PRODUCT SHEET

CHIAVE

Key management solution for banks and payment processors with a growing number of cryptographic keys to manage.

Why key management?

Cryptographic keys play a central part in securing ATM and POS transactions as well as in online payments and Internet banking. As threats against payment transactions and digital identity theft have increased, managing the generation, storage and distribution of keys has become a primary concern for the IT security departments within these organizations.

Regulatory compliance is also driving banks and processors to increase the use of cryptographic keys to protect and encrypt data, secure audit trails, guarantee data integrity, enable digital signing of documents, authenticate users and machines, and much more.

Chiave

Chiave is a key management appliance designed to support the common key types within a financial services organisation. Keys can be generated, securely stored as well as exported from and imported to the appliance. Chiave will handle notification to key custodians as to when a key is due to be renewed and guides the user through the policy governing the generation and key ceremony for that key.

Challenges

Best practice requires a number of people and functions to be involved in the key management process in order to prevent a single individual from compromising security. The result is a complex process that needs to be meticulously documented and people that have to be notified when a key is due to be replaced.

As the complexity of the key management process increases, so does the risk for human error. It is not uncommon for downtime on a web server, for example, to be caused by a key custodian forgetting to renew a key or for a key ceremony to be delayed due to the necessary resources not having been scheduled on time.

In addition, for lack of a central key management function, cryptographic keys are typically owned and managed by the people managing a particular resource protected by that key, and these are distributed throughout the organization. Maintaining a comprehensive, consistent and compliant key management policy for the entire organization can therefore be difficult.

The promise

Chiave will help financial services companies centralize the generation and secure storage of keys, as well as ensure that the appropriate individuals are made aware of when a key will expire and the policies associated with the generation of a replacement key and the associated key ceremony.

By centralizing the generation and storage of keys and by automating many of the hitherto manual processes associated with keys, Chiave helps to reduce human error and ensure regulatory compliance.

CHIAVE

VERISEC

Target markets

Chiave is ideal for companies that handle large number of cryptographic keys, such as banks and payment processors.

Chiave references

Chiave was built in collaboration with Point (VeriFone) which was aware of the exponential growth in the number of keys they would have to manage. Knowing that over the next five to ten years the number of keys would likely increase from hundreds to the tens of thousands, the company understood the need to build a robust and centralized key management solution with the ability to keep track of all the policies governing the generation, storage and key ceremony associated with their cryptographic keys. Together with Verisec, requirements were specified and are now the foundation for the Chiave product.

During the early development period Verisec has engaged in dialogue with a number of banks and payment processors to include functionality required by those organizations as well, and this process is still ongoing as the company is expanding into new geographic markets with differing key management requirements.

Tecnical summary

- Dual control over all sensitive actions such as export, import.
- Strong, two-factor authentication of both administrators and key custodians.
- Component encryption and Remote PED: Key components can only be viewed and entered in clear text via secure PED:s, components are encrypted end-to end, from smart card to HSM within Chiave.
- Remote component transfer: Component transfer from and to Chiave does therefore not require a secure physical connection, normal card readers and regular network can be used.
- Built-in FIPS 140-2 level 2 hardware cryptographic engine. Level 3 optional.
- Symmetric key algorithms: AES, double- and triple-key DESede.
- Asymmetric key algorithms: RSA 2048 and larger; PKI support through PKCS#10 certification requests and PKCS#7 certification responses.
- Key export formats: Component based onto individual key custodian smartcards, 2-9 components; PKCS#12; Sun Java JKS format.
- Key import formats: Component based, 2-9 components; PKCS#12; Sun Java JKS format.
- Key custodian smartcards: JCOP21 v2.4.1.

Contact details

For more information regarding the Chiave product, please contact sales@verisec.com, +46 (0)8 723 09 00 or 0800 917 8815 (UK toll-free).

Verisec AB, Box 2034, 131 02 Nacka, Sweden. sales@verisec.com. +46 (0)8 723 09 00. UK phone (toll-free) 0800 917 8815
For more information about Verisec and contact information to our offices in UK and Serbia, please visit www.verisec.com