CIC Multi-factor Working Group

Background

A multi-factor working group was formed with participants from the CIC InCommon Silver Project. Their work is summarized in a discussion of multi-factor implementations and examples. Comments and questions regarding the sample implementations are welcome.

Introduction

This document is intended to aid institutions aspiring to meet the requirements of the InCommon Federation's Identity Assurance Profile (IAP) for Silver level of assurance using muilti-factor implementations. Only sections of the IAP where there is a challenge unique to multi-factor are specifically addressed.

IAP sections discussed in this document:

- 4.2.3 Credential Technology
  - 4.2.3.1 Credential Unique Identifier
  - 4.2.3.2 Resistance to Guessing Authentication Secret
  - 4.2.3.3 Strong Resistance to Guessing Authentication Secret
  - 4.2.3.4 Stored Authentication Secrets
  - 4.2.3.5 Protected Authentication Secrets

For more information about the InCommon Assurance program, terms and definitions, and links to the IAP and IAAF documents and the FAQ, see the Assurance Resources section of this wiki.

Tokens

Tokens commonly used as *something you have* for multi-factor authentication are:

- Out-of-band tokens
- One-time password devices
- X.509 digital certificates, either stored in software or on a hardware device

NIST [SP 800-63] categorizes single-factor and multi-factor tokens. A single-factor token that represents *something you have* must be used in combination with another factor -- typically *something you know* -- in order to achieve multi-factor authentication. A multi-factor token that represents *something you have* requires activation through a second factor of authentication, either *something you know* or *something you are*.

Multi-factor examples

Example 1

A university uses accounts and passwords to authenticate to many services on their campus. The account/password credential satisfies some but not all requirements of the InCommon Silver IAP. The university also issues one-time-password (OTP) devices to faculty and staff. The devices are considered to be single-factor because the device does not require a second factor of authentication for activation. The OTP devices are issued using an in-person process that is designed to meet all the identity-proofing requirements for InCommon Silver. During the issuance process, the Subscriber's university account is linked to a registration record for the OTP device. At authentication time, the user must enter their university account/password combination and must prove possession of the OTP device by entering the generated one-time-password string. The university asserts that the OTP device and its supporting infrastructure meets or exceeds the requirements for InCommon Silver.

Multi-factor problem statement

Since the IAP does not specifically address multi-factor implementations, it is not clear whether both factors used in a multi-factor implementation must meet all requirements for InCommon Silver, or whether it is sufficient for only one factor to meet the requirements. The answer may lie in whether the addition of the factor which does not meet Silver requirements strengthens or weakens the security of the authentication process.

Example 2

A university issues personal X.509 certificates on a USB hardware token device -- a multi-factor cryptographic device according to NIST [SP 800-63]. A password is required in order to activate the device. In order to obtain a certificate on the token, eligible Subjects must bring identifying documents in person to a registration station, where the identity proofing procedures are designed to comply with InCommon Silver. The technical environment and all aspects of the registration and enrollment process are designed to comply with the InCommon Silver profile.

Multi-factor problem statement

The Credential in Example 2 employs public key technology, and the Subject must prove possession of the private key component of the key pair during authentication. Since the Authentication Secret described in the IAAF is generally a password, passphrase, PIN, or symmetric key, language in the IAP is not generally oriented toward public key technology. However, the credential was designed to meet NIST [SP 800-63] LoA 4 specifications. Therefore, the institution will provide documentation supporting the assertion that the credential meets or exceeds the effect of the Silver requirements. References to NIST [SP 800-63] will be used for guidance.

Sample Management Assertions

4.2.3 Credential Technology	These InCommon IAPs are based on use of “Shared Authentication Secret” forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.

Criteria	**Management Assertion** The institution issues an X.509 personal digital certificate (PDC) onto a multi-factor (MF) cryptographic device, using public-private key technology to perform authentication. The device is activated using a password. This is not a typical "Shared Authentication Secret" form of identity Credential, but the institution asserts that this multi-factor cryptographic credential meets or exceeds the requirements of the IAP. Additional guidance is provided in NIST 800-63.
. 1 Credential unique identifier	1. The institution's personal digital certificate (PDC) is issued with a Subject Distinguished Name (DN) and a serial number.The serial number is a unique number in the serial number field. The DN of the PDC contains a UID. The UID is a uniquely assigned attribute of a person in the institution's Enterprise Directory. See the **{link to cetificate profile}** for a complete description of the certificate DN. The serial number and the UID distinguish the PDC from all other Credentials issued by the IdPO. 2. The credential unique identifier maps to at most one Subject because the UID is unique to only one person and is never re-used. 3. By including the UID in the DN, the IdPO clearly associates the Credential unique identifier to the Subject's registration record in the IdMS (Enterprise Directory.) The Verifier utilizes the UID during authentication.
. 2 Resistance to guessing Authentication Secret	See 4.2.3.3, Strong Resistance
.3 Strong resistance to guessing Authentication Secret	1. The institution's PDC on the MF device provides cryptographic strength mechanisms described in NIST [SP 800-63] for Level 3 and 4 assurance, protecting the private key against compromise by on-line guessing. The device is a multi-factor "hard" cryptographic token, requiring the user to unlock the device with a password in order to access the private key. 2. The authentication secret (1024 bit RSA key) has about 80 bits of entropy according to NIST [SP 800-57.] The password used to unlock the MF device is created by the Subject during in-person registration for the device. The password must be at least **{insert length here}** characters long and must contain a numeric (0-9), an uppercase English letter (A-Z), a lower case English letter (a-z), and a special character **(**~!@#$%^&(){}+`-{[|\;'./:"<>?**)**. Access to the MF device is locked after **{insert number here}** invalid attempts to enter the correct password. The password for a locked device must be administratively reset, requiring the Subject to visit the institution's RA office in person.
.4 Stored Authentication Secrets	The authentication secret is the x.509 private key which is generated onboard the MF cryptographic device. The private key cannot be exported off the device; thus it is not escrowed. The MF hardware cryptographic module for the token used by the institution is certified at FIPS 140-2 Level 2, with physical security at FIPS 140-2 level 2. **{insert link to FIPS 140 Certificate here}**. This credential protects stored secrets at NIST [SP 800-6] assurance Level 3, thus meeting the criteria for method 3 in section 4.2.3.4 of the IAP.
. 5 Protected Authentication Secrets	1. When issuing personal digital certificate credentials, the MF cryptogrpahic device generates and stores the user's RSA key pair inside the protected environment of the smart chip in the device. The user's private key component is never transmitted to another Credential Store and is permanently kept on the device. Access to the private key component on the device is password protected and implements a lockout threshold of 10 consecutive invalid password attempts. 2. The user's private key component is never transmitted between services for verification purposes. All cryptographic operations requiring use of the private key are performed on-board the device. 3. The user's private key component is never exposed in a transient fashion. The private key component is generated onboard the MF cryptographic device and never leaves the device.

FAQs

Q1: If your Login Processor allows both single and multi-factor authentications, and you're only asserting silver for two-factor authentications, how will shibboleth distinguish single-factor and multi-factor authentications (that is, will Silver IAQ be asserted in all cases, or only in the multi-factor authentication case). What I'm getting at here, is there any way to do this without always requiring multi-factor authentications for your Silver people?

A1: It looks like we might be able to use the resolver to peek into the login context to check to see **how** a user authenticated (that is, which mechanism they use) and then calculate the level of assurance attribute.

Q2: Does Shibboleth recognize/accept X.509 certificates?

A2: It is possible to do X509 authentication with Shib2. There is a contributed X509 authentication handler:

https://wiki.shibboleth.net/confluence/display/SHIB2/X.509+Login+Handler

Q3: Does Shibboleth recognize/accept OTP for authentication?

A3: It should be possible to use the multi-factor login handler described at https://wiki.shibboleth.net/confluence/display/SHIB2/Multi+Factor+Login+Handler with OATH-HMAC OTP tokens.