The Government Smart Card Interoperability Specification

Jim Dray
james.dray@nist.gov

CardTech/SecurTech, April 2002

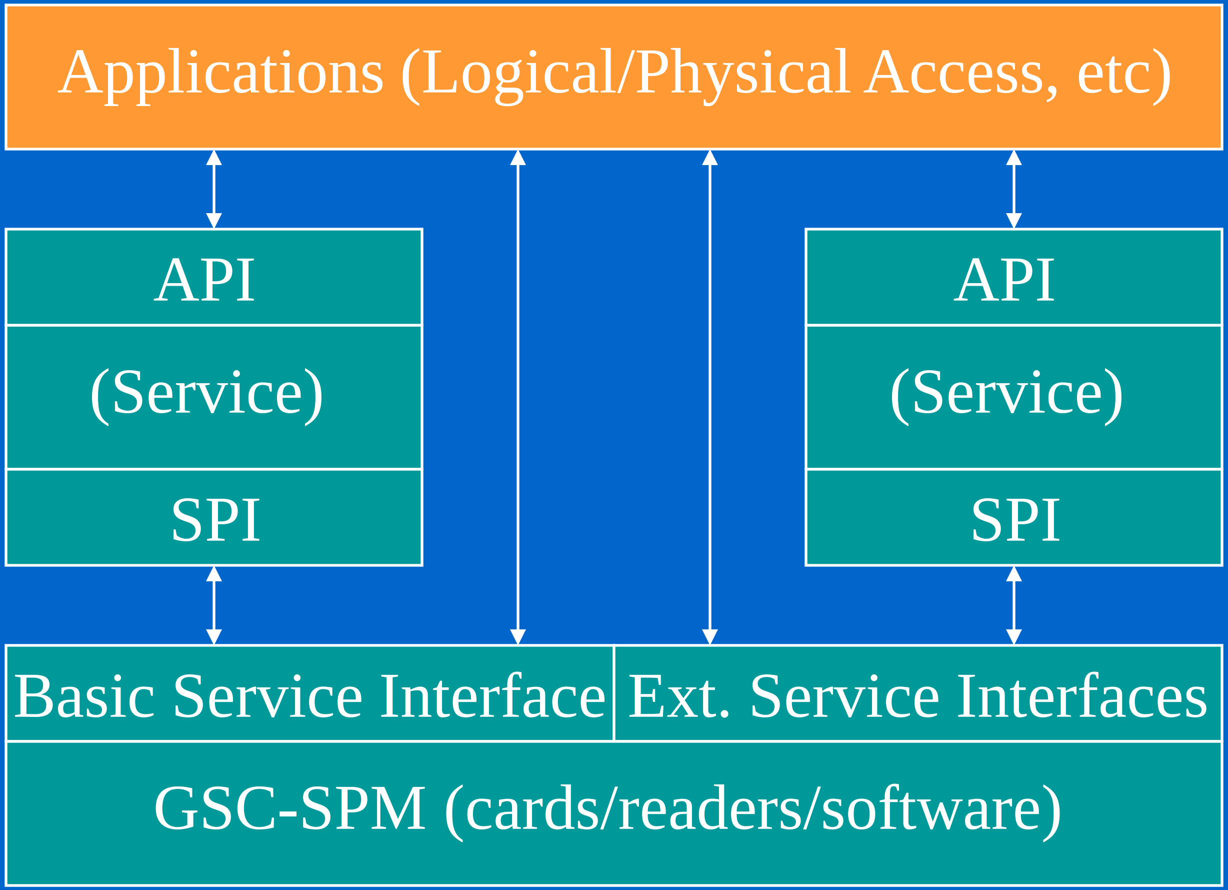
History

- GSA Smart Access Common ID Card contract May 2000
- Post-award Interoperability Committee
- 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
- APDU independence
- Extensible
- Compatible with other models

GSC Architectural Model



Applications (Logical/Physical Access, etc)

API

(Service)

SPI

API

(Service)

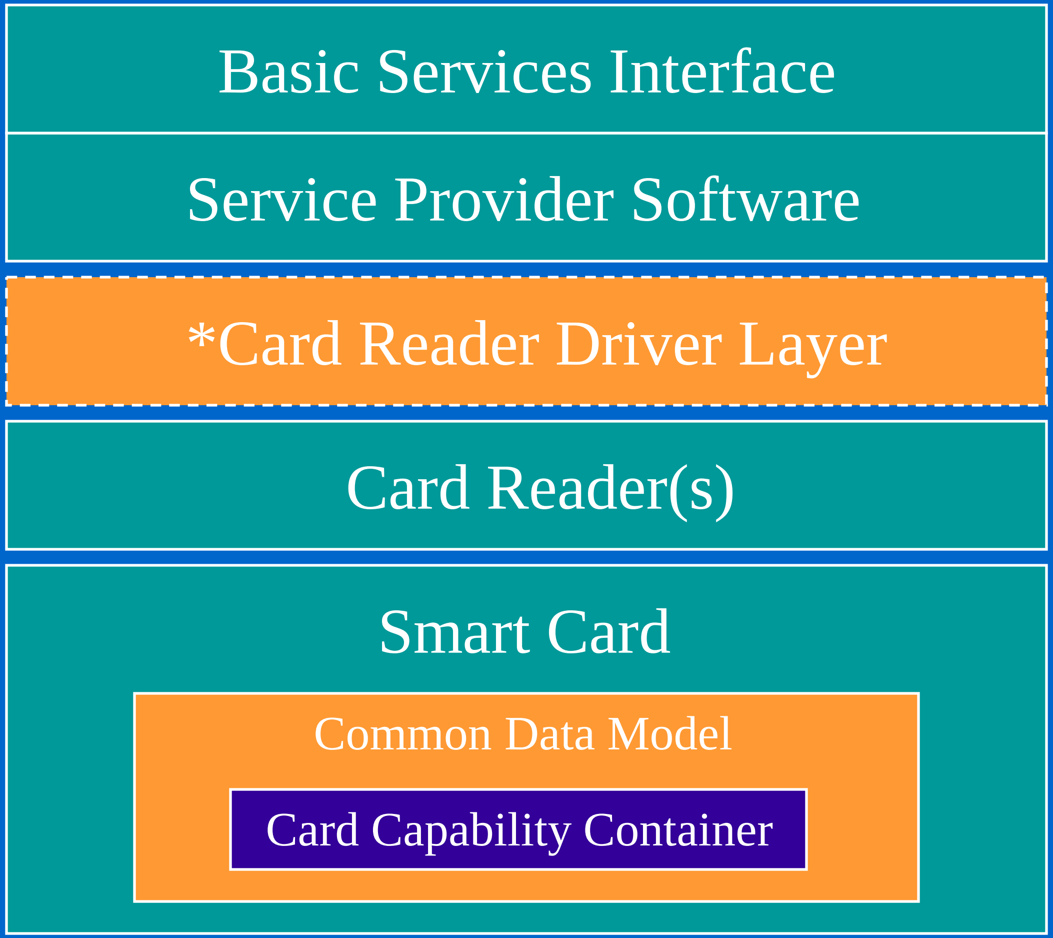
SPI

Basic Service Interface

Ext. Service Interfaces

GSC-SPM (cards/readers/software)

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

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

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
- Mandatory set of core elements:
  - 3 containers
  - 7 data elements

GSC-IS Conformance

- Card level:
  - Mandatory core data elements
  - CCC
- Middleware:
  - BSI
  - VCEI

The Future

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