White paper

Key Management with Utimaco CryptoServer

Introduction

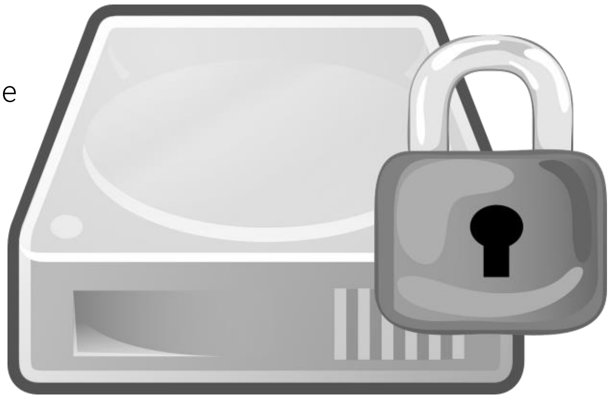
Data breaches are becoming more sophisticated and any institution managing customer or corporate information is vulnerable to an attack. Encrypting data is the first step in protecting critical business and consumer data, the second step is to create and store the cryptographic key that unlocks that data. This white paper will compare and highlight the differences of proper key generation, management and storage.

When talking about key management, one has to differentiate between managing the lifecycle of the cryptographic key, and the usage of a cryptographic key within an application.

Creating a Cryptographic Key - Pseudo or True?

Cryptographic key lifecycle management starts with key generation, generated by two different means: the first is called pseudo random number generation. This method employs a software program to create an initial seed number that is as random as possible. In many cases this method is considered secure enough. The second method is true random number generation which relies on the anomalies in physics instead of the constraints of zeros and ones found in code. The random seed number is consequently derived from electrical noise, quantum mechanics, ambient noise, and other “quirks in nature” that occur in a truly random manner. Instead of the digital equivalent of flipping a coin, Utimaco uses a true random number generator certified by the German BSI according to AIS31, ensuring the highest quality key material.

Where to Store the Keys – Software or Hardware?



Storing a cryptographic key is just as important as creating it, and a central aspect of key lifecycle management. There are a number of solutions available for safe and secure cryptographic key storage and the choice between different options will depend on the perceived value of the data. Software solutions used for this process store keys in main memory which means the system administrator, and anyone else with server access, has access to and the capability to create an extra key to access the data.

Compared to software solutions, hardware security modules (HSMs) offer strong security even in the most hostile environments. The module can detect when any attack is happening, including drilling, heat, power blackout or chemical attack, and automatically delete the keys immediately. In comparison, software-based cryptographic keys can be captured in the moment of unlocking – offering attackers the ability to learn the software, exploit vulnerabilities and run attacks remotely.

True security for cryptographic keys comes from creation within a hardware security module (HSM) as no one else will ever be able to recreate or access the key and the data. In HSMs, there are no backdoors. Utimaco provides the highest possible flexibility combined with the most stringent security controls in place through a unique general purpose HSM platform: the Utimaco CryptoServer product series.

Internal Key Storage – When a Breach is not an Option

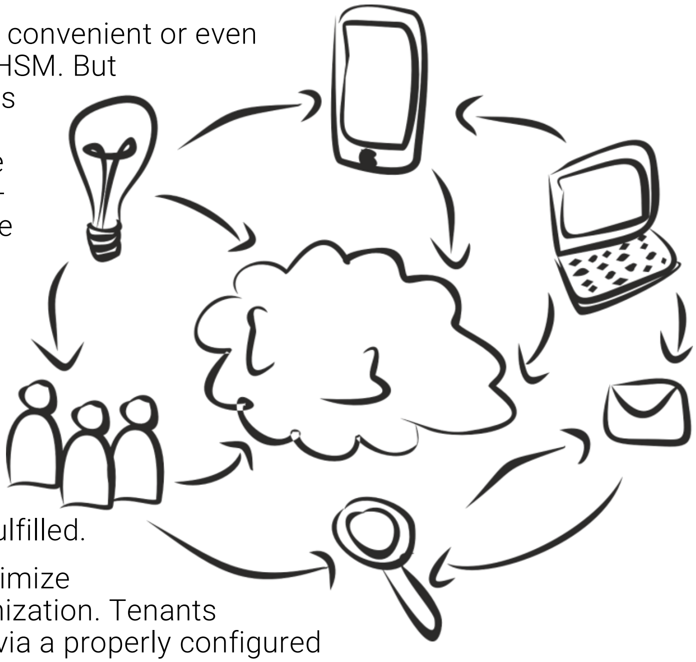
A hardware security module is a specialized device that can be rated either Level 3 (tamper evident) or Level 4 (tamper resistant) which is the highest rating in the industry. When you create a cryptographic key within a hardware security module, it is used to both encrypt and decrypt your data. Storing cryptographic keys in the internal Utimaco CryptoServer Key Store ensures that the most critical keys in your infrastructure are safeguarded according to NIST FIPS 140-2 Level 3 and 4 guidelines at all times: when in use, in transit or while stored.

The ability to physically and logically safeguard keys, in accordance with the highest standards in the industry, inside the isolated CryptoServer environment becomes particularly useful in modern IT infrastructure deployments. Multitenant data center environments are a typical example of IT resources that are under the control of a third, potentially untrusted, party, shared by multiple, sometimes competing, clients. To meet the security requirements imposed by such IT environments, Utimaco offers an out-of-the-box solution to provide a physically secured device that is accessible only via dedicated APIs and that enforces dual control and segregation of duty policies.

By declaring a key as non-exportable during its generation, it will never leave the HSM, not even in encrypted form for backup or replication. Using such restrictive settings complies with the requirements often set forth by security policies to create *qualified signatures* by Secure Signature Creation Devices (SSCD).

This method of internal key storage is recommended to any organization that needs to adhere to the highest level of control and security.

External Key Storage – When Sharing Cryptographic Resources



There are several circumstances that make it more convenient or even necessary to store cryptographic keys outside the HSM. But in situations where the clustering of HSMs becomes a necessity and where redundancy and fail over capabilities are as important as secure storage, the usage of dedicated encrypted external Key Stores—accessible only via HSMs—are the most appropriate approach.

In SECaS deployments, where multiple tenants share cryptographic resources provided by a single HSM to integrate trust and security into their infrastructure, control over dedicated Key Stores becomes one of the most critical requirements. With a Flexible CryptoServer HSM, the individual key lifecycle management requirements of any given tenant can be properly fulfilled.

Key Stores can be configured and deployed to maximize redundancy and to automate external key synchronization. Tenants entitled to these Key Stores can only access them via a properly configured HSM. For additional segregation of duty, an encrypted Key Store can be placed inside the trusted environment of one tenant who holds sole control. In such a set-up, the HSM and cryptographic keys required to access the keys that are stored in the external Key Store are under the control of the SECaS provider, while at the same time the Key Store itself is under the control of the tenant. Apart from that, different and independent security policies with respective key lifecycle management set-ups can be easily enforced.

The same way keys stored inside an HSM can be managed automatically, external Key Stores can be made part of an automated backup procedure, freeing key managers or administrators from the responsibility of regular manual backups.

Conclusion

The Utimaco CryptoServer HSM is designed to meet the needs of both internal and external key storage, no matter what the security requirements are. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. With German precision engineering, tamperproof Utimaco HSM offers scalable performance with the highest level of physical security and self-defense for hostile environments.