Password Reset Practices

April 1, 2015

Eric Goodman
Identity and Access Management Architect
University of California Office of the President

Password Reset Practices

with a focus on, but not limited to,
InCommon Bronze IAP requirements

Password Reset Practices

Areas for discussion

- Self-service password reset allowed by Bronze
- “Failover” (re-proofing) allowed by Bronze
- General best practices discussion

My intent is some specific focus on “re-proofing”

- That is, what happens when *self-service* fails?
- Largely because *self-service* is better understood.
  - https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet
  - Though debates still do exist even there! E.g.,:
    - Are questions good ideas?
    - Do we trust SMS as secure delivery?

Background (IAP Related)

Relevant sections from IAP:

- 4.2.4.3: Defines credential reissuance methods
- 4.2.2: Identity proofing; also referenced as "fallback" credential reissuance options
- 3.1: Defines the general purpose of the "Bronze" profile

The following 3 slides present the language from the IAP sections, highlighting specific language to prompt discussion.

Background: Bronze Re-issuance

4.2.4.3 **(S) (B)** CREDENTIAL RENEWAL OR RE-ISSUANCE

A Subject must be authenticated for purpose of Credential renewal or re-issuance by any of the following methods:

1. By use of a non-expired and valid Credential.
2. By use of a single-use secret delivered to the Subject from the IdPO by means of a pre-registered out of band delivery mechanism.
3. The Subject may supply correct answers to pre-registered personalized questions designed to be difficult for any other person to know.

After expiration of the current Credential, **if none of these methods is successful then the Subject must re-establish her or his identity with the IdPO per Section 4.2.2** before the Credential may be renewed or re-issued.

Background: Bronze Identity Proofing

4.2.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing in this IAP uses verified information to create a record for the Subject in the IdPO's IdMS.

4.2.2.1 **(S)** RA AUTHENTICATION….

4.2.2.2 **(S)** IDENTITY VERIFICATION PROCESS….

4.2.2.3 **(S)** REGISTRATION RECORDS….

4.2.2.4 **(S)** IDENTITY PROOFING….

4.2.2.4.1 Existing relationship….

4.2.2.4.2 In-Person proofing….

4.2.2.4.3 Remote proofing….

4.2.2.5 **(S)** ADDRESS OF RECORD CONFIRMATION….

4.2.2.6 **(S)** **(B)** PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Any personally identifiable information collected during registration or identity proofing must be protected from unauthorized disclosure or modification.

Background: Bronze "Summary"

3.1 INCOMMON BRONZE IDENTITY ASSURANCE PROFILE

The InCommon Bronze identity assurance profile focuses on sequential identity, that is, reasonable assurance that the same person is authenticating each time with a particular Credential. Assertions under this profile are likely to represent the same Subject each time a Subject identifier is provided.

While no identity proofing requirements are specified, it is expected that IdPOs use reasonable care when issuing Credentials to confirm that a single individual applies for and receives a given Credential and its Authentication Secret.

InCommon Bronze qualified Assertions are typically usable by individuals seeking access to online information resources licensed to an organization and for which the Subject is an eligible user. They also may be usable for access to online services where the SP will invoke other methods for linking of the Subject identifier to information the SP already has regarding individuals who should have access to its services.

IAP-Specific Questions

Does section 4.2.2 allow Bronze identity “re-proofing”?

- Language in summary states “*uses verified information*”
- Prescriptive for Silver, no requirements/allowable process defined for Bronze
- (How) is Bronze identity re-proofing constrained by the “uses verified information” language?

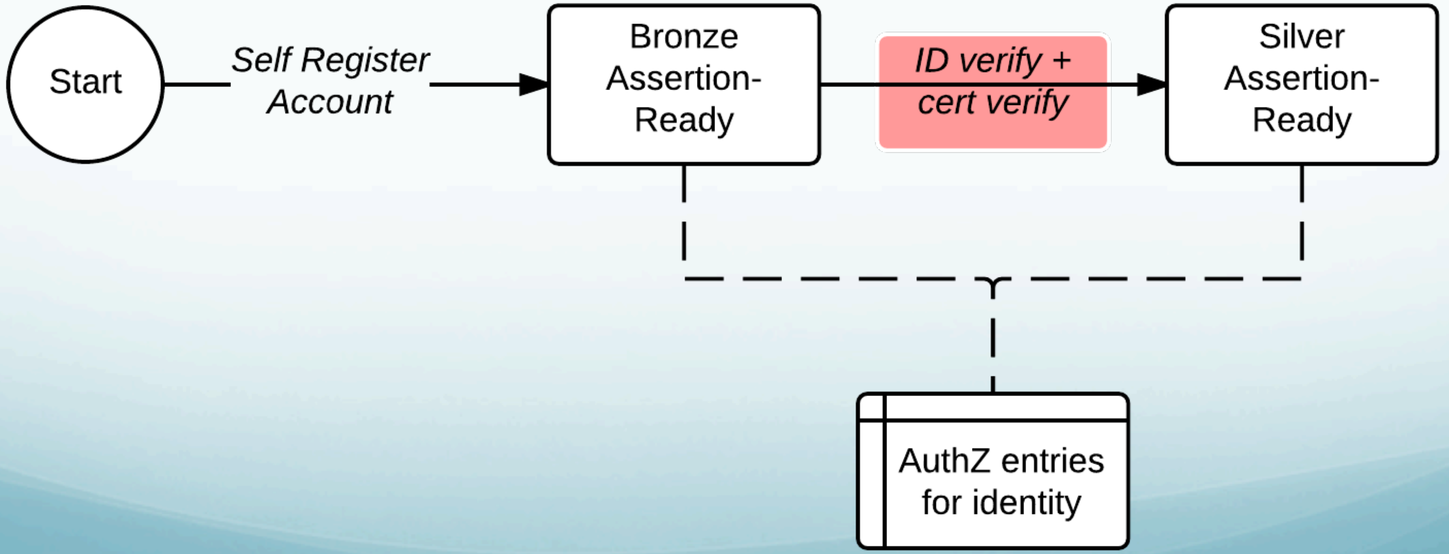
Do auditors audit against 3.1? Is 3.1 normative?

- Section 4.2 is “SPECIFICATION OF IDENTITY ASSURANCE REQUIREMENTS”
- Is 3.1 language (“reasonable assurance”, “likely”, “reasonable care”) implicitly part of IAP compliance requirements?

Relationship to Assurance Escalation

"Assurance escalation" presumes authoritative ID info or existence of shared secret.

- Does loss of certificate control *prior to ID proofing* affect assurance escalation?



More General Questions

Irrespective of formal IAP, most campuses have procedures for non-Silver re-proofing.

- What do you do when 4.2.4.3-type approaches fail?
- Is it worth codifying "reasonable" identity re-proofing processes?
  - Could be added to the IAP, submitted as alternative means, or collected in a standalone guidance doc.

Potentially Tangential Question

Can rules for automated person-matching processes inform reasonable identity re-proofing processes?

- Observation (admittedly small "n")
  - In many cases it appears there is detailed documentation of how use cases in 4.2.4.3-style cases should be implemented, but not much around "if that fails".
- Supposition
  - Processes for automated account matching (including how much to "implicitly trust" the inbound or existing identity data) may be more clearly spelled out – given that they must be coded explicitly – than help desk operational procedures.