ISO/IEC 24727-6
Authentication Protocols and their Registration

An IAS Interoperability Standard

NIST

Authentication Protocols (APs)

- Existing ISO standards are very general re APs (ISO/IEC 9798, and some in 7816 series)
- Existing Interoperability standards are very explicit re APs (EMV, GlobalPlatform etc etc)
- Up until the publication of ISO/IEC 24727-3 there was no generic methodology for describing a smartcard (or any other) AP
- MOST interoperability problems related to smartcards are due to subtle discrepancies between APs
- Most people think that APs and cryptographic algorithms/ciphers are the same thing – they are not

Then what is a cryptographic algorithm/cipher?

- A mathematical method to convert plaintext to cipher text such that it can only be recovered with a secret key
- Two types of crypto cipher
  - Symmetric (shared secret)
    - Philips/NXP Stream Cipher Crypto-1 (Proprietary)
    - DES – IBM “Data Encryption Standard”
    - 3DES – DES applied 3 times
    - AES (Advanced Encryption System)
    - Many others
  - Asymmetric - one way ciphers (Often part of PKI systems)
    - RSA (invented by Rivest, Shamir, & Adleman)
    - ECC (Elliptic Curve Cryptosystem)
    - Others
- Authentication Protocols (mostly) use crypto ciphers but they are different

NIST

Then what is an Authentication Protocol (AP) ?

- Smartcards operate with challenge <> response protocols
- Authentication protocols typically operate between trusted entities like the ICC and a back office HSM or SAM
  - Usually they pass through the reader without any involvement of the reader
- An Authentication Protocol (AP) is simply an explicit specification for this challenge <> response dialogue
- APs can be one-way (external/internal authenticate)
  - ICC determines device is authentic **OR** device determines ICC is authentic
- APs can be two-way (mutual or general authenticate)
  - ICC determines device is authentic **AND THEN** device determines ICC is authentic

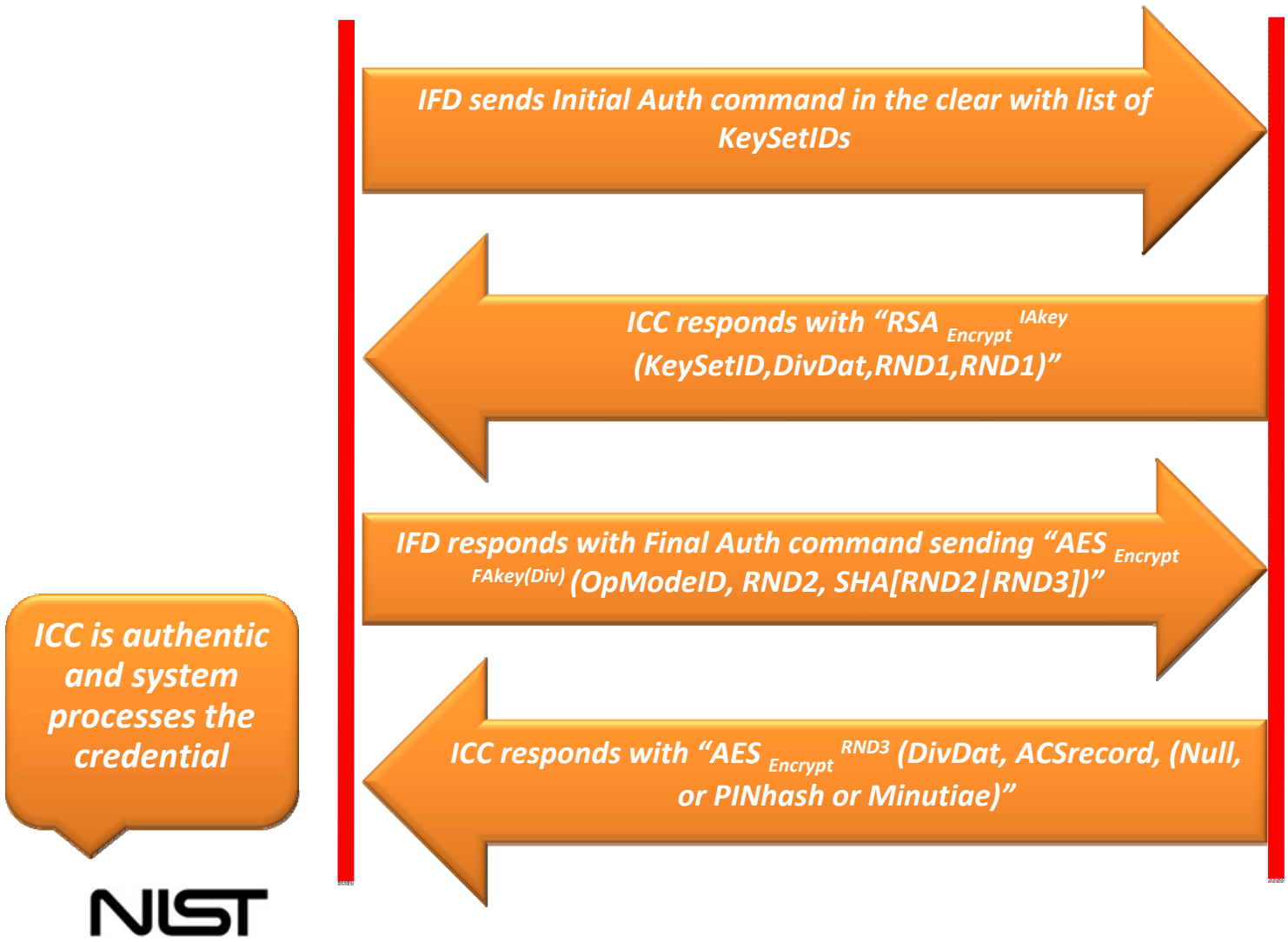
NIST

Then what is an Authentication Protocol (AP) ? (cont)

- APs generally use cryptographic ciphers to determine authenticity of ICCs or devices or back-ends
- If successful – an AP results in an authentication state being set to true, and then whatever else is required is done (like reading/writing data)
- Most successful attacks on smartcards attack the AP, not the cipher, so good APs are important.
- Lets look at an example

NIST

Simple example - PLAID Authentication Protocol



NIST

APs and Interoperability

- Prior to ISO/IEC 24727-3 every AP was either :
  - Proprietary – required same vendor to do both the ICC and IFD application and in-house accreditation
  - Explicitly specified at low level – EMV, SIM, GlobalPlatform, FIPS-201 – these required a lot of maintenance and accreditation
  - Unstable/poorly specified - this resulted in many interoperability problems
    - Smartcard based PKI got a bad reputation, mostly due to variability in vendor implementations
    - No testing or accreditation possible
- There was no common OID system for APs, particularly proprietary ones
- There was no way of finding out which implementations used which APs
- There were (are) perhaps many thousands of APs in use, many we do not know about – They are each specifically fit for their specific purpose

NIST

APs and Intellectual Property

- Prior to ISO/IEC 24727-3 every AP was either:
  - Part of explicit specifications such as EMV, GlobalPlatform, FIPS-201 etc and licensed under them
  - Licensed directly with owner
    - Even ISO/IEC standards required licensing - E.g. ISO/IEC 9798-5:2004 calls out 8 patents and 5 licensees for 5 types of APs!
  - Or (most often) it was impossible to identify the owner of a particular AP, generating un-controlled risk for many projects

NIST

How Does ISO/IEC 24727 solve these issues?

- ISO/IEC 24727-3 Defines a generic method to describe an AP (i.e. a new language)
- ISO/IEC 24727-3 Annex A documents and makes available twenty two (22) common APs (licence free)
- ISO/IEC 24727-3 Annex A provides unique OIDs for the 22 APs

NIST

ISO/IEC 24727-3 Annex A

NIST

How Does ISO/IEC 24727 solve these issues?

- ISO/IEC 24727-5 provides supporting testing for part 3 (and methodology for part 6)
- ISO/IEC 24727-6 sets up a registration authority (RA) for quickly/easily adding NEW APs and allocation of unique OIDs to each AP
- ISO/IEC 24727-6 also registers the IP owner of each AP including patent and contact info
- ISO/IEC 24727-6 sets up a registration authority for quickly/easily registering “Adoption” or use of APs including a pointer to 1st or 3rd party interoperability specifications

NIST

Why do we need a RA (or indeed ISO/IEC 24727-6)?

- Authentication requirements differ between each smartcard implementation
- To ensure interoperability between smartcard implementations APs need to be standardised and allocated unique OIDs
- ISO/IEC 24727-3 is not suitable as it would be in constant flux as new APs are required
- A RA provides a flexible alternative to the ISO/IEC standardisation process

NIST

ISO Registration Authority hosted in Australia

http://www.saiglobal.com/ISO24727-6/

SAI Global

ISO/IEC 24727-6 Registration Authority

286 Sussex Street, Sydney, NSW 2000, Australia

GPO Box 5420, Sydney, NSW 2001, Australia

Telephone 61 2 8206 6000

Facsimile 61 2 8206 6025

Email ISO24727-6@saiglobal.com

NIST

What are we registering?

- Part 6 authentication protocol
  - Authentication Protocol Logic
  - DID Command actions/responses
  - Crypto service command/response
  - Test plans
  - Intellectual Property
- NOTE - The initial state of the AP is draft or beta and the AP can be updated until it is marked final, after which no more updates to the AP are possible
- Generating a unique OID per AP
- Adoption (use)
  - ISO/IEC 24727 Stack model/s supported
  - Further specifications

NIST

AP Detail Registered

- Short name (part of ASN.1 OID)
- Short description
- General description
- Purpose
- Marker – empty or not, ASN.1 representation
- Authentication steps – step by step description with ASN.1 representation
- State Machine - rules for setting true/false

NIST

DID Commands action for Registration

- DIDCreate – didStructure parameter + ASN.1 representation
- DIDUpdate – markerList parameter + ASN.1 representation, generateFlag, publicKey/privateKey options
- DIDGet - didStructure parameter + ASN.1 representation

NIST

Response to crypto service

- Encipher – ASN.1 representation, Data returned, Code returned
- Decipher – ASN.1 representation, Data returned, Code returned
- GetRandom – ASN.1 representation, Data returned, Code returned
- Hash – ASN.1 representation, Data returned, Code returned
- Sign – ASN.1 representation, Data returned, Code returned
- VerifySignature – ASN.1 representation, Data returned, Code returned
- VerifyCertificate – ASN.1 representation, Data returned, Code returned

NIST

AP IP to be registered

- Registration points to:
  - Copyright Owner
  - Patent/s owners
  - Licensor/s
  - Applicant
- Contact details of above inc Web site
- IP Terms

NIST

AP certification to be registered

- AP can be either self certified by the organisation submitting the AP or the AP can be certified by an independent authority
- Identifies the type of certification if applicable

NIST

Example Registered Authentication Protocol OID

- In ASN.1 notation:
  - {iso(1) registration-authority (1) iso24727(24727) part6(6)PLAID(1)}
- In dot notation:
  - 1.1.24727.6.1
- In IRI notation:
  - oid:/ISO/Registration-Authority/24727/6/1

NIST

Registration of Adoption

- OID of AP adopted
  - Can be either part 3 or part 6 AP
- Cryptographic algorithms supported
- Stack model
- Name and/or URL of the document/s which has/have adopted the AP

NIST

Questions

Thank you

Alexander Gagel
Principal Advisor (Solutions Architecture)
New Queensland Driver Licence
Enterprise Information and Systems Division
Department of Transport and Main Roads
Email: alexander.z.gagel@tmr.qld.gov.au

New Queensland Driver Licence
Email: newlicence@tmr.qld.gov.au
Mail: New Queensland Driver Licence Project
GPO Box 1412 Brisbane Qld 4001

NIST