WHITEPAPER

Public Key Infrastructure

Best practices and why it's important to "get it right"

DIFENDA

Public Key Infrastructure (PKI) has become an integral component within business services and IT infrastructure. PKI provides trusted items that establish confidentiality, authentication, and authorization security services, and it can significantly reduce the cost of provisioning these services across the organization.

However, the technical complexity of cryptographic features and the need to integrate PKI services with enterprise technology is often challenging and sometimes fraught with administrative issues. This paper looks at PKI requirements, challenges, and opportunities where an investment of some extra time and detailed planning work can harvest additional dividends when implementing PKI.

It is not just a technical IT issue to build PKI—significant input is needed from other parts of the organization, so it is best to have all the right people involved from the beginning (including Security, Legal, Audit, Risk, Compliance, HR, etc.). There are also significant benefits to properly implementing Public Key Infrastructure best practices: tangible cost savings, less administrative overhead, centralized management of multiple disparate security functions, automation of critical security processes, and a much higher level of trust in your overall security posture.

Let's review some key considerations and success factors that we believe are an essential part of the foundation needed to help PKI flourish in your organization.

These include:

1) Enterprise Use Cases
2) Documenting PKI Requirements
3) Traceability Matrix
4) Establishing Trust in the PKI Solution
5) A Formal Certificate Authority Build Process
6) A Certificate Authority Key Signing Ceremony
7) Certificate Policy (CP) and Certificate Practice Statement (CPS) Documents
8) Key and Certificate Life Cycle Management
9) Use of a Hardware Security Module (HSM)

The easiest way to justify and market the value of PKI across the organization is to first find the most valuable Use Cases.

Enterprise Use Cases

Often, there is a central driver that gets PKI started or a champion who needs PKI functionality for some key operation within the organization. Normally, this starts with the team within IT that understands complex technology. However, while IT process automation, data asset management, and security are important to IT, getting all the needed resources to build a robust PKI solution may not fly if it doesn't resonate with other organizational stakeholders. What do you do to show the full value in PKI?

The easiest way to justify and market the value of PKI across the organization is to first find the most valuable Use Cases. Many vendors of PKI products and services can provide whitepapers with detailed Use Cases and the associated cost savings for using PKI services.

Some of the usual Use Cases are:

a) The use of digital certificates for securing Microsoft Active Directory (AD) services and automating the provision of organization-wide authorization and authentication services.

b) Providing trust and confidentiality services for web- based applications (TLS network encryption).

c) Digital certificates for signing and encrypting email messages to securely identify message sender, ensure message confidentiality, and provide non-repudiation services.

d) Solutions for ensuring regulatory compliance where PCI or other sensitive PII data protection requirements must be met in business functions, through the encryption or tokenization of sensitive data in files, databases, and B2B transaction processes.

Once you have identified the various Use Cases and tangible benefits to the organization coming from the use of PKI functionality, getting the resources to provide this IT service is a lot easier. If management knows that PKI is not a "one-trick pony" but in fact is suitable for deployment as a security and compliance solution in many circumstances, then PKI can become one of the central pillars supporting organization-wide services.

Documenting PKI Requirements

Documenting the requirements for a PKI should include both functional and non-functional requirements. This should include the functional elements—the what a system must do—as well as the non-functional elements—all the details on how you want the system to do it. Non-functional requirements—describing how a system will work—normally form the majority of the requirements documentation. During requirements definition, you may find that several Issuing Certificate Authorities are required for the full PKI solution, depending on your organization's structure, lines of business, kinds of certificates to be issued, their value, and any liability attached to the use of the certificates. (These detailed requirements will link back to an individual Use Case.)

Security and Compliance are both defined as being constraints on the behavior of the system, so they are non-functional requirements. Also, it is beneficial to review the NIST 800-57, NIST 800-131A special publication, and the FIPS 140-2 standards to see if any of the controls apply to your situation and the level of security required for your organization's PKI solution.

PKI architecture is normally a simple two-tier tree structure, with a Root Certificate Authority (CA) at the top and one or more linked underneath to sign and distribute the certificates used on a daily basis. However, it is important to determine whether there is a requirement to provide for a deeper third level CA functionality before setting up the Root CA, as you want to ensure that only the minimum number of levels are allowed (normally set to two).

Traceability Matrix

Use Cases lead to solution requirements and then to actual delivered functionality in the solution. But if there is a requirement for a functional component, how do you ensure you can say at the end of the project that what you said you would deliver has in fact been delivered?

The way to keep track of all the pieces is by using a Traceability Matrix. It is a simple table that allows you to track the many different items that must be documented, built, and delivered. More importantly, it allows you to ensure that all the items you intend to deliver can be traced back to the original solution requirements and Use Cases.

Establishing Trust in the PKI Solution

Your initial build of the PKI must establish an auditable and trustworthy environment. If you can't trust the PKI solution you have implemented, then nothing that follows from it or depends on these security services can in turn be trusted. But if the solution is created in a secure manner by people who can show they followed a trusted process to build each component of the solution, then we can say that trust has been formally established over the newly created PKI environment. Because so much depends on this trust requirement, the PKI implementation team should formally document all the security requirements and processes that constitute the basis for establishing trust in the PKI environment.

Trust can be established using various management and security services, such as:

a) Inclusion of key resources who can help provide compliance and management oversight.

b) Providing independently managed physical security over all the PKI hardware, software, and cryptographic components.

c) The application of appropriate system and network security over the environment.

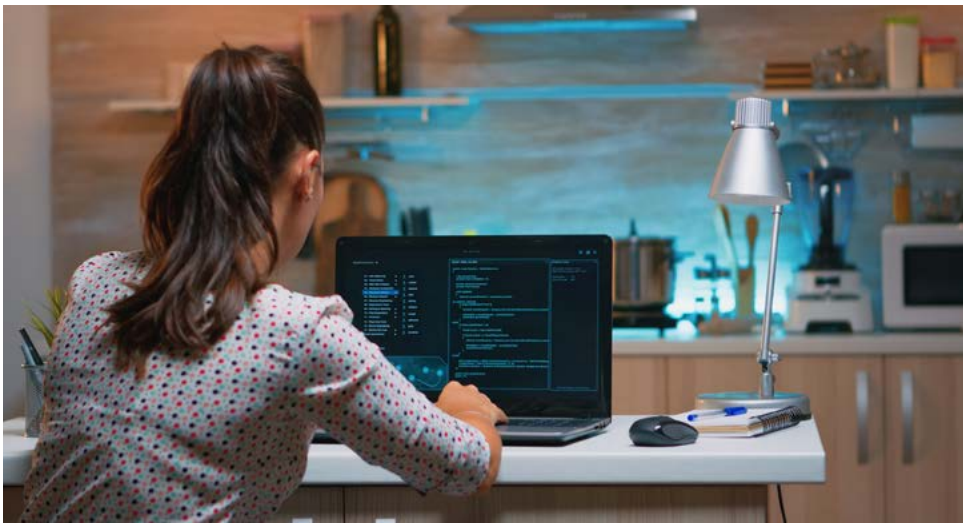
d) Documenting an auditable and trustworthy process for creating each Certificate Authority.

e) Secure generation and storage of the primary keys used by each CA (Root and Issuing CAs).

f) A formal observation that the build process has been carried out correctly and can be audited for compliance with the expected actions and controls.

g) Auditable practices and processes have been implemented to manage full certificate life cycle operations, from initial provision to final destruction of sensitive cryptographic key material.

You can complete the Microsoft CA service build process in about 20 minutes with a few clicks accepting the default options...



A Formal Certificate Authority Build Process

One of the most common mistakes that happens in the PKI creation process is an informal build of the Certificate Authority (CA) internally by IT. It's technically quite easy to build a new CA service—most of the process is automatic. You can complete the Microsoft CA service build process in about 20 minutes with a few clicks accepting the default options, setting the key length, etc., and presto, you magically have a functional CA.

However, can we trust all subsequent use of the CA to create trustworthy certificates after an informal, unaudited process lacking stringent security controls? How do we know that someone didn't surreptitiously copy the CA's private key after key creation or if a rogue Issuing CA was created and its certificate was signed by the Root CA? If the Root CA is attached to your network, or your Issuing CA is not in a secure protected network zone, or if physical and logical access to the CA is not controlled, then how do you know the CA hasn't been surreptitiously accessed for a bad purpose?

In such circumstances, if control over your CA and its keys has been lost—you will then be issuing "trusted" certificates from an untrusted source. Unless physical protection and access controls over all the PKI hardware, software, and cryptographic key components are enforced from the very start of the creation process, then we can only hope that the environment is trustworthy after the fact. For this reason, strong controls around the creation and access to any part of the PKI must be strictly maintained and audited for compliance with the controls. You must also document a detailed process for creating your CA and generating the signing keys associated with it. This process is called a "key signing ceremony" and it forms the basis for knowing that everything about the creation of the CA and the generation of the CA's keys was done in a manner that can be trusted and is auditable.

Certificate Authority Key Signing Ceremony

Having a formal key signing ceremony ensures the CA and the cryptographic keys that are used by the CA to sign and validate other CAs are all created and maintained in a secure and auditable state. A detailed, step-by-step process is first documented, reviewed by management, and then rehearsed by all the staff who will be involved. And by detailed, we mean documented down to the individual action and keystroke wherever possible.

Once the final process has been approved and everyone has been trained to carry out their role in the process, the ceremony can be executed. Normally this is a "public" ceremony, in the sense that there is nothing to hide—many organization do a live video stream of their ceremony so that anyone who is curious can see what is being done. Your ceremony should be videotaped and saved for future auditability and compliance review.

Typically, a Master of Ceremonies orchestrates the ceremony and reads out each step in the ceremony script as the appropriate person (Physical Security Manager, OS Technician, CA Operator, Crypto Operators, Auditors, Senior Management, etc.) carries out the designated action. Everyone has a copy of the ceremony script and checks off each step once completed or raises an objection if they see an issue where the process is not being carried out as documented. Everyone then knows that the key signing ceremony was properly executed and that, when completed, the CA and its signing keys have been set up in a secure and auditable fashion.

Typically, you will have a Root CA (RCA) key signing ceremony and a separate ceremony for your chained Issuing Certificate Authority (ICA) that runs under the supervening control of the Root CA.

Everyone has a copy of the ceremony script and checks off each step once completed or raises an objection if they see an issue where the process is not being carried out as documented.

Certificate Policy (CP) and Certificate Practice Statement (CPS) Documents

Each of your Issuing Certificate Authorities will require a Certificate Policy (CP) and a Certificate Practice Statement (CPS document, collectively referred to as the CP/CPS documentation. Some organizations combine them into a single CPS document, but normally it is easier to control and revise if the information pertaining to each document is kept separate.

The Certificate Policy (CP) provides information on what kinds of certificates will be issued by the ICA and details about the individual certificate fields and values allowed in each type of certificate. The Certificate Practice Statement (CPS) document describes what certificate- related activities can be carried out on the ICA. For example, will the ICA provide certificate suspension and archive processes? How will certificate revocation be done and under what circumstances? How often will a CRL be created and where will it be published? All the activities of the ICA are documented and published so that users of the PKI know what services are provided and how they will be provided.

Key and Certificate Life Cycle Management

It's a straightforward process to publish digital certificates; the hard part is providing an inventory of keys and where they are being used, and managing all the certificates and key pairs through their entire life cycle. Do you know where all your managed and unmanaged certificates are being used in your organization?

Documented certificate management processes should include key provisioning and creation, distribution, storage, usage, backup, rotation, revocation, archive, renewal, and final destruction. For a small organization, this can be a spreadsheet or database application itemizing the characteristics of each certificate being managed. For example, you need to know who owns a certificate, the type of cert, and when it expires so you can act when renewal time approaches. For growing and larger organizations though, this process will quickly become difficult to control as the number of managed and unmanaged certificates increases. Generally, once the total number of managed certificates exceeds a thousand, automation of the full certificate management process should be considered, including the onboarding of other third-party certs that are currently unmanaged.

One big advantage of using a formal certificate management tool such as Venafi is the ability to automatically stay on top of certificate renewal and compliance requirements. There is nothing as frustrating and embarrassing as having to scramble and find the right resource to renew a web server SSL certificate after customers call to complain that the secure web services are broken because the cert has expired! There are also Unix-based secure connection services, such as SSH, which can use keys that never expire. Controlling these types of keys and automating key rotation processes will greatly improve your security posture and can do away with the manual renewal processes required in the past.

Use of a Hardware Security Module (HSM)

Depending on the types, strength and value of the certificates your CA creates, you may wish to optionally deploy a Hardware Security Module (HSM) to generate and store sensitive cryptographic key material.

An HSM is a trusted, security-hardened device that provides strict control over both cryptographic keys and the cryptographic operations allowed in your CA. Trustworthy HSM devices conform to the FIPS 140-2 standard for maintaining reliable security controls over crypto operations. Small USB memory stick-sized crypto key storage devices with a FIPS 140-2 level of trust are now reasonably priced. They allow your sensitive keys to be securely transported and stored without worry about unauthorized access.

At a minimum, the keys for your CA should be stored on such a device to deter unauthorized access and ensure they can be securely locked up when not in use. If your CA keys are generated in software and stored on the CA's hard drive, then unauthorized access to the CA may also allow access to these sensitive keys. However, if the keys are managed on a security hardened storage device, then they can be protected against unauthorized access or copying.

Conclusion

If you review and action all (or most) of the PKI best practices described in this article, you have a much better chance of success in creating and maintaining a secure, robust and functional Certificate Authority. If PKI is not a part of your core business focus, the options of outsourcing PKI or using professional consulting services to help do the initial heavy lifting may also be an effective means of building a PKI for your organization.

However, while it may appear daunting for the first-time neophyte, there are many existing documents and internet resources available for review and reuse so you don't have to "reinvent the wheel." Being mindful of best practices while building your organization's PKI can result in a robust and secure system that you will be proud of for many years to come.

Partner with Difenda

Difenda is a global cybersecurity leader with decades of experience helping companies like yours defend against cyber threats and manage their security risk. Established by cybersecurity professionals and leaders with intensive practical experiences in assessing, responding, and securing organizations, Difenda has the expertise and advanced capabilities to protect your organization from evolving cyber threats.

We incorporate big data analytics, machine learning technologies, and artificial intelligence to prevent, detect, and respond against sophisticated cyber threats. Partner with us and gain peace of mind knowing cyber intelligence experts are available on demand to stop breaches, mitigate damage, and recover operations.

LEARN MORE