

CEN

CWA 16374-6

WORKSHOP

December 2011

AGREEMENT

ICS 35.240.40

English version

**Extensions for Financial Services (XFS) interface specification
Release 3.20 - 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, 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

Table of Contents

Foreword	5
1. Introduction	8
1.1 Background to Release 3.20	8
1.2 XFS Service-Specific Programming	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	39
5.1.1 WFS_CMD_PIN_CRYPT	39
5.1.2 WFS_CMD_PIN_IMPORT_KEY	42
5.1.3 WFS_CMD_PIN_DERIVE_KEY	45
5.1.4 WFS_CMD_PIN_GET_PIN.....	47
5.1.5 WFS_CMD_PIN_LOCAL_DES	50
5.1.6 WFS_CMD_PIN_CREATE_OFFSET	52
5.1.7 WFS_CMD_PIN_LOCAL_EUROCHEQUE.....	54
5.1.8 WFS_CMD_PIN_LOCAL_VISA.....	56
5.1.9 WFS_CMD_PIN_PRESENT_IDC	58
5.1.10 WFS_CMD_PIN_GET_PINBLOCK	60
5.1.11 WFS_CMD_PIN_GET_DATA	62
5.1.12 WFS_CMD_PIN_INITIALIZATION	65
5.1.13 WFS_CMD_PIN_LOCAL_BANKSYS	67
5.1.14 WFS_CMD_PIN_BANKSYS_IO	68
5.1.15 WFS_CMD_PIN_RESET	69
5.1.16 WFS_CMD_PIN_HSM_SET_TDATA.....	70
5.1.17 WFS_CMD_PIN_SECURE_MSG_SEND.....	72
5.1.18 WFS_CMD_PIN_SECURE_MSG_RECEIVE	74
5.1.19 WFS_CMD_PIN_GET_JOURNAL	76
5.1.20 WFS_CMD_PIN_IMPORT_KEY_EX.....	77
5.1.21 WFS_CMD_PIN_ENC_IO.....	80
5.1.22 WFS_CMD_PIN_HSM_INIT.....	82
5.1.23 WFS_CMD_PIN_SECUREKEY_ENTRY	83
5.1.24 WFS_CMD_PIN_GENERATE_KCV	86
5.1.25 WFS_CMD_PIN_SET_GUIDANCE_LIGHT	87
5.1.26 WFS_CMD_PIN_MAINTAIN_PIN.....	89
5.1.27 WFS_CMD_PIN_KEYPRESS_BEEP	90
5.1.28 WFS_CMD_PIN_SET_PINBLOCK_DATA	91

5.1.29	WFS_CMD_PIN_SET_LOGICAL_HSM	92
5.1.30	WFS_CMD_PIN_IMPORT_KEYBLOCK	94
5.1.31	WFS_CMD_PIN_POWER_SAVE_CONTROL	95
5.2	Common commands for Remote Key Loading Schemes	96
5.2.1	WFS_CMD_PIN_START_KEY_EXCHANGE	96
5.3	Remote Key Loading Using Signatures	97
5.3.1	WFS_CMD_PIN_IMPORT_RSA_PUBLIC_KEY	97
5.3.2	WFS_CMD_PIN_EXPORT_RSA_ISSUER_SIGNED_ITEM	100
5.3.3	WFS_CMD_PIN_IMPORT_RSA_SIGNED_DES_KEY	102
5.3.4	WFS_CMD_PIN_GENERATE_RSA_KEY_PAIR	105
5.3.5	WFS_CMD_PIN_EXPORT_RSA_EPP_SIGNED_ITEM	107
5.4	Remote Key Loading with Certificates	109
5.4.1	WFS_CMD_PIN_LOAD_CERTIFICATE	109
5.4.2	WFS_CMD_PIN_GET_CERTIFICATE	110
5.4.3	WFS_CMD_PIN_REPLACE_CERTIFICATE	111
5.4.4	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY	112
5.5	EMV	114
5.5.1	WFS_CMD_PIN_EMV_IMPORT_PUBLIC_KEY	114
5.5.2	WFS_CMD_PIN_DIGEST	117
6.	Events	118
6.1	WFS_EXEE_PIN_KEY	118
6.2	WFS_SRVE_PIN_INITIALIZED	119
6.3	WFS_SRVE_PIN_ILLEGAL_KEY_ACCESS	120
6.4	WFS_SRVE_PIN_OPT_REQUIRED	121
6.5	WFS_SRVE_PIN_CERTIFICATE_CHANGE	122
6.6	WFS_SRVE_PIN_HSM_TDATA_CHANGED	123
6.7	WFS_SRVE_PIN_HSM_CHANGED	124
6.8	WFS_EXEE_PIN_ENTERDATA	125
6.9	WFS_SRVE_PIN_DEVICEPOSITION	126
6.10	WFS_SRVE_PIN_POWER_SAVE_CHANGE	127
7.	C - Header File	128
8.	Appendix-A	145
8.1	Remote Key Loading Using Signatures	146
8.1.1	RSA Data Authentication and Digital Signatures	146
8.1.2	RSA Secure Key Exchange using Digital Signatures	147
8.1.3	Initialization Phase – Signature Issuer and ATM PIN	149
8.1.4	Initialization Phase – Signature Issuer and Host	150
8.1.5	Key Exchange – Host and ATM PIN	151
8.1.6	Key Exchange (with random number) – Host and ATM PIN	152
8.1.7	Enhanced RKL, Key Exchange (with random number) – Host and ATM PIN	153
8.1.8	Default Keys and Security Item loaded during manufacture	154
8.2	Remote Key Loading Using Certificates	155
8.2.1	Certificate Exchange and Authentication	155
8.2.2	Remote Key Exchange	156
8.2.3	Replace Certificate	157
8.2.4	Primary and Secondary Certificates	158
8.3	German ZKA GeldKarte	159
8.3.1	How to use the SECURE_MSG commands	159
8.3.2	Protocol WFS_PIN_PROTISOAS	160

8.3.3	Protocol WFS_PIN_PROTISOLZ	161
8.3.4	Protocol WFS_PIN_PROTISOPS.....	162
8.3.5	Protocol WFS_PIN_PROTCHIPZKA	163
8.3.6	Protocol WFS_PIN_PROTRAWDATA	164
8.3.7	Protocol WFS_PIN_PROTPBM	165
8.3.8	Protocol WFS_PIN_PROTHSMLDI	166
8.3.9	Protocol WFS_PIN_PROTGENAS	167
8.3.10	Protocol WFS_PIN_PROTCHIPINCHG.....	170
8.3.11	Protocol WFS_PIN_PROTPINCOMP.....	171
8.3.12	Protocol WFS_PIN_PROTISOPINCHG	173
8.3.13	Command Sequence.....	174
8.4	EMV Support.....	181
8.4.1	Keys loading.....	181
8.4.2	PIN Block Management.....	183
8.4.3	SHA-1 Digest.....	184
8.5	French Cartes Bancaires.....	185
8.5.1	Data Structure for WFS_CMD_PIN_ENC_IO	185
8.5.2	Command Sequence.....	187
8.6	Secure Key Entry	189
8.6.1	Keyboard Layout.....	189
8.6.2	Command Usage	193
9.	Appendix-B (Country Specific WFS_CMD_PIN_ENC_IO protocols)	194
9.1	Luxemburg Protocol	194
9.1.1	WFS_CMD_ENC_IO_LUX_LOAD_APPKEY.....	196
9.1.2	WFS_CMD_ENC_IO_LUX_GENERATE_MAC	198
9.1.3	WFS_CMD_ENC_IO_LUX_CHECK_MAC.....	199
9.1.4	WFS_CMD_ENC_IO_LUX_BUILD_PINBLOCK	200
9.1.5	WFS_CMD_ENC_IO_LUX_DECRYPT_TDES	201
9.1.6	WFS_CMD_ENC_IO_LUX_ENCRYPT_TDES	202
9.1.7	Luxemburg-specific Header File.....	203
10.	Appendix-C (Standardized <i>IpszExtra</i> fields).....	206
10.1	WFS_INF_PIN_STATUS.....	206
10.2	WFS_INF_PIN_CAPABILITIES	207

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

CWA 16374-6:2011 (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 (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>.

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.

Revision History:

3.00	October 18, 2000	Initial release.
3.02	May 21, 2003	For a description of changes from version 3.00 to version 3.02 see the PIN 3.02 Migration document.
3.03	September 24, 2004	For a description of changes from version 3.02 to version 3.03 see the PIN 3.03 Migration document.
3.10	November 29, 2007	For a description of changes from version 3.03 to version 3.10 see the PIN 3.10 Migration document.
3.20	March 2nd, 2011	For a description of changes from version 3.10 to version 3.20 see the PIN 3.20 Migration document.

1. Introduction

1.1 Background to Release 3.20

The CEN/ISSS XFS Workshop aims to promote a clear and unambiguous specification defining a multi-vendor software interface to financial peripheral devices. The XFS (eXtensions for Financial Services) specifications are developed within the CEN/ISSS (European Committee for Standardization/Information Society Standardization System) Workshop environment. CEN/ISSS Workshops aim to arrive at a European consensus on an issue that can be published as a CEN Workshop Agreement (CWA).

The CEN/ISSS XFS Workshop encourages the participation of both banks and vendors in the deliberations required to create an industry standard. The CEN/ISSS XFS Workshop achieves its goals by focused sub-groups working electronically and meeting quarterly.

Release 3.20 of the XFS specification is based on a C API and is delivered with the continued promise for the protection of technical investment for existing applications. This release of the specification extends the functionality and capabilities of the existing devices covered by the specification, but does not include any new device classes. Notable major enhancements include Mixed Media processing to allow mixed cash and check accepting, as well as the addition of new commands to the CIM, PTR and IDC to allow better support of the Japanese marketplace.

1.2 XFS Service-Specific Programming

The service classes are defined by their service-specific commands and the associated data structures, error codes, messages, etc. These commands are used to request functions that are specific to one or more classes of Service Providers, but not all of them, and therefore are not included in the common API for basic or administration functions.

When a service-specific command is common among two or more classes of Service Providers, the syntax of the command is as similar as possible across all services, since a major objective of XFS is to standardize function codes and structures for the broadest variety of services. For example, using the **WFSExecute** function, the commands to read data from various services are as similar as possible to each other in their syntax and data structures.

In general, the specific command set for a service class is defined as a superset of the specific capabilities likely to be provided by the developers of the services of that class; thus any particular device will normally support only a subset of the defined command set.

There are three cases in which a Service Provider may receive a service-specific command that it does not support:

The requested capability is defined for the class of Service Providers by the XFS specification, the particular vendor implementation of that service does not support it, and the unsupported capability is *not* considered to be fundamental to the service. In this case, the Service Provider returns a successful completion, but does no operation. An example would be a request from an application to turn on a control indicator on a passbook printer; the Service Provider recognizes the command, but since the passbook printer it is managing does not include that indicator, the Service Provider does no operation and returns a successful completion to the application.

The requested capability is defined for the class of Service Providers by the XFS specification, the particular vendor implementation of that service does not support it, and the unsupported capability *is* considered to be fundamental to the service. In this case, a `WFS_ERR_UNSUPP_COMMAND` error is returned to the calling application. An example would be a request from an application to a cash dispenser to dispense coins; the Service Provider recognizes the command but, since the cash dispenser it is managing dispenses only notes, returns this error.

The requested capability is *not* defined for the class of Service Providers by the XFS specification. In this case, a `WFS_ERR_INVALID_COMMAND` error is returned to the calling application.

This design allows implementation of applications that can be used with a range of services that provide differing subsets of the functionalities that are defined for their service class. Applications may use the **WFSGetInfo** and **WFSAsyncGetInfo** commands to inquire about the capabilities of the service they are about to use, and modify their behavior accordingly, or they may use functions and then deal with `WFS_ERR_UNSUPP_COMMAND` error returns to make decisions as to how to use the service.