Smart Card Alliance

Recommendations and observations for ISC
Identity Assurance Levels and Assertion

Salvatore D'Agostino, IDmachines LLC
LaChelle LeVan, Probaris, Inc.

IDmachines
"Maximizing Identity"

Interagency Advisory Board
April Fools, 2010
Washington, DC

Probaris

Identity Assertions

Identity: Establish who you are (for a good reason)

Credential: Bind who you are to some thing

Access:

- Assign roles to identity [Authorization] (e.g. for access)
- First role is the system administrator
  - Need to rules for privileged account holders
- Qualifications a parallel component required for authentication, (e.g. NRC, CFATS, SOX, HIPAA…)
  - Too many roles, also confusion here with certifications, attributes, privileges across organizations and within organizations

Identity Assertion: (Management)

- Authorization for Authentication

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Trust allows use

“These challenges lie in being able to verify the identity of an individual or non-person entity (NPE) in the digital realm and to establish trust in the use of that identity in conducting business.”

***Page 1**, FICAM Roadmap and Implementation Guidance, November 10, 2009*

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Identity Assurance Levels

Assurance:

1) the degree of confidence in the *vetting process* used to establish the identity..., and
2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Four (4) assurance levels:

- Level 1: Little or no confidence
- Level 2: Some confidence
- Level 3: High confidence
- Level 4: Very high confidence

Reference: E-Authentication Guidance for Federal Agencies (OMB M04-04), December 16, 2003

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Still confused about internet “identity”

On the Internet, *everybody* knows you're a dog.
By Michael Kinsley Posted Monday, Nov. 27, 2006, at 9:00 PM ET

The pre-cursor was 5 July 1993, Peter Steiner, New Yorker cartoon, “On the internet, nobody knows you’re a dog.” So which is it, ☺?

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Assurance Process and Tokens

Assurance	Process Strength	Tokens
Level 1	Self-assertion minimum standards No liability with Identity Service Provider	Username and Password Open ID Foundation, Open Identity Exchange, Kantara Initiative, OAuth, CardSpace/InfoCard, and more (e.g. Mozilla, MyOneLogIn)
Level 2	On-line instant qualification, out-of band follow-up after transaction Mutually accepted liability.	Known (trusted?) identifier provider, e.g. Educause/Shiboleth/InCommon Shared secrets (pet's name)
Level 3	On-line out-of-band verification with transaction Limited personal liability some network liability.	Cryptographic solution One time password Soft certificate (unbound to token) Machine identity
Level 4	In person proofing, separation of roles Biometrics Mixed service level liability	Cryptographic solution Hardware token **PIV, PIV-I**

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Identity versus identifiers

- Assurance levels and type of "identity" are related.
- At lower assurance (Levels 1,2) use is via an identifier and not an identity.
- Level 4 identity requires roles, responsibilities and technologies (e.g. PKI and biometric binding of identity)- PIV and PIV-I provide standards for this.

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Standards Based Approach

PIV and PIV-I sets standards

- Highest trusted assurance level
- Interoperable
- Federal Bridge is as trust anchor and root trust broker
- Chip is current method of hard token that exist in a number of form factors
- Two parts
  - Establishing identity
  - Defining credential to bind identity (for Level 4)

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

ICAM and Identity Assertions

ICAM

- The segment architecture relates to a system (People, Process and Infrastructure) driven by identity and the need to assert (use) it.
  - Identity
  - Credential
  - Application (Access in ICAM)
    - *Authentication* of credential when presented to system
      - » Level 4 accepted at Levels </=4
  - Management of the ***application*** and ***system*** requires understanding, designing, building and maintaining the use cases for identity assertions.

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Use, risk and authentication

Use requires risk assessment

- Ability to create (or measure) consistency of use
- Drives requirement for assurance level
- Include loss of life, loss of value, loss of reputation, etc.

Authentication levels

- Choice driven by risk assessment
- Have to drive proper use of the credential for the application (no backsliding)
- Maps to Assurance Level

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

PIV, PIV-I Level 4 Identity

Delivers on Authentication, Authorization, Administration, and Audit (4As)

High Assurance Version!!

- Opening doors to a facility
- Accessing information in an enterprise system
- Digitally signing documents with legal non-repudiation
- Transferring money between two organizations….

Federated Trust

- Trusted transactions or interchange of information

Multi-factor strong authentication

- Something you are (e.g., biometric)
- Something you have (e.g., token or smart card)
- Something you know (e.g., PIN or password).

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Application

Level 4 Credential

Level 4 identity using Level 1 methods

Level 1 Transactions

- Username and Password log-on
- Free-read of FASC-N physical access
- Optional proximity antenna physical access
- Use as flash pass

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Application

Level 4 Credential

Level 4 identity using Level 4 methods

Level 4 Transactions

- Cryptographic log on (Certificate and PIN)
- Contact smart card reader for physical access control
- Machine read
  - Certificate
  - PIN
  - Fingerprint
  - Digitally Signed Photograph
- Machine sure credential is valid (current, challenge, revocation, trust)

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Recommendations and Comments

1. **Assurance level needs to meet assertion use case.**

2. **Both process and technology**

3. **Lower assurance levels evolved from B2C world use cases.**
   1. Allows large numbers of people easier access to web sites
   2. Single Sign On (low assurance, not “robot”)

4. **Need to be careful of building on top of weak credentials such as username and password and Physical Access Control Systems (PACS).**

5. **Need to be extremely careful with privileged credential**

6. **Federal ICAM initiative provides solid framework for use in C2G, B2G, G2G world in addition to the enterprise**
   1. Cybersecurity and Physical Security
   2. Converging initiatives in:
      1. Aerospace and Defense
      2. Education
      3. Finance and Banking
      4. Pharmaceuticals and Research
      5. Other Critical Infrastructure (CIPP and NIPP)

7. **PIV and PIV-I use COTS to provide high assurance for IT applications**
   1. Strong case to leverage existing credentials and infrastructure
   2. PKI PACS exists and can address physical security

8. **If you have a Level 4 credential why introduce other methods?**
   1. Particularly given standards based approach.

Smart Card Alliance Confidential
Property of the Smart Card Alliance © 2010

Sal D'Agostino
+1 617.201.4809
sal@idmachines.com

Smart Card Alliance

191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828

www.smartcardalliance.org

IDmachines
"Maximizing Identity"

Probaris