Utimaco HSM
Introduction
JIPDEC Seminar June 2017

Joerg Horn
Director Business Development

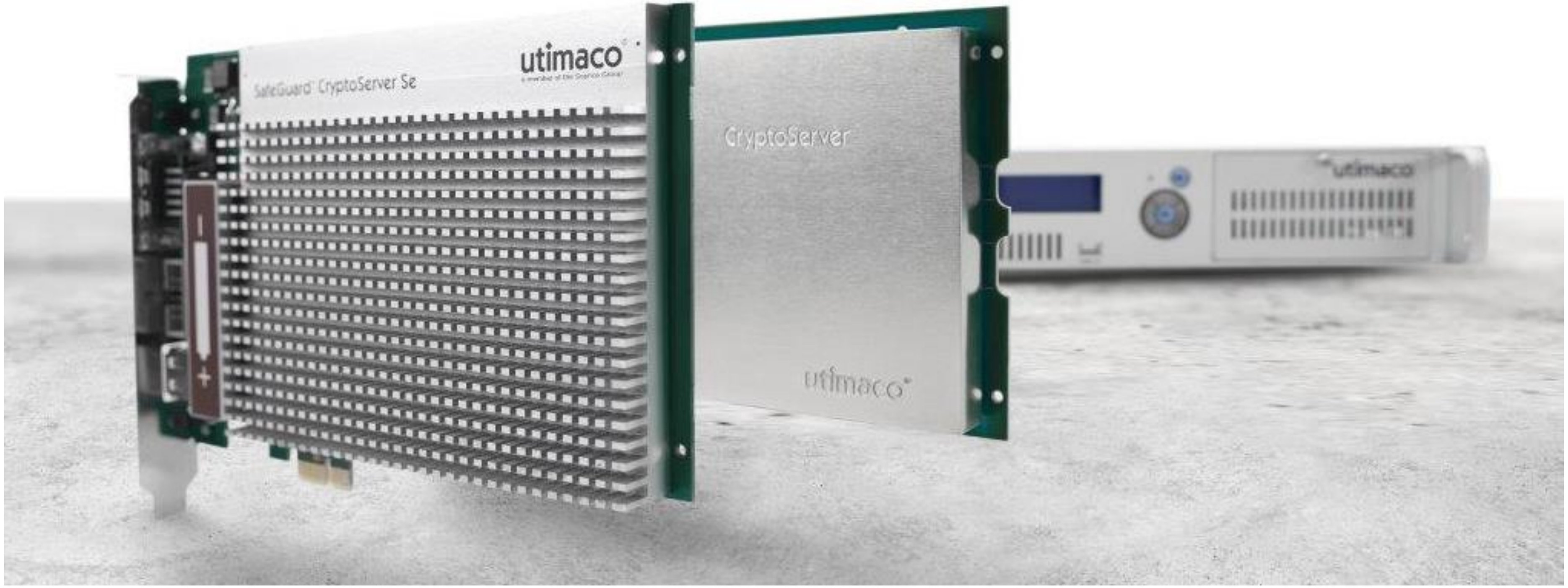
utimaco®

- Part 1
  - Introduction
    - Utimaco
    - History
    - HSM
    - HSM Produkt Portfolio
- Part 2
  - eIDAS
  - Signature Creation
  - TimeStamping
  - Outlook

- About Utimaco

Utimaco Hardware Security Modules

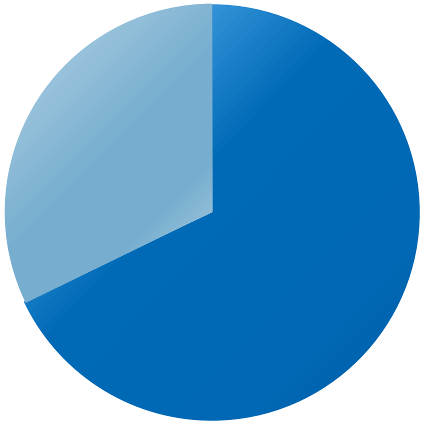
- precision engineering for your security needs

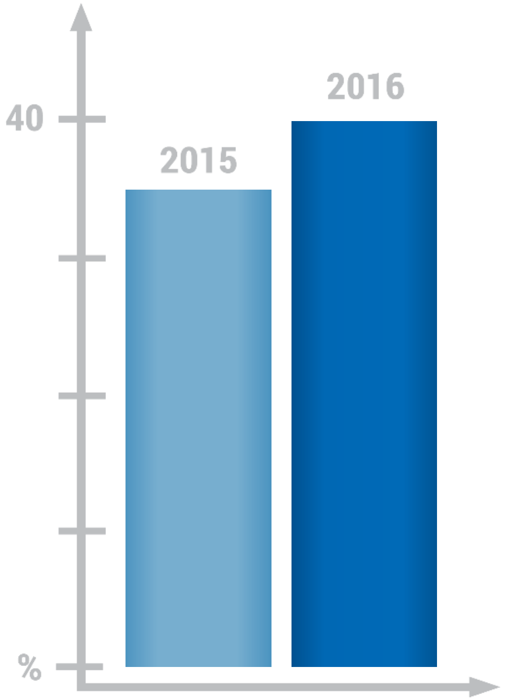


Utimaco: Facts and Figures

170+ Employees

70% in R&D, Support and Production





~ € 40 Million

Revenue

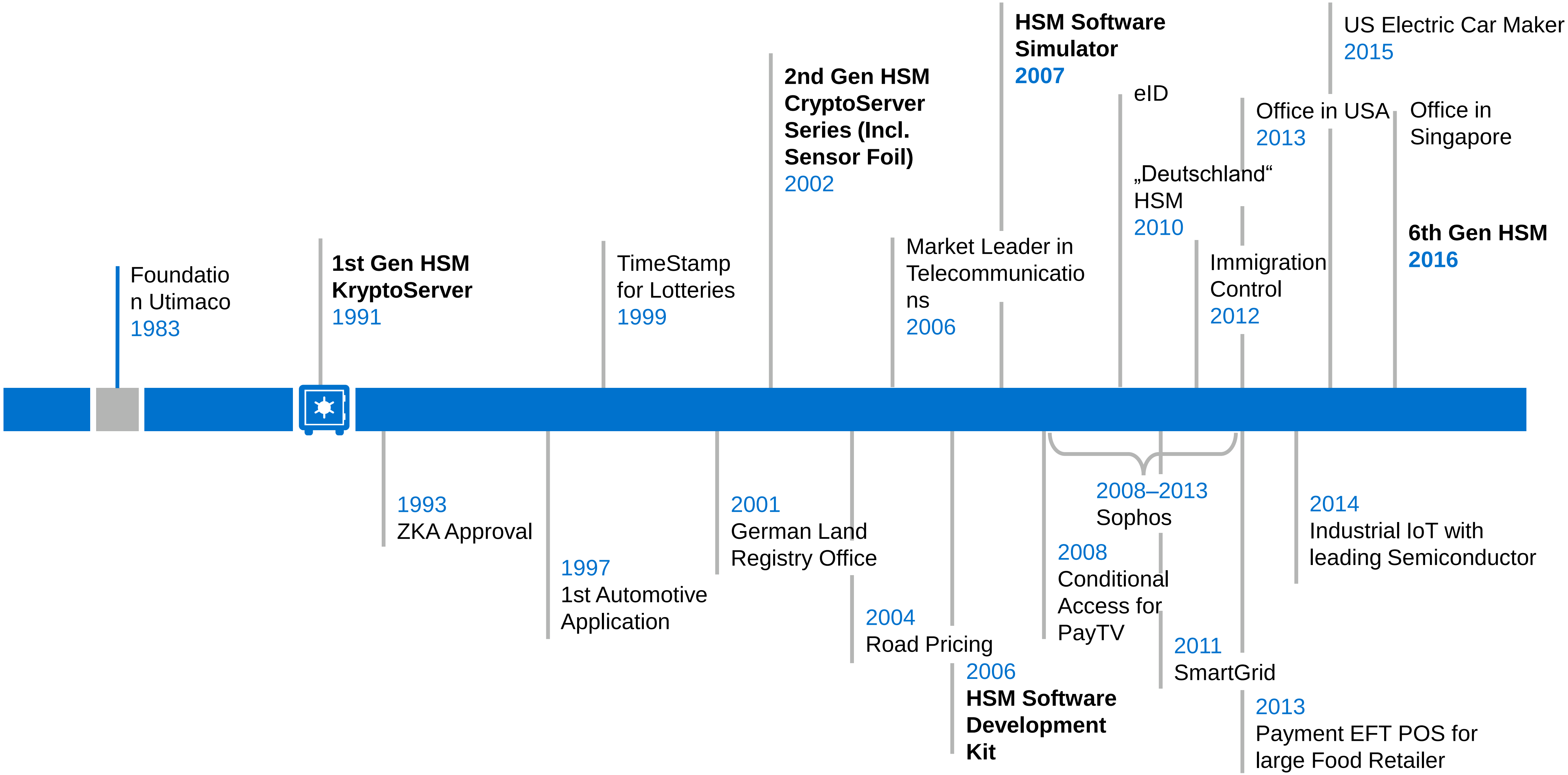
1.000+ Installations

Fastest growing independent HSM vendor worldwide

Aachen, Germany

Headquarters

Utimaco: 25 years of experience in IoT security



Foundation Utimaco
1983

1st Gen HSM KryptoServer
1991

1993
ZKA Approval

1997
1st Automotive Application

TimeStamp for Lotteries
1999

2001
German Land Registry Office

2nd Gen HSM CryptoServer Series (Incl. Sensor Foil)
2002

2004
Road Pricing

Market Leader in Telecommunications
2006

2006
HSM Software Development Kit

HSM Software Simulator
2007

2008–2013
Sophos

2008
Conditional Access for PayTV

eID

„Deutschland“ HSM
2010

2011
SmartGrid

Immigration Control
2012

Office in USA
2013

2013
Payment EFT POS for large Food Retailer

2014
Industrial IoT with leading Semiconductor

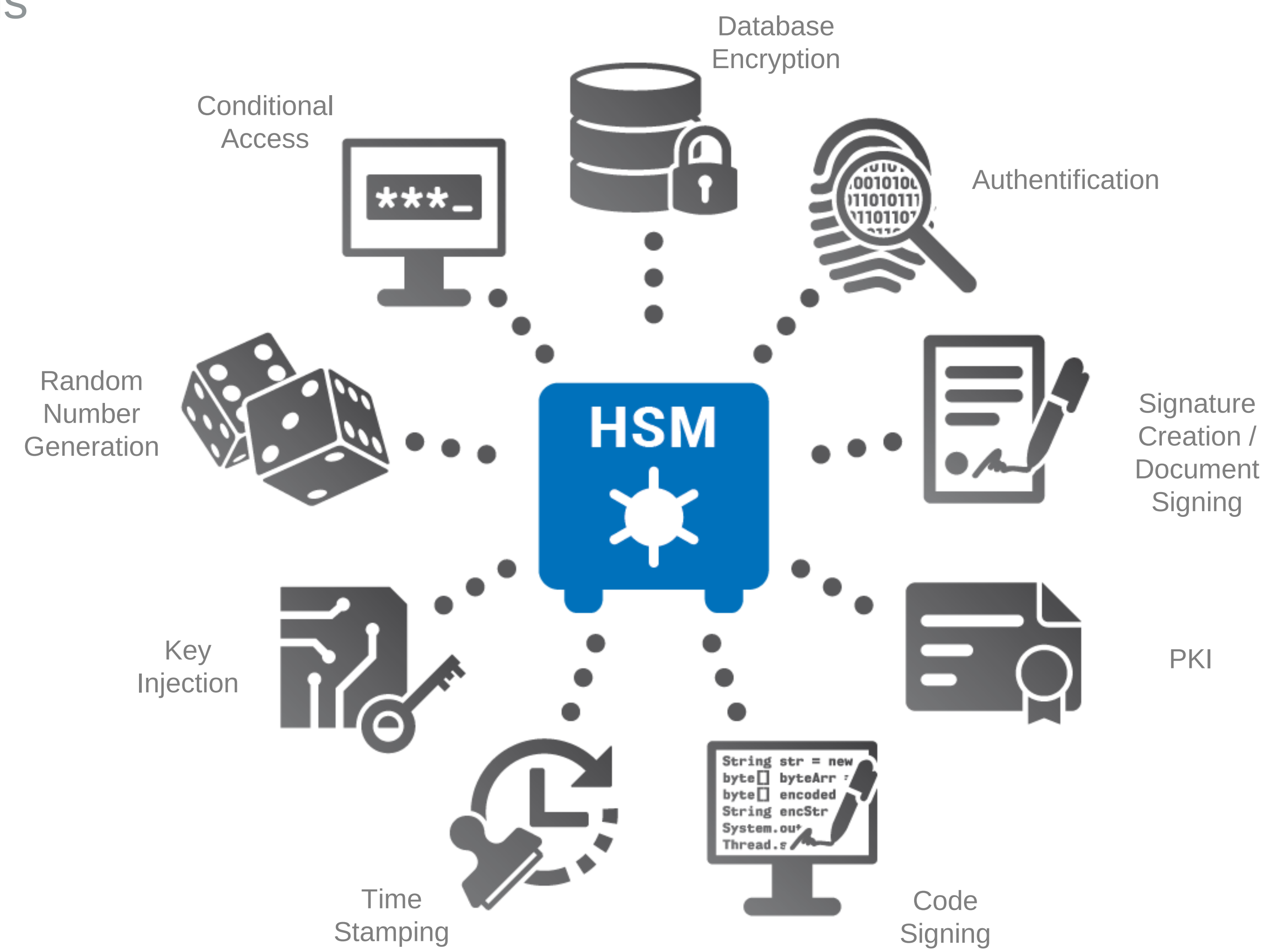
US Electric Car Maker
2015

Office in Singapore

6th Gen HSM
2016

- About HSM

HSM applications



Database Encryption

Conditional Access

Authentification

Random Number Generation

Signature Creation / Document Signing

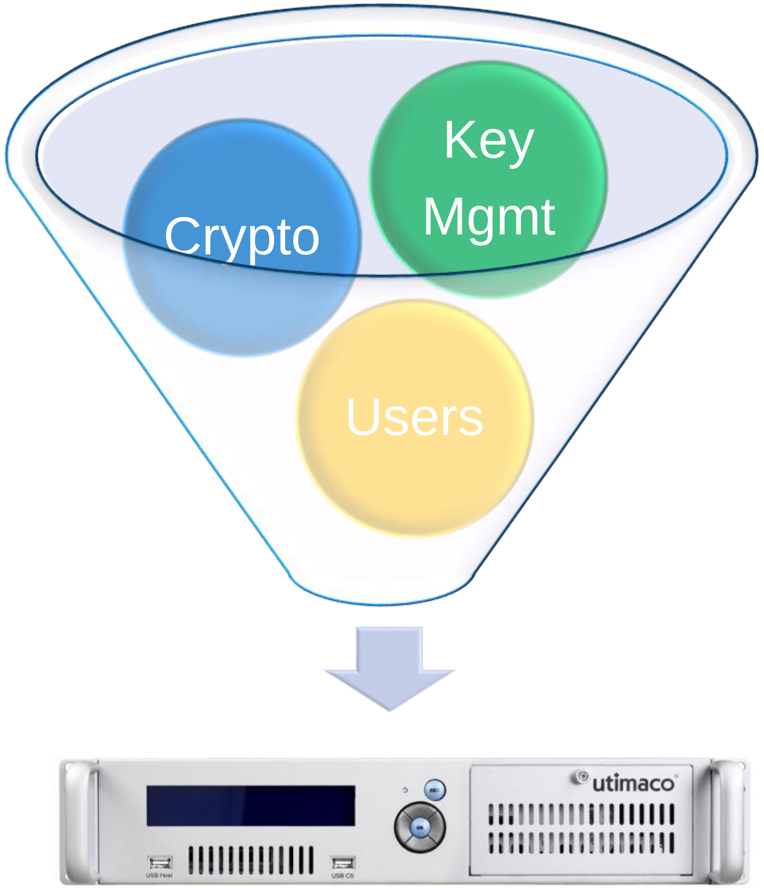
Key Injection

PKI

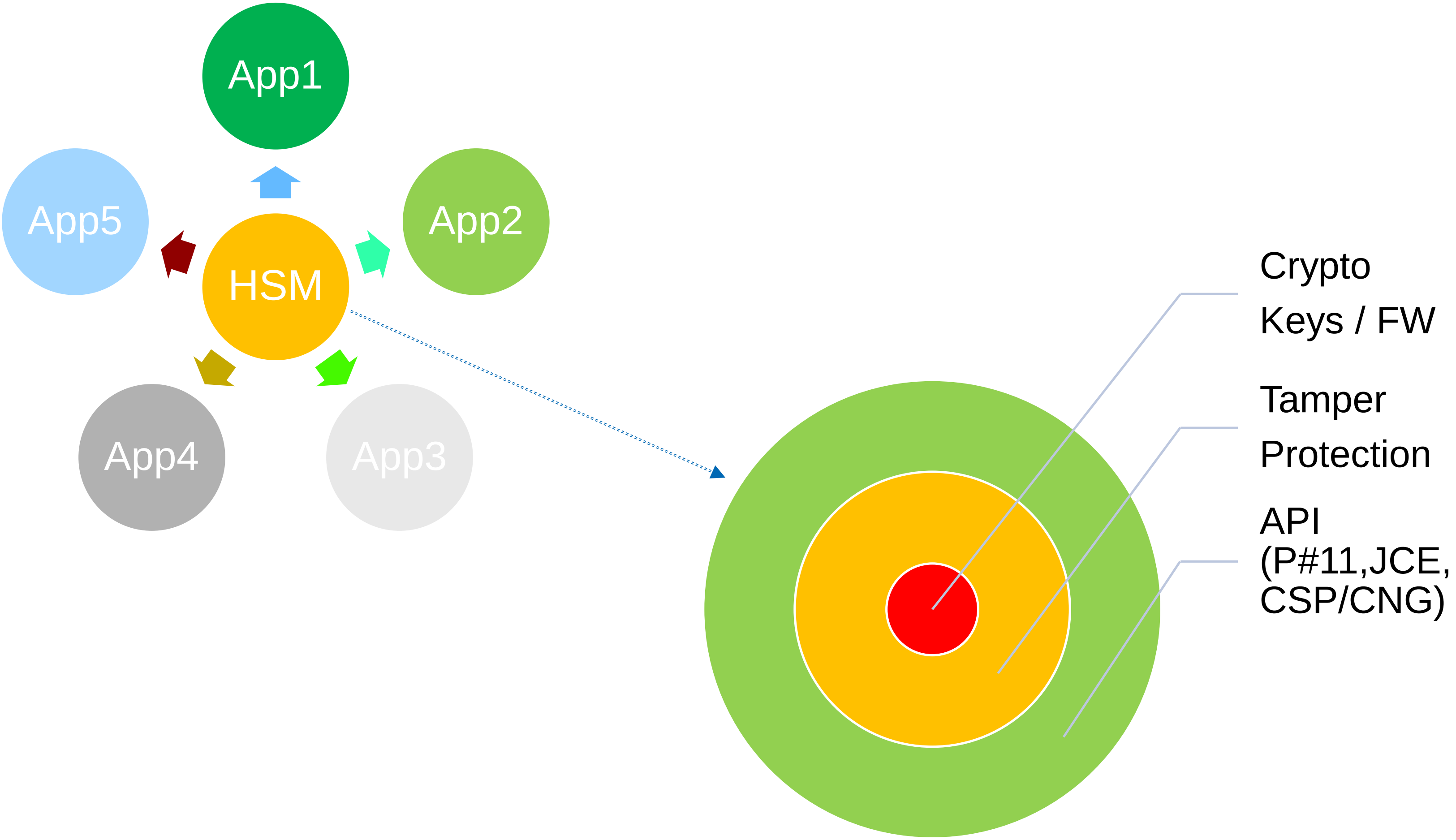
Time Stamping

Code Signing

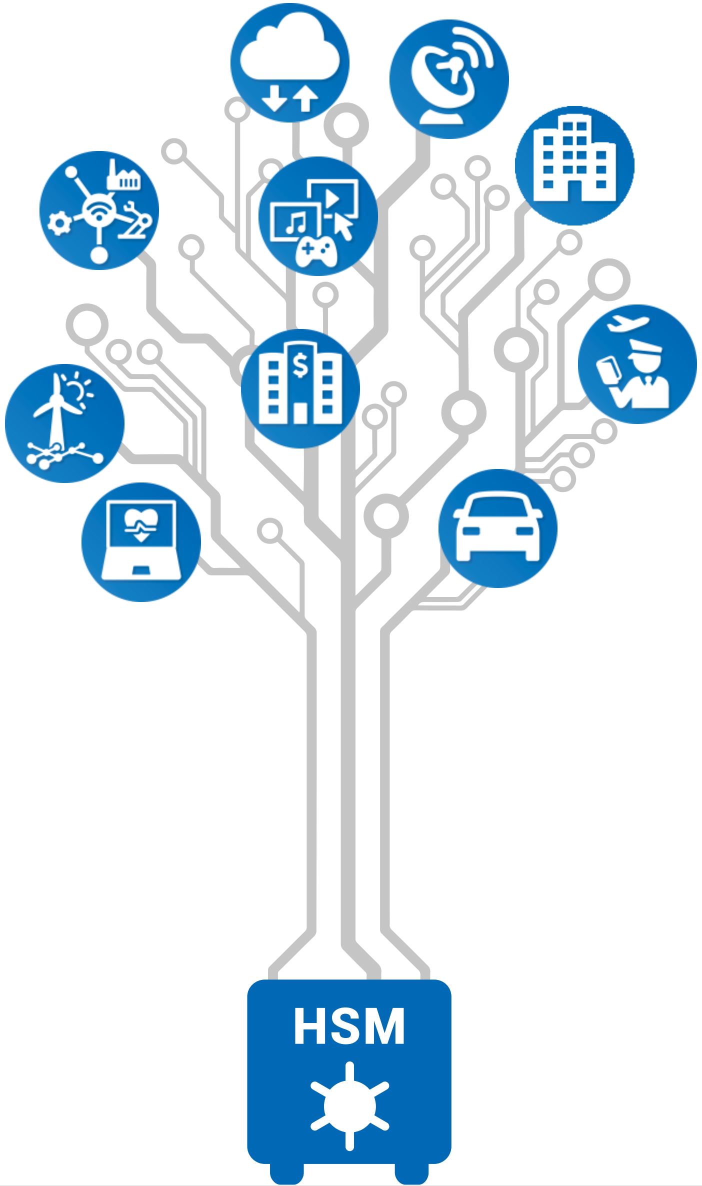
Offload sensitive data operations from Apps to an HSM.



Trustworthy Cryptographical Resource



Utimaco: The Root of Trust

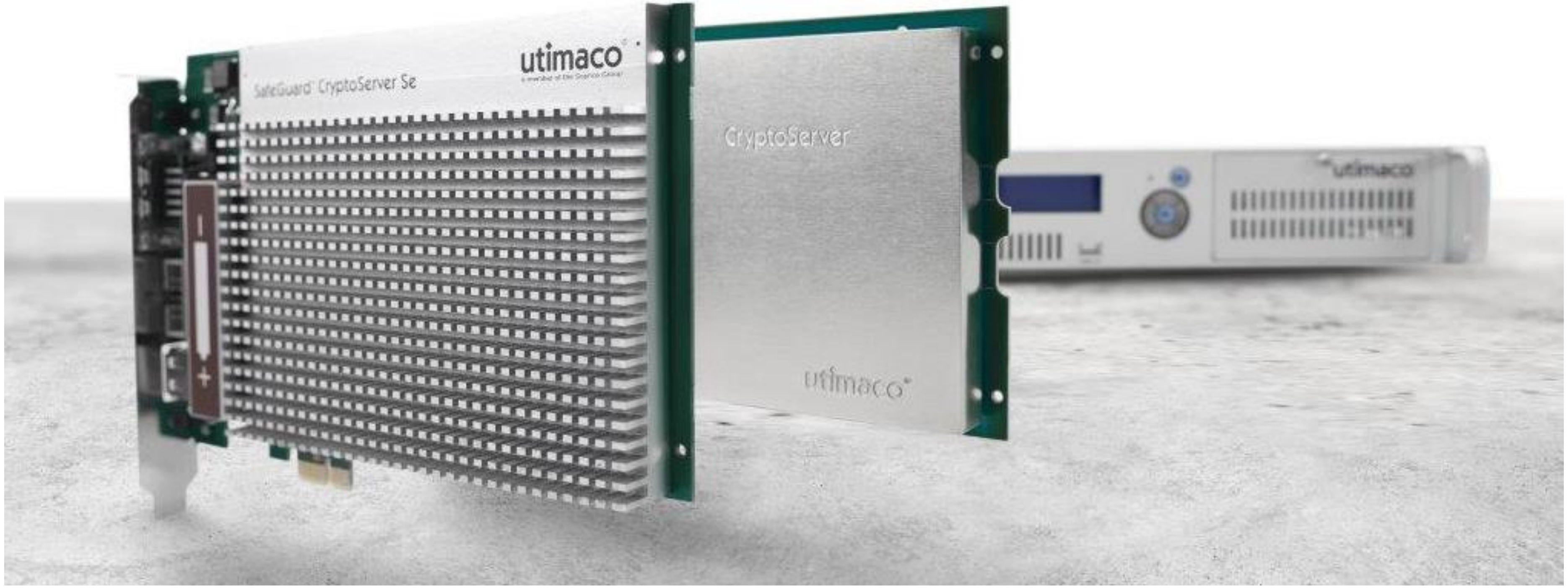


We keep your cryptographic keys safe

- Product Portfolio

Utimaco Hardware Security Modules

- precision engineering for your security needs



Product Portfolio: CryptoServer

Hardware Security Modules

	Se-Series 12/52/500/1500		CSe-Series 10/100	
Physical Interface	PCIe plug-in card	Network attached	PCIe plug-in card	Network attached
Certifications (* in progress)	**FIPS 140-2 Level 3,** **CC EAL4+*** Based on CEN PP EN 419 221-5 „Cryptographic Module for Trust Services“		**FIPS 140-2 L3 Phys.Sec. L4,** **PCI HSM* (PCI PTS).** CC Attack Potential “High”, Deutsche Kreditwirtschaft	
Cryptographic Support	(T)DES, AES, RSA, (EC)DSA, (EC)DH, SHA, …			
OS	WIN / LINUX / AIX* (*Appliance only)			

Product Portfolio - Product Packages

Se-Series
12/52/500/1500

CSe-Series
10/100

SecurityServer (General Purpose HSM)	PKCS#11, JCE, MS CSP/CNG/SQL EKM, CXI
CryptoServer SDK / CryptoScript *	Development Kit for CryptoServer Firmware Customization
TimestampServer	Signature Creation acc. RFC 3161, CTS API
More..	Free HSM Software Simulator (Win/Linux), PCI HSM /Payment Program (Free EFT POS API)

HSM market drivers

- Critical Infrastructure (backbone of a nation's economy, security, and health)
  - Energy/Smart Grid
  - Industry/IOT
  - Government PKIs and application (ID cards, passport, health system,.)
  - Finance
  - Transportation
  - Health System
- Secure Cloud Services
  - Cryptographical services for all cloud architectures
- GDPR
  - General Data Protection Regulation (EU) 2016/679. Applies from May 2018
- eIDAS
  - EU Regulation on electronic identification and trust services, since July 2016

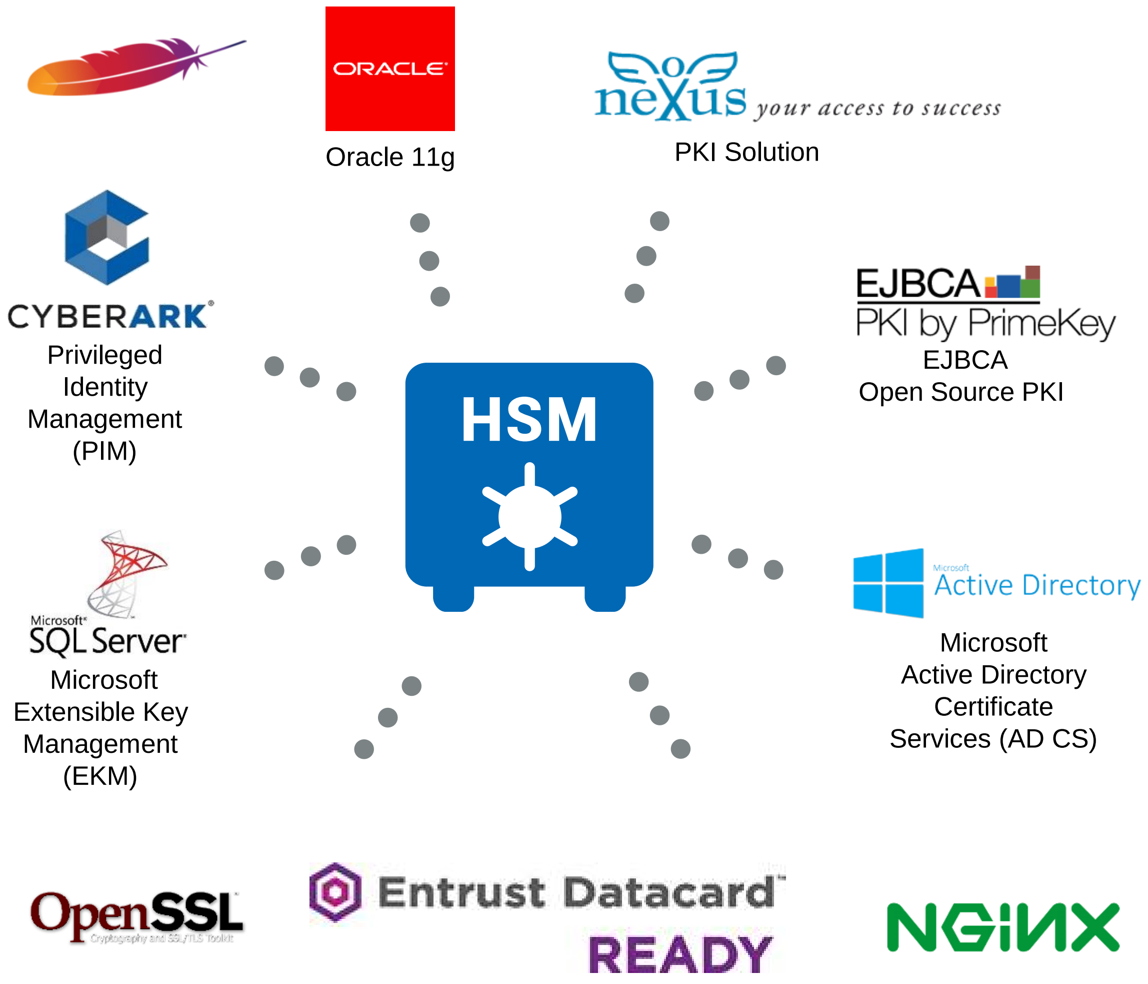
Unique Benefits

- Unmatched capacity/scalability
  - Internal and external key storage
  - Virtually unlimited #slots (partitions)
  - High performance
- Lowest TCO
  - Fixed-price policy, no hidden costs
  - no extra charges
    - for algorithms (ECC etc), clients/hosts/tenants/ partitions/ connections
  - Best price/performance ratio
- Easy-to-use remote mgmt.
  - No additional cost
  - Backup of FW and user/key DB to disk
  - FW update preserves keys
- Full-functionality HSM simulator
  - Cryptography, mgmt., logs, SDK, …
  - Testing, training, integrations, …
  - Rapid product evaluations
- Highly configurable
  - Configurable role-based access
  - Extended authentication (2FA, M:N)
  - Configurable hardening of crypto providers
- Best-in-class SDK
  - Virtually unlimited number of FW modules
  - Script or C based SDK

Utimaco

utimaco®

Selected integrations


ORACLE
nexus your access to success
CYBERARK
EJBCA PKI by PrimeKey
HSM
Microsoft SQL Server
Microsoft Active Directory
OpenSSL Cryptography and SSL/TLS Toolkit
Entrust Datacard READY
NGINX

Oracle 11g

PKI Solution

Privileged Identity Management (PIM)

EJBCA
Open Source PKI

Microsoft Extensible Key Management (EKM)

Microsoft Active Directory Certificate Services (AD CS)