Metadata Signing Process

Metadata Signing Process

The InCommon *metadata signing process* involves the following components and actors:

1. The metadata signing key
2. A Key Authority Officer
3. A Technical Authority Officer
4. The metadata repository

The *metadata signing key* is the private key used to sign InCommon metadata. The public key that corresponds to the private metadata signing key is bound to the metadata signing certificate, which is stored on a secure web server (ops.incommon.org). This key pair together form the basis of the trust fabric of the InCommon Federation.

The metadata signing key is a secure offline key. It is stored on the hard drive of an offline laptop, which is kept in a safe in a secure facility (#1) with strict physical access controls.

Access to the safe itself requires both a key and a pin. A *Key Authority Officer* provides the key while a *Technical Authority Officer* knows the pin. A single individual can not be both a Key Authority Officer and a Technical Authority Officer, that is, no one person knows both the location of the key and the pin. Thus two people with strict separation of duties are required to access the laptop in the safe.

Unsigned metadata is stored in a digital repository on a secure server with limited physical and network access. The server is locked in a cage in a secure facility (#2) with strict physical access controls and video surveillance. The server is protected by a firewall that restricts network access to the InCommon F ederation Manager and the eduGAIN metadata server.

A software process that orchestrates metadata import and signing is run daily according to precise hours of operation. This software process runs on the offline laptop. The Technical Authority Officer initiates the software process in the presence of the Key Authority Officer.

In the same way that a bank deposit box requires two distinct physical keys, the metadata signing process requires two human actors, a Key Authority Officer and a Technical Authority Officer. Only the Key Authority Officer can access the safe while only the Technical Authority Officer can run the software process. Both are needed to complete the metadata signing process. Each limits the actions of the other.