White Paper

Best Practice: Securing the Root CA of a PKI with a Utimaco HSM

Introduction: Why is PKI important?

Public Key Infrastructure (PKI) plays a vital role in securing IT infrastructure. From passport issuance to border control and all the way to user and device authentication within an enterprise – PKI plays a key role in ensuring trust. It helps establish a chain of trust both within and across the boundaries of an organization. As such, it facilitates the exchange of data in a secure and trustworthy manner.

Securing the Root CA of a PKI: Securing the Root of Trust

Since transactions in such an infrastructure have to be validated all the way up to the root certificate of a PKI, the entire trust model depends on the trust that can be placed in the measures taken to properly safeguard the Root of Trust – the Root CA. It is the Root CA's private key which is directly or indirectly used for signing any public / private key pair down the line, all the way to the end user or device certificate. Thus, it is exactly this single point of failure which needs to be guarded according to all the principles of modern information assurance. But what are those principles and how can Utimaco CryptoServer HSMs help you implement them?

The Utimaco CryptoServer as network-attached appliance is a 19", 2U HSM platform, delivered as a FIPS 140-2 Level 3 (Se-Series Gen2) or FIPS 140-2 Level 4 for physical security Level 3 overall (CSe-Series) certified device. It comes equipped with dual field exchangeable power supplies in a hot-hot layout and redundant Ethernet ports guaranteeing high availability setups.

Best Practices for securing the Root CA:

When it comes to securing the Root CA's private key in a PKI, the following best practices should be considered:

- Dual control:
  - Security principle: Access and usage of the Root CA's private key for signing new certificate requests should always take place under the supervision of multiple different roles within your organization.
  - Utimaco offers: A highly flexible and configurable role-based access control (RBAC) architecture which allows you to map the different roles defined in your Root CA's security policy to the different authorization levels provided by the CryptoServer.

- Least privilege:
  - Security principle: Root CA administrators should only have access to the data necessary to perform their duties.
  - Utimaco offers: The RBAC architecture strictly separates the rights assigned to each predefined role and, moreover, allows you to further harden or disable specific functions as per to your security policy requirements.

- Keep CA offline:
  - Best practice: Keep the Root CA offline whenever not required for signing new certificate requests.
  - Utimaco offers: A highly flexible and configurable role-based access control (RBAC) architecture which allows you to map the different roles defined in your Root CA's security policy to the different authorization levels provided by the CryptoServer.

- Physically lock the offline CA away:
  - If it is a requirement to store the offline CA in a secure place, physically disconnected from the network (e.g. in a Safe), this can be done easily. Therefore, the HSM is backed up onto an external storage device, e.g. a USB thumb drive. This external device shall be placed in the secure place e.g. in the Safe, together with the smartcards which containing the MasterBackupKey (MBK) of the HSM carrying the root CA. Once this has been done, the HSM is cleared by pressing its external erase button, so none of the CA key material is present anywhere outside of the safe.
  - To reactivate the HSM for the root CA, the backup and the MBK is taken from the safe and restored onto the device.

- Secure audit trails:
  - Meeting compliance requirements: Generating and safeguarding logging information produced while operating your CA is vital for proving compliance to various regulations. It also helps significantly in backtracking all the transactions performed by your CA.
  - Utimaco offers: Configurable logging capabilities and the safeguarding of the produced logs within the secure HSM environment.

Conclusion

Securing the Root of Trust in your infrastructure is vital. It is no longer a question of whether you need to do it, but rather how you can best implement the key security principles. Utimaco has extensive experience in the field of hardware-based security solutions and offers a variety of highly configurable HSM models which can be tailored to fit any defined security policy. Furthermore, you have the opportunity to perform any testing in advance and free of charge with the help of our fully functional HSM simulator.

About Utimaco

Utimaco is a leading manufacturer of HSMs that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions.

Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 200 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit https://hsm.utimaco.com

Would you like to try out our HSM or implement new algorithms yourself?

Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product. Register here for your download.

Ready to take off?
Download our HSM simulator!

Register for free

The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.