SVENSK STANDARD
SS 614332:2011

Fastställd/Approved: 2011-12-13
Publicerad/Published: 2011-12-23
Utgåva/Edition: 3
Språk/Language: engelska/English
ICS: 03.060; 35.240.15

Identifieringskort – Elektroniskt ID-kort – Svensk profil

Identification cards – Electronic ID card – Swedish profile

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Denna standard ersätter SS 614332, utgåva 2. och har kompletterats med profilinformation som saknas i SS-ISO/IEC 7816-15:2004, men som tidigare fanns i den nu upphävda standarden SS 614330, utg 2.

This standard supersedes the Swedish Standard SS 614332, edition 2. Profile information, which was included in the withdrawn standard SS 614330 edition 2, but not in SS-ISO/IEC 7816-15:2004, has been added.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Standarden är framtagen av kommittén för Identifieringskort, SIS/TK 448.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Contents

Page

Introduction

Microprocessor-based integrated circuit cards (often called smart cards) with cryptographic functions can be used for secure identification of users of information systems as well as for other core security services such as non-repudiation with digital signatures and distribution of encryption keys for confidentiality. The objective of this Standard is to provide a specification of an IC-card integrated circuit application for such services based on available international standards. A main goal has been to provide a solution that may be used in large-scale systems with several issuers of compatible cards, primarily in a national context but also providing for international interchange. Therefore a number of data structures have been provided to support a public key certificate infrastructure and flexible management of PIN codes.

Integrated Circuit Cards are intrinsically secure computing platforms ideally suited to providing enhanced security and privacy functionality to applications. They can handle authentication information such as digital certificates and capabilities, authorizations and cryptographic keys. Furthermore, they are capable of providing secure storage and computational facilities for sensitive information such as:

— Private keys and key fragments;

— Account numbers and stored value;

— Passwords and shared secrets; and

— Authorizations and permissions.

At the same time, many of these cards provide an isolated processing facility capable of using this information without exposing it within the host environment where it is at potential risk from hostile code (viruses, Trojan horses, and so on). This becomes critically important for certain operations such as:

— Generation of digital signatures, using private keys, for personal identification;

— Network authentication based on shared secrets;

— Maintenance of electronic representations of value; and

— Portable permissions for use in off-line situations.

The objectives of this Standard are therefore to:

— Enable interoperability among components running on various platforms (platform neutral);

— Enable applications to take advantage of products and components from multiple manufacturers (vendor neutral);

— Enable the use of advances in technology without rewriting application-level software (application neutral); and

— Maintain consistency with existing, related standards while expanding upon them only where necessary and practical.

As a practical example, the holder of a card containing a digital certificate should be able to present the card to any application running on any host and successfully use the card to present the contained certificate to the application. As a first step to achieve these objectives, this Standard specifies a file and directory format for storing security-related information on cards. It has the following characteristics:

— Dynamic structure enables implementations of several types of identity cards.

— Supports storage of any type of objects (keys, certificates and data); and

— Support for multiple PINs.

In general, an attempt has been made to be flexible enough to allow for many different card types, while still preserving the requirements for interoperability. A key factor for this in the case of IC cards is the notion of ”Directory Files”, which provides a layer of indirection between objects on the card and the actual format of these objects.

There are some implementation guidelines for software developers in Annex B, which is informative.

1 Scope

This Standard specifies a cryptographic token information application for use in cards compatible with ISO 7816-4, -5, -6, -8 and -15.

This Standard does not cover the internal implementation within the card.

The electronic identity application contains provisions for several cryptographic algorithms, the choice of which may affect exportability for a certain implementation. The evaluation of the suitability for these algorithms is outside the scope of this Standard. It shall not be mandatory for cards complying with this Standard to support all algorithms or options described herein.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-5, *Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers*

SS-ISO/IEC 7816-15:2004, *Information Technology — Identification Cards — Integrated Circuit(s) cards with contacts — Part 15: Cryptographic information application*

ISO/IEC 9594-8:1997, *ITU-T Recommendation X.509 (1997*), Information technology — Open Systems Interconnection — The Directory: Authentication framework

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
application
data structure, data elements and program modules needed for a specific functionality to be satisfied

[ISO/IEC 7816-9:1999]

3.2
application identifier
data element that identifies an application in a card

NOTE Adapted from SS-ISO/IEC 7816-15:2004.

3.3
authentication object directory
optional elementary file containing information about authentication objects known to the CTIA

3.4
card holder
person to whom the card was issued

[SS-ISO/IEC 7816-15:2004]

3.5
card issuer
organization or entity that issues smart cards and card applications

NOTE Adapted from [ISO/IEC 7816-15:2004].

3.6
command
message that initiates an action and solicits a response from the card

[SS-ISO/IEC 7816-15:2004]

3.7
cryptographic token
portable device capable of storing cryptographic credentials such as cryptographic keys and digital certificates

3.8
dedicated file
file containing file control information, and, optionally, memory available for allocation, and which may be the parent of elementary files and/or other dedicated files

NOTE Adapted from ISO/IEC 7816-4:2005.

3.9
directory file
DIR file
optional elementary file containing a list of applications supported by the card and optional related data elements

NOTE Adapted from ISO/IEC 7816-4:2005.

3.10
elementary file
set of data units or records sharing the same file identifier, and which cannot be a parent of another file

NOTE Adapted from ISO/IEC 7816-4:2005.

3.11
file identifier
2-byte binary value used to address a file on a smart card

NOTE Adapted from ISO/IEC 7816-4:2005.

3.12
function
process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction

NOTE Adapted from SS-ISO/IEC 7816-15:2004.

3.13
message
string of bytes transmitted by the interface device to the card or vice versa, excluding transmission-oriented characters

[SS-ISO/IEC 7816-15:2004]

3.14
object directory file
mandatory elementary file containing information about other directory files in the CIA

3.15
password
data that may be required by the application to be presented to the card by its user for authentication purpose

3.16
path
concatenation of file identifiers without delimitation

[ISO/IEC 7816-4:2005]

NOTE 1 If the path starts with the MF identifier (0x3F00), it is an absolute path; otherwise it is a relative path. A relative path shall start with the identifier '0x3FFF' or with the identifier of the current DF.

3.17
personal identification number
PIN
typically a 4 to 8 digit number entered by the card holder to verify that the card holder is authorized to use the card

3.18
record
string of bytes which can be handled as a whole by the card and referenced by a record number or by a record identifier

[ISO/IEC 7816-4:1995]

4 IC-card requirements

The card shall have at least the following attributes:

— two RSA keys, one for non-repudiation use, and the other for all other use;

— two PIN-codes: one PIN for the card, and one for the RSA-key used for nonRepudiation.

5 EID application functionality

5.1 Private RSA keys

The EID application shall contain two private RSA keys as specified in Table 1.

Table 1 — Private RSA keys

Private key number	RFC 5280 key usage	Public exponent
1	DigitalSignature + keyEnciphennent + dataEnci-phennent	65537 (F4)
2	nonRepudiation	3

5.2 Card holder certificates

The following card holder certificates shall be stored into the EID application, see Table 2.

Table 2 — Card holder certificates

Corresponding user private key number	RFC 5280 key usage
1	DigitalSignature + keyEnciphennent + dataEnci-phennent
2	nonRepudiation

End entity certificates are described in SS 614331.

5.3 EID application

Because multi-application smart cards contain multiple independent applications, EID application shall be selected before further card access. When smart card reset occurs, EID application might not be the default smart card application.

The EID application is selected using following Application Identifier (AID):

```
E8 28 BD 08 0F 00 50 4B 43 53 2D 31 35
```

For backwards compatibly, existing application may use the old AID:

```
AO 00 00 00 63 50 4B 43 53 2D 31 35
```

It is recommended that the first AID be used, for future compatibility.

NOTE The Swedish National ID Card (NIDEL) uses the old OID for backward compatibility reasons.

Application selection resets also PIN -codes verification status.

6 EID object classes

Any number of 'FF' octets should, if used, occur before, between or after the values of these objects without any meaning (i.e. as padding for unused space or deleted values).

This document defines four general classes of objects (see SS-ISO/IEC 7816-15 for additional information):

— Key information objects;

— Certificate information objects;

— Data container information objects;

— Authentication information objects.

All these object classes have sub-classes, e.g. Private Key Information is a sub-class of the Key Information Object. Objects can be private, meaning that they are protected against unauthorized access, or public. In EID application, access to private objects is defined by Access Conditions. Conditional access is usually achieved with PINs. Public objects are not protected from read-access.