Certification Policy
Unizeto CERTUM – CCP

Version 2.0

Effective date: 15th July, 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

Content

1. Introduction

Unizeto Certum Certification Policy describes general rules and regulations applied by Unizeto CERTUM for public key certification process and usage of Notary Authority (DVCS), Time-Stamping Authority (TSA) and remaining non-repudiation services. Document defines parties of this processes, their responsibilities and obligations, types of certificates, types of confirmations, identity verification procedures and applicability range. Detailed description of the above rules is presented in Certification Practice Statement. The knowledge of the nature, goal and role of the Certification Policy, as well as Certification Practice Statement is particularly important from the point of view of the subscriber and relying party.

2. Certificates

Certificate is the a string of data (message), containing at least name and identifier of authority issuing the certificate, subscriber's identifier, his/her/its public key, validity period, serial number and signed by the authority **Certum CA**.

Certum CA upon issuance of the certificate to the subscriber confirms his/her identity or the credibility of other data, such as email address box. It also confirms, the public key possessed by such subscriber is the property of this very subscriber. Due to above, the relying party upon reception of signed message is able to verify the owner of the certificate, which signed the message and, optionally, account him/her of the actions he/she performed or obligations he/she made.

Unizeto CERTUM provides services in accordance with the *WebTrust*™ (see http://www.webtrust.org) requirements for the certification authorities. Certification authority keys are protected with the hardware security module. The authority implemented physical and procedural controls of the system. Unizeto CERTUM issues certificates in four level of distinctive credibility. Credibility of the certificate depends of enforced subscriber's identity verification procedure and the effort used by Unizeto CERTUM verifiers to verify the data submitted by the requester in his/her/its registration application. The more complicated such procedure is, the more reliable the certificate is. The level of the certificate may depend of the level of the security of the operating system or service server of the network hardware device subjected to the certification. Unizeto CERTUM system engineers may verify the technical state and the security level of the information system prior to the issuance of the certificate of highest (Level IV) credibility level.

2.1. Level I Certificates

Level I certificates are issued by intermediate authority **Certum Level I.** This certificates are intended mainly for the application or device test performance prior to purchasing final certificate. Certum Level I issues certificates for all purposes and verifies the data provided by the subscriber in the certification process. In most cases email box address and name and surname of the private entity or the representative of the legal entity are subjected to verification. Certificates of Level I, issued to end subscribers, contain identifier of the policy governing the issuance of the certificate. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-
certum(2) id-certum-level-I(1)
```

Unizeto CERTUM does not bear any financial liability and no warranties apply to the certificates (and their content) issued within above policy.

2.2. Level II Certificates

Level II certificates are issued by intermediate authority **Certum Level II.** This certificates are intended mainly for the securing electronic correspondence, encrypting binary objects and protecting data transmission. Operators of Certum Level II authority verify the information provided by the requesters during the certification process. A names of the companies and organizations, as well as authenticity of the email box addresses provided in the certificates are the main objects of verification. An identity of the person, acting on behalf of the legal entity is subjected to detailed verification. It is not recommended to unambiguously verify the identity of the subject of the certificate on the basis of Certum Level II ID's. Certificates of Level II, issued to end subscribers, contain identifier of the policy governing the issuance of the certificate. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-
certum(2) id-certum-level-II(2)
```

Financial responsibility of Unizeto CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl/CPS). Certificates issued within this policy have limited guarantees and responsibilities.

2.3. Level III Certificates

Level III certificates are issued by the intermediate authority **Certum Level III.** This certificates are intended mainly for the securing electronic correspondence, securing binary objects against forgery and protecting data transmission on the basis of SSL and TLS protocol. Operators of Certum Level III authority verify the information provided by the requesters during the certification process. All the data contained within the certificate are subjected to verification. Additional documents, confirming the right to provided internet domain name and the authenticity of the corporation are required. It is possible to unambiguously verify the identity of a subject or authenticity of the organization on the basis of the Certum Level III ID's. Certificates of Level III, issued to end subscribers, contain identifier of the policy governing the issuance of the certificate. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-
certum(2) id-certum-level-III(3)
```

Financial responsibility of Unizeto CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl/CPS). Certificates issued within this policy have full guarantees and responsibilities.

2.4. Level IV Certificates

Level IV certificates are issued by the intermediate authority **Certum Level IV.** This certificates are intended mainly for the certification authorities, non-repudiation authorities and global network-based electronic transaction systems. Operators of Certum Level IV authority verify the identity of the requester, who has attend in person the point of registration. Authorization to act on behalf of the company, authenticity and correctness of provided identity documents and documents of organization are subjected to verification. Certum Level IV authority also accepts authenticity and identity documents confirmed by the notary. It is possible to unambiguously verify the identity of a subject, authenticity of the organization or credibility of the external certification authority on the basis of the Certum Level IV ID's. Validity period of the certificates of Level IV is set to 2 years or more. It is required to protect keys of the subscriber in hardware security module. Certificates of Level IV, issued to end subscribers, contain identifier of the policy governing the issuance of the certificate. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-
certum(2) id-certum-level-IV(4)
```

Financial responsibility of Unizeto CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl/CPS). Certificates issued within this policy have full guarantees and responsibilities.

Subscriber should decide by his/her/its own, which type of the certificate will be most appropriate for his/her/its needs. The typed of the certificates are described in details in Certification Practice Statement, presented on the WWW pages. This information are also available by the means of electronic mail, directed to: info@certum.pl.

3. Non-repudiation tokens

Non-repudiation token is the string of data (message), containing at least information provided by the client (e.g. cryptographic hash, serial number of certificate, number of request, etc.) to one of the non-repudiation authority and signed electronically by that authority. Non-repudiation authorities, providing services for their clients are affiliated by the **CA-Certum**.

Non-repudiation authority, upon tokens issuance confirms the occurrence of an event in the past or in that moment. This event might be submission of the electronic document, date of signature creation, etc. Relying party on the basis of received data accepts the certificate and verifies the correctness of the signature relying on the trustiness of **CA-Certum**.

3.1. Time-Stamps

Time-stamps are issued by intermediate authority **Certum Time-Stamping Authority**. Time-stamps, as the confirmation of non-repudiation, are issued to private and commercial customers. Time stamps may be incorporated in electronic signature creation, acceptance of electronic transactions, archive of the data, notary of electronic documents, etc. The regulations concerning operation of Time Stamp Authority and additional information associated with this system are described in separate document (see **Certum Time-Stamping Authority Policy**).

Time stamp token contain identifier of the policy governing the issuance of the token. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-time-stamping(5)
```

Financial responsibility of Unizeto CERTUM for the date, time and additional information in the timestamps issued within above policy is presented in **Time Stamp Authority Policy** (see http://www.certum.pl/CPS). **Certum Time-Stamping Authority** gives full guarantees for issued timestamps. Information concerning fees for timestamps are presented on WWW page (see http://www.certum.pl/repository).

3.2. DVCS tokens

DVCS tokens are issued by intermediate authority **Certum Notary Authority**. This tokens, as confirmations of non-repudiation, are issued to private and commercial customers. DVCS certificates may be incorporated mainly in verification of certificates issued in the past, notary of the documents and electronic transactions and verification of electronic signatures. The regulations concerning operation of Time Stamp Authority and additional information associated with this system are described on WWW page (see http://www.certum.pl).

DVCS tokens contain identifier of the policy governing the issuance of the dvcs token. This identifier has a following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-notary-authority(6)
```

Financial responsibility of Unizeto CERTUM for information in the DVCS certificate and archive time of the DVCS certificates issued within above policy is controlled by separate agreement with the customers. Certum Notary Authority gives full guarantees for issued DVCS certificates. Information concerning fees for electronic notary services are presented on WWW page (see http://www.certum.pl/repository).

3.3. OCSP confirmation response

OCSP (*Online Certificate Status Protocol*) confirmation response are issued by intermediate authority **Certum Validation Service**. This documents, as confirmations of non-repudiation, are issued to private and commercial customers. OCSP may be incorporated mainly in verification of the status of the certificates. This services are available to public and are the alternative for the Certificate Revocation List (CRL). Certum Notary Authority gives full guarantees for issued DVCS certificates. Information concerning OCSP authority operation and additional information concerning provided services are presented on WWW page (see http://www.certum.pl/repository).

4. Unizeto CERTUM guarantees

Depending on type of issued certificate, Unizeto CERTUM guarantees, that it uses reasonable efforts to verify information included in the certificates (see Certification Practice

Statement – Chapter 2.1: Obligations). This verification is particularly important from the point of view of the relying party, who is the addressee of subscriber's messages, confirmed with the certificates issued by Unizeto CERTUM. Due to above, Unizeto CERTUM is financially responsible for every damages resulting from Unizeto CERTUM fault or negligence. Range of the liability and liability cap depends of the level of subscriber's certificate and might include not only the subscriber but the relying party as well (see Certification Practice Statement – Chapter 2.2: Liability).

Unizeto CERTUM guarantees might be limited with many restrictions. Knowledge of this restrictions is confirmed by the subscriber in appropriate statement (see Certificate Acceptance). Unizeto CERTUM guarantees uniqueness of electronic signatures of its subscriber's.

5. Certificate Acceptance

Unizeto CERTUM liabilities and guarantees enter are applicable since the moment of acceptance of issued certificate by a subscriber. General provision and method of certificate acceptance are described in Certification Practice Statement (see Certificate Acceptance), whereas detailed – in subscriber's statement, dependant of a type of issued certificate (see Subscriber's Statement, Relying Party Statement, Statement of Subscriber of Server Certificate).

6. Certification Service

Unizeto CERTUM, within its infrastructure, provides four basic services: (1) registration and issuance of a certificate, (2) renewal of the certificate, (3), revocation of the certificate and (4) verification of certificate status. Remaining services: (5) Time-Stamping Authority (TSA), (6) Notary Authority (DVCS), (7) Electronic Vault, (8) Delivery Authority, (9) Online Certificate Status Protocol (OCSP) are non-repudiation services and may be provided irrespectively of Unizeto CERTUM.

Registration is intended for confirming identity of a subscriber and proceeds issuance of a certificate (see Certification Practice Statement, Chapter 4.1 Application Submission and Chapter 4.3 Certificate Issuance).

Renewal of a certificate is used when registered subscriber wishes to obtain certificate of a new public key or modify any of the data contained within the certificate, e.g. email box address (see Certification Practice Statement, Chapter 4.9 Certification and Rekey).

Revocation of a certificates is used when private key, associated with public key, contained within the certificate or a media used for private key storage is or is suspected to be revealed (see Certification Practice Statement, Chapter 4.9 Revocation and Suspension of a Certificate).

Verification of certificate status applies Unizeto CERTUM confirmation of validity of certificate issued by Unizeto CERTUM, check against placement on CRL and conformation of issuance by one of the affiliated authorities. Verification of certificate status may be also carried out by OCSP (see Certification Practice Statement, Chapter 4.9.11 On-line certificate status verification availability)

Unizeto CERTUM requires every key pair (private an public) to be generated by the subscriber. Unizeto CERTUM may recommend devices which allow key pair generation. In particular cases Unizeto CERTUM might generate unique key pair on its own and deliver it to the subscriber.

7. Relying Party

Relying party is obligated to appropriate verification of every electronic signatures created on the document (including the certificate), he/she/it receives. During verification process, relying party should incorporate procedures and resources available to public in Unizeto CERTUM. It applies, among others, to the requirement of verification of CRL published by Unizeto CERTUM and allowable certification paths (see Certification Practice Statement, Chapter 2.1.4 Relying Party Obligations).

Every document containing deficiency in electronic signature or resulting from this deficiency doubts should be rejected or, optionally, subjected to other means or procedures of validity verification, e.g. notary verification.

8. Subscriber

Subscriber is obligated to securely store his/her/its private key, prevention it from being revealed to any third party. In case of private key revelation or suspicion of such revelation, the subscriber must immediately notify the authority which issued his/her/its certificate. Information about the revelation must be delivered in the manner not arising doubts to the identity of person revoking the certificate.

9. Certification Policy Update

Unizeto CERTUM Certification Policy may be subjected to periodical modifications. This modifications will be available to all of the subscribers and their final content will be accepted PKI Services Development Team. Subscribers who does not accept implemented modifications must submit to Unizeto CERTUM appropriate statement and resign from services provided by Unizeto CERTUM.

10. Fees

Certification services, provided by Unizeto CERTUM are commercial. Height of charged fees depend of the level of issued or owned certificate and of type of requested service. Fees are presented in the pricelist, available on WWW page (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
V 2.0	15th July, 2002	Detailed definition of types of certificates. Addition of non-repudiation services.