ISO/IEC 24727 – Identification cards – integrated circuit card programming interfaces

A multi-part standard for identification, signature, and authentication services
Topics

- Background
- National committee
- International committee
- Uses
Background

- GSA survey on slow adoption of smart card technology in Federal workspace
  - Barriers to interoperability
  - Concerns over proprietary solution
- US proposal to develop international interoperability standard
  - Approval received August 2004
  - Basis of proposal from US government smart card work
- About the same time, HSPD-12 was issued (August 27, 2004)
  - Resulted in FIPS 201 and other NIST publications
INCITS (http://www.incits.org) is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT) encompassing storage, processing, transfer, display, security, management, organization, and retrieval of information.

- TAGs establish US positions
- Technical committees serve as TAG for various IT standards
  - Languages and databases
  - Media and Education
  - Security and ID
  - Storage
  - Information Services/Office/Text
INCITS B10 Technical committee

- B10 – Identification cards and related devices
  - US TAG to international committee
  - Responsible for smart card standards
  - ISO/IEC 7816, ISO/IEC 14443, ICAO...

- B10.12 – Integrated circuit cards and interfaces
  - Responsible for ISO/IEC 24727
  - US TAG to international work group
ISO/IEC JTC 1 SC 17
International Committee

- ISO/IEC JTC 1 Sub Committee 17 - Cards and personal identification
  - SC 17 Secretariat: UK British Standards Institute (BSI)
  - Secretary: Mr. Chris Starr, Chris.Starr@apacs.org.uk
  - SC 17 web site http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45144
SC 17 work groups

WG1 - PHYSICAL CHARACTERISTICS AND TEST METHODS FOR IDENTIFICATION CARDS
Physical characteristics, embossing, magnetic stripe, and test methods for conformance and card durability.

WG3 - MACHINE READABLE TRAVEL DOCUMENTS
To prepare a revised text of ISO 7501; monitor the standards referenced; consider and define standards for machine readable travel documents and related machine readable cards (see Recommendation 3 of N 379); co-ordination of JTC1 liaison with ICAO for maintenance of ICAO 9303, machine readable passports and related ICAO documents.

WG4 - INTEGRATED CIRCUIT CARDS WITH CONTACTS
To define specifications related to the Integrated Circuits Card with Contacts within the area of SC17.

WG5 - REGISTRATION MANAGEMENT GROUP

WG7 - FINANCIAL TRANSACTION CARDS THIS WORKING GROUP HAS BEEN STOOD DOWN
To revise ISO/IEC 7813 and its amendment 1 in accordance with SC17 resolution 365 and to carry out any further revisions as necessary.

WG8 - CONTACTLESS INTEGRATED CIRCUIT(S) CARDS, RELATED DEVICES AND INTERFACES
The scope of WG8 is to develop standards for the Contactless Integrated Circuit(s) Card which do not preclude the incorporation of other Standard technologies on the card.

WG9 - OPTICAL MEMORY CARDS AND DEVICES
Enhanced OMC technologies enabling more data capacity, fast access and high reliability based on existing standard technologies or new technologies. Software or programming interface for accessing OMC data contents. (Host application program will be able to use this interface for easier implementation. Access method software of OMCs application program.) Physical assignment and/or logical assignment for OMC media use. Logical data structures in OMCs data (file structure etc).

WG10 - MOTOR VEHICLE DRIVER LICENCE AND RELATED DOCUMENTS
Draft Terms of Reference: Standardization in the filed of Motor vehicle driver licences.

WG11 - Application of Biometrics to Cards and Personal Identification
Interoperability for interindustry and government applications using personal identification technologies, e.g. biometrics. Excludes generic biometrics as undertaken by SC37.
ISO/IEC JTC 1 SC 17 Work Group 4

- Responsible for ISO/IEC 24727, 7816, ...

- WG 4 Secretariat
  - France (AFNOR)
  - Secretary: Laurence Douville
    - laurence.douville@afnor.org
  - Chair: Jean-Yves Duveau
    - jean-yves-duveau@cartes-bancaires.com

- WG 4 meeting participants
  - Australia, France, Germany, Japan, USA
  - Netherlands, UK
  - CEN TC 224 WG 15 Convener
Cyber Security Standards Developers

**International**

- ISO
- IEC
- IETF
- ITU-T
- ICAO

ISO TC 68
Banking, Securities and Other Financial Services

ISO/IEC JTC 1
Information Technology

- SC 17
  Cards & Personal Identification
- SC 27
  IT Security Techniques
- SC 37
  Biometrics

OASIS
Liberty Alliance

**National**

- ANSI

- NIST/ITL
- X9 (US TAG - ISO TC 68)
- INCITS (US TAG - ISO/IEC JTC 1)
- IEEE
- NIST

- X9F
  Data & Information Security
- B10
  Identification Cards & Related Devices
- CS1
  Cyber Security
- M1
  Biometrics

Department of State
ISO/IEC 24727 – current status

- ISO/IEC 24727-6 (FDIS) Identification cards – Integrated circuit card programming interfaces – Part 6: Registration authority for authentication protocols for interoperability
ISO/IEC 24727 – miscellaneous

- ISO/IEC 24727 applications/users
  - Queensland Transport driver license
  - CEN TC 224 WG 15 European Union Citizen Card
  - German Health Card
  - European Health Card

- Recent NIST publication
  NISTIR 7811: Use of ISO/IEC 24727 Identification cards
  – Integrated circuit cards programming interfaces, Service Access Layer Interface for Identity (SALII): support for development and use of interoperable identity credentials

How do I get a copy of ISO standards?

- You can buy finalized standard at http://www.iso.org/iso/store.htm

- Also available at ANSI store
  - Discounted price if ISO standard adopted as national standard
  - ISO/IEC 24727 parts 1, 2, 3, & 4 adopted
  - Available for $30USD each
    http://webstore.ansi.org/
Teresa Schwarzhoff

U.S. Department of Commerce,
National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division

Gaithersburg, Maryland
Ph: 301.975.5727

teresa.schwarzhoff@nist.gov
Backup slides
ISO/IEC JTC 1 SC 17 Membership

<table>
<thead>
<tr>
<th>Participating countries</th>
<th>Observing countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenia (SARM)</td>
<td>Malaysia (DSM)</td>
</tr>
<tr>
<td>Australia (SA)</td>
<td>Netherlands (NEN)</td>
</tr>
<tr>
<td>Austria (ASI)</td>
<td>Norway (SN)</td>
</tr>
<tr>
<td>Belgium (NBN)</td>
<td>Poland (PKN)</td>
</tr>
<tr>
<td>Canada (SCC)</td>
<td>Portugal (IPQ)</td>
</tr>
<tr>
<td>China (SAC)</td>
<td>Romania (ASRO)</td>
</tr>
<tr>
<td>Czech Republic (UNMZ)</td>
<td>Russian Federation (GOST R)</td>
</tr>
<tr>
<td>Denmark (DS)</td>
<td>Singapore (SPRING SG)</td>
</tr>
<tr>
<td>Finland (SFS)</td>
<td>Slovakia (SUTN)</td>
</tr>
<tr>
<td>France (AFNOR)</td>
<td>South Africa (SABS)</td>
</tr>
<tr>
<td>Germany (DIN)</td>
<td>Spain (AENOR)</td>
</tr>
<tr>
<td>India (BIS)</td>
<td>Sweden (SIS)</td>
</tr>
<tr>
<td>Israel (SII)</td>
<td>Switzerland (SNV)</td>
</tr>
<tr>
<td>Italy (UNI)</td>
<td>USA ( ANSI</td>
</tr>
<tr>
<td>Japan (JISC)</td>
<td></td>
</tr>
<tr>
<td>Kenya (KEBS)</td>
<td></td>
</tr>
<tr>
<td>Korea, Republic of (KATS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Estonia (EVS)</td>
</tr>
<tr>
<td></td>
<td>Hungary (MSZT)</td>
</tr>
<tr>
<td></td>
<td>Iceland (IST)</td>
</tr>
<tr>
<td></td>
<td>Indonesia (BSN)</td>
</tr>
<tr>
<td></td>
<td>Iran, Islamic Republic of (ISIRI)</td>
</tr>
<tr>
<td></td>
<td>Ireland (NSAI)</td>
</tr>
<tr>
<td></td>
<td>Kazakhstan (KAZMEMST)</td>
</tr>
<tr>
<td></td>
<td>Lithuania (LST)</td>
</tr>
<tr>
<td></td>
<td>New Zealand (SNZ)</td>
</tr>
<tr>
<td></td>
<td>Serbia (ISS)</td>
</tr>
<tr>
<td></td>
<td>Thailand (TISI)</td>
</tr>
<tr>
<td></td>
<td>Turkey (TSE)</td>
</tr>
<tr>
<td></td>
<td>Ukraine (DSSU)</td>
</tr>
</tbody>
</table>
Useful references

- ASN.1 references
- POSIX reference
ASN.1 – Abstract Syntax Notation

- ISO/IEC 8825-1:2002 defines a set of Basic Encoding Rules (BER) that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding. ISO/IEC 8825-1:2002 defines also a set of Distinguished Encoding Rules (DER) and a set of Canonical Encoding Rules (CER) both of which provide constraints on the Basic Encoding Rules (BER). The key difference between them is that DER uses the definite length form of encoding while CER uses the indefinite length form. DER is more suitable for the small encoded values, while CER is more suitable for the large ones. It is implicit in the specification of these encoding rules that they are also used for decoding.
"ASN.1 - Communication between heterogeneous systems"
by Olivier Dubuisson
translated by Philippe Fouquart

The link to the book can be found here:
http://www.oss.com/asn1/dubuisson.html
POSIX®– Portable Operating System Interface


- ISO Abstract: ISO/IEC/IEEE 9945:2008 defines a standard operating system interface and environment, including a command interpreter (or "shell"), and common utility programs to support applications portability at the source code level. ISO/IEC/IEEE 9945:2008 is intended to be used by both application developers and system implementers and comprises four major components (each in an associated volume).