Portfolio Overview for Payment & GP HSMs

Malte Pollmann, CEO
Priyank Kumar, Product Management, Payment HSMs
Dieter Bong, Product Management, General Purpose HSMs
Utimaco is a worldwide leader in highly specialized Cyber Security markets

- Deep expertise in providing security for Critical Infrastructures
- Our Global Market Leading Position

1.000+ Utimaco HSM protected infrastructures worldwide
300+ Telecom and ISP networks worldwide protected by Utimaco

Headquarters: Aachen, Germany & Campbell (CA), USA
Worldwide offices and global partner landscape

>220 highly skilled experts
>50 years in IT and >35 years in IT-Security

#1 in Telecom Compliance Solutions

#2 in Hardware Security Modules
Utimaco Vision & Mission

Providing Security creates Trust

Vision
The leading global provider of critical data security, identity and threat detection technologies

Mission
“Utimaco: Providing Security creates Trust”
Trusted to protect the most critical infrastructures and organizations against the most critical threats

Information Security

Hardware Security Modules
Key Management
Data Protection

Telecom Compliance

LI Mediation

Hardware Security Modules
- Mastercard
- Visa
- FIS
- JPMorgan Chase & Co.
- Entrust Datacard
- Fiserv
- Diebold Nixdorf
- Swedbank
- NTT Data

Key Management
- Deloitte
- 3M
- Philips
- Intel
- Visa
- Nokia
- The Home Depot
- Bank-Verlag
- Secunet

Data Protection
- Bundesamt für Sicherheit in der Informationstechnik
- Cisco
- Huawei
- Noki
- Swisscom
- Vodafone
- NBN
- Deutsche Telekom
Utimaco: 35+ Years of Experience in IT Security

1964 Formation of IT company
1973 Foundation Utimaco (IT security)
1987 Tandem Computers Inc. acquires Atalla Corporation
   "1500 customers, numerous patents"
1991 1st Gen HSM KryptoServer
1993 ZKA Approval
1997 1st Automotive Application
1999 TimeStamp for Lotteries
2002 2nd Gen HSM CryptoServer Series (Incl. Sensor Foil)
2005 Hewlett Packard (HP) acquires Compaq Computers
2006 HSM Software Simulator
2007 HSM Software Development Kit
2008-2013 Sophos
2009 "85% of all ATM transactions worldwide are secured by Atalla Box"
2010 "Deutschland" HSM
2013 Payment EFT POS for large Food Retailer
2014 Industrial IoT with leading Semiconductor
2015 Hewlett Packard splits: HP Inc. for PCs/Printers
   And HPE for B2B business
2016 Office in USA
2017 Office in Singapore
2018 Bank-Verlag: signature activation module (SAM) for banks
2018 MicroFocus acquires HPE's Software business (incl. Atalla)
2018 MicroFocus acquires HPE's Software business (incl. Atalla)

2018 Utimaco acquires Atalla Business

Atalla Corporation founded by John Atalla
   the "Father of the PIN" (1924-2009)
1973
1987 Tandem Computers Inc. acquires Atalla Corporation
   "1500 customers, numerous patents"
1991 1st Gen HSM KryptoServer
1993 ZKA Approval
1997 1st Automotive Application
1999 TimeStamp for Lotteries
2002 2nd Gen HSM CryptoServer Series (Incl. Sensor Foil)
2005 Hewlett Packard (HP) acquires Compaq Computers
2006 HSM Software Simulator
2007 HSM Software Development Kit
2008-2013 Sophos
2009 "85% of all ATM transactions worldwide are secured by Atalla Box"
2010 "Deutschland" HSM
2013 Payment EFT POS for large Food Retailer
2014 Industrial IoT with leading Semiconductor
2015 Hewlett Packard splits: HP Inc. for PCs/Printers
   And HPE for B2B business
2016 Office in USA
2017 Office in Singapore
2018 Bank-Verlag: signature activation module (SAM) for banks
2018 MicroFocus acquires HPE's Software business (incl. Atalla)
2018 MicroFocus acquires HPE's Software business (incl. Atalla)

2018 Utimaco acquires Atalla Business

Atalla Corporation founded by John Atalla
   the "Father of the PIN" (1924-2009)
1973
1987 Tandem Computers Inc. acquires Atalla Corporation
   "1500 customers, numerous patents"
1991 1st Gen HSM KryptoServer
1993 ZKA Approval
1997 1st Automotive Application
1999 TimeStamp for Lotteries
2002 2nd Gen HSM CryptoServer Series (Incl. Sensor Foil)
2005 Hewlett Packard (HP) acquires Compaq Computers
2006 HSM Software Simulator
2007 HSM Software Development Kit
2008-2013 Sophos
2009 "85% of all ATM transactions worldwide are secured by Atalla Box"
2010 "Deutschland" HSM
2013 Payment EFT POS for large Food Retailer
2014 Industrial IoT with leading Semiconductor
2015 Hewlett Packard splits: HP Inc. for PCs/Printers
   And HPE for B2B business
2016 Office in USA
2017 Office in Singapore
2018 Bank-Verlag: signature activation module (SAM) for banks
2018 MicroFocus acquires HPE's Software business (incl. Atalla)
2018 MicroFocus acquires HPE's Software business (incl. Atalla)

2018 Utimaco acquires Atalla Business

Atalla Corporation founded by John Atalla
   the "Father of the PIN" (1924-2009)
1973
1987 Tandem Computers Inc. acquires Atalla Corporation
   "1500 customers, numerous patents"
1991 1st Gen HSM KryptoServer
1993 ZKA Approval
1997 1st Automotive Application
1999 TimeStamp for Lotteries
2002 2nd Gen HSM CryptoServer Series (Incl. Sensor Foil)
2005 Hewlett Packard (HP) acquires Compaq Computers
2006 HSM Software Simulator
2007 HSM Software Development Kit
2008-2013 Sophos
2009 "85% of all ATM transactions worldwide are secured by Atalla Box"
2010 "Deutschland" HSM
2013 Payment EFT POS for large Food Retailer
2014 Industrial IoT with leading Semiconductor
2015 Hewlett Packard splits: HP Inc. for PCs/Printers
   And HPE for B2B business
2016 Office in USA
2017 Office in Singapore
2018 Bank-Verlag: signature activation module (SAM) for banks
2018 MicroFocus acquires HPE's Software business (incl. Atalla)
2018 MicroFocus acquires HPE's Software business (incl. Atalla)

2018 Utimaco acquires Atalla Business

Atalla Corporation founded by John Atalla
   the "Father of the PIN" (1924-2009)
1973
Drivers for both Telecommunication Compliance and Information Security

Digital transformation

Digital transformation is driven by changing consumer behavior and digital transformation of companies and the resulting creation of digital assets and (sometimes) disruptive technologies. It certainly means more cyber security.

Breaches

The number of breaches of is ever increasing as the value of the assets at stake are permanently on the rise. All industries are impacted: from Automotive to banking, from industrial to governments.

Regulation

To ensure security of critical infrastructures in the light of increase in cyber criminality governments issue more stringent regulations. Compliance is a driver for the adoption of information security technology & encryption.
“At Utimaco, we see Atalla as an integral player in the future of providing security.”

Innovations, New Players, New Applications in the non-cash markets

Mobile, Cloud & Regulations disrupt old Business Models

We offer unrivalled trust – now and in future!

Utimaco‘s Payment HSMs
Utimaco Payment HSMs

- Utimaco **Atalla AT1000**
  - Utimaco **Atalla AT1000** is a payment HSM for the inter-banking network to protect sensitive data and associated keys for non-cash retail payment transactions like cross-border settlements, PIN translations and cardholder authorization

- Utimaco **PaymentServer**
  - Utimaco **PaymentServer** is a Payment Card Industry (PCI) PIN Transaction Security (PTS) HSM for the *card schemes* programs like Visa, MasterCard, Amex, UnionPay; including card personalization
Atalla AT1000 HSM

Hardened & secure environment for payment specific cryptographic operations

▪ **Value Proposition**
  - ACH and Interbanking Support
  - RSA ATM management
  - Market leading performance for PIN translations

▪ **Features at a Glance**
  - Advance Backup / Restore Capability
  - AES support
  - **Certified**: NIST FIPS 140-2 L3 & PCI-HSM* validated

* in progress
Use Case Examples

**ATM network**
- STAR, NYCE, Pulse, eftpos
- PIN translation & verification
- Network approved device

**Interbanking**
- Support of large set of PIN formats
- APACS 40 & 70, ISO 9564, ANSI X9
- PTS PIN validated device

**ATM/POS Device Management**
- RSA ATM remote keying
- DUKPT key management

**Secure Remote Management**
- Remote upgrade of software
- Remote initialization and configuration
- Performance monitoring

---

Traditional Payment Use Cases Continually Evolve (New Algorithms & Keys) as per Industry Mandates
Value Proposition

- Payments & GP functionality on the same box
- Self Customizable HSM Firmware SDK
- PCI HSM certification assistance for customized firmware

Features at a Glance

- **High Availability**: Support for both native & customer HA
- **Scalable**: Vertical & horizontal scalability to always satisfy your needs
- **Certified**: NIST FIPS 140-2 L3 & PCI-HSM validated

Hardened & secure environment for payment specific cryptographic operations
Use Case Examples

**Payments Schemes**
- EMV, Visa, MasterCard, Amex, UnionPay
- CVC/CVV verification
- *Cloud-based payments

**Card Issuance**
- Credit cards
- Debit cards
- Gift cards
- eID cards

**Secure Remote Management**
- Remote upgrade of software
- Remote initialization and configuration
- Performance monitoring

*Currently being developed

Traditional Payment Use Cases Continually Evolve (New Algorithms & Keys) as per Industry Mandates
Payments Use Cases
EMV Card Personalization Use Case

Executive Summary – Card Personalization

Business Challenge

▪ Meet strict regulatory production / timelines of EMV Credit Cards (e.g. AES, ISO4…)
▪ Able to integrate with existing systems

Solution

▪ Built-in EMV personalization command sets along with P11, JCE, CNG to have a single HSM meet the customer’s full portfolio for card personalization

Result

▪ High assurance to allow “no-stoppage” to automated line
▪ Ability for customization to cover edge cases and application integrations
Executive Summary – PIN Translation

**Business Challenge**
- Mandate to comply with the New PIN Block Format (AES / ISO4)

**Solution**
- Support for **ISO standards** & large set of **PIN formats** for PIN translation methods in the market

**Result**
- Extreme high reliability to meet & comply with the business SLA
Authorization Use Case

Executive Summary – Issuer Approval / Denial of a Card (Credit or Debit) Transaction

Business Challenge

▪ Quick turn-around to meet stringent SLA
▪ Additionally support new payment types including need for AES & ISO4

Solution

▪ Built-in functions for standard and proprietary authorization

Result

▪ Meet regulatory requirements effectively while expanding new business needs
“At Utimaco, we see Atalla as an integral player in the future of providing security.”

Innovations, New Players, New Applications in the non-cash markets

Mobile, Cloud & Regulations disrupt old Business Models

We offer unrivalled trust – now and in future!

Utimaco’s General Purpose HSMs
CryptoServer Hardware Security Modules

**CryptoServer**

- **Se-Series 12/52/500/1500**
  - PCIe plug-in card
  - Network attached
  - Cloud Connection
  - (T)DES, AES, RSA, (EC)DSA, (EC)DH, SHA, ...
  - FIPS 140-2 Level 3, Common Criteria EAL4+, PCI-HSM (* in progress)

**CryptoServer**

- **CSe-Series 10/100**
  - PCIe plug-in card
  - Network attached
  - Cloud Connection
  - (T)DES, AES, RSA, (EC)DSA, (EC)DH, SHA, ...
  - FIPS 140-2 Level 3

**Physical Interface**

- PCIe plug-in card
- Network attached
- Cloud Connection

**Cryptographic Support**

- (T)DES, AES, RSA, (EC)DSA, (EC)DH, SHA, ...

**Certifications**

- FIPS 140-2 Level 3, Common Criteria EAL4+, PCI-HSM (* in progress)
Utimaco’s General Purpose Product Portfolio

Product Packages

- **SecurityServer**
- **TimestampServer**
- **CryptoServer CP5**
- **CryptoServer SDK**
- **CryptoScript SDK**

**General Purpose HSM**

- **CryptoServer Se-Series 12/52/500/1500**
- **CryptoServer CSe-Series 10/100**

- **RFC 3161**
- **Common Criteria certified for eIDAS Trust Services**
- **Development Kit for CryptoServer Firmware Development**
- **Development Kit for Scripting HSM Extensions**
PKCS#11, JCE, MS CSP/CNG/SQLEKM, CXI
- Plug-and-play integration into numerous 3rd party applications
  - PKI – certificate issuing, OCSP responder
  - Database encryption
  - Document signing, code signing
  - And many more …

Internal and external key storage
- Internal key storage fulfills most stringent compliance requirements
- External key storage provides much greater storage capacity and easy setup of an HSM cluster

HSM cluster for high-availability or load-balancing

Great performance
Extremely Powerful and Flexible Access Control Mechanisms

- Multitude of authentication mechanisms
  - Username/password
  - 2 factor authentication
    - Keyfile
    - Smartcard

- 4 eyes principle and M of N authentication

- Configurable role-based access control
  - Granular definition of required permissions

- Interface hardening

=> Fulfil any security policy from straightforward to most-demanding
Free HSM simulator

- Fully functional software simulator for Windows and Linux
  - HSM administration, user authentication, key management, cryptography, etc.

- Ideal for
  - Product evaluation
  - Dry-run before setup of production HSM
  - Integration testing
  - Training

Ready to take off?
Download our HSM simulator!

Register for free

Take me there
Standardized cryptographic APIs support many cryptographic algorithms and mechanisms …
  - PKCS#11, JCE, Microsoft CSP/CNG

… but do not
  - Cover all algorithms and mechanisms used worldwide
    - (Secret) Government algorithms
    - Key derivation mechanisms only used for payment transactions in selected countries
  - Immediately incorporate new algorithms as they get designed and standardized
    - Post Quantum Cryptography
  - Support complex protocols or sequences of functions as atomic operations
    - Key derivation and PIN calculation for card personalization
Utimaco's CryptoServer SDK is the most powerful and flexible development kit that enables you to

- Define and implement custom functionality with optimized application interfaces
- Develop custom code that runs inside the secure boundary of any Utimaco HSM
- Extend PKCS#11 functionality by Vendor Defined Mechanisms
Utimaco CryptoServer SDK

Most Powerful SDK for HSM Firmware Development

▪ Full control of HSM functionality

▪ Modular firmware concept allowing for a high number of firmware modules

▪ C / C++ programming language
  ▪ Complete Utimaco base firmware re-usable

▪ Support for common development tools
  ▪ Microsoft Visual Studio
  ▪ gcc

▪ HSM simulator for testing and debugging

▪ Sample firmware modules and host applications
Other Utimaco GP HSM products

- **CryptoServer Cloud**
  - Reliable and trustworthy HSM-as-a-Service that helps you secure your assets in the cloud
  - Covered last week in dedicated webinar: [https://hsm.utimaco.com/downloads/webinars/](https://hsm.utimaco.com/downloads/webinars/)

- **CryptoServer CP5**
  - Common Criteria EAL4+ certified HSM for eIDAS-compliant Trust Services and Remote Signing

- **TimestampServer**
  - Proof of existence of documents/data, and proof of occurrence of events, using the Timestamp protocol specified in RFC 3161
  - Watch out for webinar about TimestampServer 3.00 in 2019

- **CryptoScript SDK**
  - Implementation of HSM extensions made easier than ever by scripting
  - Watch out for webinar about CryptoScript SDK 4.30 in 2019
▪ If you’d like to stay in touch: follow us on social media or register for our mailing list at https://hsm.utimaco.com/newsletter/

▪ The Utimaco Enterprise Secure Key Manager (ESKM) will be addressed in a dedicated webinar session early 2019.

▪ Let’s move to your questions now!

▪ Any more questions? Don’t hesitate to get in touch.
Thanks for your attention

Utimaco HSM
Product Management
priyank.kumar@utimaco.com
dieter.bong@utimaco.com

Utimaco IS GmbH
Germanusstraße 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