cpl.thalesgroup.com

THALES
Building a future we can all trust

Secure PKI Management solutions with DigiCert® and Thales

DigiCert, the world's leading provider in PKI solutions, has teamed up with Thales, the worldwide leader in data protection, to provide a joint solution for authenticating and encrypting user communications, systems, emails, documents, websites and servers.

The Problem

With today's challenging business environment, organizations need secure remote access for their employees and partners in order to maintain business continuity. Cybercrime is increasing and organizations strive to ensure that only authorized users and devices can access sensitive corporate assets. They also implement email and document exchanges that are secure and can be trusted.

Public Key Infrastructure (PKI) is the defacto security industry standard for authenticating the identity of users and devices, encrypting data and verifying the integrity of documents and communications. In delivering end-to-end protection, PKI requires a robust platform for digital certificate and identity management, and Hardware Security Modules (HSM) to securely generate, manage and store the private keys at the core of the PKI process.

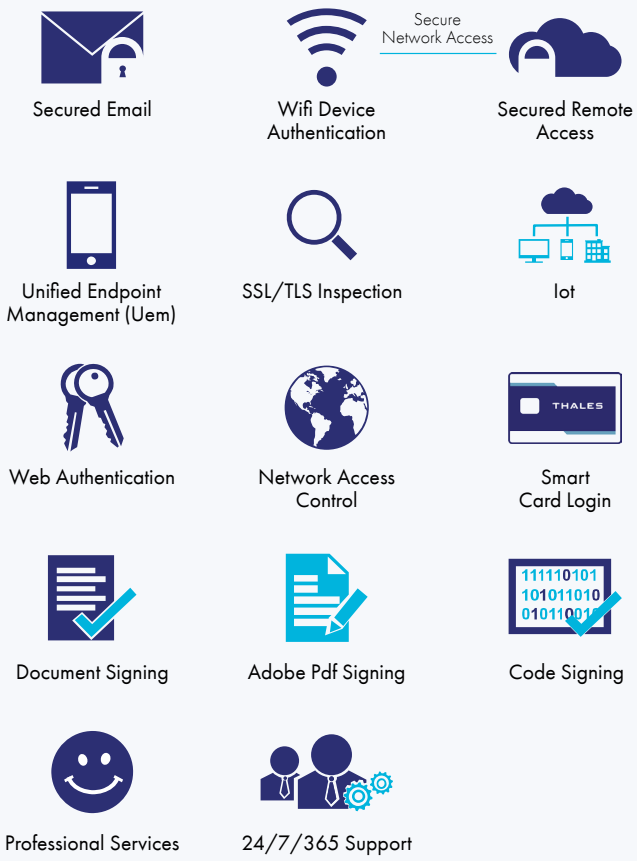
Without an established root of trust creation and storage of PKI private keys, the entire PKI environment can be at risk. Without the right management solutions and tools, PKI deployment and maintenance can be complex and time-consuming.

The Solution

DigiCert PKI solutions secure devices, user access, emails, systems, and documents. With DigiCert PKI Platform 8 or DigiCert ONE managers, organizations can manage digital certificates and user enrollments to power strong authentication, encryption, and data integrity for many use cases. The support for the onpremises Thales Luna HSM or the cloud-based Thales Luna Cloud HSM Service add the assurance that the critical private keys and digital identities are always secure.

PKI enables digital transformation by securing a broad set of use cases and meeting compliance mandates globally. Some organizations need to store their user and certificate data at their enterprise location which necessitates the setting up of a Registration Authority (RA) account. Some set up a private Certificate Authority (CA) hierarchy for their internal servers and communications. Others require a way to recover their private keys if lost.

Use Cases



Key Features & Benefits

Root of Trust for PKI private keys

- NIST FIPS 140-2 Level 3 & Common Criteria EAL 4+ HSM
- Rapid setup, including account, HSM and CA creation
- Protection for Registration Authority (RA) keys used in strong authentication
- Protection of Local key escrow key issuance process

Maintain compliance readiness

- Centralized authentication management of devices, users and servers
- Auto-enrollment and Active Directory (AD) /LDAP integration

Cost effective with maximum scalability

- Can be on-premises or cloud-based, providing high performance and scalability

Full PKI process audit and reporting

- Easy integration with best-of-breed logging, monitoring and alerting packages

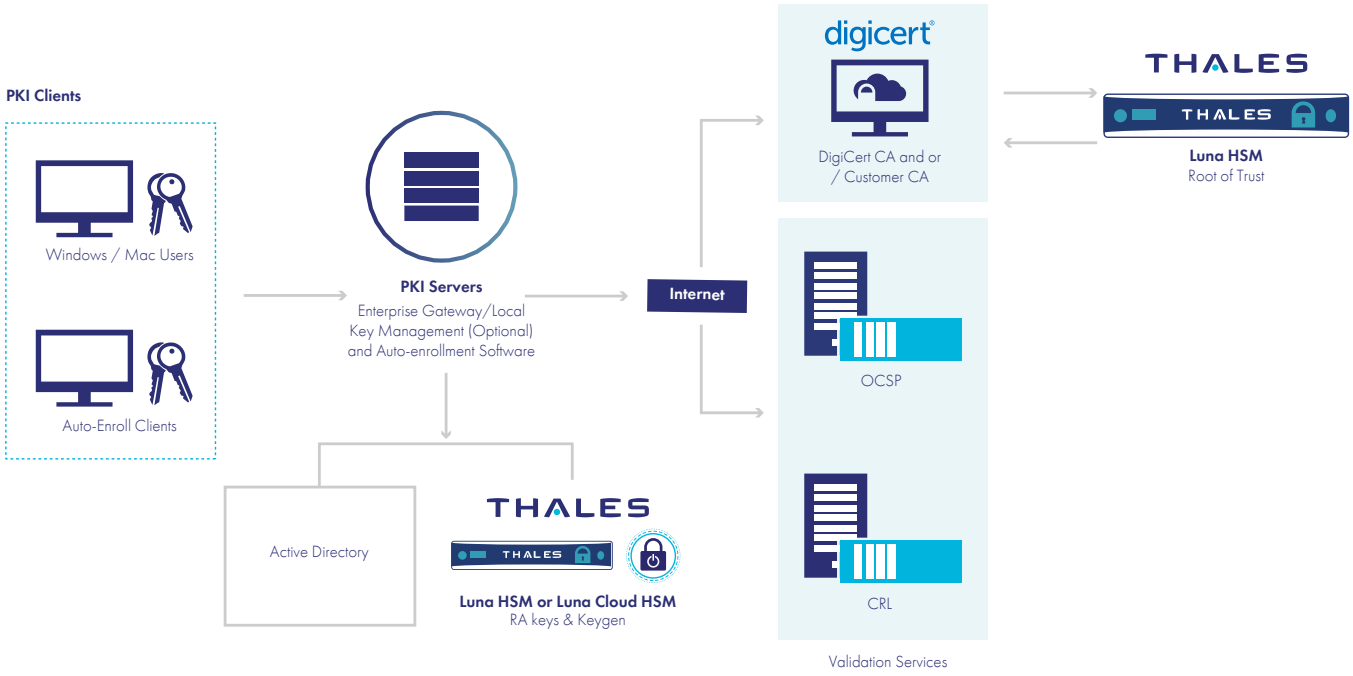
Technical specifications

- Certificate management protocols, including: REST API; SCEP; CMPv2; EST

DigiCert PKI solutions enable organizations to comply easily with their security policies and protect the essential digital certificates and keys. The organizations can store their RA certificates and private keys in Thales HSMs that are connected via a DigiCert RA application or a DigiCert ONE manager.

Thales HSMs are FIPS 140-2 Level 3 validated and add critical levels of security to the PKI solution with a strong architecture that includes side channel attack protection; audit logging; and multifactor authentication. Thales HSMs ensure the critical private keys and digital identities are always secure by generating, managing and storing them in a hardware root of trust to help meet compliance needs.

DigiCert: Thales Solution



This PKI workflow pertains to DigiCert PKI Platform 8 deployment. For DigiCert ONE managers integration with Thales HSM deployment, please contact pki_info@digicert.com

In Summary

Organizations can implement strong security and bestin-class PKI management and key storage solutions from two security industry leaders.

DigiCert PKI and Thales HSMs integrated solutions provide end-to-end key creation and management from certificate issuance to revocation. The seamless integration makes it easy for organizations to deploy PKI and adhere to best practices.

About Digicert

DigiCert is the world's leading provider of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. The most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management solution, CertCentral®. The company is recognized for its enterprisegrade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. DigiCert's cuttingedge PKI platform, DigiCert ONE, was awarded the 2020 IoT Evolution Product of the Year.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

digicert®

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us