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

National Standards Authority of Ireland

STANDARD

I.S. CWA 14170:2004

ICS 03.160
35.040

National Standards
Authority of Ireland
Dublin 9
Ireland

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

SECURITY REQUIREMENTS FOR SIGNATURE CREATION APPLICATIONS

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 S

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 14170

May 2004

ICS 03.160; 35.040

Supersedes CWA 14170:2001

English version

Security requirements for signature creation applications

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

© 2004 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

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

Contents

Contents 2

Foreword 5

Introduction 6

1. Scope 7

2. References 8

3. Definitions 9

4. Abbreviations 11

5. Signature Creation Functional Model 12
5.1 Signature Creation Objectives 12
5.2 Model 12
5.3 Signature Creation Applications 14
5.4 Secure Signature Creation Devices 15
5.5 Signature Creation Application Instantiation 16
5.6 Control and possession of Signature Creation Systems 16

6. Signed Data Object Information Model 17
6.1 Signer’s Document (SD) 17
6.2 Signature Attributes 18
6.3 Data To Be Signed (DTBS) 18
6.4 Data To Be Signed (Formatted) (DTBSF) 19
6.5 Data To Be Signed Representation (DTBSR) 19
6.6 Advanced Electronic Signature 19
6.7 Qualified Electronic Signature 19
6.8 Signed Data Object 19
6.9 Signer’s Authentication Data (not shown) 19

7. Overall Security Requirements of the SCA 20
7.1 Introduction 20
7.2 Trusted Path 20
7.2.1 Basic Trusted Path Requirement 20
7.2.2 Requirements for Public SCA 20
7.2.3 Referencing the correct SD and Signature Attributes 20
7.3 Requirements for Distributed Signature Creation Applications 21
7.4 Requirements resulting from un-trusted processes and communications ports 21
7.5 Post signature verification of the Signed Data Object 22
7.6 Requirements of the DTBS 22

8. SD Presentation Component (SDP) 23
8.1 Purpose 23
8.2 Background 23
8.3 Data Content Type Requirements 24
8.4 SD Non-ambiguity Requirements 25
8.5 Requirements for Presentation Insensitive SDs 25
8.6 Hidden Text and Active Code Requirements 25

9. Signature Attribute Viewer (SAV) 27

10. Signer Interaction Component (SIC) 29
10.1 High level user interface principles 29
10.2 Signature Invocation 29
10.3 Signature process inactivity timeout 30
10.4 Signer Control Functions 30
10.5 Retrieval of Signer’s Characteristics 30
10.6 User Interface Aspects 31

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

11. Signer's Authentication Component (SAC) ... 32
11.1 General Aspects ... 32
11.2 Obtaining the Signer’s Authentication Data ... 32
11.3 Knowledge based Signer Authentication ... 33
11.4 Biometric Signer Authentication ... 33
11.5 Provision of the wrong Signer's Authentication Data ... 34
11.6 Change of Signer's Authentication Data and Reset of the Retry Counter ... 34
11.7 Signer’s Authentication Data User Interface Aspects ... 34
11.8 Security Requirements for the SAC Component ... 34

12. Data To Be Signed Formatter (DTBSF) ... 37
12.1 Functions of the DTBSF component ... 37
12.2 Security Requirements for the DTBSF component ... 37

13. Data Hashing Component (DHC) ... 38
13.1 Functions of the DHC Component ... 38
13.2 Production of the DTBS Representation ... 38
13.3 Formatting of the electronic signature input ... 39
13.4 Security Requirements for the DHC Component ... 40

14. SCDev /SCA Communicator (SSC) ... 41
14.1 Interaction Sequences ... 41
14.2 Establishing the Physical Communication ... 42
14.3 Retrieval of SCDev Token Information ... 42
14.4 Selection of the SCDev functionality on a multi-application platform ... 44
14.5 Retrieval of Certificates ... 44
14.6 Selection of Signature Creation Data ... 44
14.7 Performing Signer Authentication ... 44
14.8 Digital Signature Computation ... 45
14.9 Signature Logging ... 45
14.10 Security requirements for the SSC Component ... 45

15. SCD/SCA Authenticator (SSA) ... 46
15.1 SCA - SCDev Authentication for SCA under service provider’s control ... 46
15.2 Security Requirements for the SSA Component ... 47

16. SD Composer (SDC) ... 48
16.1 Security Requirements for the SDC Component ... 48

17. Signed Data Object Composer (SDOC) ... 49

18. External Interface for Input/Output ... 50
18.1 Risks to the SCA ... 50
18.2 Import of Certificates ... 50
18.3 Import of an SD and Signature Attributes ... 50
18.4 Download of SCA Components ... 50
18.5 Security Requirements for Input Control ... 51

Annex A (Informative) – General Recommendations ... 52
A.1 Operation of the Signature Creation Application ... 52
A.2 Requirement on the environment. ... 53
A.3 Presentation insensitive SD ... 53

Annex B Guidance to implement a User Interface ... 54
B.1 Purpose ... 54
B.2 User interface consistency ... 54
B.3 Use of colour ... 54
B.4 Feedback ... 54
B.5 Security Breach detection ... 55
B.6 Invalid choice ... 55
B.7 Preservation of information presentation ... 55
B.8 Personalisation ... 55
B.9 Signer's Control when integrating with user profiling techniques ... 55
B.10 Configure /Edit Signature Creation process ... 55
B.11 Distinguishing between certificates ... 55

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

B.12 Timing of operations ... 56
B.13 Security of terminals in public domain ... 56
B.14 User retention of secrets ... 56
B.15 User instructions ... 56
B.16 Presentation of operational sequence ... 56
B.17 Presentation of distinguishable parts ... 57
B.18 Guidance ... 57
B.19 Terminology ... 57
B.20 Error tolerance ... 57
B.21 Informative error messages ... 57
B.22 Single handed operation of public SCAs ... 57
B.23 Cancellation of operation ... 57
B.24 Undo operation ... 58
B.25 Signer's Authentication Component (SAC) ... 58
B.25.1 Choice of signer authentication method ... 58
B.25.2 Biometric signer authentication ... 58

Annex C Signature Logging Component (SLC) ... 60

Annex D (Informative) - SCDev Holder Indicator (SHI) ... 61

Annex E (Informative) - References ... 62

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