



NSAI
Standards

Irish Standard Recommendation
S.R. CWA 16926-65:2015

Extensions for Financial Services (XFS)
interface specification Release 3.30 - Part 65:
PIN Keypad Device Class Interface - Migration
from Version 3.20 (CWA 16374) to Version
3.30 (this CWA) - Programmer's Reference

S.R. CWA 16926-65:2015

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

CWA 16926-65:2015

Published:

2015-08-12

This document was published under the authority of the NSAI and comes into effect on:

2015-08-29

ICS number:

35.200

35.240.15

35.240.40

NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

S.R. CWA 16926-65:2015 is the adopted Irish version of the European Document CWA 16926-65:2015, Extensions for Financial Services (XFS) interface specification Release 3.30 - Part 65: PIN Keypad Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

CEN

CWA 16926-65

WORKSHOP

August 2015

AGREEMENT

ICS 35.240.40; 35.240.15; 35.200

English version

**Extensions for Financial Services (XFS) interface specification
Release 3.30 - Part 65: PIN Keypad Device Class Interface -
Migration from Version 3.20 (CWA 16374) to Version 3.30 (this
CWA) - Programmer's Reference**

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-CENELEC 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, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Table of Contents

European foreword.....	6
1. Migration Information.....	9
2. PIN Keypad.....	10
2.1 Encrypting Touch Screen (ETS).....	12
3. References.....	15
4. Info Commands.....	17
4.1 WFS_INF_PIN_STATUS.....	17
4.2 WFS_INF_PIN_CAPABILITIES.....	21
4.3 WFS_INF_PIN_KEY_DETAIL.....	33
4.4 WFS_INF_PIN_FUNCKEY_DETAIL.....	35
4.5 WFS_INF_PIN_HSM_TDATA.....	38
4.6 WFS_INF_PIN_KEY_DETAIL_EX.....	39
4.7 WFS_INF_PIN_SECUREKEY_DETAIL.....	42
4.8 WFS_INF_PIN_QUERY_LOGICAL_HSM_DETAIL.....	46
4.9 WFS_INF_PIN_QUERY_PCPTS_DEVICE_ID.....	47
4.10 WFS_INF_PIN_GET_LAYOUT.....	48
5. Execute Commands.....	51
5.1 Normal PIN Commands.....	51
5.1.1 WFS_CMD_PIN_CRYPT.....	51
5.1.2 WFS_CMD_PIN_IMPORT_KEY.....	54
5.1.3 WFS_CMD_PIN_DERIVE_KEY.....	57
5.1.4 WFS_CMD_PIN_GET_PIN.....	59
5.1.5 WFS_CMD_PIN_LOCAL_DES.....	62
5.1.6 WFS_CMD_PIN_CREATE_OFFSET.....	64
5.1.7 WFS_CMD_PIN_LOCAL_EUROCHEQUE.....	66
5.1.8 WFS_CMD_PIN_LOCAL_VISA.....	68
5.1.9 WFS_CMD_PIN_PRESENT_IDC.....	70
5.1.10 WFS_CMD_PIN_GET_PINBLOCK.....	72
5.1.11 WFS_CMD_PIN_GET_DATA.....	74
5.1.12 WFS_CMD_PIN_INITIALIZATION.....	77
5.1.13 WFS_CMD_PIN_LOCAL_BANKSYS.....	79
5.1.14 WFS_CMD_PIN_BANKSYS_IO.....	80
5.1.15 WFS_CMD_PIN_RESET.....	81
5.1.16 WFS_CMD_PIN_HSM_SET_TDATA.....	82
5.1.17 WFS_CMD_PIN_SECURE_MSG_SEND.....	84
5.1.18 WFS_CMD_PIN_SECURE_MSG_RECEIVE.....	86
5.1.19 WFS_CMD_PIN_GET_JOURNAL.....	88
5.1.20 WFS_CMD_PIN_IMPORT_KEY_EX.....	89
5.1.21 WFS_CMD_PIN_ENC_IO.....	92
5.1.22 WFS_CMD_PIN_HSM_INIT.....	94
5.1.23 WFS_CMD_PIN_SECUREKEY_ENTRY.....	95
5.1.24 WFS_CMD_PIN_GENERATE_KCV.....	98
5.1.25 WFS_CMD_PIN_SET_GUIDANCE_LIGHT.....	99
5.1.26 WFS_CMD_PIN_MAINTAIN_PIN.....	101
5.1.27 WFS_CMD_PIN_KEYPRESS_BEEP.....	102
5.1.28 WFS_CMD_PIN_SET_PINBLOCK_DATA.....	103
5.1.29 WFS_CMD_PIN_SET_LOGICAL_HSM.....	104

5.1.30	WFS_CMD_PIN_IMPORT_KEYBLOCK	106
5.1.31	WFS_CMD_PIN_POWER_SAVE_CONTROL	107
5.1.32	WFS_CMD_PIN_DEFINE_LAYOUT	108
5.1.33	WFS_CMD_PIN_START_AUTHENTICATE	111
5.1.34	WFS_CMD_PIN_AUTHENTICATE	113
5.1.35	WFS_CMD_PIN_GET_PINBLOCK_EX	116
5.1.36	WFS_CMD_PIN_SYNCHRONIZE_COMMAND	118
5.2	Common commands for Remote Key Loading Schemes	119
5.2.1	WFS_CMD_PIN_START_KEY_EXCHANGE	119
5.3	Remote Key Loading Using Signatures	120
5.3.1	WFS_CMD_PIN_IMPORT_RSA_PUBLIC_KEY	120
5.3.2	WFS_CMD_PIN_EXPORT_RSA_ISSUER_SIGNED_ITEM	123
5.3.3	WFS_CMD_PIN_IMPORT_RSA_SIGNED_DES_KEY	125
5.3.4	WFS_CMD_PIN_GENERATE_RSA_KEY_PAIR	128
5.3.5	WFS_CMD_PIN_EXPORT_RSA_EPP_SIGNED_ITEM	130
5.4	Remote Key Loading with Certificates	132
5.4.1	WFS_CMD_PIN_LOAD_CERTIFICATE	132
5.4.2	WFS_CMD_PIN_GET_CERTIFICATE	133
5.4.3	WFS_CMD_PIN_REPLACE_CERTIFICATE	134
5.4.4	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY	135
5.4.5	WFS_CMD_PIN_LOAD_CERTIFICATE_EX	137
5.4.6	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY_EX	139
5.5	EMV	142
5.5.1	WFS_CMD_PIN_EMV_IMPORT_PUBLIC_KEY	142
5.5.2	WFS_CMD_PIN_DIGEST	145
6.	Events	146
6.1	WFS_EXEE_PIN_KEY	146
6.2	WFS_SRVE_PIN_INITIALIZED	147
6.3	WFS_SRVE_PIN_ILLEGAL_KEY_ACCESS	148
6.4	WFS_SRVE_PIN_OPT_REQUIRED	149
6.5	WFS_SRVE_PIN_CERTIFICATE_CHANGE	150
6.6	WFS_SRVE_PIN_HSM_TDATA_CHANGED	151
6.7	WFS_SRVE_PIN_HSM_CHANGED	152
6.8	WFS_EXEE_PIN_ENTERDATA	153
6.9	WFS_SRVE_PIN_DEVICEPOSITION	154
6.10	WFS_SRVE_PIN_POWER_SAVE_CHANGE	155
6.11	WFS_EXEE_PIN_LAYOUT	156
7.	C - Header File	158
8.	Appendix-A	178
8.1	Remote Key Loading Using Signatures	179
8.1.1	RSA Data Authentication and Digital Signatures	179
8.1.2	RSA Secure Key Exchange using Digital Signatures	180
8.1.3	Initialization Phase – Signature Issuer and ATM PIN	182
8.1.4	Initialization Phase – Signature Issuer and Host	183
8.1.5	Key Exchange – Host and ATM PIN	184
8.1.6	Key Exchange (with random number) – Host and ATM PIN	185
8.1.7	Enhanced RKL, Key Exchange (with random number) – Host and ATM PIN	186
8.1.8	Default Keys and Security Item loaded during manufacture	187
8.2	Remote Key Loading Using Certificates	188

CWA 16926-65:2015 (E)

8.2.1	Certificate Exchange and Authentication.....	188
8.2.2	Remote Key Exchange	189
8.2.3	Replace Certificate	190
8.2.4	Primary and Secondary Certificates	191
8.2.5	TR34 BIND To Host.....	192
8.2.6	TR34 Key Transport	193
8.2.7	TR34 REBIND To New Host	195
8.2.8	TR34 Force REBIND To New Host.....	196
8.2.9	TR34 UNBIND From Host.....	197
8.2.10	TR34 Force UNBIND From Host.....	198
8.3	German ZKA GeldKarte	199
8.3.1	How to use the SECURE_MSG commands	199
8.3.2	Protocol WFS_PIN_PROTISOAS	200
8.3.3	Protocol WFS_PIN_PROTISOLZ	201
8.3.4	Protocol WFS_PIN_PROTISOPS	202
8.3.5	Protocol WFS_PIN_PROTCHIPZKA	203
8.3.6	Protocol WFS_PIN_PROTRAWDATA	204
8.3.7	Protocol WFS_PIN_PROTPBM	205
8.3.8	Protocol WFS_PIN_PROTHSMLDI	206
8.3.9	Protocol WFS_PIN_PROTGENAS	207
8.3.10	Protocol WFS_PIN_PROTCHIPINCHG.....	210
8.3.11	Protocol WFS_PIN_PROTPINCMF	211
8.3.12	Protocol WFS_PIN_PROTISOPINCHG	213
8.3.13	Command Sequence.....	214
8.4	EMV Support.....	221
8.4.1	Keys loading.....	221
8.4.2	PIN Block Management	223
8.4.3	SHA-1 Digest.....	224
8.5	French Cartes Bancaires	225
8.5.1	Data Structure for WFS_CMD_PIN_ENC_IO	225
8.5.2	Command Sequence.....	227
8.6	Secure Key Entry	229
8.6.1	Keyboard Layout.....	229
8.6.2	Command Usage.....	233
8.7	WFS_PIN_USERRESTRICTEDKEYENCKEY key usage	234
8.7.1	Command Usage.....	234
9.	Appendix-B (Country Specific WFS_CMD_PIN_ENC_IO protocols)	237
9.1	Luxemburg Protocol	237
9.1.1	WFS_CMD_ENC_IO_LUX_LOAD_APPKEY	239
9.1.2	WFS_CMD_ENC_IO_LUX_GENERATE_MAC	241
9.1.3	WFS_CMD_ENC_IO_LUX_CHECK_MAC.....	242
9.1.4	WFS_CMD_ENC_IO_LUX_BUILD_PINBLOCK	243
9.1.5	WFS_CMD_ENC_IO_LUX_DECRYPT_TDES.....	244
9.1.6	WFS_CMD_ENC_IO_LUX_ENCRYPT_TDES.....	245
9.1.7	Luxemburg-specific Header File	246
9.2	China Protocol	249
9.2.1	WFS_CMD_ENC_IO_CHN_DIGEST	251
9.2.2	WFS_CMD_ENC_IO_CHN_SET_SM2_PARAM	252
9.2.3	WFS_CMD_ENC_IO_CHN_IMPORT_SM2_PUBLIC_KEY	253
9.2.4	WFS_CMD_ENC_IO_CHN_SIGN.....	255
9.2.5	WFS_CMD_ENC_IO_CHN_VERIFY.....	257
9.2.6	WFS_CMD_ENC_IO_CHN_EXPORT_SM2_ISSUER_SIGNED_ITEM	258
9.2.7	WFS_CMD_ENC_IO_CHN_GENERATE_SM2_KEY_PAIR.....	260
9.2.8	WFS_CMD_ENC_IO_CHN_EXPORT_SM2_EPP_SIGNED_ITEM	261
9.2.9	WFS_CMD_ENC_IO_CHN_IMPORT_SM2_SIGNED_SM4_KEY.....	263
9.2.10	China-specific Header File	266

10. Appendix–C (Standardized <i>lpSzExtra</i> fields)	271
10.1 WFS_INF_PIN_STATUS	271
10.2 WFS_INF_PIN_CAPABILITIES	272
11. Appendix–D (TR-31 Key Use).....	275

European foreword

This CWA is revision 3.30 of the XFS interface specification.

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties on March 19th 2015, the constitution of which was supported by CEN following the public call for participation made on 1998-06-24. The specification is continuously reviewed and commented in the CEN/ISSS Workshop on XFS. It is therefore expected that an update of the specification will be published in due time as a CWA, superseding this revision 3.30.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available from the CEN/XFS Secretariat. The CEN XFS Workshop gathered suppliers as well as banks and other financial service companies.

The CWA is published as a multi-part document, consisting of:

Part 1: Application Programming Interface (API) - Service Provider Interface (SPI) - Programmer's Reference

Part 2: Service Classes Definition - Programmer's Reference

Part 3: Printer and Scanning Device Class Interface - Programmer's Reference

Part 4: Identification Card Device Class Interface - Programmer's Reference

Part 5: Cash Dispenser Device Class Interface - Programmer's Reference

Part 6: PIN Keypad Device Class Interface - Programmer's Reference

Part 7: Check Reader/Scanner Device Class Interface - Programmer's Reference

Part 8: Depository Device Class Interface - Programmer's Reference

Part 9: Text Terminal Unit Device Class Interface - Programmer's Reference

Part 10: Sensors and Indicators Unit Device Class Interface - Programmer's Reference

Part 11: Vendor Dependent Mode Device Class Interface - Programmer's Reference

Part 12: Camera Device Class Interface - Programmer's Reference

Part 13: Alarm Device Class Interface - Programmer's Reference

Part 14: Card Embossing Unit Device Class Interface - Programmer's Reference

Part 15: Cash-In Module Device Class Interface - Programmer's Reference

Part 16: Card Dispenser Device Class Interface - Programmer's Reference

Part 17: Barcode Reader Device Class Interface - Programmer's Reference

Part 18: Item Processing Module Device Class Interface - Programmer's Reference

Parts 19 - 28: Reserved for future use.

Parts 29 through 47 constitute an optional addendum to this CWA. They define the integration between the SNMP standard and the set of status and statistical information exported by the Service Providers.

Part 29: XFS MIB Architecture and SNMP Extensions - Programmer's Reference

Part 30: XFS MIB Device Specific Definitions - Printer Device Class

Part 31: XFS MIB Device Specific Definitions - Identification Card Device Class

Part 32: XFS MIB Device Specific Definitions - Cash Dispenser Device Class

Part 33: XFS MIB Device Specific Definitions - PIN Keypad Device Class

Part 34: XFS MIB Device Specific Definitions - Check Reader/Scanner Device Class

Part 35: XFS MIB Device Specific Definitions - Depository Device Class

Part 36: XFS MIB Device Specific Definitions - Text Terminal Unit Device Class

Part 37: XFS MIB Device Specific Definitions - Sensors and Indicators Unit Device Class

Part 38: XFS MIB Device Specific Definitions - Camera Device Class

Part 39: XFS MIB Device Specific Definitions - Alarm Device Class

Part 40: XFS MIB Device Specific Definitions - Card Embossing Unit Class

Part 41: XFS MIB Device Specific Definitions - Cash-In Module Device Class

Part 42: Reserved for future use.

Part 43: XFS MIB Device Specific Definitions - Vendor Dependent Mode Device Class

Part 44: XFS MIB Application Management

Part 45: XFS MIB Device Specific Definitions - Card Dispenser Device Class

Part 46: XFS MIB Device Specific Definitions - Barcode Reader Device Class

Part 47: XFS MIB Device Specific Definitions - Item Processing Module Device Class

Parts 48 - 60 are reserved for future use.

Part 61: Application Programming Interface (API) - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Service Provider Interface (SPI) - Programmer's Reference

Part 62: Printer and Scanning Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 63: Identification Card Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 64: Cash Dispenser Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 65: PIN Keypad Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 66: Check Reader/Scanner Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 67: Depository Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 68: Text Terminal Unit Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 69: Sensors and Indicators Unit Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 70: Vendor Dependent Mode Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 71: Camera Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 72: Alarm Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 73: Card Embossing Unit Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 74: Cash-In Module Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 75: Card Dispenser Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 76: Barcode Reader Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

Part 77: Item Processing Module Device Class Interface - Migration from Version 3.20 (CWA 16374) to Version 3.30 (this CWA) - Programmer's Reference

In addition to these Programmer's Reference specifications, the reader of this CWA is also referred to a complementary document, called Release Notes. The Release Notes contain clarifications and explanations on the CWA specifications, which are not requiring functional changes. The current version of the Release Notes is available online from <http://www.cen.eu/work/areas/ict/ebusiness/pages/ws-xfs.aspx>.

CWA 16926-65:2015 (E)

The information in this document represents the Workshop's current views on the issues discussed as of the date of publication. It is furnished for informational purposes only and is subject to change without notice. CEN makes no warranty, express or implied, with respect to this document.

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

The final review/endorsement round for this CWA was started on 2015-01-16 and was successfully closed on 2015-03-19. The final text of this CWA was submitted to CEN for publication on 2015-06-19. The specification is continuously reviewed and commented in the CEN Workshop on XFS. It is therefore expected that an update of the specification will be published in due time as a CWA, superseding this revision 3.30.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

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
-