Ensuring the Validity and Correctness of UCTrust Security Information

Ensuring the Validity and Correctness of UCTrust Security Information

The integrity and correctness of UCTrustmetadata and other security-related information is validated through the use of digital signatures, coupled with an initiator / certifier signing process to enforce appropriate review of all updates. This document describes:

- The Initiator / Certifier Process
- Key Management, and
- Organizational Responsibilities

The Initiator / Certifier Process

UCTrust's metadata must be installed nightly from a web-based repository by every Certificate Provider and Resource Provider within UCTrust. This metadata can affect the secure operation of UCTrust, so it is extremely important that incorrect or unauthorized updates are not installed. UCtrust's initiator / certifier process for deploying metadata updates allows these updates to be installed by an unattended, automated process while guarding against incorrect and unauthorized updates.

UCTrust's initiator / certifier process designates two sets of people as *initiators*and *certifiers*. Initiators are responsible for creating and updating information, while certifiers are responsible for reviewing the new information before it is deployed. In brief, the process has the following steps:

1. An initiator produces a file containing the new information
2. The initiator creates a digital signature for the file containing the new information.
3. A certifier reviews the new information for correctness and verifies the initiator's digital signature. If the everything is proper, the certifier creates a digital signature for the initiator's digital signature file. If the information is not correct, the initiator is asked for a correction.
4. The information is deployed, along with the two digital signatures, through the use of some Internet-based distribution mechanism, such as placing the information on a web server or sending it in an electronic mail message.
5. Users of the new information validate its integrity by verifying both of the digital signatures to ensure that it has not been modified, and that it has been produced by an initiator and reviewed by a certifier.

Example: The Initiator / Certifier Process for UCTrust Metadata

The following process is used to prepare updated metadata for deployment:

1. Campuses send a scanned image their UCTrust certification letters to all initiators and certifiers at UCTrust-L@ucop.edu.
2. An initiator collects the updated metadata into a compressed tar file called UCTrustMetadata.tar.gz.
3. That initiator creates the initiator's digital signature file, UCTrustMetadata.tar.gz.initiator.sig, with the following command:
   ```
   SignUCTrustInitiator UCTrustMetadata.tar.gz
   ```
4. The initiator then sends the compressed tar file and the initiator's digital signature file to a certifier.
5. The certifier verifies the correctness of the updated metadata in the compressed tar file. If it is not correct, the initiator is asked for a correction. If it is correct, the certifier creates the certifier's digital signature file, UCTrustMetadata.tar.gz.certifier.sig, from the initiator's digital signature file with the following command:
   ```
   SignUCTrustCertifier UCTrustMetadata.tar.gz
   ```
6. The three files, UCTrustMetadata.tar.gz, UCTrustMetadata.tar.gz.initiator.sig, and UCTrustMetadata.tar.gz.certifier.sig, are deployed on the UCTrust web site. Credential Providers and Resource Providers download the three files on a nightly basis and execute the following command:
   ```
   CheckUCTrustSignatures UCTrustMetadata.tar.gz
   ```
   before using the information to ensure that it has not been modified, and that it has been produced by an initiator and reviewed by a certifier.

Key Management

PGP public/private key pairs are used to create and verify the digital signatures used by the initiator / certifier process. Initiators and certifiers each have a unique key pair, and they are each responsible for the protection of their private keys in a manner consistent for *restricted* data, as described in Business and Finance Bulletin IS-3, Electronic Information Security.

The public keys of all initiators are collected in a "keyring" file called UCTrustInitiators.gpg that is distributed with the SignUCTrustInitiator, SignUCTrustCertifier, and CheckUCTrustSignatures scripts. The public keys of the certifiers are similarly collected in a file called UCTrustCertifiers.gpg. Updates to these keyring files and the associated scripts are themselves distributed via the initiator / certifier process.

Organizational Responsibilities

The UCTrust Federation Administration maintains the following information on the UCTrust web site:

- the current lists of initiators and certifiers
- the current metadata, fully signed
- the scripts and public keyring files described in this document.