Case study

Securing a key player in the US auto industry with Utimaco HSMs

The motivation: Securing the connected car. Period.

As one of the world's leading electric car manufacturers, this automotive company is a visionary in their industry. In order to meet requirements for security network communications between cars and a broad range of services that the company provides to passengers in the car, this auto manufacturer required secure solutions to a broad range of use-cases, from code and firmware signing to remote, over-the-air updates and beyond.

The challenge: A public key infrastructure based on best-of-breed technology

As engineers assessed and helped define the requirements for an enterprise-level PKI environment it became clear that this customer required a robust, flexible, and highly available public key infrastructure. To meet their needs for issuing certificates for cars, clients and code signing, while meeting production delivery timelines, the PKI system was required to be designed, built, tested, and put into production within a short span of two months.

The solution: A Utimaco HSM as the Root of Trust for robust performance, availability and scalability

Leveraging best practices and industry experience, the System Integrator C2 Company evaluated top PKI software and hardware vendors and available solutions. After a thorough examination of requirements and solutions, C2 Company proposed a PKI architecture leveraging open source PrimeKey EJBCA software, VMware, Linux, and OpenVPN based on the Utimaco HSM for maximum security while providing scalability, performance and availability.

The implementation: On-Time and Under Budget

Drawing upon broad and deep experience in security and heterogeneous technologies, Utimaco supported C2 Company engineers as they designed and implemented a secure, enterprise-grade PKI system capable of meeting the client's security needs, meeting both time and budget constraints.

The technical solution: Symmetrical keys to protect consumer data.

Utimaco provided a FIPS-certified hardware security module (physical level 4) that is used to generate and store secure encrypted keys and digital certificates, used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, the HSM, and revokes them if needed.

More resources:

https://hsm.utimaco.com/

http://www.c2company.com/files/HA-Enterprise-PKI.pdf

http://www.c2company.com/files/C2_PKI_Services.pdf

About C2

C2 Company architects, builds, protects and maintains the networks and systems that enable enterprises to:

- Accelerate IT's speed and business impact
- Minimize costs and risks

To learn more about how we can help you too, contact us at 650.357.0100 or info@c2company.com. For more information, visit www.c2company.com

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep your cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Utimaco delivers a general purpose HSM as a customizable platform to easily integrate into existing software solutions or enable the development of new ones. With professional services, we also support our partners in the implementation of their solutions. Put your trust in Utimaco – today and in the future. For more information, visit hsm.utimaco.com