Utimaco Portfolio Overview

Hardware Security Products and Services

utimaco®

About Utimaco

Your Root of Trust

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

Utimaco delivers a comprehensive product family of HSMs. Each of our hardware models can be deployed as a general purpose HSM for easy integration into existing software solutions. They can also be customized to enable the development of new solutions. With our professional services, we support our partners to implement their solutions.

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.

Today, thousands of enterprise and infrastructure companies rely on Utimaco to guard IP, critical business data and applications against internal and external threats. Our HSMs help protect hundreds of millions of consumers globally. Put your trust in Utimaco – today and in the future.

Utimaco was founded 1983

First generation HSM: KryptoServer 1991

Launch CryptoServer CS 2000 2000

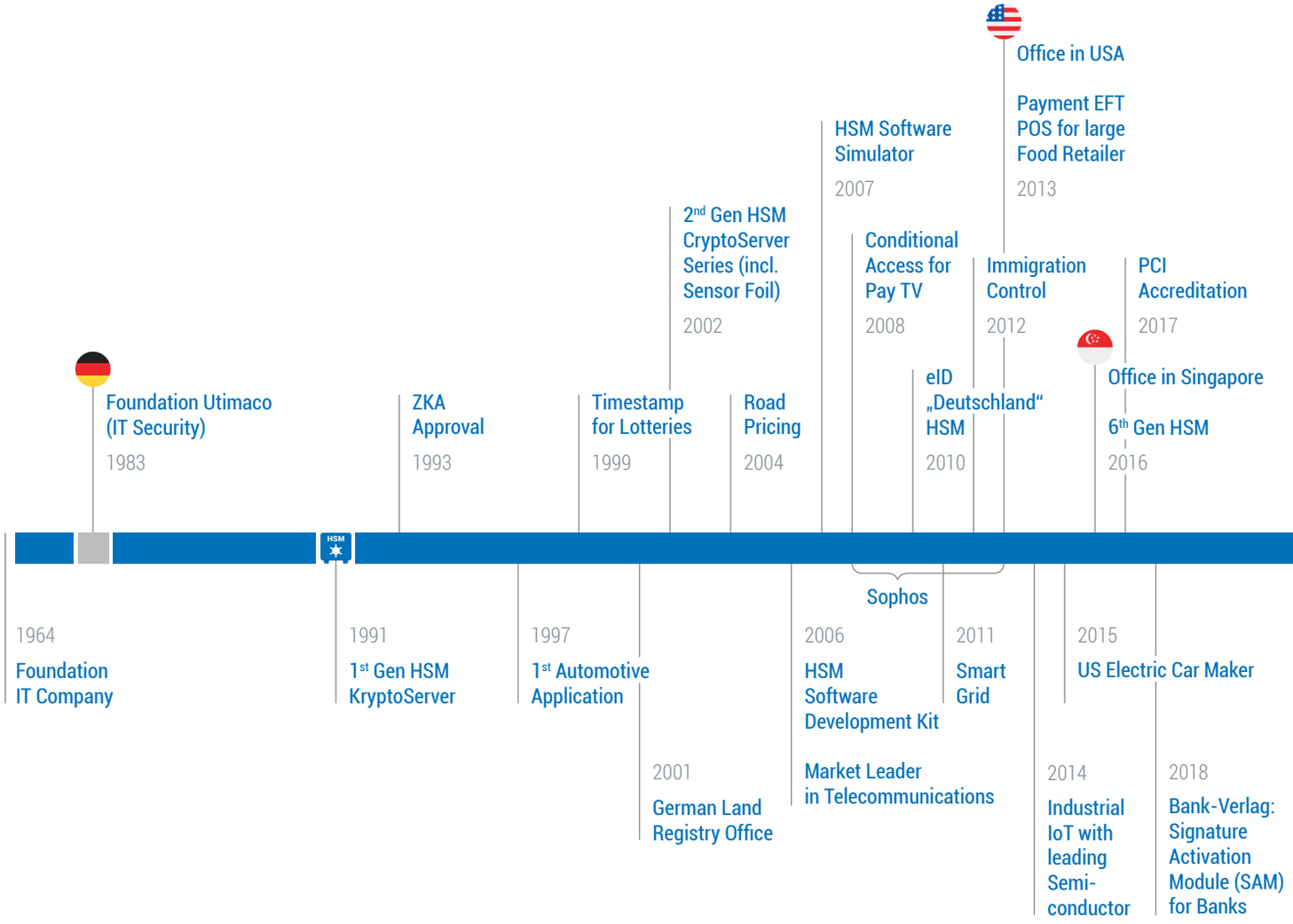
Launch CryptoServer CS 2005

Launch CryptoServer Se 2009

Launch CryptoServer CSe 2013

Launch CryptoServer Se Gen2 2016

25 years of experience in IT security



Securing the Internet of Things

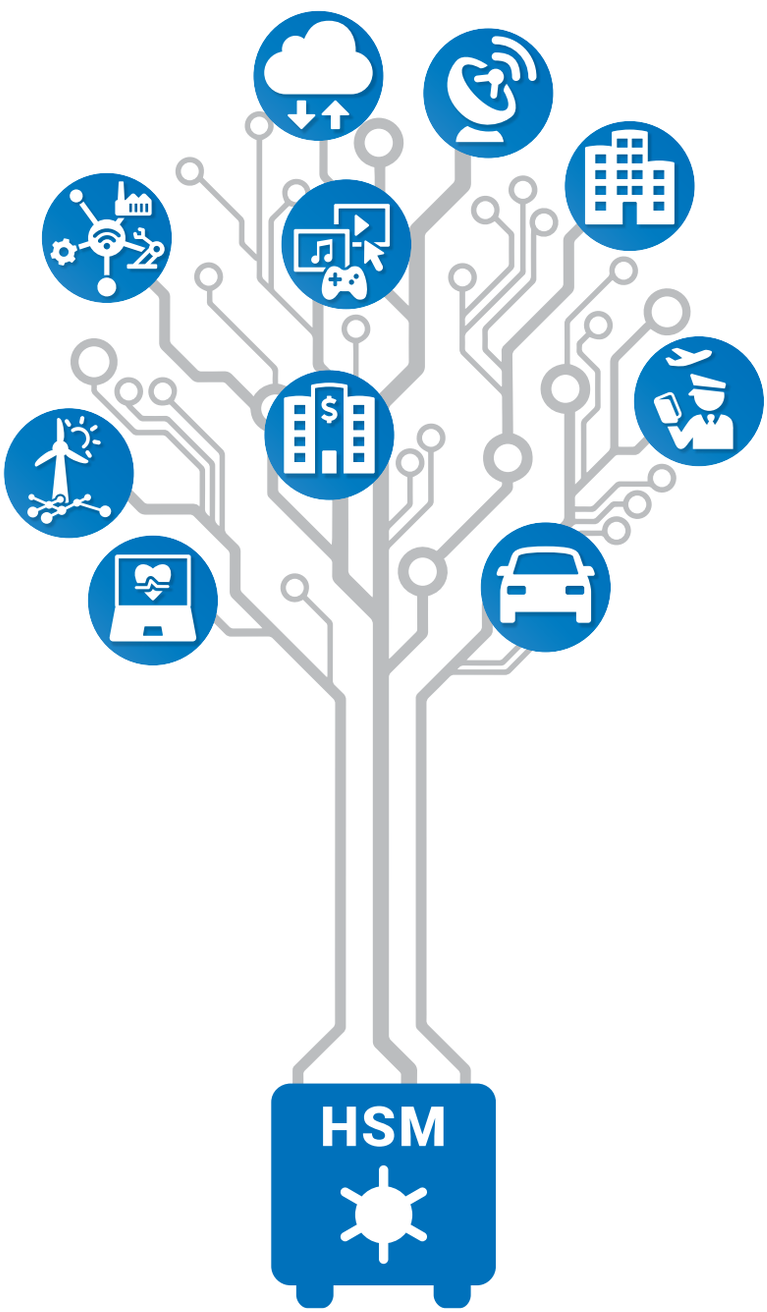
Industries and trends

Almost **every industry**, from automotive to industrial IoT, from eIdentity to eHealth, from smart metering to payment, is striving for interoperability and the open exchange of data – the core tenants behind the idea known as the **"Internet of Things"**. At the same time, this open exchange of data requires knowledge of where the data came from, assurance that the data is valid and confidence that it meets a certain level of integrity.

When sensitive information is shared, it needs to be protected. **Securing the connectivity and data exchange** between heterogeneous devices is imperative, in order to protect the data, as well as the privacy of the users and to safeguard system infrastructure.

Recent trends – such as moving into the **cloud and quantum computing** – add new IT security challenges to the agenda of businesses.

Protection of customer privacy, authenticity and authentication as well as data and communication integrity are increasingly recognized as the key enabler for the Internet of Things. To secure these, **Hardware Security Modules (HSMs)** are the first choice for providing the **Root of Trust**. How can this be done?



Utimaco HSMs are used as a Root of Trust in industries as diverse as:

- Automotive
- Industrial IoT
- eIdentity & eGovernment
- eHealth
- Utilities
- Payment
- Telecommunication
- Enterprise
- Entertainment
- Cloud

Applications

The main mechanisms for securing data, documents, identities or code while in transit and at rest are enabled by **cryptographic keys or functions**. For example via

- The injection of a cryptographic key into a chip to provide it with a unique identity (e.g. for anti-piracy or supply chain transparency reasons)
- Timestamping of code or documents, and the cryptographic signing of a document to make any modification visible
- The definition and initialization of an ecosystem like a public key infrastructure (PKI) to which access will only be granted by authentication and verification of identity
- Conditional access
- Commonly used database encryption to secure data at rest
- Random number generation which ensures high quality of the utilized keys and uniqueness of transactions

The most secure way to enable all of the mechanisms above is the use of an HSM for generation, storage, management and "withdrawal" of cryptographic keys.

This is why a **Hardware Security Module** is considered **the first choice for providing a Root of Trust** and securing privacy, authenticity and integrity of data and people in the Internet of Things.

Various application szenarios in which Utimaco HSMs are used as Root of Trust:

- Authentication
- Document signing
- Public key infrastructures
- Code signing
- Timestamping
- Key injection
- Random number generation
- Conditional access
- Database encryption

Utimaco Product Overview

Hardware Security Modules (HSMs) are the **core business** of Utimaco. It goes without saying that they comply with the most demanding security requirements to fulfill their purpose as a **Root of Trust**. They offer **easy role-based administration, scalability, low total cost of ownership** and they come with a comprehensive package of **services and training**. For regulatory compliance, **FIPS-validated** and **Common Criteria-evaluated** products are available. To ensure speed of implementation in end-customer projects and product innovation for system integrators, Utimaco also offers a fully-fledged **Software Development Kit (SDK)**.

General Purpose HSM SecurityServer

The **Utimaco SecurityServer** is a general purpose HSM that ensures the security of cryptographic key material for servers and applications. It includes integration software that supports the industry standard PKCS#11, Microsoft CSP/CNG/SQLEKM and JCE interfaces. It can therefore be used for the most common business applications, such as public key infrastructures (PKIs) or database encryption. The SecurityServer comes as a bundle with your choice of Utimaco CryptoServer Se-Series Gen2 or CSe-Series hardware, and includes a **software HSM simulator** for easy evaluation and integration testing.

Se-Series Gen2 or CSe-Series?

Utimaco's **Se-Series HSMs** have been designed to meet standard physical security and anti-tampering technology industry requirements. The **CSe-Series** integrates even stronger tamper-detection and tamper-response technology. It is therefore the best choice for use in hostile and uncontrolled environments and in market segments with the highest security requirements, such as banking and government.

Network appliance or PCIe plug-in card?

Both the SecurityServer Se-Series Gen2 and CSe-Series are available as 19 inch 1U network-attached appliance (CryptoServer LAN) for immediate use in data centers, or as PCIe plug-in card to fit into your server architecture or customized chassis.

Software Development Kit (SDK)

The **Utimaco CryptoServer SDK** is the professional development environment for all Utimaco HSMs.

- It enables system integrators and users to create specific applications, e.g. proprietary algorithms, custom key derivation procedures or complex protocols that run in the tamper-proof environment of the Utimaco HSM.
- As the CryptoServer SDK provides full access to the Utimaco base firmware, custom firmware modules can be developed in a very short time frame.
- The SDK includes the HSM simulator so you can easily test your firmware.
- Common development environment for all HSM models

With the **Utimaco CryptoScript SDK**, we are taking our professional development environment to the next level.

- It enables companies to develop customized applications with little effort and low overhead.
- You can script new key derivation mechanisms, use-case-specific data processing functions and custom extensions quickly and easily using CryptoScript SDK.
- It allows you to run multiple applications in virtual HSMs, with separate databases and roles enabling multi-tenancy.

PaymentServer

Using Utimaco's flexible Software Development Kit, companies can reach **full PCI compliance** for a solution or environment based on the standard PaymentServer product offering or via a customized and re-certified HSM application. PaymentServer can be leveraged for companies looking for

- PCI Data Security Standard (PCI DSS),
- PCI Point-to-Point Encryption (PCI P2PE), or even for
- PCI HSM as a delta certification with custom code running on the HSM.

CryptoServer Cloud

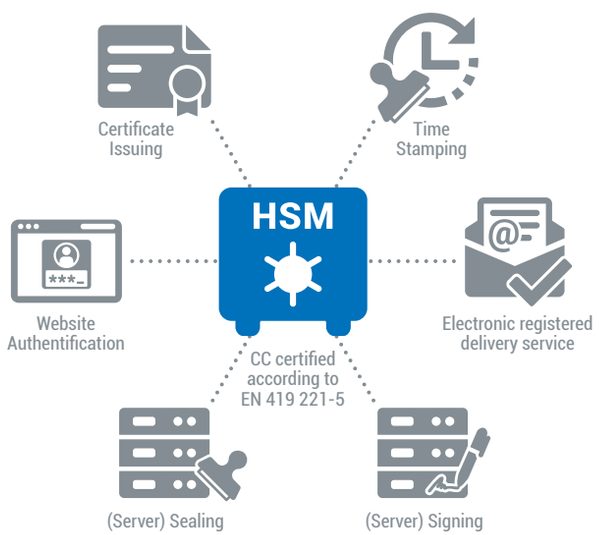
The Utimaco CryptoServer Cloud is **the Root of Trust for all cloud applications**. Cloud-based Hardware Security Modules (HSMs) in co-located data centers secure high value data and assets.

The CryptoServer Cloud is an HSM as a Service that offers the following advantages:

- Reduces your CAPEX
- Protects cryptographic keys and custom code in a dedicated HSM
- Seamlessly works with any major Cloud Service Provider (CSP) and supports multi-cloud deployments
- Gives you migration flexibility: no vendor lock-in to a specific CSP
- Support directly from the HSM provider with 8/5 and 24/7 options available
- Simple pricing: no set-up cost, only monthly commitments

CryptoServer CP5

The Utimaco CryptoServer CP5 supports Trust Service Providers (TSPs) in fulfilling policy and security requirements defined in various ETSI technical standards. With key authorization functionalities, it is ideally suited for **eIDAS-compliant** qualified signature creation and remote signing. Other application areas include the issuing of (qualified) certificates, OCSP and time stamping. The CryptoServer CP5 is based on the CryptoServer Se Gen2 hardware platform and **Common Criteria-certified** according to the eIDAS Protection Profile EN 419 221-5.



TimestampServer

The Utimaco TimestampServer is the ideal Hardware Security Module for business applications that require proving the existence of a document or data at a specific point in time. It ensures the **tamper-proof creation and authenticity** of timestamps and periodical re-creation of a current timestamp guarantees continuity of the audit trail. TimestampServer exists as network appliance only.

Common fields of application are:

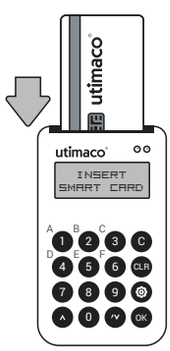
- Document management and archiving systems
- Long-term archiving solutions
- Electronic tender platforms
- Lottery and online betting
- Electronic contracts
- Support and ticketing systems

Deutschland HSM

A Hardware Security Module (HSM) specifically designed for applications such as identity management and issuing and managing eID documents. The Deutschland HSM (D-HSM) offers a secure solution with specific features and algorithms for the **production and initialization of electronic passports and identity cards**.

Accessories

Utimaco Hardware Security Modules support strong user authentication with smartcard and PIN as one of several authentication methods. In addition to **PIN Pad reader** and **smartcards** included in our product bundles, further units are available as accessories.



To facilitate the physical installation and continuous operation of our HSMs, we also offer **rack rails** and **spare power supply modules**.

Utimaco Services Overview

Our Utimaco services are designed to **support the success of our partners**. Utimaco's goal is **not competition** for end customer business, rather it is to **complement, strengthen and support** the services provided by our partners, to the end customer.

Our services teams strive for **excellence**. Consultancy, as well as technical pre- and post-sales support our product offering and maintenance can be bought with any of our products. Utimaco also offers professional services for consulting on specific solutions and individual project implementations. The Utimaco Academy training services support our partners' business growth and competence with comprehensive training on the complex HSM products.

Consultancy

The main task of the consultancy team is to understand and help translate customer requirements into technical specifications, mapping them against existing product features and performances. Consultancy is the first point of contact for technical questions during the sales process. The consultancy team provides technical training for partners and customers.

Pre-sales consultancy and support for partners and end users

- Solution mapping – translating customer requirements into technical solutions
- Integration with technology partners and applications
- Proof-of-concept work
- Feedback about market and customer needs to Utimaco product team

Support

Maintenance can be purchased for every one of our products. With support, customers have access to

- All levels of support, including premium level support with 24/7 helpdesk, but also level 1/2/3 support
- Software updates, new software versions and patches
- Hardware repair, when part of the Service Level Agreement (SLA) for general warranty, standard or premium maintenance
- Guaranteed response times (as agreed in SLA)
- Online knowledge base
- The Utimaco (Support) Portal which contains integration guides, new release documentation, security advice, and much more

Professional Services

Utimaco also offers professional services. The main purpose is to support our partners with **solution consulting**. We give advice on how to translate customer requirements into possible technical architectures, including an estimation of man power required for implementation. To do this, our professional services engineers can draw on a wealth of experience and best practices from different industries. This can be the basis for individual **project implementations** and the development of **additional cryptographic functionality** and HSM firmware.

If you wish to develop your own products based on Utimaco HSMs, our professional services team executes the training on our Software Development Kit (SDK).

Training: Utimaco Academy

The Utimaco Academy supports the growth of our partners' business and focuses on partner enablement.

Utimaco offers training for partners to help them to obtain the skills required for selling and supporting the Utimaco CryptoServer range of products. The Utimaco Academy works closely with product management and R&D to produce high quality training material that is rich in technical information, but also easy to understand.

The training portfolio includes:

Sales training

- to acquire the general background and technical knowledge necessary to understand customer requirements, and then subsequently
- to be able to recommend the right specifications from the Utimaco product range

Technical and product training

- to acquire the Utimaco-specific knowledge necessary to advise a customer at the pre-sales stage
- to be able to carry out the installations and configurations required to set up a successful "proof of concept"
- to provide support up to an agreed level

There are also regular webinars on specific industry topics and the Utimaco product portfolio.

Utimaco SecurityServer HSM Simulator

Utimaco offers a fully functional HSM software simulator for download. The SecurityServer simulator package comes with 100% functional runtime, including all administration and configuration tools. Utimaco also includes a comprehensive library of integration and how-to guides.

Purpose of the Utimaco SecurityServer simulator

The Utimaco SecurityServer simulator facilitates **evaluation, development and integration testing** without purchase, delivery or installation of hardware. It is currently available for Windows and Linux operating systems. For R&D teams, the simulator aids in the (application) development process. Customers using the CryptoServer Software Development Kit (SDK) to develop their own HSM firmware can use the SecurityServer simulator for testing and validation. Where HSMs are integrated into existing IT infrastructure, multiple users can test their developments and corresponding interfaces on the SecurityServer simulator, without affecting production.

The SecurityServer simulator can be used to integrate the HSM with third party applications that provide standardized cryptographic APIs (PKCS#11, CSP/CNG/SQLEKM or JCE). For these types of plug & play deployments, the SecurityServer simulator can be used for evaluation of different configuration options, application settings, as well as load-balancing or high-availability scenarios.

Overall, the SecurityServer simulator enables you to try out all the SecurityServer features for efficient evaluation, development and integration. It is the simplest and most cost-effictive solution to get started with a Hardware Security Module!

How to get started?

To download the Utimaco SecurityServer simulator, a registration process is required in accordance with international export regulations.

Registration is done on the Utimaco Portal
https://support.hsm.utimaco.com

Ready to take off?
Download our HSM simulator!

Register for free on
https://support.hsm.utimaco.com

or find more information on
https://hsm.utimaco.com/downloads/utimaco-portal/hsm-simulator

Contact
hsm@utimaco.com
hsm.utimaco.com

EMEA
Utimaco IS GmbH – Headquarters
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696 200

Americas
Utimaco Inc.
910 E Hamilton Ave., Suite 150
Campbell, CA 95008, USA
Phone +1 844 UTIMACO

APAC
Utimaco IS GmbH – Office APAC
One Raffles Quay, North Tower, Level 25
Singapore 048583
Phone +65 6622 5347