Certification Policy: CERTUM's Certification Services

Version 2.3

Effective date: 26th of October, 2005

Status: valid

Unizeto Technologies S.A.
(formerly Unizeto Sp. z o.o.)
"CERTUM – Powszechne Centrum Certyfikacji"
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 Technologies S.A., Królowej Korony Polskiej Street 21, 70-486 Szczecin, Poland, tel. +48 91 4801 201, fax +48 91 4801 222, email: info@certum.pl.

Content

1. Introduction

CERTUM's Certification Policy describes general rules and regulations applied by CERTUM – Powszechne Centrum Certyfikacji (further referred to as 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 process, their responsibilities and obligations, types of certificates, identity verification procedures and applicability range. Detailed description of the above rules is disclosed 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 and serial number, signed by the **Certum CA**.

Certum CA upon issuance of the certificate to the subscriber confirms his/her/its identity or the credibility of other data, such as email address. 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.

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. 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 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 on the level of the security of the operating system or service server of the network hardware device subjected to the certification. 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.

The subscriber has to state by himself/herself/itself the credibility level of the certificate most appropriate for his/her/its needs. Types of the certificates and their credibility level are described in detail in Certification Practice Statement. The document is available through web page or electronic mail (addressed to: info@certum.pl).

2.1. Level I Certificates

Level I certificates are issued by intermediate authority **Certum Level I.** These 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 address, address data 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)
```

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.** These certificates are intended mainly for 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. Names of the companies and organizations, as well as authenticity of the email 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 CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl). Certificates issued within this policy have limited guarantees and liabilities.

2.3. Level III Certificates

Level III certificates are issued by the intermediate authority **Certum Level III.** These certificates are intended mainly for 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 CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl). Certificates issued within this policy have full guarantees and liabilities.

2.4. Level IV Certificates

Level IV certificates are issued by the intermediate authority **Certum Level IV.** These 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 in the registration authority. 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 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. Hardware security modules are required for protection of subscriber's private keys. 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 CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl). Certificates issued within this policy have full guarantees and liabilities.

2.5. External authorities certificates

Certificates for external CAs are issued by intermediate certification authority Certum Partners. Entities, whom such certificates are issued to, are subjected to thorough verification, carried out by Unizeto Technologies S.A. operators. Certificates issued by Certum Partners authority are valid for 5 years and require hardware protection of private keys. Policy identifier has the following form:

```
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-
certum(2) id-certum-partners(9)
```

Financial responsibility of CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement** (see http://www.certum.pl).

3. Non-repudiation tokens

Non-repudiation token is a 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 **Certum CA**.

Non-repudiation authority, upon token issuance, confirms the occurrence of an event in the past or in that very moment. This event might be submission of the electronic document, participation in data exchange, 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 credibility of **Certum CA**.

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 the process of electronic signature creation, acceptance of electronic transactions, archive of the data, notary of electronic documents, etc. The regulations concerning operation of Time-Stamping Authority and additional information associated with the 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 CERTUM for the date, time and additional information included in the timestamps issued within above policy is presented in **Time-Stamping Authority Policy** (see http://www.certum.pl). **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).

3.2. DVCS tokens

DVCS tokens are issued by intermediate authority **Certum Notary Authority**. These tokens, as confirmations of non-repudiation, are issued to private and commercial customers. DVCS certificates may be incorporated mainly in the process of verification of certificates issued in the past, notary of the documents and electronic transactions and verification of electronic signatures. The regulations concerning operation of Notary 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 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 CERTUM for information in the DVCS certificate and archive time of the DVCS certificates issued within above policy is governed by separate agreement with the customer. 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).

3.3. OCSP confirmation response

OCSP (*Online Certificate Status Protocol*) tokens are issued by intermediate authority **Certum Validation Service**. These documents, as confirmations of certificate status, are issued to private and commercial customers. OCSP may be incorporated mainly in the process of verification of certificate status. These services are available to public and are the alternative for the Certificate Revocation List (CRL). Information on OCSP authority operation and additional information concerning provided services are presented on WWW page (see http://www.certum.pl).

4. CERTUM guarantees

Depending on type of issued certificate, 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 CERTUM. Due to above, CERTUM is financially responsible for every damages resulting from 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).

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

5. Certificate Acceptance

CERTUM liabilities and guarantees 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, 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 Services

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 CERTUM.

Registration is intended for confirming identity of a subscriber and precedes 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 CERTUM confirmation of validity of certificate issued by CERTUM and check against placement on CRL and certificate's validity period. 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)

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

7. Relying Party

Relying party is obligated to appropriatelly verify 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 CERTUM. It applies, among others, to the requirement of verification of CRL published by CERTUM and verification of 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, preventing 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

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

10. Fees

Certification services, provided by 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).

Document's history

Document modification history		
V 1.0	15th of April, 2000	Draft of the document for the discussion
V 1.27	12th ofMarch, 2002	Entire version of the document. Document approved
V 2.0	15th of July, 2002	Detailed definition of types of certificates. Addition of non-repudiation services.
V 2.1	1st of February, 2005	Extending the policy with services provided by intermediate authority of Certum Partners.
V 2.2	9th of May, 2005	Editorial changes. Change to the company legal form and name (Unizeto Sp. z o.o. changed to Unizeto Technologies S.A,)
V 2.3	26th of October, 2005	Change of service name and logo from Unizeto CERTUM – Centrum Certyfikacji to CERTUM – Powszechne Centrum Certyfikacji.