UNIZETO

CERTUM

CENTRUM CERTYFIKACJI

Certification Policy
Unizeto CERTUM – CCP

Version 1.27

Effective date: 14th January, 2002

Status: previous

UNIZETO Sp. z o.o.
„Unizeto CERTUM Certification Authority"
Królowej Korony Polskiej Street 21
70-486 Szczecin
Poland
http://www.certum.pl

Trademark and Copyright notices

All the questions, concerning copyrights, should be addressed to Unizeto Sp. z o.o., Królowej Korony Polskiej Street 21, 70-486 Szczecin, Poland, tel. +48 91 4801 201, fax +48 91 4801 220, email: info@certum.pl.

Content

1. Introduction

CA Certum Certification Policy sets forth general principles used by CA Certum during public keys certification process, defines parties of these process, their obligations and responsibilities, types of certificates, verification and authentication procedures applicable during issuance of certificate and usage of such certificates. Detailed information are disclosed in Certification Practice Statement. Knowledge of the nature and target of **Certification Policy**, as well as **Certificate Practice Statement** is essentially important for subscribers as well as for relying parties.

2.Certificates

Certificate is a string of data (message), including at least name and identification of issuer, identification of subscriber, his public key and validity period, serial number of certificate. Certificate is signed with CA Certum signing key.

CA Certum issuing certificates to subscribers verifies their authenticity and proves the possession of public key by specific entities. Relying parties, upon receiving signed message, can verify the authenticity of signing entity, whose certificate was used and draw consequences from actions taken or pledges made.

2.1. Types of certificates

CA Certum issues certificates in four distinct levels corresponding to specific level of trust. Reliability of certificate depends on subscriber identification procedure used and effort put in validation of subscriber data received in certificate request. The higher the level of complication of procedure, the higher the reliability of certificate. Certificate Class may also correspond security level of operating system or service of router or server being certified. System engineers of CA Certum may verify technical condition and security level of information system before issuance of certificate of highest level of trust.

Subscriber is expected to choose what type of certificate will be suitable for his purposes. Types of certificates are described in details in Certificate Practice Statement. Information are also available by the use of electronic mail at address: info@certum.pl.

3.CA Certum warranties

Depending on class and type of issued certificate, CA Certum warranties that appropriate measures were taken to verify information placed in certificate (see http://www.certum.pl/CPS: Warranties). Such verification is extremely important to relying parties, which are destination of subscribers messages, certified with CA Certum certificates. Due to this, CA Certum is financially liable for damages and errors arising from CA Certum acts, failure to acts or negligence. Liability cap depends on level and type of certificate and may apply to subscriber and relying parties as well (see http://www.certum.pl/CPS: CA Certum Responsibilities)

CA Certum guaranties may be determined by many circumstances. Knowledge of this circumstances is proved by subscriber is appropriate statement (see http://www.certum.pl/CPS: Certificate acceptance). CA Certum guaranties uniqueness of entities private and public keys.

4. Certificate Acceptance

Responsibilities and liability of CA Certum are becoming applicable at the moment of acceptance of issued certificate by subscriber. General circumstances and method of acceptance is specified in Certificate Practice Statement (see http://www.certum.pl/CPS: Certificate Acceptance). Details are provided in subscriber's statement, depending on type and level of issued certificate (see http://www.certum.pl/CPS: Subscriber's Statement, Relying Party Statement, Server Certificate Subscriber Statement).

5. Certification Service

CA Certum within its infrastructure provides four basic services: (1) registration and issuance of certificate, (2) renewal of certificate, (3) revocation of certificate and (4) verification of certificate status. Other services: (5) Time Stamping Authority, (6) Notary Authority, (7) Electronic Vault, (8) Delivery Authority, (9) Online Certificate Status Protocol are non-repudiation services and can be provided independently of CA Certum.

Registration is used to verify the identity of subscriber and is also initial process of **certificate issuance** (see http://www.certum.pl/CPS: Registration and certificate issuance).

Certificate renewal is applicable to registered subscriber who wants to certify new public key or modify data in existing certificate eg. email address (see http://www.certum.pl/CPS: Certificate Renewal).

Certificate revocation is made if private key that relates to the public key contained in existing certificate or device containing such a key is - or is suspected to be - compromised (see http://www.certum.pl/CPS: Certificate Revocation)

Verification of certificate status: CA Certum determines the authenticity of issued certificate, whether it was placed on certificate revocation list and whether its validity period was not exceeded. Verification of certificate status may also be made with OCSP (see http://www.certum.pl/CPS: Verification of Certificate Status)

CA Certum requires key pairs (public and private) to be generated by subscriber. CA Certum may recommend tools for generating key pair. In exceptional cases CA Certum may generate unique key pair and deliver it to subscriber.

6. Relying Party

Relying parties are obligated to proper verification of every digital sign placed on document (including certificates) they receive. During verification process relying party should use means and procedures available at CA Certum. relying parties are obligated to use certificate revocation list (CRL) published by CA Certum and verification of certification path (see http://www.certum.pl/CPS: Relying Party Obligations).

Each document with detected defect in digital sign or corresponding doubts, should be rejected or subjected to other verification procedures eg. notary verification.

7. Subscriber

Subscriber is obligated to store his private key securely, protecting it from disclosure to third parties. In case of compromise or suspect of compromise subscriber is obligated to inform issuing CA about such compromise immediately. Information should be transferred to CA Certum in the means identifying source of information undeniably.

8. Actualization of Certification Policy

CA Certum Certification Policy is subjected to periodical modification. Such modifications will be made available to each subscriber and their final form accepted by Certificate Policy Authority. Subscribers who don't accept such modification should send suitable notification to CA Certum and cease usage of CA Certum services.

9. Fees

Services provided by CA Certum are commercial. Height of fees is determined by level of issued or existing certificate and type of requested service (see http://www.certum.pl/repository).

Document History

Document modification history		
V 1.0	15th April, 2000	Draft of the document for the discussion
V 1.27	12th March, 2002	Entire version of the document. Document approved