

CEN

CWA 16926-6

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 6: PIN Keypad Device Class Interface -
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. Introduction.....	9
1.1 Background to Release 3.30	9
1.2 XFS Service-Specific Programming.....	9
2. PIN Keypad	11
2.1 Encrypting Touch Screen (ETS).....	13
3. References	16
4. Info Commands.....	18
4.1 WFS_INF_PIN_STATUS	18
4.2 WFS_INF_PIN_CAPABILITIES	22
4.3 WFS_INF_PIN_KEY_DETAIL	34
4.4 WFS_INF_PIN_FUNCKEY_DETAIL.....	36
4.5 WFS_INF_PIN_HSM_TDATA	39
4.6 WFS_INF_PIN_KEY_DETAIL_EX.....	40
4.7 WFS_INF_PIN_SECUREKEY_DETAIL	43
4.8 WFS_INF_PIN_QUERY_LOGICAL_HSM_DETAIL	47
4.9 WFS_INF_PIN_QUERY_PCIPTS_DEVICE_ID	48
4.10 WFS_INF_PIN_GET_LAYOUT	49
5. Execute Commands.....	52
5.1 Normal PIN Commands.....	52
5.1.1 WFS_CMD_PIN_CRYPT	52
5.1.2 WFS_CMD_PIN_IMPORT_KEY	55
5.1.3 WFS_CMD_PIN_DERIVE_KEY.....	58
5.1.4 WFS_CMD_PIN_GET_PIN	60
5.1.5 WFS_CMD_PIN_LOCAL_DES.....	63
5.1.6 WFS_CMD_PIN_CREATE_OFFSET	65
5.1.7 WFS_CMD_PIN_LOCAL_EUROCHEQUE.....	67
5.1.8 WFS_CMD_PIN_LOCAL_VISA	69
5.1.9 WFS_CMD_PIN_PRESENT_IDC.....	71
5.1.10 WFS_CMD_PIN_GET_PINBLOCK	73
5.1.11 WFS_CMD_PIN_GET_DATA	75
5.1.12 WFS_CMD_PIN_INITIALIZATION.....	78
5.1.13 WFS_CMD_PIN_LOCAL_BANKSYS	80
5.1.14 WFS_CMD_PIN_BANKSYS_IO.....	81
5.1.15 WFS_CMD_PIN_RESET.....	82
5.1.16 WFS_CMD_PIN_HSM_SET_TDATA	83
5.1.17 WFS_CMD_PIN_SECURE_MSG_SEND	85
5.1.18 WFS_CMD_PIN_SECURE_MSG_RECEIVE	87
5.1.19 WFS_CMD_PIN_GET_JOURNAL.....	89
5.1.20 WFS_CMD_PIN_IMPORT_KEY_EX	90
5.1.21 WFS_CMD_PIN_ENC_IO	93
5.1.22 WFS_CMD_PIN_HSM_INIT	95
5.1.23 WFS_CMD_PIN_SECUREKEY_ENTRY	96
5.1.24 WFS_CMD_PIN_GENERATE_KCV	99
5.1.25 WFS_CMD_PIN_SET_GUIDANCE_LIGHT	100
5.1.26 WFS_CMD_PIN_MAINTAIN_PIN	102

5.1.27	WFS_CMD_PIN_KEYPRESS_BEEP	103
5.1.28	WFS_CMD_PIN_SET_PINBLOCK_DATA	104
5.1.29	WFS_CMD_PIN_SET_LOGICAL_HSM	105
5.1.30	WFS_CMD_PIN_IMPORT_KEYBLOCK	107
5.1.31	WFS_CMD_PIN_POWER_SAVE_CONTROL	108
5.1.32	WFS_CMD_PIN_DEFINE_LAYOUT	109
5.1.33	WFS_CMD_PIN_START_AUTHENTICATE	112
5.1.34	WFS_CMD_PIN_AUTHENTICATE	114
5.1.35	WFS_CMD_PIN_GET_PINBLOCK_EX	117
5.1.36	WFS_CMD_PIN_SYNCHRONIZE_COMMAND	119
5.2	Common commands for Remote Key Loading Schemes	120
5.2.1	WFS_CMD_PIN_START_KEY_EXCHANGE	120
5.3	Remote Key Loading Using Signatures	121
5.3.1	WFS_CMD_PIN_IMPORT_RSA_PUBLIC_KEY	121
5.3.2	WFS_CMD_PIN_EXPORT_RSA_ISSUER_SIGNED_ITEM	124
5.3.3	WFS_CMD_PIN_IMPORT_RSA_SIGNED_DES_KEY	126
5.3.4	WFS_CMD_PIN_GENERATE_RSA_KEY_PAIR	129
5.3.5	WFS_CMD_PIN_EXPORT_RSA_EPP_SIGNED_ITEM	131
5.4	Remote Key Loading with Certificates	133
5.4.1	WFS_CMD_PIN_LOAD_CERTIFICATE	133
5.4.2	WFS_CMD_PIN_GET_CERTIFICATE	134
5.4.3	WFS_CMD_PIN_REPLACE_CERTIFICATE	135
5.4.4	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY	136
5.4.5	WFS_CMD_PIN_LOAD_CERTIFICATE_EX	138
5.4.6	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY_EX	140
5.5	EMV	143
5.5.1	WFS_CMD_PIN_EMV_IMPORT_PUBLIC_KEY	143
5.5.2	WFS_CMD_PIN_DIGEST	146
6.	Events	147
6.1	WFS_EXEE_PIN_KEY	147
6.2	WFS_SRVE_PIN_INITIALIZED	148
6.3	WFS_SRVE_PIN_ILLEGAL_KEY_ACCESS	149
6.4	WFS_SRVE_PIN_OPT_REQUIRED	150
6.5	WFS_SRVE_PIN_CERTIFICATE_CHANGE	151
6.6	WFS_SRVE_PIN_HSM_TDATA_CHANGED	152
6.7	WFS_SRVE_PIN_HSM_CHANGED	153
6.8	WFS_EXEE_PIN_ENTERDATA	154
6.9	WFS_SRVE_PIN_DEVICEPOSITION	155
6.10	WFS_SRVE_PIN_POWER_SAVE_CHANGE	156
6.11	WFS_EXEE_PIN_LAYOUT	157
7.	C - Header File	159
8.	Appendix-A	179
8.1	Remote Key Loading Using Signatures	180
8.1.1	RSA Data Authentication and Digital Signatures	180
8.1.2	RSA Secure Key Exchange using Digital Signatures	181
8.1.3	Initialization Phase – Signature Issuer and ATM PIN	183
8.1.4	Initialization Phase – Signature Issuer and Host	184
8.1.5	Key Exchange – Host and ATM PIN	185
8.1.6	Key Exchange (with random number) – Host and ATM PIN	186
8.1.7	Enhanced RKL, Key Exchange (with random number) – Host and ATM PIN	187

8.1.8	Default Keys and Security Item loaded during manufacture	188
8.2	Remote Key Loading Using Certificates	189
8.2.1	Certificate Exchange and Authentication	189
8.2.2	Remote Key Exchange	190
8.2.3	Replace Certificate	191
8.2.4	Primary and Secondary Certificates	192
8.2.5	TR34 BIND To Host	193
8.2.6	TR34 Key Transport	194
8.2.7	TR34 REBIND To New Host	196
8.2.8	TR34 Force REBIND To New Host	197
8.2.9	TR34 UNBIND From Host	198
8.2.10	TR34 Force UNBIND From Host	199
8.3	German ZKA GeldKarte	200
8.3.1	How to use the SECURE_MSG commands	200
8.3.2	Protocol WFS_PIN_PROTISOAS	201
8.3.3	Protocol WFS_PIN_PROTISOLZ	202
8.3.4	Protocol WFS_PIN_PROTISOPS	203
8.3.5	Protocol WFS_PIN_PROTCHIPZKA	204
8.3.6	Protocol WFS_PIN_PROTRAWDATA	205
8.3.7	Protocol WFS_PIN_PROTPBM	206
8.3.8	Protocol WFS_PIN_PROTHSMLDI	207
8.3.9	Protocol WFS_PIN_PROTGENAS	208
8.3.10	Protocol WFS_PIN_PROTCHIPINCHG	211
8.3.11	Protocol WFS_PIN_PROTPINCMF	212
8.3.12	Protocol WFS_PIN_PROTISOPINCHG	214
8.3.13	Command Sequence	215
8.4	EMV Support	222
8.4.1	Keys loading	222
8.4.2	PIN Block Management	224
8.4.3	SHA-1 Digest	225
8.5	French Cartes Bancaires	226
8.5.1	Data Structure for WFS_CMD_PIN_ENC_IO	226
8.5.2	Command Sequence	228
8.6	Secure Key Entry	230
8.6.1	Keyboard Layout	230
8.6.2	Command Usage	234
8.7	WFS_PIN_USERRESTRICTEDKEYENCKEY key usage	235
8.7.1	Command Usage	235
9.	Appendix-B (Country Specific WFS_CMD_PIN_ENC_IO protocols)	238
9.1	Luxemburg Protocol	238
9.1.1	WFS_CMD_ENC_IO_LUX_LOAD_APPKEY	240
9.1.2	WFS_CMD_ENC_IO_LUX_GENERATE_MAC	242
9.1.3	WFS_CMD_ENC_IO_LUX_CHECK_MAC	243
9.1.4	WFS_CMD_ENC_IO_LUX_BUILD_PINBLOCK	244
9.1.5	WFS_CMD_ENC_IO_LUX_DECRYPT_TDES	245
9.1.6	WFS_CMD_ENC_IO_LUX_ENCRYPT_TDES	246
9.1.7	Luxemburg-specific Header File	247
9.2	China Protocol	249
9.2.1	WFS_CMD_ENC_IO_CHN_DIGEST	252
9.2.2	WFS_CMD_ENC_IO_CHN_SET_SM2_PARAM	253
9.2.3	WFS_CMD_ENC_IO_CHN_IMPORT_SM2_PUBLIC_KEY	254
9.2.4	WFS_CMD_ENC_IO_CHN_SIGN	256
9.2.5	WFS_CMD_ENC_IO_CHN_VERIFY	258
9.2.6	WFS_CMD_ENC_IO_CHN_EXPORT_SM2_ISSUER_SIGNED_ITEM	259
9.2.7	WFS_CMD_ENC_IO_CHN_GENERATE_SM2_KEY_PAIR	261
9.2.8	WFS_CMD_ENC_IO_CHN_EXPORT_SM2_EPP_SIGNED_ITEM	262
9.2.9	WFS_CMD_ENC_IO_CHN_IMPORT_SM2_SIGNED_SM4_KEY	264

9.2.10	China-specific Header File	267
10.	Appendix–C (Standardized <i>lpzExtra</i> fields)	272
10.1	WFS_INF_PIN_STATUS	272
10.2	WFS_INF_PIN_CAPABILITIES	273
11.	Appendix–D (TR-31 Key Use).....	276

This document is a preview generated by EVS

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