



# Glossary

---

## **Access**

Ability to use and employ any information system resource.

## **Access control**

Process of granting access to information system resources only to authorized users, programs, processes or systems.

## **Activation data**

Data (other than cryptographic keys) that must be protected (e.g. PIN, passwords, dissipated co-shared secrets) and is essential for normal operation of a cryptographic module.

## **Audit**

Independent review and assessment of a system in order to:

- test system management controls
- verify whether a system operation is performed according to the accepted certification policy and resulting operating procedures
- discover possible security gaps
- recommend suitable modifications to control measures, certification policy and procedures

## **Authenticate**

To confirm the declared identity of an entity.

## **Authentication**

Security controls aimed at providing the reliability of transferred data, messages or their sender or controls of authenticity verification of a person prior to the delivery of certain categories of the information to the person concerned.

...

## **Card reader**

Device designed to establish a connection with an encryption card.

## **Certificate activity period**

Period between a starting and ending date of the certificate validity or between a starting date of the certificate validity and date of revocation or suspension of the certificate.

## **Certificate class**

Certificate credibility level that results out of the accuracy of supervising a user and the permissible conditions regarding the use of a certificate.



## **Certificate management**

Storage, proliferation, issuance, revocation and suspension of certificates. The above functions are performed both by an issuing body and subscriber starting after subscriber's registration and issuance of the relevant certificate. The proliferation and issuance of certificates are governed by the certification policy.

## **Certificate (public key certificate)**

Electronic confirmation issued by a certification authority. It enables the validation of e-signature and identification of a user (individual, server, web site) creating e-signature. It contains at least subscriber's identifier, his public key, validity period and serial number of a certificate and shall be signed by the issuer.

NOTICE: Certificate may be in one of the three basic states (see Cryptographic key states): waiting for activation, active and inactive.

## **Certificate revocation**

Procedures to revoke the validity of a pair of keys (certificate) to prevent a subscriber from the access to the pair and use thereof for, e.g. encryption or signing . The revoked certificate is placed on a certificate revocation list (CRL).

## **Certificate Revocation List (CRL)**

List, signed electronically by a certification authority, that contains serial numbers of revoked or suspended certificates and dates and reasons for their revocation or suspension, a name of CRL issuer, dates of CRL publication and next update. The above data shall be confirmed electronically by a certification authority.

## **Certificate serial number**

Integer or sequence of characters, unique within a certificate issuing body, that explicitly identifies a certificate (e.g. on a CRL). The serial no can be checked through an overlap called 'Details of certificate service window'. Subsequent certificates issued to the same persons carry different numbers.

## **Certificate status token**

Electronic data containing the data on current certificate status, certification path that the certificate belongs to and other data useful for the verification , electronically certified by the certificate validation authority.

## **Certificate status verification authority**

Trusted third party providing relying parties with mechanisms for certificate credibility verification or subject certification statement as well as providing additional information on attributes of the certificate or certification statement.

## **Certificate suspension**

Special form of the revocation of a certificate (and corresponding pair of keys) that results in temporary lack of certificate acceptance in cryptographic operations (irrespective of the status of



such operations); a suspended certificate is listed on a CRL.

### **Certificate update**

Prior to the expiration of a certificate validity period the certification authority may refresh (update) the certificate confirming its validity for the following period of time.

### **Certification application**

Set of documents and data to identify a body subject to the certification.

### **Certification authority**

Entity providing certification services that is a part of a trusted third party, able to create, sign and issue certificates, certification statements and time stamping and certificate status tokens.

### **Certification path**

Ordered sequence of certificates leading from a certificate of a point of trust chosen by a verifier up to a certificate subject to the verification and made to verify certificates. Each certification path may, but not necessarily, be associated with one or more certification policies. Policies assigned to a certain certification path form an intersection of sets of policies the identifiers of which are contained in each certificate belonging to the certification path and identified in their extension certificate Policies.

### **Certification policy**

Document that specifies general rules applied throughout the certification process of public keys. It identifies parties to the process, their obligations and responsibilities, types of certificates and their legal use and identity authentication procedures. Each certification authority issues and uses their own certification policy. The policy can be found in a repository on the Internet.

### **Certification practice code**

Document describing details of public key certification, parties to the above process and a scope of certificate applications. Each certification authority develops its own practice code. CERTUM code can be found in a repository on the Internet.

### **CERTUM**

CERTUM – General Certification Authority, unit providing certification and qualified certification services (certification authority).

### **Co-shared secret**

Part of a cryptographic secret, e.g. of a key, shared by  $n$  trusted users (more precisely: cryptographic tokens, e.g. electronic card) in such a manner that  $m$  ( $m < n$ ) parts be needed to restore it.

### **Cross-certificate**

Public key certificate of a certification authority signed by a certification authority belonging to another domain. It makes it possible to verify a certificate issued by a 'foreign' authority by means



of a certificate issued by 'my' authority. Sometimes it simplifies the certification path. Mutual (cross) certificates provide trusted connections between networks, each possessing its own certification authority. Contrary to their name, the certificates are not always mutually issued ('crosswise').

### **Cross-certification**

Procedure of issuance of a certificate by a certification authority to another authority, not directly or indirectly affiliated with the issuing authority. Two certification authorities may issue cross-certification to each other. A cross-certificate is usually issued to simplify the building and verification of certification paths containing certificates issued by various CA's (certificates issued by one authority are equivalent to the ones issued by another authority).

### **Cryptographic module**

Set of hardware and software performing operations of encryption and decryption in a secure manner.

...

### **Data for audit**

Information on the occurrence of events connected with security measures regarding a computer system and their history that are sufficient for the reenactment, review and assessment of the events and associated actions or lead towards the fulfillment of an operation.

### **Digital / electronic signature**

Data in electronic form that is attached to or logically associated with other data and serves as a method of authentication of a signatory and provides the protection against forgery (providing data integrity); asymmetric digital signature can be generated by certificate subjects with use of a private key and asymmetric algorithm, e.g. RSA.

### **Distinguished name (DN)**

Set of attributes forming a distinguished name of a legal person that distinguishes it from other entities of the same type, e.g. C=US/OU=Business Society Ltd., etc.

...

### **End entity**

Authorized entity using a certificate as a subscriber or a relying party (not applicable to a certification authority).

### **E-signature validation**

Validation aims at 1) verification whether the digital signature has been created by means of a private key corresponding to a public key contained in the subscriber's certificate certified by the certification authority, 2) whether the signed message (document) has not been modified since the signature creation.

...

### **Key management**



Generation, storage, distribution, use, removal and archiving of keys. The distribution and issuance of keys are governed by the certification policy.

### **Key state transformations**

State of a key may be changed only when one of the following transformations occurs (according to ISO/IEC 11770-1 standard):

- generation – key generation process
- activation – makes a key valid and available for cryptographic operations
- deactivation – imposes constraints on a key; such a situation may occur in case of the expiration of key validity or revocation of the key
- reactivation – allows further use of an inactive certificate for cryptographic operations
- destruction – results in the termination of a key life cycle; this notion means the key logical destruction as well as the real, physical key destruction

...

### **Main point of registration**

Registration point that accredits other registration points and can generate pairs of keys on behalf of a certification authority for further certification process.

...

### **OCSP (Online Certificate Status Protocol)**

A service which provides on-line information on the status of a given non-qualified certificate (correct, revoked or unknown).

...

### **Personal Identification Number (PIN)**

Code securing a cryptographic card against unauthorized use.

### **Personal Unlocking Key (PUK)**

Code used for unlocking a cryptographic card and changing the PIN.

### **Point of registration**

Place where a customer is provided with complete range of certification services. Main tasks of the point of registration:

- providing information on possible applications of e-signature for personal or commercial, conditions of its application and use, its consequences and a procedure for purchasing a certificate
- presenting author's software for the creation and verification of the signature (on request)
- receiving subscriber's documents used to confirm his identification, check authenticity, make copies and confirm conformity with originals
- filling in an application for the issuance of a qualified certificate (filled in by an operator, the application is then printed and signed by the applicant and operator)
- printing and signing an agreement (required number of copies)
- issuance of certificates on the grounds of applications for qualified certificates



- selling certificates on a card and kits for creating a secure signature

### **Point of trust**

The most trusted certification authority that does not have to be certified by another authority. A certificate of such an authority is the first step on a certification path created by a subscriber or a relying party. The choice of the point of trust is usually enforced by the certification policy governing the operation of a certificate issuer. The point of trust can be automatically chosen from among authorities that have been pre-qualified by software producers.

### **Private key**

One of two asymmetric keys known only to a subscriber. In case of asymmetric key system, a private key is used for signature creation. In case of asymmetric encryption system, a private key is used for decryption.

A private key shall be carefully protected against the disclosure. The disclosure of a key may result in use thereof (signature creation or decryption of data) by unauthorized parties, that is why private keys for certificates of higher credibility are stored on a smart card and cannot be copied.

### **Proof of possession of private key (POP)**

Submitting the proof a user makes it possible to associate him with a public key. Such associations are verified at CERTUM by a registration point and certificate issuing body. Any given message shall be signed to prove the possession of the private key. The successful signature verification by means of a public key lays ground for assuming the possession of the private key of the same pair. The encryption of any message is proof in case of decryption keys.

### **Public key**

One of two asymmetric keys, accessible to the public and whose connection with a certain individual (or organization) is confirmed by a certificate. In case of asymmetric signature system, a public key is used for signature validation. In case of asymmetric encryption system, a public key is used for encryption.

### **Public Key Infrastructure (PKI)**

System for secure exchange of information that consists of hardware, software, staff, processes, policies and legal obligations. The system provides public key certificates and data on their validity. It provides a verifiable bond between a public key and an owner of a related private key. The PKI also includes certification authorities, registration points, repository.

...

### **Qualified certificate**

Certificate that meets requirements of the 'Act on Electronic Signature' and is issued by a qualified certification service provider. A signature created by means of a certificate and a secure device is legally equivalent to a personal signature. The requirements of the said Act and relevant executive regulations regard, inter alia, equipment security standards, uniqueness of certain data and customer service methods.

...



## **Regulations on CERTUM Certification Services**

Document governing main rights and obligations of parties to contracts for providing qualified certification services. The document forms an integral part of the contract for a qualified certificate.

### **Relying party**

Recipient of encrypted or electronically signed information. The recipient decides whether to accept or reject a signature on the basis of the data contained in the certificate, information on the issuing entity and certification policy. Pursuant to provisions of the certification policy the recipient shall thoroughly verify each signature.

It shall be noted, however, that too reckless acceptance of a signature might be risky. The digital signature does not release from the application of standard security measures – it just provides guarantee of origin (confirmed identity of a sender) and integrity of data subject to verification.

### **Repository**

On-line available databases containing issued certificates, documents related to operations of CERTUM, certification policy, lists of registration points.

### **Revoked certificate**

Certificate placed on a Certificate Revocation List (CRL) without cancellation of a reason for the revocation.

...

### **Secret**

Unique, confidential information transferred to a certificate user. It is used for the identification of the user upon the application for the revocation of a certificate.

### **Secure electronic signature**

Pursuant to provisions of the 'Act on Electronic Signature' a secure electronic signature is:

- uniquely linked to a signatory,
- created using secure creation device and signature creation data that a signatory can maintain under his sole control,
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

This is an e-signatory that is equivalent to a personal signature and can be used to sign declarations of will, tax declarations, applications, quotations, contracts, etc. Such a signature can only be created with use of a qualified certificate.

### **Security policy**

Set of rules that govern the use, processing, storage, distribution and presentation of information. It provides the reliability of an information system, in particular, the protection of data contained therein. It also specifies a plan or a schedule of actions adopted to maintain the assumed level of security.



### **Self-signed certificate**

Public key certificate issued by a certification authority for itself: a subject of the certificate is at the same time an issuer. A signature of the issuer is validated by a public key contained in the certificate itself. Certificates of the main certification authorities are of this particular type.

### **Signature creation data**

Unique data assigned to a certain person and used to create e-signature (private key of a certificate). The data shall be kept confidential; in case of disclosure thereof, a certificate shall be revoked.

### **States of cryptographic key (private, public)**

Cryptographic keys may have one of the three basic states (acc. to ISO/IEC 11770-1 standard):

- waiting for activation (ready) – the key has already been generated but is not available for use
- active – the key may be used in cryptographic operations (e.g. creation of e-signature)
- inactive – the key may be used for e-signature validation or decryption only

### **Subject of certificate**

Certificate possessor indicated in a field called 'subject' in a public key certificate. A subject can be an individual, organization or a piece of equipment (e.g. server, www).

### **Subscriber**

Entity (individual, legal person, body without legal personality, a piece of equipment under custody of the aforementioned or organization) that is a subject shown or identified in a certificate issued thereto or possesses a private key associated with a public key contained in the certificate and does not issue certificates to other parties itself.

### **Subscriber's sponsor (payer)**

Organization financing certification services for the benefit of its representative – certificate user. The sponsor owns a certificate and has right to revoke it.

...

### **Time stamp authority (TSA)**

Entity providing certification services that issues time stamping tokens.

### **Time stamp token**

Electronic data binding existence of a message (data) in a specified, trusted moment of time. Time stamp is certified by the time stamping certification authority.

### **Time stamping**

Services by which data in electronic form linked to data identified by e-signature or electronic confirmation is marked with the specification of exact time at the moment of providing the services and at the moment of electronic confirmation of the result data by the certification service provider.



### **Token**

Element of data used for exchange between parties. Tokens contain information transformed by means of cryptographic techniques. A token may be signed by a registration authority operator and used for the authentication of its holder while dealing with the certification authority.

### **Trusted path**

Inheritance of trust in keys of a certification authority (CERTUM) connected with storage of the certificates in user's computer software.

### **Trusted Third Party (TTP)**

Organization or its representative trusted by an authenticated entity and/or entity performing verification and other entities in the area of operations associated with security and authentication.

...

### **Valid certificate**

Certificate is valid when and only when:

- it has been issued by a certification authority
- has been accepted by the subscriber (subject of the certificate)
- has not been revoked

### **Violation (e.g. data breach)**

Disclosure of the information to unauthorized persons or such interference that violates the system security policy resulting in unauthorized (intended or unintentional) disclosure, modification, destruction or revelation of any object.

...

### **X.500**

International standard specifying Directory Access Protocol and Directory Service Protocol.

...