STANDARDISERINGEN I SVERIGE
SWEDISH INSTITUTE FOR STANDARDS

SWEDISH STANDARD SS 61 43 32

Handläggande organ/Standardizing body	Fastställd/Approved	Utgåva/Edition	Sida/Page
ITS Information Technology Standardization	1998-09-14	1	1 (4)

Identification Cards – Electronic ID Card – Swedish Profile

Identifieringskort – Elektroniskt ID-kort – Svensk profil

0 Foreword

This specification is based on developments within the framework of the Swedish SEIS organisation.

1 Scope

This standard specifies a Swedish Profile for an Electronic ID (EID) Application with keys and certificates on microprocessor cards issued to physical persons and intended for general purpose security functions and for inter-sector use.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

SS 61 43 30	Identification Cards – Electronic ID Application
SS 61 43 31	Identification Cards – Electronic ID Certificate
SS 61 43 14, utgåva 6	Identifieringskort – Identitetskort av typ ID-1
SBC 151	Särskilda bestämmelser för certifiering av identitetskort

ICS 03.060.00

Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.
Postadress: SIS, Box 6455, 113 82 STOCKHOLM
Telefon: 08 - 610 30 00. *Telefax*: 08 - 30 77 57

Upplysningar om **sakinnehållet** i standarden lämnas av ITS.
Telefon: 08 - 793 90 00. *Telefax*: 08 - 751 53 63
E-post: info@its.se
Prisgrupp G
Tryckt i februari 1999

3 Definitions and abbreviations

3.1 Definitions

3.1.1 authentication: The process of corroborating a claimed identity.

3.1.2 certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.

3.1.3 digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of that data to prove the source and integrity of the data unit. It protects against forgery, even by the recipient.

3.1.4 electronic ID-card (EID card): IC card with private keys, certificates and other information, to be used for secure identification of users of information systems and other basic security services such as authentication and non-repudiation with digital signatures and distribution of encryption keys for confidentiality.

3.1.5 identification: The process of confirming the identity of a person or an object

3.2 Abbreviations

AUF Application Usage File

CIF Certificate Index File

EID Electronic Identification

PIN Personal Identification Number

RSA Rivest, Shamir, Adleman

SEIS Secure Electronic Information in Society

URL Uniform Resource Locator

4 Card requirements

4.1 EID application

The specification SS 61 43 30 ”Identification cards – Electronic ID Application” shall be used in this profile. The requirements specified below in this implementation profile give further details on certain optional elements of that standard.

4.2 Visual identification data of card surface

An identification card following this profile shall contain visual identification data as specified by SS 61 43 14. The issuing of an identification card following this implementation profile shall follow the provisions of SBC 151 as regards the visual data on the surface.

4.3 RSA keys

4.3.1 Key usage

The EID Application directory shall contain three separate and unique private RSA keys for the following purposes:

Key Usage
Digital Signature (Authentication)
Key encipherment
Non-repudiation

4.3.2 Key modulus length

The modulus length of the three keys shall be as follows:

Key Usage	Key length (bits)
Digital Signature (Authentication)	1024
Key encipherment	1024
Non-repudiation	1024

4.4 PIN functions

An EID card contains a number of PIN codes. The functions of these are specified in this section.

4.4.1 Issuer verification

Issuer verification is a function that often is used in card to enable the issuer to perform administrative functions in the card. An issuer verification may under no circumstances enable the use of or any kind of manipulation of the private RSA keys or user PIN codes stored in the EID card. The verification of the issuer – for functions at the discretion of the issuer – may use a secret code (Issuer PIN) or a management key with a challenge response method (algorithm to be defined by the issuer).

4.4.2 User Master PIN

The EID card shall contain a User Master PIN located in the Master File directory. This User Master PIN shall be referred to as PIN number 1, and shall be used to protect private keys in the EID application as defined in the next section.

The User Master PIN may also be used by other, non-EID, applications on the card, at the discretion of the application provider.

4.4.3 User PIN codes

Any use of the private RSA keys in the card shall be preceded by user PIN verification. There are two user PIN codes in the card that control the three keys.

Key Usage	User PIN
Digital Signature (Authentication)	1
Key encipherment	1
Non-repudiation	2

Any positive verification of one PIN code shall not enable the use of security services associated with another PIN code.

Three consecutive and incorrect verifications of a certain user PIN code shall block all security services associated with that PIN code.

The length and character set of the PIN code shall be described in the issuer's certificate policy declaration.

Note: It is technically possible that both PIN codes from a user point of view are set to the same value.

4.4.4 PIN unblocking

When a PIN is blocked through three consecutive incorrect PIN verifications, the PIN may only be unblocked through a special unblocking procedure, defined in the issuer's policy declaration.