Certum Time-Stamping Authority Policy

version 1.1

Date: 26th November 2002

Status: previous

Unizeto Sp. z o.o.
ul. Królowej Korony Polskiej 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., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Poland, tel. +48 91 4801 201, fax +48 91 4801 220, email: info@certum.pl.

Foreword

Certum Time-Stamping Authority Policy has been elaborated with participation of many people; lawyers, technical crew and information security specialists. This policy is an integral part of time-stamp service and maintenance.

Contents

Introduction

Certification Policy specifies general rules used by Time-Stamping Authority during issuing tokens containing singed time-stamp. This documents defines participants of this process, specifies their responsibilities, rights and applicability range. Detailed description of this rules is presented in a **Certification Practice Statement**[1]. The structure and content of this Policy is compatible with ETSI[2]. This time-stamping policy addresses *Certum Time-Stamping Authority* via internet service:

http://time.certum.pl

Time-Stamps issued in accordance with this policy may be used, in particular, to protect long-term electronic signature[3], executable code and transactions made in the global network. Additional information and service help is available at: info@certum.pl.

1. Scope

Present document may be used by relaying parties and the subscribers of certification authority affiliated by Unizeto Sp. z o.o. as a base for confirming reliability of services, which are the subject of this document. Time-Stamping Authority Policy is based on public key cryptography, trusted time sources and X.509 certificates.

2. References

Documents containing any information about TSA, procedures, directives, law regulations are placed in footnotes to this policy. Some additional footnotes to the professional literature are placed in the CPS, Chapter *Literature*.

3. Definitions and abbreviations

3.1. Definitions

Time-stamp token – data object used in a process of electronic signature creation, containing information which has been transformed with cryptographic techniques. This token is signed by TSA and is a proof that data object existed before the date placed in this token.

Time-stamping authority – trusted system issuing and managing trusted time-stamps tokens.

Explanations of the others definitions are described in **CPS**, Appendix: *Glossary*.

---

[1] Current **Certification Practice Statement** is available at: https://www.certum.pl/CPS

[2] ETSI TS 102 023 V1.1.1 (2002-04), *Policy requirements for time-stamping authorities.*

[3] IETF RFC 3126, *Electronic Signature Formats for long term electronic signatures*, September 2001

3.2. Abbreviations

TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TST	Time Stamping Token
UTC	Universal Co-ordinated Time (formerly GMT)
PKI	Public Key Infrastructure

Other abbreviations are described in Certum CPS.

4. General concepts

4.1. Time-Stamping Service (TSS)

Data communication infrastructure of Unizeto Sp. z o.o. issuing and managing time-stamping tokens consists of two basic components:

- Technical component which issues time-stamping tokens,
- System logistics managing, monitoring and supervising the issuance of time-stamping tokens.

System logistics assures among others direct access to the reliable UTC time source and proper management of the system program components.

4.2. Time-stamping Authority (TSA)

Data communication infrastructure, which Chapter 4.1 of this document is referring to, which possess trust of Unizeto CERTUM customers and relying parties connected with above certification authority.

4.3. Subscribers

The subscribers may be subjects described in Certification Practice Statement, Chapter 3 *Identification and authentication,* as well as other subjects, especially non-profit organisations.

4.4. General Provision and TSA Policy

This policy is the part of Certification Practice Statement, which regulates operation of Unizeto CERTUM and associated non-repudiation services.

Time-Stamping Authority issues tokens to every interested party without any technical limits. General rule governing the issuance of the tokens is not to charge fees from private persons and non-profit organisations. Regulations describing charging fees from others subjects are described in pricelist, presented on WWW page at:

http://www.certum.pl/repsitory

4.4.1. Purpose

This documents is available to public. Distribution of this document is limited with restrictions described in Certification Practice Statement, Chapter 2.9 *Intellectual Property Right*.

Personnel management, personnel selection and physical security are also described in **CPS**.

4.4.2. Level of specificity

This document describes only general rules of issuing and managing the time-stamp tokens. Detailed description of the system is described in additional documents which in general are non-public. Non-public documents, together with reports, results of the equipment review and results of inner audits are composing documentation set, available solely to authorised personnel and the *WebTrust*[4] auditor. Specification of significant documents being the part of auditor documentation, is presented in Table 1.

Table 1 Important documents connected with TSA policy.

No	Document's name	Status	availability
1.	*Unizeto CERTUM –CCP Certification Practice Statement*	*public*	*http://www.certum.pl/CPS*
2.	*Database technical documentation*	*Non-public*	*Locally – only entitled persons and auditors*
3.	*Procedure for Unizeto CERTUM CA key archive and destruction*	*Non-public*	*Locally – only entitled persons and auditors*
4.	*Emergency System Recovery and Backup Copy Creation Book*	*Non-public*	*Locally – only entitled persons and auditors*
5.	*Procedure for Hardware Security Module Handling*	*Non-public*	*Locally – only entitled persons and auditors*
6.	*Procedure for Unizeto CERTUM CA key generation*	*Non-public*	*Locally – only entitled persons and auditors*
7.	*Server Software Exchange Book*	*Non-public*	*Locally – only entitled persons and auditors*

4.4.3. Approach

This policy has been worked out in general level, and does not describe any technical details according to the data communication system, structure of the organisation, operating procedures or technical protection. This policy does not define the environment in which the time-stamp token system is functioning. Technical and operating details are included in CPS and additional documents, mentioned above.

[4] *WebTrust Principles and Criteria for Certification Authorities* can be found on the website: http://www.webtrust.org

5. Time-stamp policy

5.1. Overview

This policy is a set of rules used during issuing and managing time-stamp tokens and regulating security level for TSA. General rules are placed in Chapter 4.4 *Time-stamp policy and TSA* of this document.

TST are issued with an accuracy of 1 second or higher.

Profile of a public key certificate, which is used by Time-Stamping Authority complies with IETF[5] recommendation. Extensions of certificate issued by superior certification authority **CA-Certum** are described in Certification Practice Statement, Chapter 7.1.2.6 *Cross-certification and non-repudiation certificates*. Profile of basic field of certificate of TSA is described in Table 2.

Tab.2 Profile of basic certificate fields

Field's name	Value or value limit	
Version	Version 3	
Serial Number	Unique value for all certificate issued by certification authorities within Unizeto CERTUM – CCP	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Common Name (CN) =	Certum {CA,Level{I,II,III,IV}}
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (validity period beginning date)	Universal Time Coordinated based. Unizeto CERTUM owns satellite clock controlled by Atomic Frequency Standard. Unizeto CERTUM clock is known as valid world Stratum I service	
Not after (validity period ending date)	Universal Time Coordinated based. Unizeto CERTUM owns satellite clock controlled by Atomic Frequency Standard. Unizeto CERTUM clock is known as valid world Stratum I service	
Subject (Distinguished Name)	Distinguished names comply with the X.501 requirements.	
Subject Public Key Info	Encoded in accordance with RFC 2459, contains information about RSA public keys. Key size is 2048 bits	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 2459.	

Time-stamp Authority, providing the services within the Unizeto CERTUM infrastructure issues time-stamp tokens according to ETSI[6] recommendation. Every time-stamp token includes identifier of authority policy[7], described in Chapter 5.2 *Identification of TSA policy* of this policy.

5.2. Identification of TSA

Information (identifier) of the policy, governing the issuance and management of time-stamp tokens is defined in Table. 3.

[5] IETF RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001

[6] ETSI TS 101 861,Time stamping profile, August 2001

[7] Not applicable for customers using Microsft Authenticode time-stamp tokens

Tab.3 TSA policy identifier

policy identifier	Certification policy name
iso(1) member-body(2) pl(616) organisation(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5))[8]	Certum Time-Stamping Authority Identifies Time-Stamping Authority policy, providing services within CA-Certum.

Identifier of authority policy of TSA, providing services within Unizeto CERTUM **p**ublic key infrastructure is included in every time-stamp token. This policy is available to relaying party and Unizeto CERTUM customers in accordance to the rules described in Chapter 4.4.2 *Level of specificity* of this document.

5.3. Time-stamp applicability

This document does not defines any limits in applicability of TST, issued in accordance to this policy. Time-stamping authority can provide public services in time-stamping of: electronic transaction, forms, archived data, system registers, electronic signature described in the IETF[3] document, etc. TSA can also provide services for the closed corporation systems. Certum TSA issues time-stamp tokens for Microsoft Authenticode technology, as countersignature.

5.4. Conformance

Issued TST include identifiers described in Chapter 5.2 *Identification of TSA* of this document. TSA supports only the requests which include tokens of this policy or does not include any token. In case of a notarisation of electronic transactions it is permitted to support cryptographic hash function service[9] as a request of TST.

TSA authority ensures compliance of provided services with regulations specified in Chapter 6.1 *TSA obligations* of this document and ensures reliability of control mechanism described in Chapter 7 *Requirements on TSA practice* of this policy.

6. Obligations and liability

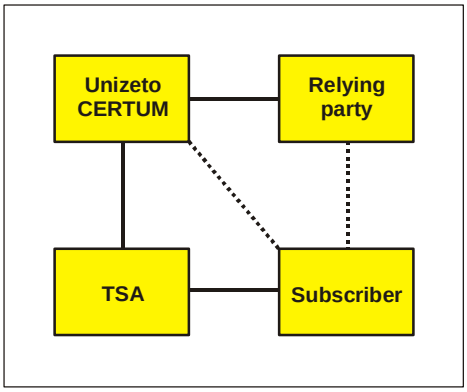
6.1. TSA obligations

6.1.1. General.

This chapter includes all the obligations, liabilities, guarantees and responsibilities of TSA, its subscribers and TST users (relying parties). This obligation and responsibilities are regulated by mutual agreements signed between parties as shown (Picture 1).

[8] identyfikator obiektu Cetum CA: {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) certum(2)}.

[9] NIST FIPS PUB 180-1, *Secure Hash Standard*, April 17, 1995



Pic. 1 Contracts signed between parties.

Unizeto CERTUM agreements (including Certum TSA agreements) with the relaying parties and subscribers describes mutual obligations and responsibilities including Unizeto Sp. z o.o. financial responsibilities.

Certificate Practice Statement and TSA Certification Policy are the integral parts of the agreements signed between Unizeto CERTUM and the subscribers, relying parties and others subjects who are suppliers of public key infrastructure services incl. TST.

Unizeto Sp. z o.o. guarantees, that all the requirements of TSA Authority , incl. procedures, practices related to issuance of a tokens, review of system and security audit are in accordance with regulations described in Chapter 7 *Requirements on TSA practices* of this policy.

TSA acts in accordance with the above procedures. No exclusions of this regulations are allowed. Additional obligations of the authority, subscribers and relying parties are described in Certification Practice Statement, Chapter 2.1 *Obligations*.

6.1.2. TSA obligations towards subscribers.

Unizeto Sp. z o.o. guarantees permanent access to Certum TSA services, due to the course 24/7/365 excluding scheduled technical breaks, disclosed in separate documents, concerning equipment and system conservation. UTC time, which is being placed in TST ensures an accuracy of ±100 ms. Service guarantees proficiency and accuracy with many simultaneous connections (e.g. over 2000 customers) the accuracy can be changed to ±200 ms. In a case of service heavy loading this accuracy may vary.

Moreover, Unizeto Sp. z o.o. guarantees that:

- its commercial activity provided on the basis of reliable equipment and software creating the system, which comply with requirements described in CWA[10],
- its activity and services provided are legal, in particular they does not violate intellectual property, license and other related rights,
- services provided are conforming with generally accepted norms described in Chapter 5.1 *Overview* of this policy,
- issued token does not contain any false data or mistakes

[10] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*

Additional information defining Unizeto CERTUM obligations are described in Certification Practice Statement, Chapter 2.1.1 *Unizeto CERTUM – CCP obligations.*

6.2. Subscribers obligations

Subscriber retrieving TST, should verified electronic signature of the Authority and check CRL, for TSA certificate revocation. Current CRL is available on the website http://crl.certum.pl/ca.crl. TSA identifier verification can be made also with OCSP service usage on the website http://ocsp.certum.pl. Additional subscribers obligations are described in Certification Practice Statement, Chapter 2.1.3 *Subscribers Obligations.*

6.3. Relying party obligations

General obligation of the relying party is verification of TST signature. Relying party should check validity of authority certificate, and its validity period. In case of a verification of the time-stamps, after expiry of the validity of the certificate of TSA the relying parts should:

- verify if TSA identifier have not been placed on CRL ,
- verify if cryptographic hash function used in a token is still secure,
- ensure if size of cryptographic key of TSA and incorporated algorithm is still regarded as a safe,

This policy does not specify any limits according to usage of tokens, except the general agreement conditions, (see Attachment 1). Other requirements towards relying parties are described in Certification Practice Statement, Chapter 2.1.4. *Relying party obligations.*

6.4. Financial liability

The liability of Certum TSA and relying parties connected with the services is the result of routine activity of this subject or the thirds parties. The responsibility of every subject is specified in mutual agreement or is a results of compound statement of will. Liability cap for TSA is presented in Table. 3.

Tab.3 Maximum financial responsibility

Policy name	Subject type	
	Private person	Commercial client
Certum Time-Stamping Authority (OID: 1.2.616.1.113527.2.2.5)	20 000 zł*	20 000 zł*

* - from the subscribers, who does not signed the agreements with Time-Stamping Authority, Unizeto Sp. z o.o. will demand high compensation in a civil process. Above requirements are not applicable for Microsoft Authenticode clients.

The others liabilities and regulations of their provision are described in Certification Practice Statement, Chapter 2.3 *Liability*. Time-stamping with MS Authenticode is absolutely free for private, commercial and non-commercial customers.

7. TSA Requirements

TSA implemented controls, allowing provision of non-repudiation services in accordance with the regulations of this policy. To supervise efficient operation of time-stamping systems, and to account users and the personnel of their activities, all the events in the system are registered.

It is required that every side, related in any way with the procedures of time-stamping should record the information and manage adequately to performed duties. The records of registered information create the event journal and should be save in a manner allowing access of affected parties to proper and appropriate information, required in specific moment, accompaniment in dispute resolving and detection of security of data communication system violation. Recorded events are subjected to backup creation. The copies are stored outside Unizeto Sp. z o.o. seat. The type of registered events is described in Certification Practice Statement, Chapter 4.10.1 *Types of Events.*

7.1. Practice and Disclosure Statements

7.1.1. TSA Practice statement

Procedures, control mechanisms and technical infrastructure described in Chapter 6, *Obligations and liability* of this document are the basis of TSA functioning. Other controls are described in CPS, particularly in Chapter 6.6.1, *System Development Controls* and Chapter 6.6.3, *Life Cycle Security Ratings.*

Vulnerability assessment, relating in the security procedures is described in CPS, Chapter 6.5.1 *Specific Computer Security Technical Requirements*.

TSA policy is a part of CPS, which together with associated internal documents regulates the rules of time-stamping service operation.

CPS regulates the obligations of external subjects related to the time-stamp issuance system. CPS and TSA policy are the documents available to public in accordance with the regulations described in CPS, Chapter 2.9 *Intellectual Property Rights.*

Regulation and procedure creation, their modification and long-term business plans creation is supervised by the PKI Service Development Team. Representatives of the Management, PKI consultants, system engineers and lawyers are part of above Team. Contact with the Team was defined in CPS, Chapter 1.5.1 *Administration Organisation Data*.

Accordance of TSA operation with applicable practice is regulated by resolutions of CPS, Chapter 2.7. *Audit*. Regulation of changes in CPS and in this policy is described in CPS, Chapter 8.1. *CPS Changes procedure*, whereas the process of acceptance of changes is described in CPS, Chapter 8.3. *CPS Approval Procedures*.

7.1.2. TSA Policy Disclosure

CPS and TSA policy are the documents available to public as described in Chapter 7.1.1 *TSA Practice statement* of this document.

The contact information related the content of this document is regulated with resolutions of CPS, Chapter 1.5.1 *Administration Organisation Data*. Every TST issued by Certum TSA include policy identifier, defined in Chapter 5.2 *Identification* of this document. Cryptographic hush functions, used in a time-stamping process are in accordance with normative requirements of NIST[8]. Validity period of time-stamp token is 10 years since the moment of expiry of validity

period of the authority certificate, provided that the situations described in Chapter 6.3 *Relying party obligation* of this document would not occur. Accuracy of the time, which is provided in a TST is regulated in Chapter 6.1.2 *TSA obligations towards subscribers* of this policy.

Limitations related with TSA system have been defined in Chapter 5.3 *Time-stamp applicability* of this policy. Subscribers' obligations are described in Chapter 6.2 while the relying party obligations in Chapter 6.3 of this policy. TST verification should be performed with the usage of the software defined in CPS, Chapter 1.4.2 *Recommended Applications*. Event journal are subjected to archive by the period of time defined in CPS, Chapter 4.11.3 *Archive retention period*. Certum TSA is currently subjected to the Polish law regulations. Liabilities are defined in Chapter 6.4 *Financial obligations* of this policy.

Complaints, suggestions and notices regarding Certum TSA operation should be forwarded to the board defined in CPS, Chapter 1.5.1 *Administration Organisation Data*. Regulations concerning backup copies are disclosed in CPS, Chapter 4.11 *Records archival*. Certum TSA posses emergency facility in case of disaster as well as procedures regulating recovery of the system. Current version of TSA policy is published on the website:

http://www.certum.pl/repository

7.2. Key management life cycle

7.2.1. TSA key generation

TSA keys are generated within hardware security module complying with NIST FIPS 140-1 level 3, by trusted personnel with defined, trusted roles. The description of the requirements of the personnel selection is described in CPS, Chapter 5.3 *Personnel controls*. The environment of TSA keys generation complies with recommendations for the trusted operations systems[11] and fulfils EAL4[12] requirements. TSA key algorithm is described in Chapter 5.1 *Overview* of this policy.

7.2.2. TSA private key protection

The procedures for TSA key recovery in case of a disaster, failure of the system or system conservation are described in separate documents being a part of Unizeto CERTUM documentation and verified periodically by the auditor. The circumstances accompanying TSA key generation as well as suitable procedures are described in CPS, Chapter 6.2. *Private Key Protection*. The security level of the environment and the hardware security module are described in Chapter 7.2.1 *TSA key generation* of this policy.

7.2.3. TSA Public key distribution

TSA certificates, together with corresponding public keys are published within the software, including internet browsers. Additionally this keys are published on the website, at http://www.certum.pl. Public keys of TSA are signed by superior authority **CA-Certum**. Additional information concerning publication of the certificates of public keys are described in CPS, Chapter 6.1.4 *Certification authority public key delivery to relying parties*.

7.2.4. TSA Rekey

TSA rekey procedure is executed upon expiry of validity period of certificate of TSA. Expired keys are archived for the period of 5 years. After this time the keys are destroyed. TSA

[11] http://www.nsa.gov

[12] ISO 15408

public key is stored for additional 20 years to allow verification of time-stamps issued in the past. Key archive is described in CPS, Chapter 6.2.5 *Private Key Archive*.

7.2.5. TSA Key Destruction

Procedures for destruction of the TSA keys are described in CPS, Chapter 6.2.9 *Method of Destroying Private Key*. Additional information are available in Chapter 7.2.4 *TSA Rekey* of this policy. Time-stamp token issuance system, operating within Unizeto CERTUM will reject any request related with the attempts to use expired key.

7.2.6. Hardware Security Module Management

Hardware security modules, intended for non-repudiation services, including time-stamping, are delivered by their manufacturer directly to the seat of Unizeto CERTUM, with the usage of trusted delivery agents. Immediately upon the delivery manufacturer security seals of the on the package are inspected. The module is subsequently transferred to the unit of Unizeto CERTUM, responsible for management of the PKI systems within the Unizeto Sp. z o.o., where the next verification of the manufacturer seals is performed. Basic tests of the unit are executed. The module is stored in a safe-deposit box only accessible by two authorized person. Every above operation should be recorded.

Installation and initiation of the HSM is performed by trusted personnel, in the presence of witnesses. Service functionality tests on the basis of new module are performed in the next step. In a case of removal of the module from usage or transfer of the module for the service, keys from the module are erased and destroyed according to manufacturers recommendations. Unizeto CERTUM has separates procedures, regulating the rules of hardware security module handling. This procedures are not available to public but are the part of documentation verified by the auditor.

7.3. Time-stamping

7.3.1. Time-stamping token

Every TST issued by Certum TSA, shall include an unique identifier of the policy, described in Chapter 5.2 *Identification* of this policy. TST issued by Certum TSA include date and time value time traceable to the real UTC time value, the basic clock is provided by ntp.certum.pl (satellite receiver and atomic standard of second PPS). TSA owns auxiliary clocks in a case of failure of the satellite clock. Accuracy of the time used in TST is defined in Chapter 6.1.2 *Obligations towards subscribers* of this policy. It is not necessary to provide this information within the time-stamp token.

In case of malfunction or decalibration of primary clock, TSA system retrieves the time from auxiliary clock. If the auxiliary clock also decalibrates, rendering impossible the submission of time in accordance with Chapter 6.1.2 *Obligations towards subscribers* of this policy, time-stamp token cannot be issued.

TST are issued on the basis of the data delivered by the subjects requesting TSQ. TSR tokens in the response (time-stamp) include data submitted in the TSQ token. Cryptographic hush function described in NIST[8] standard might also be the request of the TST. TST are signed with the key, which certificate has a profile and extensions described in Chapter 5.1 *Overview* of this policy. TST have the identifier unambiguously binding them with **Certum TSA**. They comply with the requirements of ETSI § 7.3.1h) „Time-stamp token".

7.3.2. Clock Synchronisation with UTC

Certum TSA clock incorporates the time in the TST with the accuracy described in Chapter 6.1.2 *TSA obligations towards subscribers* of this policy. Clock calibration is activated automatically upon discovery of a difference between the universal UTC time and the basic clock higher than ±100 ns. Unizeto Sp. z o.o. owns security controls preventing unauthorized operation, aimed at decalibration of the clock out of order, any manipulation or physical damage to the clock.

Unizeto Sp. z o.o. incorporates controls which allow detection of any difference between the clock time and the time included in TST. Time calculation complies with BIPM[13] and NTP[14] recommendation.

7.4. TSA management and operation

7.4.1. Security management

All the subjects related to security management are described in CPS, Chapter 5.2 *Organizational security controls.*

7.4.2. Risk Assessment

The description of methods and measures undertaken for affirmation of continuity and stability of Certum TSA system operation is described in CPS, Chapter 5.1.1 *Unizeto CERTUM - CCP physical security controls.*

7.4.3. Personnel security

Characteristic of a personnel, as well as the trusted roles they perform is described in CPS, Chapter 5.3 *Personnel Controls*.

7.4.4. Physical and environmental security

The description of physical and environmental security is described in CPS, Chapter 5 *Physical, organizational and personnel security controls*. This security controls comply with ISO[15] normative requirements.

7.4.5. Operations management

Certum TSA system possess the procedural security, according to the WebTrust[4] and ETSI[3] requirements. This documents are mainly the internal company documentation, disclosed periodically to the auditor.

7.4.6. System access management

The problems of access supervision have been described in CPS, Chapter 5.1.1.2 *Physical access.*

---

[13] Bureau International des Poids et Mesures, http://www.bipm.org

[14] Network Time Protocol, http://www.ntp.org

[15] ISO/IEC 17799

7.4.7. Trusted Environment

The generation of the keys in Certum TSA is always performed in trusted environment described in Chapter 7.2.1 *TSA Key generation* of this document. The system comply with the requirements of EAL411. Every changes in the system are monitored and recorded in the event journal.

7.4.8. TSA Key Revelation

In a case of the Certum TSA keys revelation, controls described in CPS, Chapter 4.13 *Key security violation and disaster recovery* should be executed.

7.4.9. TSA termination

In a case of TSA activity termination the controls described in CPS 4.14 *Certification authority termination or service transition* should be executed.

7.4.10. Compliance with legal requirements

Certum TSA system is acting according to the Polish law regulations and other normative requirements defined in Chapter 7.4.10 *Compliance with Legal Requirements* of the ETSI document.

7.4.11. TSA Event Journal

Certum TSA system incorporates event journal mechanisms allowing to recording of every events accompanying TST issuance. This controls are described in CPS, Chapter 4.10 *Certification authority termination or service transition*.

7.5. Organisational Scheme

Certum TSA is a part of Unizeto Sp. z o.o. The organization is incorporated in the area of Republic of Poland. NIP (Tax Identification Number): 852-000-64-44, address Królowej Korony Polskiej 21, 70-486 Szczecin, Poland Tel. +48 91 4801 201. E-mail: info@certum.pl.

The Unizeto Sp. z o.o. organisational structure is presented in *„Organisational structure of Unizeto Sp. z o.o.”*.

Document History

Document change history		
v1.0	05th September, 2002	First version of the policy.
v1.1	26th November, 2002	Added information about time-stamp tokens in Microsoft Authenticode format. New standard of second is described in current document. Other minor changes are applied.