InC Ops Assurance Requirements

InCommon Operations Assurance Requirements

InCommon Operations is planning to deploy a two-factor login interface to the InCommon Federation Manager by the end of Q2 2012. At the same time, InCommon and Comodo are considering the feasibility of deploying a two-factor login interface to the InCommon Certificate Manager. This document enumerates the assurance requirements of these two, high-profile services.

Executive Summary

The InCommon Federation Manager and the InCommon Certificate Manager are *high-security applications that must know their users in advance*. Since these applications do not require strong identity-proofing, it follows that Silver is not required for access to the FM or the CM. On the other hand, the applications do require strong authentication, stronger than password alone. Consequently, the FM and the CM implicitly depend on an assurance profile that rationalizes Bronze requirements in the presence of two-factor authentication. Such a profile, dubbed **Bronze + 2FA**, is the logical conclusion of this requirements analysis of the FM and the CM.

Terminology

- The phrase *Identity Assurance Profile* (IAP) refers to the current published version (1.1) of the InCommon Identity Assurance Profiles Bronze and Silver.
- The words *Bronze* and *Silver* refer to the corresponding sections of the IAP.
- For our purposes, *two-factor authentication* (2FA) consists of a password (something you know) followed by something you have.
- The *InCommon Federation Manager* (FM) is a web application for administering Federation metadata.
- The *InCommon Certificate Manager* (CM) is a web application for administering X.509 certificates.

Assurance Requirements Analysis

Federation Manager Requirements

The following requirements are the actual requirements of the InCommon Federation Manager, to be deployed by the end of Q2 2012.

1. InC Ops requires 2FA for all FM users except when the user's physical location is inside the Internet2 security domain.
2. The InC Ops IdP issues Bronze passwords and 2FA credentials to all FM users.
3. The InC Ops IdP accepts a federated Bronze password in lieu of a locally issued Bronze password for any FM user (but remains authoritative for the 2FA credential).
4. The FM accepts assertions from the InC Ops IdP only.

Certificate Manager Requirements

The following requirements are under discussion and for illustration only. Actual requirements will be jointly determined by Comodo and InCommon.

1. InC Ops requires 2FA for all CM users except when the user's physical location is inside the Internet2 security domain.
2. The InC Ops IdP issues Bronze passwords and 2FA credentials to any CM user that needs them.
3. The InC Ops IdP accepts a federated Bronze password in lieu of a locally issued Bronze password for any CM user.
4. The CM accepts assertions from any InCommon IdP that is certified Bronze + 2FA.

Conclusions

- Access to both the FM and the CM is based on access control lists of persistent user identifiers (i.e., lists of ePPNs). Every time the IdP asserts such an identifier, the organization implicitly authorizes access. (Organizations essentially agree to this by signing the Participation Agreement.)
- Section 4.2.2 (Registration and Identity Proofing) of the IAP is irrelevant for the FM and the CM, which implies that Silver is not required for these applications.
- The FM can not leverage federated Silver credentials (or even Gold credentials, if such existed) since InCommon Operations must issue credentials to all FM users. In particular, InCommon Operations will issue and manage the critical second factor.
- Given that the CM currently relies on ordinary passwords, it might seem on the surface that the CM could leverage federated Silver credentials. However, Silver will probably not be enough to justify the total cost of federating the CM. A proposal to federate the CM will be more compelling if it embraces 2FA (not to mention the fact that there are good security reasons for doing so).
- The InC Ops IdP is necessarily certified Bronze + 2FA.
- InCommon IdPs that are certified Bronze will federate with the InC Ops IdP.
- InCommon IdPs that are certified Bronze + 2FA will federate directly with the CM.
- If the InCommon Assurance Program defines a profile for Bronze + 2FA, InCommon Operations will require it for federated access to the CM. Otherwise, InCommon Operations will issue and manage the second factor for all CM users.
- Section 4.2.3 (Credential Technology) of the IAP concentrates on passwords exclusively and therefore needs to be augmented with a new section describing corresponding 2FA requirements.
- Both sections 4.2.4 (Credential Issuance and Management) and 4.2.8 (Technical Environment) of the IAP are specific to Silver but not strictly required for the FM and CM in the presence of 2FA.

Open Questions

- Will the FM or the CM require IAP section 4.2.4?
- Will the FM or the CM require IAP section 4.2.8?