



National Standards Authority of Ireland

STANDARD

I.S. CWA 14890-2:2004

ICS 35.240.15

**APPLICATION INTERFACE FOR SMART
CARDS USED AS SECURE SIGNATURE
CREATION DEVICES - PART 2: ADDITIONAL
SERVICES**

National Standards
Authority of Ireland
Dublin 9
Ireland

Tel: (01) 807 3800
Fax: (01) 807 3838

*This Irish Standard was
published under the
authority of the National
Standards Authority of
Ireland
and comes into effect on:
July 23, 2004*

**NO COPYING WITHOUT NSAI
PERMISSION EXCEPT AS
PERMITTED BY COPYRIGHT
LAW**

© NSAI 2004

Price Code R

Údarás um Chaighdeán Náisiúnta na hÉireann

CEN

CWA 14890-2

WORKSHOP

May 2004

AGREEMENT

ICS 35.240.15

English version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Table of Contents

Foreword	4
1 Scope	5
3 Abbreviations and notation	10
3.1 Abbreviations.	10
4 Definitions	11
5 Additional Service Selection	12
6 Client/Server Authentication	14
6.1 Client/Server protocols	14
6.2 Steps preceeding the client/server authentication	15
6.3 Padding format	15
6.4 Execution flow	16
7 Encryption Key Decipherment	20
7.1 Steps preceeding the key decryption	21
7.2 Key Management with RSA	21
7.3 Diffie-Hellman key exchange.	23
7.4 Algorithm Identifier for DECIPHER	26
8 Signature verification	27
8.1 Signature verification execution flow	27
9 Certificates for additional services	30
9.1 File structure	31
9.2 EF.C.CH.AUT	31
9.3 EF.C.CH.KE.	31
9.4 Reading Certificates and the public key of CAs	32
10 APDU data structures	33
10.1 Algorithm Identifiers	33
10.2 CRTs	33
Annex A. Security Service Descriptor Templates (normative)	36
A.1 Security Service Descriptor Concept	36
A.2 SSD Data Objects.	37
A.3 Location of the SSD templates	40
A.4 Examples for SSD templates	40
Annex B. (informative) Security environments	42
B.1 Definition of CRTs (examples)	43
B.2 Security Environments (example)	49
B.3 Definition of File Control Information Templates (example)	50
Annex C. Interoperability aspects (informative)	55
C.1 Choosing device authentication	55
C.2 Choosing User verification method.	57
Annex D. Example of DF.CIA	58

Foreword

This document is part of a series of standards for secure signature creation devices (SSCDs), developed to support the EU-directive on electronic signatures. It is dedicated to smart cards as an important representation of SSCDs (e.g. SIMs, USB tokens). The key issue of this document is to enable interoperability, so that smart cards from different manufacturers can interact with different kind of signature creation applications. The specification is applicable to smart cards supporting file system oriented applications as well as for smart cards supporting object oriented applications (e.g. Java applets).

This standard consists of two parts

- Part1 - “Basic Requirements” describes the mandatory specifications for an SSCD to be used in compliance with the ESIGN-G1 and F specifications.
- Part 2 - “Optional Features” describes additional features relevant for use with SSCDs.

The error handling of commands is out of scope of this document.

This is the second volume of the ESIGN specification for the Application Interface for smart cards used as Secure Signature Creation Device. It contains the specification of additional services, which are not required for the generation of a digital signature. They are, however, frequently used and typical in the context of digital signature applications.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-