The Government Smart Card Interoperability Specification

Jim Dray
james.dray@nist.gov
Symposium on Secure Identification Initiatives, June 4, 2002
Why Does NIST Care?

• Computer Security Division’s mission
• Smart cards can improve the security of our national information infrastructure
• Large scale deployment hampered by lack of interoperability (for > 15 years!)
• Proprietary, “stovepipe” systems unacceptable
Barriers to Interoperability

- Each smart card family speaks a different language
- No common high level smart card service provider model
- Programmers must build card specific knowledge into applications!
Inception of the Government Smart Card Program

• Federal customer base wants interoperability (GSA customer survey ‘99)!
• Clear need for a governmentwide smart card interoperability framework
• Driven by contract
Government Smart Card Program

Milestones

• GSA Smart Access Common ID Card contract awarded May 2000
• Post-award Interoperability Committee
• Government Smart Card Interoperability Specification (GSC-IS) v1.0 August 2000
• Government Smart Card Interagency Advisory Board, Standards TWG
• GSC-IS v2.0 NIST Special Pub Q3-02
GSC-IS Objectives

- Generic card service provider model
- Common high level card service interface
- Card independence
- Extensible
- Compatible with other architectural models
GSC Architectural Model

Applications (Logical/Physical Access, etc)

API
(Service)

SPI

Basic Service Interface

Ext. Service Interfaces

GSC-SPM (cards/readers/software)
GSC-IS Architecture

- Government Smart Card Service Provider Module
- Basic Services Interface: Common, interoperable smart card services
- Virtual Card Edge Interface: Common card level “language”
- Card Capabilities Container: Dictionary
- Common Data Models
Card Capabilities Container

- Carried on each card
- Defines how a card’s APDU set differs from the GSC-IS Virtual Card Edge Interface (VCEI)
- Formal grammar
- Size depends on number of differences
- Low overhead: < 100 bytes
GSC-IS Conformance

- Card level:
  - Data model
  - Card Capabilities Container
- Middleware:
  - Basic Services Interface
  - Virtual Card Edge Interface
The Government Smart Card Interoperability Specification defines an architecture for smart card interoperability. This architecture provides a common high level smart card services interface, and common data models and access methods. It works with any smart card regardless of differences in the card edge interface, and imposes minimal conformance requirements at the card level. The Interoperability Specification sets the foundation for a governmentwide smart card infrastructure.
The Future

- Implementation guidance
- Reference implementations
- Developer’s toolkits/workshops
- Collaborations
- Standardization
- Security and conformance testing
Additional Material
Definitions

• Application Protocol Data Units:
  – Defined by ISO 7816-4
  – Specifies a command to/response from the card
  – *Lots of “leeway”…

• Card Edge Interface
  – Set of APDUs implemented by a card
GSC Service Provider Module

Basic Services Interface

Service Provider Software

*Card Reader Driver Layer

Card Reader(s)

Smart Card

Common Data Model

Card Capability Container
Constraints

• The BSI is:
  – Interoperable
  – NOT operational
  – APDU set differences preclude interoperability of some essential operational functions
  – All GSC-IS implementations will require XSIs

• A card reader driver layer is not defined
APDU Independence

• Possible approaches:
  – Standardize on one APDU set (compatibility?)
  – Software drivers for all APDU sets (maintenance?)

• Card Capabilities Container
  – A “hybrid” approach
Communications Sequence

- SPS reads a card’s CCC
- A CCC parser uses the CCC to map APDUs
- Card specific APDU set is mapped to the VCEI
- SPS also links BSI methods to the VCEI
- Card reader driver layer = raw APDU transport
Data Models

- Original “J.8” model from GSC-IS v1.0
- DoD Common Access Card model
- Define a set of containers and data elements