Fylgiskjal: Kröfur til öruggs undirskriftarbúnaðar

Fylgiskjal 1 við viðauka B við rammasamning Auðkennis
Fylgiskjal 4 við viðauka A við rammasamning Auðkennis

Fylgiskjal þetta er almennur viðauki annars vegar við samning Auðkennis við fjarskiptafyrirtæki og hins vegar við samning Auðkennis um skráningarstöð Auðkennis, og lýsir þeim kröfum sem gerðar eru til öruggs undirskriftabúnaðar hjá Auðkenni. Skjalið er á ensku þar sem gert er ráð fyrir því að gagnaðilar Auðkennis sendi það út til birgja sinna.

Auðkenni PKI Requirement Specifications for Smart Cards used with Qualified Certificates

Specifications of Auðkenni's requirements for the PKI specifications of smart cards used with qualified certificates and their applicability and interoperability

1. Preface

1.1. Introduction

Auðkenni has been issuing electronic certificates on regular sized smart cards – particularly debit cards – since 2008 and recently also SIM cards.

Currently Auðkenni's CA structure for certificates issued to individuals, is emphasising on qualified certificates for authentication (digital signature) and signing (non-repudiation via qualified signature), with encryption as a possible add-on later.

Each smart card will host at least two private keys. The PKI application on the chip will use one of the keys for authentication, the other for non-repudiation signing. Different PIN policies will possibly apply to different types of smart cards (e.g. two PINs for debit cards, one PIN for SIM cards), but this is subject to change. Support for a two PIN policy is required.

1.2. Purpose and Readers

This document is intended for those who are providing the underlying hardware (smart card chips), operating system and cryptographic functionality as well as those who are developing applications, modules and scripts for Auðkenni's PKI structure.

1.3. Revision notes

Date	Author	Comments
12.06.2007	Sverrir B. Sverrisson	First edition of the document.
17.02.2014	Haraldur Bjarnason	Second edition. Mobile requirements added.
27.03.2014	Elfur Logadóttir	V2.01. Minor editorial changes.
13.06.2014	Elfur Logadóttir	V2.02. ECC requirements and 3DES specification.
11.09.2014	Elfur Logadóttir	V2.03. Minor editorial changes.

1.4. Scope

This document describes Auðkenni's requirements for the PKI functionality of the smart card chips which will be used for the PKI project in Iceland and all other relevant hardware and software components. The requirements have changed as the project has evolved.

1.5. Definitions and abbreviations

EF	Elementary file
FR	Functional Requirement
MUST	Requirement which must be fulfilled
MAY	Requirement which may optionally be fulfilled
APPLICATION	The PKI application running on the card chip (e.g. applet or codelet)
CSP	Cryptographic Service Provider. Middleware/Driver Software running on workstation which interfaces between the workstation and the PKI application stored on the chip. Also referred to as Middleware or Client.

2. General requirements

2.1. The product

FR 2.1.1. The product MUST fulfil the requirements of the relevant Common Criteria Protection Profile of Secure Signature Creation Device (SSCD). Preferably the product has a certification to that effect, however variations of certification can be considered (such as composite certification of different components).

FR 2.1.2. If the product does not have an SSCD certification, it MUST come with a clear statement of the manufacturer that it does fulfil the SSCD requirements that are laid down in Directive 1999/93/EC, Annex III.

FR 2.1.3. The product MUST include a cryptographic module capable of cryptography functionality.

2.2. Algorithm

FR 2.2.1. The application MUST support on-board generation of at least 2048-bit RSA keys and at least 224-bit ECC keys.

FR 2.2.2. The application MUST support signing and decryption using at least 2048-bit RSA keys and at least 224-bit ECC keys.

FR 2.2.3. The application MAY support reading out the public parts of at least 2048-bit RSA keys and at least 224-bit ECC keys. By public parts is meant the modulus and the public exponent.

FR 2.2.4. The private keys on the chip MUST be unreadable and protected in a secure storage.

FR 2.2.5. The chip MUST support hosting up to 10 key pairs.

2.3. Certificates

FR 2.3.1. The chip MUST support hosting up to 5 certificates.

2.4. User PIN

FR 2.4.1. PIN RETRY counter MUST be configurable and support at least 5 retries.

FR 2.4.2. A successful PIN operation MUST reset the PIN retry counter to 0.

PIN policies are further defined in related product policies (chapter 3 and onward).

2.5. Access conditions on private keys

FR 2.5.1. It MUST be possible to protect private key operations, such as signing and decryption, of using different private keys with different user PINs. In other words, it must be possible to set the access condition for a private key operation with an arbitrary key to be the verification of an arbitrary user PIN.

FR 2.5.2. The access conditions MUST be on a per key basis (and optionally in combination with a per operation basis), not on a per operation basis only. In other words, the access condition shall be connected to a specific key and one or more operations which that key can perform, NOT just a key operation in general without any correlation to a key. This is how access conditions in 'CREATE EF' normally works, the access conditions are attached to the EF.

2.6. Access Conditions in General

FR 2.6.1. The application MAY support verification of an arbitrary PIN as access condition on file/object operations (the operation in question is only allowed if the PIN specified in the access condition is verified).

FR 2.6.2. The application MAY support the access condition 'NEVER' on file/object operations (the operation in question is never allowed; no matter what PIN is verified).

FR 2.6.3. If FR2.6.1 or FR2.6.2 are implemented, the access conditions MUST be on a per file/object basis (and optionally in combination with a per operation basis), not on a per operation basis only. In other words, the access condition shall be connected to a specific file/object and one or more operations which that can be perform on/with that object, NOT just an operation in general without any correlation to a specific object. This requirement is a generalization of FR2.6.2.

FR 2.6.4. All cryptographic functions e.g. authentication and non-repudiation signature are to be performed on the chip.

2.7. Standards Compliance and Interoperability Issues

FR 2.7.1. The public key infrastructure for the Icelandic market is to comply with all relevant standards in order to ensure a completely open and interoperable PKI environment. The Project's requirements emphasize the use of industry standards, especially CEN, ETSI and ISO.

FR 2.7.2. Auðkenni also expects card vendor to provide a functional CSP and relevant documentation to allow an in-house implementation of a CSP which can deliver low-level cryptographic commands to the card for personalization, including on-board-key-generation, sending certificate request (e.g. via Web CA Interfaced) and certificate injection.

3. Mobile certificates (SIM cards)

Additional requirements for Mobile certificates (SIM cards).

FR 3.1.1. The product MUST include Audkenni VMAC configuration, to be supplied by Valimo upon request.

FR 3.1.2. The product MUST be UICC compliant with JAVA card 2.2.1 or higher. Global Platform 2.1.1 or higher support.

FR 3.1.3. The VMAC must be installed on a dedicated Security Domain.

FR 3.1.4. The VMAC card application MUST use OTA secure messaging.

FR 3.1.5. The chip MUST have 50k-70k of non-volatile memory available for this service.

FR 3.1.6. The product MUST use at least 3DES algorithm for OTA communication.

FR 3.1.7. The product MAY NOT include DES algorithm for OTA communication.

4. Qualified certificates on regular sized smart cards

Additional requirements for qualified certificates on regular sized smart cards (e.g. debit cards).

FR 4.1.1. The application MUST support secure key injection of two 2048-bit keys. By secure is meant secure encrypted transport of keys during personalization – for example using the following methods:

- Secure Messaging (Global Platform)
- Confidential ALU (Multos)

FR 4.1.2. The chip MUST support hosting up to five certificates.

- Digital signature certificate
- Non-repudiation certificate
- Root certificate
- Two intermediate CA certificates.

4.2. Unblock PIN (PUK)

FR 4.2.1. The application MAY support PIN unblocking in one single APDU (like 'RESET RETRY COUNTER' with P1 = 0x00 from ISO 7816-8).

FR 4.2.2. One PUK MUST be used to unblock both PINs.

FR 4.2.3. PUK MUST be numerical and length 12.

FR 4.2.4. PUK retry MUST be set to 10 times. Exceeding maximum tries the card is permanently blocked by PKI application

FR 4.2.5. A successful PUK operation MUST reset the PUK retry counter to 0.

4.3. User PIN

FR 4.3.1. The PKI application MUST support at least two different user PINs both of which MUST be unblocked by the same unblocking code (PUK).

FR 4.3.2. One PIN MUST be for authentication (digital signature) and MUST allow digits only. The length of the authentication PIN MUST be 4 characters.

FR 4.3.3. One PIN MUST be for non-repudiation and MUST allow digits only. The length of the non-repudiation PIN MUST be 6 characters.