Key Considerations in Setting up a PKI Environment
Implementing enterprise-wide strong authentication is critical in today’s word of increasing cyber insecurity. As hackers get smarter and intrusions get more widespread and more damaging, no enterprise can depend on old school protocols to keep their data, networks and people safe. User names and passwords have been the trusty lock on the front door for decades, but they’re no longer secure enough. With more than 90 percent of organizations reportedly being breached, you can’t afford to be caught off guard. A breach can cost hundreds of thousands of dollars and do irreversible damage to your reputation.

Public Key Infrastructure or PKI is a well-known security protocol used by top enterprises, defense departments and governments around the world. Increased use of cloud-based services and the Internet of Things (IoT) are prompting a surge in PKI adoption. But even though PKI technology has been around for years and is widely used, especially in security-minded organizations, there remains a hesitance when it comes to undertaking an enterprise-wide deployment.
Why do you need PKI?

PKI is military-grade security, so you’re assured of the highest protection of your sensitive documents and authentication of your users. But PKI is so much more.

**Additional security functionalities:** With PKI, you can encrypt data, disk, and email, as well as digitally sign. These functions are becoming increasingly important as companies need to protect digital file exchange and encrypt content to prevent hackers from intercepting communications.

**Optimized authentication and cost savings:** Password management is costly. PKI eliminates the need for users to remember long, complex passwords that they will need to change frequently. A single credential will give users access to multiple applications. In addition, it’s much more cost effective to have a single solution that includes multiple functions than adding each separately.

**Improved business processes:** Eliminating password protocols will reduce helpdesk calls and overall IT overhead. And with a certificate management system in place, administrators have control of the complete certificate lifecycle management (enrolling, provisioning, and revoking) and auditing tools at their fingertips.

Don’t fear PKI

It is true, PKI used to be difficult to implement, and was seen as complex, labor intensive and expensive. The development of powerful credential management software brought considerable improvements and now does much of the manual work that used to be left up to the administrators. And it’s important to note that not all PKI implementations are created equal. Some are inherently more complex, depending on the level and layers of security needed for your organization.

Gemalto has created a PKI Implementation Guide, broken into five-steps for easier understanding. Follow our lead and you can have a PKI solution up and running in no time. Or if you decide not to tackle the implementation yourself, we offer professional services to help.
Manageability—in the context of automation, how much do you want? Do you want to automate the full lifecycle of the token or smart card? If so, you will need to consider a Certificate Management System. You will also need to plan whom in your organization will be in charge of assigning user roles, certificate enrollment and revocation.

Security policy—the security policy should include approval processes for managing users and assigning certificates. The PKI policy should follow corporate security policies and should also consider any government or industry regulations.

Flexibility and Scalability—as mentioned, PKI solutions can vary from very simple to very complex. Small to medium sized businesses can have a fairly simple design. Organizations that need to support different technologies and levels of security many need a more complex design.

CA type—you can acquire your certificates from a public CA or you can choose to operate an in-house private CA to issue certificates. Whether you decide on a public or private CA will depend on how you plan to use the certificates. For example, companies that won’t be issuing many certificates (more costly) and that don’t want the added responsibility of issuing certificates may choose a public CA.

Key considerations before setting up a PKI
Before running full steam ahead into the PKI configuration and implementation, it’s important to adequately plan and understand that certain decisions influence other decisions. If you ignore the planning part, you may spend much time undoing and going backwards in the process. So take time to carefully consider the following planning guidelines.
Companies who choose to set up a private CA will benefit from better security because they’ll be issuing certificates only to those users who are trusted members of the company. With a private CA, you have complete control over the certificate process. Although setting up a private CA may require more management, there are solutions to make this process easier.

Also, if considering a public CA, it’s important to look at the reputation of the firm. All CAs must pass security audits, but there are some who have made security errors. Do your research and make sure you choose a CA with a solid reputation.

**CA deployment model**—generally, the higher you want to secure your environment, the more tiers are needed to separate CA roles. For example if your organization

> **One-Tier Hierarchy**—contains one single CA that acts as both a root CA and an issuing CA. This is not recommended for production PKIs because the compromise of the single CA compromises the entire PKI. Only for the simplest of implementations.

> **Two-Tier Hierarchy**—this is the most common architecture. It is also more secure than the one-tier design because the Root and issuing CAs are separated. In the two-tier, the Root CA is offline, and a subordinate issuing CA is online.

> **Three-Tier Hierarchy**—contains a root CA tier (offline), an issuing CAs tier (usually online), and an intermediate tier placed between them. A company may have several reasons for needing the additional tier (for instance to have a policy CA that restricts the types of certificates issued), however with the additional tier comes additional costs and manageability issues.

**Security aspects**—ensuring the proper controls are in place is a critical consideration when planning a PKI solution. How will you protect the private keys? Hardware Security Modules are considered the most secure method, but there are other options.

**CA configuration**—certificates have a period of time for which they’re considered valid. When planning your PKI solution, you should determine an appropriate lifetime (start and end dates) you will apply for each CA certificate issued by your CAs.
Getting down to it

Using our five step process, you can setup at PKI environment quickly and without too many headaches. However, we use Microsoft servers and Active Directory, so it is assumed you have a Microsoft environment already in place. In addition, you will need a Certificate Authority.

Using the Gemalto Five Step Implementation Guide, you will learn to set up a two tier Microsoft PKI infrastructure with Gemalto SafeNet Authentication Manager and SafeNet Luna HSM to perform smart card log on for small to medium sized enterprises.

Main steps to creating your own PKI environment

1. Install and configure SafeNet Luna HSM

2. Install the root CA and configure it with SafeNet Luna HSM

3. Install and configure the issuing CA

4. Configure the permissions of users and create certificate templates

5. Install and configure SafeNet Authentication Manager
Ready to go?

Gemalto’s Five Step plan is available for any small to medium size business that wants to implement PKI internally. Please contact sales to receive the Implementation Guide and to inquire about the necessary solutions:

www.gemalto.com/companyinfo/contact-us
About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.