Sicherheit durch Kooperation
Thomas Krenn und Utimaco Hardware-Sicherheitsmodule sorgen für digitalen Schutz- Aber wie?

THOMAS KRENN®

utimaco®

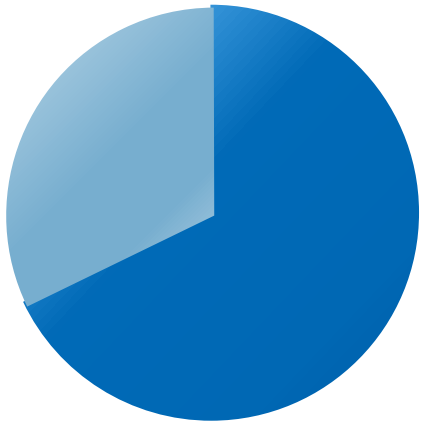
Agenda

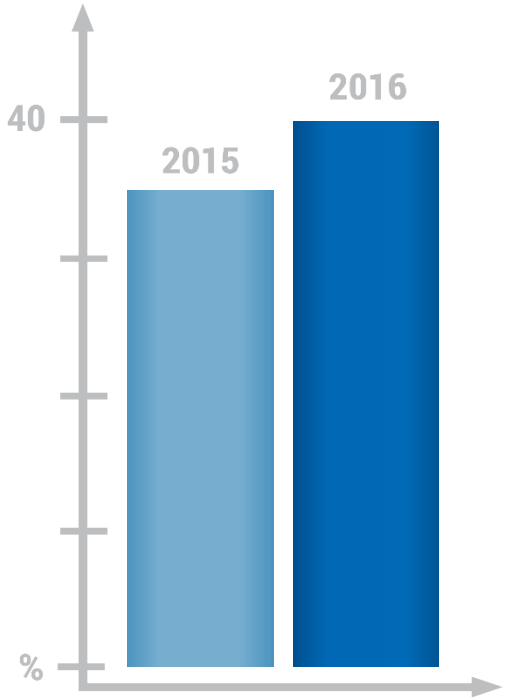
- Über die Utimaco GmbH
- Was ist ein Hardware Security Modul (HSM)?
- Use Cases für Hardware Security Module
- Warum ist Hardware-Verschlüsselung ein Wachstumsmarkt?
- Über die Kooperation zwischen Utimaco und Thomas-Krenn
- Getestete HSM-Appliances von Thomas-Krenn

Utimaco: Facts and Figures

170+ Employees

70% in R&D, Support and Production





€ 40 Million
Revenue

5000+ Installations in more than 80 countries

Fastest growing HSM vendor worldwide

Aachen, Germany
Headquarters

What is an HSM ?

A Hardware Security Module (HSM) is a **secure crypto processor** with the main purpose of managing cryptographic keys and offer accelerated cryptographic operations using such keys.

A Hardware Security Module is:

- A purpose built, physical computing device
- Generating cryptographic keys
- Managing cryptographic keys
- Secure storage of cryptographic keys
- Hardware designed to detect attack and respond by deleting keys
- Providing excellent tamper resistance
- Hardware device (as opposed to software service) enforces Separation of Duties away from Admin/System/Ops/IT personnel to dedicated Security team

How do they work?

- HSMs perform functions for applications:

  Key generation, encryption and decryption, signing, hashing……

- Application Server sends instruction to HSM to process data using specific key that never leaves HSM

- Application integrated with HSM via client API running on server – crypto function calls/instructions forwarded by client to HSM for execution

- 3 main Crypto APIs – libraries of functions for programming language used by application:

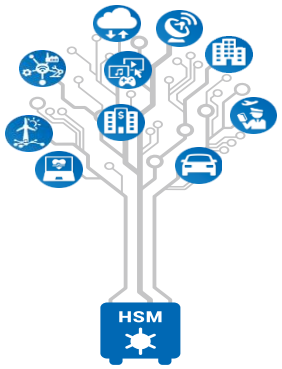
  PKCS#11 (C), Microsoft (CSP/CNG), Java/JCE

Supported Operating Systems

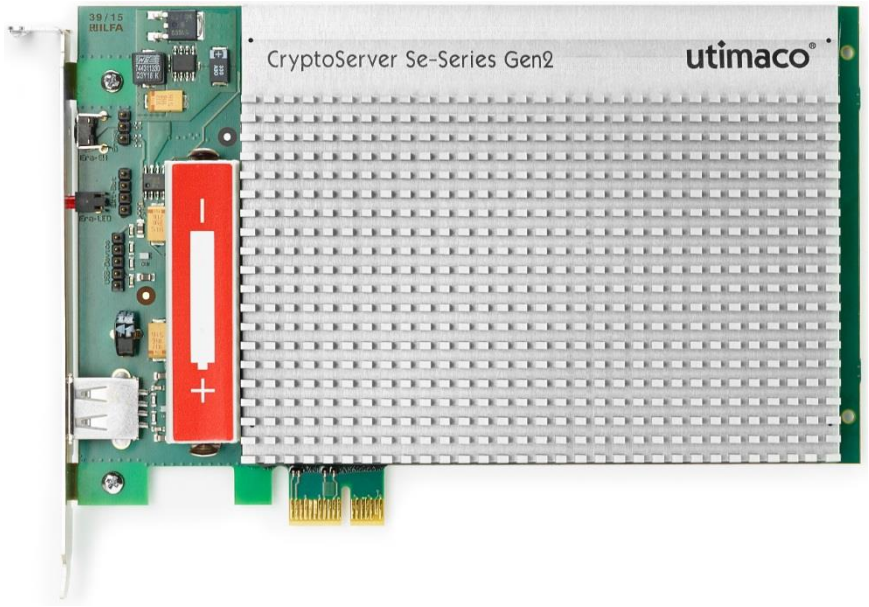
- Microsoft Windows
- Linux

Cryptography

- Asymmetric: RSA, DSA, Diffie-Hellmann, Elliptic Curve (ECDSA, ECDH, ECIES), with named Brainpool and NIST curves.
- Symmetric: AES, DES, Triple DES, Retail MAC
- Hash algorithms: SHA-1, SHA-2 family, RIPEMD-160



Utimaco HSM Se Gen 2 series



- FIPS 140-2 Level 3 (CC EAL 4+ in progress)
- Epoxy Bonding
- Sensitive to changes in:
  - Voltage
  - Temperature
- Designed for general high security

Performance Level

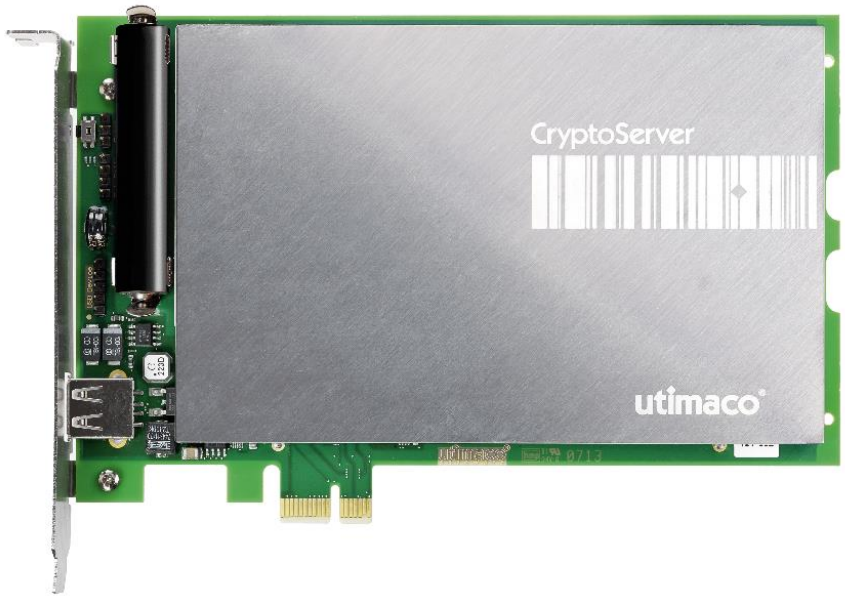
- Available as LAN Appliance or PCIe Card

- 4 x Performance Levels (licence-controlled):

Se 12	(16 signings/sec	- RSA 2048)
Se 52	(85 signings/sec	- RSA 2048)
Se 500	(2200 signings/sec	- RSA 2048)
Se 1500	(3400 signings/sec	- RSA 2048)

Hardware asymmetric crypto accelerator

Utimaco HSM CSe-series



- FIPS 140-2 Level 4 (physical), overall Level 3
- Foil Sensor
- Sensitive to changes in:
  - Voltage
  - Temperature
  - Pressure and Chemical attack
  - Physical attack (drilling, machining etc)
- Designed for installations where maximum security is essential

Performance Level

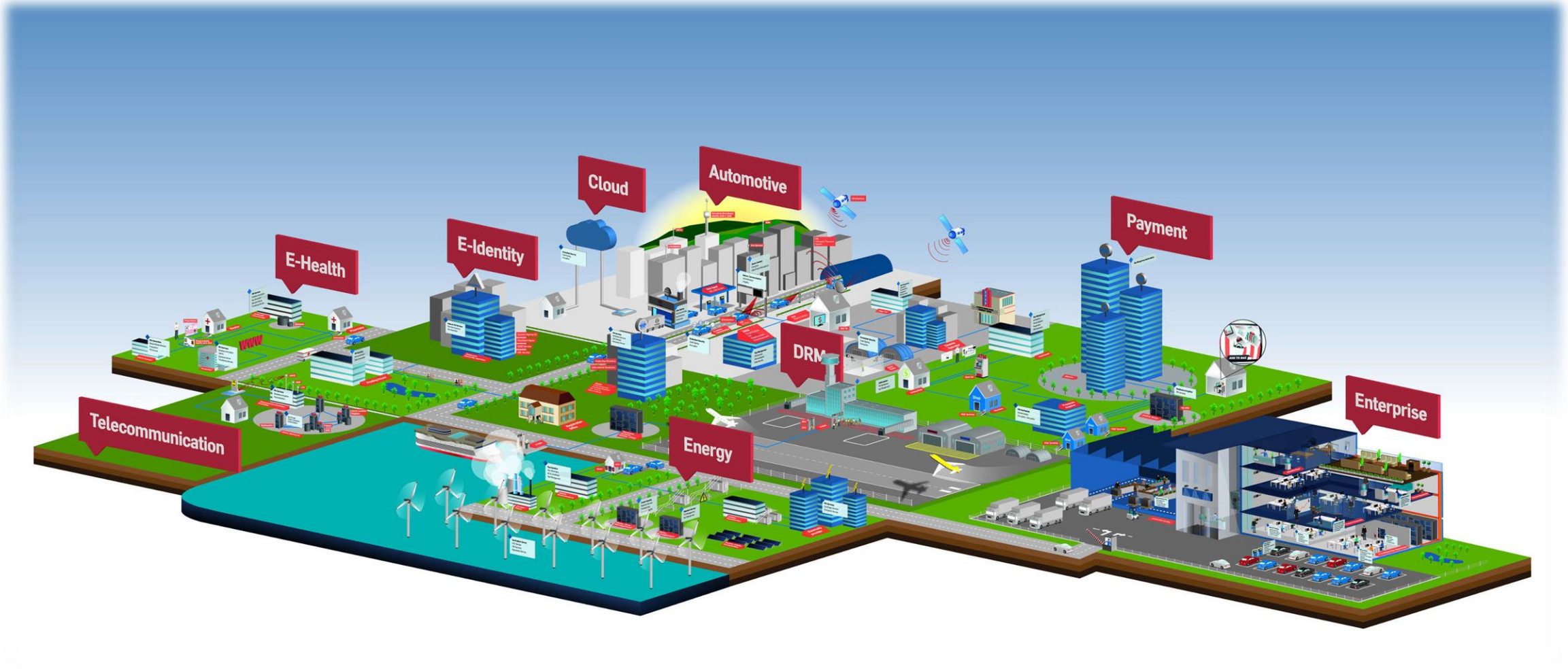
- Available as LAN Appliance or PCIe Card

- 2 x Performance Levels (licence-controlled):

  CSe 10 (17 signings/sec - RSA 2048)

  CSe 100 (100 signings/sec - RSA 2048)

Use Cases


Cloud
Automotive
E-Health
E-Identity
Payment
DRM
Telecommunication
Energy
Enterprise

Uses Cases

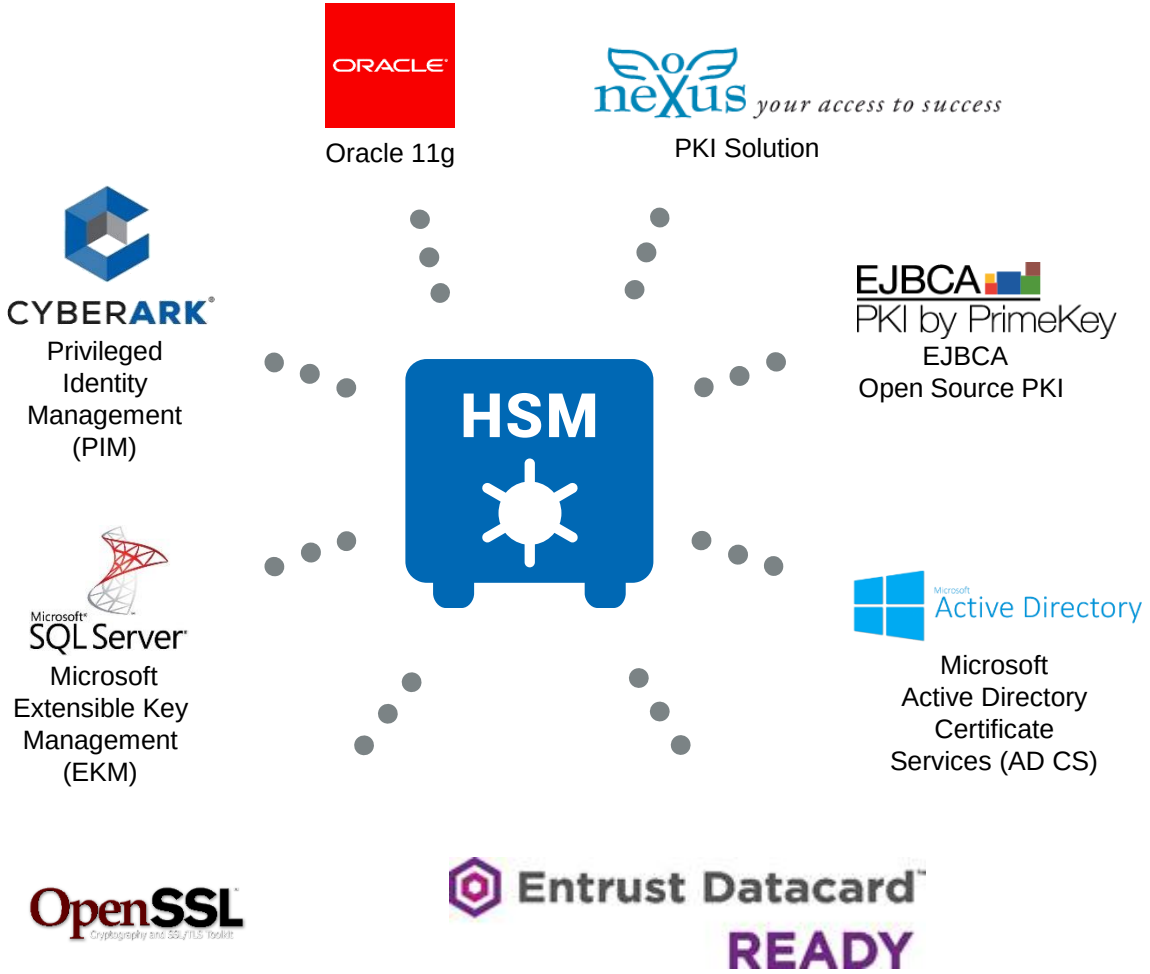
The Route Of Trust Of Different Use Cases

- Electronic Payment
  - PIN generation, card personalization, database encryption
- eID
  - Key Generation, Passport issuing + verification, Driver license
- Telco Networks
  - Home Location Register, verification of devices
- Smart Metering
  - Code Signing of smart meter, preventing manipulation
- Digital Rights Management (Pay-TV)
  - Code signing, key generation, key management,
- Timestamp Solutions (Lottery, Gaming, workflow approvals)
  - Ensuring that no games or lottery times were manipulated
- Automotive
  - „Car2X“ communication
  - Anti-theft device
- Road Toll Systems
  - In Germany, Belgium, Czech Republic, Singapore
- M2M

Application Use Cases

- HSM holds PKI Root Key to sign Certificates for IDs – Police, Healthcare, Students, Banks
- HSM holds key to secure website for SSL and protect purchaser's data used for ecommerce
- HSM holds key to secure retail database of customer details (Credit Card Numbers)
- HSM holds key to sign official documents to provide legal validity , (Land Registry title deeds)
- HSM holds key to timestamp lottery tickets
- HSM holds key to generate crypto material on ID Cards, ePassports, Credit Cards, SIM Cards
- HSM used in Manufacturing to generate crypto material on Smart Meters, Tachographs, TV decoders
- HSM holds key to sign code running in Cars to identify for servicing and prevent running rogue code

Selected integrations



Warum ist HW-Verschlüsselung ein Wachstumsmarkt?

The Future (almost here!)

- “Internet of Things” – connected devices having an identity
- “Smart Buildings”
- “Smart Cities” “Smart Grid”
- Fridges, Heating Systems, Security Systems, Advertising, Cameras ……..
- ID defined by crypto material (e.g. Certificate) generated on HSM by secure Key
- Vital for Driverless Cars; M2M communication…
- Sensitive Data should be protected using Cryptography and **Securing the Key**
- Regulations over holding of data often now mandate security (e.g. GDPR)

What is new with GDPR Europäische Datenschutzgrundverordnung

utimaco®

…and relevant to most businesses?

Supervisory Authority
Data protection regulators on national level

Need to inform of breach within 72h
(Article 33)
to Supervisory Authority;
in severe cases also to persons concerned **(Recital 75)**

Tough Penalties
Fines up to **4%** of annual global revenue

Or
20 Mio €

Cloud

Processor
Person (legal entity or individual) that processes personal data on behalf of the controller

Data subjects have **the right to be forgotten** and erased from the record**

Personal Data (PII)*
- NOT sensitive data
- Personal Data

Controller
Person (legal entity or individual) that determines the purpose and the means of the processing of personal data (collects data)

Data Protection Officer (DPO)
Advises & monitors GDPR privacy law/policy compliance; DPO contact details must be published

* Excludes “sensitive” information: on religion, sexual orientation, criminal records, „racial origin“, „electoral activity“, personal information of children
** Data subjects have the right not to be part of automatic decision making based on personal information, e.g. for credit applications or e-recruiting practices (Recital 71)

Security of processing

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

Security of processing

- “In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as *encryption*.” (recital 83)

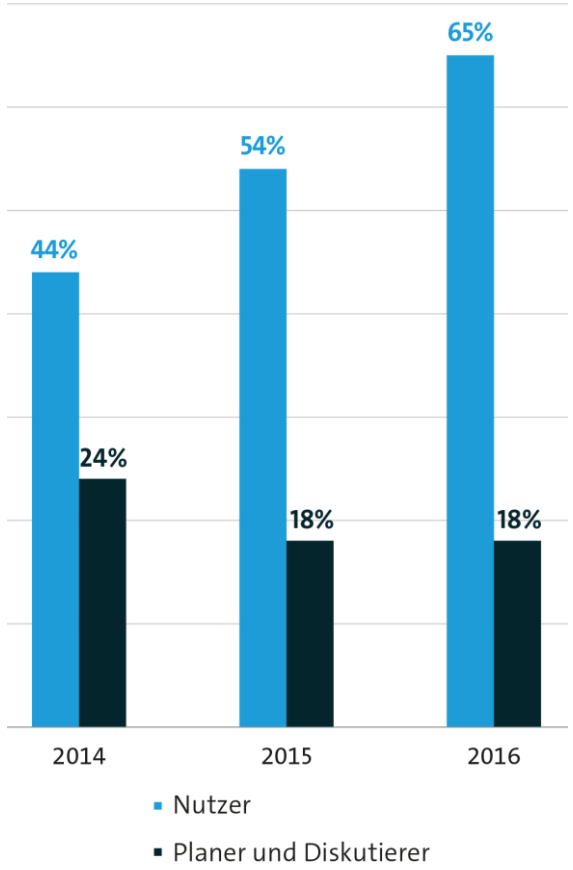
- The *communication* to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
  - (a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as *encryption*; (Article 2, § 1a)

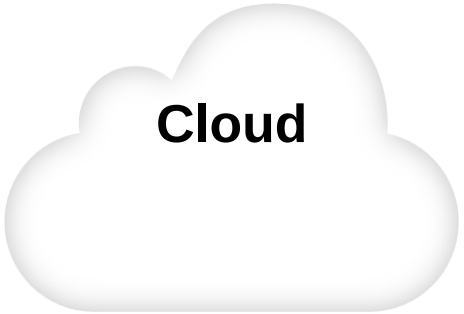
- ‘pseudonymisation’ means the processing of personal data in such a manner that
  - the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such ***additional information*** is ***kept separately*** and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Warum ist HW-Verschlüsselung ein Wachstumsmarkt?

CLOUD

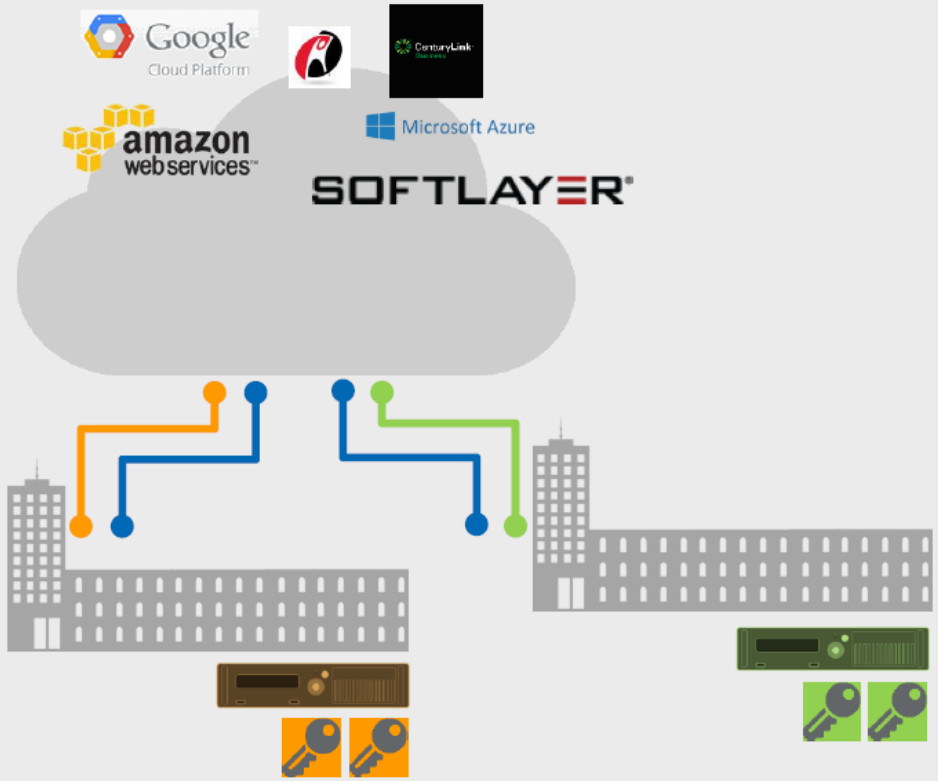
- BitKom/KPMG: 65%





Hardware Security in Cloud Scenarios

utimaco®



Colocation

HSM on site, with a link to the cloud application

Pros:

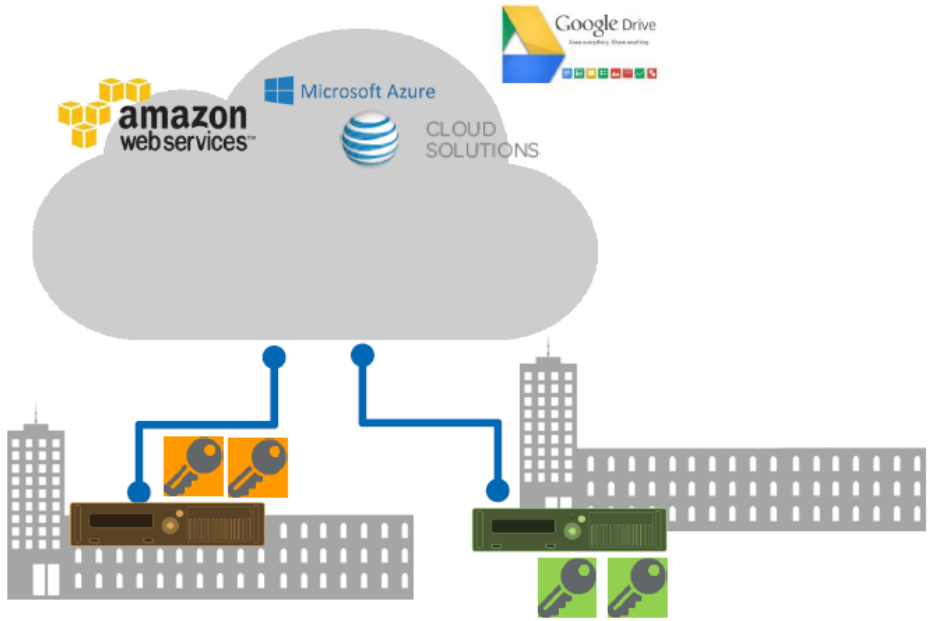
- Never give up key sovereignty
- Clear separation of duty

Cons:

- Security administration needed
- Business critical application hard to implement

Hardware Security in Cloud Scenarios

utimaco®



Cloud Gateway

HSM are part of gateway appliances

Pros:

- Secure key storage
- Maximum privacy
- Integrated key management

Cons:

- Additional hardware management
- HSM integration into gateway solution
- Administration

Kooperation Thomas Krenn AG – Utimaco

Zielsetzung

- Zielsetzung war es, gemeinsam mit der Thomas Krenn AG unseren Partnern und Kunden eine mit Utimaco Hardware Security Modulen integrierte und getestete Gesamtlösung als „Thomas Krenn Security Appilances“ mit einem einheitlichen Support- und Service Konzept anzubieten.

Visit our new website www.hsm.utimaco.com
Register for HSM Simulator https://support.hsm.utimaco.com/hsm-simulator

Thanks for your attention!

Stephan Otten

Head Of Sales EMEA
stephan.otten@utimaco.com

Utimaco IS GmbH

Germanusstr. 4
52080 Aachen
Germany
Tel +49 241 1696 200
Fax +49 241 1696 199
Email hsm@utimaco.com

Utimaco Inc.

Suite 150
910 E Hamilton Ave
Campbell, CA 95008
United States of America
Tel +1 844 884 6226
Email hsm@utimaco.com

Sicherheit durch Kooperation Thomas-Krenn und Utimaco Hardware-Sicherheitsmodule sorgen für digitalen Schutz – Aber wie?

Michael Haderer

08.11.2017

AGENDA

1. Problemstellung

2. Lösung: Getestete Server in zweierlei Ausbaustufen

3. Fragen

Problemstellung

THOMAS KRENN®

Die HSM Module von Utimaco sind als PCIe Karten per default mit gängigen Mainboards und Systemen kompatibel. Die Herausforderung besteht aber vielmehr darin, die Komponente sowohl thermisch in ein getestetes System zu integrieren, als auch sicherzustellen, dass mit gängigen OS Versionen entsprechende Treiberkonflikte vermieden werden.

redhat

debian
GNU/Linux

SUSE

Windows Server

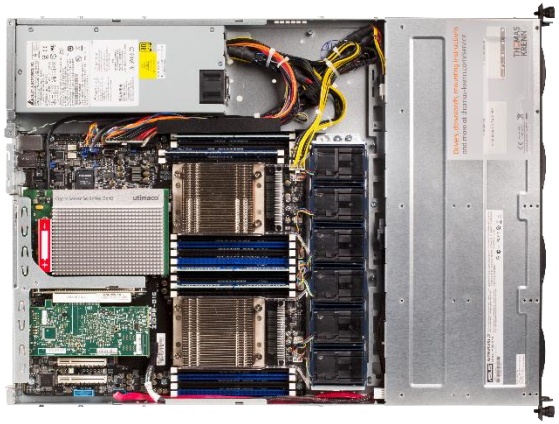
AGENDA

THOMAS KRENN®

1. Problemstellung
2. Lösung: Getestete Server in zweierlei Ausbaustufen
3. Fragen

Lösung

Server in zweierlei Ausbaustufen



1HE Intel Dual-CPU RI2104-HSM

1HE Intel Single-CPU RI1104H-HSM

Live Shop Konfiguratoren

https://www.thomas-krenn.com/de/produkte/appliances/security-appliance.html

Tests mit verschiedenen Betriebssystemen

Microsoft	Linux
Windows Server 2012 R2	Suse Linux Enterprise Server SP4
Windows Server 2016	Red Hat Enterprise Linux 7.2
Windows 8.1	Debian 8.7.1

Fragen?

Kontakt:

Thomas-Krenn.AG
Michael Haderer
Project Development
Speltenbach-Steinäcker 1
94078 Freyung
T +49 (0) 8551 9150 355
M +49 (0) 171 29 79 376
mhaderer@thomas-krenn.com

Vielen Dank
für Ihre Aufmerksamkeit!