HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Case Study:

Thales and Digitcert team up to increase cybersecurity for Hyperledger Fabric

Results

- Rapid set up of PKI for Hyperledger fabric users
- Scalable and cost-effective data security
- On premises or cloud-based solutions

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.

Yet security is not a nice-to-have feature. It's not an opt-in. It's a must. No one will buy your solution if they cannot trust it. It's no wonder companies are exercising diligence when choosing a solution, ideally one that is system agnostic, automated, and simple.

With the emergence of distributed ledger technologies (DLTs) like blockchain, there was a promise that the answer to security was just around the corner.

So, are DLTs the answer to your cybersecurity concerns?

DLTs promise a lot: immutability, transparency, and auditability. Once the network achieves a consensus and information is put on a ledger, users can trust what they're seeing is identical to what was approved as "truth". And if the data is encrypted, only users who are approved will be able to see it. In these ways, DLTs secure data.

However, as with any storage solution, blockchains are not immune to compromise. They are not, by themselves, 100% secure. Blockchains are only one part of an entire system—what happens before the consensus and what happens after data is retrieved has nothing to do with DLTs.

"What blockchains do is provide avenues," explains Avesta Hojjati, Head of R&D at DigiCert®. "They provide an avenue to explore, an avenue to save money, and an avenue to increase security."

"Yet even with this cutting edge, novel technology, cybersecurity still boils down to the good old problems of Public Key Infrastructure and the three rules of security: confidentiality, integrity, and availability," adds Sol Cates, Principal Technologist, CTO Office at Thales. "No matter how amazing your system is, if you forego the basic tenets of security as you integrate blockchain, you are inviting breaches."

This is particularly true when it comes to authenticating and managing the identity of blockchain and DLT users and devices.

“No matter how amazing your system is, if you forego the basic tenets of security as you integrate blockchain, you are inviting breaches.”

— Sol Cates, Principal Technologist, CTO Office, Thales

Identity authentication and management basics

Public Key Infrastructure (PKI) authenticates the identity of users and devices. It includes a Certificate Authority (CA), which verifies an identity and issues a trusted certificate.. It also includes the management of key pairs—the public and private keys that allow secure digital transactions.

Hardware Security Modules (HSMs) securely generate, manage and store the critical keys. These devices are physically protected and tamper-resistant, and may be operationally isolated from other systems. HSMs don’t share space with servers storing emails, documents, or system back-ups. Whether physical or cloud-based, HSMs have just one job: to manage and secure keys.

Certificates are often likened to your passport or driver’s license. They’re issued by a trusted party—or a “CA”. They verify your identity. And they’re hard to fake. Other people can rely on them to identify you.

But that analogy doesn’t explain keys particularly well. For a simplified example, consider a Post Office.

The Post Office checks your identification and issues you a PO Box. In this way, the Post Office is like a CA. It verified your identity and tied your name to a PO Box, which acts somewhat like a certificate. Your box number then serves as your public key. You can share it with others, or they can find it. Once they know it, they can communicate with you. And you can send information to people whose public keys—mailboxes—you know.

But you also have a private key to access your mail. Without this private key, no one can get to the contents of your mailbox. To keep your information safe, you must protect that key. To keep it really secure, you might store it in a wall safe—which acts as the HSM in this example—rather than in your kitchen catch-all drawer, where this key gets jumbled with junk and others might come across it inadvertently or purposefully.

While this example is extremely oversimplified, it offers a basic sense of how PKI and HSMs secure data and transactions.

In reality, PKI and HSMs provide more than mere authentication of identity and secure access via your private key.

PKI also provides encryption…imagine a magical envelope that renders the contents unreadable until you retrieve the correspondence from your mailbox. And it ensures the integrity of sent information, preventing alteration in transit by any other party. HSMs generate these private keys using advanced cryptography and protect user information, data confidentiality, and authentication of networks.

To be secure, blockchain and DLT solutions must still meet standard cybersecurity practices and requirements. Key management—making sure that keys are kept confidential, their integrity is protected, and they are always readily available—is critical.

Without this key management, you may as well make copies of your PO Box key and hand them out to anyone who wants one, with the knowledge that they'll make their own copies to pass around.

Understandably, key management is a constant challenge for companies. They don't have just one set of keys to secure or a few documents to protect. Enterprises can generate many hundreds of key pairs an hour—and each key contains from 2048 to 3072 bits.

With remote employees and partners, multiple devices accessing networks, and secure email and document exchange, enterprises authenticate identities, encrypt data, and verify the integrity of documents and communications countless times a day.

That's a lot of information to manage and secure. It requires a robust platform for certificate, key, and identity management; and it requires a way to generate, manage and store the private keys.

Yet blockchain by itself does not provide all of these requirements.

And this is where DigiCert and Thales come together.

A security partnership moves to Hyperledger Fabric

DigiCert, a leading provider of PKI, and Thales, a leader in data protection, have a decade's long partnership helping their clients authenticate and encrypt communications, systems, emails, documents, websites and servers.

They've also been co-members of Hyperledger for several years. A number of their industry partners, including IBM, Oracle, financial service providers, and others, use Hyperledger Fabric. The companies wanted to support the demands of their industries on Hyperledger Fabric, so a collaboration was only a matter of time.

DigiCert and Thales believe in security by design—a principal in which a solution is designed to include established security principles from the beginning, rather than relying on reactive add-ons. Consider the difference between building a bank from the ground up versus converting an old primary school into a bank. The former would have a vault integrated into the foundation, hardened walls, and limited access points. The latter's retrofits would never reach the same quality standards.

Both DigiCert and Thales have seen companies take the latter approach with blockchain solutions or services and then given up because "it didn't work." They would like to address that for users of Hyperledger Fabric.

"The fundamentals of security have not changed, just because we're going to a cloud-based or highly distributed blockchain environment," says Cates. "The same principles of protecting those keys apply. We don't need to pivot into a new architecture. We can use the same principles financial institutions have been using for decades."

Over those decades, performance improvements and efficiencies developed. These refined principles now allow infrastructure to scale while maintaining performance. And whether on-premises or cloud-based, the approaches to key authentication and management are the same.

Establishing trust

Public trust requires trust within internet browsers. This means browsers trust that "you are who you say you are", so when users access your site, those users can also trust this to be true. This is where certificates and CAs come in.

Private trust, on the other hand, could be IoT devices in a closed environment not accessed by the public. For private trust, there are emerging security compliance requirements, though security best practices are making a significant impact.

For public trust, however, a CA must meet several compliance requirements. These are mandated by the Certification Authority Browser (CA/B) Forum. All publicly trusted CAs and browsers belong to it.

One of the CA/B compliance requirements is an HSM to manage private keys.

And while HSMs are not strictly required for all situations, it's a best practice to use one "I get asked all the time: 'Can't we do this without HSMs?' And yes, technically you can," explains Cates. "But why would you? Why would you take the risk of leaving those keys unsecured when you could have the comfort of knowing the keys are protected at all costs in a hardware root of trust?"

"Anytime you have a public or private key," adds Hojjati, "you want an HSM to increase your security."

DigiCert, which focuses only on PKI, operates at the highest level of compliance for publicly trusted certificates. Using its easy-to-set-up and scalable solutions, organizations can manage digital certificates, user enrollments and implement strong authentication, encryption, and data integrity across all use cases.

Storing certificates and private keys in a Thales Luna HSM adds critical levels of security. Luna HSMs are FIPS 140-2 Level 3 validated, which is one of the highest levels of government certified assurance available on the market. Additionally, Luna HSMs are also Common Criteria EAL4+ certified.

When both are incorporated into the blockchain, the integrity of the blockchain is heavily assured and protected.

> **"Anytime you have a public or private key, you want a Luna HSM to increase your security."**
>
> — Avesta Hojjati, Head of R&D, DigiCert

How it works: Now and in the future

Simply put, DigiCert secures devices with keys and Thales secures those keys. And together they serve to secure solutions using Hyperledger Fabric.

To start, a client creates an account within DigiCert's platform, which allows the client to issue publicly and privately trusted certificates. Then they use DigiCert's API to integrate it with Hyperledger Fabric and replace the native CA. From that point, clients can use Luna HSMs as a strong foundation of digital trust.

Thales manages its integrations utilizing Hyperledger Fabric, which is a delicate and highly exacting type of integration. Within the nuance of security, there is no "good enough"; it has to be fundamentally as sound as you can possibly get. "It's got to be done right, but once it's done you build on that, ensuring the maintenance is easier over time," says Cates.

Though the integrations are separate now, the companies are looking at broader integration. "We're working with Thales to have this as a single product," says Hojjati. "In that product you'd have CA and the HSM integrating to Hyperledger Fabric with one point of contact for key pairs and certificates."

Beyond integrating into one product, DigiCert and Thales keep watch on the trends in cloud HSMs, quantum computing, and function based operations.

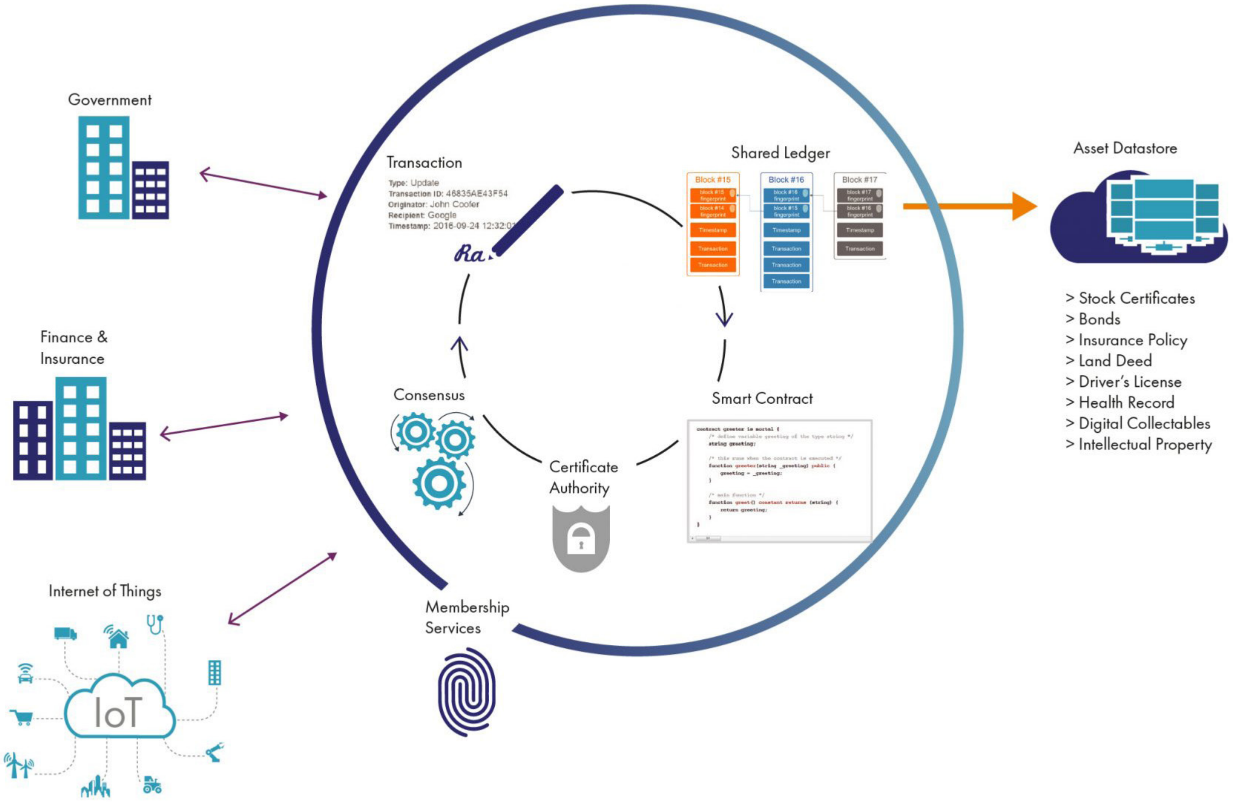
With more IoT devices and distributed models deploying, a more distributed and scalable approach to HSMs may be necessary. “The lifecycle of HSMs is often long, so the migration to the cloud may take some time,” says Hojjati. “But more and more customers are asking about cloud-based HSMs.”

And Luna HSMs are not only blockchain ready, but they’re also quantum ready and crypto agile. “We can swap out algorithms on the fly in front of the problem or as the problem presents itself,” explains Cates. ”Crypto agility provides you with the ability to quickly react to cryptographic threats by implementing alternative methods of encryption, including quick migration to a new post-quantum resistant PKI root, and new algorithms.”

“We build our projects on the same fundamentals we provide banking, government, and other security-minded clients,” he adds. By focusing on the underlying tenets of security, DigiCert and Thales provide trust and assurance for blockchain, now and into the future.

> **“Security has to be done right, but once it’s done and you build on that, the maintenance is easier over time.”**
>
> — Sol Cates, Principal Technologist, CTO Office, Thales

Blockchain as an Infrastructure



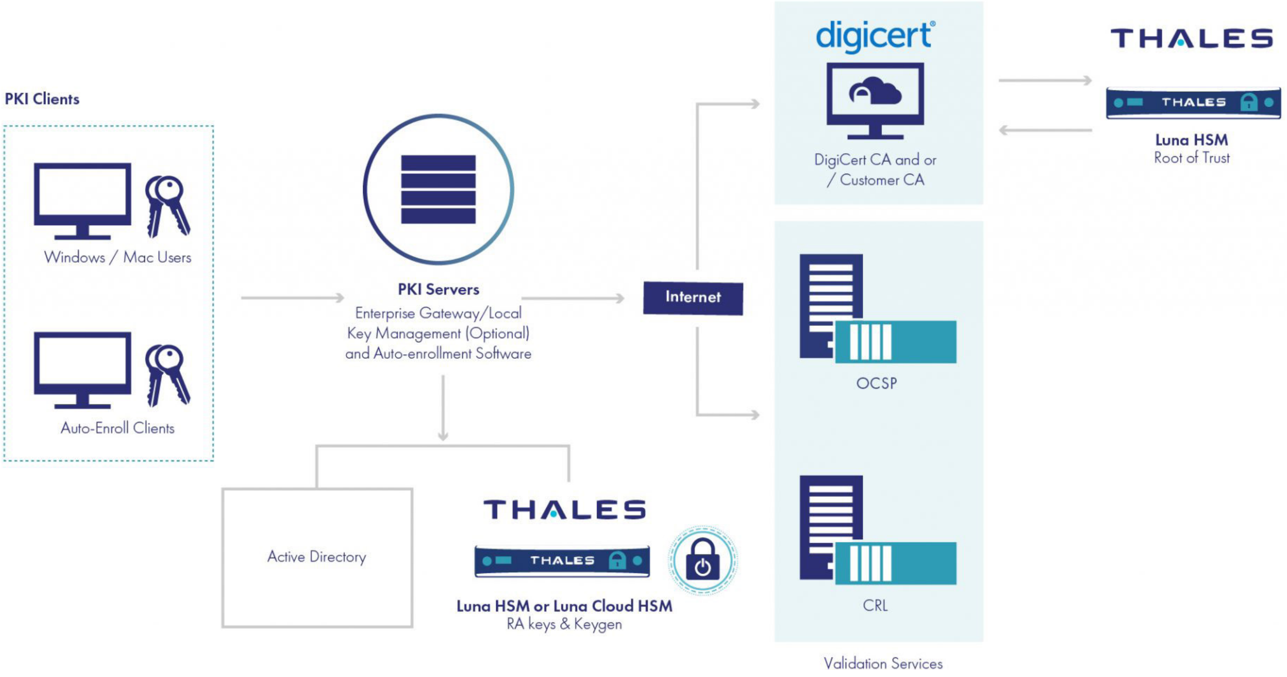
Type: Update
Transaction ID: 46835AE43F54
Originator: John Coofer
Recipient: Google
Timestamp: 2016-09-24 12:32:0

```
contract greeter is mortal {
    /* define variable greeting of the type string */
    string greeting;

    /* this runs when the contract is executed */
    function greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

> Stock Certificates
> Bonds
> Insurance Policy
> Land Deed
> Driver's License
> Health Record
> Digital Collectables
> Intellectual Property



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. To learn more, visit https://www.thalesgroup.com/en

About DigiCert®

DigiCert is a leading provider of scalable security solutions for a connected world. The most innovative companies, including the Global 2000, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports SSL/TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management platform, CertCentral®. The company has been recognized with dozens of awards for its enterprise-grade management platform, fast and knowledgeable customer support, and market-leading growth. To learn more, visit https://www.digicert.com/

About Hyperledger

Hyperledger is an open source effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in banking, finance, Internet of Things, manufacturing, supply chains, and technology. The Linux Foundation, the nonprofit organization enabling mass innovation through open source, hosts Hyperledger. The Linux Foundation also enables a worldwide developer community to work together and share ideas, infrastructure, and code. To learn more, visit https://www.hyperledger.org/

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS