ISO/IEC 24727
General Concepts & Terminology
ISO/IEC 24727

An international standard aimed at IAS system INTEROPERABILITY
Token Based IAS Systems

Identification
- Trusted, personal store for identity based information
- Access limited by authenticated identity requirement

Authentication
- Perform trusted protocols to verify identity assertion
- Hold secret keys and biometrics used to authenticate identity

Signature
- Perform trusted encryption operation (digital signature)
- Hold secret keys used to perform encryption operation
- Verify signatures (including digital certificates)
IAS Token Triangle

- **Bearers**
  - Identify
  - Trust
  - Verify

- **Issuers**
- **Services**
Creation of a Trust Platform

1. Gather Personalization Information
2. Generate Public and Private Key on the Card
3. Trust Certificate Request with Personalization Information
4. Trust Approval
5. Trust Certificate
6. Write Certificate and Personalization Data to the Card
Value of Smart Card Tokens in Public Key Cryptography

• Hardware security - Tamper-resistant
• Portable and personal
• Biometric marker storage (enhanced personal privacy)
• Private Key storage
• Digital ID (Certificate) storage
• Encryption/decryption [careful about export]
• Key generation
Utility of Token Based IAS

- Provide strong authentication of Identity
- Confirm actions based on Identity (signing)
- Trusted conveyance of sensitive information
  - Physical address
  - Birth date (age)
  - Logical addresses (telephone & e-mail)
- Trusted connection of Identity and Information
  - Driver License credential
  - Social Security credential
  - Credit Card credential
Use Cases: IAS Services

- Authenticate your identity to log-in to this computer platform.
- Sign this receipt to prove that you received it.
- I’m a pharmacist, tell me your prescription medications.
- I’m a police officer, prove to me you’re a licensed driver.
- Store this document exclusively for me.
- Authenticate your identity to open this office door.
- Authenticate your identity to start this car.
- Prove to me you’re an employee of this company.
- Prove to me you’re old enough to purchase liquor in this bar.
Potential IAS Tokens

- U.S. Government ID Cards (CAC & PIV)
- Queensland Driver License
- First Responder Authentication Credential
- Texas Driver License
- Transport Cards (RIS)
- United Kingdom Passport
- State of Texas Employee Badge
- Federal Employee Health Care Identification Card
- National ID Cards
Personal Token System Paradigm

Host Based Program

Client-Application (Client)

Sentinel System

Request

Response

Card-Application (Server)

Smart Card Based Program

Personal Token
Absent a single, all encompassing identification system

Multiple identification systems are formed based on multiple foundations of trust
Utility suggests...

Interaction systems should be able to use multiple identification systems
In other words...

Interaction systems and identification systems should **INTEROPERA**TE
INTEROPERABILITY IS THE DOMAIN OF ISO/IEC 24727
Interoperation

Department of Defense

Middleware

Department of State

Middleware

PIV Card
Vendor B Card

PIV Card
Vendor A Card

PIV Card
Vendor A Card

Electronic Passport

PIV Card
Vendor B Card

Electronic Passport

Electronic Passport

PIV Card
Vendor A Card
Full Interoperability

The Goal of ISO/IEC 24727

Applications become Card & Middleware Independent
IAS In The Commercial Marketplace

Interoperability Middleware Establishes A Framework That Allows Multiple System Cards To Be Used

- Neighborhood Convenience Store
- Vacation Drug Store
- Middleware
- NY Driver License
- Texas Driver License
- Texas Driver License
- Canada Electronic Passport
- NY Driver License
- UK Electronic Passport
- US Electronic Passport
- Texas Driver License

ISO/IEC Workshop December 1-3, 2009
Interoperability Goals

- Re-use of Middleware and Tokens
- Independence of Middleware
- Independence of Tokens
- Independence of Token administration
- Independence of component certification procedures
Interoperability Mechanisms

- **Definition:** Independent implementations are interchangeable
- **Based on:**
  - Formally defined interfaces
  - Common semantics
  - Discoverability
  - Extensibility
  - Backward compatibility
  - Conformance testing
- **Resulting in:**
  *Flexible stack configurations with interoperable components*
Formally defined interfaces

- Application programming interface: API
- Network connectivity interface: TC API
- Smart card access interface: IFD API
- Generic smart card interface: GCI
Distinct Problem Domains

- Host computer application domain
  - aimed at a particular problem
    e.g. access, finance, health services
  - usage (end-user) oriented

- Token computer application domain
  - constrained resources
  - aimed at a specific problem (security)
  - technically (trust) oriented
Distinct Naming Domains

- Host Application seeks to deal with people through social information (name, address, age, SSN, education, capabilities, etc.)

- Token application seeks to deal with people through resource information (directories, files, records, tags, etc.)

- Function of ISO/IEC 24727 is to translate between these domains.
Characteristics of API (ISO/IEC 24727-3: Application Interface)

- Client-application (host computer) centric
- Formal definition (ASN.1)
- Provide use of token through host methods
- Establish semantics via Model of Computation (MOC)
- Allow for token administration
- Provide MOC level discoverability mechanisms
- Extensible
Characteristics of TC API
(ISO/IEC 24727-4: API Administration)

- Client-application independent
- Use existing standards for communications
- Connectivity between client-application and card-application
- Secure channel between client-application and card-application
- Security properties of the channel established by client-application
Characteristics of IFD API
(ISO/IEC 24727-4: API Administration)

- Card access via platform neutral semantics
- Card access via different interface devices
- Anticipate evolving platforms and interface devices
- Exclusive or shared access to card
- Support for card initialization (reset)
- Secure, network access to local card resources
Characteristics of GCI
(ISO/IEC 24727-2: Generic Card Interface)

- Token centric
- Uniform smart card command set capable of supporting the API
- Conform to ISO/IEC 7816-4, 8, 9, 13 and 15
- Allow translation of uniform (standard) command set to proprietary command sets
Common Model of Computation Semantics

- Card-Application
- Service
- Action
- Target

A well defined language syntax

- Access Control List (client-application centric)
- Access Control Rule (card-application centric)
Common Infrastructure Semantics

- Card-application uniquely identifiable across a network environment
- Client-application to card-application “path” uniquely identifiable
- Mapping between client-application & card-application name spaces
- Security state establishment through differential-identity
- Information storage / retrieval through named data service
- Information and process protection via access control lists
Common IAS Semantics

- Data-Set
  - Client-application named set of information with common security characteristics

- Data Structure for Interoperability (DSI)
  - Client-application named quantum of information stored in dataset – a storage mechanism for certificates

- Differential-Identity
  - Mapping of client-application named entities to card-application “marked” entities allowing authentication via standard protocols

- Cryptographic Services
  - Protected Sign, VerifySignature, Encipher, & Decipher procedures
Discoverability Concepts

- Client-Application “discovers” the semantic content of the card-application through the Part 3 API
  - Differential-identity information
  - Data-set information
  - Request fulfillment facilities (Sign, etc.)
  - Security state requirements
- Part 3 Layer creates and retrieves a mapping structure (Registry) between Part 3 concepts and Part 2 mechanisms
- Part 3 Layer creates and retrieves the Card Capability Description
- Part 3 Layer creates and retrieves the Application Capability Description
Client-application level discovery

- Through the ISO/IEC 24727-3 API, a client-application can learn:
  - What card-applications are on a card.
  - What differential-identities can be authenticated.
  - What data-sets are available in each card-application.
  - What DSI’s are available in each data-set.
  - What security state must be established to access a data-set.
Implementation level discovery

- A Part 3 Layer writes a mapping (The Registry) of its use of the Part 2 Interface

- Mapping via The Registry conveys:
  - How are Data Sets mapped to the GCI?
    - Files or Data Objects?
  - How are DSI's mapped to the GCI?
    - Files or Data Objects
  - What are the ACLs for a specific card-application?
  - What is the mapping of client-application names to Tags?
  - What is the mapping of differential-identity names to key references?
Extensibility

- Allow complete administration of the token through the API
  - Create card-applications
  - Modify card-applications
  - Delete card-applications

- Including subordinate elements of card-applications
  - Identification elements
  - Processing elements
  - Storage elements
Backward Compatibility

- Translation Script
  - Translation scripts may be found on-card or off-card.
  - They may be created (off-card) for legacy tokens.
  - Translation scripts may make semantic as well as procedural translations, allowing use of legacy concepts.

- Registry
  - Registry may be found on-card or off-card.
  - It may be created (off-card) to describe a family of legacy cards.
QUESTIONS?