Intel Cloud Integrity Technology 3.0

**Key Replacement**

# Background

The key server provides APIs for managing keys but some applications use locally stored keys and are not written to use a key server. For these applications, the key server must be able to reach out and manage the keys where they are stored. There are some commercial key management products that perform this task for specific applications, such as SSL key management or SSH key management.

# Architecture

## Remote Key Placement

This solution is to maintain SSH/SFTP or HTTPS/WebDav client credentials in the key server for remote managed application servers and connect to them as necessary to replace the keys. This would work for things like TLS private keys and certificates, SSH authorized keys, and other keys that are simply kept as files on the remote system.

The simplest form of placement would be entire-file replacement. The key server would maintain the complete contents of the key file and replace the entire file on the remote system. Entire-file replacement should be the default behavior. Another form of placement would be a merge. The key server would maintain some contents of the key file and merge them with what is found on the remote system. Merge behavior may need the user to configure which keys to insert if not present, which keys to replace if present with the same alias but different content, and which keys to delete if present on the remote system.

## NFS Key Retrieval

This solution is to mount an NFS filesystem on the application server and replace the application’s key store file or directory with a link to the mounted filesystem. When the application attempts to access the key store file or directory on the mounted filesystem, the NFS client makes a request to the key server that is implementing the NFS share. The key server can then grant access to the keys based on NFS credentials. If the key transfer policy requires trust, the key server may also request a trust report from Mt Wilson on the application server.

# Implementation

Note: this blueprint has not been completed and is not implemented.