Alternative Means for Meeting Criteria in IAP V1.2 Section 4.2.3

Alternative Means for Credential Technology (IAP 4.2.3) to Satisfy the InCommon Assurance Profiles Bronze and Silver, version 1.2.

1. **Requirements of the IAP that the alternative means is proposed to address**

   The organization proposes an alternative means to address the criteria in the InCommon Identity Assurance Profiles version 1.2, section 4.2.3, Credential Technology.

2. **Reasons for proposing the alternative**

   The alternative is being proposed because the current InCommon IAPs are based on use of "Shared Authentication Secret" forms of identity Credentials, typically an identifier and password. The organization has implemented a scalable and secure infrastructure to issue multi-factor credentials, but multi-factor credentials are not included in the Credential Technology described in section 4.2.3. The organizational credential is an x.509 personal digital certificate (PDC) stored on the SafeNet 64K USB eToken Pro device. In Virginia Tech's implementation, the "shared Authentication Secret" is the private key component of the x.509 certificate.

   The rationale for using the PDC on the eToken as the Silver credential is that this multi-factor credential meets or exceeds the effect of the IAP requirements, and a secure, in-person process is in place to issue PDCs on eTokens to employees and graduate students at Virginia Tech. The in-person identity proofing and issuance process adheres to the InCommon Silver profiles and continues to strengthen the security of the infrastructure and processes surrounding use of the PDCs and eTokens.

3. **Mitigation of risks potentially exposed by the alternative means**

   The most likely risk involved in using the eToken is that it can be lost or stolen, and someone else could attempt to use the PDC on the eToken.This risk is mitigated by the fact that the device requires the user to enter an activation password to access the x.509 certificate's RSA private key component, which is generated on the eToken and cannot be exported off the device. Recipients of eTokens are required to sign an agreement not to share their eTokens or activation passwords. Additional mitigating factors are that PDCs are issued with a two year validity period and can be revoked in the event the eToken is lost or stolen.

4. **Management assertion that alternative means is comparable or superior to the cited IAP requirement**

   Management asserts that the organizational credential used to authenticate the Subject to the IdP meets or exceeds the requirements of section 4.2.3 of the IAP. The credential is an x.509 personal digital certificate issued onto a SafeNet 64K USB eToken Pro device. The eToken is activated using a password. Public-private key exchange (client SSL/TLS) is used to perform authentication.

5. **Why and how the alternative means is comparable or superior to the cited IAP requirement**

   The PDC on the SafeNet 64K USB eToken Pro meets or exceeds the effect of the requirements in section 4.2.3 of the InCommon IAP version 1.2 because the SafeNet eToken is a Level 3 multi-factor hardware token as defined in NIST [SP 800- 63-1]. The cryptographic module is validated at FIPS140-2 Level 2 or higher, and the token is initialized with FIPS enabled. A password is required to activate the private key, which is generated onboard the eToken and cannot be exported off the device. Complexity rules are implemented on the activation password to meet the requirements for Strong resistance to guessing specified in section 4.2.3.3 of the IAP version 1.2. The device locks out after 10 consecutive invalid attempts to enter a password.