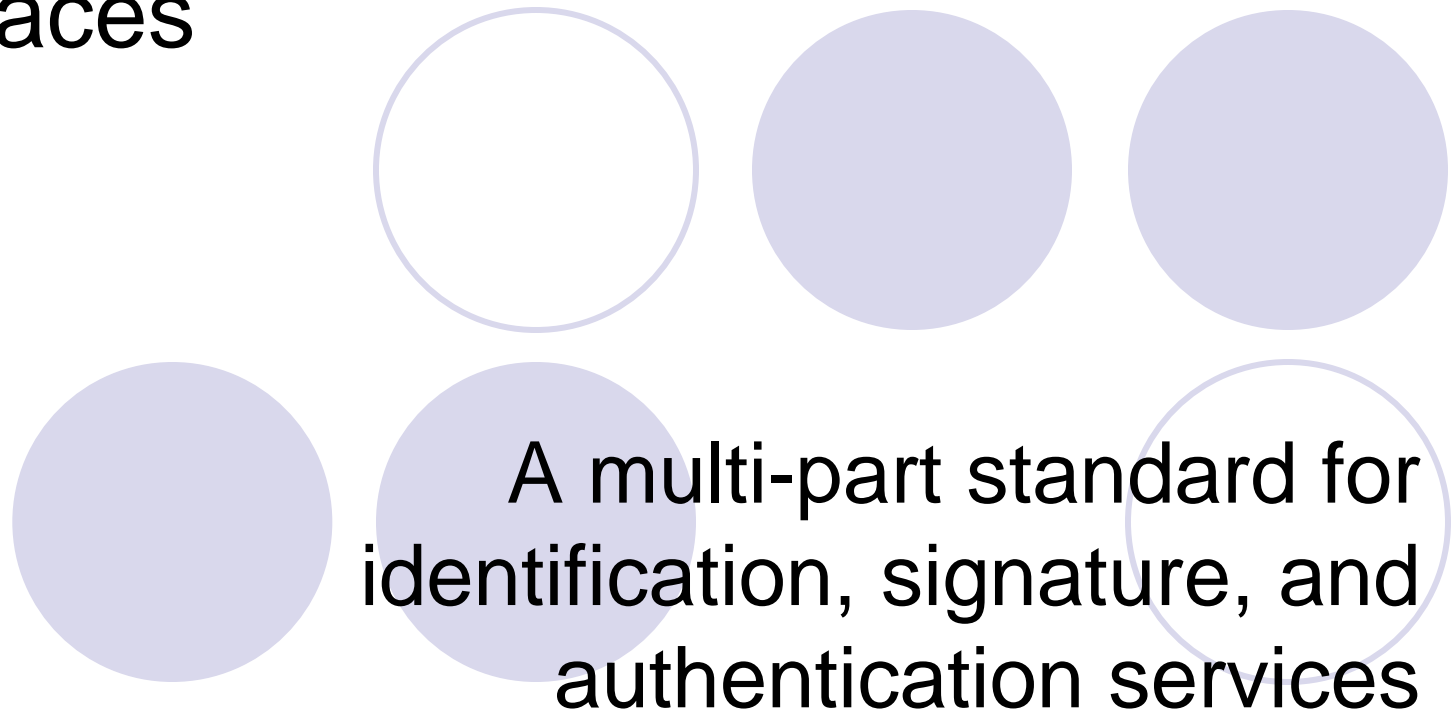


# ISO/IEC 24727 – Identification cards – integrated circuit card programming interfaces



A decorative graphic at the top of the slide consists of two groups of circles. The first group on the left has a solid light purple circle on the left and an empty light purple circle outline on the right. The second group on the right has a solid light purple circle on the left, an empty light purple circle outline in the middle, and a solid light purple circle on the right.

# 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

# InterNational Committee for Information Technology Standards (INCITS)

- 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.

# INCITS - national

- U.S. INCITS serves as ANSI's designated US Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1.
- 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](mailto: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](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

To serve as the RMG for ISO/IEC 7812 Parts 1 & 2 and ISO/IEC 7816-5. Responsibility for maintenance of ISO/IEC 7812 Parts 1 & 2. Responsible for Registration of Application providers under ISO/IEC 7816-5. To liaise, when necessary with Working Group 4 on matters relating to ISO/IEC 7816-5.

## 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 field 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.

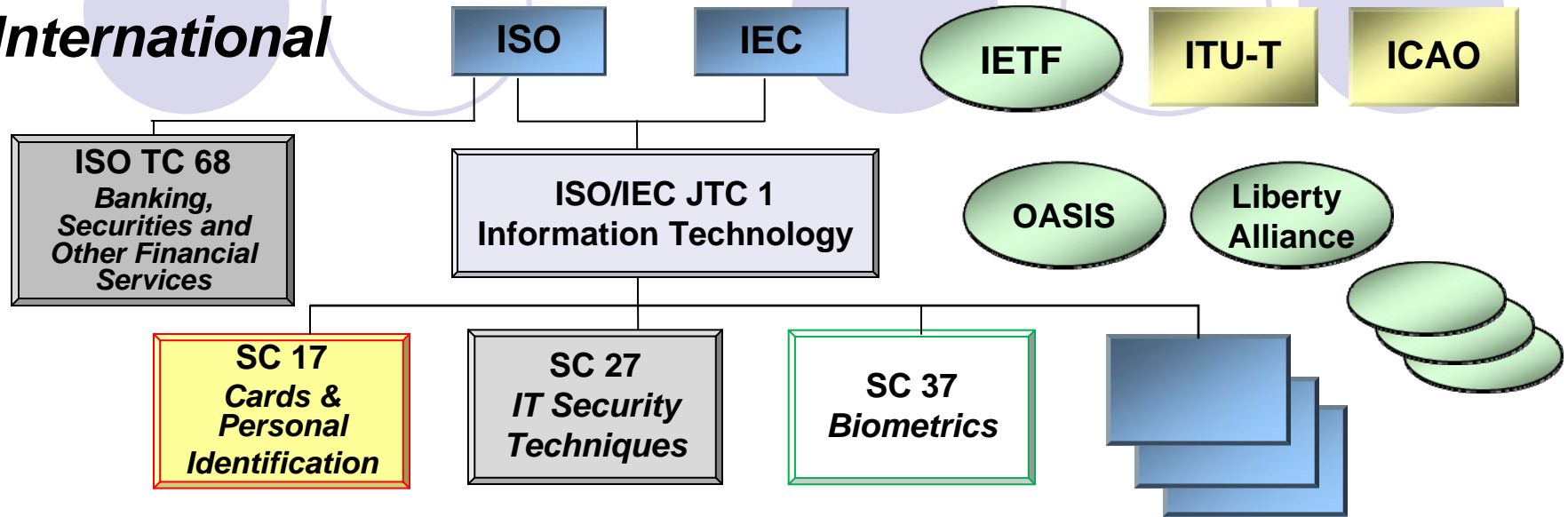


# ISO/IEC JTC 1 SC 17 Work Group 4

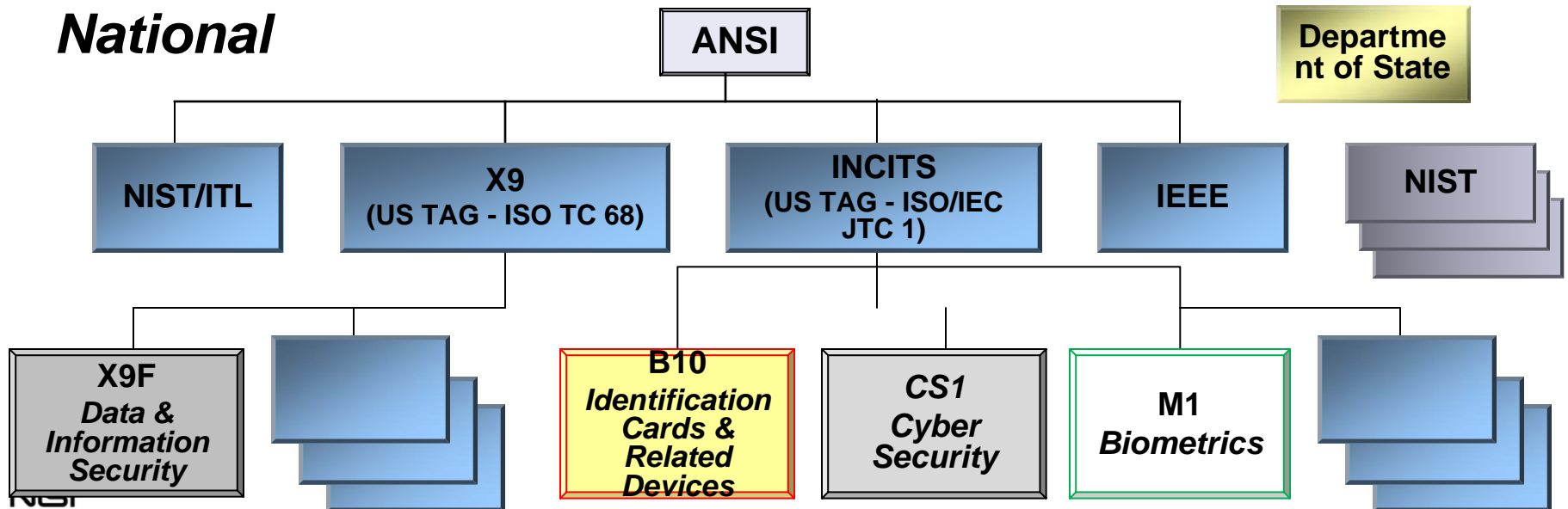
- Responsible for ISO/IEC 24727, 7816, ...
- WG 4 Secretariat
  - France (AFNOR)
  - Secretary: Laurence Douville
    - [laurence.douville@afnor.org](mailto:laurence.douville@afnor.org)
  - Chair: Jean-Yves Duveau
    - [jean-yves-duveau@cartes-bancaires.com](mailto:jean-yves-duveau@cartes-bancaires.com)
- WG 4 meeting participants
  - Australia, France, Germany, Japan, USA
  - Netherlands, UK
  - CEN TC 224 WG 15 Convener

# Cyber Security Standards Developers

## International



## National



# ISO/IEC 24727 – current status

- ISO/IEC 24727-1: 2007 Identification cards – Integrated circuit card programming interfaces – Part 1: Architecture
- ISO/IEC 24727-2:2008 Identification cards – Integrated circuit card programming interfaces – Part 2: Generic card interface
- ISO/IEC 24727-3:2008 Identification cards – Integrated circuit card programming interfaces – Part 3: Application interface
- ISO/IEC 24727-4:2008 Identification cards – Integrated circuit card programming interfaces – Part 4: API administration
- ISO/IEC 24727-5 (FCD) Identification cards – Integrated circuit card programming interfaces – Part 5: Testing
- 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

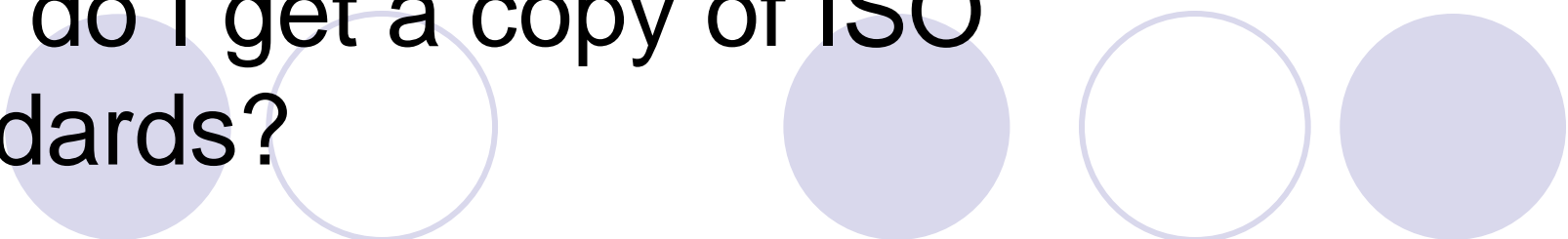
- Queensland Transport driver license
- CEN TC 224 WG 15 European Union Citizen Card
- German Health Card
- European Health Card

- 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

[http://csrc.nist.gov/publications/nistir/ir7611/nistir7611\\_use-of-isoiec24727.pdf](http://csrc.nist.gov/publications/nistir/ir7611/nistir7611_use-of-isoiec24727.pdf)

# How do I get a copy of ISO standards?

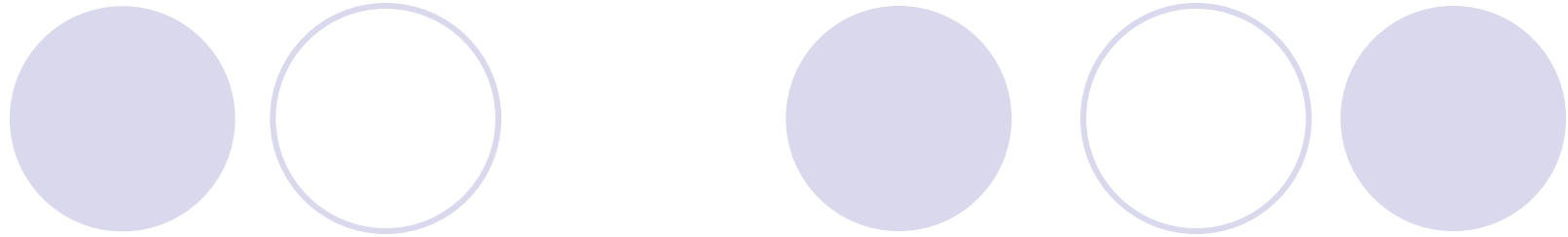


- You can buy finalized standard at <http://www.iso.org/iso/store.htm>

- **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/>



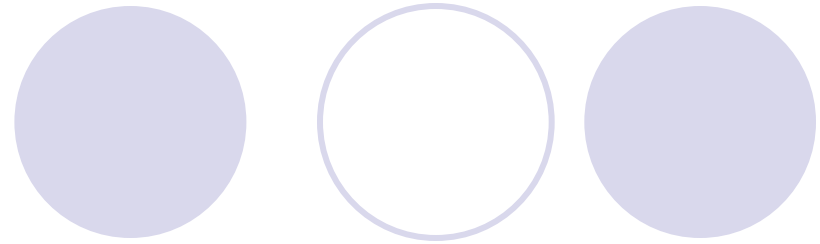
Teresa Schwarzhoff

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](mailto:teresa.schwarzhoff@nist.gov)

# Backup slides



# ISO/IEC JTC 1 SC 17 Membership

## Participating countries

Armenia (SARM)  
Australia (SA)  
Austria (ASI)  
Belgium (NBN)  
Canada (SCC)  
China (SAC)  
Czech Republic (UNMZ)  
Denmark (DS)  
Finland (SFS)  
France (AFNOR)  
Germany (DIN)  
India (BIS)  
Israel (SII)  
Italy (UNI)  
Japan (JISC)  
Kenya (KEBS)  
Korea, Republic of (KATS)

Malaysia (DSM)  
Netherlands (NEN)  
Norway (SN)  
Poland (PKN)  
Portugal (IPQ)  
Romania (ASRO)  
Russian Federation (GOST R)  
Singapore (SPRING SG)  
Slovakia (SUTN)  
South Africa (SABS)  
Spain (AENOR)  
Sweden (SIS)  
Switzerland (SNV)  
USA (ANSI)

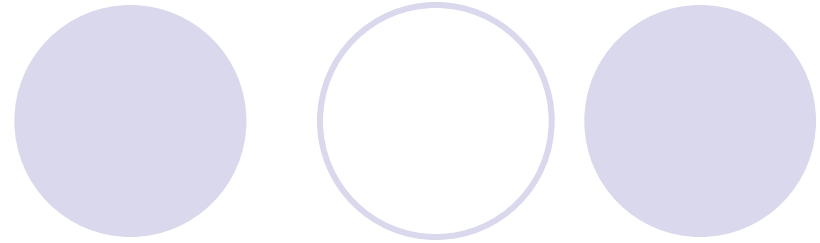
## Observing countries

Estonia (EVS)  
Hungary (MSZT)  
Iceland (IST)  
Indonesia (BSN)  
Iran, Islamic Republic of (ISIRI)  
Ireland (NSAI)  
Kazakhstan (KAZMEMST)  
Lithuania (LST)  
New Zealand (SNZ)  
Serbia (ISS)  
Thailand (TISI)  
Turkey (TSE)  
Ukraine (DSSU)



# Useful references

- ASN.1 references
- POSIX reference



# ASN.1 – Abstract Syntax Notation

- ISO/IEC 8825-1:2002 - Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- ISO/IEC Abstract: 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 Reference Book

"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/IEC 9945:2009 Information technology -- Portable Operating System Interface (POSIX®) Base Specifications, Issue 7
- 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).