Comparing cost of ownership: DigiCert® Trust Lifecycle Manager vs. on-premise software

Who should read this paper

Deploying and managing a PKI solution can be a complex undertaking. This is particularly the case with on-premise PKI software implemented and maintained by the organization. This white paper explores the hidden costs of PKI when implemented in house. It also demonstates how the DigiCert Trust Lifecycle Manager is an extremely cost-effective alternative that reduces the complexity of implementation while enabling trusted authentication, verification, integrity, and encryption for critical enterprise applications.

digicert®

Table of contents

Introduction

Whether it's complying with mandates to protect sensitive data, enabling trust in a business ecosystem, or securing corporate digital assets against unauthorized access, enterprises turn to public key infrastructure (PKI)-based solutions for the highest levels of protection. Enterprises, government organizations, and digitally connected communities recognize PKI as the gold standard for highly secure and trusted authentication, digital signatures, and encryption.

While cryptography is the core mechanism within PKI, certificate issuance, management, and revocation need to be properly established for relying parties to effectively enjoy the benefits of PKI. As such, not all PKI deployments are the same. Some provide limited functions to support simple applications, like sending and receiving encrypted email within an organization, while others deliver complex methods of integrating physical and logical access to secure sites and networks that protect matters of national security.

Regardless of the application, deploying and managing a PKI solution can be a complex undertaking. Unlike other technology solutions, PKI has many moving parts that go far beyond the software involved — from training to policy development, from data center security to certificate management. All the components that make up a robust, secure PKI environment can add to the cost of implementing PKI. These sometimes hidden or forgotten costs can be far more substantial than the acquisition cost of the software.

Enterprises, government organizations, and digitally connected communities recognize PKI as the gold standard for highly secure and trusted authentication, digital signatures, and encryption.

This is particularly the case with on-premise PKI software, implemented and maintained by the organization in its data center. This white paper explores the hidden costs of PKI when implemented in house. It also demonstrates how the DigiCert® Trust Lifecycle Manager is an extremely cost-effective alternative that reduces the complexity of implementation while ensuring trust and simplifying the goal of achieving authentication, verification, integrity, and encryption for the most critical enterprise applications.

The complexity of on-premise PKI

Unlike other technology solutions, PKI requires far more than the authentication software and the support infrastructure. For organizations that desire to implement an on-premise PKI, dedicated, trained personnel are required to create, manage, and support the infrastructure. Highly secure facilities are critical, as well as robust policies and procedures, to ensure that the keys used for certificates are protected. Another consideration is the need for failover technology and a scalable infrastructure to ensure continuous operation, availability can be a major concern. Employees and partners who are unable to validate their identities due to PKI unavailability may be prevented from conducting business in a timely manner.

Security of the root certificate and the certificate issuance process is a critical issue enterprises must be prepared to handle when implementing an on-premise PKI. Appropriately high levels of security, background checks, procedures, and more must be in place or the root certificate could be compromised — at great risk to the enterprise. If the root certificate should ever become compromised, all certificates issued from the governing Certificate Authority (CA) are also compromised and their validity may be called into question, jeopardizing the entire PKI trust hierarchy.

Trust is the key building block of PKI. If the enterprise plans to use its PKI to securely communicate and transact business with third parties outside of the organization, it needs a trusted, third-party CA as the root certificate. Certificates issued by companies acting as their own CA are less likely to receive the full trust of parties outside of the organization, thereby requiring a separate, additional PKI infrastructure using a trusted CA for business-to-business communications.

Alternatively, two (or more) independent organizations could create a cross-certification trust infrastructure. In which case, one organization's root CA hierarchy issues a subordinate CA certificate to a CA in the other organization's CA hierarchy. Each of the participating members in the cross-certification trust network could then work in an interoperable fashion. However, the cost and effort to create the cross-certification can be prohibitively expensive and time consuming.

Uncovering the true cost of on-premise PKI

When considering a PKI implementation, organizations often focus on only the traditional solution costs such as software licensing, hardware, and installation services. But with PKI, there are a number of additional factors and costs that organizations must consider when weighing whether to implement PKI in house. In fact, software and hardware for the PKI solution are often a small component of the overall cost of ownership for an on-premise PKI solution.

To create a scalable, reliable, and secure on-premise PKI, companies need to carefully consider not only the acquisition costs, but the ongoing costs, including:

- Software acquisition and maintenance
- Hardware and networking infrastructure
- Secure facilities
- Creation and auditing of policies and procedures
- Management of the certificate lifecycle
- Highly available validation (Certificate Revocation List (CRL)/Online Certificate Status Protocol (OCSP)) infrastructure
- End-user support
- IT training
- Backup and disaster recovery
- Scalability to support user and application growth

What if the software is free?

Free PKI capabilities included in some server operating systems (OS) can appear to be a low-cost PKI solution. The reality is that the hidden labor and infrastructure costs still make this type of on-premise solution an expensive undertaking.

Additionally, with this do-it-yourself form of PKI, the onus is on the enterprise to create the PKI infrastructure, customize it to suit the needs of the organization, and maintain it. While organizations assume that this can be achieved with existing IT personnel at no additional cost, often in-house personnel lack the PKI expertise needed to effectively implement an on- premise solution. Furthermore, enterprises must be prepared to commit significant IT resources to ongoing PKI support requirements. Maintaining audit logs, creating a CRL and other tasks are not trivial matters, requiring trained, dedicated PKI personnel or costly external consultants. Without serious consideration to these matters, organizations could potentially undermine the strength of their "trust anchor" and likewise the value of PKI.

Comparing a managed PKI service to an on-premise solution

Alternatively, organizations can use a managed PKI service, which delivers PKI capabilities on demand. A managed service dramatically reduces the burden on the enterprise while ensuring scalability and availability. Policies, operational processes, and certificate management can be handled by the service provider.

A managed service can also scale more easily to the growing needs of the business. To scale an on-premise solution, organizations must often install separate instances of the software, requiring more hardware, backup, disaster recovery, and other infrastructure. The cost of deploying PKI using a managed PKI service is also drastically lower than implementing an on-premise solution. To illustrate this, let's compare DigiCert Trust Lifecycle Manager to an alternative on-premise PKI solution. We'll look at three major areas of cost that organizations incur when deploying and using a PKI solution: software, infrastructure, and personnel.

Assumptions

The following cost analysis is based on a three-year time- frame, with one-time costs occurring in the first year. All amounts are in U.S. dollars and are based on publicly available U.S. General Services Administration (GSA) Advantage pricing. Professional services costs are based on industry averages for comparable services. The number of seats/certificates used in the analysis is 1,000 — representing an average enterprise deployment.[1]

> The number of seats/certificates used in the analysis is 1,000 — representing an average enterprise deployment.[1]

Software

To deploy PKI into a production environment, for the Platform, there are no set-up fees, but there are annual service fees. Basic support is included in the service fee[2], and there are no license or maintenance fees. With the on-premise solution, the organization incurs the software license, maintenance, and support fees.

Included in the calculation are costs incurred to pilot a solution before rolling it out to the broader organization as well as disaster recovery costs. For DigiCert Trust Lifecycle Manager, disaster recovery is included as part of the standard Certification Practice Statement (CPS).

The table below shows that the on-premise software is significantly more expensive to acquire and deploy than the managed service.

1 - This sample comparison is made available to you to independently evaluate the benefits of implementing managed PKI and the associated direct costs of managed PKI deployment, including customer care and solution-related costs. This sample comparison is not intended to provide financial or investment advice, and should not be relied upon as such. The information presented is only to highlight issues for your consideration. All scenarios are hypothetical and are for illustrative purposes only. Deployment/investment decisions should not be based upon this sample comparison alone. There are no representations or warranties of any kind, either express or implied. Symantec cannot and does not guarantee results.

2 - Premium support is available for additional charges.

DigiCert Trust Lifecycle Manager	Total amount		On-premise PKI	Total amount	
	One-time	Recurring		One-time	Recurring
Pilot or Preproduction			**Pilot or Preproduction**		
Annual managed service fee	$0	$0	Registration Authority	$15,065	N/A
Annual per-seat fee	$0	$0	Digital ID	$1,188	N/A
Support	$0	$0	Support	$0	N/A
Subtotal	**$0**	**$0**	**Subtotal**	**$16,253**	**$0**
Production			**Production**		
Annual managed service fee	N/A	$17,000	Registration Authority	$30,130	N/A
Annual per-seat fee	N/A	$26,250	Digital ID	$95,000	N/A
Support	N/A	$0	Support	N/A	$25,026
Subtotal	**$0**	**$0**	**Subtotal**	**N/A**	**$25,026**
Disaster recovery			**Disaster recovery**		
Annual managed service fee	$0	$0	Registration Authority	$0	$0
Annual per-seat fee	$0	$0	Digital ID	$0	$0
Support	$0	$0	Support	$0	$0
Subtotal	**$0**	**$0**	**Subtotal**	**$0**	**$0**
Software grand total	**$0**	**$43,250**	**Software grand total**	**$141,383**	**$25,026**

Inafrastructure

All infrastructure costs are on the on-premise side. DigiCert Trust Lifecycle Manager does not require any additional on-premise infrastructure, saving not only the costs of acquiring and maintaining the infrastructure, but the IT effort required to install and manage it.

The following costs represent fairly conservative figures for the infrastructure and assume a highly secure facility is already in place. Organizations without a secure building, data center, or equipment access, will need to invest additional funds to bring the facility to a higher security level to protect the PKI system.

DigiCert Trust Lifecycle Manager	Total amount		On-premise PKI	Total amount	
	One-time	**Recurring**		**One-time**	**Recurring**
Hardware			**Hardware**		
Servers	N/A	N/A	Servers (Dell)	$8,800	$1,760
Load balancer	N/A	N/A	Load balancer (Foundry)	$19,500	$3,900
Cryptographic hardware	N/A	N/A	Cryptographic hardware (SafeNet)	$26,200	$3,930
Subtotal	**$0**	**$0**	**Subtotal**	**$54,500**	**$9,590**
Software			**Software**		
Operating system licenses	N/A	N/A	Operating system licenses (Microsoft®)	$4,116	$823
Authentication, automation, and backup licenses	N/A	N/A	Authentication, automation, and backup licenses (various)	$4,600	$920
Database server license	N/A	N/A	Database server license (LDAP)	$2,000	$400
Subtotal	**$0**	**$0**	**Subtotal**	**$10,716**	**$2,143**
Infrastructure grand total	**$0**	**$0**	**Infrastructure grand total**	**$65,216**	**$11,733**

Personnel

PKI is a complex technology that requires knowledgeable staff for on-premise solutions. IT personnel or consultants will need to implement the required software and hardware components, create and enforce policies and procedures, manage the certificate lifecycle, create a disaster recovery plan, and more.

The following cost comparison calculates the personnel costs for deploying and managing a PKI solution. For the Platform, organizations need only one, part-time administrator to manage use of the service, no training is required. Costs were calculated based on onefourth of a full-time employee's time, where the fully loaded cost for an employee was $80k per year. No deployment, integration, or consulting costs are needed for the managed service.

As shown in the chart below, there is a considerable difference in personnel costs for the on-premise solution, with substantial recurring costs as the ongoing IT burden remains high.

DigiCert Trust Lifecycle Manager	Total amount		On-premise PKI	Total amount	
	One-time	**Recurring**		**One-time**	**Recurring**
Professional Services			**Professional Services**		
Deployment (initial installation)	N/A	N/A	Deployment (initial installation)	$17,600	N/A
Internet security consulting (PKI policy)	N/A	N/A	Internet security consulting (PKI policy)	$35,200	N/A
System administrator (PKI administrator)	N/A	$20,000	System administrator (PKI administrator)	N/A	$52,000
Subtotal	**$0**	**$20,000**	**Subtotal**	**$52,800**	**$52,000**
Training			**Training**		
Administrator course	N/A	N/A	Administrator course	$5,000	N/A
PKI comprehensive course	N/A	N/A	Security manager comprehensive course	$7,500	N/A
Toolkit course	N/A	N/A	Security toolkit for Java™ developers course	$7,500	N/A
Subtotal	**$0**	**$0**	**Subtotal**	**$20,000**	**$0**
Personnel grand total	**$0**	**$20,000**	**Personnel grand total**	**$72,800**	**$52,000**

The bottom line

In terms of total acquisition and deployment costs across all three major areas above, the on-premise solution comes in at more than $368,000 compared to $63,000 for DigiCert Trust Lifecycle Manager. Recurring costs were over 40 percent higher than those for using the platform.

Sofware and personnel were the primary contributing factors for the vast cost differential between DigiCert Trust Lifecycle Manager and the on-premise solution. Over three years, total costs for the on-premise solution were more than $545,000, averaging out to about $182,000 per year. For the platform, the total cost for three years was $189,750, about the cost of one year of the on-premise solution.

DigiCert Trust Lifecycle Manager	Total amount		On-premise PKI	Total amount	
	One-time	**Recurring**		**One-time**	**Recurring**
Software grand total	$0	$43,250	Software grand total	$141,383	$25,026
Infrastructure grand total	$0	$0	Infrastructure grand total	$65,216	$11,733
Personnel grant total	$0	$20,000	Personnel grant total	$72,800	$52,000
Total costs	**$0**	**$63,250**	**Total costs**	**$279,299**	**$88,759**

The benefits of DigiCert Trust Lifecycle Manager

DigiCert Trust Lifecycle Manager is a hosted solution enabling complete management of digital certificates (issue, revoke, renew, escrow keys, view status, run reports) for authentication, encryption, and digital signing. Using the platform, organizations can establish a robust PKI and CA system without the cost and time-to-market burden of on- premise PKI deployment.

Leading organizations, government agencies, and digitally connected communities choose our Trust Lifecycle Manager because it delivers:

- **Lower total cost of ownership:** Organizations drastically reduce up-front capital investments and ongoing IT personnel costs for PKI.
- **Fast deployment:** DigiCert enables organizations to deploy PKI rapidly to employees, customers, business partners, web services applications and network devices.
- **Seamless integration:** DigiCert Trust Lifecycle Manager can integrate into many organizations' existing architecture without expensive custom programming.

- **Ease of use:** DigiCert Trust Lifecycle Manager simplifies deployment and enables enterprises to quickly and easily manage large numbers of certificates, while offering transparency to end users.
- **Scalability and reliability:** DigiCert's trusted and reliable infrastructure scales to millions of users and flexes to meet evolving business needs.
- **Market-leading:** DigiCert's time-tested policies and practices have been proven effective across many industries and sizes of organizations. DigiCert Trust Lifecycle Manager has helped thousands of organizations, including partners and companies such as Avaya® Inc., CertiPath® LLC, and the U.S. Department of Education to protect their online data, systems, and processes against intrusion and business disruption.
- **A trusted solution:** DigiCert operates the longest running commercial Trust Lifecycle Manager in the world and has issued more than 200 million certificates.

Conclusion

By eliminating or reducing the high costs of infrastructure and IT personnel resources, a managed PKI service enables enterprises to costeffectively comply with regulatory mandates, protect sensitive corporate data, and communicate in a trusted way with external parties.

For more than a decade, DigiCert has been the trusted provider of PKI services for all types of enterprises, government organizations, and trusted communities. DigiCert Trust Lifecycle Manager delivers the high level of protection organizations need without the complexity, burden and cost of an on-premise solution. With DigiCert, organizations no longer must decide between the high price of security versus the high cost of a breach – implementing PKI is a cost effective solution for all critical business transactions.

Glossary

Certificate Authority: A trusted party, authorized to issue, revoke, or suspend digital certificates as part of a public key infrastructure (PKI)

Certificate Revocation List (CRL): A periodically issued list, digitally signed by a CA, of identified certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked certificates' serial numbers, and the specific times and reasons for revocation.

Certification Practices Statement (CPS): A document containing a statement that specifies the practices a CA or Registration Authority (RA) employs in issuing certificates. This document is revised as necessary by the CA.

Credential: A form factor that represents the digital identity of an individual or entity. Trusted parties, such as CAs, issue a form factor based on the level of authentication required/performed on that individual or entity. Digital certificates are a type of form factor and may be combined with other form factors such as tokens or hardware security modules.

Digital Certificate: A X.509 file, based on a public/private key pair. This file binds the public key to identity of the individual or entity. A digital certificate isused for authentication, encryption, and digital signature purposes.

Digital Signature: A trusted and secure form of an electronic signature, which provides verified user identity, document integrity, time stamp, and nonrepudiation of signed electronic documents.

Key Generation: The trustworthy process for generating, documenting, and storing public keys and private keys.

Private Key: The mathematical key (kept secret by the holder) used to create digital signatures and decrypt messages or files encrypted with the corresponding public key.

For more information, contact a PKI expert
1.801.770.1736 or email pki_info@digicert.com.

digicert®