D32.7: CardInfo files for selected cards

D32.7

Document Identification	
Date	2015-10-28
Status	Final
Version	1.0

Related SP/WP	SP3/WP3.2	**Document Reference**	D32.7
Related Deliverable(s)	D32.1, D32.6	**Dissemination Level**	PU
Lead Participant	ECS	**Lead Author**	Hans-Martin Haase (ECS)
Contributors	Hans-Martin Haase (ECS) Tobias Wich (ECS)	**Reviewers**	Christof Rath (TUG) Christine Neupert (AGETO)

Abstract: In this deliverable, we provide details about the process of the creation of CardInfo files. Furthermore, we provide the list of created CardInfo files and short overview about the problem which occurred while the creation process.

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the European Unions Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424.

1 Document Information

1.1 Contributors

Name	Affiliation
Hans-Martin Haase	ECS
Tobias Wich	ECS

1.2 History

0.1	2015-10-14	Tobias Wich (ECS)	Document Outline
0.2	2015-10-15	Hans-Martin Haase (ECS)	First complete version
0.9	2015-10-15	Tobias Wich (ECS)	Quality Assurance
1.0	2015-10-28	Hans-Martin Haase (ECS)	Integrate corrections according to the remarks of the reviewers and finalize document

1.3 Table of Contents


FutureID

2 Introduction

In this deliverable, we provide details about the process of the creation of CardInfo files or short CIFs. CardInfo files are needed for the access of smartcards in the FutureID client. They are used for the recognition of smartcards, for the determination of algorithms and parameters for various crypto operations, such as digital signatures, and they provide a description of the file system on the card which is necessary for operations on files, so that, e.g., certificates or files containing personal data of the card holder can be read.

The CardInfo structure is specified in CEN 15480 [1] and is suitable for a large variety of smartcards. The process of creating these CIFs can be very time consuming if done manually. This process may be sped up by using the CardInfo-Wizard developed in D32.6 but there are still cases where parts of the CIF have to be modified manually. The results of the tool are also dependent on the implementation of the card. According to the specifications, namely ISO/IEC 7816-15[2], some of the descriptive elements are optional which leads to specification conforming cards, which still provide too few information to produce sensible CardInfo files.

[1] European Committee for Standardization (CEN), Identification card systems - European Citizen Card, CEN/TS 15480, Part 1-4, 2008.

[2] ISO/IEC, Identification cards - Integrated circuit cards - Part 15: Cryptographic information application, International Standard, ISO/IEC 7816-15,2004.

3 Creation of CardInfo files

3.1 CardInfo-Wizard

The creation of CardInfo files with the CardInfo-Wizard is explained in detail in D32.6. A plug-in, a reader and card must be selected and a strategy for discovering the content of the card must be executed. This requires at least an ISO/IEC 7816-15 file structure, which is not present on every card. There are a lot of cards that contain proprietary structures, which may only be discovered by a brute force approach where all possible files are accessed. The problem with the brute force approach is that it just allows to explore the file system. Such an algorithm does not provide any information about the keys on the card or available cryptographic algorithms. An ISO 7816-15 structure on a card is able to provide such information.

A successful run of the CardInfo-Wizard produces a CardInfo file that contains the file structure of the card as well as the cryptographic objects like signature keys and the elements that are necessary for the execution of cryptographic operations such as signature creation. Such elements, e.g., are PINs or PUKs. The manual task is then to link all this information together in case the structures do not provide these details.

The keys need to be associated with the related certificates and the PIN to use them. Furthermore, the access rights of the files and data structures have to be specified, which is also dependent on the information provided by the card. Also there is no complete mapping between access rights specified in ISO/IEC 7816-4[3], ISO/IEC 7816-15 and CEN 15480.

3.2 Manual creation of CardInfo files

This approach was used in case the card does not provide an ISO/IEC 7816-15 structure but the issuer provides documentation for the card. An example for such a case is the Estonian eID card which does not provide ISO/IEC 7816-15 structures, however the specification of the card is publicly available at `http://www.id.ee/index.php?id=35772`. This documentation contains everything that is needed to write a CardInfo file by hand.

3.3 Problems with the examined smartcards

This section describes problems specific to certain smartcards that occurred during the creation of the CardInfo files.

3.3.1 Unknown file structure

There are several cards in the field which do not have a ISO/IEC 7816-15 file structure so the file system structure is in general unknown. As mentioned in the sections before there is

[3]ISO/IEC, Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange, International Standard, ISO/IEC 7816-15,2004.

the possibility to use a brute force approach to extract the file system information, however as also mentioned before, this approach does not provide information about the cryptographic specifics and other features. The required information might be taken from a publicly available specification, but very few card issuers also provide these documents to the public. Another source of information are open source projects, which use a specific card and thus have some knowledge hidden in the source code or other resources. This is also a very time consuming way to gather the needed information in contrast to an automated extraction.

3.3.2 Missing information about access rights

The access rights of files or keys may be specified in the file control parameters (FCP) of a file in the ISO/IEC 7816-15 data of the key. Certain cards do not provide this FCP data at all and some omit the necessary access and security conditions in case the FCP is present. It is also possible that this information is present in a proprietary format. Unfortunately, this is even foreseen in ISO/IEC 7816-15 and leads to a situation where the access rights can not be extracted without further information about the card from the manufacturer. In the worst case the access rights have to be evaluated by trying to access the object in question by sending hand crafted APDUs to the card.

3.3.3 Custom APDUs for standard operations

The most critical point are custom Application Protocol Data Units (APDUs) for standard operations like signature creation. In CEN 15480 there are some APDU mappings provided for cryptographic operations for instance to set a managed security environment for the signature creation. This means the signature process can not be depicted in the CardInfo structure. For this purpose an extension to the CardInfo specification has been created, which makes it possible to specify proprietary APDU calls which might be necessary to perform the actions to create a signature. The new element *LegacySignatureGenerationInfo*, which is defined below, is able to represent these custom APDUs. It can be used in the *CryptoMarkerType* as a replacement for *SignatureGenerationInfo*. It enables the client to use the specific card for the signature creation despite its deviation from the standard.

```
<simpleType name="APDUTemplateValueType">
  <restriction base="normalizedString">
    <pattern value="^([0-9a-fA-F]{2}|(\{[a-zA-Z][a-zA-Z0-9]*(\s+(([a-zA-Z][a-zA-Z0-9]*)
        |(0x([0-9a-fA-F]{2})+)))*\}))+$" />
  </restriction>
</simpleType>

<complexType name="CardCallTemplateType">
  <sequence>
    <element name="HeaderTemplate" type="iso:APDUTemplateValueType" />
    <element name="DataTemplate" type="iso:APDUTemplateValueType" minOccurs="0" />
    <element name="ExpectedLength" type="nonNegativeInteger" minOccurs="0" />
  </sequence>
```

```
</complexType>

<complexType name="LegacySignatureGenerationType">
  <sequence>
    <element name="CardCommand" type="iso:CardCallTemplateType" minOccurs="1" />
  </sequence>
</complexType>
```

3.4 List of created CardInfo files

The following list contains all CardInfo files with the corresponding ObjectIdentifier. The files can be found on the livelink server under the following URL. `https://dms-prext.fraunhofer.de/livelink/livelink.exe?func=ll&objaction=overview&objid=6312199`

- Belgium eID version 1.01
  http://eid.belgium.be/en/find_out_more_about_the_eid/the_electronic_identity_documents/the_eid/v1.01
- Belgium eID version 1.7
  http://eid.belgium.be/en/find_out_more_about_the_eid/the_electronic_identity_documents/the_eid/v1.7+
- DATEV signature card for professionals
  http://www.datev.de/smartcard
- D-TRUST card batch version 3.0
  https://www.d-trust.net/produkte/d-trust-signaturkarten/d-trust-card/batch_v3
- D-TRUST card multi version 3.0
  https://www.d-trust.net/produkte/d-trust-signaturkarten/d-trust-card/multi_v3
- D-TRUST card standard version 3.0
  https://www.d-trust.net/produkte/d-trust-signaturkarten/d-trust-card/standard_v3
- ecard Austria generation 3
  http://cif.chipkarte.at/e-card/g3
- Estonian eID version 3.0
  http://cif.id.ee/eid
- Estonian eID version 3.5
  http://cif.id.ee/eidV3.5
- Health professional card Germany
  http://www.aekno.de/eAT-light
- Latvian eID
  http://www.pmlp.gov.lv/en/home/services/personal-certificates-(eid)/
  Note: Not integrated into the client , recognition was successfully test but because of a missing PIN no cryptographic functions are tested.
- Peruvian eID
  http://portales.reniec.gob.pe/web/dni
  Note: Not integrated into the client.

- S-TRUST single signature card
  https://www.s-trust.de/produkte/strust_massensignaturkarte
- S-TRUST mass signature card
  https://www.s-trust.de/produkte/strust_einzelsignaturkarte
- TeleSec signature card
  https://www.telesec.de/tcos/produkte/telesec_signature_card
  Note: Not integrated into the client and not tested
- VR-BankCard FinTS/HBCI
  urn:oid:1.3.6.1.4.1.17696.4.3.1.6.1