White Paper

Selecting the right Hardware Security Module

By Utimaco

Introduction

Cryptography, by its very nature, is extremely difficult to understand. Likewise, is the challenge of selecting the right hardware to provide adequate security for your critical infrastructure, without overshooting your needs.

How much cryptographic security is too much? What is the industry standard? What exactly is a Hardware Security Module, and what benefits does it offer?

Day after day, the answers to these questions become critically more important as you scale your enterprise. Making the wrong choice could be a costly mistake.

There are many types of cryptographic devices to choose from, but superior to all is the Hardware Security Module (HSM). With it's hardened and resistant shell and highly advanced encryption mechanisms, the logical and physical security of HSM rules supreme in the cryptographic hardware industry.

What is a Hardware Security Module?

A Hardware Security Module (HSM) is a piece of equipment that generates high-quality keys, protects them against a wide range of logical and physical attacks, and utilizes these keys to perform cryptographic operations in a secure environment.

The Technical differentiating factors

Performance

Look at the performance factors for each type of HSM, but focus specifically on your use case: encryption/decryption/key generation/signing, symmetric, asymmetric, EC, etc. Ask about true performance figures, e.g. for a network-attached HSM, ask about the network configuration or for embedded cards, ask about standards released after the PCIe bus.

Scalability

What are the limiting factors in terms of scalability, in connection with your application? Do you need a defined number of keys stored inside the HSM? How could you add another HSM? How easy would this be?

Redundancy

What happens if one HSM breaks? How much would this impact on your operations? How easy would it be to replace without loss of service, etc.

Backups

How are backup and restore processes carried out? How much effort would it be for your organization to implement these processes? Are you able to avoid irretrievably losing your data?

API support

The API is the connection to your Application-Host environment. Here are some hints for dealing with questions about supported APIs:

Microsoft MS CSP/CNG

The Microsoft “standard” API is the easiest way to connect to an HSM when using Windows;

PKCS#11

The “industry standard”, but there are some pitfalls such as known security issues and vendor proprietary extension.

Payment APIs

Many attacks are able to exploit infrastructure vulnerabilities in key management payment systems. If the infrastructure is weak, the protection of payment transaction data can be undermined by an advanced attack using a fake or guessed key.

Sensitive card transactions can be protected by securing encryption keys within the safe confinement of a Hardware Security Module.

An HSM compliant with PCI-DSS standards provides unrivaled implementation of AES and other safeguards for payment transactions. HSM protects and manages encrypted keys required by key operations such as:

- PIN translations
- Card verification
- EFTPOS
- ATM
- Cash-card reloading
- EMV transactions processing
- Key generation and injection

The procedural factors

OS / hardware support

This requires different issues to be taken into consideration. The first of which is: Which operating systems are supported by the embedded card (PCIe-Driver)? Another issue: Which operating systems are supported by the network-attached HSM? Also: Which OS is supported by the managements tools, e.g. GUI/command line?

Management

Can the HSM be managed remotely? Which functions can be activated and controlled remotely? Programmability – Most of your development will be at the other end of the APIs, but sometimes it can be useful to have the ability to write applications that run on the device, for greater flexibility or speed and to specify your API

Physical security

Ask yourself the question: How resistant to direct physical attack does your solution need to be? If, for whatever reason, you decide that it is particularly important, you might want to look for “active tamper detection and response”, as opposed to just “passive tamper resistance and evidence”. Or alternatively, in terms of FIPS 140-2, look for FIPS 140-2 level 4 hardware, or stick to the conventional FIPS 140-2 level 3. The PCI PTS (Pin Transaction Security) HSM standard defines “Modular Security Requirements” for HSMs during their entire lifecycle (manufacturing, delivery, usage, and decommissioning). In any banking context, you need to go for version 3 of this standard.

The procedural factors

Algorithms

Does the HSM support the cryptographic algorithm you want to use– for example the quantum secure ones? Does it allow you to do this, via the selected API (primitives, modes of operation and parameters e.g. curves, key sizes)? Authentication options; passwords; quorums; n-factors; smartcards; etc.

At the very least, you should be looking for something that requires a configurable quorum size or password-authenticated users before allowing operations via use of a key.

Policy Options

You might want to be able to define policies, such as controlling whether or not: keys can be exported from the HSM (wrapped or unencrypted); a key can only be used for signing/encryption/decryption/…; authentication is required for signing, but not verifying, etc.

Audit capability

Including both HSM-like operations (generated key, something signed with key Y) and handling connection problems or crashes. How easy is it going to be to integrate the logs into your monitoring system (syslog/snmp/other network accessible – or at least non-proprietary – output)?

Key backup

If the HSM is to be used within a certificate authority, or to encrypt or verify data in a database, it is imperative that the HSM has a secure mechanism to back up the key(s) if the device fails. Ideally, the key backup should be made with three or more smart cards. Each card contains a piece of the backup key and is stored in a separate location.

"Making sure that the HSM is post-quantum enabled"

The HSM should allow to add new cryptographic functions and algorithms as the state-of-the-art in blockchain grows and changes, including new post-quantum algorithms like Hyperledger Fabric and Fabric-CA. A close look at the provided SDK is important before choosing the solution

Business and Compliance Requirements

Different companies require different solutions, for example in enterprise PKI and CAs, HSM provides an additional layer of hardware protection. It cleanly separates at a hardware level the storage of keys from the machine running the application making use of the keys.

HSMs help to Improve profitability and achieve compliance with solutions for paper-to-digital initiatives, PCI DSS, PCI P2PE, PCI PIN, digital signatures, DNSSEC, hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk key generation, data encryption, and more.

FIPS 140-2 Compliance

An important aspect of choosing an HSM is understanding the FIPS certification levels and weighing the costs of these levels versus the value of what is being secured. It is important to distinguish between vendors that claim FIPS 140 “compliance” versus “validation” since any vendor can claim that their product is compliant.

Security Level 1.	**Security Level 2.**	**Security Level 3.**	**Security Level 4.**
Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.			
Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters physically separated from other data ports.	
Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.			
Production-grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP and EFT.
Executable code. Authenticated software. Single operator.	CAPP evaluated at EAL2.	CAPP plus trusted path evaluated at EAL3 plus security policy modeling.	CAPP plus trusted path evaluated at EAL4 plus security policy modeling, covert channel analysis, and modularity.
Approved key generation/distribution techniques.		Entry/output of keys in encrypted form or direct entry/exit with split knowledge procedures.	
FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for voice).		FCC Part 15. Subpart B, Class B (Home use).	
Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.		Statistical RNG/PRNG tests – callable on demand.	Statistical RNG/PRNG tests–performed at power-up.
Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification. Functional testing.	High-level language implementation. Test Coverage analysis.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Specification of mitigation of attacks for which no testable requirements are currently available.			

Note: that operating a HSM in FIPS 140-2 level 3 or higher mode may impose restrictions on on-board key generation through the PKCS #11 API

Business and Compliance Requirements

eIDAS Compliance and ETSI Standards

The HSM’s 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 (Online Certificate Status Protocol) and timestamping.

Trust Service Providers look to HSM for support in fulfilling policy and security requirements defined in various ETSI technical standards. For example, Utimaco Cryptoserver CP5 meets all Policy and Security Requirements for Trust Service Providers. The following chart is a list of those standards, which qualify Utimaco’s HSM for Electronic Signatures, Electronic Seals, and Time Stamp.

Policy and Security Requirements

Standards	Title
ETSI EN 319 401	General Policy Requirements for Trust Service Providers
ETSI EN 319 411	Policy and security requirements for Trust Service Providers issuing certificates
	Part 1 – General requirements
	Part 2 – Requirements for Trust Service Providers issuing EU qualified certificates
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
Drafts	Title
ETSI TS 119 441	Policy requirements for TSP providing signature validation services
ETSI TS 119 495	Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU

Common criteria

Effective October 1, 2009, any product accepted into evaluation under the U.S. CC Scheme must claim compliance to a NIAP-approved PP. The following Protection Profiles (PP) have been approved for use by vendors for evaluation of products under the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the Common Criteria Recognition Arrangement (CCRA).

NIAP is currently working with industry, our customers, and the Common Criteria community to create Protection Profiles for each technology. These Protection Profiles include assurance activities with the goal of achievable, repeatable and testable evaluation activities for each particular technology (see PPs in Development for a status of each PP).

The following chart is a list of 37 Validated Protection Profiles accepted under CC.

Tech Type	Profile Name	CC Ver.	Short Name	Approval Date
Email Client	Extended Package for Email Clients v2.0	3.1	PP_APP_EMAILCLIENT_EP_ v2.0	2015-06-18
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0	3.1	CPP_FDE_AA_V2.0	2016-09-09
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0	3.1	CPP_FDE_EE_V2.0	2016-09-09
Encrypted Storage	Extended Package for Software File Encryption Version 1.0	3.1	PP_APP_SWFE_EP_v1.0	2014-11-10
Enterprise Security Management	Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1	3.1	PP_ESM_ICM_V2.1	2013-11-21
Enterprise Security Management	Protection Profile for Enterprise Security Management - Policy Management Version 2.1	3.1	PP_ESM_PM_V2.1	2013-11-21
Enterprise Security Management	Protection Profile for Enterprise Security Management-Access Control Version 2.1	3.1	PP_ESM_AC_V2.1	2013-11-12
Firewall	collaborative Protection Profile for Stateful Traffic Filter Firewalls Version 2.0 + Errata 20180314	3.1	CPP_FW_V2.0E	2018-03-14
IDS/IPS	Extended Package for Intrusion Prevention Systems Version 2.11	3.1	EP_IPS_V2.11	2017-06-15
IDS/IPS	Extended Package for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) Version 1.0	3.1	EP_WIDS_V1.0	2016-10-06
Mobility	Extended Package for Mobile Device Management Agents Version 3.0	3.1	EP_MDM_AGENT_V3.0	2016-11-21
Mobility	Protection Profile for Mobile Device Fundamentals Version 3.1	3.1	PP_MD_V3.1	2017-06-16
Mobility	Protection Profile for Mobile Device Management Version 3.0	3.1	PP_MDM_V3.0	2016-11-21
Multi Function Device	Protection Profile for Hardcopy Devices Version 1.0	3.1	PP_HCD_V1.0	2015-09-11

Tech Type	Profile Name	CC Ver.	Short Name	Approval Date
Network Device	collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314	3.1	CPP_ND_V2.0E	2018-03-14
Network Device	Extended Package for Authentication Servers Version 1.0	3.1	PP_NDCPP_APP_AUTHSVR_EP_V1.0	2015-08-07
Network Device	Extended Package for Session Border Controller Version 1.1	3.1	EP_SBC_V1.1	2016-09-28
Network Encryption	Extended Package for MACsec Ethernet Encryption Version 1.2	3.1	PP_NDCPP_MACSEC_EP_V1.2	2016-05-10
Network Encryption	Functional Package for TLS Version 1.0	3.1	PKG_TLS_V1.0	2018-12-17
Operating System	Protection Profile for General Purpose Operating Systems Version 4.2	3.1	PP_OS_V4.2	2018-05-22
Peripheral Switch	Protection Profile for Peripheral Sharing Switch Version 3.0	3.1	PP_PSS_V3.0	2015-02-13
Redaction Tool	Extended Package for Redaction Tools	3.1	PP_APP_RED_EP_V2.0	2015-12-11
Remote Access	Extended Package for Secure Shell (SSH)	3.1	PP_SSH_EP_v1.0	2016-02-19
SIP Server	Extended Package for Enterprise Session Controller (ESC) Version 1.0	3.1	EP_ESC_V1.0	2016-10-25
USB Flash Drive	Protection Profile for USB Flash Drives Version 1.0	3.1	PP_USB_FD_v1.0	2011-12-01
Virtual Private Network	Extended Package for VPN Gateways Version 2.1	3.1	EP_VPN_GW_V2.1	2017-03-08
Virtual Private Network	PP-Module for VPN Client Version 2.1	3.1	MOD_VPN_CLI_V2.1	2017-10-05
Virtualization	Extended Package for Client Virtualization Version 1.0	3.1	EP_CV_V1.0	2016-11-22
Virtualization	Extended Package for Server Virtualization Version 1.0	3.1	EP_SV_V1.0	2016-11-22
Virtualization	Protection Profile for Virtualization Version 1.0	3.1	PP_BASE_VIRTUALIZATION_V1.0	2016-11-22
VoIP	Extended Package for Voice and Video over IP (VVoIP) Version 1.0	3.1	EP_VVOIP_V1.0	2016-09-28
Web Browser	Extended Package for Web Browsers v2.0	3.1	PP_APP_WEBBROWSER_EP_v2.0	2015-06-16
Wireless LAN	Extended Package for Wireless LAN Access System	3.1	PP_WLAN_AS_EP_V1.0	2015-05-28
Wireless LAN	Extended Package for Wireless LAN Client Version 1.0	3.1	PP_WLAN_CLI_EP_V1.0	2016-02-11

Business and Compliance Requirements

Other Certification Schema

Like the PCI-HSM or DK approval, these schemes are useful if you are in the industry concerned. In addition to the certifications, ask for specific references to your industry or government space. Do not just rely on ISO certification lifecycles for software development.

The deployment – on site or as-a-service

Cloud services have been a godsend for small start-ups and even medium sized businesses. Rather than investing scarce resources on significant upfront capex outlays, start-ups can instead tap into cloud services and pay for what they use. Let's take a brief look at the benefits of using HSM as a Service for PCI compliance.

Scalability

This is one of the main reasons why fast-growing businesses opt for cloud solutions in the first place. Rather than continuously expanding your systems every few months, you can use a scalable cloud service provider and scale near-instantly based on your current volumes. This is especially true for things like Hardware Security Modules where you cannot afford to compromise on security or speed as they are part of the core service experience for your customers.

Ease of Use

FinTech start-ups don't have access to the massive resources of large established players. They cannot have a dedicated compliance or IT security department or at least not one big enough to cover every aspect of security or compliance. Using a cloud service allows them to focus on their core competencies and leave the details to the dedicated service providers. The fact is, even if these companies did hire in-house staff for many of these functions, a dedicated service provider will almost always have a cost and experience advantage.

The deployment – on site or as-a-service

Speed of Deployment and Training

Banks spend a lot of time and money on training their staff. This can lead to downtime and lost productivity. A cloud service provider for your Hardware Security Modules will most definitely save you some time and money here. Obviously, it is always a good idea for everyone to have a basic understanding about all aspects of cyber security, but you shouldn't have to deploy a full-time resource to manage things as a small business.

Cost optimizations

You pay for what you need. There is no need for upfront capex expenditures. HSMs can help you meet several PCI DSS requirements like data encryption, key injection, authentication and conditional access.

Customizability

What is the capability of supporting vendor or customer proprietary extensions or mechanisms for use case-specific API extensions and are not part of the PKCS #11 standard. This will increase costs when switching vendor but may also fuel ability to innovate and differentiate HSM users secure offering to his market.

A secure time source

Secure auditing and non-repudiation requires logged messages containing a time and date from a safe source. The system clock of a server can be easily changed. If a digitally signed message is created using an unsafe time source, it is easier to dispute the time and date of the message (and the whole transaction). Only an authenticated administrator should have access the the HSM time log.

Conclusion

HSM are the apex of cryptographic modules, and offer both logical and physical security. But, as you can see, the factors to consider when choosing an HSM are numerous. It all depends on your own specific preference and security level requirements. In any case, data security in every area of a company is needed for the company to grow. The key factors to consider are security, availability, and your level of experience.

Limitations

Also keep in mind no matter what HSM you choose, it should be backed by stingend internal policies and procedure of implementing those policies too. Management must address these areas simultaneously if the company to safely scale its number of cryptographic keys and the databases they protect.

Prospects

We strongly recommend Utimaco for companies who require and HSM to be EAL4+ Common Criteria certified in compliance with eIDAS Protection Profile EN 419 221-5.

Beginning October 09, 2018 companies can now rely on Utimaco's CryptoServer CP5 HSM to comply with European eIDAS regulations for digital signatures, seals and timestamps Certification according to eIDAS Protection Profile EN 419 221-5 opens up new business opportunities for Utimaco and its partners Dedicated Utimaco CryptoServer CP5 simulator available for evaluation and integration testing

Utimaco Solutions

SecurityServer Se Gen2

The SecurityServer Se Gen2 from Utimaco 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 numerous applications, including e.g. public key infrastructures (PKIs), database encryption. The SecurityServer Se Gen2 is available as a PCIe plug-in card or as network-attached appliance.

SecurityServer CSe

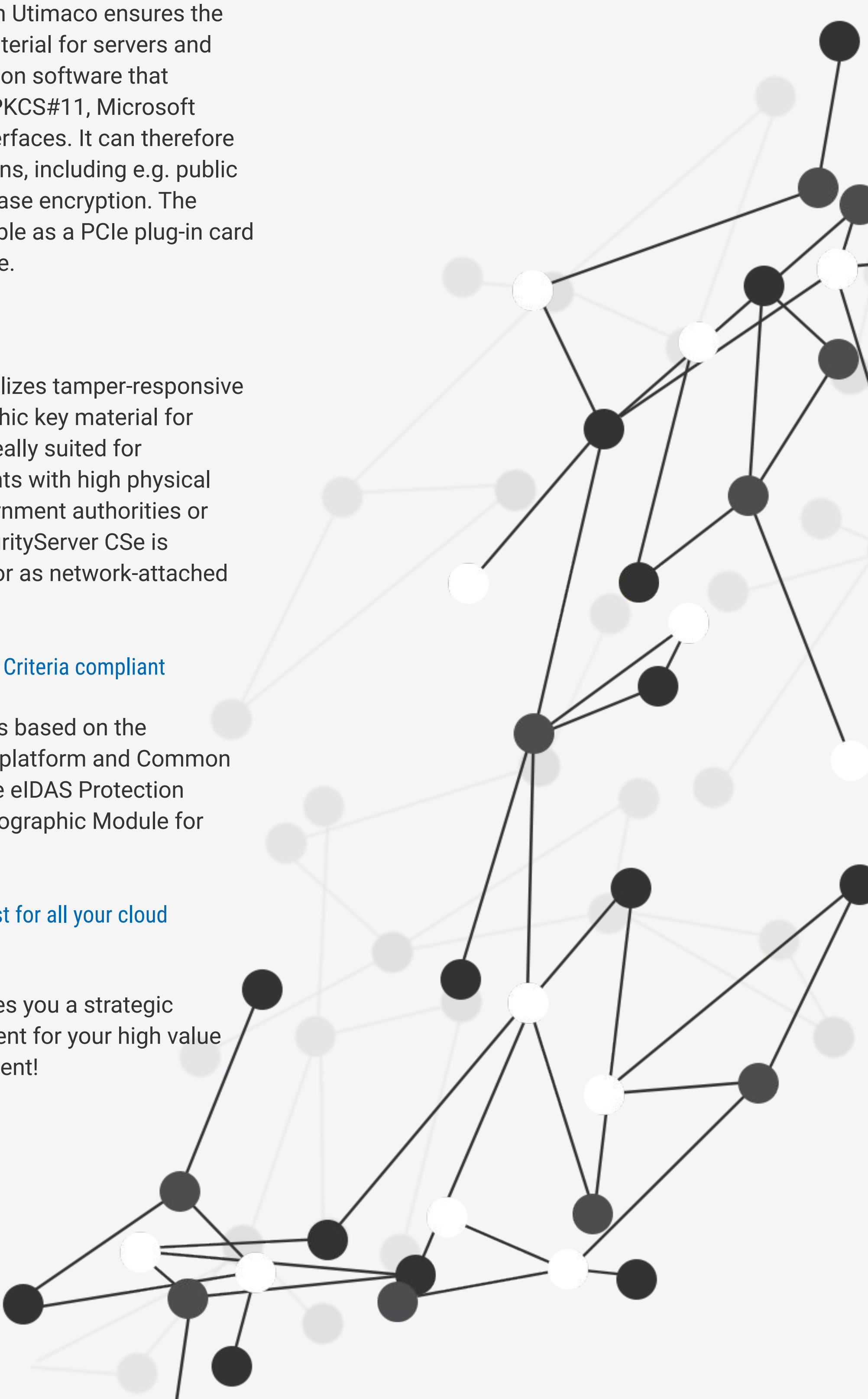
Utimaco's SecurityServer CSe utilizes tamper-responsive technology to secure cryptographic key material for servers and applications. It is ideally suited for applications and market segments with high physical security requirements, e.g. government authorities or banking environments. The SecurityServer CSe is available as a PCIe plug-in card or as network-attached appliance.

CryptoServer CP5, eIDAS & Common Criteria compliant

The Utimaco CryptoServer CP5 is based on the CryptoServer Se Gen2 hardware platform and Common Criteria-certified according to the eIDAS Protection Profile (PP) EN 419 221-5 "Cryptographic Module for Trust Services".

CryptoServer Cloud, The Root of Trust for all your cloud applications

Utimaco CryptoServer Cloud gives you a strategic architectural fit & risk management for your high value assets in a multi-cloud environment!



Utimaco Solutions

TimestampServer, the tamper-proof timestamping solution

The Utimaco TimestampServer is the ideal Hardware Security Module (HSM) for business applications that require proving the existence and status of a document or data at a specific point in time.

Deutschland HSM for secure ePassport and eID applications

The Hardware Security Module (HSM) specifically for applications such as identity management and the issuance and management of electronic ID documents. The Germany HSM (D-HSM) offers a secure solution with specific features and algorithms for the production and initialization of electronic passports and identity cards.

Hardware Security Modules:

For Payment use cases, Utimaco offers the following Hardware Security Module:

Utimaco Atalla AT1000 payments security module for protecting sensitive data and associated keys

The Utimaco Atalla AT1000 Hardware Security Module (HSM) is a payments security module for protecting sensitive data and associated keys for non-cash retail payment transactions like cross-border settlements cardholder authentication, and cryptographic keys.

PaymentServer Se Gen2 and PaymentServer CSe to reach full PCI compliance for your solutions

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. The Utimaco Software Development Kit (SDK) allows for self-customization of the PaymentServer by your team to handle proprietary and secret algorithms.

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. The Utimaco Software Development Kit (SDK) allows for self-customization of the PaymentServer by your team to handle proprietary and secret algorithms.

Company

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

Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 260 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit https://hsm.utimaco.com