Levels of Assurance In Electronic Identity

Considerations for Implementation

Benjamin Oshrin

Rutgers University

March 2009

About This Presentation

- Based on what we think we're going to have to do
- Discussion about what you think you're going to have to do (or already are doing) would be valuable

Table of Contents

- What Does LoA Mean?
- NIST Special Publication 800-63
- InCommon, a Higher Ed Federation
- Considerations For Implementation
  - Registration
  - Identity Proofing
  - Issuance of Credentials
  - Token and Credential Management
  - Authentication Processes
  - Assertions

What is LoA?

- "Level of Assurance"
  - Risk assessment of electronic authentication
  - ie: How confident you are that the person who is authenticating really is the person who is authenticating
- LoA is complicated
  - Weakest component determines overall LoA
  - Partly calculated at run time due to access methods
  - Identity proofing generally not robustly done today

NIST Recommendations

- NIST is the National Institute of Standards and Technology, a non-regulatory US federal agency
- NIST Special Publication 800-63-1
  - Prepared for use by Federal agencies
  - Use by others is voluntary
  - Purpose: "This recommendation provides technical guidelines to agencies for the implementation of electronic authentication (e-authentication)."
- Based on 4 levels of identity assurance, as defined in OMB 04-04 (*E-Authentication Guidance for Federal Agencies*)

OMB Levels of Authentication

- Intended to assess risks associated with various aspects of e-authentication

Criteria	Level 1	Level 2	Level 3	Level 4
Confidence in asserted identity's validity	Little/No	Some	High	Very High
Risk of inconvenience or liability	Low	Mod	Mod	High
Risk of release of sensitive data	None	Low	Mod	High
Risk to personal safety	None	None	Low	Mod/High

E-Authentication Model

- **Applicant** applies to a **Registration Authority**
- Registration Authority vets and approves Applicant, who becomes a **Subscriber** of a **Credential Service Provider** (possibly same as the RA)
- Subscriber is issued a **token** (secret) and **credentials** (binds token to Subscriber name)
- Subscriber may participate in **identity proofing**, to have a **verified name**, or else use a **pseudonym**
- When Subscriber accesses a service, the Subscriber becomes a **Claimant** accessing a service provided by a **Relying Party**, and the Claimant's identity is authenticated by a **Verifier** (probably the CSP)

Calculating NIST LoA

- Level of Assurance is lowest level reached for 5 metrics
  - Registration and Issuance
  - Tokens
  - Token and Credential Management
  - Authentication Process
  - Assertions

Registration and Issuance

Level	Requirements
١	Anonymous credentials permitted, no explicit requirements
٢	Anonymous credentials permitted, no explicit requirements Otherwise, valid government ID (in person) or Valid gov't ID and financial account numbers (remote)
٣	As for Level ٢, but IDs must be validated, not just inspected
٤	Validated gov't ID and additional ID or account number, as per L3 In person registration only, no remote registration Biometric record must be taken at registration

Tokens

Level	Requirements
1	Password, Pre-Registered Knowledge, Look-up Secret, Out of Band
2	Password, Pre-Registered Knowledge, Look-up Secret, Out of Band, Single Factor One Time Password Device, Single Factor Cryptographic Device
3	Multifactor Software Cryptographic Token
4	Multifactor One Time Password Hardware Token Multifactor Hardware Cryptographic Token Biometric record must be taken at registration

Pre-Registered Knowledge: eg “What is your favorite color?”
Look-up Secret: Lookaside table, eg: TreasuryDirect card
Out of Band: eg SMS to cellphone
SF OTP: eg SecureID without PIN
SF Crypto: eg Prox card
MF SW: eg Encrypted certificate (must type passphrase)
MF OTP HW: eg SecureID with PIN
MF HW: eg PIN activated USB cert store

Token and Credential Management

Level	Requirements
1	Password hashed and protected by ACLs
2	Strong statements about storage of tokens Renewal of credentials by presentation of unexpired existing tokens 72 hours to revoke credentials Record retention for 7.5 years beyond expiration of credentials
3	Stronger statements about storage of tokens Secure methods for verification of credentials Renewal of credentials by presentation of unexpired existing tokens 24 hours to revoke credentials Record retention for 7.5 years beyond expiration of credentials
4	Token storage as per Level 3 Verification of credentials as per Level 3 Stronger crypto for renewal of credentials 24 hours to revoke credentials Recommendation to destroy tokens upon disuse Record retention for 10.5 years beyond expiration of credentials

Authentication Process

Level	Requirements
1	Shared secrets may not be transmitted in plaintext
2	Resist session hijacking, replay, and online guessing Weak Man-in-the-middle resistance
3	Shared secrets may not be revealed except to Credential Service Provider (CSP)
4	Stronger resistance to Man-in-the-middle

TLS is generally suitable for all levels

Assertions

Level	Requirements
1	Must be single use, short lifespan, signed or transmitted securely
2	Mutually authenticated channel or Signed by Verifier and encrypted for Relying Party Protected channel required to resist hijacking
3	Signed for non-repudiation, shorter lifespan in single domain context Exception for Single Sign On when certain requirements met
4	Assertions not permitted

Types include Cookies, SAML, Indirect (backchannel dereference)

InCommon

- InCommon is a federation of over 100 higher ed, government, non profit, and commercial organizations
  - Includes NIH, NSF, TerraGrid, JSTOR, Microsoft, Apple, etc
- Certifies that IdPs conform to certain standards and may be trusted
  - Vs a series of point to point agreements
- Standards are defined as Identity Assurance Profiles (IAPs)
- Funding agencies may start requiring InCommon IAP

InCommon IAP Tech Requirements

- Perform assessment of IdP policies, processes, practices, and controls against IAPs
  - Assessment of current conditions, not future plans
- Have assessment reviewed by a "sufficiently independent" IT Auditor
- Auditor submits report to InCommon
- Periodic reassessment, and notification upon material changes that could affect compliance
- (InCommon also requires legal agreements and registration and annual fees of $700/$1000)

InCommon IAPs

- Bronze is interoperable with NIST Level 1
- Silver is interoperable with NIST Level 2
  - Funding agencies, including FAFSA (Financial Aid) are likely to require Level 2/Silver
  - Bronze is a subset of Silver
- Can have a mix of users at different levels
- A given user could be represented at different levels in different contexts
- No IAP is also possible
- Additional IAPs may be defined in the future

IAP Assessment Factors (Overview)

- Business Policy and Operational Factors
- Registration and Identity Proofing
- Digital Electronic Credential Technology
- Credential Issuance and Management
- Security and Management of Authentication Events
- Identity Information Management
- Identity Assertion Content
- Technical Environment

IAP Assessment Factors

- Following factors in addition to appropriate NIST-1,-2
- Business Policy and Operational Factors (Bronze, Silver)
  - IdP Operator is a legal entity, and **designated by institutional executive management to provide IdMS services**
  - Post terms, conditions, and privacy policies
  - Operations audited at least every 24 months

IAP Assessment Factors

- Business Policy and Operational Factors (Silver)
  - All security policies and procedures are documented
    - Undocumented procedures not considered
  - **IdP Operator has sufficient staff with sufficient skills to operate according to stated policies and procedures**
  - Outsourced services have written, binding contracts stipulating policies and procedures relevant to IAP
  - Helpdesk available during regular hours (M-F, 8 hours)
  - Risk Management Plan
    - **Background checks on critical staff**
    - ACLs over critical data
    - Strong digital credentials
    - **Separation of duties**
  - Logging of critical events, **retained for at least 6 months**

IAP Assessment Factors

- Registration and Identity Proofing (Silver)
  - Identity proofing and registration processes documented
    - (Various requirements of documentation)
  - Protection of personal identifying information
  - **Retention of registration records for at least 7.5 years past revocation or expiration**
    - Identity proofing document numbers
    - Full name
    - Date of birth
    - Current address of record
  - Ability to recover identifying information from Subject of credentials

IAP Assessment Factors

- Digital Electronic Credential Technology (Bronze, Silver)
  - Unique identifiers per Subject
  - Subject may have multiple Tokens, not vice versa
  - Subject-changeable shared secret (password, PIN)
    - Resistance to guessing per NIST-1 and -2 standards

IAP Assessment Factors

- Credential Issuance and Management (Bronze, Silver)
  - Unique, **non-reassignable** identifiers
  - Revocation of credentials to prevent authentication

IAP Assessment Factors

- Credential Issuance and Management (Silver)
  - Offer secure, automated mechanism for determining status of credentials, with at least 99% availability (3.65 days of downtime per year)
  - In the event of attempted compromise of a Subject's credentials, do not assert Silver until credentials reset and notify Subject
    - 10 or more failed attempts in 10 minutes requires validation backoff, lockout, or non-assertion of Silver
  - Credential revocation, renewal, re-assertion according to NIST-2

IAP Assessment Factors

- Security and Management of Authentication Events (Bronze, Silver)
  - Secure communication, proof of possession, session authentication, protection of secrets, resistance to online guessing, resistance to eavesdropping according to NIST-1 & -2
  - Storage of secrets according to NIST-2 (or higher)
  - Mitigate risk of sharing credentials
    - Reminder of institutional policies
    - Confirmation of sensitive operations via separate channels (eg: email)
  - Authentication via challenge-response (Bronze only, eg: Digest auth), password tunneled over TLS, zero-knowledge based password (eg: Kerberos)

IAP Assessment Factors

- Identity Information Management (Silver)
  - Review of identity attributes required for Silver every 2 years
- Identity Assertion Content (Silver, Bronze)
  - Align attribute definitions with InCommon requirements
    - eduPerson
    - Silver, Bronze IAQ
    - Cryptographic security per NIST-2

IAP Assessment Factors

- Technical Environment (Silver)
  - Configuration management
    - Version control
    - Up to date on patches
    - **Logging of all software and configuration changes**
  - Network security measures against threats including eavesdropper, replay, verifier impersonation, DNS hijacking, and man-in-the-middle attack; and intrusion detection/prevention
  - Physical access control and access logs for data center and other sensitive areas
  - Continuity of operations
    - System failures do not cause false positives
    - **Disaster recovery and resistance**
      - Or notification to subjects of absence of such a plan

References

- NIST E-Authentication Guidelines
  - http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- OMB E-Authentication Guidance for Federal Agencies
  - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
- InCommon Identity Assurance
  - http://www.incommonfederation.org/assurance