



**NSAI**  
Standards

Irish Standard  
I.S. EN 14890-2:2008

# Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

## I.S. EN 14890-2:2008

*Incorporating amendments/corrigenda issued since publication:*

|   |  |   |                         |
|---|--|---|-------------------------|
| <i>This document replaces:</i><br>S.R. CWA 14890-2:2004   | <i>This document is based on:</i><br>EN 14890-2:2008<br>CWA 14890-2:2004   | <i>Published:</i><br>12 November, 2008<br>23 July, 2004                   |                         |
| This document was published under the authority of the NSAI and comes into effect on:<br>16 January, 2009 |  | ICS number:<br>35.240.15  |                         |
| <b>NSAI</b><br>1 Swift Square,<br>Northwood, Santry<br>Dublin 9   | T +353 1 807 3800<br>F +353 1 807 3838<br>E standards@nsai.ie<br>W NSAI.ie | <b>Sales:</b><br>T +353 1 857 6730<br>F +353 1 857 6729<br>W standards.ie | <b>Price Code:</b><br>V |
| Údarás um Chaighdeáin Náisiúnta na hÉireann   |  |   |                         |

English Version

## Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Interface d'application des cartes intelligentes utilisées  
comme dispositifs sûrs de création de signature - Partie 2 :  
Services complémentaires

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung  
qualifizierter elektronischer Signaturen verwendet werden -  
Teil 2: Zusätzliche Dienste

This European Standard was approved by CEN on 5 October 2008.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

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

## Contents

Page

|  |    |
|--|----|
| Foreword.....  | 5  |
| 1 Scope .....  | 6  |
| 2 Normative references .....   | 7  |
| 3 Terms and definitions .....  | 8  |
| 4 Abbreviations and notation .....   | 9  |
| 5 Additional Service Selection .....   | 11 |
| 6 Client/Server Authentication .....   | 13 |
| 6.1 General.....   | 13 |
| 6.2 Client/Server protocols .....  | 13 |
| 6.3 Steps preceding the client/server authentication .....                     | 13 |
| 6.4 Padding format.....  | 14 |
| 6.4.1 PKCS #1 v 1-5.....   | 14 |
| 6.4.2 DSI according to PKCS #1 V 2.x (PSS) .....                               | 15 |
| 6.5 Client/Server protocol .....   | 16 |
| 6.5.1 General.....   | 16 |
| 6.5.2 Step 1 — Read certificate.....   | 17 |
| 6.5.3 Step 2 — Set signing key for client/server internal authentication ..... | 17 |
| 6.5.4 Step 3 — Internal authentication.....                                    | 19 |
| 6.5.5 Client/Server authentication execution flow .....                        | 20 |
| 6.5.6 Command data field for the client server authentication .....            | 22 |
| 7 Role Authentication .....  | 23 |
| 7.1 Role Authentication of the card .....                                      | 23 |
| 7.2 Role Authentication of the server .....                                    | 23 |
| 7.3 Symmetrical external authentication .....                                  | 23 |
| 7.3.1 Protocol .....   | 23 |
| 7.3.2 Role description.....  | 26 |
| 7.4 Asymmetric external authentication.....                                    | 26 |
| 7.4.1 Protocol based on RSA.....   | 26 |
| 7.4.2 Role description.....  | 29 |
| 8 Encryption Key Decipherment .....  | 30 |
| 8.1 Steps preceding the key decryption.....                                    | 31 |
| 8.2 Key Management with RSA .....  | 31 |
| 8.2.1 General.....   | 31 |
| 8.2.2 OAEP padding.....  | 31 |
| 8.2.3 Execution flow.....  | 32 |
| 8.3 Diffie-Hellman key exchange .....  | 34 |
| 8.3.1 General.....   | 34 |
| 8.3.2 Execution flow.....  | 36 |
| 8.4 Algorithm Identifier for DECIPHER .....                                    | 37 |
| 9 Signature verification .....   | 39 |
| 9.1 Signature verification execution flow.....                                 | 39 |
| 9.1.1 Step 1: Receive Hash .....   | 40 |
| 9.1.2 Step 2: Select verification key .....                                    | 41 |
| 9.1.3 Step 3: Verify digital signature .....                                   | 42 |
| 10 Certificates for additional services .....                                  | 43 |
| 10.1 File structure .....  | 43 |
| 10.2 EF.C.CH.AUT .....   | 44 |
| 10.3 EF.C.CH.KE.....   | 44 |

|                |  |           |
|----------------|--|-----------|
| <b>10.4</b>    | <b>Reading Certificates and the public key of CAs</b> .....                                      | <b>44</b> |
| <b>11</b>      | <b>APDU data structures</b> .....  | <b>45</b> |
| <b>11.1</b>    | <b>Algorithm Identifiers</b> .....   | <b>45</b> |
| <b>11.1.1</b>  | <b>AlgIDs for Client/Server authentication</b> .....   | <b>45</b> |
| <b>11.1.2</b>  | <b>Algorithm Identifier for DECIPHER</b> .....   | <b>45</b> |
| <b>11.2</b>    | <b>CRTs</b> .....  | <b>46</b> |
| <b>11.2.1</b>  | <b>CRT DST for selection of ICC's private client/server auth. key</b> .....                      | <b>46</b> |
| <b>11.2.2</b>  | <b>CRT AT for selection of ICC's private client/server auth. key</b> .....                       | <b>46</b> |
| <b>11.2.3</b>  | <b>CRT CT for selection of ICC's private key</b> .....   | <b>47</b> |
| <b>11.2.4</b>  | <b>CRT CT for selection of ICC's DH encryption key</b> .....                                     | <b>47</b> |
| <b>11.2.5</b>  | <b>CRT DST for selection of IFD's public key (signature verification)</b> .....                  | <b>47</b> |
| <b>Annex A</b> | <b>(normative) Security Service Descriptor Templates</b> .....                                   | <b>48</b> |
| <b>A.1</b>     | <b>Introduction</b> .....  | <b>48</b> |
| <b>A.2</b>     | <b>Security Service Descriptor Concept</b> .....   | <b>48</b> |
| <b>A.3</b>     | <b>SSD Data Objects</b> .....  | <b>49</b> |
| <b>A.3.1</b>   | <b>DO Extended Header List, tag '4D'</b> .....   | <b>49</b> |
| <b>A.3.2</b>   | <b>DO Instruction set mapping (ISM), tag '80'</b> .....  | <b>49</b> |
| <b>A.3.3</b>   | <b>DO Command to perform (CTP), tag '52' (refer to ISO/IEC 7816-6)</b> .....                     | <b>49</b> |
| <b>A.3.4</b>   | <b>DO Algorithm object identifier (OID), tag '06' (refer to ISO/IEC 7816-6)</b> .....            | <b>49</b> |
| <b>A.3.5</b>   | <b>DO Algorithm reference, tag '81'</b> .....  | <b>49</b> |
| <b>A.3.6</b>   | <b>DO Key reference, tag '82'</b> .....  | <b>50</b> |
| <b>A.3.7</b>   | <b>DO FID key file, tag '83'</b> .....   | <b>50</b> |
| <b>A.3.8</b>   | <b>DO Key group, tag '84'</b> .....  | <b>50</b> |
| <b>A.3.9</b>   | <b>DO FID base certificate file, tag '85'</b> .....  | <b>50</b> |
| <b>A.3.10</b>  | <b>DO FID adjoined certificate file, tag '86'</b> .....  | <b>50</b> |
| <b>A.3.11</b>  | <b>DO Certificate reference, tag '87'</b> .....  | <b>50</b> |
| <b>A.3.12</b>  | <b>DO Certificate qualifier, tag '88'</b> .....  | <b>50</b> |
| <b>A.3.13</b>  | <b>DO FID for file with public key of the certification authority PK(CA), tag '89'</b> .....     | <b>50</b> |
| <b>A.3.14</b>  | <b>DO PIN usage policy, tag '5F2F'</b> .....   | <b>50</b> |
| <b>A.3.15</b>  | <b>DO PIN reference, tag '8A'</b> .....  | <b>51</b> |
| <b>A.3.16</b>  | <b>DO Application identifier (AID), tag '4F' (refer to ISO/IEC 7816-6)</b> .....                 | <b>51</b> |
| <b>A.3.17</b>  | <b>DO CLA coding, tag '8B'</b> .....   | <b>51</b> |
| <b>A.3.18</b>  | <b>DO Status information (SW1-SW2), tag '42' (refer to ISO/IEC 7816-6)</b> .....                 | <b>51</b> |
| <b>A.3.19</b>  | <b>DO Discretionary data, tag '53' (refer to ISO/IEC 7816-6)</b> .....                           | <b>51</b> |
| <b>A.3.20</b>  | <b>DO SE number, tag '8C'</b> .....  | <b>52</b> |
| <b>A.3.21</b>  | <b>DO SSD profile identifier, tag '8D'</b> .....   | <b>52</b> |
| <b>A.3.22</b>  | <b>DO FID mapping, tag '8E'</b> .....  | <b>52</b> |
| <b>A.4</b>     | <b>Location of the SSD templates</b> .....   | <b>52</b> |
| <b>A.5</b>     | <b>Examples for SSD templates</b> .....  | <b>52</b> |
| <b>Annex B</b> | <b>(informative) Key and signature formats for elliptic curves over prime fields GF(p)</b> ..... | <b>54</b> |
| <b>B.1</b>     | <b>General</b> .....   | <b>54</b> |
| <b>B.2</b>     | <b>Elliptic curve parameters</b> .....   | <b>54</b> |
| <b>B.3</b>     | <b>Public key point</b> .....  | <b>55</b> |
| <b>B.4</b>     | <b>ECDSA signature format</b> .....  | <b>55</b> |
| <b>Annex C</b> | <b>(informative) Security environments</b> .....   | <b>56</b> |
| <b>C.1</b>     | <b>Introduction</b> .....  | <b>56</b> |
| <b>C.2</b>     | <b>Definition of CRTs (examples)</b> .....   | <b>57</b> |
| <b>C.2.1</b>   | <b>General</b> .....   | <b>57</b> |
| <b>C.2.2</b>   | <b>CRT for Authentication (AT)</b> .....   | <b>58</b> |
| <b>C.2.3</b>   | <b>CRT for Cryptographic Checksum (CCT)</b> .....  | <b>59</b> |
| <b>C.2.4</b>   | <b>CRT for Digital Signature (DST)</b> .....   | <b>60</b> |
| <b>C.2.5</b>   | <b>CRT for confidentiality (CT)</b> .....  | <b>61</b> |
| <b>C.3</b>     | <b>Security Environments (example)</b> .....   | <b>62</b> |
| <b>C.3.1</b>   | <b>General</b> .....   | <b>62</b> |
| <b>C.3.2</b>   | <b>Security Environment #10</b> .....  | <b>62</b> |
| <b>C.3.3</b>   | <b>Security Environment #11</b> .....  | <b>62</b> |
| <b>C.4</b>     | <b>Coding of access conditions (example)</b> .....   | <b>63</b> |

|                              |   |           |
|------------------------------|---|-----------|
| <b>C.4.1</b>                 | <b>General.....</b>   | <b>63</b> |
| <b>C.4.2</b>                 | <b>Access Conditions.....</b>   | <b>64</b> |
| <b>C.4.3</b>                 | <b>Access rule references .....</b>                                     | <b>64</b> |
| <b>C.4.4</b>                 | <b>Access conditions for EF.ARR.....</b>                                | <b>66</b> |
| <b>C.4.5</b>                 | <b>EF.ARR records .....</b>   | <b>66</b> |
| <b>Annex D (informative)</b> | <b>Interoperability aspects .....</b>                                   | <b>69</b> |
| <b>D.1</b>                   | <b>General.....</b>   | <b>69</b> |
| <b>D.2</b>                   | <b>Choosing device authentication .....</b>                             | <b>69</b> |
| <b>D.2.1</b>                 | <b>General.....</b>   | <b>69</b> |
| <b>D.2.2</b>                 | <b>Signature generation flow with possible processing options .....</b> | <b>71</b> |
| <b>D.3</b>                   | <b>Choosing User verification method .....</b>                          | <b>72</b> |
| <b>Annex E (informative)</b> | <b>Example of DF.CIA .....</b>  | <b>73</b> |
| <b>Bibliography .....</b>    |   | <b>78</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](#)
-