digicert®

Dedicated Private CA with DigiCert Software Trust Manager

Maintain complete control of duration of trust for long-life devices

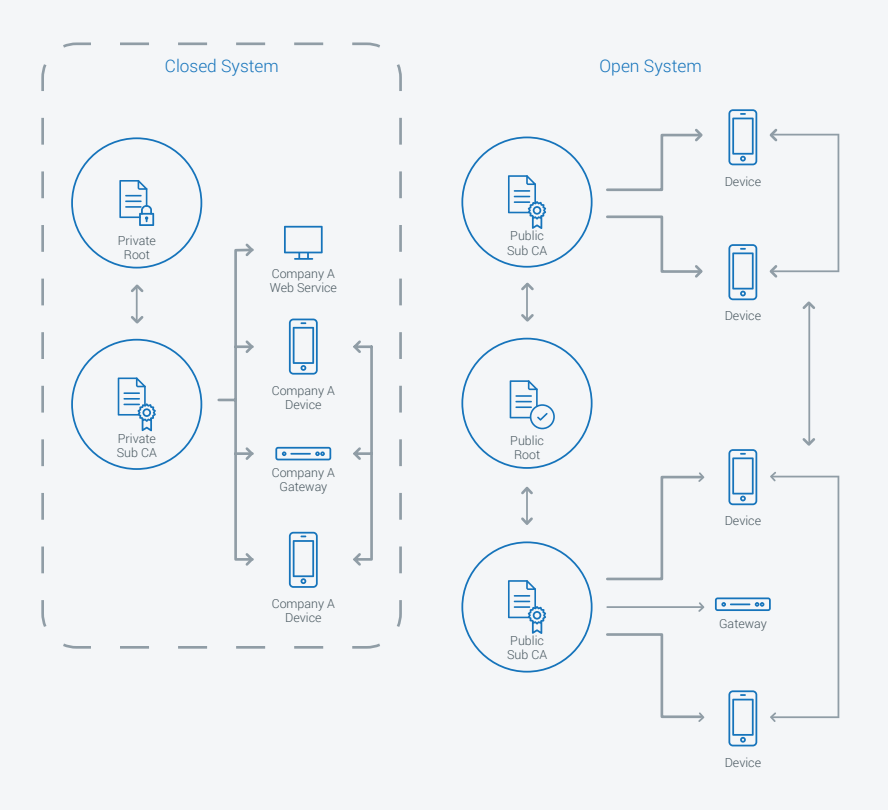
Many machines and devices in the industrial, healthcare and automotive industries have unique trust requirements. Often, these use cases need longer validity periods than baseline requirements allow, and trust needs to be checked on the device. As such, organizations are using private hierarchy services to customize and control deployments for updates, signatures and code on long-life and IoT devices.

Dedicated Private CA + DigiCert Software Trust Manager

With the Dedicated Private CA solution provided by DigiCert Software Trust Manager, you have full control over the chain of trust—from the private root to intermediary to end-entity certificate. Our powerful management solution gives you visibility, agility, flexibility and security.

More, with a Dedicated Private CA, you get management capabilities for private certificates that complement publicly trusted capabilities. You can control every deployment while maintaining secure key management and user management without the upfront costs of running your own CA. You can even save your signing keys in a Federal Information Processing Standard (FIPS) 140-2-compliant Hardware Secure Module (HSM), similar to how you secure public Extended Validation (EV) code signing certificates.

Example Organization's Private and Public Trust



Key benefits

- Secure your keys in the signing service with state-of-art protection. Options include HSMs.
- Maintain agility by deploying unique keys where each release can be signed by a different private key and certificate
- Use dedicated private CAs with flexible end-entity validity duration
- Control who can sign code for specific application, who can issue certificates, and which parameters are set for certificate issuance
- Gain visibility and granular insight into all code signing activity
- Easily integrate with existing tools
- Minimize impact when a certificate needs to be revoked
- Access via the web or API to manage activity from anywhere
- Increase ease-of-use with Command Line Interface/Controller that enables authorized users to generate and manage keypairs and certificates from the command line
- Exercise flexibility with multiple options in storing signing keys
- Centralize signing activities with easy import of existing keys, certificates, ICAs and/or root certificates

Support

DigiCert Software Trust Manager supports a range of files types, enabling signing for firmware and IoT device apps, including:

- Android
- Debian
- Docker Notary
- GPG
- Java
- Linux
- OpenSSL
- RPM
- XML
- Any signing tools that are compatible with PKCS11, Microsoft KSP and Apple CryptoTokenKit

For more information on Software Trust Manager, contact one of our PKI experts at pki_info@digicert.com or visit: www.digicert.com/software-trust-manager