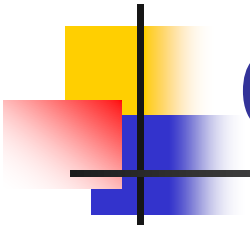
CardTech/SecureTech 2002

Government Smart Card

Smart Card Standards and the Government Smart Card Interoperability Specification (GSC-IS)

April 24, 2002

Presenter: T.Schwarzhoff/NIST



GSC-IS Goals

- Government Smart Card Interoperability Specification (GSC-IS)
  - Provides a standard, high level smart card services interface for applications
  - Card vendor neutral
  - Works with any reader driver layer

GSC-IS Components

- Card Edge Interface (CEI)
  - Card Capabilities Container (CCC)
  - Data Models
  - Mandatory Data Elements
- Basic Services Interface (BSI)
- Extended Services Interface (XSI)

Card Edge Interface (CEI)

- Default set of interoperable commands at card level layer (APDUs)
  - Abstracts differences between heterogeneous card-level command sets
- Card Capabilities Container(CCC)
  - Maps differences from GSC-IS CEI
  - ‘Grammar’ that maps card native APDU set to CEI
- Data Models (GSC-IS Appendix C)
  - GSC-IS Model
  - DoD Common Access Card

Card Edge Interface (CEI) con't.

- Mandatory data elements
  - General information: FN, MI, LN, Suffix, Gov't Agency, Error Detection Code (EDC)
  - Access control: PIN, EDC
  - Card information:Issue Date, Expiration Date, EDC
- Bottom Line: "Any card, Any reader"
  - Card A and Card B using GSC-IS CEI can work on same or different SPMs

Basic Service Interface (BSI)

- Provides services needed by client applications
- Accomplished with 21 BSI functions
  - 3 categories
    - Utility: establishes physical environment
    - General Container: provides for data manipulation
    - Cryptographic: key discovery mechanisms, authentication
  - Must implement all 21 functions to be GSC-IS conformant
- BSI provides interoperability at the client layer and across clients ... not trivial

Extended Services Interface (XSI)

- Augments BSI: BSI is not ‘operational’ interface
- XSI supports application specification requirements
- GSC-IS architecture accommodates XSI but goes no further...to do so breaks the GSC-IS architectural model and interoperability

What doesn't the GSC-IS provide???

- Interoperability not addressed for:
  - Smart card initialization
  - Cryptographic Key Management
  - Communication between card and CADs
- Other
  - Proximity and contactless cards
  - Biometrics: mechanism provided for storing template
- It isn't perfect ... but it's a start ...

Who's using the GSC-IS?

- Federal Agencies
  - DoT, DoD*, Treasury Dept
  - FAA, GSA, VA
- Interest from:
  - Air Line Pilots Association
  - American Association of Motor Vehicle Administrators (AAMVA)

Where to next?

- Implementation guidelines
- Security testing and certification
- ISO standard, international collaboration
- SDKs and workshops
- Next version....

Smart Card Alliance Abstract (Feb 2002)

“The release of the Government Smart Card Interoperability Specification is a significant event in the smart card world as it is the first comprehensive effort to address the interoperability requirements of the enterprise market.

It will become as important as Europay/Mastercard/Visa (EMV) specification is to the Payment market and Global System Mobile (GSM) specification is to the mobile telephony market. ”

http://www.smartcardalliance.org/alliance_activities/dsi_resources.htm

Contact Information

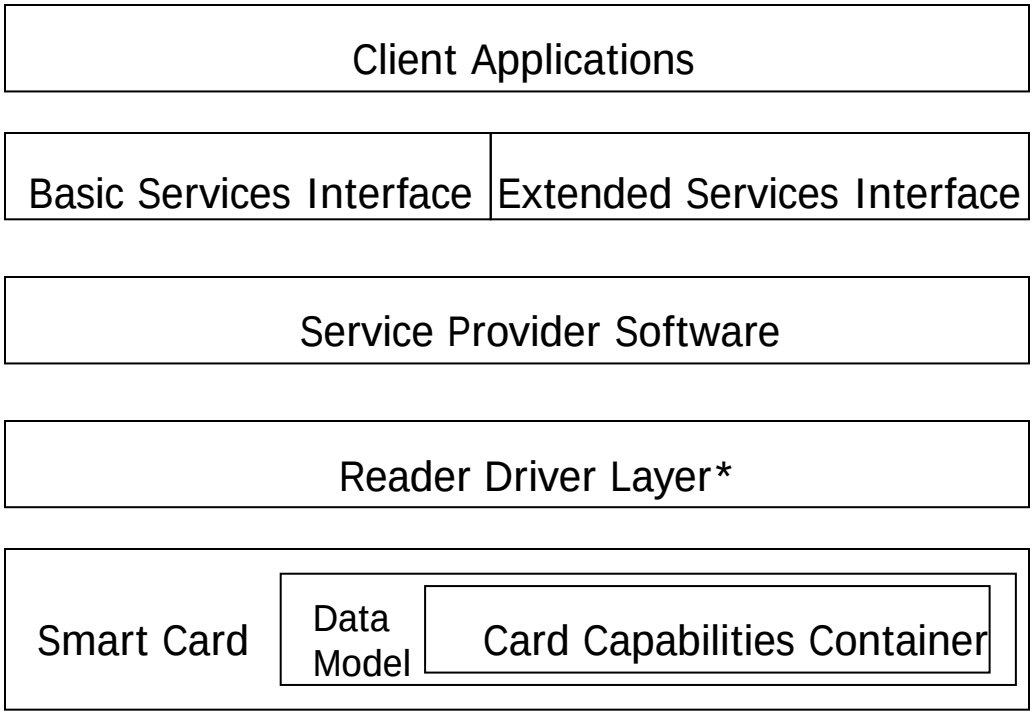
Terry Schwarzhoff
schwarzhoff@nist.gov
voice: 301.975.5727

NIST Information Technology Laboratory,
Computer Security Division

NIST GSC Project Leader: Jim Dray, dray@nist.gov

Additional Information

GSC-IS Architectural Overview



* GSC-IS does not specify a particular reader driver layer, can use PC/SC, OCF, proprietary, etc.

Background

- GSA awarded smart card contract May 2000
  - Five Primes (EDS, KPMG, Litton-PRC, Logicon, Maximus)
  - Base yr + 9 option years
- Post award requirement: Development of Government Smart Card Interoperability Specification (GSC-IS):
  - Collaborative effort with Federal agencies and Industry, led by GSA and NIST
  - DoD major contributor