Technical Guideline TR-03110

Amendment: Protocol extensions and specifications for Smart-eID

Version 1.0
14.10.2021
## Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>14.10.2021</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>
Contents

1 Introduction .............................................................................................................................. 5
  1.1 Terminology ...................................................................................................................... 5
2 Document Type .......................................................................................................................... 6
  2.1 Mobile Document Type ..................................................................................................... 6
  2.2 Mobile eID Security Mechanism ....................................................................................... 6
Bibliography .................................................................................................................................... 7

Tables
Table 1: Key words .......................................................................................................................... 5
1 Introduction

This Amendment to the Technical Guideline TR-03110 specifies the electronic security mechanisms for the mobile ID (Smart-eID). In addition to the DocumentType of the mobile ID, the MobileEIDTypeInfo is defined, which describes the underlying realization of the mobile ID enabling eID-Client and eID-Server to distinguish between the different types.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1]. The key word "CONDITIONAL" is to be interpreted as follows:

CONDITIONAL: The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

When used in tables (profiles), the key words are abbreviated as shown in Table 1.

<table>
<thead>
<tr>
<th>Key word</th>
<th>Abbrev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUST / SHALL</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>MUST NOT / SHALL NOT</td>
<td>-</td>
</tr>
<tr>
<td>SHOULD</td>
<td>RECOMMENDED</td>
</tr>
<tr>
<td>MAY</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>-</td>
<td>CONDITIONAL</td>
</tr>
</tbody>
</table>

Table 1: Key words
2 Document Type

2.1 Mobile Document Type

The document type of any mobile electronic identity is defined in TR-03127 [2] and MUST be:

Document type: “OA”

The document type must be encoded in data group 1 (DG1) of the eID application.

The Security Objects of the file CardSecurity SHALL be signed by a dedicated Document Signer, which is exclusively allowed to issue mobile electronic identities. The DocumentType extension of that Document Signer MUST indicate the document type for mobile electronic identities and MUST NOT indicate any other document type.

2.2 Mobile eID Security Mechanism

Any mobile electronic identity MUST provide evidence on the underlying security mechanism used. Therefore SecurityInfos of EF.CardAccess and EF.CardSecurity MUST contain the following entry:

- Exactly one MobileEIDTypeInfo MUST be present.

MobileEIDTypeInfo: This data structure provides info on the security mechanism used by the mobile electronic identity (eID Type) as defined in section 4 of TR-03159 [3] and MUST be set accordingly.

```
\text{id-eIDType} \text{OBJECT IDENTIFIER ::= } \{ \\
\text{bsi-de} \text{ applications}(3) \text{ eID}(2) \text{ 3} \\
\}
\text{id-cardEIDType} \text{OBJECT IDENTIFIER ::= } \{ \\
\text{id-eIDType} \text{ 1} \\
\}
\text{id-mobileEIDType} \text{OBJECT IDENTIFIER ::= } \{ \\
\text{id-eIDType} \text{ 2} \\
\}
\text{id-mobileEIDType-SECertified} \text{OBJECT IDENTIFIER ::= } \{\text{id-mobileEIDType 1}\}
\text{id-mobileEIDType-SEEndorsed} \text{OBJECT IDENTIFIER ::= } \{\text{id-mobileEIDType 2}\}
\text{id-mobileEIDType-HWKeyStore} \text{OBJECT IDENTIFIER ::= } \{\text{id-mobileEIDType 3}\}
```

MobileEIDTypeInfo ::= SEQUENCE {
protocol \text{OBJECT IDENTIFIER } \{ \\
\text{id-mobileEIDType-SECertified} \text{ |} \\
\text{id-mobileEIDType-SEEndorsed} \text{ |} \\
\text{id-mobileEIDType-HWKeyStore}\}
version \text{INTEGER, -- SHOULD be 1} 
}
Bibliography

[1] S. Bradner. RFC 2119, Key words for use in RFCs to indicate requirement levels, 1997