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.

## 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 either 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.