Oberthur Technologies

incits SM
Where IT all begins

InterNational Committee for Information Technology Standards

Generic **I**D-Card **C**ommand **S**et
G.I.C.S

Oberthur Technologies

Background

- **July 2002**: Government Smart Card Interoperability Specification v2.0
  - The industry endorsed the spec and developed compatible products
- **July 2003**: GSC-IS v2.1
  - Move toward more ISO compliance
- **August 2004**: HSPD#12
  - Creates a mandatory market for Personal Identity Verification cards
- **April 2005**: Interface for (PIV) SP 800-73
  - Previous development (GSC-IS) allowed only for transitional phase
  - Brand new development required for End Point product
    - GET DATA vs READ BINARY
- **April 2006**: SP 800-73-1
  - 1st modification of the specification
- **June 2006**: FDIS 24727-1
  - Brand new approach to address card interoperability

Many costly development changes - No ROI from market deployment

GICS Genesis

- **Summer 2006**: Using experiences from the development of PIV products, a group of smart card technical experts from the industry decided to work together to define a stable generic card command set that would piggyback on the PIV End Point card edge developed by NIST, but extend its reach outside of the Government area, to extend the market.

- **August 2007**: The Project Proposal for a technical report is approved by INCITS

- **July 2008**: A draft Technical Specification is proposed to B10.12

- **April 2009:**: First public demonstrations of GICS implementations at RSA show

- **April 2009**: Start of the work from B10.12 to develop a multi-part ANSI standard based on the current technical specification.

Oberthur Technologies

GICS Overview

- Proposal from the Smart Card Industry
  - Not a US Federal Standard
  - Available to all applications, government and non-government ones
- Backward compatible with SP 800-73-2 Part 2
  - Preserve the sizable investment already made around PIV and other related identity credential initiatives (TWIC, RT, …)
- Addresses the needs for:
  - Greater interoperability
  - Generalization to other applications than just PIV
  - Shorter time to market for Smart Card Identity Applications
- Encompasses both usage and administration commands:
  - Non proprietary, unified and stable APDU set
  - Minimized learning curve for application developers

Not an Application Specification but a Card Command Set

Oberthur Technologies

Expected Benefits

Boost the development of the identity market for smart cards:

1. Card Manufacturers and third party application developers will be more inclined to develop and use a card edge commonly available to multiple applications.

2. Cards implementing GICS would provide in some situations better interoperability without requiring a translation mechanism that could be costly in terms of overhead, security and performances.

3. When the market requires a security validation like FIPS 140 or Common Criteria, the card manufacturer may be more willing to go through validation if such validation could benefit multiple applications and therefore increase the size of the potential market.

Oberthur Technologies

Expected Benefits (cont.)

4. If a card with the G.I.C.S. card edge is validated as FIPS 140 compliant, the cost to extend the validation to another application using the same card edge even with a different name space, will be greatly reduced, and the validation of the second application greatly accelerated. This translates to lower cost and shorter time to market for applications that require security validations.

5. A stable card edge, regardless of whether it is developed by a card manufacturer or by a third party application developer, could be hard coded (ROM) to further improve performance and reduce the end product cost.

6. Personalization/Card Management Systems Suppliers will be able to offer their customers a Personalization/Card Management System compatible with a broader range of card suppliers and minimize customization.

7. Customers will have an easier to manage multi-source supply of cards, allowing them to mix suppliers based on quality of products and services.

8. Overall cost of ownership lowers as critical mass is achieved sooner.

GICS Main Technical Characteristics

- **Data object oriented card edge**
  - All data can be accessed using the industry standard GET DATA and PUT DATA commands.
- **Built in parser**
  - A second or third level data object can be retrieved / updated separately
  - No need to read the complete CHUID when only the FASCN is needed
- Allows to create templates with Data Object of different access conditions
  - example: Card Holder Data
- Support for **Tag List**
  - To retrieve all data objects available within a context
  - To retrieve first level tags only
- Support **Extended Header List and Wrappers** (7816-4)
  - Truncate data to retrieve
  - Create template
- Support **Aliases** (Same DO accessible under different Tags)
  - Smooth application migration
- Support **On-Card Fingerprint verification** (MINEX II)

Cryptographic Mechanisms

- **Algorithms**
  - 2 Key Triple DES
  - 3 Key Triple DES
  - AES 128
  - AES 192
  - AES 256
  - RSA 1024 bit
  - RSA 2048 bit
  - RSA 3072 bit
  - RSA 4096 bit
  - ECC: Curve P-192
  - ECC: Curve P-224
  - ECC: Curve P-256
  - ECC: Curve P-384
  - ECC: Curve P-521
- **Confidentiality** with Sym. Algo.
  - No Padding on card
  - ISO/IEC 9797
  - CBC mode
  - ECB mode
- **Confidentiality** with Asym. Algo.
  - RSAES- PKCS1-v1_5
  - RSAES-OAEP
- **Digital Signature**
  - RSAES- PKCS1-v1_5
  - RSASSA PKCS1 PSS
  - Partial SHA off card
  - Partial and Full SHA off card
  - on card SHA only
- **SHA**
  - SHA1
  - SHA 224
  - SHA 256
  - SHA 384
  - SHA 512

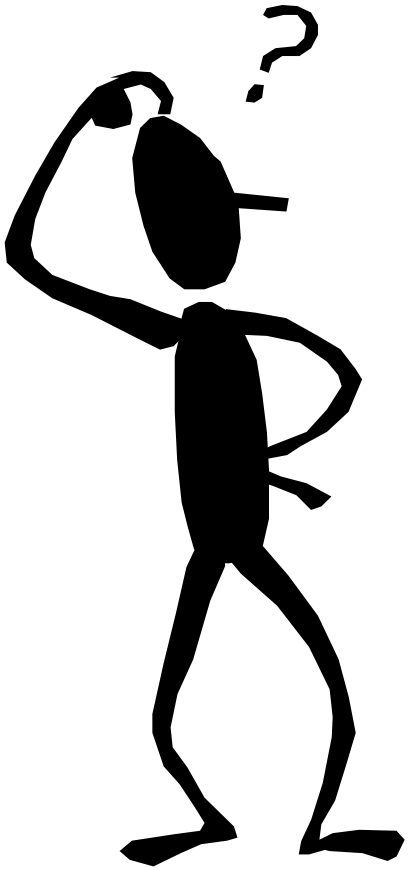
Multiple Authentication Protocols

- Symmetrical and Asymmetrical Algorithms
- Internal, External and Mutual Authentications
- Session Key Establishment for subsequent Secure Messaging
- Different levels of optimization (PAC, LAC, Without leaking any personal information, etc..)
- New authentication protocol can be added if needed
  - Opacity from AI
  - PLAID
  - …

Non-Proprietary, Unified and Stable APDU set

INS	Command name	Note
44	ACTIVATE FILE	
E0	CREATE FILE	
24, 25	CHANGE REFERENCE DATA	Allow reference data of variable lengths (i.e. different from 8 to allow password).
E4	DELETE FILE	
47	GENERATE ASYMMETRIC KEY PAIR	Includes information on how to encode the optional cryptographic mechanism parameters when the key pair to generate is an RSA key pair
87	GENERAL AUTHENTICATE	
CB	GET DATA	Include a parser to retrieve only part of a structured Data Object or template. Allow P1 -P2 = File identifier as well as P1-P2 = '3F FF'
CB	GET PUBLIC KEY	Extension of the GET DATA command to support retrieval of a public key.
88	INTERNAL AUTHENTICATE	Allows internal authentication schemes without witness.
22	MANAGE SECURITY ENVIRONMENT	
2A	PERFORM SECURITY OPERATION	Supports on card signature generation/verification and encryption/decryption functions with on card formatting.
DB	PUT DATA	Allow to load data objects of any tags.
DB	PUT KEY	Extension of the PUT DATA command to support the loading data objects representing keys.
2C, 2D	RESET RETRY COUNTER	Allow referenced data of variable length. Provides the capability to execute the command without resetting code when a secure messaging with mutual authentication has been established.
A4	SELECT	The returned FCI can be customized to meet application needs. Allows SELECT APDU response absent (without FCI or FCP returned) when explicitly requested by the calling application (for instance to speed up transaction over contactless interface)
E6	TERMINATE DF	
20, 21	VERIFY	Allow referenced data of variable length. Provides the capability to clear the application security status without leaving the application.

Questions ?



Christophe J. Goyet

c.goyet@oberthur.com