CIO COUNCIL

ICAM
Identity, Credential,
& Access Management

Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

Federal ICAM Sub-Committee Plan for FIPS 201-2 Revision Recommendations

April 19, 2011

Tim Baldridge
AWG Co-Chair
NASA

ICAM SC Vision Statement

- Cloud computing, mobile devices, broadband and wireless communication, and intelligent devices are transforming a broad spectrum of applications (both access to information resources and facilities) and enabling a quantum step in efficiency and effectiveness.

- Over the next five years, implementations across government and private sector will align PIV, PIV-I and other credentialing requirements with business and technology trends that support private sector, consumer and governmental interests.

ICAM SC Vision Statement (cont.)

- The realized benefits among government, private sector and consumers are to increase assurance of identity and increase efficiency of operations while enhancing privacy.   In addition, the governments will innovate more rapidly by the encouragement of public/private partnerships and the procurement of aligned products.

- Through experience with Federal PKI, personal identity verification and federated identity, the Government has proven its capabilities in implementing federal identity, credential and access management across the Federal space.

ICAM SC Vision Statement (cont.)

- We recommend that the FIPS 201 standard specify the capability to issue credentials based on a PIV or PIV-I identity, with form factors in addition to the credit card form factor (ISO/IEC 7810), that are interoperable in the PIV System.

Work Strategy for ICAM-SC FIPS 201-2 Review

- ➢ Requested Agency Comments through mailing lists for:
  - ICAM-SC, ICAM-AWG and ICAM-CPWG
- ➢ Next ICAM-SC Meeting April 27 – Last Call for Comments
  - Due COB May 2
- ➢ Combined AWG and CPWG meeting on May 5
- ➢ Inputs Organized and Redistributed to ICAM-SC by May 11
- ➢ ICAM-SC Recommendations Reviewed
  - May 18 ICAM-SC Meeting, Discussion and Approval
- ➢ Submit Agreed on FIPS 201-2 Recommendations to NIST

Some suggested thinking points…

FIPS 201-2 – LEAD BY EXAMPLE FOR NSTIC

CHAIN-OF-TRUST – FIPS 201-2 speaks to Identity Lifecycle Management.

a) Reference to FICAM, Roadmap & Implementation Guidance

b) Independence of Identity Lifecycle Management and Credential Lifecycle Management.

c) HSPD-12 does not indicate a card, only FIPS 201

d) Perpetual requirement to issue card form factor for permanent employees and contractors

e) Allow greater flexibility for contractors credentialing such that conformant PIV-I, with Government Attribute Claim or Government BAE provider may be used in place of PIV

f) Only Government entities may assert PIV equivalent suitability or fitness. Attribute Certificate or equivalent, must be cryptographically protected to insure integrity

g) PIV-I or equivalent electronic validated credential single requirement for I-9 enrollment.

ALTERNATE FORM FACTORS

a) Subscriber activation of conformant Secure Element in a variety of form factors

b) Secure Element must meet FIPS 140 Level 2 or 3 Logical, FIPS 140 Level 3 Physical

c) Contactless form factors must use Secure Channel , recommend for contact

d) Credentials on alternate form factors must be electronically distinguishable from PIV and PIV-I cards

e) Mobile phones, etc., are network connected and can be updated more frequently – trust anchor and attribute/claims

f) FIPS 140/CMVP Validation Certificate for Secure Element

g) FIPS 140 Level 1 (software) on phone, Secure Element Level 2 or 3.

FACTOR VECTOR – HKA

a) Primary use case is H (have) must be tied to PKI Compute function for private/secret key in Secure Element ("only-one-of" requirement)

b) Typical K (know) secure subscriber PIN to Card to enable PKI Compute function. MUST always be used with H/PIV Auth

c) Typical A (are) signed object retrieved and validated by RP. Validation both of issuance integrity and match to live scan

d) OCC (On Card Comparison - are) A alternate activation for enable PKI Compute function and other protected card PIV functions. MAY NOT be used in combination with PIN to CARD to establish 3 factor authentication

e) Geo-location – Where do you "have" it and proof-of-local

SECURE CHANNEL

a) All communication secured both contact (optional) and contactless (required)

b) All features enabled on both contact and contactless secured changes. Fingerprint, PIN

c) Anticipate future requirement to secure contact communication as required

d) Include capability for “Closed RP/Federation”

e) Trust Anchor on card – Trust Anchor lifecycle management

UUID Required

a) All same places (five) as FASC-N
b) LUI/PPID also defined as UUID, different from Credential UUID

APPLICATION LOA

a) Reconcile Disjoining of TFP LOA 1-3 (non-PKI) and LOA 3 (PKI) and LOA 4
b) Implication of LOA 4 – HOC (holder of key)
c) Use of PIV (LOA 4) for LOA 1, 2 & 3 Applications