



National Standards Authority of Ireland

IRISH STANDARD

I.S. CWA 14174-5:2004

ICS 35.240.15

National Standards
Authority of Ireland
Dublin 9
Ireland

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

**FINANCIAL TRANSACTIONAL IC CARD
READER (FINREAD) - PART 5: DOWNLOAD
FILE FORMAT**

*This Irish Standard was
published under the
authority of the National
Standards Authority of
Ireland
and comes into effect on:
December 17, 2004*

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

© NSAI 2004

Price Code J

Údarás um Chaighdeáin Náisiúnta na hÉireann

CEN

CWA 14174-5

WORKSHOP

October 2004

AGREEMENT

ICS 35.240.15

Supersedes CWA 14174-5:2004

English version

Financial transactional IC card reader (FINREAD) - Part 5: Download file format

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

CWA 14174-5:2004 (E)

Contents

1 Scope 5

2 Normative references 5

2.1 Definitions 6

2.2 Abbreviations 6

3 FINREAD Certificate Architecture 7

3.1 Why Use X.509v3 7

3.2 FINREAD Scheme within a CA infrastructure 7

3.3 Root Certificate profile 9

3.4 Certificate Path Validation 11

4 Format of signature on download packages 13

5 Types of Download Packages and their ASN.1 definition 16

5.1 ASN.1 structure of ContentInfo 17

Annex A P-AK (FINREAD Root Certificate) 19

Annex B AK level 1 CA Certificate 21

Annex C AK level 2 CA Certificate 23

Annex D FCRA/FCRIA Signer Public Key Certificate 25

Annex E FCR P-Auth_k Certificate 26

Annex F P-CK and P-MK certificates 27

Annex G Approach to Encryption 28

FIGURES

Figure 1 - FCR keys 8
Figure 2 - FINREAD Scheme within a four level CA Infrastructure 8
Figure 3 – Manufacturer generates certificates for its FCRs 9
Figure 4 - FCRA/FCRIA Signer Public Key Certificate Process 9
Figure 5 – Signed applet and certificate Path..... 12

List of tables

Table 1 - Mandatory Certificate Fields..... 10
Table 2 - Certificate extensions as used in FINREAD certificates..... 11
Table 3 - PKCS#7 SignedData Format 15
Table 4 - Data Items to be included in Download Packages 16
Table 5 - AK Root Certificate 19
Table 6 – AK level 1 CA Certificate 21
Table 7 – AK level 2 CA Certificate 23
Table 8 – FCRA/FCRIA Signer Public Key Certificate 25
Table 9 – FCR Certificate 26
Table 10 – P-CK and P-MK Certificate Profile 27

CWA 14174-5:2004 (E)

Foreword

The production of this CWA (CEN Workshop Agreement) specifying a financial transactional IC card reader (FINREAD) was formally accepted at the FINREAD Workshop's kick-off meeting on 1999-09-08 and published on 2001.

This revised document was approved as CWA at a meeting of the WS-FINREAD participants on 2003-10-30, after a final review/endorsement round. The final text was submitted to CEN for publication on 2003-11-10.

This revised version (mainly editorial changes and lay-out issues) was submitted to CEN for publication on 2004-06-14.

This document supersedes CWA 14174-5:2004.

The document has been developed through the collaboration of a number of contributing partners in WS-FINREAD, representing smart card interests as well as financial services.

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 CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN Management Centre.

This CWA consists of the following parts, under the general title *Financial transactional IC card reader (FINREAD)*:

- Part 1 : *Business requirements*
- Part 2 : *Functional requirements*
- Part 3 : *Security requirements*
- Part 4 : *Architectural overview*
- Part 5 : *Download file format*
- Part 6 : *Definition of the virtual machine*
- Part 7 : *FINREAD card reader application programming interfaces (APIs)*
- Part 8 : *FINREAD client application programming interfaces (APIs)*

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](#)
-