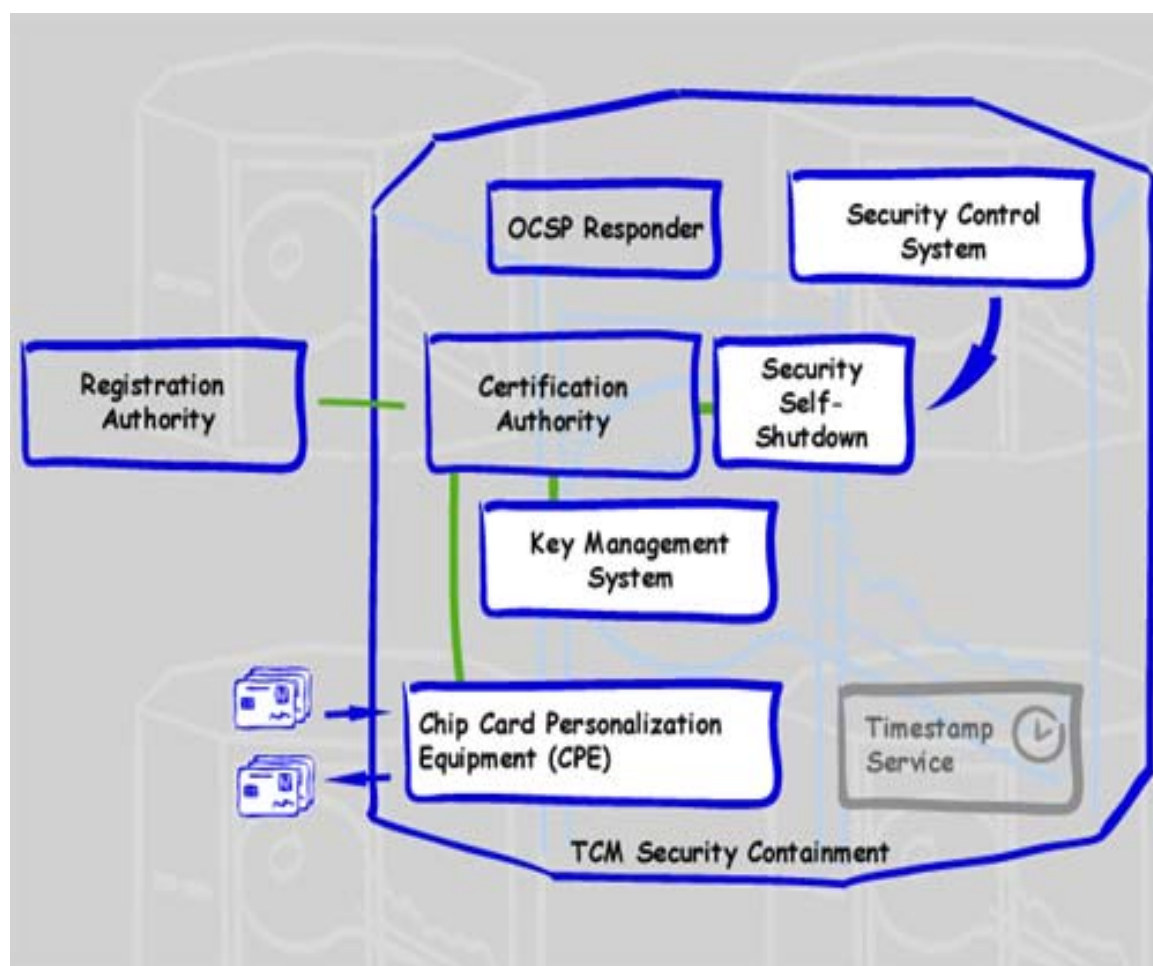


Components of TrustSuite TCM



Chip Card Personalization Equipment (CPE)



Key Features

- Tamper-proof smart card personalization
- High quality key generation based on hardware
- Flexible interfaces to certification and registration authority systems
- Trustworthy key escrow
- High volume batch processing
- Comprehensive user interface
- Compatible with state-of-the-art smart cards
- Pneumatic transport system
- Verifiable logging

Benefits

- Automatic operation with low wear out nearly maintenance-free
- Scalable throughput of up to 10 cards/minute
- Low operating costs
- Tamper-proof key management
- Security design without compromises
- Proven control systems from process industry
- Easy integration with third party Trust Center software



Operation Requirements

- Designed for the TrustSuite Trust Center Module

For stand-alone operation:

- Power supply (1 x 230V AC 16A)
- Compressed air supply 8bar 10l/min

Security Features

- Key generation within tamper-proof Hardware Security Modules (HSM)
- Tamper-proof chip card personalization when operated inside the TrustSuite Trust Center Module (TCM)
- Extended key-length support
- Identification and automatic selection of defect smart cards

Interfaces

- PKIX protocols for CA interconnection
- HTTP/HTTPS and API interface to remote registration authority systems
- API for trustworthy key escrow functions

Online Certificate Status Protocol (OCSP) Responder

In contrast to revocation list management using CRL's, an online status enquiry through OCSP (Online Certificate Status Protocol) allows a simple and, more importantly, a current status check of digital certificates. This is particularly important for transactions where the watchwords are confidentiality and authenticity.

High-quality CA system solutions either offer a OCSP Responders Implementation or products from third-party manufacturers can be integrated into the TrustSuite TCM.

Time Stamp Service

Time stamp services provide digital data with a time stamp using a tamper-proof and reliable clock. This enables a PKI user to confirm that a document was submitted at a certain point in time and has since not been changed.



Registration Centre

Most commercial available CA components have their own registration authority system (RA), which can usually communicate securely with the CA components through SSL/TLS.

High-quality CA/RA systems also have several variants of registration centres, from simple Web registration through to customer-specific, modifiable registration centres, which allow user data to be transferred from ERP systems and Chip Card personalization systems to be actuated. The latter variant is particularly suitable for combining with the TrustSuite Chip Card Personalization Equipment.

In the event that a CA component is to be used on a customer-specific basis and this component does not have the flexible registration centre functions required, the [TrustSuite Chip Card Personalization System](#) offers its own registration data transfer function, which must then however, be modified to suit that particular customer.

Certification Authority

The Certification Authority (CA) is the key instance within a PKI. It issues the digital certificates for the users. To do this, the CA links the personal data of the certificate owner with a "Public Key" and signs this digitally. The digital certificate of the user thus created is published in a linked Directory and is therefore available for use.

As well as certification, the CA also performs the important function of certification revocation. If a digital certificate is recalled, the CA triggers a revocation and places this revocation data onto what is known as a Certificate Revocation List (CRL). This list is also regularly published in the Directory and enables a third party to check the current validity of a digital certificate.

The TrustSuite TCM is designed to allow the use of CA components from various manufacturers. This hinges on being able to shut-down the CA component quickly, i.e. the CA key can be deleted by the TCM security control unit and has a backup function provided by a high-quality CA key.

CA systems from prominent manufacturers usually exhibit this functionality. Any that do not can be retrofitted accordingly with a TrustSuite [Key Management System](#) and [fast shut-down system](#) developed specifically for that purpose.



System for Key Management

The operating concept of the TrustSuite TCM assumes the existence of a permanently secure key management strategy, which on the one hand can restore CA keys at any time, to be able to handle technical defects in key components for example or total CA failure, and on the other, considerably hinders the unauthorised regeneration of a CA Key for manipulative purposes.

Since only very few vendors of commercial CA system solutions offer this type of high-value Key Management Function, a proprietary system has been developed as part of the TrustSuite TCM Project. This is a separate computer system, which is fitted with a hardware crypto-module.

In this module, good CA keys are generated and [backed up](#). This process involves splitting the key backed up into sub-keys, which are stored in separate Smart Cards. To restore the key, all sub-keys are then required again. This allows a high-quality, "Multi-Eye-Principle" to be realised.

The Key Management System also supports the supply of soft CA's with good keys. Thus, an OpenSSL CA for example can be provided with a signing key in the format required by Open SSL. This takes place within the TCM via a serial interface, which prevents having to deal with any compromise in respect of security. Soft CA's require a CA [fast shut-down system](#).

System for Secure Key Storage

One problem, which in the past has been faced by only a few available products, is brought closer to an efficient solution through use of the TrustSuite TCM, namely secure, long-term key storage.

If encryption processes are applied to maintain the confidentiality of sensitive data, particular importance is placed on the security of encryption keys while authorised persons ought to be able to restore such keys at any time, in order to keep the encrypted data accessible.

This controversial requirement can be satisfied with the aid of a TrustSuite TCM. Specifically, the encryption keys generated in the [Chip Card Personalization System](#) are automatically restored, split and archived using Recovery Keys.

Recovery Keys are subject to the same management procedures as CA keys, so as to ensure tamper-proof key archiving at all times. Because the physical whereabouts of Recovery Keys can be checked and established at all times, it is also possible to know and prove who is in possession of which encryption key and when.



Fast CA shut-down system

To quickly shut-down a CA, the CA key must be quickly and reliably destroyed. By contrast with a hardware crypto-module with deletable key memory, a software CA does not afford the same level of reliability due to the keys being available in the file system on the hard drive. To securely shut-down such systems, a fast shut-down facility has been developed for TrustSuite on the basis of a solid state disk and integrated into OpenSSL-based CA system, which is run on an operating system certified as secure.

The fast shut-down system is subject to redundant, direct control by the security control unit on the TCM, thereby achieving a very high level of reliability. The CA fast shut-down system can be integrated into various computer/operating system configurations.

CPE Touch Screen Control Panel

The CPE control panel allows to administrate and maintenance all central components of TCM outside of the security environment. Because of the low-administration and low-maintenance conception of TCM a direct access to different hardware-components is not necessary. Primary function of the control panel is to allow operating staff to control the personalization equipment and to display internal TCM figures, such as pressure or number of cards in preparation.