification in the certificate public key : wrong O.I.D</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_36</td>
</tr>
</tbody>
</table>
| Content        | 7F 21 \(aa\)  

\[
\begin{align*}
7F 21 & \quad aa \\
7F 4E & \quad bb \\
5F 29 & \quad 01 00 \\
42 & \quad cc dd \\
7F 49 & \quad ee ff \\
5F 20 & \quad xx yy \\
7F 4C & \quad 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 \\
5F 25 & \quad 06 gg \\
5F 24 & \quad 06 hh \\
5F 37 & \quad ii jj
\end{align*}
\]

*aa* is the encoded combined length of certificate body and signature objects  
*bb* is the encoded length the certificate body object  
*cc* is the encoded length of the Certification Authority Reference  
*dd* is the placeholder for the Certification Authority Reference (cc bytes)  
*ee* is the encoded length of the certificates public key,  
*ff* is the placeholder for the certificates public key bytes (ee bytes) – The O.I.D has **an incorrect value that does not indicate id-TA: (0.4.0.127.0.7.2.2.3.x.y)**,  
*xx* is the encoded length of the Certificate Holder Reference  
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)  
*gg* is the placeholder for the BCD encoded effective date of the certificate  
*hh* is the placeholder for the BCD encoded expiration date of the certificate  
*ii* is the encoded length of the certificates signature object,  
*jj* is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.12.10 DV_CERT_12j

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12j</th>
</tr>
</thead>
</table>
| Purpose        | **For ECDSA profile only:**  
Modification in the certificate public key : the elliptic curve public point is missing |
| Version        | 1.11                                            |
| Referred by    | ISO7816_J_38                                    |
| Content        | 7F 21 \(aa\)  

\[
\begin{align*}
7F 21 & \quad aa
\end{align*}
\]
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td>As defined by the CVCA</td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA\textsubscript{eff} + 1 month + 20 days</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA\textsubscript{eff} + 1 month + 25 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
</tr>
</tbody>
</table>

**2.4.12.11 DV\_CERT\_12k**

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12k</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>For RSA profile only:</td>
</tr>
<tr>
<td></td>
<td>Modification in the certificate public key: the RSA modulus is missing</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_39</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content definition</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 7F 21 \textit{aa} | \begin{verbatim}
7F 21 aa
7F 4E bb
5F 29 01 00
42 cc dd
7F 49 ee ff
5F 20 xx yy
7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
5F 25 06 gg
5F 24 06 hh
5F 37 ii jj
\end{verbatim} |

aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes) – The elliptic curve public point is missing,

xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)
aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee bytes) – The RSA modulus is missing.
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

**2.4.12.12 DV_CERT_12l**

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12l</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td><strong>For RSA profile only:</strong></td>
</tr>
<tr>
<td></td>
<td>Modification in the certificate public key : the RSA public exponent is missing</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_1_40</td>
</tr>
</tbody>
</table>

| Content definition  | 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj |

**aa** is the encoded combined length of certificate body and signature objects
**bb** is the encoded length the certificate body object
**cc** is the encoded length of the Certification Authority Reference
**dd** is the placeholder for the Certification Authority Reference (cc bytes)
2.4.12.13 DV_CERT_12m

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCAeff + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCAeff + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

ID | DV_CERT_12m

| Purpose | Modification in the certificate public key
For ECDSA profile: an unknown D.O. is present within the EC parameters (tag ‘77’),
For RSA profile: an unknown D.O. is present within the RSA parameters (‘77 01 00’).

| Version | 1.11

| Referred by | ISO7816 J_41

| Content definition |

| 7F 21 | aa  
| 7F 4E | bb  
| 5F 29 | 01 00  
| 42 cc | dd  
| 7F 49 | ee ff  
| 5F 20 | xx yy  
| 7F 4C | 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83  
| 5F 25 | 06 gg  
| 5F 24 | 06 hh  
| 5F 37 | ii jj  |

- aa is the encoded combined length of certificate body and signature objects
- bb is the encoded length the certificate body object
- cc is the encoded length of the Certification Authority Reference
- dd is the placeholder for the Certification Authority Reference (cc bytes)
- ee is the encoded length of the certificates public key,
- ff is the placeholder for the certificates public key bytes (ee bytes) – An unknown D.O. ‘77’ is present
- xx is the encoded length of the Certificate Holder Reference
- yy is the placeholder for the Certificate Holder Reference (xx bytes)
- gg is the placeholder for the BCD encoded effective date of the certificate
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff} + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

2.4.12.14 DV_CERT_12n

**ID** | DV_CERT_12n
---|---
**Version** | Has been merged with DV_CERT_12m in version 1.1

2.4.12.15 DV_CERT_12o

**ID** | DV_CERT_12o
---|---
**Purpose** | For RSA profile only: Certificate with a wrong signature
**Version** | 1.11
**Referred by** | ISO7816_J_32

**Content definition**

```
7F 21 aa
  7F 4E bb
    5F 29 01 00
    42 cc dd
    7F 49 ee ff
    5F 20 xx yy
    7F 4C 0E 06 09 04 00 00 7F 00 07 03 01 02 01 03 01 05 01 83
    5F 25 06 gg
    5F 24 06 hh
    5F 37 ii jj
```

*aa* is the encoded combined length of certificate body and signature objects
*bb* is the encoded length the certificate body object,
*cc* is the encoded length of the Certification Authority Reference
*dd* is the placeholder for the Certification Authority Reference (cc bytes)
*ee* is the encoded length of the certificates public key,
*ff* is the placeholder for the certificates public key bytes (ee bytes),
*xx* is the encoded length of the Certificate Holder Reference
*yy* is the placeholder for the Certificate Holder Reference (xx bytes)
*gg* is the placeholder for the BCD encoded effective date of the certificate
*hh* is the placeholder for the BCD encoded expiration date of the certificate
*ii* is the encoded length of the certificates signature object,
*jj* is the placeholder for the certificates signature (ii bytes) – the signature is greater than the modulus of the issuing key CVCA_KEY_00, the length of
signature matches the length of the modulus

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 25 days</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_12</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.12.16 DV_CERT_12p

**ID**  
DV_CERT_12p

**Purpose**  
For ECDSA profile only:  
The certificate signature is wrong. It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime.

**Version**  
1.11

**Referred by**  
ISO7816_J_33

**Content definition**

```
7F 21 aa
  7F 4E bb
    5F 29 01 00
    42 cc dd
    7F 49 ee ff
    5F 20 xx yy
    7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
    5F 25 06 gg
    5F 24 06 hh
    5F 37 ii jj
```

- **aa** is the encoded combined length of certificate body and signature objects.
- **bb** is the encoded length the certificate body object,
- **cc** is the encoded length of the Certification Authority Reference.
- **dd** is the placeholder for the Certification Authority Reference (cc bytes).
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference.
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes),
- **gg** is the placeholder for the BCD encoded effective date of the certificate.
- **hh** is the placeholder for the BCD encoded expiration date of the certificate.
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes) – with r = 0

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE012</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 20 days</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 1 month + 25 days</td>
<td></td>
</tr>
</tbody>
</table>
Public Key reference | Public key of key pair DV_KEY_12
---|---
Signing Key reference | Signed with the private key of key pair CVCA_KEY_00

### 2.4.12.17 DV_CERT_12q

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_12q</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>For ECDSA profile only: The certificate signature is wrong. It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ still matches the size of the prime.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816_J_34</td>
</tr>
<tr>
<td><strong>Content definition</strong></td>
<td>7F 21 aa &lt;br&gt;7F 4E bb &lt;br&gt;5F 29 01 00 &lt;br&gt;42 cc dd &lt;br&gt;7F 49 ee ff &lt;br&gt;5F 20 xx yy &lt;br&gt;7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 &lt;br&gt;5F 25 06 gg &lt;br&gt;5F 24 06 hh &lt;br&gt;5F 37 ii jj</td>
</tr>
</tbody>
</table>

**aa** is the encoded combined length of certificate body and signature objects  
**bb** is the encoded length the certificate body object,  
**cc** is the encoded length of the Certification Authority Reference  
**dd** is the placeholder for the Certification Authority Reference (cc bytes)  
**ee** is the encoded length of the certificates public key,  
**ff** is the placeholder for the certificates public key bytes (ee bytes),  
**xx** is the encoded length of the Certificate Holder Reference  
**yy** is the placeholder for the Certificate Holder Reference (xx bytes)  
**gg** is the placeholder for the BCD encoded effective date of the certificate  
**hh** is the placeholder for the BCD encoded expiration date of the certificate  
**ii** is the encoded length of the certificates signature object,  
**jj** is the placeholder for the certificates signature (ii bytes) – with s = 0

**Parameter** | Certification Authority Reference | As defined by the CVCA
---|---|---
Certificate Holder Reference | DETESTDVDE012 |
Certificate Holder Authorisation | domestic DV, DG 3, DG 4 |
Certificate effective date | CVCAeff + 1 month + 20 days |
Certificate expiration date | CVCAeff + 1 month + 25 days |
Public Key reference | Public key of key pair DV_KEY_12 |
Signing Key reference | Signed with the private key of key pair CVCA_KEY_00 |
2.4.13 Certificate Set 13

This certificate set defines a link certificate used to update the chip signature mechanism according to
the migration policy as defined by the manufacturer. The cryptographic elements of these certificates
MUST use the new mechanisms besides the signature of the LINK_CERT_13 which is done with the
original signature mechanism. This certificate set is only needed if the “Migration” profile is
supported.

2.4.13.1 LINK_CERT_13

Note for ECDSA profile: Since the crypto mechanism is changed by this certificate, the domain
parameter MUST be included in this certificate.

<table>
<thead>
<tr>
<th>ID</th>
<th>LINK_CERT_13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>For MIG profile only: This certificate is a link certificate, which defines a new crypto mechanism to be used by the chip.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_N_1</td>
</tr>
</tbody>
</table>

**Content definition**

```
7F 21  aa
    7F 4E  bb
      5F 29 01 00
      42  cc  dd
      7F 49  ee  ff
      5F 20  xx  yy
      7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3
      5F 25 06 gg
      5F 24 06 hh
      5F 37  ii  jj
```

*aa* is the encoded combined length of certificate body and signature objects

*bb* is the encoded length the certificate body object

*cc* is the encoded length of the Certification Authority Reference

*dd* is the placeholder for the Certification Authority Reference (cc bytes)

*ee* is the encoded length of the certificates public key,

*ff* is the placeholder for the certificates public key bytes (ee bytes),

*gg* is the placeholder for the BCD encoded effective date of the certificate

*hh* is the placeholder for the BCD encoded expiration date of the certificate

*ii* is the encoded length of the certificates signature object,

*jj* is the placeholder for the certificates signature (ii bytes)

**Parameter**

- Certification Authority Reference: DETESTCADE011
- Certificate Holder Reference: DETESTCADE013
- Certificate Holder Authorisation: CVCA, DG 3, DG 4
- Certificate effective date: CVCAexp + 7 months
- Certificate expiration date: CVCAexp + 10 month
- Public Key reference: Public key of key pair CVCA_KEY_13
- Signing Key reference: Signed with the private key of key pair CVCA_KEY_11
### 2.4.13.2 DV_CERT_13

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_13</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td><strong>For MIG profile only:</strong> This certificate is a domestic DV certificate, which was issued by the new CVCA.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816_N_1</td>
</tr>
<tr>
<td><strong>Content definition</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **aa** is the encoded combined length of certificate body and signature objects
- **bb** is the encoded length the certificate body object
- **cc** is the encoded length of the Certification Authority Reference
- **dd** is the placeholder for the Certification Authority Reference (cc bytes)
- **ee** is the encoded length of the certificates public key,
- **ff** is the placeholder for the certificates public key bytes (ee bytes),
- **xx** is the encoded length of the Certificate Holder Reference
- **yy** is the placeholder for the Certificate Holder Reference (xx bytes)
- **gg** is the placeholder for the BCD encoded effective date of the certificate
- **hh** is the placeholder for the BCD encoded expiration date of the certificate
- **ii** is the encoded length of the certificates signature object,
- **jj** is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTCADE013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE013</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{exp} + 7 months</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{exp} + 8 months</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_13</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_13</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.13.3 IS_CERT_13

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_13</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td><strong>For MIG profile only:</strong> This certificate is a regular IS certificate, which is issued by the DV_CERT_13</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.11</td>
</tr>
<tr>
<td><strong>Referred by</strong></td>
<td>ISO7816_N_1</td>
</tr>
<tr>
<td><strong>Content definition</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

69/207
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>DETESTDVDE013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE013</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>(\text{CVCA}_{\text{exp}} + 7) months</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>(\text{CVCA}_{\text{exp}} + 8) months</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_13</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV_KEY_13</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.14 Certificate Set 14

The certificate set follows a certification scheme where the DV and IS contain public key information from a generated key whose length is shorter than the CVCA key length.

#### 2.4.14.1 DV_CERT_14a

<table>
<thead>
<tr>
<th>ID</th>
<th>DV_CERT_14a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular domestic DV certificate which is issued by the CVCA</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816 J_56</td>
</tr>
<tr>
<td>Content</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
aa is the encoded combined length of certificate body and signature objects
bb is the encoded length the certificate body object
cc is the encoded length of the Certification Authority Reference
dd is the placeholder for the Certification Authority Reference (cc bytes)
ee is the encoded length of the certificates public key,
 ff is the placeholder for the certificates public key bytes (ee bytes),
xx is the encoded length of the Certificate Holder Reference
yy is the placeholder for the Certificate Holder Reference (xx bytes)
gg is the placeholder for the BCD encoded effective date of the certificate
hh is the placeholder for the BCD encoded expiration date of the certificate
ii is the encoded length of the certificates signature object,
jj is the placeholder for the certificates signature (ii bytes)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE014</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff}</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair DV_KEY_14a</td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair CVCA_KEY_00</td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.14.2 DV_CERT_14b

**ID**  
DV_CERT_14b

**Purpose**  
Certificate with a wrong (too short) public key.
For the RSA profile, the same Algorithm Identifier is used, but PK.DVCA’s modulus length is shorter than the CVCA’s key modulus length.
For the ECDSA profile, the same Algorithm Identifier is used, but DVCA’s domain parameters are different and have a shorter prime length than the CVCA’s key. The hash algorithm should be adapted if necessary.

**Version**  
1.11

**Referred by**  
ISO7816_J_55

**Content definition**

```
7F 21 aa
7F 4E bb
5F 29 01 00
42 cc dd
7F 49 ee ff
5F 20 xx yy
7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83
5F 25 06 gg
5F 24 06 hh
5F 37 ii jj
```
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Certification Authority Reference</th>
<th>As defined by the CVCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTDVDE014</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>domestic DV, DG 3, DG4</td>
<td></td>
</tr>
<tr>
<td>Certificate effective date</td>
<td><strong>CVCA</strong>_{eff}</td>
<td></td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td><strong>CVCA</strong>_{eff} + 1 month</td>
<td></td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair <strong>DV_KEY_14b</strong></td>
<td></td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair <strong>CVCA_KEY_00</strong></td>
<td></td>
</tr>
</tbody>
</table>

2.4.14.3 IS_CERT_14a

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_14a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This certificate is a regular IS certificate, which is issued by the DV_CERT_14</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_55</td>
</tr>
</tbody>
</table>

Content definition

```
7F 21  aa
    7F 4E  bb
      5F 29 01 00
      42    cc dd
      7F 49  ee ff
      5F 20 xx yy
      7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
      5F 25 06 gg
      5F 24 06 hh
      5F 37 ii jj
```

*aa* is the encoded combined length of certificate body and signature objects

*bb* is the encoded length the certificate body object

*cc* is the encoded length of the Certification Authority Reference

*dd* is the placeholder for the Certification Authority Reference (cc bytes)

*ee* is the encoded length of the certificates public key,

*ff* is the placeholder for the certificates public key bytes (ee bytes),

*xx* is the encoded length of the Certificate Holder Reference

*yy* is the placeholder for the Certificate Holder Reference (xx bytes)

*gg* is the placeholder for the BCD encoded effective date of the certificate

*hh* is the placeholder for the BCD encoded expiration date of the certificate

*ii* is the encoded length of the certificates signature object,
**Test plan for eMRTDs with EACv1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DETESTDVDE014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE014</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
</tr>
<tr>
<td>Certificate effective date</td>
<td>CVCA_{eff}</td>
</tr>
<tr>
<td>Certificate expiration date</td>
<td>CVCA_{eff} + 14 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS_KEY_14a</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV_KEY_14b</td>
</tr>
</tbody>
</table>

**2.4.14.4 IS_CERT_14b**

<table>
<thead>
<tr>
<th>ID</th>
<th>IS_CERT_14b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Certificate with a wrong (too short) Public key. For the RSA profile, the same Algorithm Identifier is used, but IS key modulus length is shorter than the DVCA’s key modulus length. For the ECDSA profile, same Algorithm Identifier is used, but IS key domain parameters are different and have a shorter prime length than the DVCA’s key. The hash algorithm should be adapted if necessary.</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Referred by</td>
<td>ISO7816_J_56</td>
</tr>
</tbody>
</table>

**Content definition**

```
7F 21 aa
  7F 4E bb
  5F 29 01 00
  42 cc dd
  7F 49 ee ff
  5F 20 xx yy
  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03
  5F 25 06 gg
  5F 24 06 hh
  5F 37 ii jj
```

- `aa` is the encoded combined length of certificate body and signature objects
- `bb` is the encoded length the certificate body object
- `cc` is the encoded length of the Certification Authority Reference
- `dd` is the placeholder for the Certification Authority Reference (cc bytes)
- `ee` is the encoded length of the certificates public key,
- `ff` is the placeholder for the certificates public key bytes (ee bytes),
- `xx` is the encoded length of the Certificate Holder Reference
- `yy` is the placeholder for the Certificate Holder Reference (xx bytes)
- `gg` is the placeholder for the BCD encoded effective date of the certificate
- `hh` is the placeholder for the BCD encoded expiration date of the certificate
- `ii` is the encoded length of the certificates signature object,
- `jj` is the placeholder for the certificates signature (ii bytes)

**Parameter**

<table>
<thead>
<tr>
<th>Certification Authority</th>
<th>DETESTDVDE014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Certificate Holder Reference</td>
<td>DETESTISDE014</td>
</tr>
<tr>
<td>Certificate Holder Authorisation</td>
<td>IS, DG 3, DG 4</td>
</tr>
</tbody>
</table>

---

73/207
<table>
<thead>
<tr>
<th>Certificate effective date</th>
<th>CVCA&lt;sub&gt;eff&lt;/sub&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate expiration date</td>
<td>CVCA&lt;sub&gt;eff&lt;/sub&gt; + 14 days</td>
</tr>
<tr>
<td>Public Key reference</td>
<td>Public key of key pair IS.Key_14b</td>
</tr>
<tr>
<td>Signing Key reference</td>
<td>Signed with the private key of key pair DV.Key_14a</td>
</tr>
</tbody>
</table>
3  Tests for layer 6 (ISO 7816)

This chapter defines the additional tests required for the extended command set used by the extended access control mechanisms.

3.1  Test case notation

The test cases defined below specify a set of command APDU which have to be sent to the test sample. While some parts of these APDUs are fixed, other elements have variable values which cannot be defined in general. The variable parts are marked by placeholder values which have to be replaced by the actual values. The following placeholders commonly used and therefore defined here in a global manner. All other placeholders are defined within the corresponding test case definition.

<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Lc&gt;</td>
<td>The length byte containing the length of the APDU command data.</td>
</tr>
<tr>
<td>&lt;Le&gt;</td>
<td>The length byte containing the length of the requested response data.</td>
</tr>
<tr>
<td></td>
<td>Depending on the size of &lt;Lc&gt; the &lt;Le&gt; element must consist of one or two</td>
</tr>
<tr>
<td></td>
<td>bytes (extended length). See ISO 7816-4 5.1 “In any command-response pair</td>
</tr>
<tr>
<td></td>
<td>comprising both Lc and Le fields (see ISO/IEC 7816-3), short and extended</td>
</tr>
<tr>
<td></td>
<td>length fields shall not be combined: either both of them are short, or both</td>
</tr>
<tr>
<td></td>
<td>of them are extended.”</td>
</tr>
<tr>
<td>&lt;Lxy&gt;</td>
<td>The encoded length of the data object xy.</td>
</tr>
<tr>
<td>&lt;Cryptogram&gt;</td>
<td>The encrypted part of a Secure Messaging APDU. The data content of this</td>
</tr>
<tr>
<td></td>
<td>cryptogram is defined in the corresponding test case definition.</td>
</tr>
<tr>
<td>&lt;Checksum&gt;</td>
<td>The cryptographic checksum which is calculated over the protected parts of</td>
</tr>
<tr>
<td></td>
<td>the Secure Messaging command.</td>
</tr>
<tr>
<td>&lt;fid.EF.CVCA&gt;</td>
<td>With version 1.1 of the EAC specification a passport may define a different</td>
</tr>
<tr>
<td></td>
<td>FID for the EF.CVCA file. This definition can be done in the</td>
</tr>
<tr>
<td></td>
<td>TerminalAuthentication element in Data Group 14. If this is the case for</td>
</tr>
<tr>
<td></td>
<td>the test object, this placeholder has to be set to the passport specific</td>
</tr>
<tr>
<td></td>
<td>FID for the EF.CVCA file, otherwise this placeholder is set to the default</td>
</tr>
<tr>
<td></td>
<td>value of ’01 1C’.</td>
</tr>
<tr>
<td>&lt;sfi.EF.CVCA&gt;</td>
<td>With version 1.1 of the EAC specification a passport may define a different</td>
</tr>
<tr>
<td></td>
<td>SFI for the EF.CVCA file. This definition can be done in the</td>
</tr>
<tr>
<td></td>
<td>TerminalAuthentication element in Data Group 14. If this is the case for</td>
</tr>
<tr>
<td></td>
<td>the test object, this placeholder has to be set to the passport specific</td>
</tr>
<tr>
<td></td>
<td>SFI for the EF.CVCA file, otherwise this placeholder is set to the default</td>
</tr>
<tr>
<td></td>
<td>value of ’1C’.</td>
</tr>
</tbody>
</table>

Note: It may happen that there is only a FID defined in the TerminalAuthenticationInfo element, but NO SFI. In this case, the corresponding test cases have to be skipped.

3.2  General requirements

3.2.1  Security Status

According to the definition in the ICAO documents [R3] and the BSI technical guidelines [R10] the Secure Messaging session MUST be aborted if and only if a secure messaging error occurs or a plain APDU is received.
In respect to the Chip Authentication mechanism the EAC specification contains an additional specification about the security status:

**Security Status**
If Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys $K_{MAC}$ and $K_{ENC}$. Otherwise, Secure Messaging is continued using the previously established session keys (PACE or Basic Access Control).

Reference 1 : Security Status definition in the EAC specification

Based on these definitions, all responses received during the test cases MUST be coded in secure messaging context unless stated different in the test case. The test setup MUST check this and MUST verify the cryptographic checksum.

### 3.2.2 Extended length APDUs

If the size of cryptographic keys leads to certificates that exceed the size of a standard APDU, all appropriate commands have to be performed as extended length APDUs. Extended length APDUs have to be managed according to [R12], clause 5.1 “Command-response pairs”.

### 3.3 Unit ISO7816_H – Security Conditions for EAC protected MRTDs

On an EAC protected eMRTD, the Data Groups containing sensitive biometric data MUST be protected by the terminal authentication mechanisms. While all other Data Groups are accessible after the “Open ePassport Application” procedure [R11] has been performed, the Data Group 3 and/or Data Group 4 MUST only be accessible after a successful terminal authentication process.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

Note: Chip Authentication must be performed as described in [R10] and [R11] either with command $MSE: Set KAT$ or commands $MSE: Set AT$ and $General Authenticate$.

### 3.3.1 Test case ISO7816_H_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>SELECT command for EF.DG3 within an established PACE or BAC session, but before the terminal authentication mechanism has been performed.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed, too.

**Test scenario**

1. Send the given SELECT APDU for EF.DG3 (FID '01 03') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 3 MUST be denied.
   
   `0C A4 02 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   
   - <Cryptogram> contains the encrypted FID ('01 03').
   
2. Send the following READ BINARY command to the eMRTD:
3.3.2 Test case ISO7816_H_2

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>SELECT command for EF.DG4 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG4</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed, too.

Test scenario
1. Send the given SELECT APDU for EF.DG4 (FID '01 04') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 4 MUST be denied.
   '0C A4 02 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the encrypted FID ('01 04').
2. Send the following READ BINARY command to the eMRTD:
   '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results
1. ISO checking error or '90 00' within a valid SM response. If this step returns an ISO checking error, the next step SHALL be skipped.
2. ISO checking error within a valid SM response

3.3.3 Test case ISO7816_H_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with SFI for EF.DG3 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed, too.

Test scenario
1. Send the given READ BINARY APDU for EF.DG3 (SFI '03') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 3 MUST be denied.
   '0C B0 00 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results
1. ISO checking error within a valid SM response.

3.3.4 Test case ISO7816_H_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with SFI for EF.DG4 within an established PACE or</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>BAC session, but without the terminal authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
</tr>
<tr>
<td><strong>Profile</strong></td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed, too. |
| **Test scenario** | 1. Send the given READ BINARY APDU for EF.DG4 (SFI '04') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 4 MUST be denied.  
'0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00' |
| **Expected results** | 1. ISO checking error within a valid SM response |

#### 3.3.5 Test case ISO7816_H_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>READ BINARY command with odd instruction byte and SFI for EF.DG3 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA, DG3, OddIns</td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed, too. |
| **Test scenario** | 1. Send the given READ BINARY APDU for EF.DG3 (SFI '03') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 3 MUST be denied.  
'0C B1 00 03 <Lc> 85 <L85> <Cryptogram> 97 01 07 8E 08 <Checksum> 00'  
- The cryptogram contains the encrypted data object 54 with the encoded offset of 00: ‘54 01 00’ |
| **Expected results** | 1. ISO checking error within a valid SM response |

#### 3.3.6 Test case ISO7816_H_6

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>READ BINARY command with odd instruction byte and SFI for EF.DG4 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA, DG4, OddIns</td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed, too. |
| **Test scenario** | 1. Send the given READ BINARY APDU for EF.DG4 (SFI '04') to the eMRTD. Though PACE or BAC and the CA mechanisms have been performed, the access to the Data Group 4 MUST be denied.  
'0C B1 00 04 <Lc> 85 <L85> <Cryptogram> 97 01 07 8E 08 <Checksum> 00'  
- The cryptogram contains the encrypted data object 54 with the encoded offset of 00: ‘54 01 00’ |
encoded offset of 00:
‘54 01 00’

Expected results 1. ISO checking error within a valid SM response

3.3.7 Test case ISO7816_H_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>SELECT command for EF.CVCA without established PACE or BAC session</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

Preconditions 1. The "Open ePassport Application" procedure MUST NOT have been performed.
2. The FID information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.

Test scenario 1. Select the ePassport application.
‘00 A4 04 0C 07 A0 00 00 02 47 10 01’
2. Send the given SELECT APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to this file MUST be denied.
‘00 A4 02 0C 02 <fid.EF.CVCA>’
3. Some chip implementations allow the selection of a protected file. In these cases an additional READ BINARY SHOULD be used to verify that at least the READ BINARY command is prohibited.
‘00 B0 00 00 01’

Expected results 1. ISO checking error or ‘90 00’ as a plain response without Secure Messaging.
If this step returns ISO checking error, the next steps SHALL be skipped.
2. ISO checking error or ‘90 00’ as a plain response without Secure Messaging
3. ISO checking error as a plain response without Secure Messaging

3.3.8 Test case ISO7816_H_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with SFI for EF.CVCA without established PACE or BAC session</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

Preconditions 1. The SFI information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a FID, but no SFI, this test case is skipped.

Test scenario 1. Select the ePassport application.
‘00 A4 04 0C 07 A0 00 00 02 47 10 01’
2. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. Since the "Open ePassport Application" procedure has not been performed, the access to the EF.CVCA has to be denied.
3.3.9 Test case ISO7816_H_9

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and with SFI for EF.CVCA without established PACE or BAC session</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, OddIns</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The SFI information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a FID, but no SFI, this test case is skipped</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Select the ePassport application. ‘00 A4 04 0C 07 A0 00 00 02 47 10 01’ 2. Send the given READ BINARY APDU for EF.CVCA (&lt;sfi.EF.CVCA&gt;) to the eMRTD. Since the &quot;Open ePassport Application&quot; procedure has not been performed, the access to the EF.CVCA has to be denied. ‘00 B1 00 &lt;sfi.EF.CVCA&gt; 03 54 01 00 07’</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. ISO checking error or ‘90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error as a plain response without Secure Messaging</td>
</tr>
</tbody>
</table>

3.3.10 Test case ISO7816_H_10

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and with FID for EF.CVCA without established PACE or BAC session</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, OddIns</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The FID information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Select the ePassport application. ‘00 A4 04 0C 07 A0 00 00 02 47 10 01’ 2. Send the given READ BINARY APDU for EF.CVCA (&lt;fid.EF.CVCA&gt;) to the eMRTD. Since the &quot;Open ePassport Application&quot; procedure has not been performed, the access to the EF.CVCA has to be denied. ‘00 B1 &lt;fid.EF.CVCA&gt; 03 54 01 00 07’</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. ISO checking error or ‘90 00’ as a plain response without Secure Messaging. If this step returns ISO checking error, the next steps SHALL be skipped. 2. ISO checking error as a plain response without Secure Messaging</td>
</tr>
</tbody>
</table>
### 3.3.11 Test case ISO7816_H_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and FID for EF.DG3 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3, OddIns</td>
</tr>
</tbody>
</table>
| Preconditions| 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed, too. |
| Test scenario| 1. Send the given READ BINARY APDU for EF.DG3 (FID '01 03') to the eMRTD. Though "Open ePassport Application" procedure and the CA mechanisms have been performed, the access to the Data Group 3 MUST be denied.  
```
0C B1 01 03 <Lc> 85 <L85> <Cryptogram> 97 01 07  
8E 08 <Checksum> 00'
```

- The cryptogram contains the encrypted data object 54 with the encoded offset of 00:
  `'54 01 00'` |
| Expected results | 1. ISO checking error within a valid SM response |

### 3.3.12 Test case ISO7816_H_12

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and FID for EF.DG4 within an established PACE or BAC session, but without the terminal authentication</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG4, OddIns</td>
</tr>
</tbody>
</table>
| Preconditions| 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed, too. |
| Test scenario| 1. Send the given READ BINARY APDU for EF.DG4 (FID '01 04') to the eMRTD. Though "Open ePassport Application" procedure and the CA mechanisms have been performed, the access to the Data Group 4 MUST be denied.  
```
0C B1 01 04 <Lc> 85 <L85> <Cryptogram> 97 01 07  
8E 08 <Checksum> 00'
```

- The cryptogram contains the encrypted data object 54 with the encoded offset of 00:
  `'54 01 00'` |
| Expected results | 1. ISO checking error within a valid SM response |

### 3.3.13 Test case ISO7816_H_13

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>SELECT command for EF.CVCA with established PACE or BAC session (Positive test)</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
</tbody>
</table>
## Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Profile</th>
<th>TA</th>
</tr>
</thead>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The FID information from Data Group 14 TerminalAuthenticationInfo element MUST be used if present. Otherwise the default value has to be used. |

### Test scenario

1. Send the given SELECT APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD.  
   `'0C A4 02 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`  
   - The cryptogram contains the encrypted FID of the EF.CVCA file `<fid.EF.CVCA>`.

2. According to [R11], the size of the EF.CVCA MUST be 36 bytes. So try to read the entire EF.CVCA file with a single READ BINARY Command.  
   `'0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00'` 

### Expected results

1. `90 00` within a valid SM response  
2. 36 bytes of content data and `90 00` in an SM response

### 3.3.14 Test case ISO7816_H_14

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with SFI for EF.CVCA with established PACE or BAC session (Positive test)</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The SFI information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a FID, but no SFI, this test case is skipped. |

### Test scenario

1. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. According to [R11], the size of the EF.CVCA MUST be 36 bytes. So try to read the entire EF.CVCA file with a single READ BINARY Command.  
   `'0C B0 <sfi.EF.CVCA> 00 0D 97 01 24 8E 08 <Checksum> 00'` 

### Expected results

1. 36 bytes of content data and `90 00` in an SM response

### 3.3.15 Test case ISO7816_H_15

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and with SFI for EF.CVCA with established PACE or BAC session (Positive test)</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, OddIns</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been</td>
</tr>
</tbody>
</table>
performed.

2. The SFI information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used. If the TerminalAuthenticationInfo element specifies a FID, but no SFI, this test case is skipped

Test scenario

1. Send the given READ BINARY APDU for EF.CVCA (<sfi.EF.CVCA>) to the eMRTD. According to [R11], the size of the EF.CVCA MUST be 36 bytes. So try to read the EF.CVCA file with a single READ BINARY Command

   '0C B1 00 <sfi.EF.CVCA> <Lc> 85 <L85> <Cryptogram> 97 01 26 8E 08 <Checksum> 00

   • The cryptogram contains the encrypted data object 54 with an encoded offset of 00:
     '54 01 00'

Expected results

1. 38 bytes of data including the tag 53 and the BER encoded length. The Status must be '90 00'. The response must be protected by Secure Messaging.

3.3.16 Test case ISO7816_H_16

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_H_16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>READ BINARY command with odd instruction byte and with FID for EF.CVCA with established PACE or BAC session (Positive test)</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, OddIns</td>
</tr>
</tbody>
</table>

Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.

2. The FID information from Data Group 14 TerminalAuthenticationInfo element must be used if present. Otherwise the default value has to be used.

Test scenario

2. Send the given READ BINARY APDU for EF.CVCA (<fid.EF.CVCA>) to the eMRTD. According to [R11], the size of the EF.CVCA MUST be 36 bytes. So try to read the EF.CVCA file with a single READ BINARY Command

   '0C B1 <fid.EF.CVCA> <Lc> 85 <L85> <Cryptogram> 97 01 26 8E 08 <Checksum> 00

   • The cryptogram contains the encrypted data object 54 with an encoded offset of 00:
     '54 01 00'

Expected results

1. 38 bytes of data including the tag 53 and the BER encoded length. The Status must be '90 00'. The response must be protected by Secure Messaging.
3.4 Unit ISO7816_I – Chip Authentication (MSE:Set KAT)

Test for Chip Authentication Version 1 with MSE:Set KAT are now part of [R7].

3.5 Unit ISO7816_II – Chip Authentication (MSE:Set AT & GA)

Test for Chip Authentication Version 1 with MSE:Set AT and GA are now part of [R7].

3.6 Unit ISO7816_J – Certificate verification

During the Terminal Authentication process the certificate chain from the trust point stored in the chips EF.CVCA file down to the inspection systems CV certificate is verified. This is done by an alternating sequence of MSE: Set DST and Verify Certificate commands. All test cases of this test unit cover all certificate verification test cases which do NOT update the chips persistent memory. This means that all tests in this unit can be repeated with the same set of certificates.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.6.1 Test case ISO7816_J_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>Purpose</th>
<th>Version</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO7816_J_1</td>
<td>Positive test with a valid chain of CV certificates.</td>
<td>1.2</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   `'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’`
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   `'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’`
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`

3. Send the given MSE: Set DST APDU to the eMRTD.
   `'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08`
Test plan for eMRTDs with EACv1

<Checksum> 00’
- <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certification Authority Reference>
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

Expected results
1. '90 00' in a valid SM response.
2. '90 00' in a valid SM response.
3. '90 00' in a valid SM response.
4. '90 00' in a valid SM response.

3.6.2 Test case ISO7816_J_2

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with an invalid Certification Authority Reference.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>

Test scenario
1. Send the given MSE: SET DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <BAD Certification Authority Reference>
   - The Certification Authority Reference read from the EF.CVCA is changed in the last character to create an invalid reference.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: SET DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate
sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

Expected results

1. ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
2. ISO checking error or ‘6300’ in a valid SM response.
3. ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.3 Test case ISO7816_J_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with an invalid certificate signature.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
</table>
| 1. Send the given MSE: Set DST APDU to the eMRTD.  
\`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
- <Cryptogram> contains the following encrypted data objects  
  83 <L83> <Certification Authority Reference>  
- The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
  | 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
\`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
- <Cryptogram> contains the following encrypted data objects  
  7F 4E <L7F4E> <certificate body>  
  5F 37 <L5F37> <bad certificate signature>  
- The signature object of the certificate has been changed in last digit to make it invalid.  
  | 3. Send the given MSE: Set DST APDU to the eMRTD.  
\`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
- <Cryptogram> contains the following encrypted data objects  
  83 <L83> <Certification Authority Reference>  
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
  | 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
\`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
- <Cryptogram> contains the following encrypted data objects  
  7F 4E <L7F4E> <certificate body>  
  5F 37 <L5F37> <certificate signature>  

<table>
<thead>
<tr>
<th>Expected results</th>
</tr>
</thead>
</table>
| 1. '90 00’ in a valid SM response.  
2. ISO checking error or '63 00' in a valid SM response.  
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.  
4. ISO checking error or '63 00' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.  

### 3.6.4 Test case ISO7816_J_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with a missing certificate signature.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well. |
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.

   '0C 22 81 B6 <Le> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the
     EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

   '0C 2A 00 BE <Le> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
   - The certificate signature object is omitted.

3. Send the given MSE: Set DST APDU to the eMRTD.

   '0C 22 81 B6 <Le> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate
     sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.

   '0C 2A 00 BE <Le> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

### Expected results

1. '90 00’ in a valid SM response.
2. ISO checking error or ‘63 00’ in a valid SM response.
3. '90 00’ or ISO checking error in a valid SM response. Note that some chip
   OS accept the selection of an unavailable public key and return an error
   only when the public key is used for the selected purpose.
4. ISO checking error or ‘63 00’ in a valid SM response. Since the DV
   certificate was not verified successfully, it MUST NOT be possible to use
   it as the trust point for the IS-Certificate verification.

### 3.6.5 Test case ISO7816_J_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with a missing certificate body.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
</tbody>
</table>
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td><code>0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00</code></td>
</tr>
<tr>
<td>- <code>&lt;Cryptogram&gt;</code> contains the following encrypted data objects</td>
</tr>
<tr>
<td>83 <code>&lt;L83&gt;</code> <code>&lt;Certification Authority Reference&gt;</code></td>
</tr>
<tr>
<td>- The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.</td>
</tr>
<tr>
<td><code>0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;</code></td>
</tr>
<tr>
<td>- <code>&lt;Cryptogram&gt;</code> contains the following encrypted data objects</td>
</tr>
<tr>
<td>5F 37 <code>&lt;L5F37&gt;</code> <code>&lt;certificate signature&gt;</code></td>
</tr>
<tr>
<td>- The certificate body object is omitted.</td>
</tr>
<tr>
<td>3. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td><code>0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00</code></td>
</tr>
<tr>
<td>- <code>&lt;Cryptogram&gt;</code> contains the following encrypted data objects</td>
</tr>
<tr>
<td>83 <code>&lt;L83&gt;</code> <code>&lt;Certification Authority Reference&gt;</code></td>
</tr>
<tr>
<td>- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.</td>
</tr>
<tr>
<td>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.</td>
</tr>
<tr>
<td><code>0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;</code></td>
</tr>
<tr>
<td>- <code>&lt;Cryptogram&gt;</code> contains the following encrypted data objects</td>
</tr>
<tr>
<td>7F 4E <code>&lt;L7F4E&gt;</code> <code>&lt;certificate body&gt;</code></td>
</tr>
<tr>
<td>5F 37 <code>&lt;L5F37&gt;</code> <code>&lt;certificate signature&gt;</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. '90 00' in a valid SM response.</td>
</tr>
<tr>
<td>2. ISO checking error or '63 00' in a valid SM response.</td>
</tr>
<tr>
<td>3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.</td>
</tr>
<tr>
<td>4. ISO checking error or '63 00' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.</td>
</tr>
</tbody>
</table>

### 3.6.6 Test case ISO7816_J_6

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a missing Holder Authorization.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td></td>
</tr>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
<td></td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
<td></td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

#### 3. Test scenario

| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
<Checksum> 00'  
- `<Cryptogram>` contains the following encrypted data objects  
  83 <L83>  
  `<Certification Authority Reference>`  
- The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| | 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1a.  
`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
<Checksum> <Le>'  
- `<Cryptogram>` contains the following encrypted data objects  
  7F 4E `<L7F4E>` `<certificate body>`  
  5F 37 `<L5F37>` `<certificate signature>`  
- The certificate does not contain a certificate holder authorization |
| | 3. Send the given MSE: Set DST APDU to the eMRTD.  
`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
<Checksum> 00'  
- `<Cryptogram>` contains the following encrypted data objects  
  83 <L83>  
  `<Certification Authority Reference>`  
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. |
| | 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
<Checksum> <Le>'  
- `<Cryptogram>` contains the following encrypted data objects  
  7F 4E `<L7F4E>` `<certificate body>`  
  5F 37 `<L5F37>` `<certificate signature>` |

#### Expected results

| Expected results | 1. ’90 00’ in a valid SM response  
2. ISO checking error or ‘6300’ in a valid SM response.  
3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.  
4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification. |

### 3.6.7 Test case ISO7816_J_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a missing effective date.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
</tbody>
</table>
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   \(0C\ 22\ 81\ B6\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ 00'\)
   - \(<Cryptogram>\) contains the following encrypted data objects
     \(83\ <L83>\ <Certification\ \ Authority\ \ Reference>\)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the "Certificate Set 1" chapter as DV_CERT_1b.
   \(0C\ 2A\ 00\ BE\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ <Le>’\)
   - \(<Cryptogram>\) contains the following encrypted data objects
     \(7F\ 4E\ <L7F4E>\ <certificate\ \ body>\)
     \(5F\ 37\ <L5F37>\ <certificate\ \ signature>\)
   - The certificate does not have a certificate effective date tag.

3. Send the given MSE: Set DST APDU to the eMRTD.
   \(0C\ 22\ 81\ B6\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ 00'\)
   - \(<Cryptogram>\) contains the following encrypted data objects
     \(83\ <L83>\ <Certification\ \ Authority\ \ Reference>\)
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the "Certificate Set 1" chapter as IS_CERT_1.
   \(0C\ 2A\ 00\ BE\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ <Le>’\)
   - \(<Cryptogram>\) contains the following encrypted data objects
     \(7F\ 4E\ <L7F4E>\ <certificate\ \ body>\)
     \(5F\ 37\ <L5F37>\ <certificate\ \ signature>\)

### Expected results

1. '90 00' in a valid SM response.
2. ISO checking error or '6300' in a valid SM response.
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or '6300' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

### 3.6.8 Test case ISO7816_J_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a missing expiration date.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been</td>
</tr>
</tbody>
</table>
performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00`
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1c.
   \`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>'
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • The certificate does not have a certificate expiration date tag.

3. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00`
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   \`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

Expected results

1. '90 00' in a valid SM response
2. ISO checking error or '6300' in a valid SM response.
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or '6300' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

3.6.9 Test case ISO7816_J_9

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with an incorrect encoded effective date. (bad BCD coding)</td>
</tr>
<tr>
<td></td>
<td>Note: The date format verification is not mandatory for the chip. This test is set optional.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>---------</td>
<td>-----</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DATE</td>
</tr>
</tbody>
</table>

### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`

   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1d.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’

   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`
   - The certificate contains a badly encoded BCD effective date.

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`

   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’

   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`

### Expected results
1. ’90 00’ in a valid SM response
2. ISO checking error or ’63 00’ in a valid SM response.
3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or ’63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

#### 3.6.10 Test case ISO7816_J_10

| Test - ID | ISO7816_J_10 |
| Purpose | Test a DV certificate with an incorrect encoded expiration date. (bad BCD coding)  
Note: The date format verification is not mandatory for the chip. This test is set optional. |
| Version | 1.2 |
| Profile | TA, DATE |
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • The certificate contains a badly encoded BCD expiration date.  
3. Send the given MSE: Set DST APDU to the eMRTD.  
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature> |
| Expected results | 1. ‘90 00’ in a valid SM response  
2. ISO checking error or ‘6300’ in a valid SM response.  
3. ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.  
4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification. |
3.6.11 Test case ISO7816_J_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the “Current Date” update mechanism with a new foreign IS certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   \‘0C 22 81 B6 \<Lc> 87 \<L87> 01 \<Cryptogram> 8E 08 \<Checksum> 00’
   - \<Cryptogram> contains the following encrypted data objects
     83 \<L83> \<Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 2” chapter as DV_CERT_2.
   \‘0C 2A 00 BE \<Lc> 87 \<L87> 01 \<Cryptogram> 8E 08 \<Checksum> \<Le>’
   - \<Cryptogram> contains the following encrypted data objects
     7F 4E \<L7F4E> \<certificate body>
     5F 37 \<L5F37> \<certificate signature>
   - This DV-certificate is marked as a foreign DV-certificate.
3. Send the given MSE: Set DST APDU to the eMRTD.
   \‘0C 22 81 B6 \<Lc> 87 \<L87> 01 \<Cryptogram> 8E 08 \<Checksum> 00’
   - \<Cryptogram> contains the following encrypted data objects
     83 \<L83> \<Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 2” chapter as IS_CERT_2a.
   \‘0C 2A 00 BE \<Lc> 87 \<L87> 01 \<Cryptogram> 8E 08 \<Checksum> \<Le>’
   - \<Cryptogram> contains the following encrypted data objects
     7F 4E \<L7F4E> \<certificate body>
     5F 37 \<L5F37> \<certificate signature>
   - This certificate has an advanced effective date. Since the DV certificate was marked as a foreign one, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
5. Send the given MSE: Set DST APDU to the eMRTD.
   \‘0C 22 81 B6 \<Lc> 87 \<L87> 01 \<Cryptogram> 8E 08 \<Checksum> 00’
6. Send the appropriate DV-Certificate as specified in the “Certificate Set 2” chapter as DV_CERT_2.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This DV-certificate is marked as a foreign DV-certificate.

7. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 6 has to be used.

8. Send the appropriate IS-Certificate as specified in the “Certificate Set 2” chapter as IS_CERT_2b.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This certificate expiration date is BEFORE the effective date of the IS-Certificate used in step 4.

<table>
<thead>
<tr>
<th>Test case ISO7816_J_12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test - ID</strong></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Version</strong></td>
</tr>
<tr>
<td><strong>Profile</strong></td>
</tr>
<tr>
<td><strong>Preconditions</strong></td>
</tr>
</tbody>
</table>
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   ‘00 22 81 B6 <Lc> 83 <Certification Authority Reference>’
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
   - The APDU is send in plain without Secure Messaging

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The APDU is send as a valid SM APDU.
   After step 2, the passport is reset and the preconditions of this test case are reestablished.

3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
   - The APDU is send as a valid SM APDU.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘00 2A 00 BE <Lc> 7F 4E <L7F4E> <body> 5F 37 <L5F37> <signature>’

5. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 4 has to be used.
   - The APDU is send as a valid SM APDU.

Expected results

1. ‘90 00’ or Checking error. A chip OS may accept the use of an unprotected MSE APDU, however, the SM channel MUST be closed as soon as an unprotected APDU is sent. Therefore, the response MUST be send without SM encoding.
2. ISO checking error. Since the SM channel MUST have been closed in Step 1, the chip MUST return an error without SM encoding here.
3. ‘90 00’ in a valid SM response
4. ISO checking error. The SM channel MUST be closed as soon as an
unprotected APDU is sent. The error code SHALL be returned as plain data without SM encoding.

5. ISO checking error. Since the SM channel MUST have been closed in Step 4, the chip MUST return an error without SM encoding here.

### 3.6.13 Test case ISO7816_J_13

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the MSE: Set DST command with an invalid class byte.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td>'8C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td>• The class byte is set to an invalid value.</td>
</tr>
<tr>
<td>2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped.</td>
</tr>
<tr>
<td>The Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ISO checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response.</td>
</tr>
<tr>
<td>2. Skipped or ‘90 00’ in a valid SM response</td>
</tr>
</tbody>
</table>

### 3.6.14 Test case ISO7816_J_14

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 1.1</td>
</tr>
</tbody>
</table>

### 3.6.15 Test case ISO7816_J_15

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the Verify Certificate command with an invalid class byte.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been</td>
</tr>
</tbody>
</table>
performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | Send the given MSE: Set DST APDU to the eMRTD.  
   | ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   | - <Cryptogram> contains the following encrypted data objects  
   |   | 83 <L83> Certification Authority Reference  
   | - The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. | Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
   | ‘8C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   | - <Cryptogram> contains the following encrypted data objects  
   |   | 7F 4E <L7F4E> certificate body  
   |   | 5F 37 <L5F37> certificate signature  
   | - The class byte has been set to an invalid value (‘8C’). |
| 3. | If the error code in step 2 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped.  
   | The Command APDU as defined in the ICS (Annex A, Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions. |

### Expected results

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | '90 00’ in a valid SM response  
   | 2. | ISO checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response.  
   | 3. | Skipped or ‘90 00’ in a valid SM response |

### 3.6.16 Test case ISO7816_J_16

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| Test - ID | ISO7816_J_16  
   | Version | Deleted in version 1.1 |

### 3.6.17 Test case ISO7816_J_17

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| Test - ID | ISO7816_J_17  
   | Purpose | Test with an invalid certificate body tag.  
   | Version | 1.2  
   | Profile | TA  
   | Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
   |   | 2. The Chip Authentication mechanism MUST have been performed as well.  
   |   | 3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
Test plan for eMRTDs with EACv1

| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
|              | ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
|              | <Checksum> 00’  
|              | • <Cryptogram> contains the following encrypted data objects  
|              | 83 <L83> <Certification Authority Reference>  
|              | • The Certification Authority Reference MUST be used as read from the  
|              | EF.CVCA file.  
|              | 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”  
|              | chapter as DV_CERT_1.  
|              | ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
|              | <Checksum> <Le>’  
|              | • <Cryptogram> contains the following encrypted data objects  
|              | 7F 4F <L7F4F> <certificate body>  
|              | 5F 37 <L5F37> <certificate signature>  
|              | • The certificate body tag has been changed to ‘7F 4F’  
|              | 3. Send the given MSE: Set DST APDU to the eMRTD.  
|              | ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
|              | <Checksum> 00’  
|              | • <Cryptogram> contains the following encrypted data objects  
|              | 83 <L83> <Certification Authority Reference>  
|              | • The Certification Holder Reference stored inside the DV-Certificate  
|              | sent in step 2 has to be used.  
|              | 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1”  
|              | chapter as IS_CERT_1.  
|              | ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
|              | <Checksum> <Le>’  
|              | • <Cryptogram> contains the following encrypted data objects  
|              | 7F 4E <L7F4E> <certificate body>  
|              | 5F 37 <L5F37> <certificate signature>  
| Expected results | 1. ’90 00’ in a valid SM response  
|                  | 2. ISO checking error or ‘63 00’ in a valid SM response.  
|                  | 3. ’90 00’ or ISO checking error in a valid SM response. Note that some chip  
|                  | OS accept the selection of an unavailable public key and return an error  
|                  | only when the public key is used for the selected purpose.  
|                  | 4. ISO checking error or ‘63 00’ in a valid SM response. Since the DV  
|                  | certificate was not verified successfully, it MUST NOT be possible to use  
|                  | it as the trust point for the IS-Certificate verification.  

### 3.6.18 Test case ISO7816_J_18

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with an invalid certificate signature tag.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the
### Test Scenario

| 1. | Send the given MSE: Set DST APDU to the eMRTD. |
|    | `'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' |
|    | - `<Cryptogram>` contains the following encrypted data objects |
|    | 83 `<L83>` `<Certification Authority Reference>` |
|    | - The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. | Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. |
|    | `'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' |
|    | - `<Cryptogram>` contains the following encrypted data objects |
|    | 7F 4E `<L7F4E>` `<certificate body>` |
|    | 5F 38 `<L5F38>` `<certificate signature>` |
|    | - The certificate signature tag has been changed to ‘5F 38’ |
| 3. | Send the given MSE: Set DST APDU to the eMRTD. |
|    | `'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' |
|    | - `<Cryptogram>` contains the following encrypted data objects |
|    | 83 `<L83>` `<Certification Authority Reference>` |
|    | - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. |
| 4. | Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. |
|    | `'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' |
|    | - `<Cryptogram>` contains the following encrypted data objects |
|    | 7F 4E `<L7F4E>` `<certificate body>` |
|    | 5F 37 `<L5F37>` `<certificate signature>` |

### Expected Results

| 1. | ‘90 00’ in a valid SM response |
| 2. | ISO checking error or ‘63 00’ in a valid SM response. |
| 3. | ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. |
| 4. | ISO checking error or ‘63 00’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification. |

### 3.6.19 Test case ISO7816_J_19

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with an incorrect Gregorian effective date.</td>
</tr>
<tr>
<td>Note:</td>
<td>The date format verification is not mandatory for the chip. This test is set optional.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DATE</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The certificate contains an invalid Gregorian effective date.

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

### Expected results

1. '90 00' in a valid SM response
2. ISO checking error or '63 00' in a valid SM response.
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or '63 00' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

### 3.6.20 Test case ISO7816_J_20

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with an incorrect Gregorian expiration date.</td>
</tr>
</tbody>
</table>

Note:
The date format verification is not mandatory for the chip. This test is set optional.

<table>
<thead>
<tr>
<th>Version</th>
<th>1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>TA, DATE</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     - 83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1g.
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     - 7F 4E <L7F4E> <certificate body>
     - 5F 37 <L5F37> <certificate signature>
   - The certificate contains an invalid Gregorian expiration date.

3. Send the given MSE: Set DST APDU to the eMRTD.
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     - 83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     - 7F 4E <L7F4E> <certificate body>
     - 5F 37 <L5F37> <certificate signature>

**Expected results**

1. '90 00' in a valid SM response
2. ISO checking error or '6300' in a valid SM response.
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or '6300' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.
### 3.6.21 Test case ISO7816_J_21

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with an expiration date BEFORE the effective date.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

#### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1h.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The certificate contains an expiration date BEFORE the effective date.

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

#### Expected results
1. '90 00' in a valid SM response
2. ISO checking error or '6300' in a valid SM response.
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or '6300' in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.
### 3.6.22 Test case ISO7816_J_22

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test correct removal of temporary keys.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

#### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   ```
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ```
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Reset the chip, perform the “Open ePassport Application” procedure and the Chip Authentication.
   Send the given MSE: Set DST APDU to the eMRTD.
   ```
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ```
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

#### Expected results
1. ‘90 00’ in a valid SM response.
2. ‘90 00’ in a valid SM response
3. ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
4. ISO checking error or ‘6300’ in a valid SM response. The temporary key of the DV certificate MUST have been deleted during the reset. Therefore it MUST NOT be possible to verify the IS certificate based on this key.
### 3.6.23 Test case ISO7816_J_23

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with invalid OID in the Certificate Holder Authorization element.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions| 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario| 1. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   - <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1i.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   - <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   - The certificate has an invalid OID in the Certificate Holder Authorization element. Note: If the chip supports further OIDs in addition to the ones specified in [R11], this MUST be stated in the ICS (See 4.3). For this test an OID MUST be used which is NOT supported by the chip.  
3. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   - <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   - <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature> |
| Expected results| 1. '90 00' in a valid SM response  
2. ISO checking error or '6300' in a valid SM response.  
3. '90 00' or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error |
only when the public key is used for the selected purpose.

4. ISO checking error or ‘6300’ in a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS-Certificate verification.

### 3.6.24 Test case ISO7816_J_24

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate invalid OID in the Public Key element.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.

```
0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
```

- <Cryptogram> contains the following encrypted data objects
  - 83 <L83> <Certification Authority Reference>
- The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1j.

```
0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
```

- <Cryptogram> contains the following encrypted data objects
  - 7F 4E <L7F4E> <certificate body>
  - 5F 37 <L5F37> <certificate signature>
- The certificate has an invalid OID in the Public Key element.

3. Send the given MSE: Set DST APDU to the eMRTD.

```
0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
```

- <Cryptogram> contains the following encrypted data objects
  - 83 <L83> <Certification Authority Reference>
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.

```
0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
```

- <Cryptogram> contains the following encrypted data objects
  - 7F 4E <L7F4E> <certificate body>
  - 5F 37 <L5F37> <certificate signature>

**Expected results**

1. '90 00’ in a valid SM response
2. ISO checking error or ‘6300’ in a valid SM response.
3. '90 00’ or ISO checking error in a valid SM response. Note that some chip
OS accept the selection of an unavailable public key and return an error 
only when the public key is used for the selected purpose.

4. ISO checking error or ‘6300’ in a valid SM response. Since the DV 
 certificate was not verified successfully, it MUST NOT be possible to use 
it as the trust point for the IS-Certificate verification.

3.6.25 Test case ISO7816_J_25

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the CVCA root key selection with a wrong name (CAR) - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions| 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the 
   EF.CVCA file (Primary trust point). |
| Test scenario| 1. Send the MSE Set DST APDU to initiate the certificate verification to the 
eMRTD with a wrong CAR.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 
   <Checksum> 00'  
   • <Cryptogram> contains the encrypted wrong CVCA key Name.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 
12” chapter as DV_CERT_12a.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 
   <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • The certificate is issued by the CVCA whose selection SHOULD have 
     failed.  
   • This certificate has an advanced effective date. Since the DV 
     certificate failed, the chip MUST NOT update the current date.  
   • Reset the chip after this step and restore the preconditions for this test 
     case before the next step is performed.  
3. Send the MSE Set DST APDU to initiate the certificate verification to the 
eMRTD with a correct CVCA key name (CAR).  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 
   <Checksum> 00'  
   • <Cryptogram> contains the encrypted Name (CAR)  
   • The Certification Authority Reference MUST be used as read from the 
     EF.CVCA file.  
4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” 
chapter as DV_CERT_1.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 
   <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects|
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. '90 00' or ISO checking error in a valid SM response. A chip may permit the selection of an unknown key.</td>
</tr>
<tr>
<td>2. ISO checking error or warning processing '63 00' in a valid SM response</td>
</tr>
<tr>
<td>3. '90 00' in a valid SM response</td>
</tr>
<tr>
<td>4. '90 00' in a valid SM response</td>
</tr>
</tbody>
</table>

#### 3.6.26 Test case ISO7816_J_26

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate body tag - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the MSE Set DST APDU to initiate the certificate verification:
   \[ \text{C2 22 B6}<L_{c} \text{ 87}<L_{m} \text{ 01}<\text{Cryptogram} \text{ 8E 08}<\text{Checksum} \text{ 00} \]
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12b:
   \[ \text{C2 A0 BE}<L_{c} \text{ 87}<L_{m} \text{ 01}<\text{Cryptogram} \text{ 8E 08}<\text{Checksum} \text{ Le} > \]
   - `<Cryptogram>` contains the following encrypted data objects:
     7F 4F <L_{7F4F}> <certificate body>
     5F 37 <L_{5F37}> <certificate signature>
   - The tag of the certificate body is wrong.
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA:
   \[ \text{C2 22 B6}<L_{c} \text{ 87}<L_{m} \text{ 01}<\text{Cryptogram} \text{ 8E 08}<\text{Checksum} \text{ 00} \]
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Expected results</th>
<th>1. '90 00' in a valid SM response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. ISO checking error or warning processing '63 00' in a valid SM response</td>
</tr>
<tr>
<td></td>
<td>3. '90 00' in a valid SM response</td>
</tr>
<tr>
<td></td>
<td>4. '90 00' in a valid SM response</td>
</tr>
</tbody>
</table>

### 3.6.27 Test case ISO7816_J_27

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate signature tag - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the MSE Set DST APDU to initiate the certificate verification. 
   \`OC 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
   - \<Cryptogram> contains the encrypted CVCA key Name (CAR).  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12c. 
   \`OC 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`
   - \<Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>
   - The tag of the certificate signature is wrong.  
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.  
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA. 
   \`OC 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
   - \<Cryptogram> contains the encrypted CVCA key Name (CAR)
• The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’

   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

   • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results

1. '90 00' in a valid SM response
2. ISO checking error or warning processing '63 00' in a valid SM response
3. '90 00' in a valid SM response
4. '90 00' in a valid SM response

### 3.6.28 Test case ISO7816_J_28

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_28</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate body length - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

#### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario

1. Send the MSE Set DST APDU to initiate the certificate verification

   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’

   • <Cryptogram> contains the encrypted CVCA key Name (CAR).  ’

   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12d.

   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’

   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> + 1 <certificate body>
     5F 37 <L5F37> <certificate signature>

   • The length of the certificate body is inconsistent.

   • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.

   • Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the
eMRTD with the CAR of the CVCA.

\`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00`'  
- `<Cryptogram>` contains the encrypted CVCA key Name (CAR)  
- The Certification Authority Reference MUST be used as read from the
  EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”
   chapter as DV_CERT_1.

\`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>’
- `<Cryptogram>` contains the following encrypted data objects
  7F 4E <L7F4E> <certificat body>
  5F 37 <L5F37> <certificate signature>
- This certificate expiration date is BEFORE the effective date of the
  DV-Certificate used in step 2.

**Expected results**
1. '90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response

### 3.6.29 Test case ISO7816_J_29

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_29</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Test a DV certificate with a wrong certificate signature length - Current date not updated</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the
   EF.CVCA file (Primary trust point).

**Test scenario**
1. Send the MSE Set DST APDU to initiate the certificate verification.

\`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00`'  
- `<Cryptogram>` contains the encrypted CVCA key Name (CAR).
- The Certification Authority Reference MUST be used as read from the
  EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set
   12” chapter as DV_CERT_12e.

\`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>’
- `<Cryptogram>` contains the following encrypted data objects
  7F 4E <L7F4E> <certificat body>
  5F 37 <L5F37> + 1 <certificate signature>
- The length of the certificate signature is inconsistent.
- This certificate has an advanced effective date. Since the DV
  certificate failed, the chip MUST NOT update the current date.
Test plan for eMRTDs with EACv1

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.

   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'

   - <Cryptogram> contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>

   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results
1. '90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response

3.6.30 Test case ISO7816_J_30

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate signature (Last byte increased by 1) - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.
   2. The Chip Authentication mechanism MUST have been performed as well.
   3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

| Test scenario | 1. Send the MSE Set DST APDU to initiate the certificate verification
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the encrypted CVCA key Name (CAR).
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

   2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12f.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature + 1> |
• The certificate signature is wrong. It is obtained by increasing a correct signature by one.
• This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
• Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the encrypted CVCA key Name (CAR)
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results
1. '90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response

3.6.31 Test case ISO7816_J_31

Test - ID | ISO7816_J_31
---|---
Purpose | Test a DV certificate with a wrong certificate signature (Dropping last byte of the signature) - Current date not updated
Version | 1.2
Profile | TA

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the MSE Set DST APDU to initiate the certificate verification.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the encrypted CVCA key Name (CAR).
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12g
Test plan for eMRTDs with EACv1

1. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.

   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`

   - <Cryptogram> contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.

   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`

   - <Cryptogram> contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

### Expected results

1. ‘90 00’ in a valid SM response
2. ISO checking error or warning processing ‘63 00’ in a valid SM response
3. ‘90 00’ in a valid SM response
4. ‘90 00’ in a valid SM response

3.6.32 Test case ISO7816_J_32

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_32</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate signature (Signature greater than the modulus) - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>RSA, TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the MSE Set DST APDU to initiate the certificate verification.  
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
Test plan for eMRTDs with EACv1

• <Cryptogram> contains the encrypted CVCA key Name (CAR).
• The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12o
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • The certificate signature is wrong. It is obtained by setting the signature to a value greater than the modulus. The length of the signature MUST match the length of the modulus.
   This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   • Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the encrypted CVCA key Name (CAR)
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results
1. ‘90 00’ in a valid SM response
2. ISO checking error or warning processing ‘63 00’ in a valid SM response
3. ‘90 00’ in a valid SM response
4. ‘90 00’ in a valid SM response

3.6.33 Test case ISO7816_J_33

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate signature (r = 0) - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>ECDSA, TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.
  2. The Chip Authentication mechanism MUST have been performed as well. |
### Test plan for eMRTDs with EACv1

#### Test scenario

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. | Send the MSE Set DST APDU to initiate the certificate verification.  
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR).  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. | Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12p  
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
   - `<Cryptogram>` contains the following encrypted data objects  
     - `7F 4E <L7F4E> <certificate body>`  
     - `5F 37 <L5F37> <certificate signature>`  
   - The certificate signature is wrong. It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime.  
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.  
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed. |
| 3. | Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.  
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR)  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 4. | Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
   - `<Cryptogram>` contains the following encrypted data objects  
     - `7F 4E <L7F4E> <certificate body>`  
     - `5F 37 <L5F37> <certificate signature>`  
   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2. |

#### Expected results

1. ‘90 00’ in a valid SM response  
2. ISO checking error or warning processing ‘63 00’ in a valid SM response  
3. ‘90 00’ in a valid SM response  
4. ‘90 00’ in a valid SM response

### 3.6.34 Test case ISO7816_J_34

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_34</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong certificate signature (s = 0) - Current date not updated</td>
</tr>
</tbody>
</table>
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Version</th>
<th>1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>ECDSA, TA</td>
</tr>
</tbody>
</table>

#### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario
1. Send the MSE Set DST APDU to initiate the certificate verification.
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR).
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12q
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> `<certificate body>`
     5F 37 <L5F37> `<certificate signature>`
   - The certificate signature is wrong. It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ is still matches the size of the prime.
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> `<certificate body>`
     5F 37 <L5F37> `<certificate signature>`
   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

#### Expected results
1. ‘90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. ‘90 00’ in a valid SM response
4. ‘90 00’ in a valid SM response
### 3.6.35 Test case ISO7816_J_35

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_35</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Test a DV certificate without selecting any root key - Current date not updated</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA</td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
                      2. The Chip Authentication mechanism MUST have been performed as well.  
                      3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| **Test scenario** | 1. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12a.  
                         '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
                         <Checksum> <Le>’  
                         - <Cryptogram> contains the following encrypted data objects  
                           7F 4E <L7F4E> <certificate body>  
                           5F 37 <L5F37> <certificate signature>  
                         - As no current key is selected, the certificate verification SHOULD fail.  
                         - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.  
                         - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.  
                         2. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.  
                            '0C 22 81 B6 <Lc> 87 <L87> 01 < Cryptogram> 8E 08  
                            <Checksum> 00’  
                            - <Cryptogram> contains the encrypted CVCA key Name (CAR)  
                            - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
                            3. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
                               '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
                               <Checksum> <Le>’  
                               - <Cryptogram> contains the following encrypted data objects  
                                 7F 4E <L7F4E> <certificate body>  
                                 5F 37 <L5F37> <certificate signature>  
                               - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2. |
| **Expected results** | 1. ISO checking error or warning processing ’63 00’ in a valid SM response  
                          2. ’90 00’ in a valid SM response  
                          3. ’90 00’ in a valid SM response |

### 3.6.36 Test case ISO7816_J_36

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_36</th>
</tr>
</thead>
</table>

119/207
### Purpose
Test a DV certificate while the Public Key D.O has a wrong O.I.D field - Current date not updated

### Version
1.2

### Profile
TA

### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario
1. Send the MSE Set DST APDU to initiate the certificate verification.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the encrypted CVCA key Name (CAR).
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12i
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The Public Key D.O. in the certificate body contains an incorrect O.I.D that does not indicate id-TA (0.4.0.127.0.7.2.2.3.x.y).
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

### Expected results
1. '90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response
### 3.6.37 Test case ISO7816_J_37

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_37</th>
</tr>
</thead>
</table>

**Purpose**
Test a DV certificate while the Public Key D.O has no O.I.D field - Current date not updated

**Version**
1.2

**Profile**
TA

**Preconditions**
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**
1. Send the MSE Set DST APDU to initiate the certificate verification.

   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR).
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12h.

   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` <certificate body>
     5F 37 `<L5F37>` <certificate signature>
   - The Public Key D.O. in the certificate body does not contain an O.I.D field.
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.

   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - `<Cryptogram>` contains the encrypted CVCA key Name (CAR)
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` <certificate body>
     5F 37 `<L5F37>` <certificate signature>
   - This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

**Expected results**
1. ’90 00’ in a valid SM response
2. ISO checking error or warning processing ‘63 00’ in a valid SM response
3. ‘90 00’ in a valid SM response
4. ‘90 00’ in a valid SM response

### 3.6.38 Test case ISO7816_J_38

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_38</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate while the Public Key D.O has no Public point field - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>ECDSA, TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
               2. The Chip Authentication mechanism MUST have been performed as well.  
               3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the MSE Set DST APDU to initiate the certificate verification.  
               ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
               - <Cryptogram> contains the encrypted CVCA key Name (CAR).  
               - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
               2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12j  
               ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
               - <Cryptogram> contains the following encrypted data objects  
                 7F 4E <L7F4E> <certificate body>  
                 5F 37 <L5F37> <certificate signature>  
               - The Public Key D.O. in the certificate body does not contain any EC Public point field.  
               - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.  
               - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.  
               3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.  
               ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
               - <Cryptogram> contains the encrypted CVCA key Name (CAR)  
               - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
               4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
               ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
               - <Cryptogram> contains the following encrypted data objects  
                 7F 4E <L7F4E> <certificate body> |
Test plan for eMRTDs with EACv1

5F 37 <L5F37> <certificate signature>
- This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

| Expected results | 1. '90 00' in a valid SM response  
2. ISO checking error or warning processing '63 00' in a valid SM response  
3. '90 00' in a valid SM response  
4. '90 00' in a valid SM response |

3.6.39 Test case ISO7816_J_39

| Test - ID | ISO7816_J_39 |
| Purpose | Test a DV certificate while the Public Key D.O has no Modulus field - Current date not updated |
| Version | 1.2 |
| Profile | RSA, TA |
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the MSE Set DST APDU to initiate the certificate verification.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
- <Cryptogram> contains the encrypted CVCA key Name (CAR).  
- The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12k  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
- <Cryptogram> contains the following encrypted data objects  
  7F 4E <L7F4E> <certificate body>  
  5F 37 <L5F37> <certificate signature>  
- The Public Key D.O. in the certificate body does not contain any RSA Modulus field.  
- This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.  
- Reset the chip after this step and restore the preconditions for this test case before the next step is performed.  
3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
- <Cryptogram> contains the encrypted CVCA key Name (CAR)  
- The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” |
Test plan for eMRTDs with EACv1

| Expected results | 1. '90 00' in a valid SM response
|                  | 2. ISO checking error or warning processing '63 00' in a valid SM response
|                  | 3. '90 00' in a valid SM response
|                  | 4. '90 00' in a valid SM response

### 3.6.40 Test case ISO7816_J_40

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_40</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate while the Public Key D.O has no public exponent field - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>RSA, TA</td>
</tr>
</tbody>
</table>

#### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario

1. Send the MSE Set DST APDU to initiate the certificate verification.
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - <Cryptogram> contains the encrypted CVCA key Name (CAR).
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12.
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The Public Key D.O. in the certificate body does not contain any RSA public exponent field.
   - This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.
   - Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the eMRTD with the CAR of the CVCA.
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
Test plan for eMRTDs with EACv1

1. <Cryptogram> contains the encrypted CVCA key Name (CAR)
2. The Certification Authority Reference MUST be used as read from the EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’

   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.

Expected results
1. ’90 00’ in a valid SM response
2. ISO checking error or warning processing ’63 00’ in a valid SM response
3. ’90 00’ in a valid SM response
4. ’90 00’ in a valid SM response

3.6.41 Test case ISO7816_J_41

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_41</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate while the Public Key D.O contains an unknown D.O. - Current date not updated</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
</table>
| 1. Send the MSE Set DST APDU to initiate the certificate verification. ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’ |
| • <Cryptogram> contains the encrypted CVCA key Name (CAR). |
| • The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 12” chapter as DV_CERT_12m
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’ |
| • <Cryptogram> contains the following encrypted data objects
   7F 4E <L7F4E> <certificate body>
   5F 37 <L5F37> <certificate signature>
| • The Public Key D.O. in the certificate body contains an unknown D.O (tag ’77”). |
| • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. |
| • Reset the chip after this step and restore the preconditions for this test |
case before the next step is performed.

3. Send the MSE Set DST APDU to initiate the certificate verification to the
   eMRTD with the CAR of the CVCA.
   \(0C\ 22\ 81\ B6\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ 00'\n   
   • <Cryptogram> contains the encrypted CVCA key Name (CAR)
   • The Certification Authority Reference MUST be used as read from the
     EF.CVCA file.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”
   chapter as DV_CERT_1.
   \(0C\ 2A\ 00\ BE\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ <Le>'
   
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This certificate expiration date is BEFORE the effective date of the
     DV-Certificate used in step 2.

Expected results
1. '90 00' in a valid SM response
2. ISO checking error or warning processing '63 00' in a valid SM response
3. '90 00' in a valid SM response
4. '90 00' in a valid SM response

3.6.42 Test case ISO7816_J_42

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_42</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8 (Merged with ISO7816_J_41)</td>
</tr>
</tbody>
</table>

3.6.43 Test case ISO7816_J_43

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_43</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA (\Rightarrow) IS key</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been
   performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the
   EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   \(0C\ 22\ 81\ B6\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ 00'\n   
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the
     EF.CVCA file.

2. Send the appropriate IS-Certificate as specified in the “Certificate Set 10”
   chapter as IS_CERT_10.
   \(0C\ 2A\ 00\ BE\ <Lc>\ 87\ <L87>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ <Le>'
   
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The eMRTD MUST return status bytes ‘90 00’ in a valid SM response</td>
</tr>
<tr>
<td>2. The eMRTD MUST return an ISO checking error or status bytes ‘63 00’ in a valid SM response</td>
</tr>
</tbody>
</table>

### 3.6.44 Test case ISO7816_J_44

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_44</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA $\Rightarrow$ domestic DV $\Rightarrow$ CVCA</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | ![](image)

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
</tr>
<tr>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a. '0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
<tr>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>3. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
</tr>
<tr>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>4. Send the appropriate CA-Certificate as specified in the “Certificate Set 10” chapter as LINK_CERT_10. '0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
<tr>
<td><img src="image" alt="" /></td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

| Expected results | 1. The eMRTD MUST return status bytes '90 00' in a valid SM response
|                  | 2. The eMRTD MUST return status bytes '90 00' in a valid SM response
|                  | 3. The eMRTD MUST return status bytes '90 00' in a valid SM response
|                  | 4. The eMRTD MUST return status bytes an ISO checking error or status bytes '63 00' in a valid SM response |

### 3.6.45 Test case ISO7816_J_45

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_45</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇄ foreign DV ⇄ CVCA</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

#### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   
   - `<Cryptogram>` contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
     - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10b.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   
   - `<Cryptogram>` contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   
   - `<Cryptogram>` contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
     - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate CA-Certificate as specified in the “Certificate Set 10” chapter as LINK_CERT_10.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   
   - `<Cryptogram>` contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  

#### Expected results

1. The eMRTD MUST return status bytes '90 00' in a valid SM response
2. The eMRTD MUST return status bytes '90 00' in a valid SM response
### 3.6.46 Test case ISO7816_J_46

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_46</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ domestic DV ⇒ domestic DV</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Precondition  | 1. The "Open ePassport Application" procedure MUST have been performed.  
               2. The Chip Authentication mechanism MUST have been performed as well.  
               3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
               '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
               - <Cryptogram> contains the following encrypted data objects  
                 83 <L83> <Certification Authority Reference>  
               - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
               2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a.  
               '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
               - <Cryptogram> contains the following encrypted data objects  
                 7F 4E <L7F4E> <certificate body>  
                 5F 37 <L5F37> <certificate signature>  
               3. Send the given MSE: Set DST APDU to the eMRTD.  
               '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
               - <Cryptogram> contains the following encrypted data objects  
                 83 <L83> <Certification Authority Reference>  
               - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
               4. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10c.  
               '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
               - <Cryptogram> contains the following encrypted data objects  
                 7F 4E <L7F4E> <certificate body>  
                 5F 37 <L5F37> <certificate signature> |
| Expected results | 1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                      2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                      3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                      4. The eMRTD MUST return status bytes an ISO checking error or status bytes ’63 00’ in a valid SM response. |
## 3.6.47 Test case ISO7816_J_47

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇔ domestic DV ⇔ foreign DV</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>,'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10d.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>,'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

### Expected results
1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
4. The eMRTD MUST return status bytes an ISO checking error or status bytes ’63 00’ in a valid SM response.
### 3.6.48 Test case ISO7816_J_48

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_48</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ foreign DV ⇒ domestic DV</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

#### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   
   ```
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10b.
   
   ```
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   ```
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10c.
   
   ```
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   ```
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

#### Expected results
1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response
4. The eMRTD MUST return status bytes an ISO checking error or status bytes ’63 00’ in a valid SM response.
### 3.6.49 Test case ISO7816_J_49

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_49</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Test the transition CVCA ⊛ foreign DV ⊛ foreign DV</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA</td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
                    2. The Chip Authentication mechanism MUST have been performed as well.  
                    3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| **Test scenario** | 1. Send the given MSE: SET DST APDU to the eMRTD.  
                                `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
                                • `<Cryptogram>` contains the following encrypted data objects  
                                   83 <L83> <Certification Authority Reference>  
                                   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
                                2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10b.  
                                `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
                                • `<Cryptogram>` contains the following encrypted data objects  
                                   7F 4E <L7F4E> <certificate body>  
                                   5F 3F <L5F3F> <certificate signature>  
                                3. Send the given MSE: SET DST APDU to the eMRTD.  
                                `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
                                • `<Cryptogram>` contains the following encrypted data objects  
                                   83 <L83> <Certification Authority Reference>  
                                   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
                                4. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10d.  
                                `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
                                • `<Cryptogram>` contains the following encrypted data objects  
                                   7F 4E <L7F4E> <certificate body>  
                                   5F 3F <L5F3F> <certificate signature> |
| **Expected results** | 1. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                           2. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                           3. The eMRTD MUST return status bytes ’90 00’ in a valid SM response  
                           4. The eMRTD MUST return status bytes an ISO checking error or status bytes ’63 00’ in a valid SM response. |
### 3.6.50 Test case ISO7816_J_50

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ DV ⇒ IS ⇒ foreign DV</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions   | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario   | 1. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   • <Cryptogram> contains the following encrypted data objects  
   83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11a.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
   7F 4E <L7F4E> <certificate body>  
   5F 37 <L5F37> <certificate signature>  
3. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   • <Cryptogram> contains the following encrypted data objects  
   83 <L83> <Certification Authority Reference>  
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11a.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
   7F 4E <L7F4E> <certificate body>  
   5F 37 <L5F37> <certificate signature>  
5. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   • <Cryptogram> contains the following encrypted data objects  
   83 <L83> <Certification Authority Reference>  
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Expected results</th>
<th>Test case ISO7816_J_51</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. '90 00’ in a valid SM response</td>
<td>3.6.51 Test case ISO7816_J_51</td>
</tr>
<tr>
<td>2. '90 00’ in a valid SM response</td>
<td>Test - ID ISO7816_J_51</td>
</tr>
<tr>
<td>3. '90 00’ in a valid SM response</td>
<td>Purpose Test the transition CVCA $\Rightarrow$ DV $\Rightarrow$ IS $\Rightarrow$ domestic DV</td>
</tr>
<tr>
<td>4. '90 00’ in a valid SM response</td>
<td>Version 1.2</td>
</tr>
<tr>
<td>5. '90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.</td>
<td>Profile TA</td>
</tr>
<tr>
<td>6. ISO checking error or '63 00’ in a valid SM response.</td>
<td>Preconditions</td>
</tr>
</tbody>
</table>

### 3.6.51 Test case ISO7816_J_51

<table>
<thead>
<tr>
<th>Test scenario</th>
<th>Test scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Send the given MSE: Set DST APDU to the eMRTD.</td>
<td>1. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
</tr>
<tr>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
<tr>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td>3. Send the given MSE: Set DST APDU to the eMRTD.</td>
<td>3. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00’</td>
</tr>
<tr>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
<td>• The Certification Authority Reference stored inside the DV-Certificate sent in step 2 has to be used.</td>
</tr>
<tr>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
</tbody>
</table>
<Cryptogram> contains the following encrypted data objects
7F 4E <L7F4E> <certificate body>
5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.

6. Send the appropriate DV-Certificate as specified in the “Certificate Set
   11” chapter as DV_CERT_11c.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

Expected results
1. '90 00’ in a valid SM response
2. '90 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response
5. '90 00’ or ISO checking error in a valid SM response. Note that some chip
   OS accept the selection of an unavailable public key and return an error
   only when the public key is used for the selected purpose.
6. ISO checking error or ‘63 00’ in a valid SM response.

3.6.52 Test case ISO7816_J_52

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_52</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ DV ⇒ IS ⇒ IS</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
   2. The Chip Authentication mechanism MUST have been performed as well.  
   3. The Certification Authority Reference MUST have been read from the 
      EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the 
     EF.CVCA file.  
   2. Send the appropriate DV-Certificate as specified in the “Certificate Set
      11” chapter as DV_CERT_11a.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’ |
Test plan for eMRTDs with EACv1

- `<Cryptogram>` contains the following encrypted data objects
  7F 4E `<L7F4E>` <certificate body>
  5F 37 `<L5F37>` <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 `<Lc>` 87 `<L87>` 01 `<Cryptogram>` 8E 08
   `<Checksum>` 00'
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate
     sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11”
   chapter as IS_CERT_11a.
   '0C 2A 00 BE `<Lc>` 87 `<L87>` 01 `<Cryptogram>` 8E 08
   `<Checksum>` `<Le>'`
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` <certificate body>
     5F 37 `<L5F37>` <certificate signature>

5. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 `<Lc>` 87 `<L87>` 01 `<Cryptogram>` 8E 08
   `<Checksum>` 00'
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` <Certification Authority Reference>
   - The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.

6. Send the appropriate IS-Certificate as specified in the “Certificate Set 11”
   chapter as IS_CERT_11b.
   '0C 2A 00 BE `<Lc>` 87 `<L87>` 01 `<Cryptogram>` 8E 08
   `<Checksum>` `<Le>'`
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` <certificate body>
     5F 37 `<L5F37>` <certificate signature>

Expected results
1. '90 00’ in a valid SM response
2. '90 00’ in a valid SM response
3. '90 00’ in a valid SM response
4. '90 00’ in a valid SM response
5. '90 00’ or ISO checking error in a valid SM response. Note that some chip
   OS accept the selection of an unavailable public key and return an error
   only when the public key is used for the selected purpose.
6. ISO checking error or '63 00’ in a valid SM response.

3.6.53 Test case ISO7816_J_53

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_53</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ DV ⇒ IS ⇒ CVCA</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions     | 1. The "Open ePassport Application" procedure MUST have been
                   | performed.        |
### Test plan for eMRTDs with EACv1

**2.** The Chip Authentication mechanism MUST have been performed as well.

**3.** The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. **Send the given MSE: Set DST APDU to the eMRTD.**
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. **Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11a.**
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. **Send the given MSE: Set DST APDU to the eMRTD.**
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. **Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11a.**
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. **Send the given MSE: Set DST APDU to the eMRTD.**
   ```
   0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. **Send the appropriate CVCA-Certificate as specified in the “Certificate Set 11” chapter as LINK_CERT_11a.**
   ```
   0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   ```
   - **<Cryptogram>** contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

### Expected results

1. ’90 00’ in a valid SM response
2. ’90 00’ in a valid SM response
3. ’90 00’ in a valid SM response
4. ’90 00’ in a valid SM response
5. ‘90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.

6. ISO checking error or ‘63 00’ in a valid SM response.

### 3.6.54 Test case ISO7816_J_54

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>ISO7816_J_54</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ CVCA ⇒ IS</td>
</tr>
<tr>
<td>Version</td>
<td>Has been moved to M_5 in version 1.1</td>
</tr>
</tbody>
</table>

### 3.6.55 Test case ISO7816_J_55

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a DV certificate with a wrong Public Key (shorter key length).</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism must have been performed as well.
3. The Certification Authority Reference must have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 \(\text{Lc}\) 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference must be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 14” chapter as DV_CERT_14b.
   \`0C 2A 00 BE \(\text{Lc}\) 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> \(\text{Le}\)’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E \(\text{L7F4E}\) <certificate body>
     5F 37 <L5F37> <certificate signature>
   - The key length of this certificate is different to the CVCA public key.

3. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 \(\text{Lc}\) 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference given in the previous DVCA-Certificate sent.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set
14” chapter as IS_CERT_14a.
‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>’
• <Cryptogram> contains the following encrypted data objects
  7F 4E <L7F4E> <certificate body>
  5F 37 <L5F37> <certificate signature>

Expected
results

1. ‘90 00’ in a valid SM response
2. ISO checking error or ‘63 00’ in a valid SM response.
3. ‘90 00’ or ISO checking error in a valid SM response. Note that some
   chip OS accept the selection of an unavailable public key and return an
   error only when the public key is used for the selected purpose.
4. ISO checking error or ‘63 00’ in a valid SM response. Since the DV
   certificate was not verified successfully, it MUST NOT be possible to
   use it as the trust point for the IS-Certificate verification.

3.5.56 Test case ISO7816_J_56

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_J_56</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test a IS certificate with a wrong Public Key (shorter key length).</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

Preconditions

1. The "Open ePassport Application" procedure MUST have been
   performed.
2. The Chip Authentication mechanism must have been performed as
   well.
3. The Certification Authority Reference must have been read from the
   EF.CVCA file (Primary trust point).

Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference must be used as read from
     the EF.CVCA file.

2. Send the appropriate CA-Certificate as specified in the “Certificate Set
   14” chapter as DV_CERT_14a.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference given in the previous DVCA-
     Certificate sent.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 14” chapter as IS\_CERT\_14b. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>
   • The key length of this certificate is different to the CVCA and DV certificates public keys.

Expected results
1. ’90 00’ in a valid SM response
2. ’90 00’ in a valid SM response
3. ’90 00’ in a valid SM response
4. ISO checking error or ’63 00’ in a valid SM response

3.7 Unit ISO7816\_K – Terminal Authentication\(^1\)

This unit tests the second part of the terminal authentication process. In this step, the terminal proves the possession of the private key which belongs to the IS certificate.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.7.1 Test case ISO7816\_K\_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_1_template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Positive test with a valid terminal authentication process</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>see Table 1</td>
</tr>
</tbody>
</table>

Preconditions
1. The “Open ePassport Application" procedure MUST have been performed. Use the protocol specified in Table 1.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.  
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV\_CERT\_1.

\(^1\) Note that some States have issued MRTDs using a static binding for the combination of PACE and Terminal Authentication. For these MRTDs some test cases of this unit will be replaced by alternative and additional test cases in [R9].
Test plan for eMRTDs with EACv1

3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 2A 00 BE <Lc> 87 <Lb> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <Lb> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

5. Send the given MSE: Set AT APDU to the eMRTD.
   ‘0C 2A 00 BE <Lc> 87 <Lb> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

6. Send the given Get Challenge APDU to the eMRTD.
   ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD as specified in Table 1.

Expected results
1. ’90 00’ in a valid SM response
2. ’90 00’ in a valid SM response
3. ’90 00’ in a valid SM response
4. ’90 00’ in a valid SM response
5. ’90 00’ in a valid SM response
6. ‘Eight bytes of random data’ 90 00’ in an SM response
7. ’90 00’ in a valid SM response

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>Profile</th>
<th>Precondition</th>
<th>Test scenario</th>
</tr>
</thead>
</table>
| ISO7816_K_1a | TA, BAC | Perform BAC with MRZ | 7. Send the given external authenticate command to the eMRTD. ‘0C 82 00 00 <Lc> 87 <Lb> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • The MRTD chip’s Document number as contain in the MRZ including the check digit MUST be used to build the encrypted terminal signature (S\textsubscript{PCD}) for |
the External Authenticate command. 
<Cryptogram> contains the encrypted 
terminal generated signature created with 
the private key of IS_KEY_01.

| ISO7816_K_1b | TA, PACE | Perform PACE with MRZ or CAN | 7. Send the given external authenticate command to the eMRTD. 
'0C 82 00 00 <Lc> 87 <L87> 01 
<Cryptogram> 8E 08 <Checksum> <Le>' |
|-------------|----------|-------------------------------|---------------------------------------------------------------|
|             |          |                               | • The MRTD chip’s ephemeral PACE public key MUST be used to build the encrypted terminal signature (SPCD) for the External Authenticate command. 
ID_PICC = Comp(ehpPK_PICC) 
<Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. |

Table 1: Test case ISO7816_K_1

3.7.2 Test case ISO7816_K_2

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with an invalid certificate reference for the MSE:Set AT command</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed. 
2. The Chip Authentication mechanism MUST have been performed as well. 
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD. 
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' 
• <Cryptogram> contains the following encrypted data objects 
83 <L83> <Certification Authority Reference> 
• The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. 
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' 
• <Cryptogram> contains the following encrypted data objects 
7F 4E <L7F4E> <certificate body> 
5F 37 <L5F37> <certificate signature>
3. Send the given MSE: Set DST APDU to the eMRTD. 
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
• <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certification Authority Reference>
  The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’

• <Cryptogram> contains the following encrypted data objects
  7F 4E <L7F4E> <certificate body>
  5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’

• <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certification Holder Reference>

To generate an invalid certification holder reference, the last character of the holder reference stored inside the IS-Certificate sent in step 4 is changed.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’

• <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.

### Expected results

1. ’90 00’ in a valid SM response
2. ’90 00’ in a valid SM response
3. ’90 00’ in a valid SM response
4. ’90 00’ in a valid SM response
5. ’90 00’ or ISO checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.
6. ‘<Eight bytes of random data> 90 00’ or ISO checking error in an SM response
7. ISO checking error or ‘6300’ in an SM response

### Test case ISO7816_K_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8 (Identical with ISO7816_L_11)</td>
</tr>
</tbody>
</table>

### Test case ISO7816_K_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with a terminal authentication process without secure messaging</td>
</tr>
</tbody>
</table>
## Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Version</th>
<th>1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   \`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   \`0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   \`0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   \`0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   \`0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   \`00 82 00 00 <Lc> <Terminal generated signature>’
   - The APDU is sent in plain without SM encoding
   - The signature is created with the private key of IS_KEY_01.
Expected results
1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' in an SM response
4. '90 00' in an SM response
5. '90 00' in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ISO checking error as a plain response (without Secure Messaging)

3.7.5 Test case ISO7816_K_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that the effective access rights in a DV-Certificate are ignored</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions   | 1. The "Open ePassport Application" procedure MUST have been performed.  
                    2. The Chip Authentication mechanism MUST have been performed as well.  
                    3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario   | 1. Send the given MSE: Set DST APDU to the eMRTD.  
                    '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
                    • <Cryptogram> contains the following encrypted data objects  
                      83 <L83> <Certification Authority Reference>  
                      • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
                    2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
                    '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
                    • <Cryptogram> contains the following encrypted data objects  
                      7F 4E <L7F4E> <certificate body>  
                      5F 37 <L5F37> <certificate signature>  
                    3. Send the given MSE: Set AT APDU to the eMRTD.  
                    '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
                    • <Cryptogram> contains the following encrypted data objects  
                      83 <L83> <Certification Holder Reference>  
                      • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
                    4. Send the given Get Challenge APDU to the eMRTD.  
                    '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'  
                    5. Send the given external authenticate command to the eMRTD.  
                    '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
                    • <Cryptogram> contains the encrypted terminal generated signature
### Expected results

1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' or ISO checking error in an SM response
4. '<Eight bytes of random data> 90 00' or ISO checking error in an SM response
5. ISO checking error or '6300' in an SM response

#### 3.7.6 Test case ISO7816_K_6

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that the effective access rights in a CVCA-Certificate are ignored</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the</td>
</tr>
<tr>
<td></td>
<td>EF.CVCA file (Primary trust point).</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Send the given MSE: Set AT APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 22 81 A4 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Holder Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Authority Reference as read from the EF.CVCA file</td>
</tr>
<tr>
<td></td>
<td>has to be used.</td>
</tr>
<tr>
<td></td>
<td>2. Send the given Get Challenge APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 84 00 00 0D 97 01 08 8E 08 &lt;Checksum&gt; 00’</td>
</tr>
<tr>
<td></td>
<td>3. Send the given external authenticate command to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 82 00 00 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the encrypted terminal generated signature</td>
</tr>
<tr>
<td></td>
<td>created with the private key of CVCA_KEY_00.</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. '90 00' or ISO checking error in an SM response</td>
</tr>
<tr>
<td></td>
<td>2. '&lt;Eight bytes of random data&gt; 90 00' or ISO checking error in an SM</td>
</tr>
<tr>
<td></td>
<td>response</td>
</tr>
<tr>
<td></td>
<td>3. ISO checking error or '6300' in an SM response</td>
</tr>
</tbody>
</table>

#### 3.7.7 Test case ISO7816_K_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the external authenticate command with an invalid class byte</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
</tbody>
</table>
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

<table>
<thead>
<tr>
<th>Test scenario</th>
</tr>
</thead>
</table>
| 1. Send the given MSE: Set DST APDU to the eMRTD.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> 00'  
   - <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> <Le>'  
   - <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature> |
| 3. Send the given MSE: Set DST APDU to the eMRTD.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> 00'  
   - <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. |
| 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> <Le>'  
   - <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature> |
| 5. Send the given MSE: Set AT APDU to the eMRTD.  
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> 00'  
   - <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Holder Reference>  
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. |
| 6. Send the given Get Challenge APDU to the eMRTD.  
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' |
| 7. Send the given external authenticate command to the eMRTD.  
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08  
   <Checksum> <Le>'  
   - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.  
   - The class byte is set to an invalid value (‘8C’) |
| 8. If the error code in step 7 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. |
The Command APDU as defined in the ICS (Annex A Table 2) must be send as SM-protected APDU using the session keys derived in step 2 of the preconditions.

| Expected results | 1. '90 00' in an SM response |
|                 | 2. '90 00' in an SM response |
|                 | 3. '90 00' in an SM response |
|                 | 4. '90 00' in an SM response |
|                 | 5. '90 00' in an SM response |
|                 | 6. ‘<Eight bytes of random data> 90 00’ in an SM response |
|                 | 7. ISO checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. |
|                 | 8. Skipped or '90 00' in an SM response |

### 3.7.8 Test case ISO7816_K_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 1.1</td>
</tr>
</tbody>
</table>

### 3.7.9 Test case ISO7816_K_9

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8</td>
</tr>
</tbody>
</table>

### 3.7.10 Test case ISO7816_K_10

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Terminal authentication process with two Get Challenge commands (Using the first challenge)</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects 83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td></td>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. '0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;’</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

- <Cryptogram> contains the following encrypted data objects
  7F 4E <L7F4E> <certificate body>
  5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L5F37> 01 <Cryptogram> 8E 08
   <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate
     sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1”
   chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L83> 01 <Cryptogram> 8E 08
   <Checksum> <Le>'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L83> 01 <Cryptogram> 8E 08
   <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   - The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'

7. Send the given a second Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'
   - If the chip returns an ISO checking error for this second Get
     Challenge, the remaining steps of this case MUST be skipped.

8. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>'
   - <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_01.
   - The signature is based on the first challenge received in step 6

| Expected results | 1. '90 00' in an SM response |
|                 | 2. '90 00' in an SM response |
|                 | 3. '90 00' in an SM response |
|                 | 4. '90 00' in an SM response |
|                 | 5. '90 00' in an SM response |
|                 | 6. '<Eight bytes of random data> 90 00' in an SM response |
|                 | 7. '<Eight bytes of random data> 90 00' or ISO checking error in an SM response |
|                 | 8. Skipped or ISO checking error or '63 00' in an SM response |
### 3.7.11 Test case ISO7816_K_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8 (Superseded by ISO7816_K_14)</td>
</tr>
</tbody>
</table>

### 3.7.12 Test case ISO7816_K_12

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Terminal authentication process with short challenge</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`
   
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`
   
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`

5. Send the given MSE: Set AT APDU to the eMRTD.
   
   `0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   
   - `<Cryptogram>` contains the following encrypted data objects
• The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.  
   `0C 84 00 00 0D 97 01 07 8E 08 <Checksum> 00`

7. If the chip returns a short challenge (only 7 bytes) then send the given external authenticate command to the eMRTD, otherwise skip this step.  
   `0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>`  
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.  
   • The signature is based on the short challenge received in step 6

<table>
<thead>
<tr>
<th>Expected results</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. '90 00' in an SM response</td>
<td></td>
</tr>
<tr>
<td>2. '90 00' in an SM response</td>
<td></td>
</tr>
<tr>
<td>3. '90 00' in an SM response</td>
<td></td>
</tr>
<tr>
<td>4. '90 00' in an SM response</td>
<td></td>
</tr>
<tr>
<td>5. '90 00' in an SM response</td>
<td></td>
</tr>
<tr>
<td>6. '&lt;Seven bytes of random data&gt; 90 00' or ISO checking error in an SM response</td>
<td></td>
</tr>
<tr>
<td>7. Skipped, ISO checking error or warning processing '63 00' in an SM response</td>
<td></td>
</tr>
</tbody>
</table>

### 3.7.13 Test case ISO7816_K_13

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8 (Identical with ISO7816_L_11)</td>
</tr>
</tbody>
</table>

### 3.7.14 Test case ISO7816_K_14

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Check the Terminal authentication – No Get Challenge Performed</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
<td></td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
<td></td>
</tr>
<tr>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test scenario</th>
<th></th>
</tr>
</thead>
</table>
| 1. Send the given MSE: Set DST APDU to the eMRTD.  
  `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
  • <Cryptogram> contains the following encrypted data objects  
    83 <L83> <Certification Authority Reference>  
  • The Certification Authority Reference MUST be used as read from the EF.CVCA file. |   |
| 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
  `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>` |   |
Test plan for eMRTDs with EACv1

3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>
   <Lc>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   ‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>
   <Lc>’
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.
   • The wrong signature is calculated without any challenge.

7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted.
   ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

<table>
<thead>
<tr>
<th>Expected results</th>
<th>1. '90 00' in an SM response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. '90 00' in an SM response</td>
</tr>
<tr>
<td></td>
<td>3. '90 00' in an SM response</td>
</tr>
<tr>
<td></td>
<td>4. '90 00' in an SM response</td>
</tr>
<tr>
<td></td>
<td>5. '90 00' in an SM response</td>
</tr>
<tr>
<td></td>
<td>6. ISO checking error or warning processing ’63 00’ in an SM response.</td>
</tr>
<tr>
<td></td>
<td>7. ISO checking error in an SM response</td>
</tr>
</tbody>
</table>

3.7.15 Test case ISO7816_K_15

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Check the Terminal authentication – No authentication key selection performed</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>
### Preconditions

1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   •  <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   •  The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   •  <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <Certificate body>  
     5F 37 <LSF7> <Certificate signature>  
3. Send the given MSE: Set DST APDU to the eMRTD.  
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   •  <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   •  The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   •  <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <Certificate body>  
     5F 37 <LSF7> <Certificate signature>  
5. Send the given Get Challenge APDU to the eMRTD.  
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’  
6. Send the given external authenticate command to the eMRTD.  
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   •  If the Get Challenge command in step 5 returns an ISO checking error, the remaining steps of this test case are skipped.  
   •  <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.  
   •  The signature is based on the challenge received in step 5.
7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted.  
   '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
### Expected results

1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' in an SM response
4. '90 00' in an SM response
5. '<Eight bytes of random data> 90 00' or ISO checking error in an SM response
6. Skipped, or ISO checking error or warning processing '63 00' in an SM response
7. Skipped, or ISO checking error in an SM response

### 3.7.16 Test case ISO7816_K_16

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 0.8 (Identical with ISO7816_K_2)</td>
</tr>
</tbody>
</table>

### 3.7.17 Test case ISO7816_K_17

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Check the Terminal authentication – Wrong structure in the MSE Set AT command</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>
1. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the
     EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”
   chapter as DV_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>
     <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate
     sent in step 2 has to be used.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1”
   chapter as IS_CERT_1.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>
     <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
5. Send the given MSE: Set AT APDU to the eMRTD.
   ‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     84 <L84> <Certification Holder Reference> instead of tag 83
   • The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.
6. Send the given Get Challenge APDU to the eMRTD.
   ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’
7. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum>
     <Le>’
   • If the Get Challenge command in step 6 returns an ISO checking error,
     the remaining step of this test case are skipped.
   • <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_01.
   • The signature is based on the challenge received in step 6.
8. Send the given READ BINARY (with SFI) command to the eMRTD, to
   verify the access to the Data Group 3 has NOT been granted.
   ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results
1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' in an SM response
4. '90 00' in an SM response
5. ISO checking error in an SM response
6. '<Eight bytes of random data> 90 00' or ISO checking error in an SM response
7. Skipped or ISO checking error or warning processing '63 00' in an SM response
8. Skipped or ISO checking error in an SM response

3.7.18 Test case ISO7816_K_18

<table>
<thead>
<tr>
<th>Test-ID</th>
<th>ISO7816_K_18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Check the Terminal authentication – Reset of the access rights in case of Application reset</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
<tr>
<td>Test scenario</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td></td>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. '0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td></td>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td></td>
<td>3. Send the given MSE: Set DST APDU to the eMRTD. '0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.</td>
</tr>
<tr>
<td></td>
<td>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. '0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
</tbody>
</table>
5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
   83<L83> <Certification Holder Reference >
   • The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <L87>’
   • <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_01.
   • The signature is based on the challenge received in step 6.

8. Reset the chip by switching off the field and switching in on again
   • Perform the “Open ePassport Application”.
   • Do NOT perform Chip Authentication
   • Send the given READ BINARY (with SFI) command to the eMRTD,
     to verify the access to the Data Group 3 has NOT been granted.
     ‘0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

| Expected results | 1. '90 00’ in an SM response |
|                 | 2. '90 00’ in an SM response |
|                 | 3. '90 00’ in an SM response |
|                 | 4. '90 00’ in an SM response |
|                 | 5. '90 00’ in an SM response |
|                 | 6. ‘<Eight bytes of random data> 90 00’ in an SM response |
|                 | 7. '90 00’ in an SM response |
|                 | 8. ISO checking error in an SM response |

### 3.7.19 Test case ISO7816_K_19

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Check the Terminal Authentication – Passive [R4] and optionally Active Authentication between Chip Authentication and Terminal authentication</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Passive Authentication [R4] MUST have been performed after CA.</td>
</tr>
<tr>
<td></td>
<td>4. If available, DG15 MAY have been read and verified and Active Authentication have been performed after PA.</td>
</tr>
<tr>
<td></td>
<td>5. The Certification Authority Reference MUST has been read from the</td>
</tr>
</tbody>
</table>
**Test plan for eMRTDs with EACv1**

<table>
<thead>
<tr>
<th>Test scenario</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. | Send the given MSE: Set DST APDU to the eMRTD.  

`'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`  

- `<Cryptogram>` contains the following encrypted data objects  
  83 `<L83>` `<Certification Authority Reference>`  
- The Certification Authority Reference MUST be used as read from the EF.CVCA file. |
| 2. | Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  

`'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'`  

- `<Cryptogram>` contains the following encrypted data objects  
  7F 4E `<L7F4E>` `<certificate body>`  
  5F 37 `<L5F37>` `<certificate signature>` |
| 3. | Send the given MSE: Set DST APDU to the eMRTD.  

`'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`  

- `<Cryptogram>` contains the following encrypted data objects  
  83 `<L83>` `<Certification Authority Reference>`  
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. |
| 4. | Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  

`'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'`  

- `<Cryptogram>` contains the following encrypted data objects  
  7F 4E `<L7F4E>` `<certificate body>`  
  5F 37 `<L5F37>` `<certificate signature>` |
| 5. | Send the given MSE: Set AT APDU to the eMRTD.  

`'0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'`  

- `<Cryptogram>` contains the following encrypted data objects  
  83 `<L83>` `<Certification Holder Reference>`  
- The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. |
| 6. | Send the given Get Challenge APDU to the eMRTD.  

`'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'` |
| 7. | Send the given external authenticate command to the eMRTD.  

`'0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'`  

- `<Cryptogram>` contains the encrypted terminal generated signature created with the private key of IS_KEY_01.  
- The signature is based on the challenge received in step 6. |

<table>
<thead>
<tr>
<th>Expected results</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. | '90 00’ in an SM response  
| 2. | '90 00’ in an SM response  
| 3. | '90 00’ in an SM response  
| 4. | '90 00’ in an SM response  
| 5. | '90 00’ in an SM response  
| 6. | ‘<Eight bytes of random data> 90 00’ in an SM response  
| 7. | '90 00’ in an SM response |
### 3.7.20 Test case ISO7816_K_20

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_K_20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Perform Terminal Authentication with an invalid PACE binding</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, PACE</td>
</tr>
</tbody>
</table>

**Preconditions**

1. The "Open ePassport Application" procedure MUST have been performed. PACE with MRZ MUST be used.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.
   
   | 0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00 |
   
   • <Cryptogram> contains the following encrypted data objects
   
   83 <L83> <Certification Authority Reference>
   
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   
   | 0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le> |
   
   • <Cryptogram> contains the following encrypted data objects

   7F 4E <L7F4E> <certificate body>
   
   5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   | 0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00 |
   
   • <Cryptogram> contains the following encrypted data objects

   83 <L83> <Certification Authority Reference>
   
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   
   | 0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le> |
   
   • <Cryptogram> contains the following encrypted data objects

   7F 4E <L7F4E> <certificate body>
   
   5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   
   | 0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00 |
   
   • <Cryptogram> contains the following encrypted data objects

   83 <L83> <Certification Holder Reference>
   
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   
   | 0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00 |
7. Send the given external authenticate command to the eMRTD. ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • Generate a invalid signature, e.g. modify last byte of the signature by adding 0x01.
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.

Expected results
1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. '<Eight bytes of random data> 90 00’ in an SM response
7. ISO checking error or SW '63 00’ in an SM response

3.8 Unit ISO7816_L – Effective Access Conditions

This unit tests the evaluation of effective access conditions by the chip. The chip has to grant access to sensitive data only if the complete terminal authentication mechanism has been performed. Furthermore the access to the specific Data Groups depends on the access condition flags encoded in the DV and IS certificate.

All test cases of this test unit which require the “Open ePassport Application” procedure MUST be performed twice (one test run with BAC and one with PACE) if the chip supports both protocols. If the chip only supports one of these protocols (BAC or PACE), only one test run has to be performed with the supported protocol used in the “Open ePassport Application” procedure.

3.8.1 Test case ISO7816_L_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Positive test with a valid terminal authentication process with access permission for DG 3 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD. ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the
EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3.
   '0C 2A 00 BE <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This DV-Certificate grants access to Data Group 3 and Data Group 4.

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3a.
   '0C 2A 00 BE <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This IS-Certificate grants only access to Data Group 3.

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has been granted.
   '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. ’90 00’ in an SM response
2. ’90 00’ in an SM response
3. ’90 00’ in an SM response
4. ’90 00’ in an SM response
5. ’90 00’ in an SM response
6. ’<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ‘<Data Group 3 content data> 90 00’ in an SM response

### 3.8.2 Test case ISO7816_L_2

#### Test - ID
ISO7816_L_2

#### Purpose
Test that Data Group 4 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.

#### Version
1.2

#### Profile
TA, DG4

#### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

#### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - This DV-Certificate grants access to Data Group 3 and Data Group 4.

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3a.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   - This IS-Certificate grants only access to Data Group 3.

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
• <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certification Holder Reference>
• The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 4 has NOT been granted.
   ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. '<Eight bytes of random data> 90 00’ in an SM response
7. '90 00’ in an SM response
8. ISO checking error in an SM response

3.8.3 Test case ISO7816_L.3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Positive test with a valid terminal authentication process with access permission for DG 4 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG4</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
Test plan for eMRTDs with EACv1

1. <Checksum> <Le>’

2. <Cryptogram> contains the following encrypted data objects
   7F 4E <L7F4E> <certificate body>
   5F 37 <L5F37> <certificate signature>

3. This DV-Certificate grants access to Data Group 3 and Data Group 4.

3. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’

   a. <Cryptogram> contains the following encrypted data objects
      83 <L83> <Certification Authority Reference>
      The Certification Holder Reference stored inside the DV-Certificate
      sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3”
   chapter as IS_CERT _3b.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’

   b. <Cryptogram> contains the following encrypted data objects
      7F 4E <L7F4E> <certificate body>
      5F 37 <L5F37> <certificate signature>
      This IS-Certificate grants only access to Data Group 4.

5. Send the given MSE: Set AT APDU to the eMRTD.
   ‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’

   c. <Cryptogram> contains the following encrypted data objects
      83 <L83> <Certification Holder Reference>
      The Certification Holder Reference stored inside the IS-Certificate
      sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   ‘0C 84 00 0D 97 01 01 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’

   d. <Cryptogram> contains the encrypted terminal generated signature
      created with the private key of IS_KEY_03.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to
   verify the access to the Data Group 4 has been granted.
   ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results

1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ‘<Data Group 4 content data> 90 00’ in an SM response
### 3.8.4 Test case ISO7816_L_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that Data Group 3 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>

| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |

| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
\[0C 22 81 B6 \text{<Le> } 87 \text{<L87> } 01 \text{<Cryptogram> } 8E 08 \text{<Checksum> } 00\]  
• <Cryptogram> contains the following encrypted data objects  
\[83 \text{<L83> <Certification Authority Reference>}\]  
• The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3  
\[0C 2A 00 BE \text{<Le> } 87 \text{<L87> } 01 \text{<Cryptogram> } 8E 08 \text{<Checksum> } \text{<Le>’}\]  
• <Cryptogram> contains the following encrypted data objects  
\[7F 4E \text{<L7F4E> <certificate body>}\]  
\[5F 37 \text{<L5F37> <certificate signature}>\]  
• This DV-Certificate grants access to Data Group 3 and Data Group 4.  
3. Send the given MSE: Set DST APDU to the eMRTD.  
\[0C 22 81 B6 \text{<Le> } 87 \text{<L87> } 01 \text{<Cryptogram> } 8E 08 \text{<Checksum> } 00\]  
• <Cryptogram> contains the following encrypted data objects  
\[83 \text{<L83> <Certification Authority Reference>}\]  
• The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3b.  
\[0C 2A 00 BE \text{<Le> } 87 \text{<L87> } 01 \text{<Cryptogram> } 8E 08 \text{<Checksum> } \text{<Le>’}\]  
• <Cryptogram> contains the following encrypted data objects  
\[7F 4E \text{<L7F4E> <certificate body>}\]  
\[5F 37 \text{<L5F37> <certificate signature}>\]  
• This IS-Certificate grants only access to Data Group 4.  
5. Send the given MSE: Set AT APDU to the eMRTD.  
\[0C 22 81 A4 \text{<Le> } 87 \text{<L87> } 01 \text{<Cryptogram> } 8E 08 \text{<Checksum> } 00\]  
• <Cryptogram> contains the following encrypted data objects  
\[83 \text{<L83> <Certification Holder Reference>}\]  
• The Certification Holder Reference stored inside the IS-Certificate
Test plan for eMRTDs with EACv1

6. Send the given Get Challenge APDU to the eMRTD. 'OC 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD. 'OC 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted. 'OC B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. '<Eight bytes of random data> 90 00’ in an SM response
7. '90 00’ in an SM response
8. ISO checking error in an SM response

3.8.5 Test case ISO7816_L_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Positive test with a valid terminal authentication process for DG 3 if the DV certificate grant access to Data Group 3 only and the IS certificate enable access to both data 3 and 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
</tbody>
</table>
| Preconditions  | 1. The "Open ePassport Application" procedure MUST have been performed.  
   2. The Chip Authentication mechanism MUST have been performed as well.  
   3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario  | 1. Send the given MSE: Set DST APDU to the eMRTD. 'OC 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
   2. Send the appropriate DV-Certificate as specified in the “Certificate Set 4” chapter as DV_CERT_4 'OC 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects 7F 4E <LF4E> <certificate body> |
• This DV-Certificate grants access to Data Group 3 only.

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate
     sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 4”
   chapter as IS_CERT_4.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This IS-Certificate grants access to Data Group 3 and Data Group 4.

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate
     sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 01 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_04.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to
   verify the access to the Data Group 3 has been granted.
   '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results

1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ‘<Data Group 3 content data> 90 00’ in an SM response

3.8.6 Test case ISO7816_L_6

| Test - ID | ISO7816_L_6 |
## Purpose
Test that Data Group 4 cannot be accessed if the DV certificate grant access to Data Group 3 only and the IS certificate enable access to both data 3 and 4.

## Version
1.2

## Profile
TA, DG4

### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 4” chapter as DV_CERT_4
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`
   - This DV-Certificate grants access to Data Group 3 only.
3. Send the given MSE: Set DST APDU to the eMRTD.
   `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Authority Reference>`
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 4” chapter as IS_CERT_4.
   `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - `<Cryptogram>` contains the following encrypted data objects
     7F 4E `<L7F4E>` `<certificate body>`
     5F 37 `<L5F37>` `<certificate signature>`
   - This IS-Certificate grants access to Data Group 3 and Data Group 4.
5. Send the given MSE: Set AT APDU to the eMRTD.
   `0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`
   - `<Cryptogram>` contains the following encrypted data objects
     83 `<L83>` `<Certification Holder Reference>`
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.
6. Send the given Get Challenge APDU to the eMRTD.
   `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'
7. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_04.
8. Send the given READ BINARY (with SFI) command to the eMRTD, to
verify the access to the Data Group 4 has NOT been granted.
   ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ISO checking error in an SM response

3.8.7 Test case ISO7816_L_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Positive test with a valid terminal authentication process for DG 4 if the DV certificate grant access to Data Group 4 only and the IS certificate enables access to both data 3 and 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG4</td>
</tr>
</tbody>
</table>

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 5” chapter as DV_CERT_5
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This DV-Certificate grants access to Data Group 4 only.
3. Send the given MSE: Set DST APDU to the eMRTD.
Test plan for eMRTDs with EACv1

1. Send the appropriate IS-Certificate as specified in the “Certificate Set 5” chapter as IS_CERT_5.
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
   • This IS-Certificate grants access to Data Group 3 and Data Group 4.

5. Send the given MSE: Set AT APDU to the eMRTD.
   ‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   ‘0C 84 00 00 0D 97 01 01 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 4 has been granted.
   ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results

1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ‘<Data Group 4 content data> 90 00’ in an SM response

3.8.8 Test case ISO7816_L_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that Data Group 3 cannot be accessed if the DV certificate grants access to Data Group 4 only and the IS certificate enables access to both Data Group 3 and Data Group 4.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
</tbody>
</table>
### Test Plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Profile</th>
<th>TA, DG3</th>
</tr>
</thead>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| **Test scenario** | 1. Send the given MSE: Set DST APDU to the eMRTD.  
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 5” chapter as DV_CERT_5  
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • This DV-Certificate grants access to Data Group 4 only.  
3. Send the given MSE: Set DST APDU to the eMRTD.  
   ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 5” chapter as IS_CERT_5.  
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • This IS-Certificate grants access to Data Group 3 and Data Group 4.  
5. Send the given MSE: Set AT APDU to the eMRTD.  
   ‘0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Holder Reference>  
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.  
6. Send the given Get Challenge APDU to the eMRTD.  
   ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’  
7. Send the given external authenticate command to the eMRTD.  
   ‘0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ |
Test plan for eMRTDs with EACv1

- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05.

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted.
   `'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'`

| Expected results | 1. '90 00' in an SM response | 2. '90 00' in an SM response |
|                 | 3. '90 00' in an SM response | 4. '90 00' in an SM response |
|                 | 5. '90 00' in an SM response | 6. 'Eight bytes of random data> 90 00' in an SM response |
|                 | 7. '90 00' in an SM response | 8. ISO checking error in an SM response |

3.8.9 Test case ISO7816_L_9

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in Data Group 3.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td><code>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</code></td>
</tr>
<tr>
<td></td>
<td>- &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>- The Certification Authority Reference MUST be used as read from the EF.CVCA file.</td>
</tr>
<tr>
<td></td>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1</td>
</tr>
<tr>
<td></td>
<td><code>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; &lt;Le&gt;'</code></td>
</tr>
<tr>
<td></td>
<td>- &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>7F 4E &lt;L7F4E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td></td>
<td>5F 37 &lt;L5F37&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td></td>
<td>3. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td><code>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08 &lt;Checksum&gt; 00'</code></td>
</tr>
<tr>
<td></td>
<td>- &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
</tbody>
</table>
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted.
   '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. '<Eight bytes of random data> 90 00’ in an SM response
7. ISO checking error in an SM response

3.8.10 Test case ISO7816_L_10

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in Data Group 4</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, DG4</td>
</tr>
<tr>
<td>Preconditions</td>
<td></td>
</tr>
<tr>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
<td></td>
</tr>
<tr>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
<td></td>
</tr>
<tr>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
<td></td>
</tr>
<tr>
<td>Test scenario</td>
<td></td>
</tr>
</tbody>
</table>
| 1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Le> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ |
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference> |
• The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 01 8E 08 <Checksum> 00’

7. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 4 has NOT been granted.
   '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results
1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ISO checking error in an SM response.

3.8.11 Test case ISO7816_L_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test with a failed external authenticate command does not enable the access to the</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the</td>
</tr>
<tr>
<td></td>
<td>EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test scenario</th>
<th>1. Send the given MSE: Set DST APDU to the eMRTD.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Authority Reference MUST be used as read from the</td>
</tr>
<tr>
<td></td>
<td>EF.CVCA file.</td>
</tr>
<tr>
<td></td>
<td>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1”</td>
</tr>
<tr>
<td></td>
<td>chapter as DV CERT 1.</td>
</tr>
<tr>
<td></td>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; &lt;Le&gt;'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>7F 4E &lt;L74E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td></td>
<td>5F 37 &lt;L537&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td></td>
<td>3. Send the given MSE: Set DST APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 22 81 B6 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Authority Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Holder Reference stored inside the DV-Certificate</td>
</tr>
<tr>
<td></td>
<td>sent in step 2 has to be used.</td>
</tr>
<tr>
<td></td>
<td>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1”</td>
</tr>
<tr>
<td></td>
<td>chapter as IS CERT 1.</td>
</tr>
<tr>
<td></td>
<td>'0C 2A 00 BE &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; &lt;Le&gt;'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>7F 4E &lt;L74E&gt; &lt;certificate body&gt;</td>
</tr>
<tr>
<td></td>
<td>5F 37 &lt;L537&gt; &lt;certificate signature&gt;</td>
</tr>
<tr>
<td></td>
<td>5. Send the given MSE: Set AT APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 22 81 A4 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the following encrypted data objects</td>
</tr>
<tr>
<td></td>
<td>83 &lt;L83&gt; &lt;Certification Holder Reference&gt;</td>
</tr>
<tr>
<td></td>
<td>• The Certification Holder Reference stored inside the IS-Certificate</td>
</tr>
<tr>
<td></td>
<td>sent in step 4 has to be used.</td>
</tr>
<tr>
<td></td>
<td>6. Send the given Get Challenge APDU to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 84 00 00 0D 97 01 08 8E 08 &lt;Checksum&gt; 00'</td>
</tr>
<tr>
<td></td>
<td>7. Send the given external authenticate command to the eMRTD.</td>
</tr>
<tr>
<td></td>
<td>'0C 82 00 00 &lt;Lc&gt; 87 &lt;L87&gt; 01 &lt;Cryptogram&gt; 8E 08</td>
</tr>
<tr>
<td></td>
<td>&lt;Checksum&gt; &lt;Le&gt;'</td>
</tr>
<tr>
<td></td>
<td>• &lt;Cryptogram&gt; contains the encrypted terminal generated signature</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

- The last byte of the signature is changed to make it invalid
- Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 3 has NOT been granted.

```
'OC B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'
```

### Expected results

1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' in an SM response
4. '90 00' in an SM response
5. '90 00' in an SM response
6. '<Eight bytes of random data> 90 00' in an SM response
7. ISO checking error or warning processing '63 00' in an SM response
8. ISO checking error in an SM response

### 3.8.12 Test case ISO7816_L_12

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Test that a failed external authenticate command does not enable the access to the sensitive data in Data Group 4.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>TA, DG4</td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| **Test scenario** | 1. Send the given MSE: Set DST APDU to the eMRTD.  
```
'OC 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
```
   - <Cryptogram> contains the following encrypted data objects  
   - 83 <L83> <Certification Authority Reference>  
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
```
'OC 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
```
   - <Cryptogram> contains the following encrypted data objects  
   - 7F 4E <L7F4E> <certificate body>  
   - 5F 37 <LS37> <certificate signature>  
3. Send the given MSE: Set DST APDU to the eMRTD.  
```
'OC 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
```
   - <Cryptogram> contains the following encrypted data objects  
   - 83 <L83> <Certification Authority Reference>  
   - The Certification Holder Reference stored inside the DV-Certificate
sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <Certificate body>
     5F 37 <L5F37> <Certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   • The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the encrypted terminal generated signature
     created with the private key of IS_KEY_01.
   • The last byte of the signature is changed to make it invalid

8. Send the given READ BINARY (with SFI) command to the eMRTD, to verify the access to the Data Group 4 has NOT been granted.
   '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’

Expected results

1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ISO checking error or warning processing ’63 00’ in an SM response
8. ISO checking error in an SM response

3.8.13 Test case ISO7816_L_13

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that the chip rejects to fall back to BAC secure messaging after the terminal has been authenticated as extended inspection system</td>
</tr>
<tr>
<td>Version</td>
<td>1.4</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, BAC, MF</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The LDS application MUST have been selected.  
2. The BAC mechanism MUST have been performed.  
3. The Chip Authentication mechanism MUST have been performed as well.  
4. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
### Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.
   
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
   
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'

7. Send the given external authenticate command to the eMRTD.
   
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>
   - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.

8. Select the MF by sending the given Select APDU to the eMRTD:
   
   '0C A4 00 0C 0A 8E 08 <Checksum> 00'

9. Under SM, Perform an additional run of the “Open ePassport Application” procedure with BAC.

10. Use new SM keys from BAC run. Send the READ BINARY (with SFI) command to the eMRTD to verify the access to Data Group 3 has NOT been granted.
    
    '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'

### Expected results

1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘<Eight bytes of random data> 90 00’ in an SM response
7. ‘90 00’ in an SM response
8. ‘90 00’ in an SM response, or ISO checking error, or ISO checking error in an SM response. If this step returns an ISO checking error the next test steps SHALL be skipped.
9. Successful run of “Open ePassport Application” procedure or ISO checking error. If “Open ePassport Application” procedure fails, the next steps SHALL be skipped.
10. ISO checking error in an SM response (chip MUST reject access to Data Group 3 since access condition from previous Terminal Authentication MUST be reset).

3.8.14 Test case ISO7816_L_14

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that the chip rejects a second PACE run or reset extended access rights after the terminal has been authenticated as extended inspection system with a first PACE run.</td>
</tr>
<tr>
<td>Version</td>
<td>1.4</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, PACE</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed. PACE MUST be used.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.
‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file.
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_Cert_1.
‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
3. Send the given MSE: Set DST APDU to the eMRTD.
‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.
‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
Test plan for eMRTDs with EACv1

| Expected results | 1. '90 00' in an SM response | 2. '90 00' in an SM response | 3. '90 00' in an SM response | 4. '90 00' in an SM response | 5. '90 00' in an SM response | 6. '<Eight bytes of random data> 90 00' in an SM response | 7. '90 00' in an SM response | 8. '90 00' in an SM response, or ISO checking error, or ISO checking error in an SM response. If this step returns an ISO checking error the next test steps SHALL be skipped. | 9. Successful run of “Open ePassport Application” procedure or ISO checking error. If “Open ePassport Application” procedure fails, the next steps SHALL be skipped. | 10. ISO checking error in an SM response (chip MUST reject access to Data Group 3 since access condition from previous Terminal Authentication MUST be reset) |

3.8.15 Test case ISO7816_L_15

<p>| Test - ID | ISO7816_L_15 |
| Purpose | Test that the chip rejects an additional BAC run or resets extended access rights after the terminal has been authenticated as extended inspection system with a first PACE run |
| Version | 1.5 |</p>
<table>
<thead>
<tr>
<th>Test Plan for eMRTDs with EACv1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
</tr>
</tbody>
</table>
| **Preconditions** | 1. The "Open ePassport Application" procedure MUST have been performed. PACE MUST be used.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| **Test scenario** | 1. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
- <Cryptogram> contains the following encrypted data objects  
  83 <L83> <Certification Authority Reference>  
- The Certification Authority Reference MUST be used as read from the EF.CVCA file.  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
- <Cryptogram> contains the following encrypted data objects  
  7F 4E <L7F4E> <certificate body>  
  5F 37 <L5F37> <certificate signature>  
3. Send the given MSE: Set DST APDU to the eMRTD.  
'0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
- <Cryptogram> contains the following encrypted data objects  
  83 <L83> <Certification Authority Reference>  
- The Certification Authority Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1.  
'0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
- <Cryptogram> contains the following encrypted data objects  
  7F 4E <L7F4E> <certificate body>  
  5F 37 <L5F37> <certificate signature>  
5. Send the given MSE: Set AT APDU to the eMRTD.  
'0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
- <Cryptogram> contains the following encrypted data objects  
  83 <L83> <Certification Holder Reference>  
- The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.  
6. Send the given Get Challenge APDU to the eMRTD.  
'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'  
7. Send the given external authenticate command to the eMRTD.  
'0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
- <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01.  
8. Select the MF by sending the given Select APDU to the eMRTD:  
'0C A4 00 0C 0A 8E 08 <Checksum> 00’  
9. Under SM, Perform an additional run of the “Open ePassport Application” procedure with BAC.  
10. Use new SM keys from BAC run. Send the READ BINARY (with SFI)
command to the eMRTD to verify the access to Data Group 3 has NOT been granted.

\[ \text{'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'} \]

### Expected results

| 1. | '90 00' in an SM response |
| 2. | '90 00' in an SM response |
| 3. | '90 00' in an SM response |
| 4. | '90 00' in an SM response |
| 5. | '90 00' in an SM response |
| 6. | <Eight bytes of random data> 90 00’ in an SM response |
| 7. | '90 00' in an SM response |
| 8. | '90 00' in an SM response, or ISO checking error, or ISO checking error in an SM response. If this step returns an ISO checking error the next test steps SHALL be skipped. |
| 9. | Successful run of “Open ePassport Application” procedure or ISO checking error. If “Open ePassport Application” procedure fails, the next steps SHALL be skipped. |
| 10. | ISO checking error in an SM response (chip MUST reject access to Data Group 3 since access condition from previous Terminal Authentication MUST be reset) |

### 3.8.16 Test case ISO7816_L_16

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_L_16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test that the chip rejects an additional PACE run or resets extended access rights after the terminal has been authenticated as extended inspection system with a first BAC run.</td>
</tr>
<tr>
<td>Version</td>
<td>1.5</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, PACE, BAC</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed. BAC MUST be used.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).</td>
</tr>
</tbody>
</table>

**Test scenario**

1. Send the given MSE: Set DST APDU to the eMRTD.

\[ \text{‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’} \]

- <Cryptogram> contains the following encrypted data objects
  - 83 <L83> <Certification Authority Reference>
  - The Certification Authority Reference MUST be used as read from the EF.CVCA file.

2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1.

\[ \text{‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’} \]

- <Cryptogram> contains the following encrypted data objects
  - 7F 4E <L7F4E> <certificate body>
  - 5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.

\[ \text{‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’} \]
Test plan for eMRTDs with EACv1

- <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certification Authority Reference>
- The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS CERT_1.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

5. Send the given MSE: Set AT APDU to the eMRTD.
   '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Holder Reference>
   - The Certification Holder Reference stored inside the IS-Certificate sent in step 4 has to be used.

6. Send the given Get Challenge APDU to the eMRTD.
   '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'

7. Send the given external authenticate command to the eMRTD.
   '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'
   - <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS KEY_01.

8. Select the MF by sending the given Select APDU to the eMRTD:
   '0C A4 00 0C 0A 8E 08 <Checksum> 00'

9. Under SM, Perform an additional run of the “Open ePassport Application” procedure with PACE.

10. Use new SM keys from PACE run. Send the READ BINARY (with SFI) command to the eMRTD to verify the access to Data Group 3 has NOT been granted.
    '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'

Expected results

1. '90 00’ in an SM response
2. '90 00’ in an SM response
3. '90 00’ in an SM response
4. '90 00’ in an SM response
5. '90 00’ in an SM response
6. '<Eight bytes of random data> 90 00’ in an SM response
7. '90 00’ in an SM response
8. '90 00’ in an SM response, or ISO checking error, or ISO checking error in an SM response. If this step returns an ISO checking error the next test steps SHALL be skipped.
9. Successful run of “Open ePassport Application” procedure or ISO checking error. If “Open ePassport Application” procedure fails, the next steps SHALL be skipped.
10. ISO checking error in an SM response (chip MUST reject access to Data Group 3 since access condition from previous Terminal Authentication MUST be reset)
3.9  Unit ISO7816_M – Update mechanism

This unit contains all test cases which update the chips persistent memory. Therefore these tests can be performed only once with a combination of a distinct sample and set of certificates. To reproduce this test unit, a new set with future certificate dates has to be created or a different test object has to be used.

3.9.1  Test case ISO7816_M_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_M_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the “Current Date” update mechanism with a new domestic IS certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
2. The Chip Authentication mechanism MUST have been performed as well.  
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD. ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
  • <Cryptogram> contains the following encrypted data objects  
    83 <L83> <Certification Authority Reference>  
  • The Certification Authority Reference MUST be used as read from the EF.CVCA file  
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 6” as DV_CERT_6  
   ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • The DV certificate is marked as a domestic certificate  
3. Send the given MSE: Set DST APDU to the eMRTD. ‘0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
  • <Cryptogram> contains the following encrypted data objects  
    83 <L83> <Certification Authority Reference>  
  • The Certification Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.  
4. Send the appropriate IS-Certificate as specified in the “Certificate Set 6” as IS_CERT_6a.  
  ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’  
  • <Cryptogram> contains the following encrypted data objects  
    7F 4E <L7F4E> <certificate body>  
    5F 37 <L5F37> <certificate signature>  
  • This certificate has an advanced effective date. Since the DV
Test plan for eMRTDs with EACv1

1. Test case ISO7816_M_2

   Expected results

   1. '90 00' in an SM response
   2. '90 00' in an SM response.
   3. '90 00' in an SM response.
   4. '90 00' in an SM response.
   5. '90 00' in an SM response.
   6. '90 00' in an SM response.
   7. '90 00' in an SM response.
   8. ISO checking error or '6300' in an SM response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

   3.9.2 Test case ISO7816_M_2
### Purpose
Test the “Current Date” update mechanism with a new DV certificate.

### Version
1.2

### Profile
TA

### Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).

### Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file
2. Send the appropriate DV-Certificate as specified in the “Certificate Set 6” as DV_CERT_6a
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • The DV certificate has an advanced effective data. beyond the expiration date of DV_CERT_6  
   • Reset the chip after this step and restore the preconditions for this test case before the next step is performed.
3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'  
   • <Cryptogram> contains the following encrypted data objects  
     83 <L83> <Certification Authority Reference>  
   • The Certification Authority Reference MUST be used as read from the EF.CVCA file
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'  
   • <Cryptogram> contains the following encrypted data objects  
     7F 4E <L7F4E> <certificate body>  
     5F 37 <L5F37> <certificate signature>  
   • This certificate has an expiration date before the effective date that was set in step 2. Therefore, this certificate SHALL be rejected

### Expected results
1. ’90 00’ in an SM response
2. ’90 00’ in an SM response.
3. ’90 00’ in an SM response.
4. ISO checking error or ‘6300’ in an SM response. This certificate MUST no longer be valid, since the current date of the chip has been updated.
### 3.9.3 Test case ISO7816_M_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_M_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the “Trust Point” update mechanism with a new link certificate.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
              2. The Chip Authentication mechanism MUST have been performed as well.  
              3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point). |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
               `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
               - `<Cryptogram>` contains the following encrypted data objects  
                 83 <L83> <Certification Authority Reference>  
               - The Certification Authority Reference MUST be used as read from the EF.CVCA file  
               2. Send the appropriate link certificate as specified in the “Certificate Set 7" as LINK_CERT_7. The ePassport MUST update the trust point with this new certificate.  
               `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
               - `<Cryptogram>` contains the following encrypted data objects  
                 7F 4E <L7F4E> <certificate body>  
                 5F 37 <LSF37> <certificate signature>  
               3. Power down the field or remove the passport from the reader, so that the chip looses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory.  
               - Power up the chip  
               - Reestablish the preconditions  
               - Read the EF.CVCA as exactly 36 bytes, using the SELECT and READ BINARY command  
                 `0C A4 02 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
                 The cryptogram contains the encrypted FID of the EF.CVCA file `<fid.EF.CVCA>`  
                 `0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00`  
               - Check that EF.CVCA file contains now two trust points and verify that the new trust point is at the first position and the previous one has been moved to the second position.  
               - Any remaining bytes of the EF.CVCA content MUST be filled with ‘00’.  
               4. Send the given MSE: Set DST APDU to the eMRTD.  
                  `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00`  
                  - `<Cryptogram>` contains the following encrypted data objects  
                    83 <L83> <Certification Authority Reference>  
                  - The Certification Authority Reference MUST be the SECOND trust... |
5. Send the appropriate DV-Certificate as specified in the “Certificate Set 7”
as DV_CERT_7a.
\[0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>\]
- `<Cryptogram>` contains the following encrypted data objects
  7F 4E `<L7F4E>` `<certificate body>`
  5F 37 `<L5F37>` `<certificate signature>`
- Since the previous trust point is still valid, the certificate MUST be
  verified successfully.
- Reset the chip after this step and restore the preconditions for this test
  case before the next step is performed.

6. Send the given MSE: Set DST APDU to the eMRTD.
\[0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00\]
- `<Cryptogram>` contains the following encrypted data objects
  83 `<L83>` `<Certification Authority Reference>`
- The Certification Authority Reference MUST be the FIRST trust point
  as read from the EF.CVCA file.

7. Send the appropriate DV-Certificate as specified in the “Certificate Set 7”
as DV_CERT_7b.
\[0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>\]
- `<Cryptogram>` contains the following encrypted data objects
  7F 4E `<L7F4E>` `<certificate body>`
  5F 37 `<L5F37>` `<certificate signature>`
- Since the effective date of this certificate is after the expiration date of
  the original trust point, the chip MUST update the current date and
  MUST also disable the original trust point.
- Reset the chip after this step and restore the preconditions for this test
  case before the next step is performed.

8. Send the given MSE: Set DST APDU to the eMRTD.
\[0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> 00\]
- `<Cryptogram>` contains the following encrypted data objects
  83 `<L83>` `<Certification Authority Reference>`
- Use the original Certification Authority Reference (same as in step 4).

9. Send the appropriate DV-Certificate as specified in the “Certificate Set 7”
as DV_CERT_7a.
\[0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>\]
- `<Cryptogram>` contains the following encrypted data objects
  7F 4E `<L7F4E>` `<certificate body>`
  5F 37 `<L5F37>` `<certificate signature>`
- Since the trust point has been disabled, the certificate verification
  MUST fail.

<table>
<thead>
<tr>
<th>Expected results</th>
<th>1. '90 00’ in an SM response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. '90 00’ in an SM response.</td>
</tr>
<tr>
<td></td>
<td>3. true</td>
</tr>
</tbody>
</table>
3.9.4 Test case ISO7816_M_4

Test - ID | ISO7816_M_4
---|---
Purpose | Test the “Trust Point” update mechanism with two link certificates.
Version | 1.2
Profile | TA

Preconditions
1. The "Open ePassport Application" procedure MUST have been performed.
2. The Chip Authentication mechanism MUST have been performed as well.
3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).
4. This test case can only be done AFTER ISO7816_M_3 has been performed.

Test scenario
1. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Authority Reference MUST be the FIRST trust point as read from the EF.CVCA file.

2. Send the appropriate link certificate as specified in the “Certificate Set 8” as LINK_CERT_8. The ePassport MUST update the trust point with this new certificate.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>,'
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certificate reference>
   • The Certification Reference MUST be used as specified in the Link certificate used in step 2.

4. Send the appropriate link certificate as specified in the “Certificate Set 9” as LINK_CERT_9. The ePassport MUST update the trust point with this new certificate.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08
<Checksum> <Le>’
• <Cryptogram> contains the following encrypted data objects
  7F 4E <L7F4E> <certificate body>
  5F 37 <L5F37> <certificate signature>
5. Send the given MSE: Set DST APDU to the eMRTD.
   ‘0C 22 81 B6 <Lc> 87 <Lb7> 01 <Cryptogram> 8E 08
   <Checksum> 00’
• <Cryptogram> contains the following encrypted data objects
  83 <L83> <Certificate Authority Reference>
• The Certification Reference MUST be used as specified in the second
  Link certificate used in step 4.
6. Send the appropriate DV-Certificate as specified in the “Certificate Set 9”
   as DV_CERT_9.
   ‘0C 2A 00 BE <Lc> 87 <Lb7> 01 <Cryptogram> 8E 08
   <Checksum> <Le>’
• <Cryptogram> contains the following encrypted data objects
  7F 4E <L7F4E> <certificate body>
  5F 37 <L5F37> <certificate signature>
7. Read the EF.CVCA as exactly 36 bytes, using the SELECT and READ
   BINARY command
• ‘0C A4 02 0C <Lc> 87 <Lb7> 01 <Cryptogram> 8E 08
   <Checksum> 00’
   The cryptogram contains the encrypted FID of the EF.CVCA file
   <fid.EF.CVCA>
• ‘0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’
• Verify the EF.CVCA file that both new trust points are present. The
  previous trust point from the LINK_CERT_7 MUST be gone.
• The remaining (three) bytes of the EF.CVCA content MUST be
  padded with ‘00’.

Expected results
1. ‘90 00’ in an SM response
2. ‘90 00’ in an SM response.
3. ‘90 00’ in an SM response
4. ‘90 00’ in an SM response
5. ‘90 00’ in an SM response
6. ‘90 00’ in an SM response
7. true

3.9.5 Test case ISO7816_M_5

<table>
<thead>
<tr>
<th>Test-Id</th>
<th>ISO7816_M_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the transition CVCA ⇒ CVCA ⇒ IS</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
<tr>
<td></td>
<td>2. The Chip Authentication mechanism MUST have been performed as well.</td>
</tr>
<tr>
<td></td>
<td>3. The Certification Authority Reference MUST have been read from the</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

EF_CVCA file (Primary trust point).

Test scenario

1. Send the given MSE: Set DST APDU to the eMRTD.
   \[0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00\]
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Authority Reference MUST be used as read from the
     EF.CVCA file (Primary trust point).

2. Send the appropriate CVCA-Certificate as specified in the “Certificate Set
   11” chapter as LINK_CERT_11b.
   \[0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>\]
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

3. Send the given MSE: Set DST APDU to the eMRTD.
   \[0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00\]
   - <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   - The Certification Holder Reference stored inside the new CVCA-
     Certificate sent in step 2 has to be used.

4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11”
   chapter as IS_CERT_11c.
   \[0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>\]
   - <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

Expected results

1. '90 00' in an SM response
2. '90 00' in an SM response
3. '90 00' in an SM response
4. ISO checking error or '63 00' in an SM response

3.9.6 Test case ISO7816_M_6

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_M_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test sanity of the EF.CVCA</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. The &quot;Open ePassport Application&quot; procedure MUST have been performed.</td>
</tr>
</tbody>
</table>
| Test scenario | 1. Send the given SELECT APDU to the eMRTD. 
   \[0C A4 02 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00\]
   - The cryptogram contains the encrypted FID of the EF.CVCA file
     <fid.EF.CVCA>.
2. Send the given READ BINARY APDU to the eMRTD trying to read 36 bytes.
   ’0C B0 00 00 0D 97 01 24 8E 08 <Checksum> 00’
3. The EF.CVCA MUST contain two trust points
4. The remaining (six) bytes of the EF.CVCA content MUST be padded with ‘00’
5. Send another READ BINARY APDU to the MRTD trying to read another byte at offset 36
   ’0C B0 00 24 0D 97 01 01 8E 08 <Checksum> 00’

**Expected results**
1. ’90 00’ in an SM response
2. Exactly 36 bytes of content data and ’90 00’ in an SM response
3. true
4. true
5. ISO checking error in an SM response

### 3.10 Unit ISO7816_N – Migration policies

This unit covers all tests about the migration policies. This mechanism is used for the import of new CVCA key with new TA algorithm in post issuance phase.

The purpose of this unit is to ensure that the migration policy(ies) claimed by the manufacturer can be implemented.

This unit has to be performed once for each possible migration scenario indicated by the passport provider. After the algorithm has been updated, the full test specification has to be repeated based on this new algorithm.

#### 3.10.1 Test case ISO7816_N_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>ISO7816_N_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test mechanism migration according to the manufacturer’s implementation statement.</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Profile</td>
<td>TA, MIG</td>
</tr>
</tbody>
</table>
| Preconditions | 1. The "Open ePassport Application" procedure MUST have been performed.  
               2. The Chip Authentication mechanism MUST have been performed as well.  
               3. The Certification Authority Reference MUST have been read from the EF.CVCA file (Primary trust point).  
               4. This test case can only be done AFTER ISO7816_M_5 has been performed. |
| Test scenario | 1. Send the given MSE: Set DST APDU to the eMRTD.  
               ’0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’  
               • <Cryptogram> contains the following encrypted data objects  
                 83 <L83> <Certification Authority Reference>  
               • The Certification Authority Reference MUST be the FIRST trust point as read from the EF.CVCA file. |
2. Send the appropriate link certificate with the updated mechanism as defined in “Certificate Set 13” as LINK_CERT_13. The ePassport MUST update the trust point with this new certificate.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
3. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <certificate reference>
   • The Certification Reference MUST be used as specified in the Link certificate used in step 2.
   • The chip MUST be able to use the updated cryptographic algorithms as introduced by the link certificate in step 2.
4. Send the appropriate DV certificate as specified in the “Certificate Set 13” as DV_CERT_13.
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>
5. Send the given MSE: Set DST APDU to the eMRTD.
   '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’
   • <Cryptogram> contains the following encrypted data objects
     83 <L83> <Certification Authority Reference>
   • The Certification Reference MUST be used as specified in the DV certificate used in step 4.
6. Send the appropriate IS-Certificate as specified in the “Certificate Set 13” as IS_CERT_13
   '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’
   • <Cryptogram> contains the following encrypted data objects
     7F 4E <L7F4E> <certificate body>
     5F 37 <L5F37> <certificate signature>

| Expected results | 1. '90 00’ in an SM response |
|                 | 2. '90 00’ in an SM response. |
|                 | 3. '90 00’ in an SM response |
|                 | 4. '90 00’ in an SM response |
|                 | 5. '90 00’ in an SM response |
|                 | 6. '90 00’ in an SM response |
4 Tests for layer 7 (LDS)

4.1 Unit LDS_E – Data Group 14

This unit covers all tests about the coding of the Data Group 14 containing the public key information required for the chip authentication mechanism.

If the Data Group 14 contains multiple instances of the same element type (e.g. TerminalAuthenticationInfo), the corresponding test cases have to be performed for each element. A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.1.1 Test case LDS_E_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_E_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 1.5</td>
</tr>
</tbody>
</table>

4.1.2 Test case LDS_E_2

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_E_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the ASN.1 encoding of the TerminalAuthenticationInfo</td>
</tr>
<tr>
<td>Version</td>
<td>1.11</td>
</tr>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. Data Group 14 MUST have been read from the eMRTD</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. If at least one TerminalAuthenticationInfo element (with OID id-TA) is present, there MUST be at least one TerminalAuthenticationInfo element (with OID id-TA) with the version element set to 1.</td>
</tr>
<tr>
<td></td>
<td>2. There MUST be no SecurityInfo element specifying a specific TA protocol like id-TA-RSA. Only the generic identifier id-TA MUST be used inside the Data Group 14 security info.</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. true</td>
</tr>
<tr>
<td></td>
<td>2. true</td>
</tr>
</tbody>
</table>

4.1.3 Test case LDS_E_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_E_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 1.5</td>
</tr>
</tbody>
</table>

4.1.4 Test case LDS_E_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_E_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Deleted in version 1.5</td>
</tr>
</tbody>
</table>

4.1.5 Test case LDS_E_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_E_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Test the ASN.1 encoding of the TerminalAuthenticationInfo</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Version</th>
<th>1.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>TA</td>
</tr>
</tbody>
</table>
4.3 Unit LDS_G – Data Group 3

This unit includes all test cases concerning the DG 3 element (fingerprint). As the purpose of this test specification is not to test biometrics, only the general DG3 header (as defined in [R1] and [R2]) is tested to ensure minimum conformance.

Test cases LDS_G_05 to LDS_G_10 MUST are repeated for each instance of Biometric Information Template present in the DG3.

A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.3.1 Test case LDS_G_1

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>LDS_G_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the template tag; the encoded DG 3 element starts with.</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. Encoded EF.DG3 object in binary format as read from the eMRTD.</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Check the very first byte of the EF.DG3 element</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. First byte MUST be ‘63’</td>
</tr>
</tbody>
</table>

4.3.2 Test case LDS_G_2

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>LDS_G_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of DG3 length bytes.</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. Encoded EF.DG3 object in binary format as read from the eMRTD.</td>
</tr>
</tbody>
</table>
| Test scenario | 1. Analyze the encoding of the bytes that follow the template tag  
2. Verify the length of the DG3 |
| Expected results | 1. The bytes that follow the template tag MUST contain a valid length encoding (According to ASN.1 encoding rules).  
2. The encoded length MUST match the size of the DG3 value bytes. |

4.3.3 Test case LDS_G_3

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>LDS_G_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the Biometric Information Group Template (BIGT).</td>
</tr>
<tr>
<td>Version</td>
<td>1.12</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. Encoded EF.DG3 object in binary format as read from the eMRTD.</td>
</tr>
</tbody>
</table>
| Test scenario | 1. Check that the first tag in the DG 3 value is the BIGT tag.  
2. Verify the length of the BIGT.  
3. Verify that the BIGT is the only information in the DG3. |
| Expected results | 1. Tag MUST be ‘7F 61’;  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). |
3. The encoded length MUST match the number of remaining bytes of the DG 3 data element, except if the BIGT contains no BITs (no fingerprints). In this case the BIGT MAY be followed by a DO 53 containing random data to prevent the static hash value.

### 4.3.4 Test case LDS_G_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the number of instances stored in the Biometric Information Group Template (BIGT).</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
<tr>
<td>Preconditions</td>
<td>1. Encoded EF.DG3 object in binary format as read from the eMRTD.</td>
</tr>
</tbody>
</table>
| Test scenario | 1. Check the first tag inside the BIGT.  
2. Verify the length of the “number of instances” data object.  
3. Verify the value of the “number of instances” data object. |
| Expected results | 1. Tag MUST be ‘02’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The number of instances MUST match the actual number of encoded Biometric Information Templates (tag 7F 60). |

### 4.3.5 Test case LDS_G_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the Biometric Information Template (BIT).</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>
| Preconditions | 1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the tag of the BIT.  
2. Verify the length of the BIT data object.  
3. Verify that the encoded length match the size of the BIT. |
| Expected results | 1. Tag MUST be ‘7F 60’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the effective length of the encoded BIT |

### 4.3.6 Test case LDS_G_6

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the Biometric Header Template (BHT).</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>
| Preconditions | 1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the tag of the BHT  
2. Verify the length of the BHT data object. |
### Test plan for eMRTDs with EACv1

| Expected results |  
|------------------|---
| 1. Tag MUST be ‘A1’.  
| 2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
| 3. The encoded length MUST match the effective length of the encoded BHT. | --- |

#### 4.3.7 Test case LDS_G_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the presence/encoding of the CBEFF element &quot;format owner&quot;.</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>

**Preconditions**

1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. The tested CBEFF element is part of the BHT located in LDS_G_06.  
3. This test MUST be repeated for each instance of BIT

**Test scenario**

1. Check the presence of the “format owner” tag.  
2. Verify the length of the “format owner” data object.  
3. Check the length of the “format owner” value.  
4. Verify the “format owner” value.

**Expected results**

1. Tag MUST be ‘87’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The length of the value field MUST be 2 bytes.  
4. The value of the format owner MUST be a registered CBEFF owner. It MUST be ‘01 01’ for the first instance of BIT. All registered format owner can be found at www.ibia.org.

#### 4.3.8 Test case LDS_G_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the presence/encoding of the CBEFF element &quot;format type&quot;.</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>

**Preconditions**

1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. The tested CBEFF element is part of biometric header template located in LDS_G_06.  
3. This test MUST be repeated for each instance of BIT

**Test scenario**

1. Check the presence of the “format type” tag.  
2. Verify the length of the “format type” data object.  
3. Check the length of the “format type” value.  
4. Verify the “format type” value.

**Expected results**

1. Tag MUST be ‘88’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The length of the value field MUST be 2 bytes.  
4. The value of the format type MUST be a registered CBEFF type. It MUST be ‘0007’ for the first instance of BIT. All registered format types can be found at www.ibia.org.
### 4.3.9 Test case LDS_G_9

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the presence/encoding of the CBEFF element &quot;biometric subtype&quot;.</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>
| Preconditions | 1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. The tested CBEFF element is part of biometric header template located in LDS_G_06.  
3. This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the presence of the “biometric subtype” tag.  
2. Verify the length of the “biometric subtype” data object.  
3. Check the length of the “biometric subtype” value.  
4. Verify the “biometric subtype” value. |
| Expected results | 1. Tag MUST be ‘82’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The length of the value field MUST be 1 byte.  
4. The value of the format type MUST be a registered CBEFF biometric subtype. The values for the biometric subtype are defined in ISO 19785-3. |

### 4.3.10 Test case LDS_G_10

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the Biometric Data Block (BDB) tag.</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>
| Preconditions | 1. Encoded EF.DG3 object in binary format as read from the eMRTD.  
2. The BDB is part of the biometric information template tested in LDS_G_05.  
3. This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the presence of the BDB tag.  
2. Verify the length of the BDB.  
3. Verify that the encoded length match the size of encoded BDB |
| Expected results | 1. Tag MUST be ‘5F 2E’ or ‘7F 2E’  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the effective length of the encoded BDB |

### 4.3.11 Test case LDS_G_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_G_11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test verifies the consistency between the CBEFF format type and the BDB format identifier of the BIT</td>
</tr>
<tr>
<td>Version</td>
<td>0.8</td>
</tr>
<tr>
<td>Profile</td>
<td>DG3</td>
</tr>
</tbody>
</table>
| Preconditions | - Encoded EF.DG3 object in binary format as read from the eMRTD.  
- The BDB is part of the biometric information template tested in LDS_G_05. |
Test plan for eMRTDs with EACv1

- This test MUST be repeated for each instance of BIT"

<table>
<thead>
<tr>
<th>Test scenario</th>
<th>1. Check the first four bytes of the BDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected results</td>
<td>1. The value MUST be '46 49 52 00' ('F' 'I' 'R' 0x0).</td>
</tr>
</tbody>
</table>

4.4 Unit LDS_H – Data Group 4

This unit includes all test cases concerning the DG 4 element (Iris). As the purpose of this test specification is not to test biometrics, only the general DG4 header (as defined in [R1] and [R2]) is tested to ensure minimum conformance.

Test cases LDS_H_5 to LDS_H_10 MUST are repeated for each instance of Biometric Information Template present in the DG4.

A test case is only rated as a PASS if all passes of a test case are performed without any failure, so that all test runs for one test case lead to a single result.

4.4.1 Test case LDS_H_1

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the template tag; the encoded DG 4 element starts with.</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG4</td>
</tr>
<tr>
<td>Preconditions</td>
<td>Encoded EF.DG4 object in binary format as read from the eMRTD.</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Check the very first byte of the EF.DG4 element</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. First byte MUST be ‘76’</td>
</tr>
</tbody>
</table>

4.4.2 Test case LDS_H_2

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>LDS_H_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of DG4 length bytes.</td>
</tr>
<tr>
<td>Version</td>
<td>0.6</td>
</tr>
<tr>
<td>Profile</td>
<td>DG4</td>
</tr>
<tr>
<td>Preconditions</td>
<td>Encoded EF.DG4 object in binary format as read from the eMRTD.</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Analyze the encoding of the bytes that follow the template tag 2. Verify the length of the DG4</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. The bytes that follow the template tag MUST contain a valid length encoding (According to ASN.1 encoding rules). 2. The encoded length MUST match the size of the DG4 value bytes</td>
</tr>
</tbody>
</table>

4.4.3 Test case LDS_H_3

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the encoding of the Biometric Information Group Template (BIGT).</td>
</tr>
<tr>
<td>Version</td>
<td>1.12</td>
</tr>
<tr>
<td>Profile</td>
<td>DG4</td>
</tr>
<tr>
<td>Preconditions</td>
<td>Encoded EF.DG4 object in binary format as read from the eMRTD.</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

| Test scenario | 1. Check that the first tag in the DG 4 value is the BIGT tag.  
2. Verify the length of the BIGT.  
3. Verify that the BIGT is the only information in the DG 4. |
| Expected results | 1. Tag MUST be ‘7F 61’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the number of remaining bytes of the DG 4 data element, except if the BIGT contains no BITs (no iris images). In this case the BIGT MAY be followed by a DO 53 containing random data to prevent the static hash value. |

### 4.4.4 Test case LDS_H_4

| Test - ID | LDS_H_4 |
| Purpose | This test checks the encoding of the number of instances stored in the Biometric Information Group Template (BIGT). |
| Version | 0.6 |
| Profile | DG4 |
| Preconditions | Encoded EF.DG4 object in binary format as read from the eMRTD. |
| Test scenario | 1. Check the first tag inside the BIGT.  
2. Verify the length of the “number of instances” data object.  
3. Verify the value of the “number of instances” data object. |
| Expected results | 1. Tag MUST be ‘02’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The number of instances MUST match the actual number of encoded Biometrics Information Templates (tag 7F 60). |

### 4.4.5 Test case LDS_H_5

| Test - ID | LDS_H_5 |
| Purpose | This test checks the encoding of the Biometric Information Template (BIT). |
| Version | 0.6 |
| Profile | DG4 |
| Preconditions |  
• Encoded EF.DG4 object in binary format as read from the eMRTD  
• This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the tag of the BIT.  
2. Verify the length of the BIT data object.  
3. Verify that the encoded length match the effective size of the BIT. |
| Expected results | 1. Tag MUST be ‘7F 60’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the length of the encoded BIT |

### 4.4.6 Test case LDS_H_6

| Test - ID | LDS_H_6 |
| Purpose | This test checks the encoding of the Biometric Header Template (BHT). |
| Version | 0.6 |
### Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Profile</th>
<th>DG4</th>
</tr>
</thead>
</table>
| Preconditions | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the tag of the BHT.  
2. Verify the length of the BHT data object.  
3. Verify that the encoded length match the size of the BHT |
| Expected results | 1. Tag MUST be ‘A1’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the effective length of the encoded BHT |

#### 4.4.7 Test case LDS_H_7

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the presence/encoding of the CBEFF element &quot;format owner&quot;.</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Profile</td>
<td>DG4</td>
</tr>
</tbody>
</table>
| Preconditions | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• The tested CBEFF element is part of biometric header template located in LDS_H_06.  
• This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the presence of the “format owner” tag.  
2. Verify the length of the “format owner” data object.  
3. Check the length of the “format owner” value.  
4. Verify the “format owner” value. |
| Expected results | 1. Tag MUST be ‘87’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The length of the value field MUST be 2 bytes.  
4. The value of the format owner MUST be a registered CBEFF owner. It MUST be ‘01 01’ for the first instance of BIT. All registered format owner can be found at www.ibia.org. |

#### 4.4.8 Test case LDS_H_8

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the presence/encoding of the CBEFF element &quot;format type&quot;.</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Profile</td>
<td>DG4</td>
</tr>
</tbody>
</table>
| Preconditions | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• The tested CBEFF element is part of biometric header template located in LDS_H_06.  
• This test MUST be repeated for each instance of BIT |
| Test scenario | 1. Check the presence of the “format type” tag.  
2. Verify the length of the “format type” data object.  
3. Check the length of the “format type” value.  
4. Verify the “format type” value. |
| Expected results | 1. Tag MUST be ‘88’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules). |
3. The length of the value field MUST be 2 bytes.
4. The value of the format type MUST be a registered CBEFF type. It MUST be ‘0009’ or ‘000B’ for the first instance of BIT. All registered format types can be found at www.ibia.org.

### 4.4.9 Test case LDS_H_9

<table>
<thead>
<tr>
<th>Test – ID</th>
<th>LDS_H_9</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This test checks the presence/encoding of the CBEFF element &quot;biometric subtype&quot;. Note that the biometric subtype element is optional for Data Group 4. Therefore this test case is only performed if the biometric subtype element is present.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.1</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>DG4</td>
</tr>
</tbody>
</table>
| **Preconditions** | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• The tested CBEFF element is part of biometric header template located in LDS_H_06.  
• This test MUST be repeated for each instance of BIT |
| **Test scenario** | 1. Check the presence of the “biometric subtype” tag.  
2. Verify the length of the “biometric subtype” data object.  
3. Check the length of the “biometric subtype” value.  
4. Verify the “biometric subtype” value. |
| **Expected results** | 1. Tag MUST be ‘82’.  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The length of the value field MUST be 1 byte.  
4. The value of the format type MUST be a registered CBEFF biometric subtype. The values for the biometric subtype are defined in ISO 19785-3. |

### 4.4.10 Test case LDS_H_10

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This test checks the encoding of the Biometric Data Block (BDB) tag.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>0.6</td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td>DG4</td>
</tr>
</tbody>
</table>
| **Preconditions** | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• The BDB is part of the biometric information template tested in LDS_H_05.  
• This test MUST be repeated for each instance of BIT |
| **Test scenario** | 1. Check the presence of the BDB tag.  
2. Verify the length of the BDB.  
3. Verify that the encoded length match the size of encoded BDB |
| **Expected results** | 1. Tag MUST be ‘5F 2E’ or ‘7F 2E’  
2. This element MUST have a valid encoded length (According to ASN.1 encoding rules).  
3. The encoded length MUST match the effective length of the encoded BDB |

### 4.4.11 Test case LDS_H_11

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_H_11</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>This test verifies the consistency between the CBEFF format type and the BDB</td>
</tr>
</tbody>
</table>
Test plan for eMRTDs with EACv1

| Version | 1.0 |
| Profile | DG4 |
| Preconditions | • Encoded EF.DG4 object in binary format as read from the eMRTD.  
• The BDB is part of the biometric information template tested in LDS_H_05.  
• This test MUST be repeated for each instance of BIT” |
| Test scenario | 1. Check the first four bytes of the BDB |
| Expected results | 1. The value MUST be ’49 49 52 00’ (’I’ ’I’ ’R’ 0x00). |

4.5 Unit LDS_L – EF.ATR/INFO

This unit includes all test cases concerning the EF.ATR/INFO. This file is used to store Extended Length parameters.

4.5.1 Test case LDS_L_1

| Test - ID | LDS_L_1 |
| Purpose | This test checks that the EF.ATR/INFO contains a valid list of TLV data objects including tag, length and data. |
| Version | 1.5 |
| Profile | EFATR |
| Preconditions | • Encoded EF.ATR/INFO object in binary format as read from the eMRTD. |
| Test scenario | 1. Verify the TLV structure of each data object listed in this file (tag, valid length, data) |
| Expected results | 1. All TLV objects must be valid |

4.5.2 Test case LDS_L_2

| Test - ID | LDS_L_2 |
| Purpose | This test checks that the EF.ATR/INFO contains a TLV data object for extended length. |
| Version | 1.5 |
| Profile | EFATR |
| Preconditions | • Encoded EF.ATR/INFO object in binary format as read from the eMRTD. |
| Test scenario | 1. Verify that there is a TLV object with tag ’7F 66’. |
| Expected results | 1. The tag of this element must be ’7F 66’. |

4.5.3 Test case LDS_L_3

| Test - ID | LDS_L_3 |
| Purpose | This test checks that the TLV object for extended length contains two valid integers (maximum buffer for sending and receiving APDUs). |
| Version | 1.5 |
| Profile | EFATR |
| Preconditions | • Encoded EF.ATR/INFO object in binary format as read from the eMRTD. |
Test plan for eMRTDs with EACv1

<table>
<thead>
<tr>
<th>Test scenario</th>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Verify that the TLV object contains two positive integers in a valid TLV structure.</td>
<td>1. This data object contains two positive integers.</td>
</tr>
</tbody>
</table>

4.5.4 Test case LDS_L_4

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_L_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks that the DO for card capabilities encodes support of chaining in software function table.</td>
</tr>
<tr>
<td>Version</td>
<td>1.5</td>
</tr>
<tr>
<td>Profile</td>
<td>EFATR</td>
</tr>
<tr>
<td>Preconditions</td>
<td>• Encoded EF.ATR/INFO object in binary format as read from the eMRTD.</td>
</tr>
<tr>
<td>Test scenario</td>
<td>1. Verify that the DO for card capabilities contains a bit for the support of the chaining mechanism.</td>
</tr>
<tr>
<td>Expected results</td>
<td>1. This data object contains a bit b8 that encodes the support of the chaining mechanism.</td>
</tr>
</tbody>
</table>

4.5.5 Test case LDS_L_5

<table>
<thead>
<tr>
<th>Test - ID</th>
<th>LDS_L_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>This test checks the accessibility of EF.ATR/INFO in MF.</td>
</tr>
<tr>
<td>Version</td>
<td>1.5</td>
</tr>
<tr>
<td>Profile</td>
<td>EFATR</td>
</tr>
<tr>
<td>Preconditions</td>
<td>• Reset chip.</td>
</tr>
</tbody>
</table>
| Test scenario | 1. Select MF.  
2. Send the given SELECT APDU for EF.ATR/INFO (FID: 2F 01) to the eMRTD as a plain APDU.  
'00 A4 02 0C 02 2F 01' |
| Expected results | 1. '90 00' in plain.  
2. '90 00' in plain. |

Annex A Implementation conformance statement

In order to set up the tests properly, an applicant SHALL provide the information specified in this annex. Some tests defined in this document are depending on the supported functionality of the passport. The test results will only cover the function declared in this statement.

A.1 Supported profiles

Tests which require functions not supported by the provided ePassport will be skipped during the tests. Please specify the profiles supported by the provided sample. For details on the profiles please refer to section 2.2.
Table 2: Supported profiles

<table>
<thead>
<tr>
<th>Profile</th>
<th>Applicant declaration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Authenticated Connection Establishment</td>
<td></td>
</tr>
<tr>
<td>Chip Authentication</td>
<td></td>
</tr>
<tr>
<td>Chip Authentication with MSE: Set AT &amp; General Authenticate</td>
<td></td>
</tr>
<tr>
<td>for 3DES algorithm support</td>
<td></td>
</tr>
<tr>
<td>Diffie-Hellman</td>
<td></td>
</tr>
<tr>
<td>Elliptic Curve Diffie-Hellman</td>
<td></td>
</tr>
<tr>
<td>Explicit key selection supported</td>
<td></td>
</tr>
<tr>
<td>Terminal Authentication</td>
<td></td>
</tr>
<tr>
<td>ECDSA algorithm</td>
<td></td>
</tr>
<tr>
<td>RSA algorithm</td>
<td></td>
</tr>
<tr>
<td>Migration of the crypto system</td>
<td></td>
</tr>
<tr>
<td>Certificate date validation</td>
<td></td>
</tr>
<tr>
<td>Support of EF.ATR/INFO</td>
<td></td>
</tr>
<tr>
<td>Support of Master File (MF)</td>
<td></td>
</tr>
<tr>
<td>For Terminal Authentication based on ECDSA algorithm,</td>
<td>include domain parameter in link certificate</td>
</tr>
<tr>
<td>(LINK_CERT_7, LINK_CERT_8, LINK_CERT_9, LINK_CERT_11)</td>
<td></td>
</tr>
<tr>
<td>Command APDU to send to the eMRTD to verify the chip's</td>
<td>ability to still require Secured Messaging. If not provided</td>
</tr>
<tr>
<td></td>
<td>'00 B0 81 00 00' will be used. This command has to be send as SM protected command.</td>
</tr>
</tbody>
</table>

A.2 Supported cryptographic algorithm

The applicant of the passport under test SHALL declare the cryptosystem (signature algorithm and hash algorithm) used to perform the Terminal Authentication.

Table 3: Supported cryptographic algorithm

<table>
<thead>
<tr>
<th>Signature algorithm</th>
<th>Key size (incl. curve name for ECDSA)</th>
<th>Hash algorithm</th>
</tr>
</thead>
</table>

A.3 Cryptosystem migration policy

If the eMRTD under test supports the migration to another cryptosystem, the applicant SHALL provide the list of supported target(s) cryptosystem(s) (signature algorithm and hash algorithm).

Note: For each target algorithm specified in this table, the test unit ISO7816_N has to be performed. Afterward, the fully test set has to be repeated for each new algorithm.
Table 4: Targets cryptosystems table

<table>
<thead>
<tr>
<th>Signature algorithm</th>
<th>Key size (incl. curve name for ECDSA)</th>
<th>Hash algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A.4 CVCA trust point information

For the preparation of the certificate sets defined in 2.4, the applicant has to provide some information about the current trust point stored inside the ePassport EF.CVCA file. Alternatively the application can provide a CVCA certificate containing this information.

Table 5: Trust point information

<table>
<thead>
<tr>
<th>Information</th>
<th>Applicant declaration (value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary trust point CAR</td>
<td></td>
</tr>
<tr>
<td>Primary trust point “Effective date”</td>
<td></td>
</tr>
<tr>
<td>Primary trust point “Expiration date”</td>
<td>Note that for the test scenarios covered by this test plan the time span between “Effective date” and “Expiration date” must be at least 2 month, otherwise some tests will fail.</td>
</tr>
</tbody>
</table>