What is PKI?

PKI (Public Key Infrastructure) ensures secure exchange of data and authentication over the Internet through management, distribution and identification of public encryption keys.

Depending on the complexity of the deployment, PKI can include a combination of components (hardware, software, policies and standards) to manage the process of creating, distributing and revoking keys and digital certificates.

Benefits of PKI

- Military-grade security: PKI provides the highest protection of your sensitive documents and authentication of your users.
- Additional security functionalities: With PKI, you can encrypt data, disk, and email, as well as digitally sign.
- 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.
- Improved business processes: Eliminating password protocols will reduce helpdesk calls and an overall IT overhead.

Main components of a PKI?

- Digital certificates
- Public and private keys
- Secure sockets layer (SSL)
- Certificate Authority (CA)
- Key security (HSM)
- Management tools

Don’t Fear PKI!

It is not the intimidating beast it used to be, and Gemalto has developed a five step plan to help you do it yourself!

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

DIY PKI
Do It Yourself Public Key Infrastructure