Federal Office
for Information Security

Technical Guideline TR-03110

Amendment: Protocol extensions and specifications for Smart-eID

Version 1.0
14.10.2021

Document history

Version	Date	Description
1.0	14.10.2021	Initial Version

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: ExtendedAccessControl@bsi.bund.de
Internet: https://www.bsi.bund.de
© Federal Office for Information Security 2021

Contents

Tables

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.

Key word		**Abbrev.**
MUST / SHALL	REQUIRED	m
MUST NOT / SHALL NOT	–	x
SHOULD	RECOMMENDED	r
MAY	OPTIONAL	o
–	CONDITIONAL	c

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.

```
id-eIDType OBJECT IDENTIFIER ::= {
  bsi-de applications(3) eID(2) 3
}

id-cardEIDType OBJECT IDENTIFIER ::= {
  id-eIDType 1
}

id-mobileEIDType OBJECT IDENTIFIER ::= {
  id-eIDType 2
}

id-mobileEIDType-SECertified      OBJECT IDENTIFIER ::= {id-mobileEIDType
1}
id-mobileEIDType-SEEndorsed               OBJECT IDENTIFIER ::= {id-
mobileEIDType 2}
id-mobileEIDType-HWKeyStore               OBJECT IDENTIFIER ::= {id-
mobileEIDType 3}

MobileEIDTypeInfo ::= SEQUENCE {
     protocol              OBJECT IDENTIFIER (
                           id-mobileEIDType-SECertified |
                           id-mobileEIDType-SEEndorsed |
                           id-mobileEIDType-HWKeyStore)
     version               INTEGER, -- SHOULD be 1
}
```

Bibliography

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

[2] BSI: Technische Richtline TR-03127, eID-Dokumente basierend auf Extended Access Control

[3] BSI: Technische Richtlinie TR-03159, Mobile Identities