Interested in learning more about security?

SANS Institute InfoSec Reading Room

Building and Managing a PKI Solution for Small and Medium Size Business

This paper will analyze the Microsoft Windows, Mac OS X, open source, and third-party (cloud) PKI solutions and report on their ease of installation, use, management, and overall cost to operate for small to medium size business.

Building and managing a PKI solution for small and medium size business

GIAC (GSEC) Gold Certification

Author: Wylie Shanks, giac@infosecmatters.com
Advisor: Hamed Khiabani, Ph.D.

Accepted: December 16, 2013

Abstract

This paper will analyze the Microsoft Windows, Mac OS X, open source, and third-party (cloud) PKI solutions and report on their ease of installation, use, management, and overall cost to operate for small to medium size business.

1. Introduction

The use of Public Key Infrastructure (PKI) can be an effective way to meet business, regulatory, and compliance requirements. The ease of installation, use, maintenance and cost of a PKI solution can help companies determine the solution that best meets their requirements.

It is important to review the components of PKI before addressing requirements and solutions.

1.1. Encryption, algorithms, and keys

Encryption is used to protect the confidentiality of information. A mathematical algorithm (cipher) and a secret (key) are used to transform data in its original form called plaintext into ciphertext (encrypted text). Authorized individuals can decrypt the ciphertext back into plaintext using the appropriate algorithm and key. Typically, the algorithm is widely known. Therefore, the key must be protected against unauthorized use, destruction, and loss.

Symmetric key algorithms use the same key for encryption and decryption and can be implemented as a stream cipher or block cipher. Stream ciphers encrypt data one byte at a time. Conversely, block ciphers encrypt data in fixed lengths (Davies, 2011). This provides a means for bulk encryption of data at relatively fast speeds. Regardless of the cipher used the symmetric key must be securely transmitted to the intended recipient in order for the data to be decrypted. Asymmetric algorithms can support the secure distribution of symmetric keys.

Asymmetric key algorithms use mathematically related public and private key pairs. One key is used to perform a specific function such as encryption or to digitally sign a file. The other key provides a related function such as decryption or digital signature verification. For example, a public key can be used to encrypt data that only the private key holder can decrypt. Similarly, a private key may be used to digitally sign a document whereby the public key is used to verify the signature.

Wylie Shanks, giac@infosecmatters.com

The strength of the algorithm is in its ability to defend against cryptanalysis. The degree of protection it provides varies based on the algorithm's implementation and the length of its key.

1.2. Certificates

One means of transmitting a public key is through the use of certificates. A certificate is, "a signed data structure that binds a public key to a person, computer, or organization" (X. 509 Public Key Certificates, n.d.). A Certificate Authority (CA) digitally signs the certificate using its private key. This process binds the identity of the subject (as verified by the CA) to the public key. According to Komar, B (2008) certificates generally include the following information:

- The subject of the certificate (the person or device)
- The issuing Certificate Authority
- The public key of the key pair
- The algorithms used by the certificate
- Information used to determine the validity or revocation status of the certificate
- The list of included X.509 version 3 extensions in the issued certificate

Main certificate

Version
Serial Number
CA Signature Algorithm
Issuer Name
Validity Period
Subject Name
Subject Public Key
Issuer Unique ID
Subject Unique ID
Extensions (see next column)
Signature Value

Select list of extensions

KeyUsage (should be used)

Digital Signature	Public key is used to verify signature
Key Agreement	Sender and receiver use public key to derive the key without using encryption. Used in Diffie-Helman ciphers.
Key Encipherment	Public key can encrypt symmetric key for transport
Data Encipherment	Public key can be used to encrypt data
Key Cert Sign	Public key can be used to verify certificates signature

Subject Alternative Name (SAN)

Another name for the certificate's subject such as an email address, IP address, DNS or host name.

The issue of whether or not to trust a certificate can be mitigated through the use of a trusted certificate authority.

1.3. Digital Signatures

There are three components required for a digital signature – a message, a message digest and a private key. A hash function creates the message digest by processing data through a one-way mathematical function (Kuhn, D., 2001). Using the private key to encrypt the message digest results in the creation of the digital signature. The signing key can be verified by using the corresponding public key to decrypt the contents. To confirm the message has not changed the decrypted message digest is verified against the cryptographically hashed received message to ensure they are the same. The digital signature provides message integrity and non-repudiation (only the private key could have been used to sign the message digest).

1.4. Certificate Authority (CA)

A Certificate Authority is the entity that digitally signs certificates. A CA performs the following functions:

1. Validates the requestor's identity
2. Issues certificates
3. Maintains certificate status information regarding certificates
4. Issues Certificate Revocation List

The requestor's identity needs to be verified so that certificates are issued to authorized individuals. A Registration Authority (RA) provides this function. Among other tasks it is responsible for verifying the identity of requestors and approving or rejecting the certificate request (includes issuance, revocation, and renewals). As certificates are issued for specific systems in a domain an approval request email may be sent to the registered owner of that domain. Once approved, additional levels of verification may be involved such as the use of an automated telephone call to the requestor with PIN entry required to confirm their identity. In order to trust a certificate

one must trust the issuing CA. Thus, the one relying on the certificate or digital signature verification is called the relying party (Barker, E., 2009).

1.5. Trust models

Certificate Authorities generally follow a hierarchical model. The CAs in the hierarchy comprises a chain that leads up to the root CA or trusted anchor.

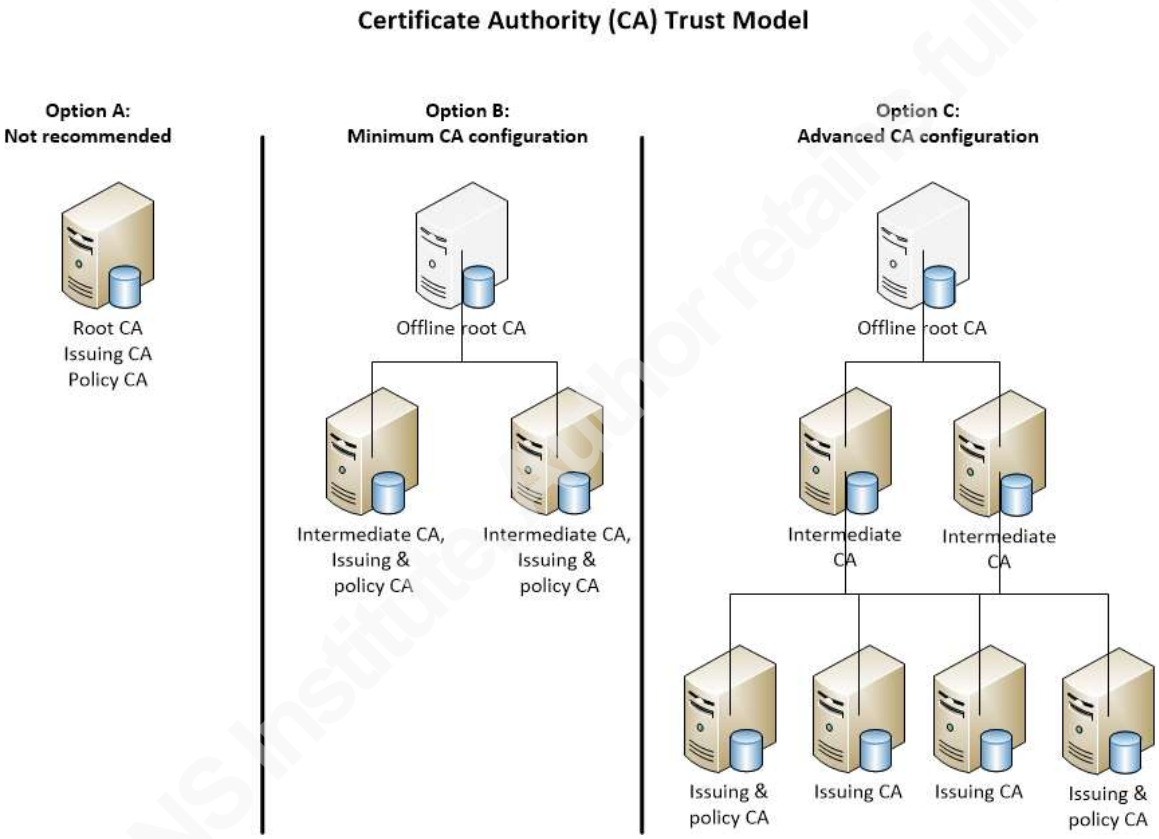

Figure 1.1 – Certificate Authority (CA) Trust Model

Root CA

The root CA's private key signs certificates it issues. Certificates signed by the root CA may include intermediate CAs, issuing CAs, and policy CAs. Root CAs do not issue certifications for users or devices. The root CA is typically kept offline (is disconnected and physically secured) as a compromise of the root CA would compromise the trust in all certificates issued by the CA. As a protective measure and to provide greater assurance the root CA generates certificates for intermediate CAs before being powered down and physically secured. In order to trust a certificate issued by the CA it is

imperative that the root CA's private key remain private and issue only authorized certificates. The certificates issued by a compromised CA should be considered untrustworthy and, thus, be replaced or re-issued.

Intermediate CA

An intermediate CA is subordinate to a higher-level CA (such as the root CA) and is designed to issue certificates to other CAs.

Issuing CA

The issuing CA issues certificates to users and devices. This CA may perform the function of a policy CA if one is not present above it in the CA hierarchy.

Policy CA

The policy CA specifies the necessary configuration settings or controls and policies to be followed such as certifying a user. Generally, certificate policies are used to create certificates that meet the designated algorithm and key length. Multiple Policy CAs can be created in order to satisfy company requirements. For example, a high-assurance policy CA could be used to satisfy digital signature requirements whereas another implementation could support secured email.

Certificate Revocation List (CRL)

It may be necessary to revoke a certificate before it has expired. This may be due to the private key having been lost, stolen, or compromised. When a certificate is revoked its serial number and the reason for revocation is included in the Certificate Revocation List.

Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol (OCSP) provides the timely status of identified certificates. The response includes a certificate status of good, revoked, or unknown. The status of good indicates that the CA has not revoked the certificate. A revoked status is due to the temporary or permanent revocation of a certificate or may be caused due to the CA having no record of issuing the certificate in the request. An unknown status is typically due to the certificate being issued by another CA (Santesson, S., 2013).

Simple Certificate Enrollment Protocol (SCEP)

Larger organizations should considering using SCEP to automate deployment of network device certificates. Most small to medium size organizations may prefer to manage and deploy certificates manually given the relatively small number of devices in scope.

Which trust model option should be used?

Several certificate authority trust model options are identified below. Choosing the best option will depend on company and project requirements.

Each server should be hardened to company server build standards. These standards should be derived from industry standard guidelines such as those published by The Center for Internet Security (http://www.cisecurity.org). In addition, software and hardware firewalls should be used to limit traffic to that which is required. Anti-malware software should be installed and functioning and application control/blocking software should be considered to limit running processes to only those authorized.

Each trust model is evaluated based on its security posture. This includes the confidentiality and availability of the solution. Only larger customers and those requiring automation in their PKI solution should consider using OCSP and SCEP.

Option A – Single root CA

The single root CA option is not recommended for several reasons. First, this solution does not provide redundancy. If the server hardware or software fails the client will experience downtime until the solution can be returned to service. This may result in a lengthy delay. Second, if the root CA is compromised then all certificates issued by the CA should be revoked. As the root CA is always online it can be scanned for vulnerabilities, unauthorized access attempted, and may be more easily exploited given the target's availability.

Option B – Minimum CA configuration

At a minimum, the root CA should be taken offline after the intermediate CAs certificate has been signed by the root CA's private key. This action protects the root CA from compromise via the network. Additional steps to protect the root CA include encrypting the full hard disk and storing the hard disk in a physically secure, locked, area

with controlled (limited) access. Only a small number of authorized individuals should have access to the hard drive.

This model provides greater confidentiality and availability than option A as the root CA is offline and the issuing and policies CAs are redundant. Thus, the servers can be patched and maintained while avoiding an overall system outage.

Option C – Advanced CA configuration

A more advanced CA configuration may be necessary for customers that require greater scalability, flexibility and availability. In this model, the root CA should be taken offline and physically secured as outlined in option B. This model, however, provides greater flexibility in how the solution is deployed. As separate servers, the intermediate CAs can be updated or replaced as required as changes in encryption algorithm and key length occur. In addition, the issuing and policy CAs can be strategically deployed based on company requirements. It is no longer necessary to rely on the issuing and policy CAs to support company-wide requirements. This option is best suited to larger organizations where management or administration of systems is distributed.

1.6. What is Public Key Infrastructure (PKI)?

Public Key Infrastructure provides key management capabilities for public key distribution. The PKI infrastructure is used to validate the requestor's identity and provide the assurance required in order to trust the security services provided by the certificates (Barker, E., 2009). This includes the root CA, intermediate or subordinate CAs, the registration authority, and certification revocation list (CRL) as required.

2. Use cases

It is important to know the type of certificates that will be required and how they are to be used before implementing the CA and Policy CA. The policy CA supports the use of multiple policies and the creation of different type of certificates. Only the required policies should be enabled on the server as a good overall security practice and to ensure that only required certificates are generated and maintained. The charts below provide the extended key information and the associated key usage extensions in order to

provide the required certificates (Key usage extensions and extended key usage, August 2008).

Extended key	Enable for these key usage extensions
TLS Web server authentication	Digital signature, key encipherment or key agreement
TLS Web client authentication	Digital signature and/or key agreement
Sign (downloadable) executable code	Digital signature
Email protection	Digital signature, non-repudiation, and/or key encipherment or key agreement
IPSEC End System (host or router)	Digital signature and/or key encipherment or key agreement
IPSEC Tunnel	Digital signature and/or key encipherment or key agreement
IPSEC User	Digital signature and/or key encipherment or key agreement
Timestamping	Digital signature, non-repudiation.

Examples of required key usage extensions

Application	Required key usage extensions
SSL Client	Digital signature
SSL Server	Key encipherment
S/MIME Signing	Digital signature
S/MIME Encryption	Key encipherment
Certificate Signing	Certificate signing
Object Signing	Digital signature

2.1. Considerations

Every successful project starts with collecting all project requirements. This is especially true of complex PKI solutions.

2.2. Requirements

The project starts with a business case, compliance (PCI DSS), or regulatory (HIPAA) mandate that must be achieved. Management support for the project is critical. They approve expenditures or otherwise provide the resources necessary to implement the project. Without their support the project will not be successful.

Understanding the confidentiality, integrity, availability and recovery needs of the business is essential when developing the CA's architecture and policies. In addition, the inventory of current vendor products and their certificate or PKI requirements aids in the refinement of the issuing or policy CA architecture. The type of certificates required, and how and when they will be used are compiled into the functional requirements list. The use of encryption, however, may reduce the visibility into data streams that data loss

prevention and intrusion detection / prevention systems rely on. Once collected, the requirements must be clearly communicated with vendors and implementers so that the desired outcome can be achieved or plans modified in order to meet stated objectives.

The project may have additional functionality, security, and performance requirements. These may be facilitated through the use of people, processes, or specific vendor products such as VPNs, smart cards, or hardware security modules (HSMs). To determine the appropriate algorithm and key lengths to be used and the validity period of these features consult National Institute of Standards and Technology (NIST) Special Publication 800-57 (Barker, E., 2009).

Taking a risk-based, phased, approach will reduce the overall implementation and operational risk associated with the solution.

2.3. Legal considerations

Where possible, legal counsel should be involved in the project to ensure that applicable laws are being followed. Some of the legal issues to consider when using PKI are:

- The legality of using a particular algorithm or key length
- The storage of data in another country (e.g. hosted or cloud solutions)
- Liability (e.g. if data is compromised)
- Indemnification (e.g. use of a system or software could result in future litigation)

2.4. Sustainment / On-going operations

The project team must consider the proper design and implementation of the PKI solution in order that the project requirements are met. This includes sustainment activities.

A properly designed PKI solution ensures that trust in the system is assured and the system functions as expected. Ensuring the private or symmetric keys remain confidential is one of the foundational security imperatives of PKI. When keys are generated, stored, and distributed they must remain secure. Fortunately, standards such as FIPS 140-2 can be used to determine whether a vendor's implementation meets security requirements (Federal Information Processing Standards Publication 140-2 – Security

Requirements for Cryptographic Modules, May 25, 2001). However, one should not rely solely on such standards as a guarantee of security posture. Where available, the vendor's instructions should be followed to assist with a secure implementation and then the system should be tested to ensure it is performing as expected.

Technology is only one component of the system. The people and processes that support the solution are extremely important. The technical knowledge and experience required to operate and maintain the system should not be underestimated. The roles and responsibility of each member of the PKI team should be documented and enforced to ensure members are accountable for their actions and proper segregation of duties is maintained. Training in these functions is an important part of the security of the solution. Failing to follow these processes could result in poor security posture, data compromise or total loss of data.

2.5. Recommendations

PKI implementations can be a major undertaking that require specialized knowledge and skill in order to be effective. The following recommendations should be considered when designing the PKI solution:

- Determine how much of the solution can and should be automated
- Reduce direct user involvement in the solution to the smallest amount possible. The solution should be as seamless as possible to the user
- Take a phased, risk-based, approach to the implementation
- Manage endpoints
- Track the deployment of certificates (e.g. where the certificates are deployed). Use caution when conducting network scans. They may be helpful when trying to find deployed certificates but they could affect network operations
- Keep technical skills and knowledge of encryption current
- Important sustainment activities include:
    - Ensuring the PKI is still functioning correctly
    - Maintaining encryption technology (e.g. algorithms and key lengths may have to change in the future resulting in deployment of new CAs)
    - Considering support of or integration with PKI solutions when choosing new applications and solutions
    - Training users on their role and the use of PKI

3. Certificate Authorities

3.1. Microsoft Windows Certificate Authority

Microsoft has offered Certificate Services system since Windows Server 2000. As a mature application, it supports manual and automated certificate enrollment (SCEP) and status (OCSP) functions. Some of these features are new to the standard version of the product - Windows Server Standard 2012. In previous releases, this functionality was only available in the higher priced data center or enterprise versions. The new version affords small and mid-size business the same opportunity to use certificate services that were once only available to larger enterprises.

3.1.1. Designing a CA hierarchy

The requirements of the business dictate the PKI solution. The size of the deployment, the security requirements, and degree of risk acceptable to the business are just a few of the considerations. As a best practice, the root CA is taken offline and stored securely once it has issued signed certificates for intermediate and/or subordinate CAs. Thus, while it is possible to implement a single tier solution a two-tier solution is a minimum best practice security requirement. With the root CA offline it is less likely for it to be compromised, issue unauthorized certificates or otherwise reduce the overall trust in the PKI solution. If additional security of the CA is required then a hardware security model (HSM) may be used with the CA to securely store its private key.

3.1.2. Preparing Active Directory

Active Directory is a pre-requisite for Microsoft Certificate Services. A proper segregation of duties ensures that only authorized individuals perform their function using least privilege permissions. Once access is correctly provisioned it should not be possible for one individual to have control over the full transaction. Otherwise, it may be possible to abuse the permissions granted. For example, only authorized individuals should have the ability to enable or disable the audit or logging function. The ability to change the audit function should not be simultaneously granted to those who review the audit logs. This would be especially important if the user can export private keys. If this

were to happen, an individual could disable the logging function, export private keys of other users, and fail to review the logs. That ability could allow for impersonation of another user – behavior that would go undetected. Ensuring that permissions are granted appropriately is extremely important to the overall security of the system.

3.1.3. Securing the CA

Maintaining the confidentiality and integrity of the PKI system provides the basis of trust in the whole system. As such, the CA must be protected against unauthorized use or other compromise. For most small and mid-sized business the necessity to secure the CAs in a limited access data center, in a locked cabinet with biometric access controls, and isolated network with key backup and recovery features is beyond their security requirements. The controls must be adequate and appropriate for the risk. Therefore, a risk assessment should be conducted against the PKI solution in order to anticipate the threats and risks to the system, determine any control or process gaps, and to provide steps to mitigate the assessed risks to an acceptable level. A variety of physical and logic controls may be implemented such as access control lists (e.g. hardware and software firewalls), role based permissions to enforce segregation of duties, and physical and logical security controls such as locked cabinets and doors. Full disk encryption may also be used to provide protection against offline attacks against the contents of the hard disk storage media. Care must be taken when full disk encryption is used to ensure that the CA maintains its operability and can be restored in the event of a disaster. Where the encryption key or passphrase is known it should be stored in a secured, access controlled, area to prevent inadvertent loss, destruction, or unauthorized use.

3.1.4. Certificate Validation / revocation

Windows Server Standard 2012 provides certificate revocation list (CRL), delta CRL, and online responder functionality to determine the status of a particular certificate. It is very important to make this information available in timely manner to avoid system misuse, as only valid certificates should be used. This forms part of the trust in the PKI solution.

3.2. Mac OS X Certificate Authority

Mac OS X 10.9 (Mavericks) is available as a free upgrade for those who have a Mac OS X 10.5 or higher license. Alternatively, this software comes with the purchase of a Mac. The Mac mini retails for $599 and the server version retails for $999.

The keychain access application contains basic certificate authority software. It is possible to conduct certificate signing requests and to manually create certificates though auto-enrollment (SCEP) and other advanced functions are not available. Given these limitations the Mac OS X Certificate Authority may be more appropriate for those organizations that have standardized on the Mac platform or require a basic CA environment.

3.2.1. Designing a CA hierarchy

The Mac OS X certificate authority (via keychain access) supports the creation of intermediate CAs. However, it appears to lack the scalability, availability and recovery functionality found in more mature certificate authority software. Thus, many of the available processes and procedures are conducted manually. Therefore, it may be possible to circumvent appropriate segregation of duties. The certificate authority does support the use of CRLs and OCSP servers but does not appear to provide one of its own to validate certificates it issued.

3.2.2. Preparing the Directory

Where necessary, Open Directory is available with the purchase of Mac OS X Server for a nominal fee. Once Open Directory has been configured it is possible to store issued certificates within the directory. Keychain access can be configured to "Search Directory Services For Certificates". User certificates used for signing and encryption and published to Open Directory (or Microsoft Active Directory) can be searched using this function. Review software license agreement (available here: http://www.apple.com/legal/sla/docs/OSX109.pdf) to determine whether you are permitted to operate up to two Mac OS X servers running on virtualization software on Mac computers owned by you.

3.2.3. Securing the CA

A risk assessment should be conducted against the system and appropriate physical and logical controls applied in order to mitigate risk to an acceptable level. Mac OS X comes with a software firewall that can be used to limit access to the system. In addition, FileVault 2 is available within recent versions of Mac OS X from the Security & Privacy pane of System Preferences. It can be used to encrypt the entire hard drive. Only authorized accounts will be allowed to logon once the system has been encrypted. These accounts can be chosen during the setup process. A recovery key will appear on the screen after the account selection has been made. This information can be used if an authorized logon account password has been forgotten. The recovery key should be stored securely. Please see Apple's knowledgebase for more information: http://support.apple.com/kb/ht4790.

3.2.4. Certificate Validation / revocation

The certificate authority does support the use of CRLs and OCSP servers but does not appear to provide one of its own to validate certificates it issued.

3.3. Open source Certificate Authority

Open source software is generally perceived to be low or no cost to acquire and use. However, the technical skill required to operate the software may be high and there may be little legal protection against litigation (indemnification) if the software infringes another's patent or copyrighted work.

A popular open source certificate authority is EJBCA. There is a community edition available for download that provides many basic and advanced features required of a CA. A commercial version is also available if additional features or support is required. The application is written in Java and thus can be run on a variety of operating systems and is available as a Live CD (pre-installed on a Linux distribution). This may reduce some of the technical knowledge required to install and operate the software. However, a support contract should be considered if technical skills within the organization are low or somewhat limited. The software's multi-tier architecture (e.g. web server, database, and application software tiers) and resulting complexity may

require more timely support of production issues as they arise than can be supported by the community at large.

3.3.1. Designing a CA hierarchy

The EJBCA CA supports a multi-tiered CA architecture. As with the other CAs, consideration should be given to meeting the company's scalability, availability, and recovery requirements and budget considerations.

3.3.2. Preparing the Directory

LDAP and Active Directory integration are available for use within EJBCA. These directories can be used to store issued certificates.

3.3.3. Securing the CA

A risk assessment should be conducted to ensure the appropriate controls are in place and risk is mitigated to an acceptable level. A variety of physical and logical controls may be implemented to secure the CA. A software firewall, at a minimum, should be installed on the CA to allow only authorized traffic.

3.3.4. Certificate Validation / revocation

EJBCA provides both certificate revocation list (CRL) and online certificate status protocol (OCSP) responder functionality. These functions provide a means of ensuring that a specified certificate has not expired or been revoked.

3.4. Cloud PKI

Symantec offers a managed PKI solution. However, this solution may not be cost effective for small to mid-size business. Cloud solutions have additional complexities that are not present in commercial software applications. Contractual considerations are key to these agreements. Therefore, an understanding of contractual language regarding system availability, service level agreements, secure backup and restore operations, indemnification, breach notification and payment of penalties are just some of the considerations. Another consideration is who is liable if the Enterprise PKI is compromised which results in a compromise of the client's systems. Indemnification is always a consideration. However, it may not be the customer that is saved from harm via

the contract. The contract must be reviewed and the risk of acceptance evaluated before proceeding.

The benefit of a cloud solution, in part, is that the infrastructure is built, managed, maintained, and supported by the third-party. The solution may offer greater redundancy, security posture, and scale compared to in-house solutions. For small and medium enterprises the cost to achieve a similar level of service and quality is prohibitive. Additional process efficiencies, workflows, and reduced staff involvement make cloud solutions an appealing choice (Ballad, B., 2011).

A risk assessment should be conducted prior to proceeding with a cloud service. The European Network and Information Security Agency offers free cloud computing risk assessment guidance via this address: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

3.4.1. Designing a CA hierarchy

As a cloud solution, the infrastructure is built and can be leveraged immediately. The CA infrastructure, policies, availability, and redundancy have already been addressed and require little customer involvement to implement. However, consideration should be given to whether or not a client requires a backup of their issued certificates. As a large company, it is unlikely that it would become insolvent or their service would be off-line for any extended period of time. Unless certificates are locally escrowed it will be difficult to obtain them under these circumstances. However, protecting backup copies of locally escrowed certificates is critical. Careful consideration should be given to certificate backups as this could give rise to a potentially valid claim against non-repudiation.

3.4.2. Preparing the Directory

This service is offered as an annual contract and requires a per-user or per-device fee (Symantec Managed PKI Service – Licensing, n.d.). Once the necessary information is provided to the service then certificates can be issued.

3.4.3. Securing the CA

Symantec has taken steps to secure their managed PKI service. Assessments such as SAS-70, Web Trust and others have been conducted to validate the security posture of their service offering. (Symantec Managed PKI Service, n.d.)

3.4.4. Certificate Validation / revocation

Symantec offers certificate validation and revocation services as would be expected from a full service managed PKI solution (Symantec Managed PKI Service 8.9 is now Live!, July 22, 2013).

4. Comparison of commercial, open source and cloud-based PKI solutions

Deciding how to meet business, regulatory, or compliance mandates demands a careful review of requirements, costs, and procedures among other considerations. While it may be possible to transfer responsibility for the operation, maintenance, and security posture of a solution a third-party the accountability of a breach typically resides with the data owner. Thus, all contracts should be carefully reviewed and risk assessments conducted in order to fully understand the risks involved before undertaking any solution.

Several PKI solutions were evaluated for their ease of installation, use, maintenance, and cost. The analysis appears below and uses a rating system of low, medium, or high as applicable.

Type of System	Cost to acquire / use	Technical skill required	Scalability	Technical Support Availability	Advanced features
Windows Server Standard 2012	Medium	Medium	High	Medium	High
Mac OS X (Keychain Access)	Low	Low	Low	Medium	Low
EJBCA	Low	Medium	High	High	High
Symantec Managed PKI Service	High	Low	High	High	High

Table 1.1 – Ease of installation, use, maintenance and cost of PKI solutions evaluated

4.1. Microsoft Windows Server Standard 2012

Microsoft Windows Server Standard 2012 is easy to install, use, and maintain with sufficient technical skills. The solution can be tested for up to 180 days using Microsoft's trial download located here: http://technet.microsoft.com/en-us/evalcenter/hh670538.aspx.

The solution can be cost effective depending on business needs and the number of certificates required. The software is licensed on a per-server basis and requires the purchase of client access licenses (CALs) for the number of client systems connected to the server. However, these costs can quickly become significant if additional hardware and storage media needs to be purchased to support the solution.

Larger customers would benefit most from this solution if they require a large number of certificates to be generated and deployed across their infrastructure and if process automation is required.

4.2. Mac OS X (Keychain Access)

Keychain Access is an application that comes with recent versions of Mac OS X. It is very easy to use. Simple certificate operations can be performed such as certificate signing requests, issuing certificates, and the creation of a CA.

Existing Mac customers with simple PKI solution requirements would benefit the most from this solution.

4.3. EJBCA

EJBCA is a very robust open source PKI solution. It is available on a Live CD that requires no installation and is relatively easy to use. As the application is written in Java it can be installed on a variety of operating system platforms. Additional software must be installed and configured to complete the installation. For some customers, this will add complexity to their environment and may make it difficult to support the solution. A commercial version of the software is available that comes with vendor technical support.

Companies that have the business need for a robust, cost-effective, PKI solution and sufficient technical resources to support it would benefit the most from this solution.

4.4. Symantec Managed PKI Service

Companies that have the business need and funding for a robust, secure, third party managed PKI solution would benefit the most from this solution. The Symantec Managed PKI Service requires no installation, is easy to use and is maintained by Symantec. Customers must purchase an annual license in addition to a per-user or per-device license. This solution can become costly compared to an in-house PKI deployment depending on the requirements.

This solution has been reviewed under SAS-70 and Web Trust and appears to offer a high level of security. However, all customers should conduct their own risk assessment and contract review to determine if the solution meets their security and risk tolerance.

5. Conclusion

Several PKI solutions were reviewed for their ease of installation, use, maintenance and cost. A single solution that will satisfy every company's requirements does not exist. It is important to conduct a risk assessment and contract review in order to ascertain whether business, compliance, and regulatory requirements can be achieved at an acceptable level of risk.

Wylie Shanks, giac@infosecmatters.com

References

Ballad, B., Ballad, T., Banks, E. (2011). *Access Control, Authentication, and Public Key Infrastructure*. Mississauga, Ontario: Jones & Bartlett Learning Canada.

Barker, E., Burr, W., Jones, A., Polk, T., Rose, S., Smid, M., & Dang, Q. (December 2009). *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance* (NIST Special Publication 800-57, 2013 Edition). Retrieved November 3, 2013, from National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

Davies, Joshua. (2011). *Implementing SSL/TLS Using Cryptography and PKI*. Indianapolis, Indiana: Wiley Publishing Inc.

Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Modules (May 25, 2001). Retrieved November 16, 2013, from National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Key usage extensions and extended key usage. (August 2008). Retrieved November 3, 2013 from http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp?topic=/com.ibm.help.domino.admin.doc/DOC/H_KEY_USAGE_EXTENSIONS_FOR_INTERNET_CERTIFICATES_1521_OVER.html

Komar, B. (2008). *Windows Server 2008 PKI and Certificate Security*. Redmond, Washington: Microsoft Press.

Kuhn, D., Hu, V., Polk, W., Chang, S. (February 2001). *Introduction to Public Key Technology and the Federal PKI Infrastructure* (NIST Special Publication 800-32). Retrieved November 16, 2013, from National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

X. 509 Public Key Certificates. (n.d.). Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/bb540819(v=vs.85).aspx

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C. (2013). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. IETF. RFC 6960. Retrieved November 18, 2013.

Symantec Managed PKI Service. (n.d.). Retrieved November 16, 2013 from http://www.symantec.com/en/ca/verisign/managed-pki-service

Wylie Shanks, giac@infosecmatters.com

Symantec Managed PKI Service 8.9 is now Live! (July 22, 2013). Retrieved November 16, 2013 from http://www.symantec.com/connect/blogs/symantec-managed-pki-service-89-now-live

Symantec Managed PKI Service – Licensing. (n.d.). Retrieved November 16, 2013 from http://www.symantec.com/en/ca/verisign/managed-pki-service/renewals-upgrades-licensing

Last Updated: June 20th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced