HYPERLEDGER IN-DEPTH

DIGICERT PKI & THALES SOLUTION OVERVIEW

digicert® THALES

September 15, 2021

HYPERLEDGER

HYPERLEDGER IN DEPTH: An Hour With...

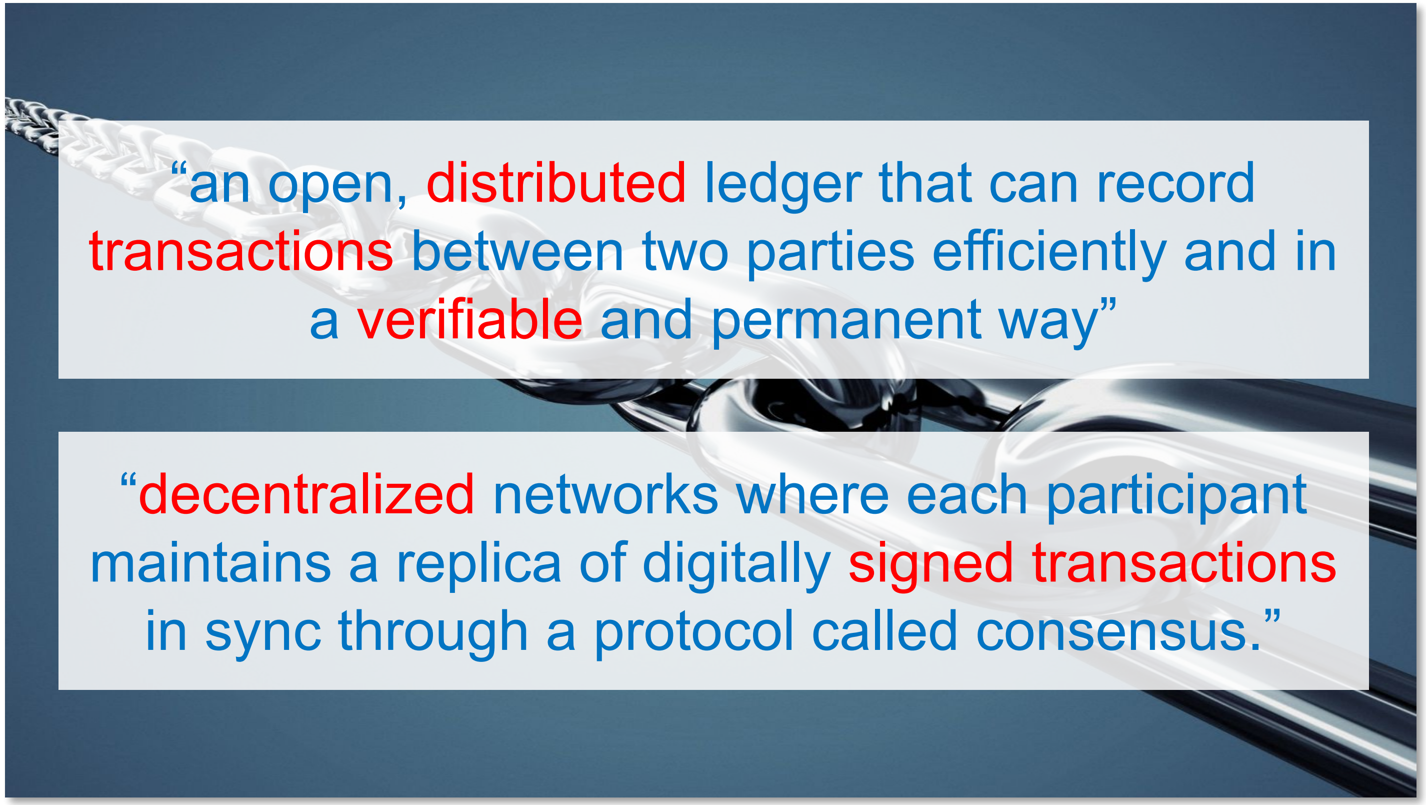
Thales

Increasing Cybersecurity for Hyperledger Fabric

Avesta Hojjati
Head of R&D
DigiCert

Blair Canavan
Director of Alliances,
Digital Identity & Security
Thales

Blockchain?



“an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”

“decentralized networks where each participant maintains a replica of digitally signed transactions in sync through a protocol called consensus.”

A blockchain is:

- A Database
- Distributed
- Secured by design

Source: Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University
https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Blockchain Overview

Overview

- Blockchains store valuable information (distributed ledger)
- Record of transactions between users (cryptocurrency balances)
- Records of contractual agreements
- Proof of ownership of assets

Challenges

- Trust of the ledger is critical in a distributed environment
- All transactions of the ledger must be digitally signed
- Uses cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights

HSM

- Critical to use an HSM to secure the blockchain identity keys
- PKI typically used to issue IDs – HSMs as hardware root of trust
- High quality entropy results in strong keys/identities
- Strong access control to signing keys

Blockchain use cases are emerging in every industry

Banking

- Supply chain and trade finance
- Know your customer
- Transaction banking, payments and digital currencies

Financial Markets

- Post trade
- Unlisted security and private equity funds
- Reference data
- Cross currency payments
- Mortgages

Retail

- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)

Supply Chain

- Workflow digitization
- Supply chain visibility
- Provenance and traceability

Healthcare

- Mediated health data exchange
- Clinical trial management
- Outcome based contracts
- Medicine supply chain

Manufacturing

- Supply chain
- Product parts
- Maintenance tracking

Governance

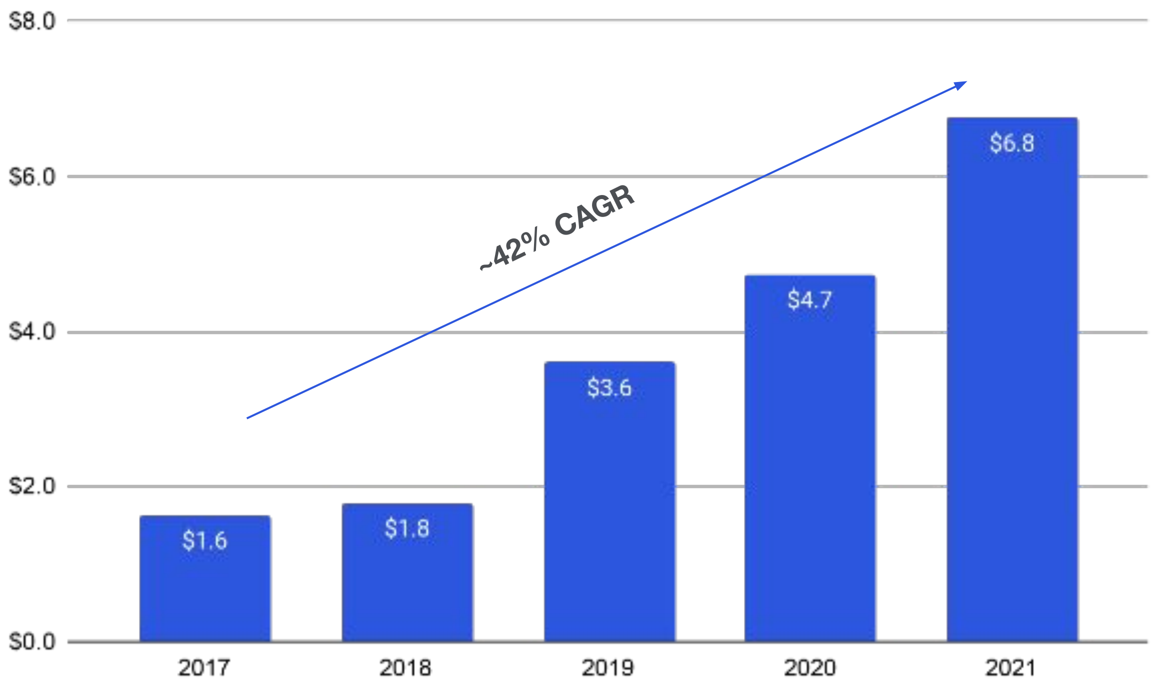
- Asset registry
- Citizen identity
- Fraud and compliance

Insurance

- Complex risk coverage
- Group benefits
- Parametric insurance
- Asset usage history
- Claims filing

Growth of Enterprise Adoption

Global Enterprise Blockchain Market Size ($B)[1]



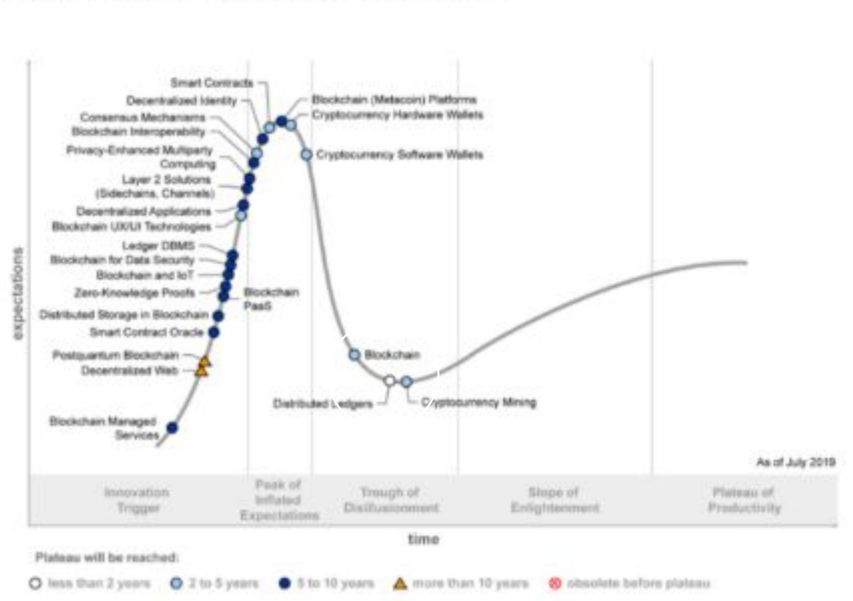
- Projected to ~$6.8B in 2021 (Source: ConsenSys, 2021)
- Increase in Fortune 500 companies across Finance, Supply Chain, Healthcare, Logistic management
- Move from R&D to production applications
- Goal of 1M developers in the ecosystem

Analyst View

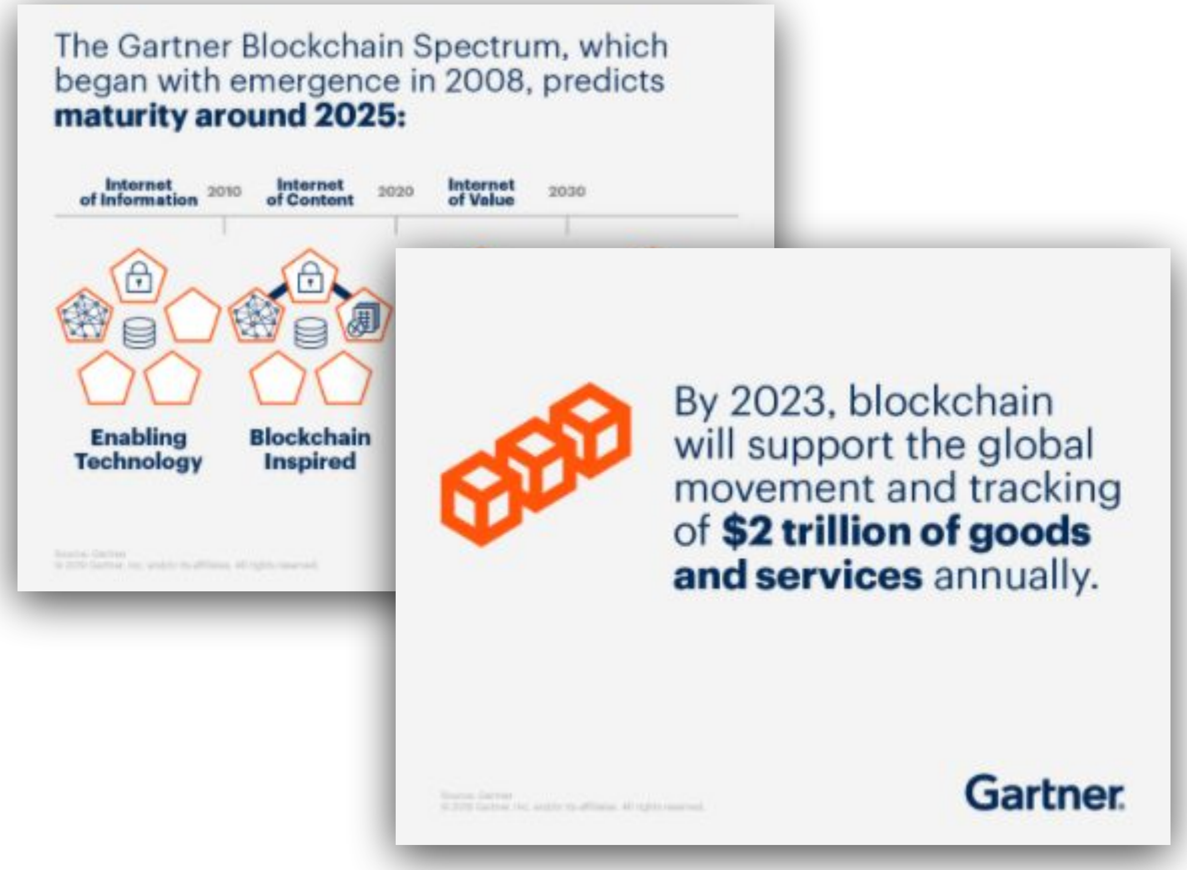
STAMFORD, Conn., October 8, 2019

Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact

Figure 1: Hype Cycle for Blockchain Technologies, 2019



Source: Gartner (October 2019)



The Gartner Blockchain Spectrum, which began with emergence in 2008, predicts **maturity around 2025:**

By 2023, blockchain will support the global movement and tracking of **$2 trillion of goods and services** annually.

Gartner.

Source: https://www.gartner.com/en/information-technology/insights/blockchain

The Value Prop

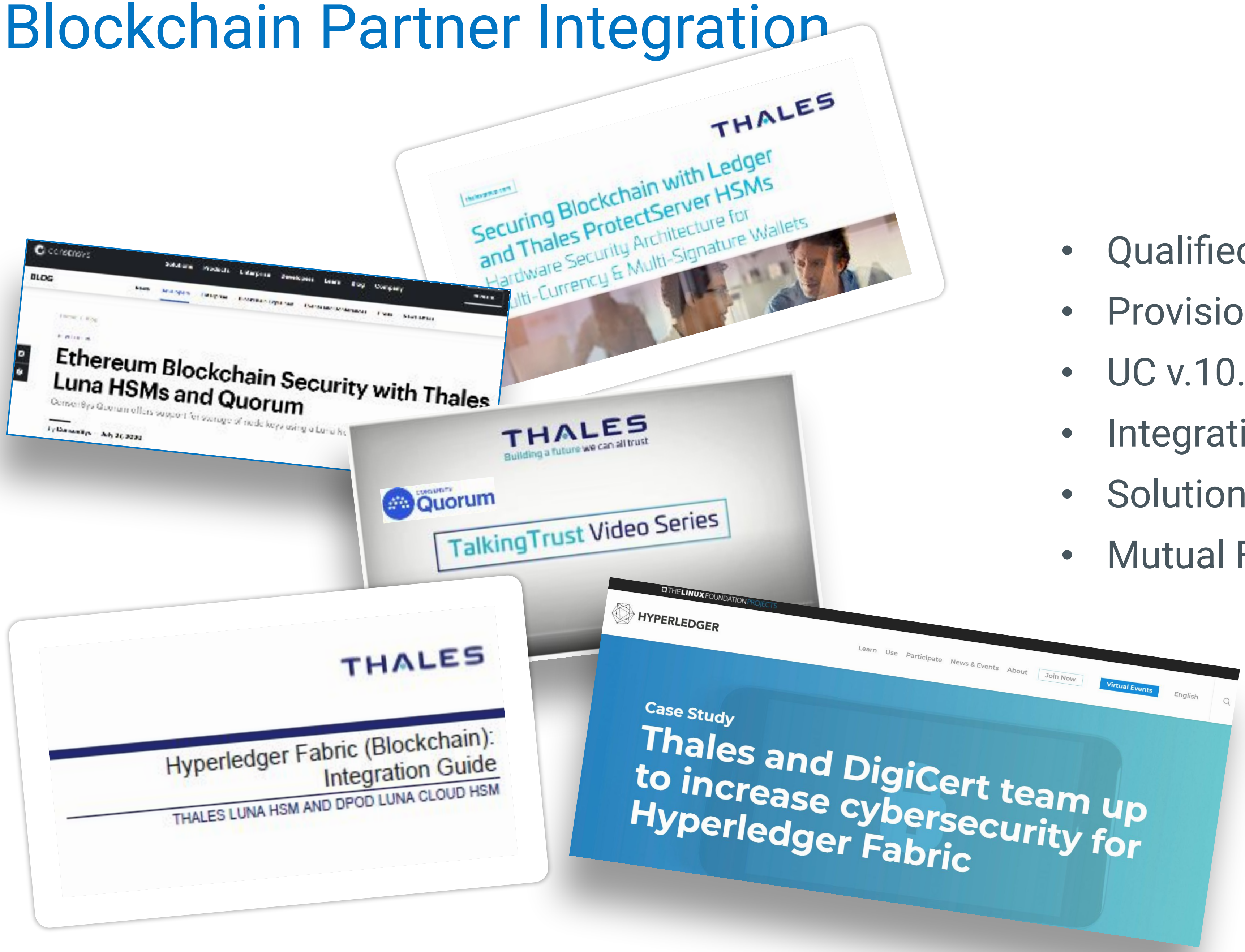
HYPERLEDGER + digicert® + THALES

In 2019, 7.9 billion data records were breached. And yet, 39% of companies aren't using robust data security measures because deployment complexity is a barrier. That's understandable. Implementing cryptography correctly is challenging. It doesn't help that compliance requirements are ever-evolving: to date, there are around 1,800 Global Privacy Laws international companies may need to meet.

Value

- Rapid set up of PKI for Hyperledger Fabric users
- Scalable and cost-effective data security
- On-premises or cloud-based solutions
- Highest level of trust and certificate management

Blockchain Partner Integration



THALES

Securing Blockchain with Ledger and Thales ProtectServer HSMs

Hardware Security Architecture for Multi-Currency & Multi-Signature Wallets

ConsenSys

Solutions Products Enterprise Developers Learn Blog Company

BLOG

Ethereum Blockchain Security with Thales Luna HSMs and Quorum

ConsenSys Quorum offers support for storage of node keys using a Luna H

By ConsenSys July 21, 2020

THALES

Building a future we can all trust

ConsenSys Quorum

TalkingTrust Video Series

THALES

Hyperledger Fabric (Blockchain): Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

THE LINUX FOUNDATION PROJECTS

HYPERLEDGER

Learn Use Participate News & Events About Join Now Virtual Events English

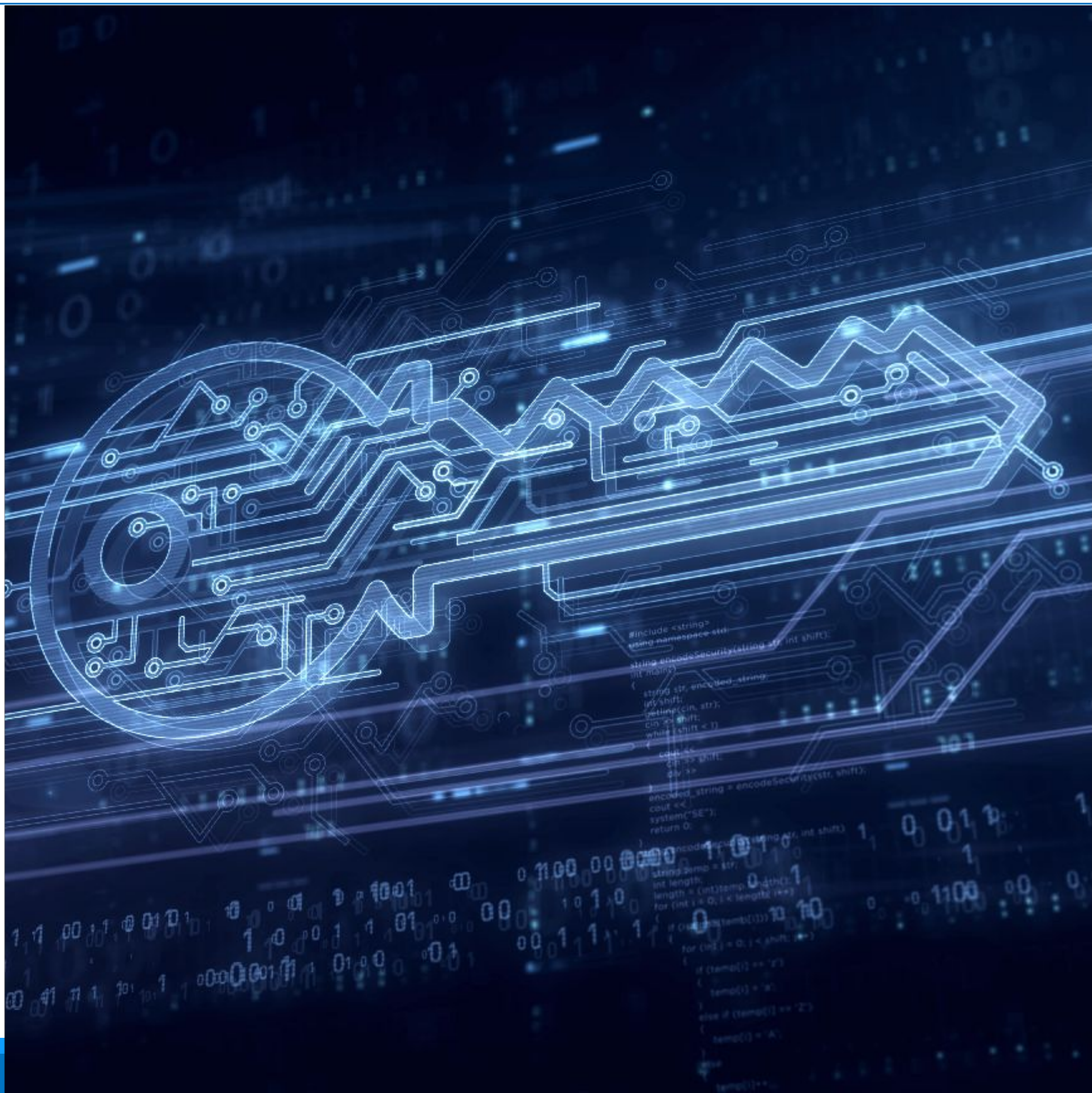
Case Study

Thales and DigiCert team up to increase cybersecurity for Hyperledger Fabric

- Qualified blockchain partners
- Provisioning through DPoD/eLab
- UC v.10.X (PKCS#11default)
- Integration Support (SE/Apps Eng suppo
- Solution Brief, Integration Guide
- Mutual Field Sales engagement

What is PKI?

- Public Key Infrastructure (PKI) is the security industry standard for authenticating the identity of users and devices
- PKI enables verification of the integrity of documents and communications
- PKI requires a robust platform for digital certificate and identity management, coupled with Hardware Security Modules (HSMs) to anchor the root-of-trust by securely generating, managing and storing the private keys at the core of the PKI process



How do Customers use PKI?

Managed Service PKI for Enterprise User Authentication/SSL

- Public/Private Trust
- Fully Managed PKI
- Automation

DigiCert Managed Private Cloud

Capable of supporting distributed environments

- Key Sovereignty
- Data Sovereignty
- Local Resources

Customer Managed Distributed

Government trusted electronic signature workflows

- Key Sovereignty
- Data Sovereignty
- Local Resources

DigiCert Managed In-Country

Government Programs

- Highest Security
- Key Sovereignty
- Data Sovereignty
- National Resources

Customer Managed In-Country

Key Components of PKI

Certificate Authority (CA)

- Stores, issues and signs the digital certificates

Registration Authority (RA)

- Verifies the identity of entities requesting their digital certificates to be stored at the CA

Central Directory

- A secure location in which keys are stored and indexed;

Certificate Management System

- Manages the PKI process, ensuring policy enforcement during access to stored certificates or the delivery of the certificates

Certificate Policy

- Defines the PKI's requirements concerning its procedures. Allows outsiders to analyze the PKI's trustworthiness

PKI Use Case

Secure Devices

Secure User Access

Secure Emails

Secure Systems

Secure Documents

PKI enables digital transformation by securing a broad set of use cases and meeting compliance mandates globally.

DigiCert PKI solutions secure devices, user access, emails, systems, and documents.

With DigiCert and Thales, organizations can manage digital certificates and user enrollments to power strong authentication, encryption, and data integrity.

DigiCert’s support for on-premises Thales Luna HSM and cloud-based Thales Luna Cloud HSM Service add the assurance that the critical private keys and digital identities are always secure, with on premise, in the cloud & in hybrid environments.

DigiCert PKI Solutions

Enterprise PKI

Providing strong authentication and encryption through a unified platform for devices, users, servers and signing backed by a scalable infrastructure.

IoT

PKI works for more than web security. Our scalable and flexible IoT solution provides authentication, encryption, and integrity for all connected devices.

Blockchain

Unparalleled identity and authentication platforms for modern distributed systems such as distributed ledgers

Document Signing

Automated document signing at any volume with options, such as Advanced and Qualified, that comply with geo-specific regulations.

TLS/SSL

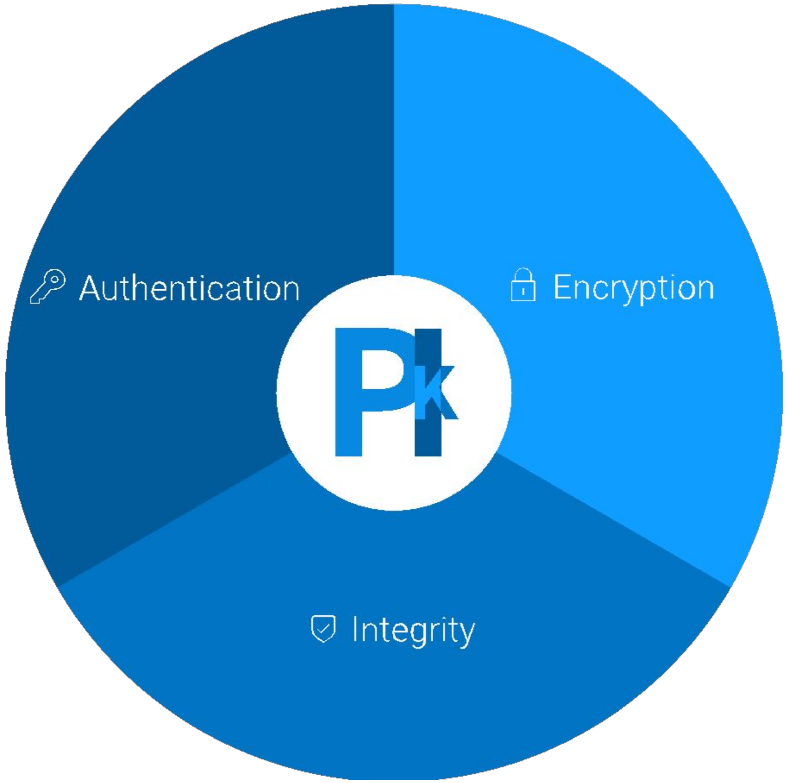
Providing global certificate control, visibility and solution scalability for uninterrupted business. For organizations who can’t afford downtime.

Thales & DigiCert

PKI Solutions for All

digicert® THALES

Why PKI? The Security Solution that Covers Every Angle



Entity Validation

Validating enterprise for a higher level of assurance

Data Encryption

Crucial encryption of sensitive data

Data & System Integrity

Code signing, Integrity of data coming to and from users and devices

Introducing DigiCert® ONE

The biggest idea in PKI - Since PKI

DigiCert ONE is a new approach to PKI that is built around how today's organizations need to deploy and manage security strategies. Unlike current PKI solutions, DigiCert ONE is a unique, containerized platform that delivers industry-leading flexibility, time-to-deployment and continuous updates to the platform's management solutions. DigiCert ONE will change the way organizations and governments deploy, unify and manage PKI at scale, specially considering distributed environments such as Blockchain

A Unified Platform

Managers built on DigiCert ONE

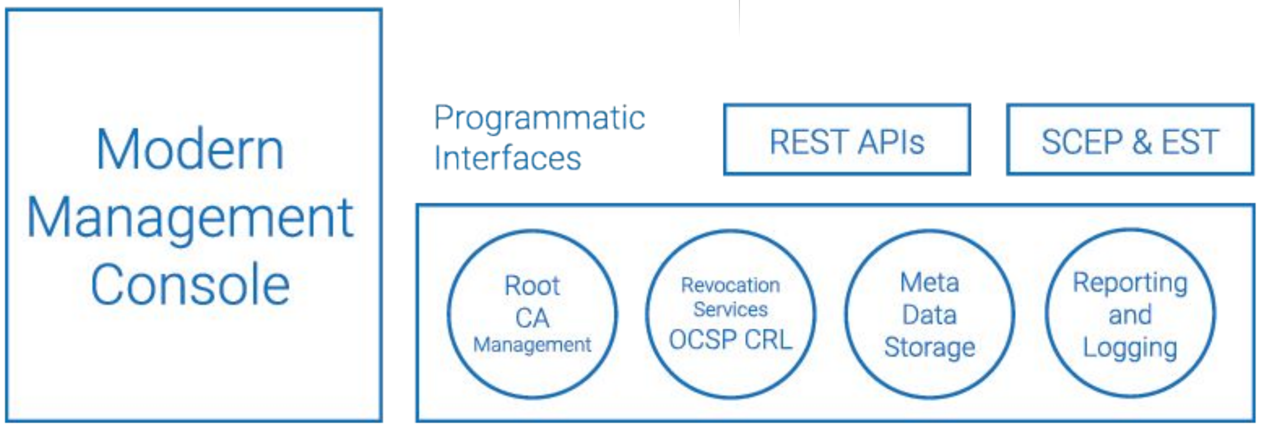
DigiCert® Enterprise PKI Manager

DigiCert® IoT Device Manager

DigiCert® CertCentral TLS Manager

DigiCert® Secure Software Manager

DigiCert® Document Signing Manager



Modern Management Console

Programmatic Interfaces

REST APIs

SCEP & EST

Root CA Management

Revocation Services OCSP CRL

Meta Data Storage

Reporting and Logging

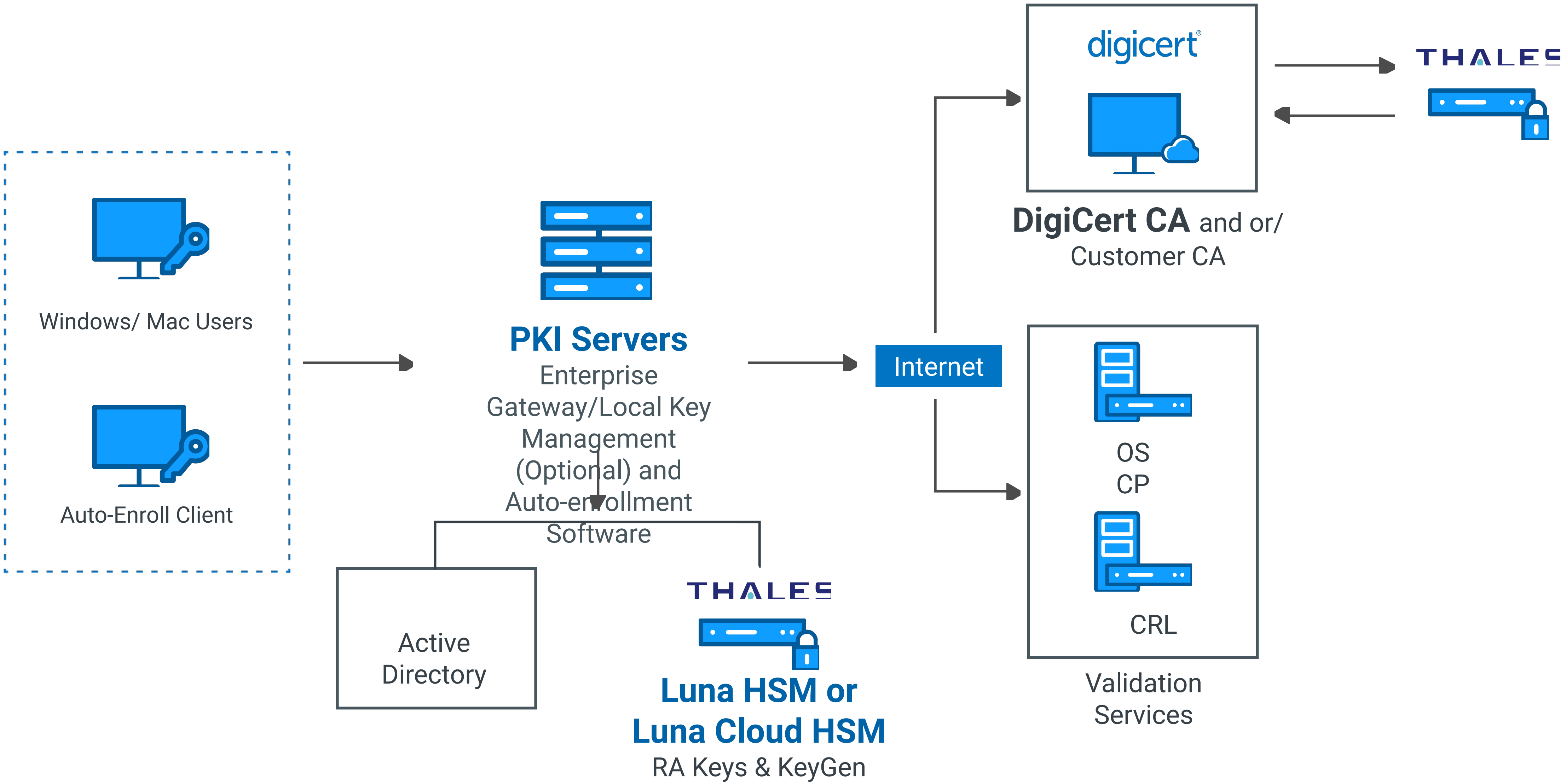
digicert® ONE

THALES

Luna HSM or Luna Cloud HSM

PKI KeyGen & RA Keys & Signing

DigiCert PKI Deployment with Thales HSM



Windows/ Mac Users
Auto-Enroll Client
PKI Servers
Enterprise Gateway/Local Key Management (Optional) and Auto-enrollment Software
Internet
digicert
DigiCert CA and or/ Customer CA
THALES
OS
CP
CRL
Validation Services
Active Directory
THALES
Luna HSM or Luna Cloud HSM
RA Keys & KeyGen

Luna HSMs protecting traditional and emerging technologies

secure PKI root keys

ensure software remains secure, unaltered and authentic with code signing

create secure digital identities for IoT applications

protect blockchain and cloud applications

provide secure IDs for manufacturing

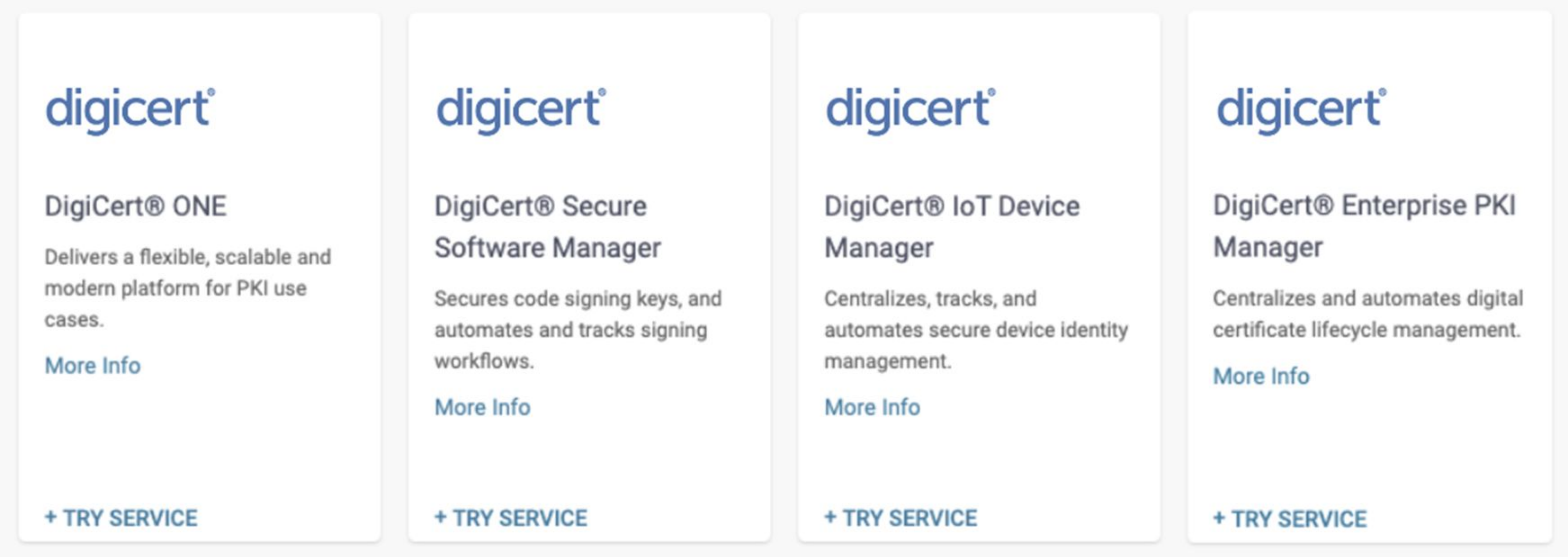
help keep you protected in the quantum era

5G

secure 5G data

ensure key ownership in the cloud

DigiCert Web Tiles on Thales Website



digicert

DigiCert® ONE

Delivers a flexible, scalable and modern platform for PKI use cases.

More Info

+ TRY SERVICE

digicert

DigiCert® Secure Software Manager

Secures code signing keys, and automates and tracks signing workflows.

More Info

+ TRY SERVICE

digicert

DigiCert® IoT Device Manager

Centralizes, tracks, and automates secure device identity management.

More Info

+ TRY SERVICE

digicert

DigiCert® Enterprise PKI Manager

Centralizes and automates digital certificate lifecycle management.

More Info

+ TRY SERVICE

https://cpl.thalesgroup.com/encryption/data-protection-on-demand/services/partner-services

Enterprise PKI Management on DigiCert ONE: A Better Solution

Challenge	Our Solution
Difficult to deploy	Accelerates deployment using standards-based tools and services
Lack of configuration options	Revolutionized HSM configuration and management
Limited options for deployment	Flexible options for deployment: public or private Cloud, or hybrid
Lack of support for third-party applications	Support for the latest business enterprise applications
Limited integration capabilities	Supports standard protocols and REST API
Performance degradation	Supports dynamic environment and scales automatically
Long lag time to create ICA	Supports near-instantaneous ICA creation

Summary Why DigiCert & Thales

ROOT OF TRUST

Protect PKI private keys and drive trust

COMPLIANCE READY

Centralize authentication management of devices, users and servers

COST-EFFECTIVE & SCALABLE

Deploy on-premises or cloud-based, with high performance and scalability

AUDIT & REPORTING

Integrate easily with best-of-breed logging, monitoring and alerting packages for end-to-end visibility

CERTIFICATE MANAGEMENT

Leverage wide range of certificate management protocols

Thales & DigiCert Key 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

HYPERLEDGER IN-DEPTH

DIGICERT PKI & THALES SOLUTION OVERVIEW

digicert® THALES

HYPERLEDGER