Interagency Advisory Board

Meeting Agenda, Wednesday, February 27, 2013

1. **Opening Remarks**

2. **Discussion on Revisions Contained in Draft SP 800-63-2** *(Bill Burr, NIST)*

3. **The Objectives and Status of Modern Physical Access Working Group (MPAWG)** *(Will Morrison and J'son Tyson, MPAWG Co-Chair)*

4. **Overview of PACS Specification from the Security Industry Association (SIA) to Include All PIV Functionality** *(Rob Zivney, Chair of the SIA PIV Working Group and Vice Chair of the Standards Committee)*

5. **Closing Remarks**

Draft NIST SP 800-63-2

What are the changes?

Bill Burr

burr44@gmail.com

william.burr@nist.gov

IAB meeting 27 February, 2013

Background: M0404

- OMB M0404 Policy Guidance for e-authentication
  - Agencies classify electronic transactions into 4 authentication assurance levels according to the potential consequences of an authentication error
  - Consider: privacy, inconvenience, damage to reputation, harm to agencies and programs, financial liability, crime, safety

Background

- NIST SP 800-63: Technical authentication Framework for remote e-authentication
  - Issued in 2005
  - Technical requirements for 4 levels of M0404
    - Identity proofing requirements
    - Authentication protocols and mechanisms based on secrets
  - Applies to Federal agencies
    - But widely adopted or referenced elsewhere
      - Used for applications the authors never considered

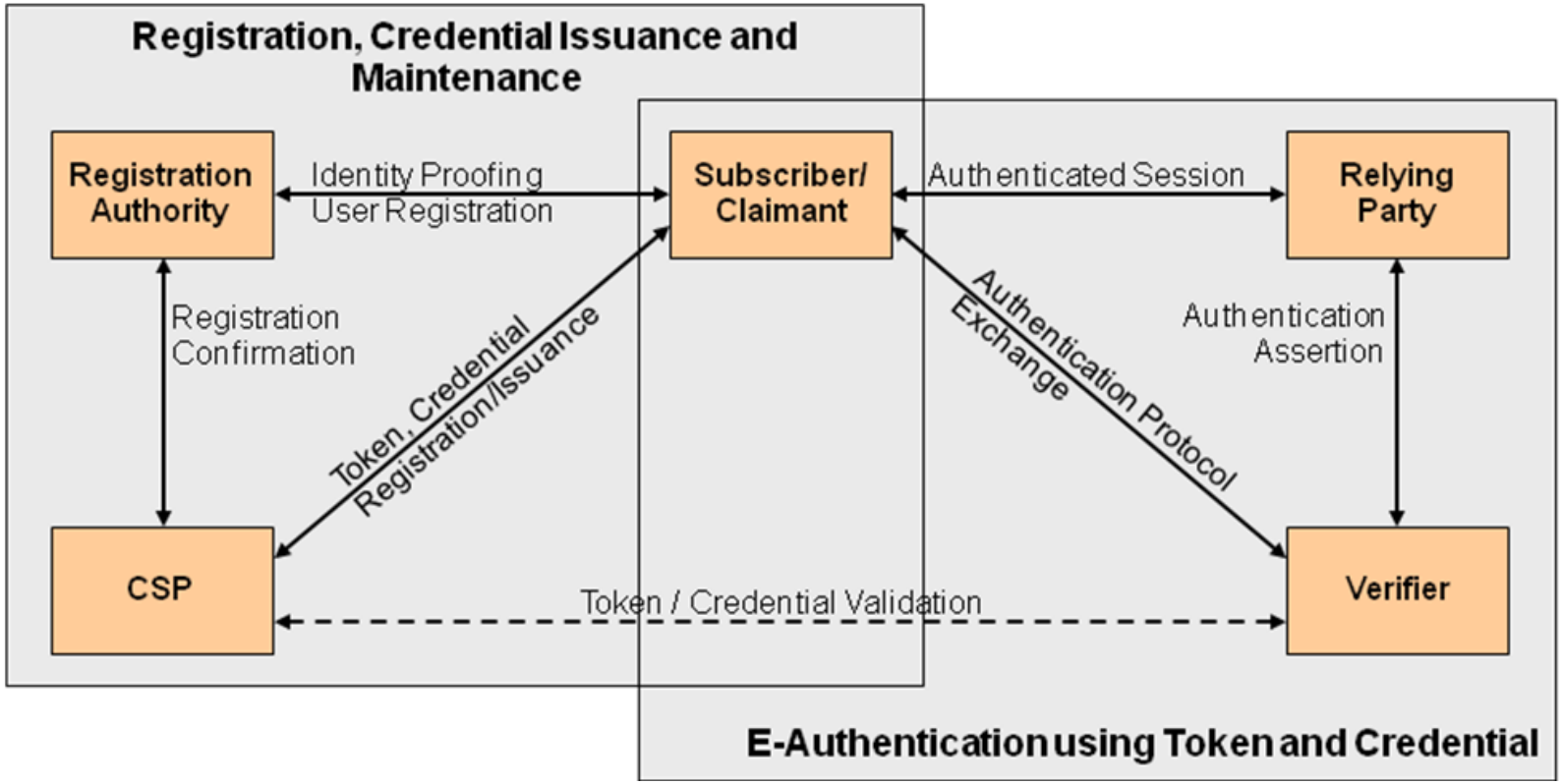
The Parties

- Applicant (hopes to become a subscriber)
- Registration Authority (RA)
- Subscriber
- Credential Service Provider (CSP)
  - Issues tokens & credentials to subscribers
- Claimant (Must be a subscriber)
  - Claims an identity
  - Could be anywhere on the Internet
- Verifier
- Relying Party

Terminology

- Credential
  - An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. May be electronic records maintained by the CSP which establish a binding between the Subscriber's token and identity
- Token
  - Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity.

Architectural Model



SP 800-63 Premise

- Authentication Factors
  - Something you have
    - a badge or a key
  - Something you know
    - Password/PIN
  - Something you are
    - Biometrics (don’t know how to apply these effectively to remote authentication)
- Two factors are better than one

Four Levels

- Level 1
  - No identity proofing
  - Relatively weak passwords allowed; may be vulnerable to eavesdroppers
- Level 2
  - Remote ID proofing is straightforward
    - Address of record notification
  - Single factor authentication & may be vulnerable to phishing, social engineering, etc.

Four Levels

- Level 3
  - In Person Remote ID proofing
    - For remote must issue token to confirm postal address or issue through a recorded voice call
  - Two factors
    - *e.g.* password + soft crypto token or one-time password device
  - Phishing attacks don’t get master auth. secret

Identity Proofing

- Level 4
  - In person ID proofing
  - Two factors with hard crypto tokens
    - e.g. a PIV card
    - something tangible that also protects key
  - Crypto binding of authentication and data transfer

Identity Proofing

- In Person or Remote
- Establish that an identity exists
  - Possession of a valid government picture ID
  - Financial or utility account number
- Is the applicant that person?
  - Match ID photo too applicant and check for consistency of records, or issue issue credentials in a way that confirms address of record

SP 800-63-1

- Added more token types
  - Memorized Secret Token
  - Pre-registered Knowledge Token
  - Look-up Secret Token
  - Out of Band Token
  - Single Factor (SF) OTP Device
  - SF Cryptographic Device
  - Multi Factor (MF) Software Cryptographic Token
  - MF OTP Device
  - MF Cryptographic Token
- Rules for combining tokens to get higher assurance level

SP 800-63-1

- Explicitly allowed for
  - Assertions (e.g. SAML & with cookies)
  - Kerberos
- Discussed Threats, Mitigation Strategies & Countermeasures
- Security requirements for Verifiers, CSPs and Relying Parties

Proposed SP 800-63-2

- Relatively small update
  - Comment period closes March 4, 2013
- Confined to identity proofing
  - All substantive changes in Section 5
- Addresses practical problems in large scale ID Proofing
  - Particularly in healthcare arena
    - Use professional licensure in ID proofing
    - Reduce need for mailing in issuing credentials
- Addresses minor ambiguities in ID proofing text and adds minor clarifications

The Changes

Section	Description	Implication
5.1	Clarifies relationship between RA and CSP)when they are implemented by separate entities: this relationship could be contractual or based on existing laws or regulations (*e.g.* a notary is the RA).	Promotes use of existing identity proofing infrastructure (such as notary services) as RAs for credential issuance.
5.3.1	Clarifies that remote ID proofing mechanisms (at levels 2 and 3) were designed for full automation. However, online mechanisms such as call centers can also complement the automated mechanisms.	Automated remote ID schemes can be done in a single session, removing delays (from mail or multiple sessions) facilitating large scale credential issuance. Call centers may reduce costs where full automation is impractical.

Based on a summary prepared by Electrosoft and found at:
http://www.electrosoft-inc.com/electroblog/2013/2/13/nist-releases-updated-electronic-authentication-guideline-fo.html

The Changes

Section	Description	Implication
5.3.1 Table 3	Gives examples of "current primary government picture ID.”	Removes ambiguity regarding acceptable types of ID for remote or in-person identity proofing.
5.3.1 Table 3	Tightens the language of remote identity proofing at Level 3 to require that both the ID number AND the account number must be associated with the Applicant's name and address in records.	Removes weaknesses in the existing text for Level 3 remote identity proofing where it was possible to use an account number (such as a pre-paid cell phone account number) that was not necessarily associated with the Applicant’s name or address.

Based on a summary prepared by Electrosoft and found at:
http://www.electrosoft-inc.com/electroblog/2013/2/13/nist-releases-updated-electronic-authentication-guideline-fo.html

The Changes

Section	Description	Implication
5.3.1 Table 3	Gives examples of "current primary government picture ID.”	Removes ambiguity regarding acceptable types of ID for remote or in-person identity proofing.
5.3.1 Table 3	Allows SMS, phone or email as confirmation of electronic address of records if these are tied to the Applicant's physical address in records. Removes the requirement for voice recording of the Applicant (or something equivalent) for non-repudiation purposes.	ID proofing and credential issuance can often be completed in real-time in a single session with the Applicant via electronic confirmation, removing delay and reducing costs. The result is faster issuance, lower costs and better usability.

Based on a summary prepared by Electrosoft and found at:
http://www.electrosoft-inc.com/electroblog/2013/2/13/nist-releases-updated-electronic-authentication-guideline-fo.html

The Changes

Section	Description	Implication
5.3.1	Allows a phone account to be used as a "financial" account for ID proofing if the account is associated with the Applicant's name and address in records. That phone number cannot be used for address confirmation.	Recognizes that if the Applicant has a phone number that is associated with their name and their physical address, this can be leveraged as an effective mechanism for identity proofing.
5.3.2	Allows use of professional licensure/registration (e.g. MD, lawyer, CPA…) in ID proofing of employees or affiliates for level 3 or 4. Licensure/registration must involve examination, post secondary education and professional supervision.	Allows CSPs to leverage existing professional licensing schemes that require stringent identity proofing mechanisms to streamline credential issuance. This lowers the cost and complexity while greatly improving the user experience.

Based on a summary prepared by Electrosoft and found at:
http://www.electrosoft-inc.com/electroblog/2013/2/13/nist-releases-updated-electronic-authentication-guideline-fo.html

Links

- Draft SP 800-63-2: http://csrc.nist.gov/news_events/#feb1
- Electrosoft summary of changes in SP 800-63-2: http://www.electrosoft-inc.com/electroblog/2013/2/13/nist-releases-updated-electronic-authentication-guideline-fo.html