An Overwhelming Need for PKI

The IT space is being dominated by the BYOD (Bring Your Own Device) and Internet of Things (IOT) boom which is exponentially increasing the number of connected devices to internal networks and the internet. Intel predicts that 200 billion objects will be internet-connected by 2020, and that number is rising every day.¹ Given that BYOD and IOT have become mainstream and more objects are connected to the Internet every day, security concerns surrounding device authentication and secure communication have become a major focus of the organizations contributing to these initiatives – more risk means more security controls.

Digital certificates issued from a Public Key Infrastructure (PKI) are undoubtedly one of the most effective methods for securing and provisioning access to both internally connected network enterprise resources and internet-connected “things.” However, an effective PKI can be difficult to implement and manage without knowledgeable and dedicated resources in-house.

Hurdles of Tackling a PKI Implementation

If you’re planning on building a PKI using internal resources, make sure you’re aware of the potential hurdles you may face when depending on your staff to get a PKI up and running:

• **Division of deliverable ownership (i.e., the "two-headed hydra"):** A PKI project has a unique construct in that it will require significant participation from at least two distinctly separate divisions within the organization. A security team (usually reporting up to the CISO) will be required to define the certificate policy the PKI will be required to operate under and a Network Operations team (usually reporting to the CIO) to execute on processes that are germane to the certificate lifecycle process.

---

Figure 1. Division of Deliverable Ownership

---
Appropriate skill level and availability of internal expertise:
Having available, knowledgeable staff who possess the expertise necessary to set up, implement and sustain a PKI on an ongoing basis is critical. As recommended by Microsoft, your Network Operations team will need specialists with the ability to:

- Create and modify certificate templates as needed by application owners
- Manually issue and revoke certificates as well as understand how to setup auto-enrollment
- Carry out server administration duties: hardware, applying patches, and creating meaningful backups
- Publish Certificate Revocation Lists and manage the CA itself

Unfortunately, the field of PKI experts with enough knowledge to sustain the day to day operation of a PKI is waning. Finding a reliable expert who can not only design and implement a “healthy” PKI, but maintain its health on an ongoing basis is becoming harder; as a result, talent is also becoming more expensive.

It is critical that the team responsible for your PKI project takes a holistic approach to implementation. They must understand that specific practices and policies must be in place from the first step of implementation in order to be able to sustain the PKI with full assurance that it will not be compromised.

Extreme sensitivity to policies and practices: A PKI cannot be implemented haphazardly (i.e., running an install wizard and clicking “next” through the options). Robust practices and policies must be in place and the PKI must be correctly configured in order to sustain the PKI’s assurance over the long-term so that specifically, the trust level required is not, and will not be, compromised. Moreover, there must be an operating procedure for how to set up your PKI, and guidelines for how it should be used throughout its life.

Failure to adhere to strong policies and practices can expose your business to a number of risks that are difficult to recover from, including but not limited to “man in the middle” attacks, identity theft, and corporate espionage. A PKI can be a very effective tool to mitigate these kinds of risks, but only if the appropriate trust level is maintained.
Executing a Successful PKI Implementation Project

The key to a successful PKI implementation is understanding the entirety of the project. Each step from the beginning stages through implementation must be thought out and planned. To begin the planning process, consider the following best practices for initiating a successful implementation.

PKI Implementation Best Practices

- **Understand What Goes into the PKI Design:** A common error organizations make before even beginning a PKI project is fully understanding what goes into the design. It may look simple on paper, but the process of architecting a design that fits your business needs and use cases is critical to verify before starting. Know and document your organization’s needs and applicable use cases thoroughly. Each following step throughout the rest of the project will depend on these use cases, and an incomplete or inaccurate inventory could, at the least, create more arduous work to remediate the shortcomings, and at the worst, create a PKI that will not satisfy the organization’s certificate needs. Note that certain settings while building the PKI are “burned” into its fabric with no option to modify them later.

- **Have a Uniform Policies and Practices Statement:** Build out robust policies and practice statements so that your security team (or external auditors) have a baseline to engage against when it comes to making sure the PKI is healthy during its lifecycle. If a PKI is implemented without proper policy and practices documented, a security or audit team will not have adequate tools to determine what was intended to be delivered with this PKI, nor will they know if the assurance level has been appropriately maintained throughout its lifecycle. Creating these documents will take a non-trivial amount of project time, but the benefits of having them after the project is complete are huge.

"The key to a successful PKI implementation is understanding the entirety of the project. Each step from the beginning stages through implementation must be thought out and planned.”
— Michael Thomas, Certified Security Solutions (CSS) Director of Delivery
• **Plan and Account for the Root Signing Ceremony:** Building the root CA (i.e., the root signing ceremony) is akin to creating a “master key” to an organization’s network and should be recognized with the same sensitivity. The building and configuration of the root CA should be well scripted in a controlled environment. Depending on the assurance level desired for the PKI, this ceremony will range from an informal execution of a scripting document (low assurance) to a formal filmed event in a pre-authorized space (high assurance). From the second the root CA is created, a chain of custody is created which must remain intact from the minute it’s incepted throughout its lifetime. If this chain of custody is broken at any time, the potential for malware polluting the machine, erroneous certificates being created, or the login security of a root CA must be assumed to have happened and the root should be considered compromised. At that point, your PKI is not trustworthy and all certificates issued must be considered invalid – do not let this happen to you. This is a security measure you have deliberate control over from the beginning.

• **Verify That All PKI Components Are Properly Operationalized:** While moving into a steady state, make sure all components of the PKI are properly operationalized. Like most assets created from a project of this type, when it moves into being part of the corporate infrastructure there’s no longer a project team accountable for the maintenance and upkeep. A PKI requires a significant amount of care and feeding to remain functional – these are dangerous tripping points for security teams who were focused on simply implementing the PKI, but not its ongoing operations.
Performing a Buildout

Whether you’re tackling PKI internally or with a partner, there are many parties involved in its successful implementation. Therefore, it is important to have a detailed implementation plan. The following sample PKI implementation outline is a good starting point to illustrate how various project phases can be broken down and executed:

PKI Implementation: Weekly Project Phase Buildout

**Phase 1**
- Project kick-off and design sessions
- First iteration of the design

**Phase 2**
- First iteration of the design
- Create first iteration of the documented certificate policy (CP) and certification practices statement (CPS)

**Phase 3**
- Review and sign-off of the design document (all security stakeholders)
- Review and revise certificate policy (CP) and certificate practices statement (CPS) documents

**Phase 4**
- Preparation for key signing ceremony and production rollout (i.e., complete change management processes and assign roles for implementation)
- Procure and install production hardware (HSMs and servers)
- Create a key signing document and prepare for the ceremony

**Phase 5**
- Complete root signing ceremony
- Create disaster recovery (DR) cryptography artifacts
- Build and configure production of subordinate CAs
- Configure other ancillary PKI servers
- Validate the health of the new PKI

**Phase 6**
- Validate migration strategy
- Begin issuing first set of production certificates

**Phase 7**
- Complete all documentation
- Move PKI to steady state and assign ownership for ongoing tasks
- Project completion
Knowing Your Options – Implementing
PKI In-house vs. Working with an Expert

Executing a PKI deployment internally can be done successfully so long as you have the necessary expertise and tools required to correctly execute all aspects of the project. The biggest common pitfalls are a lack of the right expertise and failure to give credence to preparation steps. Implementing a PKI is complex, but if your security team is experienced and armed with knowledge of all aspects of PKI, it’s a project that can be carried out favorably.

The advantage of working with an external party is having access to industry best practices for dealing with this complex infrastructure, as well as the knowledge and sensitivity to policies that ensure that your PKI isn’t compromised from the outset. If you’re not confident that you have the right internal specialists, do not go it alone!

A PKI partner will be able to:

- Provide professional PKI services with the necessary expertise to facilitate an infrastructure build.
- Assist with integration plans for PKI-enabled applications.
- Fully manage or assist with building a process to manage the lifecycle of digital certificates.
- Develop, deliver, and maintain a strong public key infrastructure that provides business value over the long term.
- Offer access to services designed specifically to meet your unique assurance requirements, which will allow your security and IT personnel to focus on the objectives critical to their roles.

Deciding Whether Internal Execution Is Right for You

Whether you deploy internally or work with a reputable provider who can support your PKI project, it has to be done right. Make the best decision for your business based on the resources available to you.

Unless you have access to a seasoned PKI consultant, carrying out a PKI implementation will be considerably difficult. A third-party expert will be objective and ensure that that the full process is carried out – no security consideration will fall to the wayside. If you’re not fully confident in your internal resources, get in touch with a PKI partner.
How CSS Can Help

PKI is not just a necessary evil – it has many beneficial business cases, and can be leveraged for identity and access management. Knowing that, it must be prepped and built correctly; if it isn’t, identity and access management capabilities can create significant vulnerabilities within your network. On the flipside, if it is done correctly, your network will be locked down in a secure and convenient fashion.

At CSS, we use an effective, repeatable methodology for PKI implementation project management for every customer. We will take the time to understand how you need to use your PKI and begin by building the use cases that work for your business.

• Define PKI use cases
• Initiate custom PKI design
• Build policies and practices
• Build infrastructure
• Complete root signing ceremony
• Implement downstream applications
• Utilize the PKI and satisfy business use cases

CSS can assist you in addressing pressing PKI implementation challenges with the knowledge, experience, and operational efficiency needed to execute an efficient and effective PKI project.

About Certified Security Solutions (CSS)

As the market leader in enterprise and IoT digital identity security for data, devices and applications, CSS is a cyber security company that builds and supports platforms to enable secure commerce for global businesses connected to the Internet. Headquartered in Cleveland, Ohio, with operations throughout North America, CSS is at the forefront of delivering innovative software products and SaaS solutions that are secure, scalable, economical and easy to integrate into any business. Visit www.css-security.com for more information.
References
