Interagency Advisory Board

Meeting Agenda, Wednesday, February 22, 2012

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*

2. **Generic Identity Command Set (GICS): Leveraging PIV to Build a Standard Platform for ID Tokens** *(Ketan Mehta, NIST)*

3. **Continuing to Move ICAM into Mobile Computing** *(Owen Unangst, USDA)*

4. **The Movement to Use PIV-I** *(David Belchick, CitiBank)*

5. **NXP and HID Global Enable Mobile Access for NFC Phones Enabling Options for Storing and Managing PIV(-I) Credentials on Mobile Devices** *(Julian Lovelock, HID/Actividentity)*

6. **Cross-Agency Federation: A Demonstration of Federated Identity Trust within the Federal Government and Industry at Level of Assurance 4** *(Tim Baldridge, NASA, and Bob Gilson, DoD)*

7. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

GICS

Leveraging PIV to Build a Standard Platform for ID Tokens

Ketan Mehta
NIST Contractor

Interagency Advisory Board Meeting
Washington, DC
April 25, 2012

NIST

Agenda

- GICS Genesis
- GICS Overview
- Expected Benefits
- Possible Uses of GICS Standard
- GICS Status

GICS Genesis

GICS (Generic Identity Command Set) platform is a Smart Card Industry initiative.

Addresses the needs for:

- Identity application interoperability
- Application management (card administration) standardization
- Support of PIV and other US Government programs (CAC, TWIC, etc.)
- Shorter time to market for smart card based identity applications

Not an Application Specification but a Card Command Set

NIST

GICS Overview

- GICS is a draft national standard developed by the B10.12 committee of INCITS (International Committee for Information Technology Standards) under ANSI/INCITS rules

- A multi-part U.S. National Standard (ANSI)
  - Part 1: Card Application Command Set (NIST)
  - Part 2: Card Administrative Command Set (HID Global)
  - Part 3: GICS Platform Testing Requirements (Exponent)
  - Part 4: Card Application Profile Template (Gemalto)

- Committee Members include:

  American Express, Athena Smartcards, Defense Manpower Data Center (DMDC), Exponent, Gemalto, Giesecke & Devrient, HID Global (ActivIdentity), Infineon, NIST, Oberthur, Unisys, VeriFone, Global Platform

NIST

GICS Overview (cont'd)

- GICS Parts 1 and 2 Provides:
  - Card Edge (ISO/IEC 7816 based APDU definition)
  - Standardization for arbitrary data, keys, certificates, PINs, and Passwords.
  - Standardization for card application administration
  - Authentication protocols
  - Global Platform based secure messaging to enable full use of contactless interface

- GICS Part 4 Provides:
  - A template for creating GICS application profiles which are based on Part 1 and Part 2 specifications.
  - Application profiles specify usage data models and security configurations.
  - PIV and CAC are application profiles in GICS. And many other application profiles can be created based on Part 1 and 2 specification.

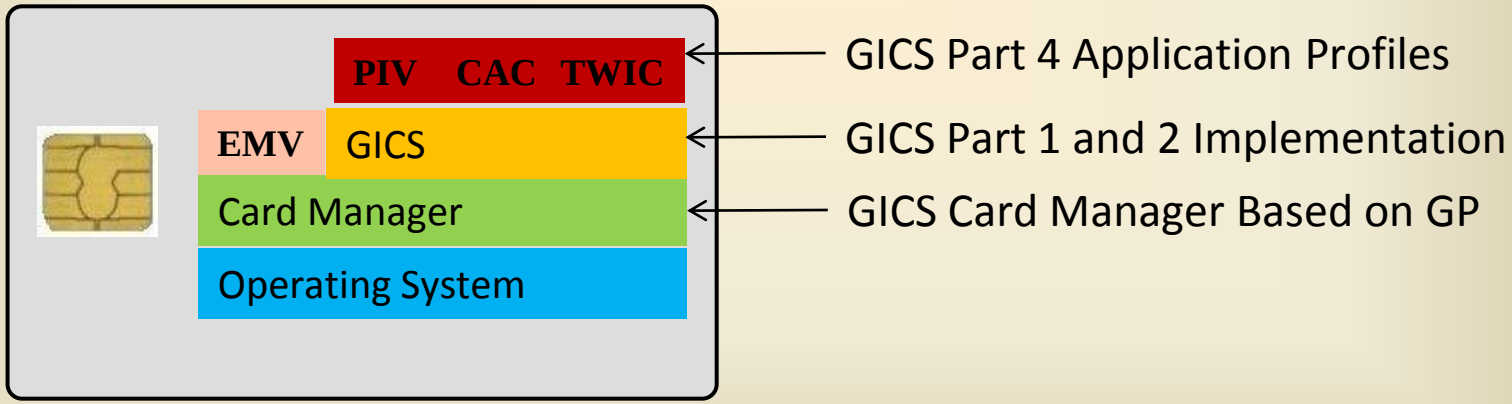
- GICS Part 3 Provides:
  - Conformance testing requirements for Parts 1 and 2.
  - A GICS platform conformant to the GICS specifications fully implements Part 1 and Part 2.

GICS will benefit…

- **Interoperability:** the GICS platform simplified interoperability – a well defined, lean and not redundant card edge
- **Application development cycle:** card issuer and third party developers benefit from the well defined set of Authentication protocols, simplifying development of card applications and middleware.
- **FIPS 140 Security Validation:** a FIPS 140 validated, or validation-ready, platform will reduce validation costs and time-to-market
- **Time to market (and cost):** this well defined and standard card edge, would be hard coded (ROM) and made available "off the shelf" also reducing costs
- **Card issuance and card management:** Personalization and Card Management Systems providers will be able to offer Provisioning and Card Management System compatible with a broader range of card suppliers and applications when the GICS platform is adopted
- **e-ID token adoption:** Operating System and Middleware providers have great motivation in support this platform creating a virtuous circle

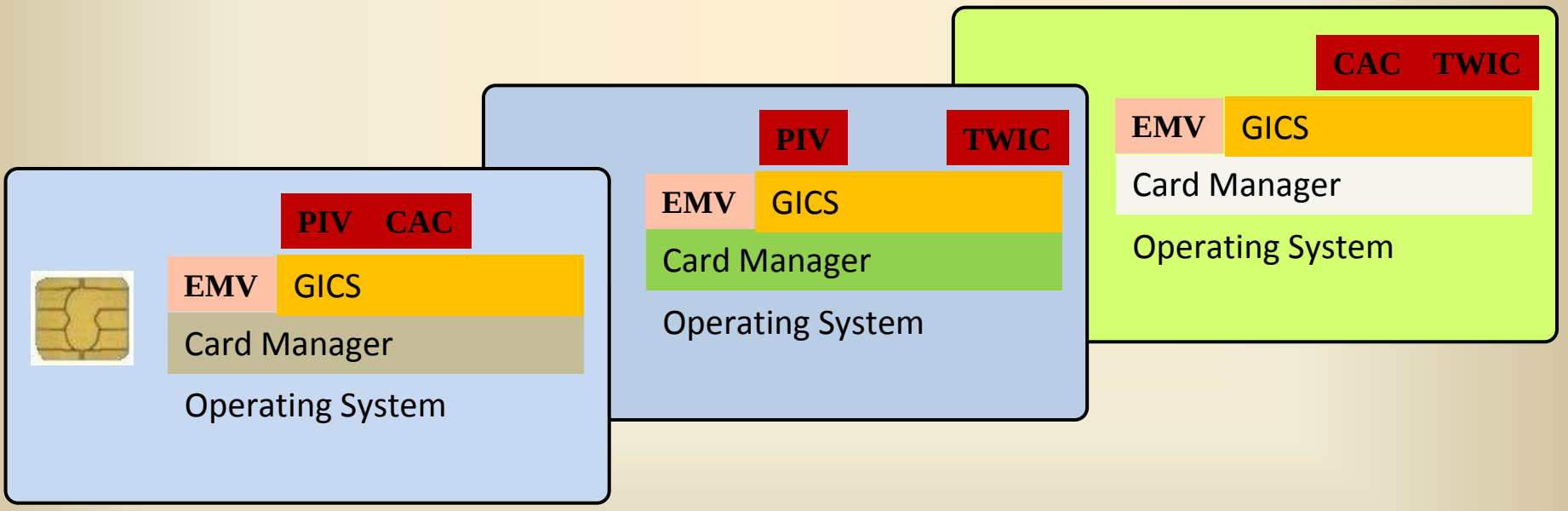
Use Case 1
Maintain FIPS 140-2 Certification

- GICS platform already includes tools to support many applications.
- Card manufacturers can develop code once and get the platform certified.
- Instantiate as many applications as the customer wants.



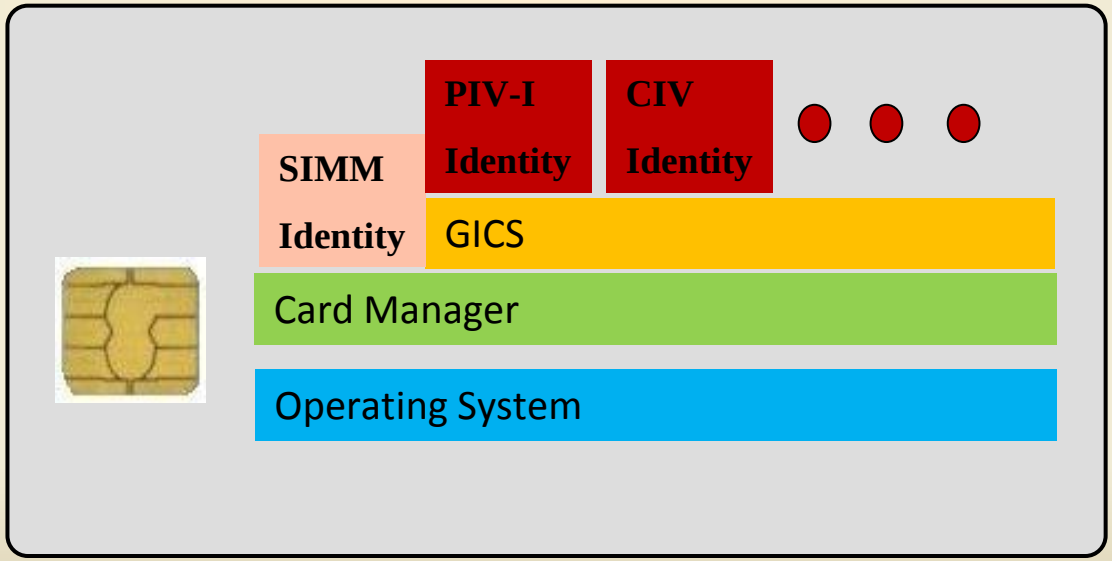
Use Case 2
Vendor Independence

- GICS platform already includes tools to support many identity applications.
- Create and use applications on any GICS cards regardless of the manufacturer.



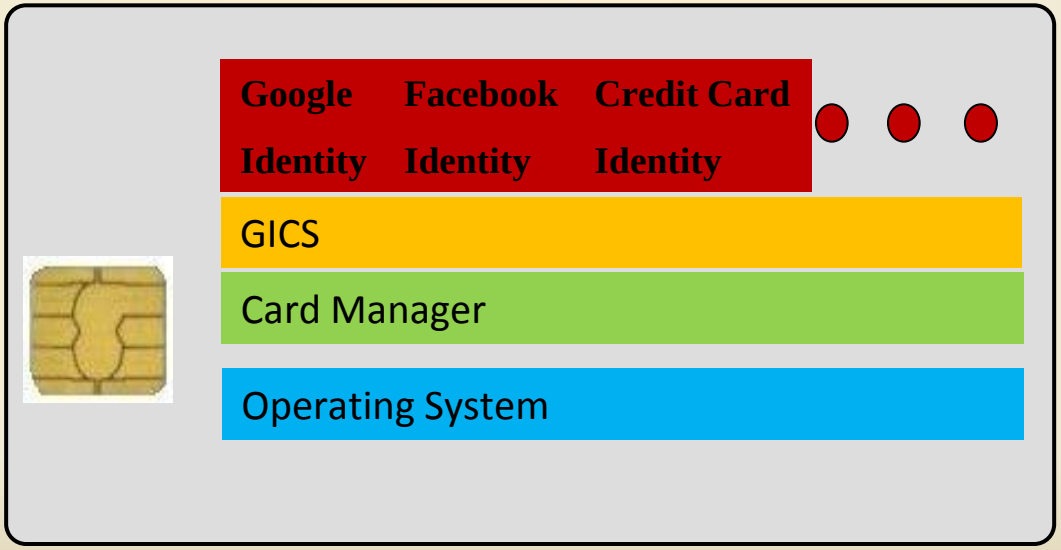
Use Case 3
Multi-issuer Card

- Identity credentials from different issuers can be loaded on to one card after a GICS Part 4 profile is created.
- GICS provides global application management keys so issuer can manage their own applications on the GICS card.



Use Case 4
Create Your Own Credential – NSTIC Model

- Consumer purchase the GICS card from convenience store.
- Get certificate binding from Identity Provider.
- Unlock the card and personalize using home PC.
- Start authenticating to the websites.



GICS Status

- Parts 1 and 2 will be published for public comments in May 2012
- Part 3 is under development
- Part 4 will be published for public comments within next six months

Questions?

Ketan Mehta
NIST Contractor
mehta_ketan@nist.gov