

## Authentication Service Standards (also for SMH applications)

List extracted from CEN/ETSI draft on Network security 1.0

This document should be continuously consulted as it develops.

### A.1 General Authentication Standards

#### International Organisation for Standardisation and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 11131: *Banking - Financial Institution Sign-On Authentication*
- ISO/IEC 9594-8: *Directory Authentication*
- ISO/IEC 9797: *Message Authentication Codes (MACs)*
- ISO/IEC 9798: *Entity Authentication*
  - Part 1: *General Model*
  - Part 2: *Entity Authentication Mechanisms using a Symmetric Algorithm*
  - Part 3: *Entity Authentication Using a Public Key Algorithm*
  - Part 4: *Entity Authentication Using Cryptographic Check Function*
  - Part 5: *Entity Authentication Using Zero Knowledge Techniques*
- ISO/IEC 10181: *Security Frameworks*
  - Part 1: *Overview*
  - Part 2: *Authentication*
  - Part 3: *Access Control*
  - Part 4: *Non-Repudiation*
  - Part 5: *Integrity*
  - Part 6: *Confidentiality*
  - Part 7: *Audit*
  - Part 8: *Key Management*

#### European Telecommunications and Standards Institute

- ETSI ETS 300 331 ed.1 (1995-11): *Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM)*
- ETSI ETS 300 759 ed.1 (1997-10): *Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Test specification for DAM*
- ETSI ETS 300 760 ed.1 (1997-06): *Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM); Implementation Conformance Statement (ICS) proforma specification*
- ETSI I-ETS 300 768 ed.1 (1997-07) - (Historical): *Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Service description*
- ETSI I-ETS 300 769 ed.1 (1997-07) - (Historical): *Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Functional capabilities and information flows*
- ETSI ETS 300 825 ed.1 (1997-10): *Digital Enhanced Cordless Telecommunications (DECT); 3 Volt DECT Authentication Module (DAM)*
- ETSI ETS 300 841 ed.1 (1998-01): *Telecommunications security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audio-visual services*

- ETSI EN 301 492-1 V1.1.2 (2000-12): *Private Integrated Services Network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 1: Test Suite Structure and Test Purposes (TSS&TP) specification for the VPN "b" service entry point*
- ETSI EN 301 492-2 V1.1.1 (2000-12): *Private Integrated Services Network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 2: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma for the VPN "b" service entry point*
- ETSI EN 301 492-2 V1.2.1 (2002-01): *Private Integrated Services network (PISN); Inter-exchange signalling protocol; Cordless terminal authentication supplementary services; Part 2: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma specification for the VPN "b" service entry point*
- ETSI EN 301 828 V1.1.1 (2003-02): *Private Integrated Services Network (PISN); Specification, functional model and information flows; Wireless terminal authentication supplementary services [ISO/IEC 15432 (1999) modified]*
- ETSI TR 101 052 V1.1.1 (1997-06): *Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1*
- ETSI TR 133 902 V4.0.0 (2001-09): *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol (3GPP TR 33.902 version 4.0.0 Release 4)*
- ETSI TR 133 902 V3.1.0 (2000-01): *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol (3G TR 33.902 version 3.1.0 Release 1999)*
- ETSI TS 135 205 V4.0.0 (2001-05): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions  $f1, f1^*, f2, f3, f4, f5$  and  $f5^*$ ; Document 1: General (3GPP TS 35.205 version 4.0.0 Release 4)*
- ETSI TS 135 205 V5.0.0 (2002-06): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions  $f1, f1^*, f2, f3, f4, f5$  and  $f5^*$ ; Document 1: General (3GPP TS 35.205 version 5.0.0 Release 5)*
- ETSI TS 135 206 V5.0.0 (2002-06): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions  $f1, f1^*, f2, f3, f4, f5$  and  $f5^*$ ; Document 2: Algorithm specification (3GPP TS 35.206 version 5.0.0 Release 5)*
- ETSI TS 135 206 V4.0.0 (2001-06): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions  $f1, f1^*, f2, f3, f4, f5$  and  $f5^*$ ; Document 2: Algorithm Specification (3GPP TS 35.206 version 4.0.0 Release 4)*
- ETSI TS 135 207 V4.0.0 (2001-06): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions  $f1, f1^*, f2, f3,$*

*f4, f5 and f5\**; Document 3: Implementors' Test Data (3GPP TS 35.207 version 4.0.0 Release 4)

- ETSI TS 135 207 V5.0.0 (2002-06): *Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1\*, f2, f3, f4, f5 and f5\**; Document3: Implementors' test data (3GPP TS 35.207 version 5.0.0 Release 5)

### **US National Institute of Standards and Technology**

- FIPS Pub 83: *Guideline on User Authentication Techniques for Computer Network Access Control*
- FIPS Pub 190: *Guideline for the use of Advanced Authentication Technology Alternatives*
- FIPS Pub 196: *Entity Authentication using Public Key Cryptography*
- NIST Spec Pub 800-9: *Good Security Practices For Electronic Commerce, Including Electronic Data Interchange*
- NCSC-TG-017: *A Guide to Understanding Identification and Authentication in Trusted Systems*

### **Internet Engineering Task Force**

- RFC 1411: *Telnet Authentication: Kerberos Version 4*
- RFC 1412: *Telnet Authentication: SPX*
- RFC 1413: *Identification Protocol*
- RFC 1414: *Identification MIB*
- RFC 1416: *Telnet Authentication Option*
- RFC 3244: *Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols*
- RFC 1510: *The Kerberos Network Authentication Service (V5)*
- RFC 1734: *POP3 AUTHentication command*
- RFC 1828: *IP Authentication using Keyed MD5*
- RFC 1961: *GSS-API Authentication Method for SOCKS Version 5*
- RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 2015: *MIME Security with Pretty Good Privacy (PGP)*
- RFC 2025: *The Simple Public-Key GSS-API Mechanism (SPKM)*
- RFC 2069: *An Extension to HTTP: Digest Access Authentication*
- RFC 2082: *RIP-MD5 Authentication*
- RFC 2085: *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2138: *Remote Authentication Dial In User Service (RADIUS)*

### **Institute of Electrical Engineers**

- IEEE 802.10: *Standards for interoperable LAN/MAN Security (SILS) and supplements: Key Management (Clause 3), IEEE Std 802.10c-1998 Security Architecture Framework (Clause 1), IEEE Std 802.10a-1999*

## A.2 Passwords

### Internet Engineering Task Force

- RFC 1929: *Username/Password Authentication for SOCKS V5*
- RFC 1760: *The S/KEY One-Time Password System (SKEY)*
- RFC 2289: *A One-Time Password System (OTP)*

### US National Institute of Standards and Technology

- FIPS Pub 112: *Standard on Password Usage*

### US National Computer Centre

- CSC-STD-002-85: *Password Management Guidelines*

## A.3 Biometrics

Though there are very few issued standards on biometrics there are numerous groups carrying out activities which could lead to the development of useful standards:

### International Organisation for Standardisation and Electrotechnical Commission (ISO/IEC)

- ISO/IEC/JTC1/SC17 work groups:
  - WG1: *Physical Characteristics of Smart Cards (e.g. location of fingerprint sensor on card)*
  - WG3: *Machine readable travel documents*
  - WG4: *Smart Cards: ISO/IEC 7816 Personal verification through biometrics*
  - WG10: *Motor Vehicle Driver Licenses: Biometrics and Encryption*
  - WG11: *Biometrics: development of BioAPI and CBEFF (see below) into ISO standards*
- ISO/IEC/JTC1/SC 37: The aim of SC37 is to accelerate the development and adoption of Biometrics standards such as BioAPI and CBEFF through the ISO process.

### ANSI/NIST

- ITL-2000: *Data Format for the interchange of Fingerprint, Facial and Scar Mark/Tattoo*
- X9.84: *Biometrics Management and Security for the Financial Services Industry*
- CBEFF: *Common Biometric Exchange Format*
- BioAPI version 1.1: *Application Programming Interface defines a generic way of interfacing to a broad range of biometric technologies*
- B10.8/AAMVA: *Driving Licenses and Identification. Format for fingerprint minutiae on Driving Licenses*
- Various other ANSI/NIST activities include Performance Testing Methodologies, Assurance, Protection Profiles, and Best Practices.

### Other Organisations/Activities

- **Biovision.** A European Union funded initiative conceived in Framework 5, the programme being carried out in Framework 6. The aim is to produce a “road map” for Biometrics.

- **UK Government.** The UK Biometrics User Group comprising a group of vendors, standards developers and users is organised by the UK National Technical Authority for Information Security (CESG) and mainly funded by the Office of the e-Envoy. The group includes representatives from the US, Canada and Germany. It is active in developing Performance Standards, Best Practice guidance, Protection Profiles and Common Criteria Evaluation Methodology. It is intended that Protection Profiles and Common Criteria may be issued under the ISO Common Criteria standard in due course. Discussions are taking place between the US Biometrics Office to attempt to rationalise the UK developed Protection Profiles and the US Protection Profiles.
- **Biometric Consortium.** A US government based group acting as a focal point for research, development, testing evaluation and application of biometric-based personal identification and verification technologies.
- **US Government.** In the US the NSA and the DoD carry out research into Biometrics. The DoD has established the Biometrics Management Office to ensure the availability of biometrics technologies within the DoD.

#### **A.4 Digital Certificates**

##### **International Organisation for Standardisation and Electrotechnical Commission (ISO/IEC)**

- ISO/IEC 9594-8: *Directory Authentication*, the ISO/IEC version of the CCITT X.509 standard

##### **European Standards Committee (CEN)**

###### Workshop Agreements

- CWA 14167-1:2001: *E-Trustworthy Systems: System Security Requirements*
- CWA 14167-2:2002: *E-Trustworthy Systems: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)*
- CWA 14167-3: *E-Trustworthy Systems: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP)*

##### **European Telecommunications and Standards Institute (ETSI)**

###### Technical Specifications

- ETSI TS 101 456 ver. 1.2.1: *Policy requirements for Certification Authorities issuing Qualified Certificates*
- ETSI TS 102 042: ver. 1.1.1: *Policy requirements for certification authorities issuing public key certificates*
- ETSI 101 862: ver. 1.2.1: *Qualified certificate profile*

##### **Internet Engineering Task Force**

- RFC 1422: *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*
- RFC 2693: *SPKI Certificate Theory*
- RFC 3039: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*

## ANSI

- ANSI X9.30: *Digital Signature Standard, provides details of the Digital Signature Standard promulgated as FIPS 186*
- ANSI X9.45: *Authorisation Certificates*
- ANSI X9.55: *Certificate Extensions for X9*
- ANSI X9.57: *Certificate Management techniques for public key certificates used in the financial sector*

## US National Institute of Standards and Technology

- FIPS Pub 196: *Entity Authentication using Public Key Cryptography*
- NIST Spec Pub 800-15: *Minimum Interoperability Specifications for PKI Components (MISPC)*

## RSA Public key Cryptography Standards

- PKCS #6: *Extended Certificate Syntax, a syntax for extended certificates based upon X.509*
- PKCS #9: *Selected Attribute Syntax for PKCS #6 extended certificates, PKCS #7 digitally signed messages, and PKCS #8 private-key information*
- PKCS #10: *Certificate Request Syntax. describing a syntax for certification requests*

## A.5 Smart Cards

### International Organisation for Standardisation and Electrotechnical Commission (ISO/IEC)

- ISO/IEC 7816: *Identification cards – Integrated circuit(s) cards with contacts*. A ten-part standard addressing the physical characteristics of smart cards. Details can be found at <http://www.iso.ch/iso/en/>.
- ISO/IEC 10202: *Financial Transaction Cards – Security Architectures of Financial Transaction Systems using Integrated Circuit Cards*. An eight part standard which specifies techniques for the protection of integrated circuit cards used in financial transactions, through the whole of life from their manufacture and issue to card termination.

### European Standards Committee - Information Society Standardisation System (CEN/ISSS)

The following standards (European Norms) have been issued by CEN.

- EN 726: *Identification Card Systems – Telecommunications Integrated circuit cards and terminals*. A seven part standard comprising:
  - Part 1: *Systems Overview*
  - Part 2: *Security Framework*
  - Part 3: *Application independent card requirements*
  - Part 4: *Application independent card related terminal requirements*
  - Part 5: *Payment Methods*
  - Part 6: *Telecommunications features*
  - Part 7: *Security Module*
- EN 1038: *Identification Card Systems, Telecommunications applications- integrated circuit(s) card payphone*

- ENV 1257: *Identification card systems – Rules for Personal Identification Number handling in intersector environments*. A three part standards comprising:
  - Part 1: *PIN presentation*
  - Part 2: *PIN protection*
  - Part 3: *PIN verification*
- ENV 1284: *Identification card systems – Intersector rules for locking and unlocking of integrated circuit(s) cards*
- EN 1332: *Identification card systems – Man-machine interface*. A four part standard comprising:
  - Part 1: *Design principles for the user interface*
  - Part 2: *Dimensions and location of a tactile identifier for ID-1 cards*
  - Part 3: *Key Pads*
  - Part 4: *Coding of user requirements for people with special needs*
- EN 1362: *Identification card systems- Device interface characteristics – classes of device interfaces*
- EN 1375: *Identification card systems- intersector integrated circuit(s) card additional formats –ID –000 card size and physical characteristics*
- EN 1387: *Machine readable cards- Health care applications – Cards: general Characteristics*
- EN 1545: *Identification Card Systems – surface Transport Applications*. A two part standard comprising:
  - Part 1: *General data elements*
  - Part 2: *Transport payment related elements*
- EN 1546: *Identification card systems – Inter-sector electronic purse*. A four part standard comprising:
  - Part 1: *Definitions, concepts and structure*
  - Part 2: *Security Architecture*
  - Part 3: *Data elements and interchanges*
  - Part 4: *Data objects*
- CR 1750: *Identification Card systems – Inter-sector messages between devices and hosts – Acceptor to acquirer messages*
- ENV 1855: *Identification card systems – Inter-sector messages between devices and hosts – Acceptor to enquirer messages*
- EN 1867: *Machine-readable cards – Healthcare applications – Numbering system and registration procedure for issuer identifiers*
- EN ISO/IEC 7810: See ISO/IEC 7810 above.
- CR 13643: *Machine-readable cards – Healthcare applications – Logical data structures and concepts for different card technologies for use by patients in health applications*
- CR 13644: *Machine-readable cards – Healthcare applications – Logical organisation of data on healthcare professional cards*
- CR 13875: *Identification card systems – Inter-sector thin flexible cards – Security features*
- CR 13909: *Identification card systems – Inter-sector thin flexible cards – Acceptance criteria*
- ENV 14062: *Identification card systems – Surface transport applications – Electronic fee collection*. A two part standard comprising:
  - Part 1: *Physical characteristics, electronic signals and transmission protocols*

- Part 2: *Electronic fee collection – Message requirements*

The following Workshop Agreements are available from CEN:

- CWA 14174: *Financial transactional IC card reader (FINREAD)*. An eight part CWA standard comprising:
  - Part 1: *Business requirements*
  - Part 2: *Functional Requirements*
  - Part 3: *Security Requirements*
  - Part 4: *Architectural overview*
  - Part 5: *Download file format*
  - Part 6: *Definition of the virtual machine*
  - Part 7: *FINREAD card reader application programming interfaces (APIs)*
  - Part 8: *FINREAD client application programming interfaces (APIs)*
- CWA 13987: *Smart Card Systems - Interoperable Citizen Services - User Related Information* (based on DISTINCT). A three part CWA comprising:
  - Part 1: *Definition of User Related Information*
  - Part 2: *Implementation Guidelines*
  - Part 3: *Guidelines to Creating, Operating and Maintaining an Interoperable Network*

CEN is also working on the following smart card specifications (see the CEN web page <http://www.cenorm.be/iss>) for the latest status of these documents:

- CEN pr TS 1332-5: *Identification card systems – Man-machine – interface – Tactile identification of applications-embossed symbols for the differentiation of applications of ID1 cards*
- CEN pr TS IOPTA: *Identification card systems – Interoperable public transport applications – Ticketing applications*
- CEN pr TS 14062-3: *Identification card systems – Electronic fee collection – Part 3: Application and security aspects*
- CEN pr TS 14062-4: *Identification card systems – Electronic fee collection – Part 4: Test procedures*
- EN ISO/IEC 7810: *Identification cards – Physical characteristics*
- EN 13343-1: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-3 – Part 1 : Implementation Conformance Statement (ICS) proforma specification*
- EN 13343-2: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-3 – Part 2: Test suite structure and test purposes (TSS and TP)*
- EN 13343-3: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-3 – Part 3: Abstract test suite (ATS) and implementation for testing (IXIT) proforma specification*
- EN 13344-1: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-4 – Part 1 : Implementation conformance statement (ICS) proforma specification*
- EN 13344-2: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-4 – Part 2 : Test suite structure and test purposes (TSS and TP)*
- EN 13344-3: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-4 – Part 3: Abstract test suite (ATS) and implementation eXtra information for testing (IXIT) proforma specification*

- EN 13345-1: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-7 – Part 1: Implementation conformance statement (ICS) proforma specification*
- EN 13345-2: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-7 – Part 2: Test suite structure and test purposes (TSS and TP)*
- EN 13345-3: *Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-7 – Part 3: Abstract test suite (ATS) and implementation eXtra information for testing (IXIT) pro-forma specification*

#### Other CEN Activities

- CEN Technical Committees 224, 251 and 278 are carrying out application specific work on smart cards in the areas of healthcare, transport and people with special needs.
- CEN/ISSS Workshop FINREAD validated a set of technical specifications produced by a consortium of banking interests for a secure IC card reader for bankcard payments and remote banking services delivered over the Internet and open networks. CEN/ISSS Workshop Embedded FINREAD is now extending the specification to card acceptance devices linked to mobiles, PDAs and set-top boxes. The FINREAD specifications are available from the CEN web site for downloading – see A.5 for details.
- A new CEN/ISSS Workshop will shortly be announced for European Electronic Authentication, to cover a functional architecture and required IAS (Identification, authentication and electronic signature) characteristics for a European Public Identity using smart cards and other aspects related to multi-application cards and user best practice. This will take the major results of the Smart Card Charter activity and collaborate with similar work in Japan and the US.

### European Telecommunications and Standards Institute (ETSI)

ETSI is also carrying out a considerable amount of work under the Smart Card Project (EP SCP) approved in March 2000 to replace the SMG Technical Sub-Committee SMG9. EP SCP provides a central focus for the standardisation of a common integrated circuit (IC) card platform for 2G and 3G mobile communication systems. It also enables the participation of companies involved in standardisation work in 3GPP, 3GPP<sup>2</sup>, GAIT, T1P1, TR45 and other related activities.

The following lists technical reports issued and maintained by the smart card committee (EP SCP) and active work items. More information can be found on the SCP portal in the “Work Item Monitoring” window.

- ETSI TS 101 220 V6.0.0 (2003-02): *Smart Cards; ETSI numbering system for telecommunication application providers (Release 6)*
- ETSI TS 102 124 V6.0.0 (2003-02): *Smart Cards; Transport Protocol for UICC based Applications; Stage 1 (Release 6)*
- ETSI TR 102 151 V6.0.0 (2003-02): *Smart Cards; Measurement of Electromagnetic Emission of SIM Cards (Release 6)*
- ETSI TS 102 221 V3.6.0 (2002-03): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.5.0 (2002-03): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.5.0 (2001-10): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*

- ETSI TS 102 221 V4.4.0 (2001-10): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.0.0 (2000-09): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V3.1.0 (2001-01): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.0.0 (2001-01): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.2.0 (2001-02): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.1.0 (2001-02): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.3.0 (2001-05): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.2.0 (2001-05): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.4.0 (2001-07): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.3.0 (2001-07): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V3.9.0 (2002-10): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.8.0 (2002-10): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V5.2.0 (2002-10): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)*
- ETSI TS 102 221 V3.8.0 (2002-07): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.7.0 (2002-07): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V5.1.0 (2002-07): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)*
- ETSI TS 102 221 V3.7.0 (2002-05): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)*
- ETSI TS 102 221 V4.6.0 (2002-05): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 4)*
- ETSI TS 102 221 V5.0.0 (2002-05): *Smart cards; UICC-Terminal interface; Physical and logical characteristics (Release 5)*
- ETSI TS 102 223 V4.3.0 (2002-07): *Smart cards; Card Application Toolkit (CAT) (Release 4)*
- ETSI TS 102 223 V5.0.0 (2002-07): *Smart cards; Card Application Toolkit (CAT) (Release 5)*
- ETSI TS 102 223 V4.0.0 (2001-07): *Smart cards; Card Application Toolkit (CAT);(Release 4)*
- ETSI TS 102 223 V4.1.0 (2001-10): *Smart cards; Card Application Toolkit (CAT);(Release 4)*
- ETSI TS 102 223 V4.2.0 (2002-03): *Smart cards; Card Application Toolkit (CAT) (Release 4)*

- ETSI TS 102 224 V6.0.0 (2002-04): *Smart Cards; Security mechanisms for UICC based Applications - Functional requirements (Release 6)*
  - ETSI TS 102 225 V6.0.0 (2002-04): *Smart Cards; Secured packet structure for UICC based applications (Release 6)*
  - ETSI TS 102 225 V6.1.0 (2003-02): *Smart Cards; Secured packet structure for UICC based applications (Release 6)*
  - ETSI TS 102 226 V6.0.0 (2002-04): *Smart Cards; Remote APDU Structure for UICC based Applications (Release 6)*
  - ETSI TS 102 226 V6.1.0 (2002-07): *Smart Cards; Remote APDU structure for UICC based applications (Release 6)*
  - ETSI TS 102 226 V6.2.0 (2002-10): *Smart Cards; Remote APDU structure for UICC based applications (Release 6)*
  - ETSI TS 102 226 V6.3.0 (2003-02): *Smart Cards; Remote APDU structure for UICC based applications (Release 6)*
  - ETSI TS 102 230 V4.1.0 (2002-04): *Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)*
  - ETSI TS 102 230 V3.1.0 (2001-07): *Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 1999)*
  - ETSI TS 102 230 V4.0.0 (2001-07): *Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)*
  - ETSI TS 102 230 V3.2.0 (2003-02): *Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 1999)*
  - ETSI TS 102 230 V4.2.0 (2003-02): *Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification (Release 4)*
  - ETSI TS 102 240 V6.0.0 (2002-07): *Smart Cards; UICC Application Programming Interface and Loader Requirements; Service description; (Release 6)*
  - ETSI TR 122 907 V3.1.3 (2000-01): *Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts (3G TR 22.907 version 3.1.3 Release 1999)*
  - TS 101 220 Rel-5: *ETSI numbering system for telecommunication application providers*
  - TS 102 221 R99, Rel-4 and Rel-5: *UICC-Terminal interface; Physical and logical characteristics for developing system specific specifications over SCP*
  - TS 102 222 R99: *Administrative commands for telecommunications application compliant with ISO/IEC 7816*
  - TS 102 223 Rel-4 and Rel-5: *Card Application Toolkit (CAT):*
  - TS 102 224 Rel-6: *Security mechanisms for UICC based Applications - Functional requirements*
  - TS 102 225 Rel-6: *Secured packet structure for UICC based applications*
  - TS 102 226 Rel-6: *Remote APDU structure for UICC based applications*
  - TS 102 230 R99 and Rel-4: *UICC-Terminal interface; Physical, electrical and logical test specification corresponding to the core specification in TS 102 221*
  - TS 102 240 Rel-6: *UICC Application Programming Interface and Loader Requirements; Service description*
- SCP WG 1 work items:
- DTR/SCP-010287: *Terminal/UICC Interface noise immunity investigations*
  - RTS/SCP-010265 TS 102 221: *UICC-Terminal interface; Physical and logical characteristics for Rel-6; (class D voltage)*
  - DTR/SCP-000286: *Definitions for EMC measurements at UICC and ME*

- MI/SCP-00500: *Support for Large Files on the UICC*
- MI/SCP-00501: *Advanced UICC Communication*
- DTS/SCP-010008: *Transport Protocol for UICC based Applications*
- DTS/SCP-010009: *Architecture of the UICC*
- MI/SCP-010004: *UICCng (Next Generation UICC)*
- RTS/SCP-010010: *Specification for a third card size*

SCP WG 2 work items:

- RTS/SCP-020368 TS 102 222: *Sensitive data creation and initialisation for Rel-6*
- RTS/SCP-020001: *Update to GlobalPlatform Card Specification 2.1*
- MI/SCP-020001: *Study of available digital authentication specifications and their suitability for a Digital Identity Module on the UICC*

SCP WG 3 work items:

- DTS/SCP-030309 TS 102 241: *Java Card API for the UICC*

SCP has established direct liaisons with the relevant bodies of all committees involved in elaborating the common platform. In particular, SCP has direct liaisons with ETSI TC SEC involved in the specification of security matters. In addition, SCP has liaison with CEN TC224. Other liaisons with regional and national bodies remain to be identified.

For further information on SCP liaison activities see:

[http://webapp.etsi.org/Forawatch/HOME.ASP?TB=534&FIND=SEARCH\\_TB](http://webapp.etsi.org/Forawatch/HOME.ASP?TB=534&FIND=SEARCH_TB)

ETSI has also published numerous specifications regarding authentication for mobile telephony. The specifications may be downloaded from the ETSI web site (<http://www.etsi.org>).

## Personal Computer Smart Card Workgroup

The Personal Computer Smart Card workgroup comprising Groupe Bull, Hewlett Packard, Microsoft, Schlumberger and Siemens Nixdorf have developed a specification to facilitate interoperability in a PC environment. The specification is in eight parts as follows:

- Part 1: *Introduction and Architecture overview*
- Part 2: *Interface Requirements for Compatible Smart cards and Interface Devices*
- Part 3: *Requirements for PC-Connected Interface Devices*
- Part 4: *IFD Design Considerations and Reference Design Information*
- Part 5: *ICC Resource Manager Definition*
- Part 6: *ICC Service Provider Definition*
- Part 7: *Application Domain/Developer Design Considerations*
- Part 8: *Recommendations for Implementation of Security and Privacy ICC Devices*

## Smart Card Alliance

The Smart Card Alliance is a US/European association of various organisations including representatives from government, the finance, computing and telecommunications, healthcare, retail and entertainment sectors. The alliance aim is to encourage the use of smart cards through education programs, market research, advocacy and open forums (see <http://www.smartcardalliance.org>).

Eurosmart is a joint project between Europe and Japan with the aim of reinforcing co-operation between Europe and Japan. In particular it has developed a series of specifications for electronic purse applications, a glossary of smart card security terms and a set of Common Criteria protection profiles for smart cards (see <http://www.eurosmart.com>).

**e-Europe Smart Card (eESC) Initiative.**

The eEurope Smart Card (eESC) is an activity that was launched by the European Commission in 1999 in response to the eEurope initiative. The aim of eESC is to accelerate and develop the development of smart cards across Europe as the preferred method of access control to information society services. The activity is industry-driven but membership is open to developers and potential users of smart card based applications. Some 350 organisations have participated to the work.

The eESC have produced a detailed (50 documents in 11 volumes) a set of documentation called OSCIE (Open smartcard Infrastructure for Europe) with the basic aim of achieving an interoperable European smart card infrastructure based upon existing standards, workshop agreements including:

- ETSI/CEN Joint Workshops EESSII
- ISSS Workshops eURI, FASTEST
- FINREAD and Embedded FINREAD
- Common Criteria for smart card security
- NICSS Documents
- US NIST GSC documents.

Part of the OSCIE, addressing Identification, Authentication and Digital signature, will be addressed in an additional CEN/ISSS workshop.

Moreover eESC has initiated some pilot projects to implement cross border interoperability of National Electronic ID cards for eGovernment and Health Insurance.

eESC has joined forces with NICSS and NIST to set up a Global Forum on interoperability of smart card based Identification, Authentication and Digital signature functionality. The outputs of this group will be fed into ISO SC 17.

Eurosmart is the umbrella organisation for the smart card industry. It represents more than 90% of the producers of cards and chips for smartcards, both memory chips and microprocessor chip. It is the official representative of industry in different IST projects like RESET, a FP5 roadmap project on R&D needs in the smart card domain for the next ten years and Smart Meji, a joint project between Europe and Japan with the aim of reinforcing co-operation between Europe and Japan in the domain of contactless cards. It also has developed a series of Common Criteria protection profiles for smart cards (see <http://www.eurosmart.com>). eESC TB 3 is the working arm in the smart card security domain.

The following specifications have been extracted from the eESC web site at <http://www.eeurope-smartcards.org>.

Volume 1, Application White papers

- Part 1:
  - *E-government White paper on smart card applications and Evolution.*
  - *Analysis of Developments*
  - *Survey*
  - *Survey on secure smart card based eGovernment applications*
- Part 2:
  - *ePayments: Migration of EMV/CEPs. Status and roll out plans*
  - *EMV Migration Synchronisation in Europe*
  - *ePurse situation in Europe*
  - *EMV Country Summary*
  - *EMV Migration (pointer to web-based information)*
  - *ePayments – Blueprint on Mobile Payments*

- *ePayments: Mobile payment business requirements*
- *Public transport: smart card transport applications and evolution*
- *Healthcare: Smart Card evolution in the health area*

Volume 2, Best Practice Manual including requirements for cost transparency and privacy code of conduct for multi-application IAS.

Volume 3, Global IAS interoperability framework:

- *Part 1: Contextual and conceptual modelling*
- *Part 2: Requirements for IAS functionality*
- *Part 3: Recommendations for IOP specifications*
- *Part 4: Deployment strategies for generic IAS*

Volume 4, Public electronic identity, electronic signature and PKI:

- *Part 1: Electronic identity White Paper*
- *Part 2: Study on legal issues in relation to the use of public ID (electronic identity)*
- *Part 3: Bionorm, Need for specifications and standardisation to achieve Interoperability in the field of smart cards and biometrics*
- *Part 4: Requirements Specification. Visual ID on smart card used as a travel document*
- *Part 5: White Paper on PKI requirements*
- *Part 6: PKI pre-inventory report*
- *Part 7: Network Authentication module for Internet users – Electronic signature (Name-ES)*
- *Part 8: Requirements of terminal manufactures and convergence model for multiplatform access to services*
- *Part 9: Telecom operators' requirements*

Volume 5, Multi-applications:

- *Part 1: Legal Framework for multi-application cards and systems*
- *Part 2: Current and Future Business models for multi-application systems*
- *Part 3: Basic Multi-application technologies for cards and systems*
- *Part 4: MAS prerequisites; Core Cross-sectorial Architecture for Interoperable Multi-application systems*
- *Part 5: Integration of Multi-application systems*

Volume 6, Contactless Technology:

- *Part 1: White paper requirements on the interoperability of Contactless cards*
- *Part 2: White paper on Security and Threat Evaluation relating to Contactless cards*
- *Part 3: White paper on the Future roadmap for Contactless cards*
- *Part 4: White paper on the Certification of Contactless cards*
- *Part 5: Field Trials Specifications and guidelines for Contactless Card Systems*

Volume 7, generalised card Reader:

- *Part 1: Generalised Card Reader (relation to FINREAD and embedded FINREAD CWAs)*

Volume 8, Security and Protection Profiles:

- *Part 1: The Application of Attack Potential to Smart Cards (Common Criteria Supporting Document)*
- *Part 2: The Application of CC to Integrated Circuits (Common Criteria Supporting Document)*
- *Part 3: ETR-lite for Composition (Common Criteria Supporting Document)*
- *Part 4: ETR-lite for Composition: Annex A Composite smart card evaluation – Recommended best practice (Common Criteria Supporting Document)*

- Part 5: *ST-lite (Common Criteria Supporting Document)*
  - Part 6: *Guidance for smart card evaluation (Common Criteria Supporting Document)*
- Volume 9, Referenced Standards:

- Europe
  - *Executive Summaries and online pointer to EESSII standards and specifications*
  - *Area K "Application Interface for smart cards used as secure signature devices, WD1 V012 Draft*
  - *Summary and references to CEN/ISSS Workshop fastest.*
  - *Summary and references to FINREAD CWAs and CEN/ISSS Workshop*
  - *Embedded FINREAD Business plan*
- Japan
  - *Japan's NICSS specifications*
  - *Prerequisites*
  - *Framework Scheme Overview*
  - *Registration Operation Interface*
  - *Operation System Interface*
  - *Card Adapter Interface*
  - *Card Interface Specification*
  - *RW Common Card Interface*
  - *Operation Guideline*
  - *Contract & Covenants Example*
- USA
  - *USA GSA Specification NISTIR 6687/GSC-IS (v2.0)*

Volume 10, eESC glossary of Smart Card terms

### **US National Institute of Standards and Technology**

- NIST Spec Pub 500-157: *Smart Card Technology: New Methods For Computer Access Control*

### **RSA Public key Cryptography Standards**

- PKCS #11: *Abstract Token Interface (Cryptoki) defines the interface between tokens when used as a cryptographic subsystem*
- PKCS #15: *Cryptographic Token Information Format Standard Background*

### **Internet Engineering Task Force**

- RFC 2808: *The SecurID(r) SASL Mechanism. SecurID is a hardware token card product for end-user authentication*