This is a free page sample. Access the full version online.

National Standards Authority of Ireland

IRISH STANDARD

**I.S. CWA 15264-1:2005**

ICS 35.240.15

National Standards
Authority of Ireland
Glasnevin, Dublin 9
Ireland

Tel: +353 1 807 3800
Fax: +353 1 807 3838
http://www.nsai.ie

**Sales**
http://www.standards.ie

# ARCHITECTURE FOR A EUROPEAN INTEROPERABLE EID SYSTEM WITHIN A SMART CARD INFRASTRUCTURE

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

*June 22, 2005*

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

**© NSAI 2005**

**Price Code R**

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

This is a free page sample. Access the full version online.

# CEN

# WORKSHOP

# AGREEMENT

**CWA 15264-1**

April 2005

**ICS** 35.240.15

English version

# Architecture for a European interoperable eID system within a smart card infrastructure

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**

© 2005 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 15264-1:2005 E

This is a free page sample. Access the full version online.



Table of Content

Foreword ....4
1 Introduction ....5
1.1 Scope and objectives ....5
1.2 Informative References ....5
1.3 Concepts and definitions ....6
1.4 Abbreviation ....12
2 Contextual Model for IAS interoperability ....17
2.1 Trust models ....17
2.2 Interoperability of IAS between schemes ....18
3 Conceptual model for IAS interoperability ....18
3.1 Roles ....19
3.2 Processes ....21
3.3 SCMF and generic trust model ....24
3.4 Smart card communities and eService communities ....24
4 The IAS functional model ....25
4.1 The IAS platform function ....25
4.2 The platform function ....26
4.3 The crypto function ....26
4.4 The application function ....26
4.5 The connectivity function ....26
4.6 The Human Interface function ....26
5 IAS system architecture ....27
5.1 The Smart Card layer ....27
5.2 The Infrastructure layer ....27
5.2 The eService layer ....28
5.4 The layer interfaces ....28
6 The functional model in the IAS system architecture ....29
6.1 The functional model in the Smart Card Layer ....30
6.2 The functional model in the User Access Point sub-layer ....31
6.3 The functional model in the eService Access Point sub-layer ....31
6.4 The functional model in the eService Layer ....31
6.5 The functional model in the PKI service sub-layer ....32
7 High level description of the primary processes - formal description ....32
7.1 UC 1.0.: Card activation ....32
7.2 UC.1.1.: Securing of the terminal-card link ....33
7.3 UC.1.2.: Component Authentication ....33
7.4 UC.N.3.: Certificate validation ....34
7.5 UC.2.0.: Connection to eService ....35

This is a free page sample. Access the full version online.



**7.6 UC.2.1.: Securing of the eService link ..... 35**
**7.7 UC.2.2.: Cardholder authentication by PKI ..... 36**
**7.8 UC.3.2.: Cardholder authentication by PIN/BioCode ..... 36**
**7.9 UC.3.0.: Interaction with the eService ..... 37**
**7.10 UC.3.1.: Signing of a data object ..... 37**
**7.11 UC.4.0.: Closing of the eService Connection ..... 38**
**7.12 UC.5.0.: Card deactivation ..... 38**
**8 IAS interoperability ..... 39**
**8.1 IAS interoperability scenarios ..... 39**
**8.2 IAS Interoperability architecture ..... 39**
**8.3 IAS interoperability processes ..... 45**
**9 Securing interoperability ..... 45**
**9.1 Introduction ..... 45**
**9.2 Securing the Card-Terminal interface (IOP#1) ..... 45**
**9.3 Securing the User Access Point - eService Access Point link (IOP#2) ..... 46**
**9.4 Securing the access to PKI services (IOP#3) ..... 46**
**9.5 Securing the eService Access Point - eService link (IOP#4) ..... 46**
**9.6 Securing the on-card applications – IAS function interface (IOP#5) ..... 46**
**10 Common requirements for IAS interoperability ..... 48**
**10.1 Requirements related to the execution of the primary processes ..... 48**
**10.2 Requirements on secondary processes ..... 55**
**Annex A Mandatory field in certificates ..... 59**

**Table of Figures**

Figure 1: Towards a smart card infrastructure based on a common eID ..... 5
Figure 2: Simple 3-entity Trust model ..... 17
Figure 3: 4-entity Trust model ..... 17
Figure 4: Role modelling ..... 20
Figure 5: eAuthentication primary process high-level use cases ..... 22
Figure 6: Generic trust model ..... 24
Figure 7: The trust model in the SCMF ..... 24
Figure 8: Interoperability of IAS services ..... 24
Figure 9: The functional box model ..... 25
Figure 10: Smart card information system architecture ..... 27
Figure 11: eAuthentication system architecture ..... 28
Figure 12: The functional model in the IAS system architecture ..... 30
Figure 13: Primary processes model ..... 32
Figure 14: The Card Activation use case (UC 1.0.) ..... 32
Figure 15: The Connection to eService use case ..... 35
Figure 16: The interaction with the eService use case ..... 37
Figure 17: Summary of interoperability scenarios and levels ..... 39
Figure 18: eService IOP ..... 40
Figure 19: Card IOP - case 1 ..... 41
Figure 20: Card IOP - case 2 ..... 42
Figure 21: Card IOP - case 3 ..... 42
Figure 22: On-card IOP - case 1 ..... 43
Figure 23: On-card IOP - case 2 ..... 43
Figure 24: On-card IOP - case 3 ..... 44

This is a free page sample. Access the full version online.



## Foreword

The production of this CWA (CEN Workshop Agreement) was formally accepted at the e-authentication Workshop's kick-off meeting on 2003-09-16.

The document has been developed through the collaboration of a number of contributing partners in WS-e-authentication, representing smart card interests.

This CWA has received the support of representatives of each of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

This CWA consists of the following parts, under the general title CWA 15264*:*

- *Part 1: Architecture for a European interoperable eID system within a smart card infrastructure*
- *Part 2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services*
- *Part 3: User Requirements for a European interoperable eID system within a smart card infrastructure*

SAI GLOBAL

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