Certification Authority represents the core of the Public Key Infrastructure to be deployed by an organization. certSAFE application has advanced mechanisms of logical and physical protection with a modular structure that assure availability and maximum scalability. It provides native support for international standards in the field, necessary for integration and interoperability with other PKI infrastructures.

certSAFE – Certification Authority Software offers

- Digital certificates lifecycle management
- Flexible policy for digital certificate management
- Modular architecture suited for any organization
- Ideal solution for deployment in extremely secured environments
- Cross-certification functions to create trust relationships with other PKIs
- Key recovery module
- Time stamp server
- On-line Certificate Status Protocol (OCSP) responder

certSAFE components:

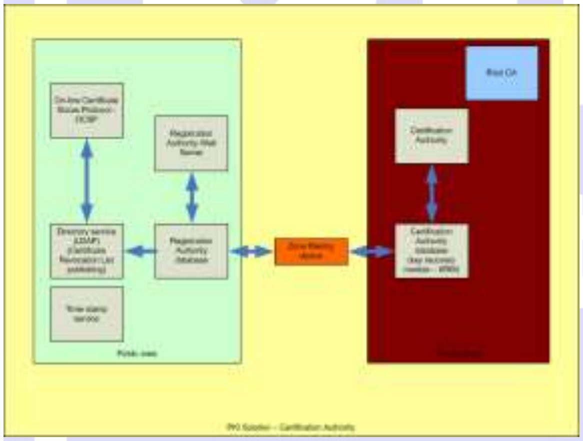
- certSAFE CA
- certSAFE RA/LRA
- certSAFE KRM
- certSAFE TS
- certSAFE OCSP

certSAFE provides a high level of security for demanding environments. It offers digital certificate lifecycle management system for a wide range of e-business or governmental systems. Beside the certificate management and key recovery options it includes also a time-stamp and a certificate validation (based on OCSP) server.

certSAFE CA is the main component. Its role is to generate and protect the Certification Authority private keys, to manage digital certificates and Certificates Revocation Lists (CRL), to safely store and allow the key recovery process for the encryption keys in a secure manner.
certSAFE CA issues all types of certificates: signing certificates, encrypting certificates, SSL server and client certificates, IPSec certificates, smartcard-logon certificates.
There is an important functionality that allows digital certificates issuing with specific private extensions.
The users' private keys can be generated either using FIPS 140-2 level 3 compliant devices, eID cards with cryptographic chips or in a software format.
The Certification Authority private keys management will be performed using FIPS 140-2 level 3 compliant devices.
The access to the certSAFE modules is very strictly controlled by using an internal administration key infrastructure for Certification Authority operators.
There are special modules: RootCA (root Certification Authority), SubCA (subordinate Certification Authority) in order to implement any type of PKI architecture.
To provide a higher security for the solution certSAFE components are running in two separate security areas:

a Public Area, storing and processing information that must be available for the end users a Private Area, where sensitive information and security operations are performed:

- Public area hosts services such as OCSP, LDAP, Timestamping, and also access for user enrolment and certificates requests, etc.
- Private area hosts services which are exclusively controlled by the Certification Authority are placed. These services include: CRL update, Certificate issuance, CA operators administration, Key Recovery for digital encryption certificates, Key management, CA crosscertification, etc


On-line Certificate Status Protocol (OCSP)
Registration Authority Web Server
Directory service (LDAP) (Certificate Revocation List publishing)
Registration Authority database
Time stamp service
Public area
Zone filtering device
Root CA
Certification Authority
Certification Authority database (key recovery module – KRM)
PKI Solution – Certification Authority

certSAFE RA/LRA is the enrolment interface of the Certification Authority with the users. It receives certificate requests in different formats and it processes them. The users can register themselves and generate the private keys on their computers or they can be registered by registration authority operators.

certSAFE KRM is the key recovery module of certSAFE. If the private keys used for encryption are lost, this module is designed to recover them. The keys are securely stored by the Certification Authority and they can be accessed only by the CA security administrators using a “k from n” shared secret recovery scheme (from *n* security administrators at least *k* of the must be present in order to allow the recovery of the keys).

certSAFE TS provides the time stamping service to establish the moment of an operation, offering thus a non repudiation evidence. It generates a digitally signed time stamp that binds together the time of the operation and the hash of the time stamped document. It provides the nonrepudiation service conforming to ETSI TS 101733 standard. The generated time stamps are securely stored on certSAFE TS server; all the events are securely logged for further auditing.

certSAFE OCSP indicates the status of a digital certificate in real time.

On-line Certificate Status Protocol – this service is implemented according to RFC 2560, which is the official description of this protocol.
It assures the on-line validation of the certificates status for different PKI enabled applications.

certSIGN solution is based on the main idea that the verification process of the certificates status must be fast and transparent to the user. A PKI enabled application, running by a user will interrogate the certSAFE OCSP server for verification of the certificate status.

Functional specifications

From the architectural trust point of view, the Certification Authority is usually implemented on the following structure:

- Root Certification Authority (Root CA)
- Subordinate Certification Authority (Policy CA an Class CA)

Root Certification Authority (Root CA)

It runs on off-line devices for which all security measures will be assured: physical, procedural and personnel. The interface with Root Certification Authority for issuing certificates for Subordinated Authorities or cross-certifications with other Certification Authorities is realized through files transmitted by optical or magnetic supports.

Subordinate Certification Authority

It is available online and it manages (issue, revoke and renew) digital certificates for users, servers and devices. The Certification Authority offers the possibility of implementation of all types of digital certificates needed by the specific of the application that will use digital certificates and by types of information whose security will be assured by using digital certificates. The Certification Authority allows defining classes of certificates according with classes of certificates from the national public key infrastructure.

Publishing issued digital certificates and the list of revoked certificates is done in directory servers LDAP v3 compliant. The managing of the main Certification Authority is done by operators from dedicated work stations using a secure communication protocol. The authentication of the operators is realized by secure methods based on cryptographic smart cards or tokens with digital certificates on them. It is not allowed that for signing of digital certificates of the operators to be used the same keys as for signing digital certificates of the system users.

The private key of the Certification Authority are stored on a FIPS 140-2 level 3 devices. The Certification Authority allows recovering encryption private key if this is necessary. This recovery must be executed in special security conditions by implementing a “k from n” scheme at HSM level (Hardware Security Module - FIPS 140-2 Level 3 certified).

Registration Authority

It is available online and allows processing of the digital certificate requests. The authentication of the operator is realized by secure methods based on cryptographic smart cards or tokens with digital certificates on them. It is not allowed that for signing of digital certificates of the operators to be used the same keys as for signing digital certificates of the system users.

At the RA level advanced authentication mechanisms will be in place using a digital certificate X.509 stored on a smart card devices.

Directory Server

It is available online and holds digital certificates and list of revoked certificates issued by the Certification Authority and by the Root Certification Authority. The list of certificates and the list of revoked certificates will be available to the users and to the applications.

certSAFE is delivered with its own directory server and it can be integrated with any directory server compliant with LDAP v3 standard. When integrated with Microsoft Active Directory the digital certificates issued by certSAFE can be successfully used for smart card log-on by Windows domain users.

certSAFE TS

To confirm the existence of a certain document at certain time a Timestamp Authority is needed, that should certify this fact. The Timestamp server creates a cryptographic binding between the document and the signing date, this way providing the non-repudiation service according to the ETSI TS 101733.
certSAFE TimeStamp receives time stamp requests from the users or/and applications. These requests contain the appropriate entity signature on the document that needs to be time stamped. Practically, TSA creates for each document the so-called time stamp that contains the date and hour when the time stamp was created, the document's signature and the time stamp server digital signature.

The server receives time stamp requests from users and/or applications, requests that have to conform to the RFC 3161. These requests contain the hash of the document that needs to be time stamped. The TSA creates the response message compliant with the RFC 3161 as well.

On-line Certificate Status Protocol (OCSP)

certSAFE OCSP server is a module developed for processing On-line Certificate Status Protocol (OCSP) requests – this service is implemented in complete concordance with RFC 2560, which is the official description of this protocol.

OCSP is used trough a Validation and Interrogation Authority. It assures the on-line validation of the certificates status for different PKI enabled applications.
The solution is based on the main idea that the verification process of the certificates status must be fast and transparent for the user.
A PKI enabled application with OCSP capabilities will interrogate the Validation and Interrogation Authority (certSAFE OCSP server)
The OCSP Responder determines the status of the signer's certificate and sends back the response. The status can be GOOD, REVOKED or UNKNOWN.

- GOOD status means that the certificate was not revoked.

- REVOKED status means that the certificate was revoked.
- UNKNOWN status means that the OCSP Responder can’t determine the exact status of the certificate

The Validation and Interrogation Authority uses the LDAP protocol for LDAP server interrogation for obtaining the CA and user certificates and certificates revocation lists (CRL).

Technical specifications

Algorithms and supported standards:

- Symmetric key encrypting algorithm– 3DES, AES, proprietary algorithm
- Digital signing algorithm– RSA with 1024 – 4096 bits key length
- Hash functions– SHA 1, SHA 256
- Keys changing algorithms - DH
- Repository– LDAP v3
- Storing the private keys according to the PKCS11 standards
- Certificate management– X509
- API interface– PKCS11
- Digital certificates X.509 v3 and CRL (certificate revocation list) X.509 v2
- PKCS#11 for hardware device access
- PKCS#12 for storing private keys and certificates in software format
- PKCS#7 for signed and encrypted data format
- PKCS#10 the certificate request format
- RFC 2560 for the OCSP
- RFC 3161 for the TimeStamp