Identity and Access Management

Identity and Access Management

In the InCommon identity and access management system, a *primary identity* is a tuple:

primary identity := (email, phone, firstname, lastname)

A primary identity is associated with a primary role:

1. InCommon Executive
2. InCommon Site Administrator
3. InCommon Registration Authority Officer

For example, we think of a Site Administrator as *a person possessing a verified primary identity*. In other words, a *Site Administrator* is a role associated with a verified primary identity in the system. Likewise an InCommon Executive has a verified primary identity, although the verification process may not be the same as the verification process for Site Administrators.

Provisioning

The InCommon Executive identifies the Site Administrators and Registration Authority Officers for the organization. In so doing, the Executive provisions primary identities into the system. Initially, a primary identity is unverified. To become an official Site Administrator or Registration Authority Officer for the organization, that person must verify their identity.

Identity Verification

Identity verification is a basic operation whose objective is to bind the email and phone of a primary identity to a single person. Thus the operation is called Identity Verification:

1. Request an email invitation
2. Click the link in the email
3. Request an one-time PIN
4. Verify the one-time PIN

When first provisioned, a primary identity is unverified. A person with an unverified primary identity has no privileges in the system. In particular, an individual may not be credentialed until their identity is verified. In fact, identity verification and credentialing occur in sequence, that is, identity verification is a prerequisite for credentialing.

A person may verify their identity many times throughout the lifecycle of that identity in the system. In fact, the system may enforce periodic or ad hoc re-verification of a primary identity subject to policy. Every verification event is recorded in the system for auditing purposes.

Credentialing

By definition, a *credential* binds an identity to a token used by a person to authenticate to a relying party (RP). Here the RP is a SAML service provider (SP) and the token is a SAML SSO token. How the person obtains the SAML token in the first place is a separate topic.

The SAML token asserts a *federated identity* for the bearer of the token. If the SAML token contains an email address, the federated identity may be linked to a verified identity in the system. In that case, SAML Web Browser SSO gives rise to a *federated credential* for the user. Assuming the SAML token is transmitted securely to the SP, the strength of the authentication event asserted in the token determines the strength of the federated credential, that is, the strength of the binding between the federated identity and the verified identity. Thus the strength of the authentication event asserted in the token is of paramount importance to the SP.