Overview

DigiCert® Software Trust Manager streamlines the complexity of managing keys and signing workflows for Gnu Privacy Guard (GnuPG or GPG) environments with the DigiCert® Software Trust Manager Smartcard Daemon (STM-SCD) feature.

With DigiCert® STM-SCD, organizations are able to leverage Software Trust Manager’s robust key management and access features with GPG’s unique keyring architecture. STM-SCD simplifies signing effort, eliminating the need for the complex scripting and configuration often required by open source tools leveraging GPG’s command line interface. And, STM-SCD provides native support for a broad range of platforms and cryptographic algorithms, simplifying key and signing management for use cases that have often been limited in other tools.

GPG Use Cases

- Debian and RPM package signing
- GPG command line file signing
- OCI-compliant container signing using Redhat tools such as podman, skopeo and buildah
- Git commit signing
- Bouncy Castle key management

GPG-Native Features

STM-SCD extends Software Trust Manager’s robust key management and access and signing workflow capabilities to GPG environments, featuring:

GPG keyring architecture support
STM-SCD supports GPG master and subkey creation and management with separation of duties, key revocation, and synchronization of private and public key servers via graphical user-interface (GUI), SMCTL (Command Line Interface) and REST APIs.

Ready-to-use smartcard interface
STM-SCD is signing-ready in three steps: 1) set up the GPG card status 2) download the keyring and 3) sign files, eliminating the complex scripting and configuration required by other tools.

Broad platform and algorithm support
STM-SCD is pre-compiled and ready for use on Windows, Linux and Mac OS and supports RSA, ECDSA and EDDSA algorithms.

Learn More

Learn more about Software Trust Manager’s Smartcard Daemon for GPG [here](#).