GIGAOM

REPORT

Public Key Infrastructure

The Value of Moving PKI to the Cloud

SIMON GIBSON

TOPICS: CLOUD SECURITY AND RISK

SPONSORED BY KEYFACTOR

GIGAOM

Public Key Infrastructure

The Value of Moving PKI to the Cloud

TABLE OF CONTENTS

1 Summary

2 Determining PKI Ownership

3 Robust PKI Cloud Deployment Simplified

4 Industry Case Studies

5 Investment in the Business: Cloud-based PKI

6 About Simon Gibson

7 About GigaOm

8 Copyright

1. Summary

The role of the CIO has evolved and encompasses more than managing servers, data centers, and the applications that ran on them. The CIO must now come to grips with potentially hundreds of cloud applications and platforms, including some that are not being secured within their organizations.

Most importantly, CIOs must manage the interconnected nature of these many SaaS applications. They must understand their use cases, the administration, and ownership of them as well as be able to make risk-based decisions about what should and should not be allowed to interconnect. At the core of it, applications, identities, and data must be validated so informed decisions can be made upstream. While the focus of the CIO has shifted, the job description is only now being updated. Given this, the CxO needs to be as flexible as possible while leveraging the cloud to control risks such as multi-factor authentication or security event management. This flexibility is not just about the tools they choose, but proactively addressing risks the business faces to secure treasury, customer data, and supply fulfillment; and of course managing audit and compliance requirements.

Public Key Infrastructure (PKI) ensures higher levels of security when deployed within organizations by validating the authenticity of resources and encrypting data as follows:

- Verifying the authenticity of an endpoint, such as mobile devices, insulin pumps, industrial control systems, and even file servers. This verification is critical when you consider the importance of something like downloading quarterly financials.
- Ensuring data has not been tampered with.
- Controlling who can get access to the data.
- Guaranteeing the servers are authentic.

Enterprises that want to stay competitive understand that reputation and trust are very difficult assets to earn back once they are lost. By using PKI, they are able to gain an edge that enables them to make security decisions based on sound cryptographic fundamentals. Doing this ensures decisions made upstream with SaaS, PaaS and identities, applications, and encryption are sound and grounded.

PKI can and should be applied to every digital identity across the enterprise including devices, apps, and people. Yet all too often it is not, due to the complexity and cost associated with an on-premises do-it-yourself implementation. Despite their necessity, successful deployments have historically remained out of reach for most organizations, and concernedly so, mistakes can put you out of business should you become unable to decrypt critical data. If not correctly deployed, the foundation of subsequent security decisions will be intrinsically flawed.

Keeping PKI centralized on-premises requires a tremendous amount of resources to run and may not even adequately cover everything like signing or public certificate authorities (CAs). Failure of any one facet can be catastrophic. For this reason, a cloud-based deployment model allows enterprises to fully

secure the environment with a simple deployment, while reducing maintenance operations – resulting in real TCC savings over time.

In Table 1 below, the necessity and risks involved in certificate use cases.

CERTIFICATE USE CASES	CHALLENGE AND RISK
Every certificate issued is important, whether it is used to encrypt communication, verify the authenticity of an endpoint, or used to grant or deny access.	When certificates expire, services are disrupted, causing unplanned outages and downtime.
Certificates ensure that only designated people and systems can connect to specific resources.	Not having a system in place to manage certificates creates a risk that rogue machines and users can connect to sensitive data and resources. Lack of central management adds overhead.
Remote access through VPNs can rely on certificates to allow or deny access to the inner enterprise networks and systems.	Failure to effectively manage could allow unauthorized access and compromise the network.
Certificates allow the organization to know which devices belong with the company and which ones are authorized for use.	Maintaining a centralized view of all certificates enables IT to know whether or not a machine is authorized.
Organizations rely on SSL/TLS certificates to secure their websites and protect their customers.	Not maintaining certificates can cause the website to malfunction, which can result in loss of business and reputational damage.
Organizations must be able to respond to cryptographic vulnerabilities quick as they arise such as HeartBleed or the Lucky 13 padding attack quickly and thoroughly.	When vulnerabilities are uncovered, organizations must upgrade their certificates quickly and do so across every platform where they are used.
For companies that sell hardware and software, PKI allows their products to be verifiably authentic.	Without authentication, hardware and software can be tampered with within the supply chain.
Organizations that rely on licensing their products recognize revenue.	Authenticated software and hardware can be pirated or the license bypassed.

Technical Example

Fundamentally PKI is the creation, issuance, management, distribution, usage, storage, and revocation of digital certificates. These certificates are used to authenticate the identities of various parts of the data transfer process, as well as encrypt traffic between different endpoints.

Take online banking as an example:

1. Phishing sites pose as authentic websites, trying to trick unwitting users into entering personal information.
   Example: Using PKI, the bank is able to create certificates that cryptographically prove they are who they claim to be and the user can distinguish the phishing site from an authentic site.

2. Entering credit cards or other sensitive information to a bank site needs to be encrypted so that other devices on the network are not able to capture the information.
   Example: Using PKI, banks are able to encrypt the traffic from their web servers directly to the user's desktop or mobile device.

3. Malware can be inserted into code that users believe to be safe, and when installed, create vulnerabilities.
   Example: With PKI deployed, software manufacturers are able to sign their software, allowing their customers to verify the authenticity of the code and confirm it has not been tampered with.

2. Determining PKI Ownership

Enterprises rely on authentication and encryption, yet most have not identified clear ownership of a comprehensive PKI policy and implementation. Not surprisingly, when it is not run by dedicated resources or the ownership model is distributed, organizations commonly get into trouble.

Enterprises should ask the question, "Who owns the PKI budget?"

In most cases, unless it is mandated and funded, the answer is often "nobody." This is not uncommon, though it is the first sign that exposure risks lie ahead. Lack of ownership can lead to costly mistakes that include failed audits, reputational damage, downtime due to expired certificates, and even the inability to decrypt data (a sort of self-inflicted ransomware attack).

With all of this at stake, cloud-based PKI is more than just a simple cost-to-value proposition; it ensures that the most fundamental components that secure your infrastructure are built reliably, are centralized, and are unequivocally protected. Getting PKI right is crucial in today's world, and should be part of every enterprise's security roadmap.

Properly deploying and managing on-premises PKI requires a significant investment in dedicated resources and security expertise that is in high demand. Taking highly skilled people from the core mission of the business and putting them on PKI projects means a lost opportunity that could stifle productivity. To run PKI correctly demands rigor. The storage of root keys and management of key issuing servers or hardware is complicated and costly. Ensuring the data center has adequate physical security that includes isolated locking cages, cameras, access controls, and procedures to ensure everything is enforced correctly is paramount. Doing this correctly requires redundancy, all the way to having a second data center, more machines, and procedures. Organizations have PKI deployed and centralized, have used processes to ensure it is secure and being run correctly. Some essential questions around processes include:

- Where in the budget is it?
  - In some cases, it may be in the IT budget
- Who is responsible for it?
  - Is there an escalation path?
  - Have they been trained, or was it added to their existing duties?
- Where are the keys stored?
  - Who has access to the servers with private keys?
- What is the usage policy that protects it?
  - Has the policy been kept up-to-date?
- Do we test the policy?
  - Can we recover keys?

3. Robust PKI Cloud Deployment Simplified

Given this complexity, more and more organizations are taking advantage of PKI cloud deployments that are based on the following:

1. **Asymmetric encryption**: Wherein two keys are created. One is private and not shared. The other is public and can be shared with all – hence the name Public Key Infrastructure. These keys are used in a number of ways to powerfully solve different types of problems like ensuring that an endpoint is what it claims to be and used to create encrypted channels.

2. **The root of trust**: The root of trust is established by a Certificate Authority (CA). This can be an organization or a governing body able to issue certificates and verify the identity of the certificate requestor. This ensures that certificates can be trusted or revoked if they are to become untrustworthy.

Keyfactor uses these two techniques and creates a secure method to manage digital identities including devices, apps, and people across the entire organization. Keyfactor runs a secure PKI that is easy to deploy and simple to use with the ability to escrow keys and set a threshold for key reassembly, key generation within a hardware security module (HSM), and managed databases that contain information about keys, their expiration date, and the ability to revoke keys. For each step of the process, Keyfactor brings experience and dedicated resources to make the process of identifying and securing assets through the use of digital certificates simple and secure. Their proven platform simplifies PKI for organizations by taking the overhead and cost of management from the enterprise and bringing it into their cloud.

The Keyfactor PKI solution, Keyfactor Command, allows customers to get up and running quickly. Keyfactor Command integrates with existing public and private Certificate Authorities, enabling a complete view into all of the PKI deployments across the organization. This capability is just one attribute that sets Keyfactor apart. The ability to monitor and manage every certificate from a single place allows for a continuous inventory and root trust management. Keys can be delivered to endpoints or generated on them. PKI enables organizations to monitor for expiring certificates, issue new ones before they cause downtime, and revoke certificates when needed.

Keyfactor customers are often surprised to see how PKI moves from an obligation to an enabler. The Operations Dashboard is designed to aid with certificate management, reporting and alerting, as well as device command and control. Keyfactor allows organizations to state their CA's Certificate Policy and issue Certification Practice Statements. All of this contributes to:

- Lower staffing costs;
- Streamlined deployment;
- Proven operations model.

Let's consider some industry examples.

4. Industry Case Studies

Use Case 1 – DIY PKI: Financial Services Enterprise

A large financial company built custom applications for employee use. Each application server and endpoint needed a certificate to verify the authenticity of the endpoints as well, and encrypt the communication. Their needs:

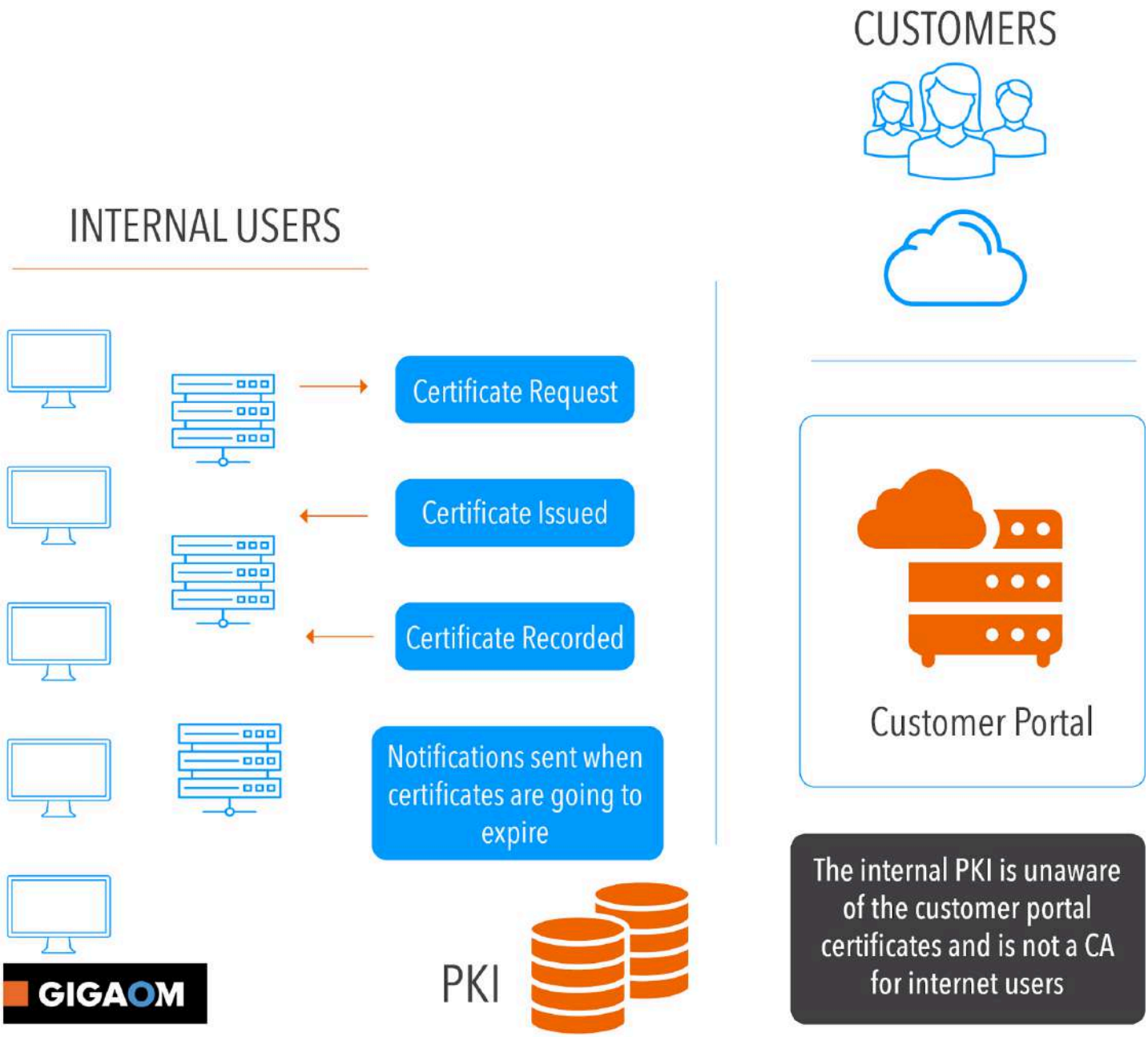
- Validate the authenticity of the server
- Validate the authenticity of the endpoint
- Create an encrypted channel for secure communications

As the company scaled, more applications were added and managing certificates became challenging. The company's R&D department went to work and wrote an application to manage its PKI. The application consisted of a root key, keys signed by the root key, as well as subordinate signing keys. The application also contained a small database that was used to keep track of which servers and endpoints had requested keys and the date that certificates would expire. It appeared to be a robust CA that solved the internal needs for managing certificates.

Shortly after its launch, the company made the news because of an outage. Their customer portal's SSL certificate had expired which caused users to be unable to connect. The engineers realized that the certificate running on their customer portal was not issued by their internal CA, and because their contract had expired with the public issuing CA, they were unable to quickly request a new one. Because their internal CA was only valid on internal machines, they lacked complete visibility which cost them time, money, and reputational damage.

In figure 1 below, the internal PKI is unaware of the customer portal certificates and is not a CA for external users.

Figure 1: Architecture Review



Total Cost of Ownership Review

The TCO for the second use case can be seen in table 2, below.

Table 2: Example cost review of the financial institution's implementation of their PKI

Physical Security

Leveraged Existing:	Net New:
• 24x7 security personnel • Video surveillance systems • Biometric data center access controls • Existing redundant data centers	• Locking alarmed cage to house Root CA • HSM x2 devices • Tamper evident bags and tags • Safe and safety deposit box to house offline Key materials

Internal Labor (Install & Management)

Tasks	Effort estimate in man days
Architecture and Design	12-18
CP/CPS Document Creation	12-18
Root CA Build	3-7
Issuing CA Builds	12-18
Template Design and Deployment	3-7
Building a CRL Hosting Location	1-3
Publishing CRLs	8-12
PKI Monitoring and Maintenance	13-17
System (OS/Application Stack) Monitoring and Maintenance	1-2
Manual Certificate Deployment to End Entity Devices	25-35
Yearly Disaster Recovery Test	3-7
Security Patching and Response	1-2

Infrastructure and Operations

Systems and Licenses	Number needed
Operating System Licenses	4-8
SQL Server License (For Key Management)	1-3
Backup Software License	4-8
System Management License (SCCM, HP OpenView etc.)	4-8
Anti-Virus/Security System Licenses	4-8
Hypervisor License	1-3
Disk/Storage Space	4-8
Physical Server Hardware	2-6
Security Logging/SIEM integration	4-8

Key Takeaways

The financial company was able to leverage existing data center and physical security

They lost four months of engineering resources building the PKI

They incurred significant costs for hardware, licensing and integration

Use Case 2 – Outsourced PKI: Hardware Manufacturer Mid-Market

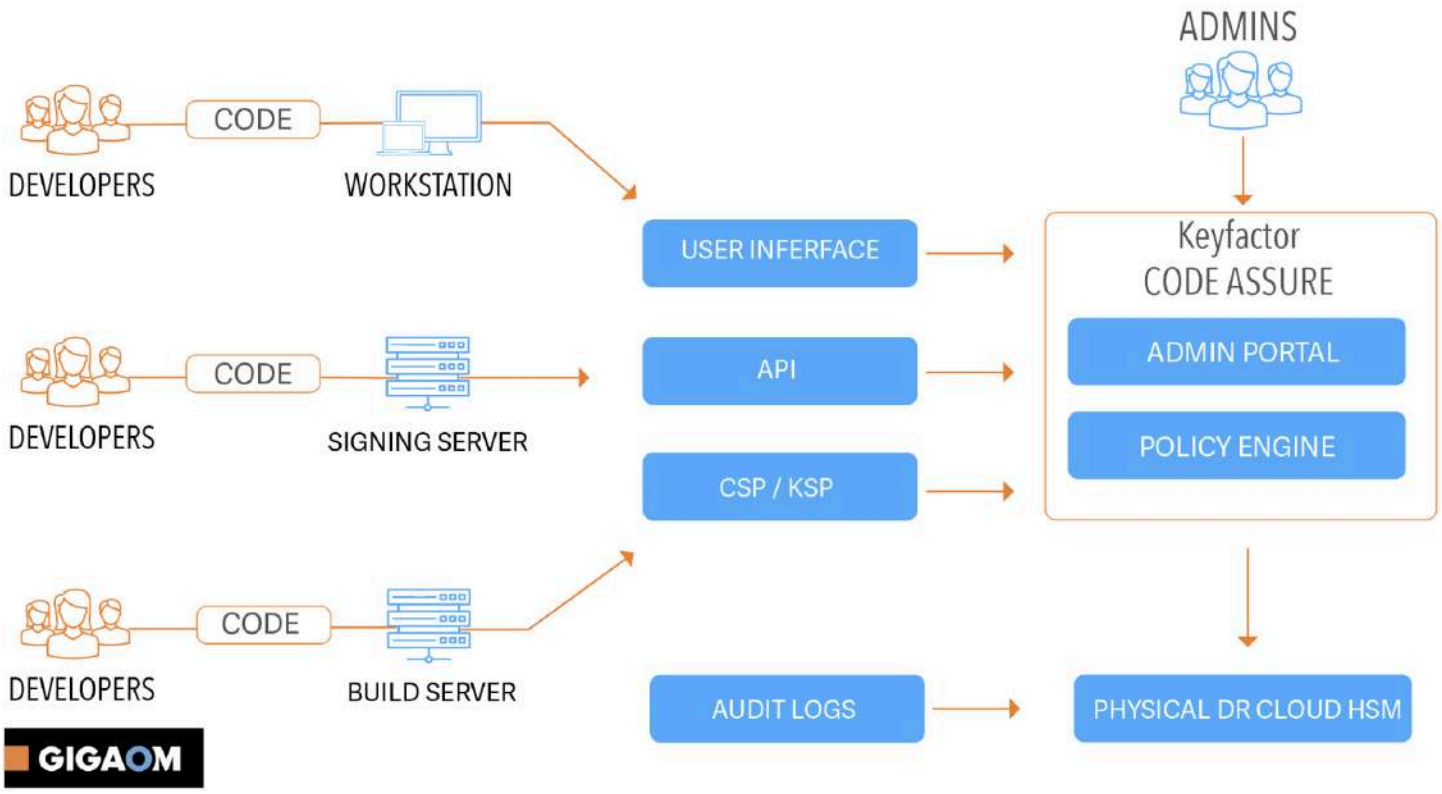
A hardware manufacturing company that sold network appliances and software that ran on them had two use cases for PKI:

1. Ensure the hardware they sold came from their manufacture so that they could track them for supportability.
2. Ensure that software updates they delivered to their clients could not be tampered with.
3. Enable SSL within their internal networks.
4. Better leverage Microsoft AD by enrolling users and computers with certificates.

The company's R&D team had expertise in networks, hardware, and embedded systems. They had been asked by a large customer to implement a method to ensure the software was secure.

When they looked at their product roadmap and commitments, they realized that they would have to hire new engineers or consultants to deploy the PKI if they were going to focus on their core business.

Figure 2: Example of Keyfactor's code signing



They looked at outsourcing the build of their PKI and found the costs of the consultants, the infrastructure to run it on, and the ongoing maintenance were within budget but the physical security costs could not be reconciled. They also realized that the loss of a private signing key would have been devastating to their reputation. See figure 2, above, as an example of Keyfactor's code signing.

They looked at Keyfactor's cloud-based PKI solution and found the following:

- It solved for all of their use cases,
- It could be rolled out securely within a fraction of the time of building one,
- It would be supported;
- And scale with them as they continued to grow.

Total Cost of Ownership Review

The TCO for the second use case can be seen in table 3, below.

Table 3: Example cost review of the hardware manufacturer's implementation of their PKI

Physical Security

Net New:
- Redundant data center x1
- Locking alarmed cage to house Root CA
- HSM x2 devices
- Tamper evident bags and tags
- Safe and safety deposit box to house offline Key materials Video surveillance systems
- Biometric data center access controls

Consulting Labor (Install & Management)

Tasks	Effort estimate in man days
Architecture and Design	5-8
CP/CPS Document Creation	5-8
Root CA Build	1-3
Issuing CA Builds	6-8
Template Design and Deployment	3-7
Building a CRL Hosting Location	1-3
Publishing CRLs	1-3
PKI Monitoring and Maintenance	13-17
System (OS/Application Stack) Monitoring and Maintenance	1-2
Manual Certificate Deployment to End Entity Devices	10-14
Yearly Disaster Recovery Test	3-7
Security Patching and Response	1-2

Infrastructure and Operations

Systems and Licenses	Number needed
Operating System Licenses	4-8
SQL Server License (For Key Management)	1-3
Backup Software License	4-8
System Management License (SCCM, HP OpenView etc.)	4-8
Anti-Virus/Security System Licenses	4-8
Hypervisor License	1-3
Disk/Storage Space	4-8
Physical Server Hardware	2-6
Security Logging/SIEM integration	4-8

Key Takeaways

The consultant hours were less than using internal engineering resource

They lacked the physical security required to manage their PKI and the costs of building it were prohibitive

Concerned around running and maintaining critical infrastructure after the consulting engagement

5. Investment in the Business: Cloud-based PKI

In many cases, the investment in cloud-based PKI is readily apparent. Take IoT: when a device or component is built and shipped, the company selling and supporting it should be able to validate it is as one of theirs and not a knock off. PKI enables this.

Companies that deliver software and code patches must be able to provide their customers assurance that code being installed is authentic and has not been tampered with. Companies that don't build devices or ship software are still reliant on SSL to secure communications, VPN's to manage access, and must be able to tell company-approved devices apart from unauthorized ones.

PKI is an investment in the business, its longevity, security, and confidence. Whether it is the ability to securely distribute software internally or to its customers, control licensing, manage the secure distribution of devices, or prevent outages, PKI is a way for enterprises to put a real stake in the ground around security. PKI provides authenticity and cryptographic proof that it cannot be tampered with or altered. It is what sets apart fact from fiction.

Gain the advantage of securely managing your PKI by using dedicated experts and infrastructure, without the overhead of lost opportunity or high costs, by moving it to the cloud with Keyfactor.

6. About Simon Gibson

Simon Gibson is a CISO and subject matter expert on security. He has been responsible for driving security capability into products, enterprises and supporting complex engagements.

Simon led the Information Security Group at Bloomberg and served as their CISO. He has managed attack teams, incident response teams and been responsible for the defensive security posture in the financial, government, manufacturing and PCI industries.

Simon is a renowned speaker and panel moderator. He has counseled fortune 100's on building their programs and worked with US Government public private information sharing initiative

7. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

8. Copyright