Identity Management

Initiatives in identity management and emerging standards

Presented to Fondazione Ugo Bordoni
Rome, Italy

November 18, 2008

Teresa Schwarzhoff
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Please Note

The presentation material, written and spoken, expresses the opinions of the presenter, and does not necessarily express an official position of the United States Government.

Topics ….

U.S. national strategy for standardization

Identity Management Task Force Report 2008

Emerging interoperability standard

Innovation, security, and standards

Telegraph, Telephone, Internet, World Wide Web

- *new communication*
- *new computer technologies*
- *new business opportunities*
- *new forms of crime*

As the scale for innovation increases

- *the assurance on identity decreases (all things equal)*
- *security mechanisms decay*
- *standardization becomes increasingly important*

Perspective

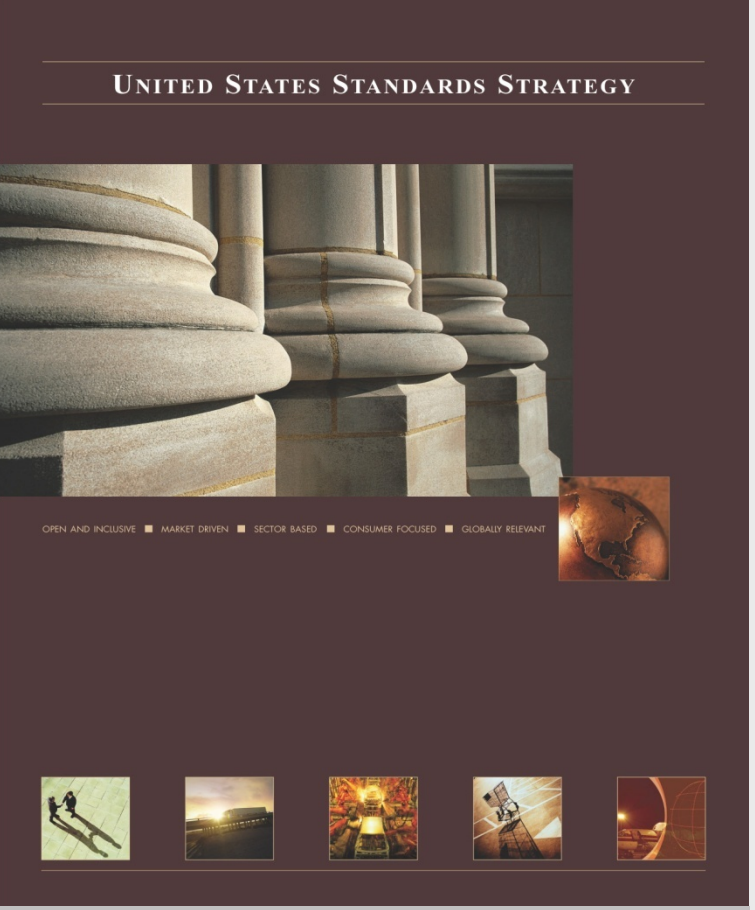
International, interoperable standards are strategic because they:

Enable positive co-dependencies that build markets

Define interoperability that preserves consumer choice

Promote connections among global IT systems

Prohibit dangerous practices and advances cybersecurity



1 – Strengthen participation by government in development and use of **voluntary consensus standards** through public/private partnerships

2 – Continue to address the environment, health, and safety in the development of **voluntary consensus standards**

3 – Improve the responsiveness of the standards system to the views and needs of consumers
4 – Actively promote the consistent worldwide application of internationally recognized principles in the development of standards.
5 – Encourage common governmental approaches to the use of voluntary consensus standards as tools for meeting regulatory needs
6 – Work to prevent standards and their application from becoming technical trade barriers to U.S. products
and services
7 – Strengthen international outreach programs to promote understanding of how **voluntary, consensus-based**, market-driven sectoral standards can benefit businesses, consumers and society as a whole
8 – Continue to improve the process and tools for the efficient and timely development and distribution of **voluntary consensus standards**
9 – Promote cooperation and coherence within the U.S. standards system
10 – Establish standards education as a high priority within the United States private, public and academic sectors
11 – Maintain stable funding models for the U.S. standardization system
12 – Address the need for standards in support of emerging national priorities

"United States Standards Strategy establishes a framework that can be used to … enhance consumer health and safety, …, and … advance U.S. viewpoints in the regional and international arena."

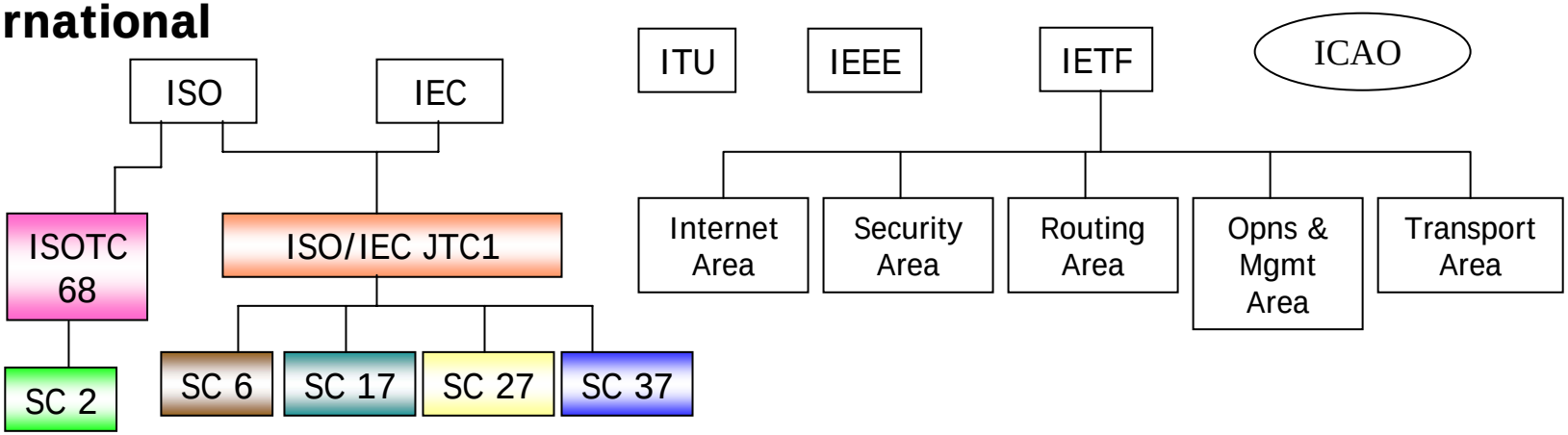
http://www.ansi.org/standards_activities/nss/usss.aspx?menuid=3

The United States standards strategy is framed by the use of

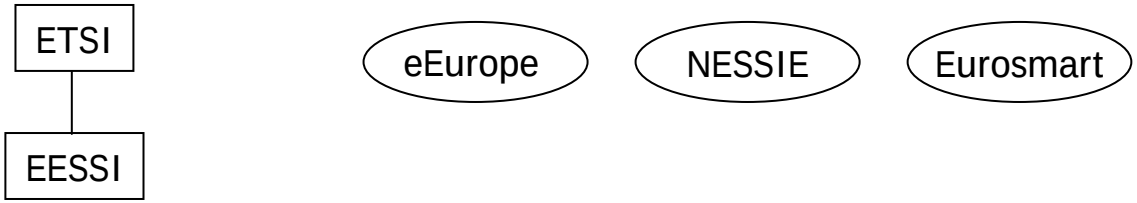
national and international consensus based voluntary standards.

Relevant standards activities

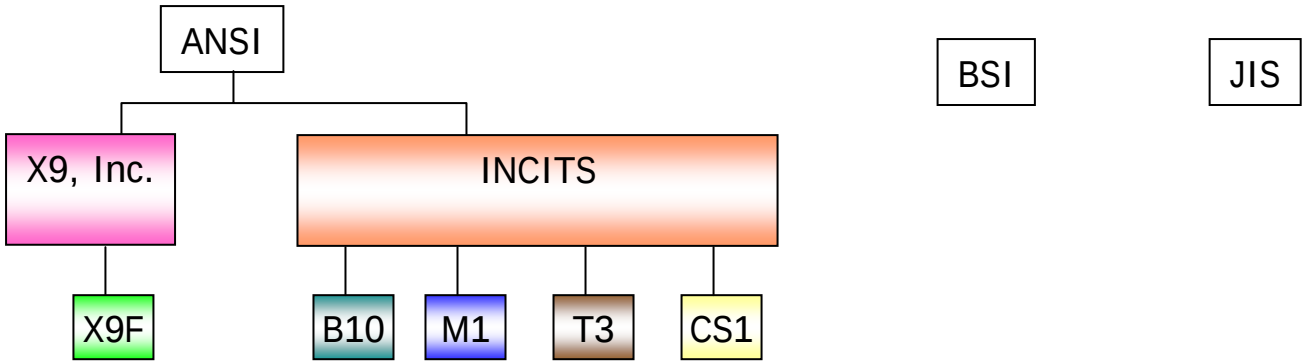
International



Regional



National



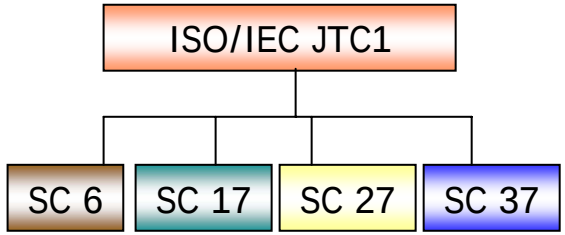
Relevant ISO/IEC JTC 1 sub-committees and the U.S. technical advisory group

SC 6 – Telecommunications and exchange between systems

SC 17 – Cards and personal identification

SC 27 – Security techniques

SC 37 - Biometrics



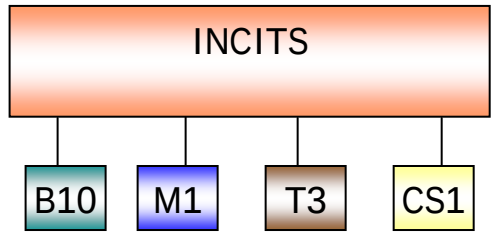
U.S. TAGS:

T3 – Open Distributed Processing

B10 – Identification Cards and Related Devices

CS1 – Cyber Security

M1 – Biometrics



http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/customview.html?func=ll&objId=327993

Why get involved with standards development?

Developing a national perspective for international bodies is the most important collaborative work for a country's TAG.

Attendance at national and international meetings brings experts together

Being part of the solution with an opportunity to influence outcome

It not just about a vote – it is also about a voice at the table.

Topics ….

U.S. national strategy for standardization

Identity Management Task Force Report 2008

Emerging interoperability standard

Highlights on U.S. Identity Management Activities

Office of Science and Technology Policy, Executive Office of the President

http://www.ostp.gov

National Science and Technology Council (NSTC)

http://www.ostp.gov/cs/nstc

NSTC Subcommittee on Biometrics and Identity Management

http://www.ostp.gov/cs/nstc

NSTC Subcommittee on Biometrics and Identity Management Task Force

Six month task force effort

Chaired by OSTP, NIST, and General Services Administration

Task force chartered to

- Provide an assessment of the current state of IdM in the U.S. government;
- Develop a vision for how IdM should operate in the future;
- Develop first-step recommendations on how to advance toward this vision.

Produced lengthy 216-page report

Main body of report is 79-pages

This report provides a identity management framework, recommendations, and considerations that will be the basis for future research activities and focus of identity management initiatives.

http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

Objective IdM Architectural Model

ID SPECIFIC "PRIVELEDGES" (Applications of ID in specific context), with *data unique to each*

Application/user Interface

IDENTITY MANAGEMENT "UTILITY"

ENTERPRISE ID SYSTEM

'NETWORK OF NETWORKS'
Digital ID Data Federation

Recommendations

1. Standards and guidance
    - Formal standards
    - Standard processes and interfaces
    - Interoperability
2. Architecture
    - Citizen centric, customer focused, service oriented
    - Federated IdM systems
    - Security
3. Additional, extensive list of recommendations and considerations

Recommendations/Considerations (1)

1. Public key technology

   Identity tools for seamless use

   Investigate capabilities that make it easier to use

   Investigate public key security

2. Privacy

   Develop tiers for levels of privacy

   Develop access control based on privacy tiers

   Personal Identifiable Information (PII)

3. Digital Identity Network of Networks

   Example: FIPS 201 - Personal Identity Verification

Recommendations/Considerations (2)

4. Identity applications interface

   Predictable services

   Research “plug and play” for ID applications

5. Secure authentication

   Research new methods of authentications

6. Scalable authentication mechanisms

   Research characteristics of large-scale IdM systems

7. Biometrics - have been studied in great detail, reference

   National Biometrics Challenge

   http://www.biometrics.gov/Documents/biochallengedoc.pdf

   Report of the Defense Science Board Task Force on Biometrics

   http://www.acq.osd.mil/dsb/reports/2007-03-Biometrics.pdf

Recommendations/Considerations (3)

8. Federation with systems outside the Federal government

   Methods for expressing policies with distinct architectures

9. Supply chain management

   Improve confidence in IT supply chain

10. Security vulnerability analysis

    IT complexity introduces vulnerabilities

11. Usability

    Research public access

    Move from “User Resistance” to “User Insistence”

Next steps

Prioritize recommendations

New administration

Stay tuned

Topics ….

U.S. national strategy for standardization

Identity Management Task Force Report 2008

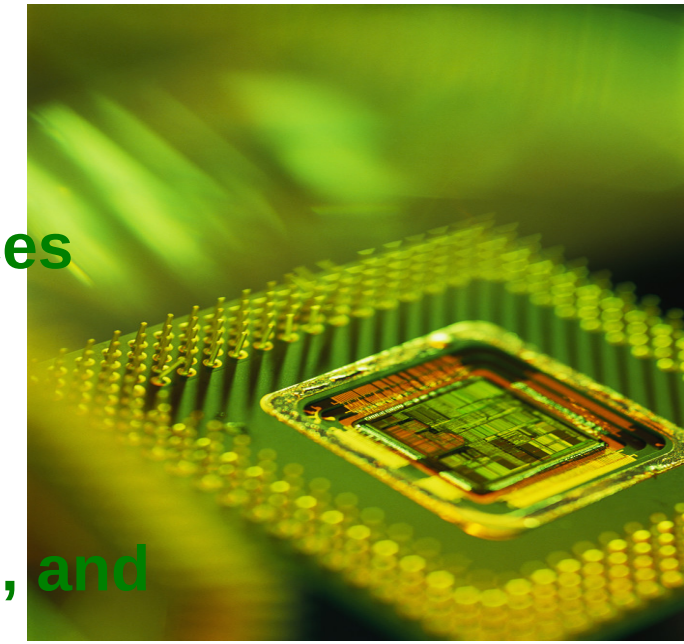
Emerging interoperability standard

Emerging interoperability standard

ISO/IEC 24727- Identification Cards - Integrated circuit cards programming interfaces

ISO/IEC 24727 multi-part standard

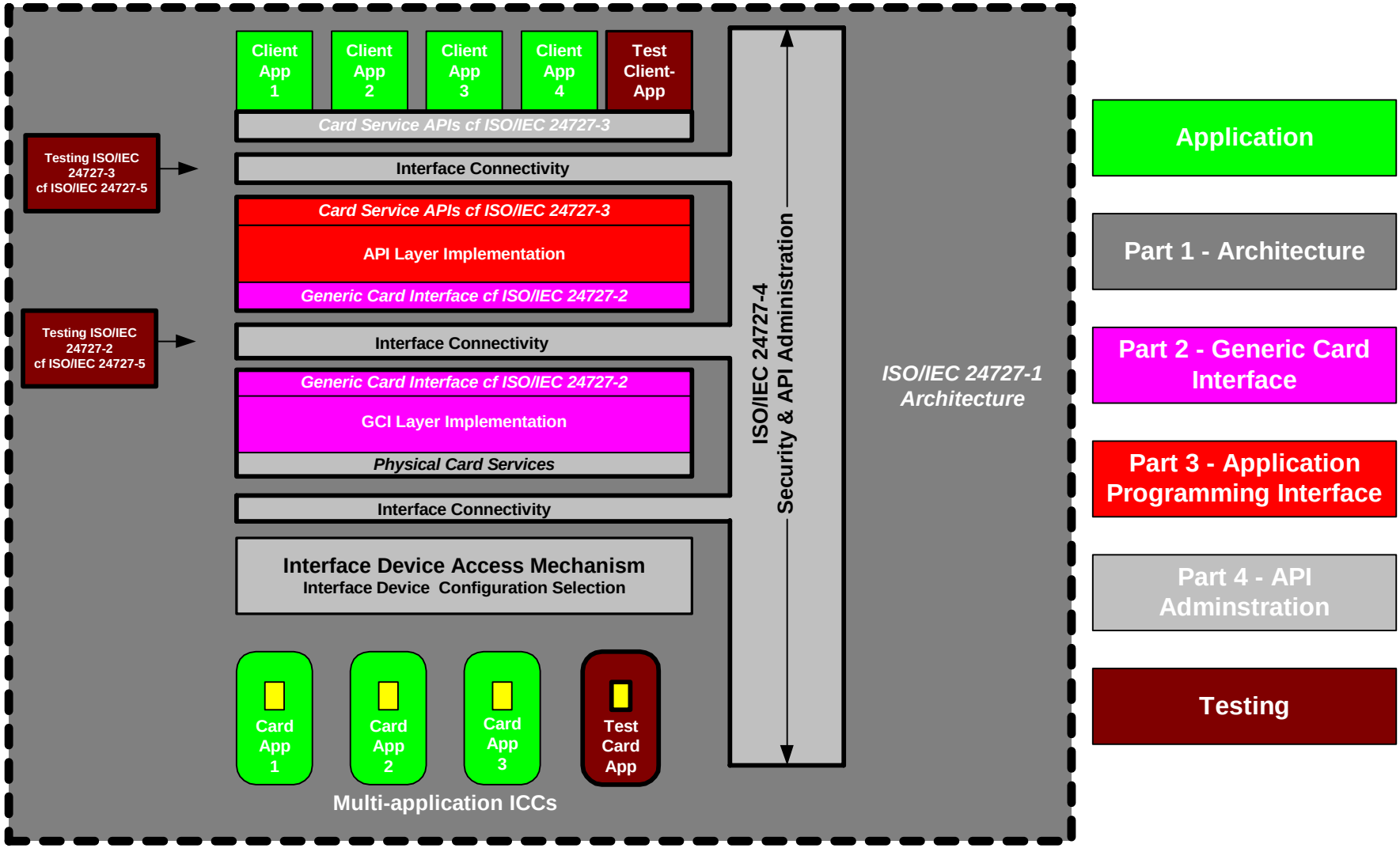
ISO/IEC 24727 – Identification Cards - Integrated circuit cards programming interfaces



- ✓Builds upon ISO/IEC 7816
- ✓**Focuses on services and interfaces**
- ✓Card type neutral
- ✓Contact and contactless agnostic
- ✓**eID: identification, authentication, and signature services**

✓✓✓ Goal: Independent implementations that are interchangeable

ISO/IEC 24727 is about interfaces for interoperability.



ISO/IEC 24727-1

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 1: Architecture

- Overarching framework
- Common terminology
- Logical architecture for framework

Status

- Published, available for purchase via your national body standards group or the ISO on-line store

ISO/IEC 24727-2

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 2: Generic card interface

- Common card interface
- 7816 toolkit fine-tuning
- Discovery mechanism
  - Card capability description (CCD)
  - Application capability description (ACD)

Status

- Published

ISO/IEC 24727-3

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 3: Application interface

- New territory for smart card standards
- Normative API/middleware
- Normative authentication protocols

Normative Services

- Connection
- Card application discovery and retrieval
- Identity
- Cryptographic
- Authorization

Status

- Soon to be published

Example of actions for a service found in ISO/IEC 24727-3:

Connection service

Initialize

Terminate

CardApplicationPath

CardApplicationConnect

CardApplicationDisconnect

CardApplicationStartSession

CardApplicationEndSession

Authentication protocols

PIN

password

symmetric key

asymmetric key

digital certificate

biometric image or template

pair of symmetric keys; e.g., one for encryption and one for message authentication code (MAC) generation

Name of authentication protocol	General definition of protocol
ASYMMETRIC INTERNAL AUTHENTICATE	Fetch certificate Send challenge to be signed (on-card) Validate (off-card) signature based on certificate
ASYMMETRIC EXTERNAL AUTHENTICATE	Fetch challenge Sign (off-card) and validate signature (on-card)
SYMMETRIC INTERNAL AUTHENTICATE	Send challenge to be signed (on-card) Validate signature (off-card)
SYMMETRIC EXTERNAL AUTHENTICATE	Fetch challenge Sign challenge (off-card) Validate signature (on-card)
COMPARE	Match input parameter with marker
PIN COMPARE	Match input parameter with marker and limiting number of incorrect compares – reset on successful compare
BIOMETRIC COMPARE	Translate input parameter to template form and compare with base template
SYMMETRIC KEY NONCE	Mutual authenticate of card-application and client-application plus generation of session keys
ANYBODY	NULL authentication protocol

ISO/IEC 24727-4

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 4: API administration

- Implementation details of Part 2 and Part 3 interactions
- Normative security architecture and stack configurations
- Normative IFD API
- TLS protocol

Status

- Published

ISO/IEC 24727-5

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 5: Testing

Developed tests as technical text matured

Testing levels with a modular approach

Status

- Second committee draft ballot – Nov – Dec 2009

Some words about testing

Conformity testing is not easy

- Minimize burden on suppliers
- Consider tendency for broad conformity requests from customers during procurement processes
- Cognizance of testing cost burden
- Multiple product providers and interoperability goals

First attempt at ISO/IEC 24727-5 yielded unmanageable testing document (over 10,000 pages half way through the process)

Refocused testing: Address what is needed to render API

Conformity testing - two phases

- Phase I: Self assertion for initial period of time
- Phase II: Conformity test program

ISO/IEC 24727-6

ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces – Part 6: *Registration authority procedures for the authentication protocols for interoperability*

- Future ISO/IEC 24727 authentication protocols
- Registration of use
- RA streamlines introduction of new normative authentication protocols
- Lead: Standards Australia Global

Status

Final committee draft Nov-Dec 2009

Summary: ISO/IEC 24727 Identification Cards - Integrated circuit cards programming interfaces

Part 1: *Architecture*

- Framework, common terminology

Part 2: *Generic card interface*

- ISO/IEC 7816 fine-tuning
- Discovery

Part 3: *Application interface*

- Basic services and actions
- Authentication protocols

Part 4: *API administration*

- Security models, stacks
- IFD API

Part 5: *Testing*

Part 6: *Registration authority procedures for the authentication protocols for interoperability*

- Registering future authentication protocols and ISO/IEC 24727 users

Who is using the standard?

Australia

- Australian smartcard framework
- Queensland drivers license – with other AU territories to follow

Europe

- EU Citizen Card (~480M)
- German health card
- German ID card

US

- Consider standard interfaces for future, diverse applications using PIV systems and non-PIV initiatives

Current status

Part 1: *Architecture*

- Published January 2007

Part 2: Generic card interface

- Published September 2008

Part 3: Application interface

- Final ballot closed this week, anticipate publication in November 2008

Part 4: API administration

- Final ballot passed this month, published November 2008

Part 5: Testing

- Initial ballot passed but agreed to launch second committee draft ballot
- Second CD ballot text anticipated in November 2008

Part 6: Registration authority procedures for the authentication protocols for interoperability

- Initial CD passed
- Final committee draft text and ballot in November 2008

Current status

Part 1: *Architecture*

- Published **January 2007**

Part 2: Generic card interface

- Published **September 2008**

Part 3: Application interface

- Final ballot closed this week, anticipate publication in **November 2008**

Part 4: API administration

- Final ballot passed this month, publication **November 2008**

Part 5: Testing

- Initial ballot passed but agreed to launch second committee draft ballot
- Second CD ballot text anticipated in November 2008

Part 6: Registration authority procedures for the authentication protocols for interoperability

- Initial CD passed
- Final committee draft text and ballot in November 2008

With the publication of parts 1, 2, 3, and 4 suppliers have a complete specification.

It is not perfect but it is ready to apply.

Thank you.

Teresa.Schwarzhoff@nist.gov
+ 1 301.975.5727