PRODUCT SHEET

CHIAVE RA

Chiave RA is a key and certification appliance that simplifies mass generation of private keys and certificates based on a public key infrastructure (PKI).

Key benefits

- Reduced manufacturing time.
- Offboard generation of keys and certificates for mass distribution or large deployments of PKI on cards.
- Secure Data processing. Has been designed for secure key generation and signing based on PKI for Banking and National ID Scheme applications.
- Scaleable: Chiave RA is a fully scaleable platform for both smaller issuing banks to large bureaus.
- Transaction processing: Applications can request keys and certificates from Hnossa through a secure communication channel.
- Audit & Event management: Chiave RA offers tamper evident logs for accounting and certification.
- Resilience and increased throughput by clustering.
- HSM includes a tamper resistant, hardware cryptographic processor used extensively by institutions world wide.

Challenges

Key lengths are successively increasing from 1024 to 2048 or even 4096-bit. This development is driven by the need for increased key lengths to maintain or increase security.

In large production facilities on-board generation of keys is not practical from a production standpoint. In addition, from a security and certification perspective the personalization preparation software solutions have to be disconnected from the outside world. Whereas keys required for personalization of EMV cards can easily be exchanged with an issuer through files, PKI certificates frequently require communication with an online, third-party driven certificate authority that will certify the keys.

Chiave RA provides an easily integrated component that offloads large-scale RSA key generation and provides online connectivity to certificate authorities for public key certification. Its output is easily merged with other inputs required for chip personalization (for example, EMV data) that can subsequently be done offline.

Typical use

Chiave RA is used to simplify and automate provisioning of PKI certificates for smartcards or equivalent carriers. Used in all instances where larger number of PKI based cards or devices need to be issued. For example:

- Payment cards with additional certificates for signing
- PKI cards for government or corporate organizations
- Passports or ID cards with embedded chip and certificates

Other uses include provisioning of certificates for manufacturing facilities for products requiring unique ID, signatures, encryption. Examples of devices includes smart card readers, gaming platforms and software licensing applications.

Intended user

- Mid to large sized centralized issuing banks
- Mid to large size personalization bureaus
- Manufacturing facilities for products requiring keys and certificates

Technical specification

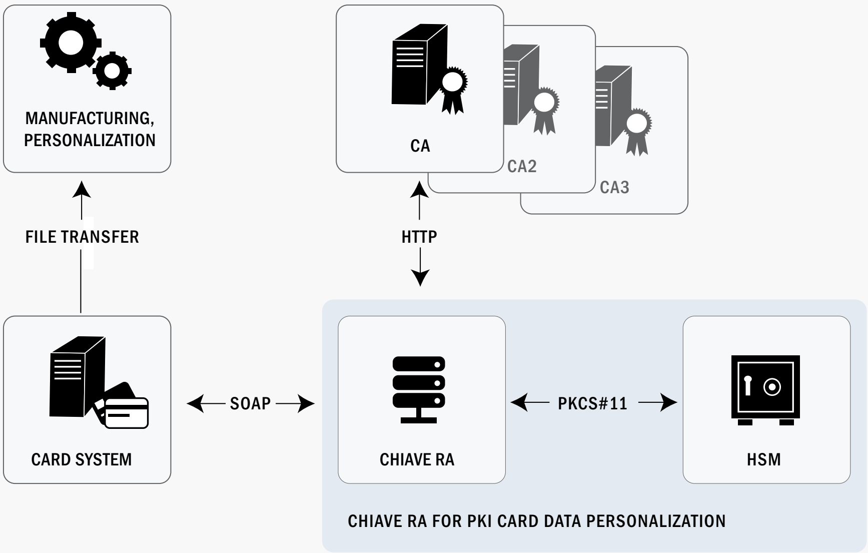
Platform

Appliance with embedded Fips 140-2 level 2 or 3 and EAL 4+ HSM*.

Integration interface

Chiave RA makes an integration possible through a SOAP interface thereby allowing programmers to integrate Chiave

VERISEC


MANUFACTURING, PERSONALIZATION
FILE TRANSFER
CA
CA2
CA3
HTTP
CARD SYSTEM
SOAP
CHIAVE RA
PKCS#11
HSM
CHIAVE RA FOR PKI CARD DATA PERSONALIZATION

Chiave RA for PKI Card Data Personalization

RA functionality with external applications. Typically this may be a smartcard or smartcard-reader programming application.

Logging

Chiave RA maintains tamper evident logs of all processed requests. Tamper evidence is achieved by a MAC "signature" generated by the local master key stored in the HSM.

Cables

- Power cable (region specific)
- Rack mounting kit

Standards supported

- PKI Service: XKMS, Bankgirocentralen Interface definitions version 2.7, 2004
- BankID: DTD definitions version 3.0, Bankgirocentralen, 2010
- HSM for generation of keys is certified to FIPS 140-2 Level 2*
- PKCS#7, PKCS#8, PKCS#10, X.509 v3

Security environment

Chiave RA is a secure product in any environment but it is always recommended to follow best practice such as:

- Avoid installing Chiave RA on open and widely accessible networks such as corporate networks.
- Chiave RA should preferably be installed in a private network together with other systems required for card production and data preparation.
- Chiave RA should be operated within an access controlled environment with physical and logical systems to limit security breaches.

Contact details

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

*Chiave RA can be factory fitted with up to FIPS 140-2 Level 3 HSM

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