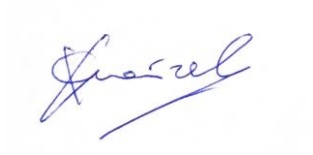
TIME-STAMP CERTIFICATION AUTHORITY POLICY

Version: 2.0

	Position	Name, surname	Date	Signature
Approved by	Executive Director	Konstantin Bezuhanov	*13.04.2017*	
Coordinated by	Representative of the management for ISMS	Stefan Hadzhistoychev	*13.04.2017*	
Developed by	Consultant for ISMS	Mariya Vladimirova	*13.04.2017*	

Date of document registration:	*13.04.2017*
The original is stored at:	*with Representative of the management for ISMS*

Type of copy and consecutive №

Original	X	**Controlled copy**		**Information**	

Distribution of the document:	**Subscriber:**
Internally:	
Externally:	

This document is part of the Information Security Management System of EVROTRUST TECHNOLOGIES INC. Everyone who uses this document shall carry out the ISMS requirements for work with sensitive information.

CONTENT

1. INTRODUCTION

This document represents the Policy and Practice for provision of qualified services for Time-Stamp Certification of the qualified certification services Provider “EVROTRUST TECHNOLOGIES” AD (EVROTRUST/Provider).

This document specifies the general rules, used from the Time-Stamp Certification Authority (“Evrotrust TSA”) for issuing qualified electronic time stamps.

In the “Policy and Practice of the Time-Stamp Certification Authority” are specified the participants in the process of issuing and maintaining user qualification electronic time stamps, as well as their responsibilities, rights and obligations. The applicable range of effect of the electronic time stamps is also specified. A detailed description of those rules is provided in the document “Practice during provision of qualified certification services”.

The structure and contents of this “Policy and Practice for Time-Stamp Certification” was prepared in compliance with the technical specification ETSI TS 102 023.

EVROTRUST executes the “Policy and Practice for Time-Stamp Certification” upon provision of electronic time stamps and publicly provides qualified certification services for provision of qualified electronic time stamps. It can be accessed on: https://www.evrotrust.com.

The qualified electronic time stamp is used by default for exactness of the date and hour specified by it for integrity of the data with which the date and time are connected.

The qualified time stamp issued by EVROTRUST is recognized in all member-states of the European Union.

The qualified electronic time stamp complies with the following requirements:

- it binds the date and time with the data in a way that largely excludes the possibility of unnoticed data change;
- is based on an exact time source associated with coordinated universal time (UTC);
- is signed with an elaborated or qualified electronic signature or is stamped with an elaborated or qualified electronic stamp of EVROTRUST in its capacity as a qualified provider of qualified certification services.

1.1. SCOPE

This document can be used by the relying parties and users of qualified certification services.

EVROTRUST guarantees the reliability of the provided qualified Time-Stamp Certification service through its Time-Stamp Certification Authority, which is an independent and inseparable unit of the Provider.

The provision of qualified electronic time stamps is based on the infrastructure with a public key, secure time sources and certificates format X.509.

2. REFERENCES

This document contains references to standards and standardization documents, procedures, directives, national legislation and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and certification services during electronic transactions on the internal market and repealing Directive 1999/93/EC (Regulation (EU) No 910/2014), including:

- Recommendation ITU-R TF.460-6: „Standard-frequency and time-signal emissions";
- ISO/IEC 19790:2012: „Information technology -- Security techniques -- Security requirements for cryptographic modules";
- ISO/IEC 15408 (parts 1 to 3): „Information technology -- Security techniques -- Evaluation criteria for IT security";
- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
- ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps";
- ETSI EN 319 422: „Electronic Signatures and Infrastructures (ESI); Time-Stampmping protocol and Time-Stamp token profiles";
- FIPS PUB 140-2: „Security Requirements for Cryptographic Modules";
- IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)";
- IETF RFC 5816: „ESSCertIDV2 update to RFC 3161";
- Certification Practice Statement/CPS of "EVROTRUST TECHNOLOGIES" AD;

3. TERMS AND ABBREVIATIONS

3.1. TERMS

- Coordinated Universal Time (UTC) - Coordinated Universal Time reported in accordance with Recommendation ITU-R TF.460-6 [1];
- Network Time Protocol (NTP) - a network protocol that is used by time synchronization programs on one or a network of many information systems;
- Relying Party - a natural person or legal entity who approves electronic time stamp and relies to the facts certified in it;

- User - natural person or legal entity (Signatory/Creator), to whom the service for the issuance of qualified electronic time stamp was provided;
- Electronic time stamp (Time-Stamp) - data in electronic form linking other data in electronic form at a specific point in time and representing evidence that the latest data existed at that time;
- Qualified Electronic Time Stamp - electronic time stamp that meets the requirements of Regulation (EU) No 910/2014;
- Time-Stamp Certification Authority ("Evrotrust TSA") - an internal infrastructure unit within EVROTRUST that issues qualified electronic time stamps;
- Qualified Time-Stamping Service (TSS) - a service for verifying the date and hour of submission of the electronic document;
- Time-Stamp token profiles (TST) - Information object defined in recommendation IETF RFC 3161 (profile of an electronically signed certificate "Evrotrust TSA" for the existence of digital content of an electronic document before a specified moment specified in the certificate, and for unchangeability of this content after this moment. Attached to an electronic signature, the certificate creates irrevocability of the signature in time);
- Time-Stamping Unit (TSU) - configured hardware and software that is managed as a unified system and has an active secret / private key for signing during the provision of the Qualified Time-Stamp Certification Service.

3.2. ABBREVIATIONS

TSA - Time-Stamping Authority
TSS - Time-Stamping Service
TSU - Time-Stamping Unit
TST - Time Stamp Token
UTC - Coordinated Universal Time
PKI - Public Key Infrastructure

4. GENERAL TERMS

4.1. QUALIFIED TIME-STAMP CERTIFICATION SERVICE (TIME-STAMPING SERVICE/TSS)

The data exchange in the infrastructure of EVROTRUST, which is used to issue and manage qualified electronic time stamps, consists of two main components:

- Technological system that issues qualified electronic time stamps, maintains a record and archive of generated time tokens for electronic time stamps;

- Management of the system, which monitors and controls the operations of receiving online requests, issuing, checking and approval of the issued tokens for electronic time stamps.

The system management guarantees direct access to a UTC secure source and reliable management of the technological system components.

The Qualified Time-Stamp Service (TSS) is performed by internal Evrotrust unit - Time-Stamp Certification Authority ("Evrotrust TSA"). The Time-Stamp Certification Authority issues qualified electronic time stamp (Qualified Time-Stamp) through which the Provider's users can certify the time for provision of electronic documents, electronic signatures, electronic transactions, etc. The qualified electronic time stamp is proof that the data object existed at the moment of the time stamping.

In order to do that “Evrotrust TSA” should:

- confirm existence of the data;
- provide evidence that the electronic signature/stamp was affixed with valid pair of cryptographic keys, used for signing/stamping the electronic document or the electronic message;
- not be a party on the arrangements described and marked in the time certificate;
- issue a qualified electronic time stamp in compliance with standard ETSI EN 319 422;
- issue a qualified electronic time stamp which does not contain errors or inexact information.

4.2. TIME-STAMP CERTIFICATION AUTHORITY

“Evrotrust TSA” is a certifying authority in the structure of EVROTRUST, which provides qualified Time-Stamp Certification services. “Evrotrust TSA” is identified in accordance with the conditions stipulated in this document.

The Provider confirms, that “Evrotrust TSA” is subject to audit, at least once every 24 months from a Compliance Evaluation Authority. Within 3 (three) days the report for compliance evaluation is submitted to the Monitoring Authority – the Communications Regulatory Commission.

4.3. USERS

The users are the persons described in the document “Certification Practice Statement”.

When the user is an organization which consists of several end users or an individual end-user, some of the responsibilities related to an organization shall also be applied to the end-users. In any event, the organization is responsible if end-user obligations are not properly executed. Therefore, the organization should inform its end-users about their responsibilities and obligations.

When the user is an end user, he/she is liable if he/she fails to perform his/her duties correctly, under the conditions stipulated in this document.

4.4. GENERAL PROVISIONS OF THE "POLICY AND PRACTICE FOR TIME-STAMP CERTIFICATION"

This document defines a set of rules that EVROTRUST complies with when issuing qualified electronic time stamps.

This document complements the "Practice in the Provision of Qualified Certification Services", which regulates the activity of EVROTRUST and the provision of qualified certification services.

The Provider issues qualified electronic time stamps to any interested party without any technical limitations. The issue of qualified electronic time stamps may be paid or free of charge. Information on fees collected by the Provider can be found on the EVROTRUST website at: https://www.evrotrust.com.

4.4.1. PURPOSE

"Policy and practice for Time-Stamp Certification" is published on the website of the Provider and is available to all stakeholders.

Management and selection of the personnel, the physical and operational security of the activities of EVROTRUST during provision of qualified certified services, are described in the document "Qualified Certification Practice Statement".

4.4.2. SPECIFICS OF THE POLICY AND PRACTICE

The "Policy and Practice of Time-Stamp Certification Authority" describes only the general rules for issuing and management of qualified electronic time stamps.

A detailed description of the technological process is contained in additional documents which are not public.

The unpublicized documents, together with reports, results from external and internal audits are accessible only for authorized persons.

4.4.3. APPROACH

This document was developed in a general plan and does not describe every technical detail from the informational exchange of data, the organizational structure, operational procedures or technical security of the activities of EVROTRUST.

It specifies the rules and conditions which EVROTRUST complies with, in its capacity as a qualified provider of certified services and is an inseparable part of the General Conditions of the contract with the users during provision of qualified electronic time stamps.

5. POLICY OF THE TIME-STAMP CERTIFICATION AUTHORITY

5.1. GENERAL PROVISIONS

The policy of the Time-Stamp Certification Authority defines a set of rules, which EVROTRUST complies with upon issuing qualified time stamps. The provided accurate time versus the Coordinated Universal Time (UTC) is accurate to 0.5 seconds. The Provider guarantees public access to receive and verify the issued qualified time certificates.

EVROTRUST's activity is organized in such a way that the issuance of qualified electronic time stamps is separated from the other activities of the Provider.

EVROTRUST guarantees that appropriate security measures are followed, in accordance with the generally accepted international practice.

The electronic time stamp token profile complies with ETSI EN 319 422.

The Electronic Time Stamp Token (TST) issued by "Evrotrust TSA" contains information for the stamp (TSTinfo structure) located in the SignedData structure (see RFC 2630), signed by "Evrotrust TSA" and embedded in ContentInfo structure (see RFC 2630). The issued time stamps are compliant with RFC 3161 recommendations. The Qualified Time Verification Service issues RSA 2048-bit encrypted qualified electronic time stamps using one of the following algorithms: SHA1 and SHA256.

The certificate profile of "Evrotrust TSA", which verifies the electronic time stamp in the issued electronic time stamp token (TST), is as follows:

Version	V3	
Serial number	38:00:00:00:03:4e:8e:cb:48:09:25:01:bc:00:00:00:00:00:03	
Signature Algorithm	SHA256RSA	
Valid from	160521004013Z	
Validit to	210521005013Z	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust TSA
	OU=	Time Stamping Authority TSS/TSU
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	

Subject Key Identifier	03:BB:3B:42:27:8E:B8:80:90:1B:51:05:DF:52:C4:4B:0F:34:85:B9
Key Usage (critical)	Digital Signature, Non Repudiation
Extended keyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Authority Key Identifier	74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70
Subject alternative name (not critical)	URL=http://www.evrotrust.com RFC822 Name=ca@evrotrust.com
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None

5.2. IDENTIFIER OF THE POLICY OF THE TIME-STAMP CERTIFICATION AUTHORITY

The identifier of this Policy (OID) is: **1.3.6.1.4.1.47272.1.2**

Through the inclusion of this object identified in the issued tokens for electronic time stamp, EVROTRUST confirms compliance with this Policy.

The object identifier described above is in compliance with ETSI BTSP (Best Practices Policy for Time-Stamps) OID=0.4.0.2023.1.1, in accordance with the standard ETSI EN 319 422.

5.3. APPLICABILITY OF ELECTRONIC TIME STAMP

The Policy of the Time-Stamp Certification Authority is directed towards execution of the requirements for qualified time stamps with long validity term (ETSI EN 319 122 [6]), but it is applicable to every other use of time stamps with equivalent requirements.

This document does not specify any limitations in the applicability of the token for electronic time stamp (TST), issued in compliance with this policy.

The qualified Time-Stamp Certification service allows certification of the date and hour of provision of the electronic signature/stamp of every document signed with electronic signature/stamp.

5.4. COMPLIANCE

The issued electronic time stamp token (TST) includes the Policy identifier, described in clause 5.2. The Time-Stamp Certification Authority (“Evrotrust TSA”) executes only requests for electronic time stamps, issued in compliance with this document. “Evrotrust TSA” conducts its activities in compliance with the applicable legislation and standards, and namely:

- Regulation (EU) № 910/2014;
- ETSI TS 119 421;
- IETF RFC 3161;
- IETF RFC 5816.

6. OBLIGATIONS AND RESPONSIBILITY OF THE TIME-STAMP CERTIFICATION AUTHORITY

6.1. OBLIGATIONS

6.1.1. GENERAL OBLIGATIONS

EVROTRUST guarantees compliance of the procedures in this document with the requirements of Regulation (EU) № 910/2014 and the legislation acts applicable to it, as well as with the national legislation. The procedures are subject to control from the Conformity Assessment Body and the Supervisory Body.

6.1.2. OBLIGATIONS TO USERS

EVROTRUST guarantees permanent assess to the Qualified Time-Stamp Certification Service (24/7/365), excluding the time of regular technical maintenance of the technological system.

The provider guarantees public access for receiving and inspection of the issued qualified time stamp tokens. The service for issuing qualified electronic time stamps is with exactness of up to 0.5 (half) second and guarantees the users exactness, even during multiple connections at the same time (for example 100 users).

Besides, EVROTRUST guarantees that:

- uses reliable and secure technological equipment (hardware and software) for provision of the qualified certification service;
- conducts their activities in accordance with the legislation;
- the provided services are complied with commonly accepted international standards and documents, described in “Practice during provision of qualified certification services”;
- the issued electronic time stamp token (TST) does not contain any untrue data or errors;
- does not breach licenses, intellectual property or other rights in the issued electronic time stamp tokens (TST);
- does not allow modification of the digital data after issuing the time stamp token (TST), without establishing it.

6.2. OBLIGATIONS OF THE USERS

The users are obliged to check the validity of the electronic signature of the Time-Stamp Certification Authority and/or the Certificate Revocation List (CRL) upon extraction of the time stamp token (TST).

The updated lists (CRLs) are published on the web page of EVROTRUST on the following address: https://www.evrotrust.com.

Check of the certificate of the Time-Stamp Certification Authority (“Evrotrust TSA”) can also be made by using the service Online Check of the Certificate Status (OCSP): https://www.evrotrust.com.

Additional obligations of the users are described in clause 9.6.3 of the document “Practice During Provision of Qualified Certification Services”.

6.3. OBLIGATIONS OF RELYING PARTIES

The relying party should have the necessary minimum of technical knowledge for using the qualified Time-Stamp Certification service and take the necessary care. The main obligation of the relying party is to check the signature on the electronic time stamp token (TST). The relying party should check the validity of the certificate of Time-Stamp Certification Authority ("Evrotrust TSA"), as well as the validity term of this certificate. In case of check of time stamp, after expiration of the validity term of the certificate of "Evrotrust TSA", the relying parties should:

- make a check in the Certificate Revocation List (CRL) of the certificate of Time-Stamp Certification Authority ("Evrotrust TSA");
- to make check for the applicability of the used hash algorithm;
- to make sure in the security of the used electronic signature by checking the applicable combination of asymmetric and hash algorithms.

Using time stamps should correspond to the requirements of this document and "Practice for provision of qualified certification services".

6.4. RESPONSIBILITY

The responsibility of every person who is participant in the activity for provision and using qualified certification service is settled by the law or is settled in the contract between EVROTRUST and the user.

EVROTRUST is responsible before the users of certification services who count on its activity, for damages caused with intent and gross negligence.

The responsibility of the provider is applicable only, if the damages were caused as direct and immediate consequence of guilty behaviour of EVROTRUST or of the parties, to whom conducting functions in relation to the provision of Time-Stamp Certification services was assigned.

If EVROTRUST confirms and approves that there were damages, it engages to remedy the damaged person. EVROTRUST is liable only to the amount of the real damages.

EVROTRUST signs obligatory insurance for its activities as qualified provider of qualified certification services. The obligatory insurance covers the liability of EVROTRUST to users, correspondingly relying parties, for caused property and non-pecuniary damage up to the limits, specified in the national legislation and this practice.

7. REQUIREMENTS TO THE TIME-STAMP CERTIFICATION AUTHORITY

The Time-Stamp Certification Authority ("Evrotrust TSA") exercises control on its activities, which allows provision of qualified certification service in compliance with the provisions of this Policy. In order to control the effective functioning of the technological time reporting system, user profiles and personnel activity, all events in the system are registered.

EVROTRUST guarantees that it realizes reliably, securely and legally the management of its activities, by controlling all parties, related in some way with the procedures for time reporting, records the information and manages the personnel in appropriate manner in order to execute its obligations correctly. All documents related to the registered information and events are recorded in journal and are archived. Storage of these records is executed in an appropriate manner. Only authorized employees of the Provider have access to the data.

7.1. PRACTICE AND PROCEDURES OF THE TIME-STAMP CERTIFICATION AUTHORITY

7.1.1. PRACTICE

Procedures, control mechanisms, security management and infrastructure management of the Provider are described in detail in the document "Practice during provision of qualified certification services".

The obligations and responsibility of the Time-Stamp Certification Authority are described in clause 6 of this document and are in the base of the functioning of the Certifying Authority.

The inspections allow constant inspection of the integrity of the technological system, duly update and troubleshooting. The exercised monitoring on the functionality of the technological system guarantees that it works correctly and in compliance with the provided production configuration.

The current configuration of the technological system of EVROTRUST as well as all amendments and updates are registered in a controlled manner.

7.1.2. SERVICE ACCESSIBILITY

In order to provide accessibility of the service, EVROTRUST applies the following measures:

- computer system reservation;
- internet connection reservation;
- use of uninterruptible power supplies.

The document “Policy and practice for Time-Stamp Certification” is publicly accessible. This document is published on the website of the Provider on the following address: https://www.evrotrust.com.

7.2. MANAGEMENT OF THE LIFESPAN OF THE KEY PAIR BY THE TIME MANAGEMENT AUTHORITY

7.2.1. GENERATING A PAIR OF KEYS OF THE TIME-STAMP CERTIFICATION AUTHORITY

Generating the signing key of the Time-Stamp Certification Authority (“Evrotrust TSA”) is made in a physically protected environment by persons with trusted roles. Access is two-stage by at least two authorized persons.

Generating the signing key is made in a cryptographic module (HSM) with security level FIPS 140-2, level 3. The generated pair of RSA keys is 2048 bits.

The requirements for the used algorithms and the length of the signing private key are complied with the technical specification ETSI TS 119 312.

7.2.2. PROTECTION OF THE PRIVATE KEY OF THE TIME-STAMP CERTIFICATION AUTHORITY

The private key of the Time-Stamp Certification Authority (“Evrotrust TSA”) is generated and stored in cryptographic module (HSM) corresponding to standard FIPS 140-2, level 3.

The archived copies of the private key of “Evrotrust TSA” are stored in a special safe.

The storage of a copy of the key is made in order to retrieve it in the event of natural disaster or crash of the system. Storage of the key is periodically inspected by the auditor of the Provider. The storage method is described in procedures from the internal documentation of EVROTRUST.

7.2.3. DISTRIBUTION OF THE PUBLIC KEY OF THE TIME-STAMP CERTIFICATION AUTHORITY

The certificate of the Time-Stamp Certification Authority (“Evrotrust TSA”) together with the corresponding public key is published on the web page of EVROTRUST: https://www.evrotrust.com.

The certificate of EVROTRUST is issued by the Root Certification Authority (“Evrotrust RSA Root CA”).

7.2.4. PROLONGING THE TERM AND/OR RE-ISSUING THE PRIVATE KEY OF THE TIME-STAMP CERTIFICATION AUTHORITY

The lifespan of the private key of the Time-Stamp Certification Authority (“Evrotrust TSA”) cannot be longer than the period of time, through which the selected algorithm or key length satisfy the purpose for which they were approved for use. The validity period of the certificate of “Evrotrust TSA” is 5 years. After expiration of this period, the validity term of the certificate is prolonged for another period of 5 years. After this period, a new key pair is generated, and its private key is stored in the cryptomodule (HSM), and the public key is certified by issuing a new certificate to “Evrotrust TSA”. The key pair with expired validity term is stored as follows:

- private key – stored for a period of 10 years;
- public key – stored for a period of 10 years.

All used algorithms are inspected once a year or when changes occur. In case the algorithm is compromised or becomes inappropriate, a regeneration of all affected keys is initiated.

7.2.5. TERMINATION OF THE PRIVATE KEY OF THE TIME-STAMP CERTIFICATION AUTHORITY

After expiration of the validity term of the private key of “Evrotrust TSA”, it is destroyed in a way that it cannot be restored.

7.2.6. MANAGEMENT OF THE LIFESPAN OF THE SIGNING CRYPTOGRAPHIC EQUIPMENT

During transportation and storage, the used cryptographic module is inspected by trusted personnel with double control. The module is expected for:

- damages on security stickers;
- damages of the module box (scratches, indentations);
- damage on the pack.

The following measures are applied additionally:

- the installation, activation and creation of a spare copy of the signing private key of “Evrotrust TSA” in the cryptographic module is executed only by trusted personnel with two-stage control in a physically protected environment;
- in case of scrappage of the cryptographic module, the private keys contained in it will be deleted and destructed in compliance with the recommendation of the producer.

7.3. TIME-STAMP CERTIFICATION (TIME-STAMPING)

The server software of “Evrotrust TSA” implements the technical specification „ETSI TS 101 861 v.1.3.1 (2006-01) Time Stamp Profile” and the international recommendation IETF RFC 3161 (Time Stamp Protocol).

The system software of „Evrotrust TSA" maintains communication with the clients of the service for protocol Time-Stamp Certification: TCP/IP, HTTP/HTTPS.

7.3.1. ELECTRONIC TIME STAMP TOKEN (TIME-STAMPING TOKEN/TST)

Every electronic time stamp token (TST) issued by EVROTRUST includes a unique identifier of the policy of the Time-Stamp Certification Authority.

The request/reply profile of the "Evrotrust TSA" system is in compliance with the technical specifications described above and includes the following attributes/parameters:

- The request for issuing TST (TSQ) includes:

Field	Attributes	Meaning/Value
Version	1	
Message Imprint	Hash Algorithm:	OID of hash SHA-1, SHA-256
	Hash Value:	Hash value of data
Requested Policy		OID=1.3.6.1.4.1.47272.2.1 (corresponds to policy with O.I.D.=0.4.0.2023.1.1)
Nonce		Optional
Certificate Request		If it is TRUE the qualification certificate of Evrotrust TSA turns on
Extensions		not used

- TST reply to the request (TSR) includes:

Field	Attributes	Meaning/Value
Version	1	
Policy		OID=1.3.6.1.4.1.47272.2.1 (corresponds to policy with O.I.D.=0.4.0.2023.1.1)
Message Imprint	Hash Algorithm:	OID of hash SHA-1, SHA-256
	Hash Value:	Hash value of data
Serial Number		Serial number of the certificate
Generated Time		Time of provision of the electronic signature/stamp (UTC certified time)
Accuracy		500ms
Ordering		Not maintained
Nonce		Only if present in the request

TSA		DN=[CN=Evrotrust TSA, OU=TSA, O=Evrotrust Technologies JSC, L=Sofia, S=Sofia, C=BG]
Extensions		not used

7.3.2. SYNCHRONIZATION OF THE CLOCK WITH COORDINATED UNIVERSAL TIME

"Evrotrust TSA" uses hardware source of exactly calibrated time with high degree of exactness. Synchronization of UTC with the source of time is automatic, based on NTP protocol, after establishing difference between the source and time in the system.

In case there is a problem in the hardware during and until its change with a spare one, time servers based in the internet are used as a source of exact time. Synchronization is on the basis of two time sources, through NTP protocol.

The provider guarantees that it provides physical and informational security of the technological system for prevention of unauthorized operations, directed to miscalibration of the clock or its physical damaging.

EVROTRUST has inspections, which allow discovering every difference between the clock and time, included in the electronic time stamp token (TST).

7.4. MANAGEMENT AND ACTIVITY OF THE TIME-STAMP CERTIFICATION AUTHORITY

7.4.1. SECURITY MANAGEMENT

Information security policy is implemented in EVROTRUST. All employees are obliged to comply with the norms of this policy. The Information security policy is reviewed on a regular basis and in case there were problems.

All issues related to the security management are described in the document "Certification Practice Statement".

7.4.2. RISK EVALUATION

In order to provide quality and reliability of the provided services EVROTRUST regularly performs risk assessment. The security inspections defined in the security concept of the Provider are controlled quarterly in order to provide control effectiveness.

Description of the procedures and plans for achieving continuity and security of the Provider's activities are described in the document "Certification Practice Statement " by EVROTRUST TECHNOLOGIES AD.

All systems included in issuing the qualified electronic time stamps provide high degree of reliability.

The technological system is located in a physically protected environment, minimizing the risk of natural disasters.

In case the private key of the Time-Stamp Certification Authority is compromised, the affected cryptomodule (HSM) is immediately isolated from the network, and corrective measures are taken:

- notifying the security administrator in order to undertake further actions;
- initiation of security audit of the rest of the cryptomodules (HSMs) – integrity inspection and journal analysis;
- notifying the relying parties which are affected by the compromising;
- initiation of substitution procedure.

7.4.3. OPERATIONAL SECURITY

EVROTRUST supports qualified employees on positions which provide execution of their obligations at any moment during conducting the activities on issuing electronic time stamp certificates, in compliance with the legislation.

The characteristics of the personnel and the trusted roles of the Provider are in compliance with the document “Certification Practice Statement” from “EVROTRUST TECHNOLOGIES” AD.

7.4.4. PHYSICAL SECURITY

The secure and reliable conducting of operations by the Time-Stamp Certification Authority (“Evrotrust TSA”) is performed by different security levels of the physical and logical access to the technological system.

The provider provides:

- protected physical environment;
- separation of network segments;
- separation of the obligations;
- network and services monitoring;
- provision of computer systems.

In case an employee who is responsible for Time-Stamp Certification activities, changes their role or leaves the company, all belonging carriers related to the security are returned or invalidated.

The physical control and access control are in compliance with the document “Qualified Certification Practice Statement” by “EVROTRUST TECHNOLOGIES” AD.

7.4.5. NETWORK SECURITY

The network infrastructure is divided to zones, based on risk assessment, considering the functional, logical and physical relation between trusted systems and services.

The provider restricts the access and communications to such level, which is necessary for the normal work of the certification services. Connections and services related to the certification services are deactivated. The established rule for access is reviewed periodically.

All elements of the critical infrastructure are kept in a protected environment.

An administrative network was developed, which is separated by the network for operational purposes. The systems used for administration cannot be used for non-administrative activities.

The test and exploitation platform is separated by other environments which have no relation to the work operations.

Communication between remote trusted systems is made only through secure channels, which are logically separated by the other communication channels and provide identification of their end points. Data protection on the channel is provided, against disclosure or modification.

Internet connection is reserved.

The private IP addresses for access are also regularly scanned for liabilities, and then a report is prepared.

Test for system penetration is conducted in the following cases: after the initial setting of the systems and after infrastructural or upgrades of applications and changes. After finishing the test, a report is prepared.

7.4.6. ACTIVITY MANAGEMENT

In every new developed system analysis of the requirements regarding the security is made, during the design and functionality planning stage.

When new versions are released, procedures for control of changes is applied, including in case of urgent changes in the software.

The integrity of the systems and information of the Time-Stamp Certification Authority is protected from viruses, malicious code and unauthorized software. All systems are protected in compliance with the security policy of EVROTRUST.

Handling external carriers in EVROTRUST is made in a secure manner in order to protect them from damage, theft or aging.

Procedures for all trusted and administrative roles related to provision of certification services were implemented.

EVROTRUST has implemented policies providing timely application of security patches (patch/software corrections).

The requirements to the capacity of computer systems are monitored, in order to provide sufficient quantity of calculation capacity and disk space.

7.4.7. SYSTEM ACCESS MANAGEMENT

EVROTRUST provides monitoring on the access to computer systems and user requests regarding:

- unusual system activities showing potential violation of the security, including breach in the network of EVROTRUST and reporting through the alarm system;
- starting and shutting off log functions;
- availability and using services in the network of EVROTRUST.

After every security breach or loss of integrity, which have significant influence on the provided trusted service, as well as on the managed personal data, EVROTRUST communicates it to the Supervisory Authority. After establishing a critical security breach, the Supervisory Authority is notified within 24 hours.

7.4.8. SECURE ENVIRONMENT

The cryptomodule (HSM) with certified with security level FIPS 140-2 Level 3 is the operational environment for storage of the private key of the Time-Stamp Certification Authority and for electronic signing of electronic time stamp tokens (TST), supplied to the users.

Documents relate to the environment security are mostly internal documentation of EVROTRUST and are periodically reviewed by the auditor.

7.4.9. COMPROMISING THE PRIVATE KEY OF THE TIME-STAMP CERTIFICATION AUTHORITY

The provider EVROTRUST takes maximum care within its abilities and resources, to minimize the risk of compromising the private key of the Time-Stamp Certification Authority (“Evrotrust TSA”), as a result of human mistake, natural disasters or emergencies.

In case of compromising or doubt for compromising a private key of the Time-Stamp Certification Authority of EVROTRUST, the following actions are taken:

- immediately terminates the certificate of “Evrotrust TSA”;
- the root authority generates new key pair and new certificate;
- all users and relying parties are informed for the events immediately with information of the web page of the Provider;
- the certificate corresponding to the compromised key is put in the Certificate Revocation List (CRL), together with the appropriate reason for termination;

- immediate analysis is performed and a report for the reason for compromising is prepared.

These operations are performed in compliance with the plan, developed by EVROTRUST for security accidents.

7.4.10. TERMINATION OF THE ACTIVITY OF THE TIME-STAMP CERTIFICATION AUTHORITY

In case of termination of “Evrotrust TSA” the following procedures from the document “Qualified Certification Practice Statement” of “EVROTRUST TECHNOLOGIES” AD are executed:

7.4.11. COMPLIANCE WITH LEGAL REQUIREMENTS

For all matters which are not settled in the “Certification Practice Statement” the provisions of Regulation 910/EU and the applicable legislation are applied.

All requirements for provision of qualified electronic time stamps, arising from this document are in compliance with the requirements of the standards and standardization documents of ETSI, arising from the provisions of Regulation (EU) № 910/2014.

7.4.12. RECORD OF EVENTS

Every evidence for the condition of the technological system and information data is recorded in a secure and reliable manner.

EVROTRUST records and keeps accessible all information related to issued or received data, for the corresponding period of time. These records are stored even after termination of the service.

EVROTRUST provides:

- confidentiality and integrity of the current and archived records, related to the activity of the services in accordance with the good practices;
- records related to the activity of the service can be provided to the competent authorities for the purposes of court proceedings, in case evidence for its correct functioning is needed;
- records of all events related to the lifespan of the keys and certificates of the Time-Stamp Certification Authority is maintained;
- records of all events related to synchronization of the clock of the Time-Stamp Certification Authority with the coordinated universal time (UTC) are maintained. This includes information related to the normal recalibration or synchronization of the clocks, used for provision of qualified electronic time stamps;
- records for all events after establishing loss of synchronization;
- all events are recorded in a manner which makes them hard for deletion.
- journals for events are kept for at least 3 months;

- the journal for the issued qualification time stamps is kept for at least 10 years.

7.5. SCHEME OF ORGANIZATION

EVROTRUST maintains internal documents for the correct work of the Time-Stamp Certification Authority, describing the operational control related to: personnel security, access control, risk assessment, etc. These internal documents are analysed by an independent Authority for evaluation of the compliance in accordance with the requirements of technical specification ETSI TS 119 421.

"EVROTRUST TECHNOLOGIES" AD is a Bulgarian legal entity, a joint-stock-company, entered in the Commercial Register to the Registry Agency with UIC 203397356, with seat and management address:

EVROTRUST TECHNOLOGIES AD
2 Nikolay Haytov Str., entr. D, fl. 2
1113 Sofia, Bulgaria

Telephone:
+ 359 2 448 58 58
Website: http://www.evrotrust.com
E-mail: office@evrotrust.com

Registry of changes																					
Page																					
Valid change																					