



NSAI
Standards

Standard Recommendation
S.R. CWA 16374-65:2011

Extensions for Financial Services (XFS)
interface specification Release 3.20 - Part
65: PIN Keypad Device Class Interface
Migration from Version 3.10 (CWA 15748)
to Version 3.20 (this CWA) Programmer's
Reference

S.R. CWA 16374-65:2011

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:

This document is based on:
CWA 16374-65:2011

Published:
3 January, 2012

This document was published under the authority of the NSAI and comes into effect on:
3 January, 2012

ICS number:

35.240.40

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

CEN

CWA 16374-65

WORKSHOP

December 2011

AGREEMENT

ICS 35.240.40

English version

**Extensions for Financial Services (XFS) interface specification
Release 3.20 - Part 65: PIN Keypad Device Class Interface
Migration from Version 3.10 (CWA 15748) to Version 3.20 (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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



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

Management Centre: Avenue Marnix 17, B-1000 Brussels

CWA 16374-65:2011 (E)

Table of Contents

Foreword	5
1. Migration Information.....	8
2. PIN Keypad.....	9
3. References	11
4. Info Commands	13
4.1 WFS_INF_PIN_STATUS.....	13
4.2 WFS_INF_PIN_CAPABILITIES	17
4.3 WFS_INF_PIN_KEY_DETAIL	25
4.4 WFS_INF_PIN_FUNCKEY_DETAIL.....	27
4.5 WFS_INF_PIN_HSM_TDATA	30
4.6 WFS_INF_PIN_KEY_DETAIL_EX.....	31
4.7 WFS_INF_PIN_SECUREKEY_DETAIL.....	33
4.8 WFS_INF_PIN_QUERY_LOGICAL_HSM_DETAIL	37
4.9 WFS_INF_PIN_QUERY_PCIPTS_DEVICE_ID	38
5. Execute Commands	39
5.1 Normal PIN Commands	40
5.1.1 WFS_CMD_PIN_CRYPT	40
5.1.2 WFS_CMD_PIN_IMPORT_KEY	43
5.1.3 WFS_CMD_PIN_DERIVE_KEY	46
5.1.4 WFS_CMD_PIN_GET_PIN.....	48
5.1.5 WFS_CMD_PIN_LOCAL_DES	51
5.1.6 WFS_CMD_PIN_CREATE_OFFSET	53
5.1.7 WFS_CMD_PIN_LOCAL_EUROCHEQUE.....	55
5.1.8 WFS_CMD_PIN_LOCAL_VISA.....	57
5.1.9 WFS_CMD_PIN_PRESENT_IDC	59
5.1.10 WFS_CMD_PIN_GET_PINBLOCK	61
5.1.11 WFS_CMD_PIN_GET_DATA	63
5.1.12 WFS_CMD_PIN_INITIALIZATION	66
5.1.13 WFS_CMD_PIN_LOCAL_BANKSYS	68
5.1.14 WFS_CMD_PIN_BANKSYS_IO	69
5.1.15 WFS_CMD_PIN_RESET.....	70
5.1.16 WFS_CMD_PIN_HSM_SET_TDATA.....	71
5.1.17 WFS_CMD_PIN_SECURE_MSG_SEND.....	73
5.1.18 WFS_CMD_PIN_SECURE_MSG_RECEIVE	75
5.1.19 WFS_CMD_PIN_GET_JOURNAL	77
5.1.20 WFS_CMD_PIN_IMPORT_KEY_EX.....	78
5.1.21 WFS_CMD_PIN_ENC_IO.....	81
5.1.22 WFS_CMD_PIN_HSM_INIT.....	83
5.1.23 WFS_CMD_PIN_SECUREKEY_ENTRY	84
5.1.24 WFS_CMD_PIN_GENERATE_KCV	87
5.1.25 WFS_CMD_PIN_SET_GUIDANCE_LIGHT	88
5.1.26 WFS_CMD_PIN_MAINTAIN_PIN.....	90
5.1.27 WFS_CMD_PIN_KEYPRESS_BEEP	91
5.1.28 WFS_CMD_PIN_SET_PINBLOCK_DATA	92
5.1.29 WFS_CMD_PIN_SET_LOGICAL_HSM.....	93
5.1.30 WFS_CMD_PIN_IMPORT_KEYBLOCK	95
5.1.31 WFS_CMD_PIN_POWER_SAVE_CONTROL.....	96

S.R. CWA 16374-65:2011

CWA 16374-65:2011 (E)

- 5.2 Common commands for Remote Key Loading Schemes..... 97**
 - 5.2.1 WFS_CMD_PIN_START_KEY_EXCHANGE.....97
- 5.3 Remote Key Loading Using Signatures 98**
 - 5.3.1 WFS_CMD_PIN_IMPORT_RSA_PUBLIC_KEY98
 - 5.3.2 WFS_CMD_PIN_EXPORT_RSA_ISSUER_SIGNED_ITEM101
 - 5.3.3 WFS_CMD_PIN_IMPORT_RSA_SIGNED_DES_KEY103
 - 5.3.4 WFS_CMD_PIN_GENERATE_RSA_KEY_PAIR106
 - 5.3.5 WFS_CMD_PIN_EXPORT_RSA_EPP_SIGNED_ITEM.....108
- 5.4 Remote Key Loading with Certificates 110**
 - 5.4.1 WFS_CMD_PIN_LOAD_CERTIFICATE.....110
 - 5.4.2 WFS_CMD_PIN_GET_CERTIFICATE111
 - 5.4.3 WFS_CMD_PIN_REPLACE_CERTIFICATE112
 - 5.4.4 WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY.....113
- 5.5 EMV 115**
 - 5.5.1 WFS_CMD_PIN_EMV_IMPORT_PUBLIC_KEY115
 - 5.5.2 WFS_CMD_PIN_DIGEST118
- 6. Events..... 119**
 - 6.1 WFS_EXEE_PIN_KEY 119
 - 6.2 WFS_SRVE_PIN_INITIALIZED 120
 - 6.3 WFS_SRVE_PIN_ILLEGAL_KEY_ACCESS 121
 - 6.4 WFS_SRVE_PIN_OPT_REQUIRED..... 122
 - 6.5 WFS_SRVE_PIN_CERTIFICATE_CHANGE..... 123
 - 6.6 WFS_SRVE_PIN_HSM_TDATA_CHANGED..... 124
 - 6.7 WFS_SRVE_PIN_HSM_CHANGED..... 125
 - 6.8 WFS_EXEE_PIN_ENTERDATA 126
 - 6.9 WFS_SRVE_PIN_DEVICEPOSITION..... 127
 - 6.10 WFS_SRVE_PIN_POWER_SAVE_CHANGE..... 128
- 7. C - Header File 129**
- 8. Appendix-A 146**
 - 8.1 Remote Key Loading Using Signatures 147**
 - 8.1.1 RSA Data Authentication and Digital Signatures147
 - 8.1.2 RSA Secure Key Exchange using Digital Signatures148
 - 8.1.3 Initialization Phase – Signature Issuer and ATM PIN150
 - 8.1.4 Initialization Phase – Signature Issuer and Host151
 - 8.1.5 Key Exchange – Host and ATM PIN.....152
 - 8.1.6 Key Exchange (with random number) – Host and ATM PIN153
 - 8.1.7 Enhanced RKL, Key Exchange (with random number) – Host and ATM PIN154
 - 8.1.8 Default Keys and Security Item loaded during manufacture.....155
 - 8.2 Remote Key Loading Using Certificates 156**
 - 8.2.1 Certificate Exchange and Authentication156
 - 8.2.2 Remote Key Exchange.....157
 - 8.2.3 Replace Certificate.....158
 - 8.2.4 Primary and Secondary Certificates159
 - 8.3 German ZKA GeldKarte..... 160**
 - 8.3.1 How to use the SECURE_MSG commands.....160
 - 8.3.2 Protocol WFS_PIN_PROTISOAS161
 - 8.3.3 Protocol WFS_PIN_PROTISOLZ162
 - 8.3.4 Protocol WFS_PIN_PROTISOPS.....163
 - 8.3.5 Protocol WFS_PIN_PROTCHIPZKA164
 - 8.3.6 Protocol WFS_PIN_PROTRAWDATA165

S.R. CWA 16374-65:2011

CWA 16374-65:2011 (E)

8.3.7	Protocol WFS_PIN_PROTPBM	166
8.3.8	Protocol WFS_PIN_PROTHSMLDI	167
8.3.9	Protocol WFS_PIN_PROTGENAS	168
8.3.10	Protocol WFS_PIN_PROTCHIPINCHG	171
8.3.11	Protocol WFS_PIN_PROTPINCOMP	172
8.3.12	Protocol WFS_PIN_PROTISOPINCHG	174
8.3.13	Command Sequence	175
8.4	EMV Support.....	182
8.4.1	Keys loading.....	182
8.4.2	PIN Block Management	184
8.4.3	SHA-1 Digest	185
8.5	French Cartes Bancaires.....	186
8.5.1	Data Structure for WFS_CMD_PIN_ENC_IO	186
8.5.2	Command Sequence.....	188
8.6	Secure Key Entry	190
8.6.1	Keyboard Layout.....	190
8.6.2	Command Usage	194
9.	Appendix-B (Country Specific WFS_CMD_PIN_ENC_IO protocols)	195
9.1	Luxemburg Protocol.....	195
9.1.1	WFS_CMD_ENC_IO_LUX_LOAD_APPKEY	197
9.1.2	WFS_CMD_ENC_IO_LUX_GENERATE_MAC	199
9.1.3	WFS_CMD_ENC_IO_LUX_CHECK_MAC.....	200
9.1.4	WFS_CMD_ENC_IO_LUX_BUILD_PINBLOCK	201
9.1.5	WFS_CMD_ENC_IO_LUX_DECRYPT_TDES	202
9.1.6	WFS_CMD_ENC_IO_LUX_ENCRYPT_TDES	203
9.1.7	Luxemburg-specific Header File.....	204
10.	Appendix-C (Standardized <i>IpszExtra</i> fields).....	207
10.1	WFS_INF_PIN_STATUS.....	207
10.2	WFS_INF_PIN_CAPABILITIES	208

Foreword

This CWA is revision 3.20 of the XFS interface specification.

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties on 2011-06-29, 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 3.20.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. These organizations were drawn from the banking sector. The CEN/ISSS 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 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

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

S.R. CWA 16374-65:2011

CWA 16374-65:2011 (E)

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

Part 40: XFS MIB Device Specific Definitions - Card Embossing Unit Device 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 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) - Service Provider Interface (SPI) - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 62: Printer and Scanning Device Class Interface - Migration from Version 3.10 (CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 63: Identification Card Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 64: Cash Dispenser Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 65: PIN Keypad Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 66: Check Reader/Scanner Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 67: Depository Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 68: Text Terminal Unit Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 69: Sensors and Indicators Unit Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 70: Vendor Dependent Mode Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 71: Camera Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 72: Alarm Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 73: Card Embossing Unit Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 74: Cash-In Module Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 75: Card Dispenser Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 76: Barcode Reader Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (this CWA) - Programmer's Reference

Part 77: Item Processing Module Device Class Interface - Migration from Version 3.10 (see CWA 15748) to Version 3.20 (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/cen/pages/default.aspx>.

S.R. CWA 16374-65:2011

CWA 16374-65:2011 (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/ISSS 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 2011-06-23 and was successfully closed on 2011-07-23. The final text of this CWA was submitted to CEN for publication on 2011-08-26.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland 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.

CWA 16374-65:2011 (E)

1. Migration Information

XFS 3.20 has been designed to minimize backwards compatibility issues. This document highlights the changes made to the PIN device class between version 3.10 and 3.20, by highlighting the additions and deletions to the text.

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](#)
-