Multi-factor Considerations

Some institutions are exploring using multi-factor authentication technologies to meet InCommon Silver standards. Motivators include deficiencies in processes for identity proofing, insecure methods for distributing credentials, and non-compliant passwords for existing credentials. Implementing multi-factor in a way that complies with Silver will help improve processes and security.

Using multi-factor technologies to meet InCommon Silver requirements is a challenge because the Identity Assurance Profile (IAP) is designed to address credentials based on an Authentication Secret used for authentication of the subject to the IdP. A typical Authentication Secret is *something you know* such as a password or passphrase. Additional factors—*something you have* or *something you are*—are not addressed in the IAP. Section 4.2.3 of the IAP states, "If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements." Since there are several references to NIST [SP 800-63] throughout this section, institutions may wish to seek guidance from that NIST publication to justify assertions that their multi-factor deployment meets or exceeds the requirements.

Multi-factor Deployment Examples

- CIC Multi-factor Working Group

Participant organizations have provided the content described on this page. Using these practices does not guarantee certification in the InCommon Assurance Program.