



**NSAI**  
Standards

Standard Recommendation  
S.R. CWA 15748-65:2008

Extensions for Financial Services (XFS)  
interface specification - Release 3.10 -  
Part 65: PIN Keypad Device Class  
Interface - Migration from Version 3.03  
(CWA 14050) to Version 3.10 (this CWA)  
- Programmer's Reference

## S.R. CWA 15748-65:2008

*Incorporating amendments/corrigenda issued since publication:*

<i>This standard replaces:</i> S.R CWA 15748-65:2008	<i>This standard is based on:</i> CWA 15748-65:2008 CWA 15748-65:2008	<i>Published:</i>  25 April, 2008
This Irish Standard was published under the authority of the NSAI and comes into effect on: 9 September, 2008		ICS number: 35.240.50
<b>NSAI</b> 1 Swift Square, Northwood, Santry Dublin 9	T +353 1 807 3800 F +353 1 807 3838 E standards@nsai.ie W NSAI.ie	<b>Sales:</b> T +353 1 857 6730 F +353 1 857 6729 W standards.ie
		<b>Price Code:</b> AG
Údarás um Chaighdeáin Náisiúnta na hÉireann		

**S.R. CWA 15748-65:2008**

**CEN**

**CWA 15748-65**

**WORKSHOP**

July 2008

**AGREEMENT**

---

ICS 35.240.50

Supersedes CWA 15748-65:2008, February

English version

**Extensions for Financial Services (XFS) interface specification -  
Release 3.10 - Part 65: PIN Keypad Device Class Interface -  
Migration from Version 3.03 (CWA 14050) to Version 3.10 (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 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, 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: rue de Stassart, 36 B-1050 Brussels**

## Table of Contents

---

<b>Foreword .....</b>	<b>5</b>
<b>1. Migration Information .....</b>	<b>7</b>
<b>2. Pin Keypad .....</b>	<b>8</b>
<b>3. References .....</b>	<b>10</b>
<b>4. Info Commands .....</b>	<b>11</b>
4.1 WFS_INF_PIN_STATUS .....	11
4.2 WFS_INF_PIN_CAPABILITIES .....	14
4.3 WFS_INF_PIN_KEY_DETAIL .....	22
4.4 WFS_INF_PIN_FUNCKEY_DETAIL .....	24
4.5 WFS_INF_PIN_HSM_TDATA .....	27
4.6 WFS_INF_PIN_KEY_DETAIL_EX .....	28
4.7 WFS_INF_PIN_SECUREKEY_DETAIL .....	30
4.8 WFS_INF_PIN_QUERY_LOGICAL_HSM_DETAIL .....	34
<b>5. Execute Commands .....</b>	<b>35</b>
<b>5.1 Normal PIN Commands .....</b>	<b>35</b>
5.1.1 WFS_CMD_PIN_CRYPT .....	35
5.1.2 WFS_CMD_PIN_IMPORT_KEY .....	38
5.1.3 WFS_CMD_PIN_DERIVE_KEY .....	41
5.1.4 WFS_CMD_PIN_GET_PIN .....	43
5.1.5 WFS_CMD_PIN_LOCAL_DES .....	46
5.1.6 WFS_CMD_PIN_CREATE_OFFSET .....	48
5.1.7 WFS_CMD_PIN_LOCAL_EUROCHEQUE .....	50
5.1.8 WFS_CMD_PIN_LOCAL_VISA .....	52
5.1.9 WFS_CMD_PIN_PRESENT_IDC .....	54
5.1.10 WFS_CMD_PIN_GET_PINBLOCK .....	56
5.1.11 WFS_CMD_PIN_GET_DATA .....	58
5.1.12 WFS_CMD_PIN_INITIALIZATION .....	61
5.1.13 WFS_CMD_PIN_LOCAL_BANKSYS .....	63
5.1.14 WFS_CMD_PIN_BANKSYS_IO .....	64
5.1.15 WFS_CMD_PIN_RESET .....	65
5.1.16 WFS_CMD_PIN_HSM_SET_TDATA .....	66
5.1.17 WFS_CMD_PIN_SECURE_MSG_SEND .....	68
5.1.18 WFS_CMD_PIN_SECURE_MSG_RECEIVE .....	70
5.1.19 WFS_CMD_PIN_GET_JOURNAL .....	72
5.1.20 WFS_CMD_PIN_IMPORT_KEY_EX .....	73
5.1.21 WFS_CMD_PIN_ENC_IO .....	76
5.1.22 WFS_CMD_PIN_HSM_INIT .....	78
5.1.23 WFS_CMD_PIN_SECUREKEY_ENTRY .....	79
5.1.24 WFS_CMD_PIN_GENERATE_KCV .....	82
5.1.25 WFS_CMD_PIN_SET_GUIDANCE_LIGHT .....	83
5.1.26 WFS_CMD_PIN_MAINTAIN_PIN .....	84
5.1.27 WFS_CMD_PIN_KEYPRESS_BEEP .....	85
5.1.28 WFS_CMD_PIN_SET_PINBLOCK_DATA .....	86
5.1.29 WFS_CMD_PIN_SET_LOGICAL_HSM .....	87
5.1.30 WFS_CMD_PIN_IMPORT_KEYBLOCK .....	89
5.1.31 WFS_CMD_PIN_POWER_SAVE_CONTROL .....	90
<b>5.2 Common commands for Remote Key Loading Schemes .....</b>	<b>91</b>

5.2.1	WFS_CMD_PIN_START_KEY_EXCHANGE.....	91
<b>5.3</b>	<b>Remote Key Loading Using Signatures.....</b>	<b>92</b>
5.3.1	WFS_CMD_PIN_IMPORT_RSA_PUBLIC_KEY .....	92
5.3.2	WFS_CMD_PIN_EXPORT_RSA_ISSUER_SIGNED_ITEM .....	95
5.3.3	WFS_CMD_PIN_IMPORT_RSA_SIGNED_DES_KEY .....	97
5.3.4	WFS_CMD_PIN_GENERATE_RSA_KEY_PAIR .....	100
5.3.5	WFS_CMD_PIN_EXPORT_RSA_EPP_SIGNED_ITEM.....	102
<b>5.4</b>	<b>Remote Key Loading with Certificates.....</b>	<b>104</b>
5.4.1	WFS_CMD_PIN_LOAD_CERTIFICATE.....	104
5.4.2	WFS_CMD_PIN_GET_CERTIFICATE.....	105
5.4.3	WFS_CMD_PIN_REPLACE_CERTIFICATE.....	106
5.4.4	WFS_CMD_PIN_IMPORT_RSA_ENCIPHERED_PKCS7_KEY.....	107
<b>5.5</b>	<b>EMV .....</b>	<b>109</b>
5.5.1	WFS_CMD_PIN_EMV_IMPORT_PUBLIC_KEY .....	109
5.5.2	WFS_CMD_PIN_DIGEST.....	112
<b>6.</b>	<b>Events.....</b>	<b>113</b>
6.1	WFS_EXEE_PIN_KEY.....	113
6.2	WFS_SRVE_PIN_INITIALIZED .....	114
6.3	WFS_SRVE_PIN_ILLEGAL_KEY_ACCESS .....	115
6.4	WFS_SRVE_PIN_OPT_REQUIRED .....	116
6.5	WFS_SRVE_PIN_CERTIFICATE_CHANGE.....	117
6.6	WFS_SRVE_PIN_HSM_TDATA_CHANGED.....	118
6.7	WFS_SRVE_PIN_HSM_CHANGED .....	119
6.8	WFS_EXEE_PIN_ENTERDATA.....	120
6.9	WFS_SRVE_PIN_DEVICEPOSITION .....	121
6.10	WFS_SRVE_PIN_POWER_SAVE_CHANGE.....	122
<b>7.</b>	<b>C - Header File .....</b>	<b>123</b>
<b>8.</b>	<b>Appendix-A .....</b>	<b>139</b>
<b>8.1</b>	<b>Remote Key Loading Using Signatures.....</b>	<b>140</b>
8.1.1	RSA Data Authentication and Digital Signatures .....	140
8.1.2	RSA Secure Key Exchange using Digital Signatures .....	141
8.1.3	Initialization Phase – Signature Issuer and ATM PIN .....	143
8.1.4	Initialization Phase – Signature Issuer and Host .....	144
8.1.5	Key Exchange – Host and ATM PIN .....	145
8.1.6	Key Exchange (with random number) – Host and ATM PIN .....	146
8.1.7	Enhanced RKL, Key Exchange (with random number) – Host and ATM PIN .....	147
8.1.8	Default Keys and Security Item loaded during manufacture.....	148
<b>8.2</b>	<b>Remote Key Loading Using Certificates.....</b>	<b>149</b>
8.2.1	Certificate Exchange and Authentication.....	149
8.2.2	Remote Key Exchange.....	150
8.2.3	Replace Certificate.....	151
8.2.4	Primary and Secondary Certificates .....	152
<b>8.3</b>	<b>German ZKA GeldKarte .....</b>	<b>153</b>
8.3.1	How to use the SECURE_MSG commands.....	153
8.3.2	Protocol WFS_PIN_PROTISOAS .....	154
8.3.3	Protocol WFS_PIN_PROTISOLZ .....	155
8.3.4	Protocol WFS_PIN_PROTISOPS.....	156
8.3.5	Protocol WFS_PIN_PROTCHIPZKA .....	157
8.3.6	Protocol WFS_PIN_PROTRAWDATA .....	158
8.3.7	Protocol WFS_PIN_PROTPBM .....	159

**S.R. CWA 15748-65:2008**

Page 4

CWA 15748-65:2008

8.3.8	Protocol WFS_PIN_PROTHSMLDI .....	160
8.3.9	Protocol WFS_PIN_PROTGENAS .....	161
8.3.10	Protocol WFS_PIN_PROTCHIPPINCHG .....	164
8.3.11	Protocol WFS_PIN_PROTPINCMF .....	165
8.3.12	Protocol WFS_PIN_PROTISOPINCHG .....	166
8.3.13	Command Sequence .....	167
<b>8.4</b>	<b>EMV Support .....</b>	<b>174</b>
8.4.1	Keys loading .....	174
8.4.2	PIN block management .....	176
8.4.3	SHA-1 Digest .....	177
<b>8.5</b>	<b>French Cartes Bancaires .....</b>	<b>178</b>
8.5.1	Data Structure for WFS_CMD_PIN_ENC_IO .....	178
8.5.2	Command Sequence .....	180
<b>8.6</b>	<b>Secure Key Entry .....</b>	<b>183</b>
8.6.1	Keyboard Layout .....	183
8.6.2	Command Usage .....	187
<b>9.</b>	<b>Appendix-B (Country Specific WFS_CMD_PIN_ENC_IO protocols) .....</b>	<b>188</b>
<b>9.1</b>	<b>Luxemburg Protocol .....</b>	<b>188</b>
9.1.1	WFS_CMD_ENC_IO_LUX_LOAD_APPKEY .....	190
9.1.2	WFS_CMD_ENC_IO_LUX_GENERATE_MAC .....	192
9.1.3	WFS_CMD_ENC_IO_LUX_CHECK_MAC .....	193
9.1.4	WFS_CMD_ENC_IO_LUX_BUILD_PINBLOCK .....	194
9.1.5	WFS_CMD_ENC_IO_LUX_DECRYPT_TDES .....	195
9.1.6	WFS_CMD_ENC_IO_LUX_ENCRYPT_TDES .....	196
9.1.7	Luxemburg-specific Header File .....	197
<b>10.</b>	<b>Appendix-C (Standardized <i>IpszExtra</i> fields) .....</b>	<b>200</b>
<b>10.1</b>	<b>WFS_INF_PIN_STATUS .....</b>	<b>200</b>
<b>10.2</b>	<b>WFS_INF_PIN_CAPABILITIES .....</b>	<b>201</b>

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
-