

FICAM impact on enterprise architecture and applications

Smart Card Alliance – IAB

FICAM Part B

Sal D'Agostino

IDmachines



Overview - Areas of Impact

- FICAM Architecture Challenges
- FICAM Infrastructure
- FICAM Identity
- FICAM Credentialing
- FICAM Access
- FICAM Management
- FICAM Application Challenges

FICAM Architecture Challenge

- Identity and the related infrastructure are critical to 21st century enterprise
- FICAM requires issuance of a level 4 identity
 - Should it issue other levels of identities?
- FICAM requires support of multiple identity levels.
 - And lots of others “identities”
 - Understand the difference between identity and identifier
- Scale and Interoperability
 - Federal Enterprise
 - ~10 million employees
 - ~500 million users
 - ~ Trillion devices

Requirement: Ubiquitous Public Key Infrastructure (PKI)

- Validation Requires Status and Trust
 - CRLs
 - OCSP
 - Server
 - » Cache
 - SCVP
 - Server
 - DPD
 - » Cache
 - DPV
 - » Cache
- Proprietary Options
 - Mini and Delta CRLs

FICAM Identity

- The hard part and in many cases already done.
- Where is ICAM in the enterprise
 - Program versus Enterprise Architecture
- Is HSPD-12 and/or ICAM a silo?
- Is Personal Identity Verification being leveraged?
 - Part 1 Identity
 - Vault
 - Roles and Rules
 - Lifecycle and Workflow
 - Synchronization
 - » Makes time something that needs to be assessed
 - Expiration Dates
 - Certifications
 - Budgets
 - Lead Time (Understanding Process)
 - Maturity Model and Roadmap



FICAM Credentialing

- PIV or PIV-I is a process of establishing and transferring an identity to a token with digital certificates and other objects, all of which require cryptography to use or trust.
- In order to use a PIV or PIV-I credential it must be provisioned to an application or a device.
- Credentialing is the binding of identity to do or be something.
- Gap exists in contactless credentialing
- Consideration needs to be given to writing information to a credential.

FICAM Access

- Some of the same drivers as with the architecture
 - X.509 authentication
 - Federated PKI as trust anchor
 - Ability to support OID policy and assurance level
- Ability to support universally unique identifiers
 - This drives the gap analysis.
 - This is a challenge for PACS.
 - Same challenge as IPv6 for IT
- Supporting legacy approaches weakens security

FICAM Applications

- Enterprise software support of FICAM
 - Microsoft Roadmap
 - Apple Roadmap
 - Oracle Roadmap
 - Symantec Roadmap
 - Open Source
 - Infrastructure
 - Applications
 - Etc.....

FICAM Applications

- Avoid tail wagging the dog
- Be prescriptive
- Determine the nature of the support
 - Scale
 - Interoperability

FICAM and the Enterprise

- Provides a number of data points to measure enterprise architecture and application decision against.
- It is wide ranging and has to be addressed.
- Roadmaps are like quality control
 - The it gets ignored the more it costs
 - And the costs grow geometrically.

Questions, Comments

IDmachines LLC

1264 Beacon Street, #5

Brookline, MA 02446

+1 617.201.4809

sal@idmachines.com

