ISO/IEC 24727

Reference Implementation Demo

NIST

Agenda

- Demonstration Objectives
- Use of ISO/IEC 24727 Framework
- PIV Card Plug-in
- Demonstration
- Closing

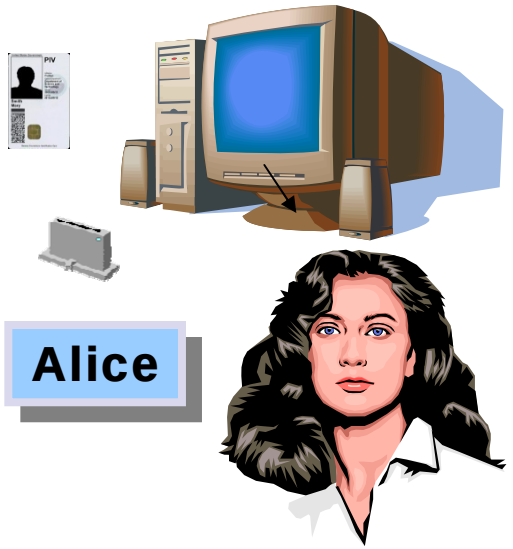
Demonstration Objectives

- Demonstrate the use of identity cards for applications such as:
  - Smart Card Logon
  - Email signing and encryption
  - SSL authentication
- Demonstrate the use of ISO/IEC 24727 framework
- Demonstrate an application independence from card functionality and its data structures

APPLICATIONS

Smart Card Logon Demonstration

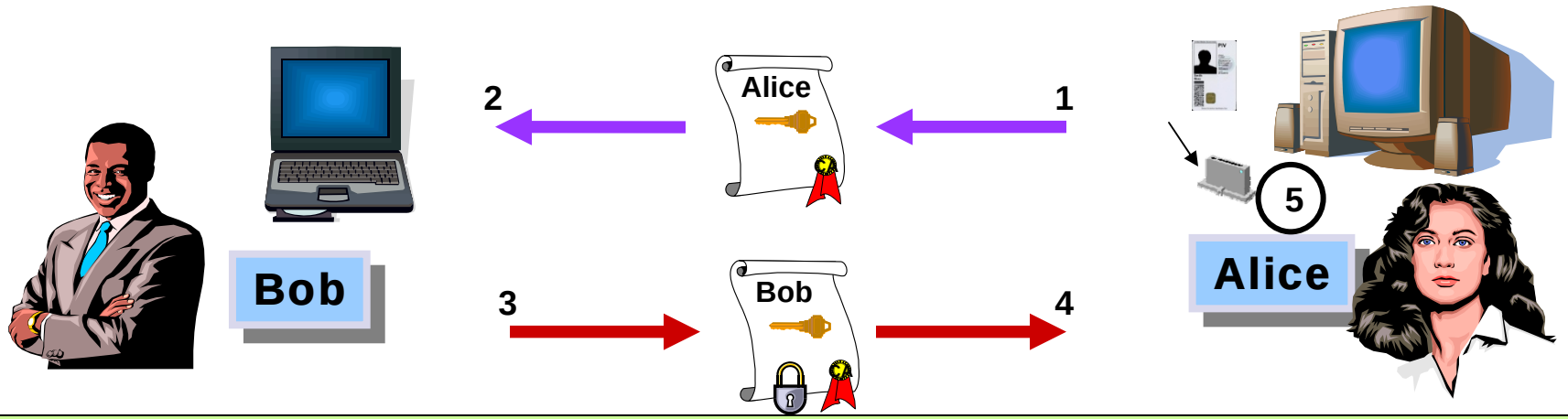
- **Alice inserts her PIV Card into the Reader**
- **At the logon prompt, Alice enters her user ID and the PIN to her PIV Card**
- **After successful authentication, involving a challenge-response and certificate path validation, Alice is logged on the machine**



Email Demonstration

- OS – Windows
- Software Components
  a) Email Client

- OS – Linux
- Smart Card Reader
- Additional Software Components
  a) Email Client



- Step 1 Alice signs an email with her on-card private Digital Signature Key.
- Step 2 Alice sends the signature and the signature key's X.509 certificate to Bob.
- Step 3 Using the public key embedded in the received X.509 certificate, Bob verifies the signed email from Alice.
- Step 4 Bob encrypts an email for Alice using her public Key Management Key (KMK) retrieved from her X.509 KMK certificate (stored locally)
- Step 5 Alice receives and decrypts Bob's message using her on-card private KMK

SSL Demonstration

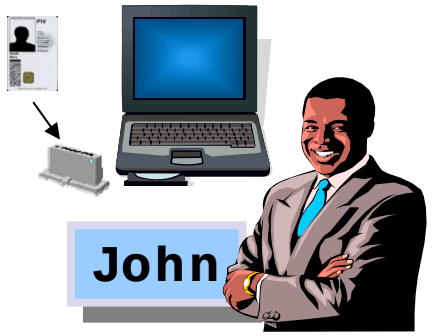
Clients Configuration
- OS - Linux
- Smart Card Reader
- Additional Software Components
  - a) Web Browser

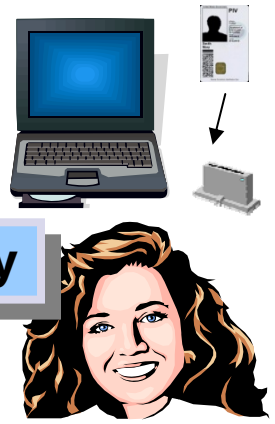
- OS – Windows
- Web Server

Alice's PIV Auth Cert

John's PIV Auth Cert

Mary's PIV Auth Cert





- Can access the application
- Has access control privileges to add new users

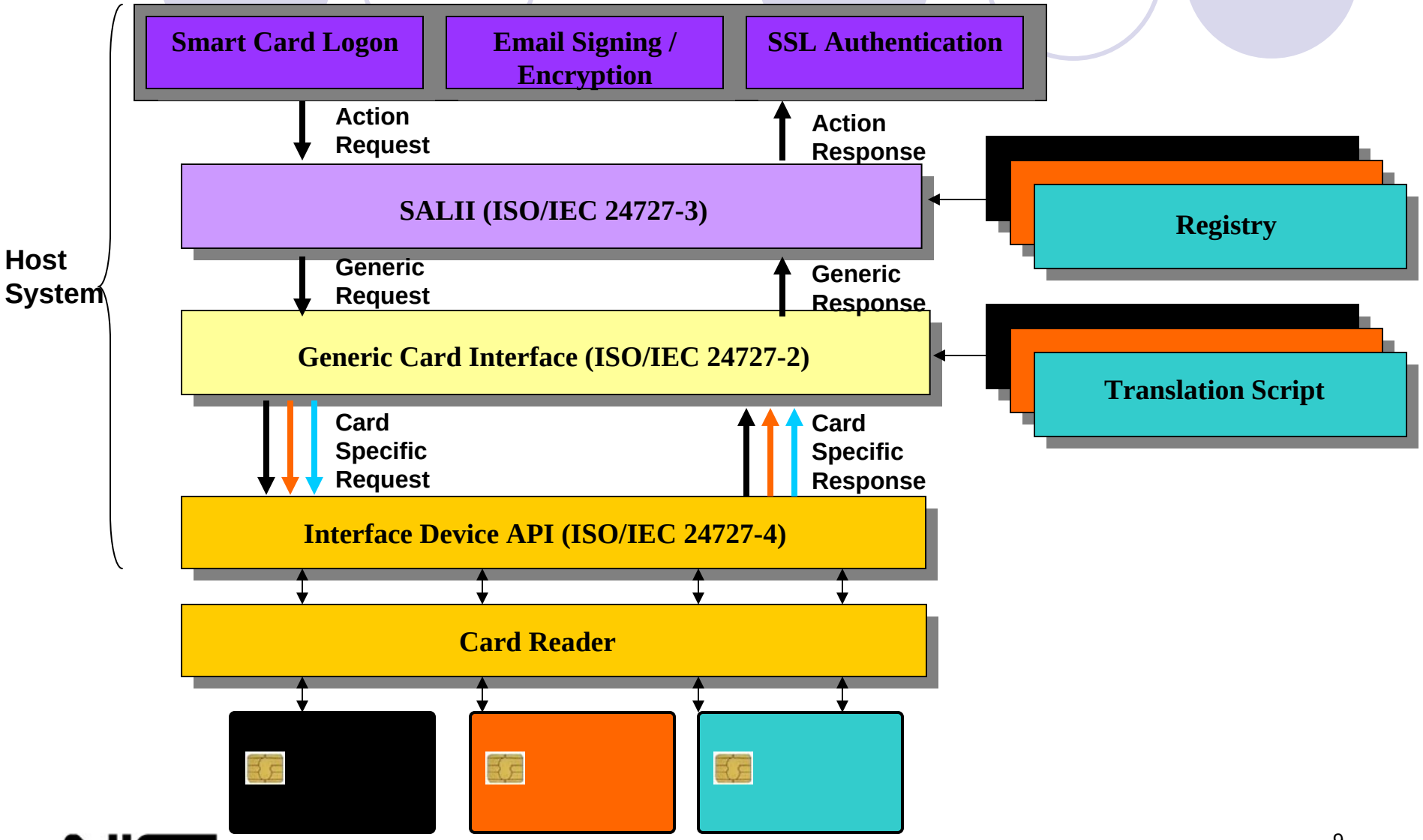
- Can access the application
- Cannot add new users

- Cannot access the application as her PIV Authentication certificate is revoked

NIST

USE OF ISO/IEC 24727 FRAMEWORK

ISO/IEC 24727 Architecture



Characteristics of Our ISO/IEC 24727 Reference Implementation

- Demonstration uses Loyal Stack configuration of ISO/IEC 24727-4.
- ISO/IEC 24727 Part 3 and Part 2 modules are written completely independent of card application.
- ISO/IEC 24727-3 does not include implementation of all functions.
- ISO/IEC 24727-3 uses off-card translation script which is currently hardcoded.
- Additional cards can be plugged-in as long as registry and translation scripts are provided.

ISO/IEC 24727 Part 3 Functions

Functions Implemented

- **Initialize**
- **Terminate**
- **CardApplicationPath**
- **CardApplicationConnect**
- **CardApplicationDisconnect**
- **CardApplicationStartSession**
- CardApplicationEndSession
- CardApplicationList
- CardApplicationServiceList
- CardApplicationServiceDescribe

- **DataSetList**
- **DataSetSelect**
- DataSetDelete

- DSIList
- DSICreate
- DSIDelete
- **DSIRead**
- DSIWrite

- GetRandom
- VerifySignature
- **Sign**
- **Encipher**
- **Decipher**

- **DIDList**
- DIDGet
- DIDUpdate
- **DIDAuthenticate**

Functions NOT Implemented

- CardApplicationCreate
- CardApplicationDelete
- CardApplicationServiceCreate
- CardApplicationServiceLoad
- CardApplicationServiceDelete
- ExecuteAction

- DataSetCreate

- Hash
- VerifyCertificate

- DIDCreate
- DIDDelete

- ACLModify

Functions in **bold**
are used by the applications

PIV PLUG-IN

PIV Data Model

- PIN
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Key pair and certificate
- Two Biometric Fingerprints
- Digital Signature key pair and certificate
- Key Management Key pair and certificate
- Card Authentication Key pair and certificate

PIV Registry

- Uses ASN.1 Encoding in ISO/IEC 7816-15
- Encodes the PIV data structure
- Encodes the differential identities available on PIV Card
- Provides data object “names” to applications through Part 3 functions
- Contains object mapping to key references and object identifiers on the card

PIV Data Representation in Registry

- PIV Data-Set
  - X.509 Certificate for PIV Authentication
  - X.509 Certificate for Card Authentication
  - Card Holder Unique Identifier
  - Card Holder Fingerprints
  - Security Object
  - Card Capability Container
  - Card Holder Facial Image
  - Printed Information
  - X.509 Certificate for Digital Signature
  - X.509 Certificate for Key Management

PIV Data Representation in Registry

- Differential-Identities in PIV
  - Global PIN
  - Application PIN
  - PIN Unblock Key
  - PIV Authentication Key
  - PIV Card Application Administration Key
  - PIV Card Application Digital Signature Key
  - PIV Card Application Key Management Key
  - PIV Card Authentication Key

PIV Data Representation in Registry

- PIV Card Services
  - Connection Service
  - Card-Application Service
  - Named Data Service
  - Cryptographic Service
  - Differential-Identity Service
  - Authorization Service

PIV Translation Script

- Contains translation from ISO/IEC 24727 Part 2 APDUs to PIV APDUs
- Implements APDU translation logic in C and Java
- Uses ISO/IEC 20060 byte codes for interoperability

PIV APDU Mapping

ISO/IEC 24727			PIV	
Command	**Ins**		**Ins**	**Command**
SELECT	0xA4	➔	0xA4	SELECT (pass through)
READ BINARY	0xB0 0xB1	➔	0xCB	Not implemented since the PIV application only contains BER-TLV data objects
UPDATE BINARY	0xD6 0xD7	➔	0xDB	Not implemented since the PIV application only contains BER-TLV data objects
GET DATA	0xCA 0xCB	➔	0xCB	GET DATA (pass through)
PUT DATA	0xDA 0xDB	➔	0xDB	PUT DATA (pass through)
GENERATE ASYMMETRIC KEY PAIR	0x46 0x47	➔	0x47	GENERATE ASYMMETRIC KEY PAIR (pass through)
VERIFY	0x20 0x21	➔	0x20	VERIFY (pass through)
CHANGE REFERENCE DATA	0x24	➔	0x24	CHANGE REFERENCE DATA (pass through)
GET CHALLENGE	0x84	➔	0x87	GENERAL AUTHENTICATE (GET CHALLENGE)
INTERNAL AUTHENTICATE	0x88	➔	0x87	GENERAL AUTHENTICATE (INTERNAL AUTHENTICATE)
EXTERNAL AUTHENTICATE	0x82	➔	0x87	GENERAL AUTHENTICATE (EXTERNAL AUTHENTICATE)
MUTUAL AUTHENTICATE	0x82	➔	0x87	GENERAL AUTHENTICATE (MUTUAL AUTHENTICATE)
GENERAL AUTHENTICATE	0x86 0x87	➔	0x87	GENERAL AUTHENTICATE (pass through)

PIV APDU Mapping

ISO/IEC 24727			PIV	
Command	**Ins**		**Ins**	**Command**
PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE (P1=0x9E, P2=0x9A)	0x2A	➔	0x87	GENERAL AUTHENTICATE
PERFORM SECURITY OPERATION: VERIFY DIGITAL SIGNATURE (P1=0x00, P2=0xA8)	0x2A	➔	0x87	Not implemented since the PIV application does not support this cryptographic operation
PERFORM SECURITY OPERATION: HASH (P1=0x90, P2=0x80 or 0xA0)	0x2A	➔	0x87	Not implemented since the PIV application does not support this cryptographic operation
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE (P1=0x00, P2=0xAE or 0xBE)	0x2A	➔	0x87	Not implemented since the PIV application does not support this cryptographic operation
PERFORM SECURITY OPERATION: ENCIPHER (P1=0x86, P2=0x80)	0x2A	➔	0x87	GENERAL AUTHENTICATE
PERFORM SECURITY OPERATION: DECIPHER (P1=0x80, P2=0x86)	0x2A	➔	0x87	GENERAL AUTHENTICATE
MANAGE SECURITY ENVIRONMENT	0x22	➔		Not sent to the card but the key reference is stored by the translation script
RESET RETRY COUNTER	0x2C	➔	0x2C	RESET RETRY COUNTER (pass through)

DEMONSTRATION…

CLOSING

Closing Remarks

- ISO/IEC 24727 provides authentication, identification, and security services
- Card applications plug-in with registry and translation script
- Demonstration uses open source products
- Build upon our work:
  - Add more identity card applications
  - Add more authentication protocols
  - Add card management functionality

QUESTIONS?