HYPERLEDGER IN DEPTH: An Hour With...

Thales
Increasing Cybersecurity for Hyperledger Fabric

Blair Canavan
Director of Alliances,
Digital Identity & Security
Thales

Avesta Hojjati
Head of R&D
DigiCert
A blockchain is:

“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.”

**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

<table>
<thead>
<tr>
<th>Banking</th>
<th>Financial Markets</th>
<th>Retail</th>
<th>Supply Chain</th>
</tr>
</thead>
</table>
| • Supply chain and trade finance  
• Know your customer  
• Transaction banking, payments and digital currencies | • Post trade  
• Unlisted security and private equity funds  
• Reference data  
• Cross currency payments  
• Mortgages | • Supply chain  
• Loyalty programs  
• Information sharing (supplier – retailer) | • Workflow digitization  
• Supply chain visibility  
• Provenance and traceability |

<table>
<thead>
<tr>
<th>Healthcare</th>
<th>Manufacturing</th>
<th>Governance</th>
<th>Insurance</th>
</tr>
</thead>
</table>
| • Mediated health data exchange  
• Clinical trial management  
• Outcome based contracts  
• Medicine supply chain | • Supply chain  
• Product parts  
• Maintenance tracking | • Asset registry  
• Citizen identity  
• Fraud and compliance | • 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
Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact

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.

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

- Qualified blockchain partners
- Provisioning through DPoD/eLab
- UC v.10.X (PKCS#11 default)
- Integration Support (SE/Apps Eng support)
- 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

**Government trusted electronic signature workflows**
- Key Sovereignty
- Data Sovereignty
- Local Resources

**Capable of supporting distributed environments**
- Key Sovereignty
- Data Sovereignty
- Local Resources

**Government Programs**
- Highest Security
- Key Sovereignty
- Data Sovereignty
- National Resources

**Customer Managed**
- Distributed
- 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 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

<table>
<thead>
<tr>
<th><strong>Enterprise PKI</strong></th>
<th>Providing strong authentication and encryption through a unified platform for devices, users, servers and signing backed by a scalable infrastructure.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IoT</strong></td>
<td>PKI works for more than web security. Our scalable and flexible IoT solution provides authentication, encryption, and integrity for all connected devices.</td>
</tr>
<tr>
<td><strong>Blockchain</strong></td>
<td>Unparalleled identity and authentication platforms for modern distributed systems such as distributed ledgers.</td>
</tr>
<tr>
<td><strong>Document Signing</strong></td>
<td>Automated document signing at any volume with options, such as Advanced and Qualified, that comply with geo-specific regulations.</td>
</tr>
<tr>
<td><strong>TLS/SSL</strong></td>
<td>Providing global certificate control, visibility and solution scalability for uninterrupted business. For organizations who can’t afford downtime.</td>
</tr>
</tbody>
</table>
Thales & DigiCert
PKI Solutions for All
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

<table>
<thead>
<tr>
<th>DigiCert® Enterprise PKI Manager</th>
<th>DigiCert® IoT Device Manager</th>
<th>DigiCert® CertCentral TLS Manager</th>
<th>DigiCert® Secure Software Manager</th>
<th>DigiCert® Document Signing Manager</th>
</tr>
</thead>
</table>

#### Modern Management Console

- **Programmatic Interfaces**
  - Root CA Management
  - Revocation Services
  - OCSP CRL
  - Meta Data Storage
  - Reporting and Logging

#### 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

Active Directory

Internet

DigiCert CA and or/ Customer CA

Luna HSM or Luna Cloud HSM
RA Keys & KeyGen

Validation Services

OS CP

CRL
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
- Secure 5G data
- Ensure key ownership in the cloud

5G
DigiCert Web Tiles on Thales Website

https://cpl.thalesgroup.com/encryption/data-protection-on-demand/services/partner-services
## Enterprise PKI Management on DigiCert ONE: A Better Solution

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ROOT OF TRUST</strong></td>
<td>Protect PKI private keys and drive trust</td>
</tr>
<tr>
<td><strong>COMPLIANCE READY</strong></td>
<td>Centralize authentication management of devices, users and servers</td>
</tr>
<tr>
<td><strong>COST-EFFECTIVE &amp; SCALABLE</strong></td>
<td>Deploy on-premises or cloud-based, with high performance and scalability</td>
</tr>
<tr>
<td><strong>AUDIT &amp; REPORTING</strong></td>
<td>Integrate easily with best-of-breed logging, monitoring and alerting packages for end-to-end visibility</td>
</tr>
<tr>
<td><strong>CERTIFICATE MANAGEMENT</strong></td>
<td>Leverage wide range of certificate management protocols</td>
</tr>
</tbody>
</table>
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