ISO 9001:2015 ISO 27001:2013
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

# POLICY AND PRACTICE

# FOR QUALIFIED ELECTRONIC TIME STAMP PROVISIONING SERVICE

**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.

The " Policy and Practice of the Time-Stamp Certification Authority " designates participants in the process of issuing and maintaining qualified electronic time stamps, specifying their responsibilities, rights and obligations. Define the applicable range of electronic time stamps. This document is an integral part of the document "Practice in the provision of Qualified Certification Services". Qualified electronic time stamp issued by Evrotrust is recognized in all EU Member States. Qualified electronic time stamp is based on the presumption of accuracy of the date and time indicated by it, and for the integrity of the data with which the date and time are bound.

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, RFC 3161, ETSI EN 319 401 и EN 319 421.The document is available at: https://www.evrotrust.com

## 1.1. REQUIREMENTS FOR QUALIFIED ELECTRONIC TIME STAMPS

Evrotrust issues qualified electronic time stamps in accordance with the requirements of Art. 42 of Regulation (EU) No 910/2014:

- binds the date and time with the data in a way that largely excludes the possibility of unnoticed data changes;
- is based on a time coordinated by UTC;
- signed with a qualified electronic seal of Evrotrust as a qualified provider of qualified certification services.

The TSU public key certificate is issued by a certifying authority in accordance with the policy set out in ETSI EN 319 411-2. ETSI EN 319 411-2 includes requirements of ETSI EN 319 411-1. Relying parties use a trusted list to determine if the time stamp is qualified. If the public key of the

TSU is included in the list and the service it represents is a qualified service, then the time stamps issued by the TSU can be considered qualified. QcStatement "esi4-qtstStatement-1" as defined in clause 9.1 of ETSI EN 319 422.

## 1.2. SCOPE

This document is publicly available on the Evrotrust website and can be used by Trusted parties and Qualified Certification Services users.

Providing a time stamping service involves generating time stamps and managment (monitoring and controlling) the time stamp generation process to ensure that a service defined by "Evrotrust TSA" is provided. "Evrotrust TSA" is responsible for installing and uninstalling the service for providing time stamps. "Evrotrust TSA" ensures that the clock used for time stamping is properly synchronized with UTC.

## 2. REFERENCES

This document contains references to standards and standardization documents, procedures, directives, national and European legislation:

- 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);
- 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)";

## 3. TERMS AND ABBREVIATIONS

### 3.1. TERMS

**Coordinated Universal Time (UTC)** - Coordinated Universal Time reported in accordance with Recommendation ITU-R TF.460-6;

**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);

**Timestamping 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. The TSU certificate contains the public key of the TSU and is signed with the Root certification authority private key.

### 3.2. ABBREVIATIONS

**TSA -** Time-Stamping Authority

**TSS** - Time-Stamping Service

**TSU** - Time-Stamping Unit

**TST -** Time Stamp Token

**TSQ** - Time Stamp Query

**UTC** - Coordinated Universal Time

**PKI** - Public Key Infrastructure

## 4. GENERAL TERMS

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

Evrotrust issues time certificates under Regulation (EU) No 910/2014 and in full compliance with ETSI EN 319 422, ETSI TS 119 421 and IETF RFC 3161.

The Authority for the Issuance of Qualified Electronic Time Stamps "Evrotrust TSA" is the legal entity Evrotrust as a Qualified Certification Service Provider. "Time-stamping service" is a service of the "Evrotrust TSA" Time Assurance Authority and is provided in accordance with ETSI EN 319 422. By including the object identifier: 1.3.6.1.4.1.47272.1.2.1 in the time/ TST certificates

issued, Evrotrust confirms compliance with the "Policy and Practice of a Service Providing Qualified Electronic Time Stamps". The object identifier complies with ETSI BTSP (best practices policy for time-stamp) OID=0.4.0.2023.1.1 according to ETSI EN 319 422. Time-stamp tokens issued according to RFC 3161.

The Authority for the Issuance of Qualified Electronic Time Stamps "Evrotrust TSA" accepts requests for the issuance of qualified electronic time stamps of the submitted content of an electronic document by a user or a relying party. He / she prepares a qualified electronic time stamp of the submitted hash value of an electronic document and provides for the possibility of subsequent (after the period of validity of the Qualified Electronic Signature / Seal Certificate) proof to the receiving Party of the fact of signing a statement or an electronic document.

Qualified electronic time stamps can be integrated into the process of creating or adopting qualified electronic signature / seal, electronically signed documents and electronic transactions, electronic data archiving, electronic notaries, and more.

To implement its TSS service, Evrotrust uses several private keys. One key pair (of the base authentication authority) is used to issue an electronic certificate used by the TSU in accordance with ETSI EN 319 411-1. One or more key pairs are used by TSU to sign user time certificates. The generating algorithm, signature key length, and signing algorithm used to sign the time certificates is ETSI TS 119 312. All private keys are stored in the FIPS 140-2 Level 3 hardware security module.

"Policy and Practice of a Service Providing Qualified Electronic Time Stamps" refers to ETSI EN 319 401 on the common requirements to any Evrotrust service. The document is intended to meet the requirements for long-term validation (ETSI EN 319 122), but is applicable to any use with equivalent quality requirements.

The time-stamp certification service uses a set of Stratum -1 NTP (Network Time Protocol) servers as an independent time source. With this configuration, TSS achieves time accuracy within +/- 500ms (half second) or better with UTC.

"Evrotrust TSA" guarantees the integrity and authenticity of TSU public keys that are available to trusted parties in TSU certificates at the Evrotrust website at https://www.evrotrust.com.

Time stamps are recorded in a register of issued certificates.

The time stamp service is available at http://ts.evrotrust.com/tsa.

## 4.2. TIME-STAMP CERTIFICATION AUTHORITY („EVROTRUST TSA")

"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.

"Evrotrust TSA" is active in the production of qualified electronic time stamps as follows:

➢ Accepts requests for time-stamping of the submitted content of an electronic document by a user or a Recipient;

➢ Uses technology to link date and time to data in a way that excludes the possibility of unnoticed data change;

➢ Its activity is based on an atomic source of precise time associated with coordinated universal time;

➢ Signs (through TSU) with advanced electronic seal;

➢ Provides the opportunity to prove in the subsequent period (after the expiry of the period of validity of the qualified electronic time stamp) the fact of signing electronic documents or another electronic object;

➢ Qualified electronic time stamps are issued to both physical and legal persons who are users of the service. Qualified electronic time stamping is based on the presumption of accuracy of the date and time indicated by it, and for the integrity of the data with which the date and time are bound.

➢ Qualified electronic time stamp issued by Evrotrust is recognized in all Member States of the European Union.

➢ Qualified electronic time stamps can be integrated in the process of creating, sending or accepting electronic signatures / stamps, electronically signed documents and electronic transactions, electronic data archiving, electronic notaries, etc.

Evrotrust develops and publishes "Policy and Practice of a Service to Provide Qualified

Electronic Time Stamps".

### 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 "Certification practice statement for 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.

** The document is intended for users, relying parties and all interested parties. The management and selection of personnel, the physical and operational security of Evrotrust activities in the provision of qualified certification services are described in the document "Certification practice statement for qualified certification services".*

### 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.

The policy is assigned a unique object identifier: 1.3.6.1.4.1.47272.1.2.

The issued time stamps (TST) have assigned a unique object identifier:

1.3.6.1.4.1.47272.1.2.1.

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.

## 5.2. PROFILE OF THE CERTIFICATE WHICH CERTIFIED THE QUALIFIED ELECTRONIC TIME STAMP

The Certification Authority issues a qualified TSS electronic certificate to sign the Timestamp Tokens (TST) issued by it. RFC 3280 recommends that qualified electronic time stamps certificates in their attribute extensions contain an Extended Key Usage field marked as critical. This means that the certificate can only be used by the TSS service for the purpose of signing of qualified electronic time stamps issued by that authority.

The time-stamp generation system shall reject any attempt to issue time-stamps when the end of the validity of the TSU private key has been reached.

**Main fields in the Qualified Certificate Profile:**

- Version - Version (Version 3);
- Serial Number - a unique time stamp identification code;
- Signature Algorithm - Electronic signature creation algorithm (sha256WithRSAEncryption)
- Issuer (Distinguished Name) - name of the time stamp issuer (Evrotrust TSA);
- Not before (validity period / beginning date) - date and time of issue (universally coordinated time presented in Zulu);
- Not after (validity period ending) - date and time of expiration of validity;
- Subject (Distinguished Name) - Name of Holder / Creator;
- Subject Public Key Info - Encoded field in accordance with RFC 3280, which

contains RSA public key information (key identifier and public key value);

- Signature - an electronic signature generated and encoded in accordance with the requirements described in RFC 3280;
- Basic Constraints - basic constraints of time stamping;
- Key Usage - purpose of the time stamp;
- Extended Key Usage - Time Stamping Authority (TSA);
- Certificate Policies - policy on the basis of which the time stamp was issued;
- Authority Key Identifier - Identifier of the Authority's Key.

Time Stamping Authority TSS / TSU" and "Evrotrust Timestamp TSU" are qualified certificates for qualified electronic seals of the qualified time stamp service. Using them the qualified time stamp service issues and electronically signs qualified time stamp claims - electronic time stamp tokens (TST), using its signing unit (SU).

Time Stamping Authority TSS / TSU qualified electronic seal certificate:

| | | |
|---|---|---|
| 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:<br>Policy Identifier=1.3.6.1.4.1.47272.1.2.1<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>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<br>Distribution Point Name:<br>Full Name:<br>URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl |
| Authority Information Access | [[1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/ocsp |
| Basic Constraints (critical) | Subject Type=End Entity<br>Path Length Constraint=None |

*Thumbprint (SHA1):* 293a771ad7e2921fb4b47a87889658b7e8b22df8

*Thumbprint (SHA256):*

0655c44c917f5846a4b30dd9b6a235715785efe0df327ee0e484c0b90ba8d3b6

The Evrotrust Timestamp TSU qualified electronic printing certificate is:

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 70 32 56 21 2e cf c2 90 20 d4 40 3f 97 57 16 02 a5 d9 d4 50 | |
| Signature Algorithm | SHA256RSA | |
| Issuer | CN= | Evrotrust Services CA |
| | organizationIdentifier | NTRBG-203397356 |
| | O= | Evrotrust Technologies JSC |
| | C= | BG |
| Valid from | 13 July 2019, 15:43:22 UTC | |
| Validit to | 11 July 2024, 15:43:22 UTC | |
| Subject | CN= | Evrotrust Timestamp TSU |
| | organizationIdentifier | NTRBG-203397356 |
| | O= | Evrotrust Technologies JSC |
| | C= | BG |
| Public Key Type/Length | RSA (2048 Bits) | |
| Authority Key Identifier | KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e | |
| Authority Information Access | [1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://services.evrotrust.com/EvrotrustServicesCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://services.evrotrust.com/ocsp | |
| Subject Alternative Name | URL=http://ts.evrotrust.com/tsa | |
| Certificate Policies | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.47272.2.1.2 | |

<table>
<tr><td></td><td>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.evrotrust.com/cps</td></tr>
<tr><td>Extended Key Usage</td><td>Time Stamping (1.3.6.1.5.5.7.3.8)</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td></tr>
<tr><td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations:<br>PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf<br>language=en</td></tr>
</table>
</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Subject Key Identifier</td><td>b9 5c 48 1b a6 46 94 8e d9 7d d3 b4 b1 2f f8 db 30 ac 20 a2</td></tr>
<tr><td>Basic Constrains (critical)</td><td>Subject Type=End Entity<br>Path Length Constraint=None</td></tr>
<tr><td>Key Usage (critical)</td><td>Digital Signature, Non-Repudiation (c0)</td></tr>
</table>

*Thumbprint (SHA1):* 8eecc027c068fe2fa9111d1c169b50e3a156f278

*Thumbprint (SHA256):*

e6ea4eb4b13cbb2dc233dfb7c3c6164efce529b121f47541d5656449173218e1

## 5.3. REQUEST FOR ISSUING OF TIME-STAMP TOKEN (TIME STAMP QUERY/TSQ)

TSS accepts time stamping requests that meet the IETF RFC 3161 and ETSI EN 319 422 specifications. The Time Stamp Query / TSQ that a user sends to the TSS must contain a hash algorithm function, which the user uses. TSS adopts the following algorithms: SHA256, SHA384 and SHA512. For the purpose of service compatibility with existing systems, the algorithms SHA1 and MD5 are also accepted, but Evrotrust not recommending their use and may at any time refuse to accept them.

The request for qualified electronic time stamp may also specify the requested identifier OID = 1.3.6.1.4.1.47272.1.2.1 to be entered in the issued TST.

The request may also contain the so-called NONCE to ensure that the generated TST response (TSR) responds exactly to the user request (TSQ).

The request that the service accepts and validates has the following profile:

| **Field** | **Attributes** | **Meaning/Value** |
|---|---|---|
| Version | 1 | |
| Message Imprint | Hash Algorithm: | OID of the used hash algorithm |
| | Hash Value: | Hash value of the data calculated using the hash algorithm specified in the previous field |
| Requested Policy | | Optional |
| Nonce | | Optional |
| Certificate Request | | If it is TRUE the qualification certificate of Evrotrust TSA turns on |
| Extensions | | not used |

Evrotrust ensures that it does not in any circumstances alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents. If there is an extension/update in policy and practice that will not affect previously issued certificates, Evrotrust presents a new object identifier that covers the new certificates or extended/updated ones. Evrotrust follows internal OID management procedure.

## 5.4. TIME STAMPING TOKEN / TST

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).

Each token for time-stamp (TST) issued by the TSS includes a unique identifier of this policy: OID = 1.3.6.1.4.1.47272.1.2.1.

The service uses the RSA 2048 bit private key to electronically sign the time certificates using the SHA512 algorithm.

The Time Stamp Response / TSR that TSS returns to the user is in accordance with the above technical specifications and includes the following attributes / parameters:

| Field | Attributes | Meaning/Value |
|---|---|---|
| Version | 1 | |
| Policy | | OID=1.3.6.1.4.1.47272.1.2.1<br>(corresponds to policy with O.I.D.=0.4.0.2023.1.1) |
| Message Imprint | Hash Algorithm: | OID of used hash algorithm |
| | Hash Value: | Hash value of the data calculated using the hash algorithm specified in the previous field |
| 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 |

## 5.5 TIMESTAMPING

The server software that uses TSS implements the technical specification ETSI TS 101 861 Time Stamp Profile and the international recommendation IETF RFC 3161 Time Stamp Protocol.

The system software that uses TSS supports communication with protocols authentication time server users: TCP/IP, HTTP/HTTPS.

## 5.6. 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**

The issued time stamps (TST) have assigned a unique object identifier: **1.3.6.1.4.1.47272.1.2.1**. 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.

## 5.7. 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), 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.

### 5.8. COMPLIANCE

The issued electronic time stamp token (TST) includes the Policy identifier, described in clause 5.3. 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 EVROTRUST

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 more than 10 users).

### 6.1.3. OBLIGATIONS TO "EVROTRUST TSA"

The qualified authority Evrotrust TSA provides a TSS service for the issuance of qualified electronic time stamps and may have one or more TSU signing the qualified certificates issued in accordance with the requirements laid down in Regulation (EC) No 910/2014, standards and standardization documents, technical and organizational conditions in Evrotrust, providing secure and reliable conditions for creation and verification of electronic time stamps, Certification Policies for Qualified Certification services.

Besides, Evrotrust guarantees that:

- use technology, operational procedures and security management procedures to prevent any possibility of manipulating time;
- uses cryptographic algorithm parameters in accordance with Regulation (EU) No 910/2014;
- provide technical and organizational conditions for the implementation of the necessary Policies for the issuance of a qualified electronic time stamp certificate and technical conditions for the devices for creation and verification of electronic time stamps;
- Defines at least one hash function that can be used to create time-tagged hash data;
- Uses coordinated universal time - UTC with the maximum allowable delay between the time of receipt of the request and the issuance of the time certificate of 1 (one) second
- Provides uninterrupted access (24/7/365) to support services, excluding technical maintenance times, accessibility and accuracy being guaranteed, even if several users are simultaneously associated with the application;
- Establishes its business of reliable devices and software in accordance with the requirements set in: CAW 14167-1 "Security Requirements for Trustworthy Systems, Managing Certificates for Electronic Signatures - Part 1: System Security Requirements" and ETSI TS 102 023 "Policy requirements for time-stamping authorities ";
- carries out its activities and services in accordance with the applicable legislation;
- issues Timestamp Tokens in accordance with ETSI EN 319 422 Time-stamping protocol and time-stamp profiles.

### 6.1.4. 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".*

### 6.1.5. 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".*

## 6.2. EVROTRAST GUARANTEES

Evrotrust assumes the following guarantees:

- for the provision of the qualified certification service, uses reliable and secure technological equipment (hardware and software);
- performs its activity lawfully;
- the certification services provided comply with generally accepted international standards and documents described in "Practice in the provision of Qualified Certification Services"
- the electronic time stamp (TST) issued does not contain any false data or errors;
- no license, intellectual property, or other rights in the token for electronic time stamps (TST) are violated;
- prevents modification of digital data after the issue of the Time Stamp Token (TST) without this being established.

## 6.3. 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. MANAGEMENT AND CONTROL OF THE TECHNICAL SECURITY OF THE TIME-STAMP CERTIFICATION AUTHORITY

## 7.1. 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.

The time-stamping authority is subject to an annual risk assessment in order to assess the business assets and threats to these assets, which determines the necessary security measures and operational procedures.

## 7.2. INTERNAL ORGANIZATION

** Procedures, mechanisms for control, security management, and maintenance of the Infrastructure of the Provider are detailed in the document "Practice in the provision of Qualified Certification Services" and are in accordance with ETSI EN 319 401.*

The controls applied by the Time-Stamp Certification Authority allow continuous verification of the integrity of the technology system, timely update and troubleshooting. The oversight of the functionality of the technology system ensures that it operates properly and in accordance with the delivered manufacturing configuration. The current configuration of the Evrotrust Technology System, as well as all amendments and updates, are recorded and

performed in a controlled manner.

Evrotrust informs all users and trustees about the terms and conditions for using Time-Stamp Certification Authority.

### 7.2.1. 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.

Evrotrust provides TSS with uninterrupted access (24/7/365), with accessibility and accuracy guaranteed, even if several users are simultaneously connected to the application. Any physical, legal or other person who has a contract with the Evrotrust for TSS is a user of that service. The TSS certification service is also available for people with disabilities.

## 7.3. MANAGEMENT OF THE LIFESPAN OF THE KEY PAIR BY TSU

### 7.3.1. GENERATING A PAIR OF KEYS OF TSU

The Time Stamp Authority ("Evrotrust TSA") is responsible for the provision of qualified electronic time stamps TSS. The TSU, as part of the TSS, signs the private time user time certificates corresponding to a certificate issued by the Basic Certifying Authority, which in this case is the "Evrotrust TSA" in the architecture of Evrotrust. The TSU signing key is generated in a physically protected environment by individuals with trusted roles. The access is twofold of at least two authorized persons. The signing key generation is performed in a cryptographic module (HSM) with security level FIPS 140-2 level 3. The generated pair of RSA keys has a length of 2048 bits. The requirements for the algorithms used and the length of the signing private key are in accordance with the technical specification ETSI TS 119 312.

### 7.3.2. PROTECTION OF THE PRIVATE KEY OF TSU

The private key of the TSU is generated and stored in a cryptographic module (HSM) compliant with FIPS 140-2, level 3. The archived copy of the private key is stored in a special safe. Keeping a copy of the key aims to restore the key in case of disaster or system crash. Key storage is periodically checked by the system auditor. The manner of storage is described in procedures of the internal documentation of Evrotrust.

When TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment

A TSU have a single time-stamp signing key active at a time.

### 7.3.3. DISTRIBUTION OF THE PUBLIC KEY OF THE TSU

The TSU certificate, which is signed by "Evrotrust TSA" and used by the TSU to sign consumer qualified electronic time stamps, is published on the Evrotrust website: https://www.evrotrust.com. The TSU certificate has been issued by the Evrotrust RSA Root CA, which acts as "Evrotrust TSA" in the architecture of Evrotrust.

The TSA guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

a) TSU signature verification (public) keys shall be made available to relying parties in a public key certificate;

b) The TSU signature verification (public) key certificate be issued by a certification authority operating under ETSI EN 319 411-1;

c) The TSU not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (public key) certificate, the TSA verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

### 7.3.4. PROLONGING THE TERM AND/OR REKEY/REISSU OF THE PRIVATE KEY OF THE TSU

The lifespan of the private key of the TSU 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 TSU is 5 years. Within 1 year before the expiration of this period a new certificate is issued. For the new certificate, a new key pair is generated, the private key is stored in the cryptomodule (HSM), and the public key is authenticated by issuing a new TSU certificate with the same validity period. All events related to the life cycle of the TSU certificate key pair are 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 and new TSU certificates are issued.

### 7.3.5. TERMINATION OF THE PRIVATE KEY OF TSU

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

### 7.3.6. MANAGEMENT OF THE LIFESPAN OF THE SIGNING CRYPTOGRAPHIC EQUIPMENT

The following particular requirements apply:

a) Time-stamp signing cryptographic hardware not is not tampered with during shipment;

b) Time-stamp signing cryptographic hardware shall is not tampered with when and while stored;

c) Installation, activation and duplication of TSU's signing keys in cryptographic hardware be done only by personnel in trusted roles using, at least, dual control in a physically secured environment;

d) TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them.

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 TSU 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.

### 7.3.7. SYNCHRONIZATION OF THE CLOCK WITH COORDINATED UNIVERSAL TIME

TSS 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;
- In the case of compromise to TSU key, suspected compromise or loss of calibration the TSU not issue time-stamps until steps are taken to recover from the compromise;
- 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 TSS 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 TSU

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 TSU;
- 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

Before the certifying authority terminates its services, it is required to:

- follows an updated and approved by the management plan and a scenario for the termination of the activity of a certifying authority. Information may be provided by email or by posting;
- informs consumers, the Supervisory Authority and third parties about the termination of the activity of its certifying authority. Information is provided by email or by posting on the Evrotrust website;
- terminates the authorization of all persons having contract activities to carry out activities related to the particular certifying body;
- before termination of the activity of the certifying authority, within a reasonable time, transfers its obligations for maintenance of all the information which is necessary to provide evidence to a trustworthy party;
- before termination of the activity, private keys, including backups, are destroyed or removed from use in such a way that personal keys can not be retrieved;
- if possible, transfer its activity to another qualified provider;
- Evrotrust applies measures to cover costs in the event of bankruptcy or for other reasons for terminating the activity of a certifying authority. In the event that it is unable to cover the costs itself, it has provided for measures within the framework of the applicable legislation;
- changes the status of the operating certificate;
- terminates the issuance of new certificates, but continues to manage the active certificates until the end of their validity;

- makes reasonable commercial efforts to minimize distortion of consumer interests.

Evrotrust monitors and prevents the issuance of a certificate for a period longer than the validity of the certifying authority that issued it.

** All business continuity procedures are described in the document "Practice in providing Qualified Certification Services" of Evrotrust Technologies AD.*

### 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.

The provision of a time-stamp in response to a request is at the discretion of the Evrotrust depending on any service level agreements with the subscriber.

### 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

Sofia, 1766, Bulgaria

„Business center MM", floor 5, Bul. "Okolovrasten pat" 251G

telephone: + 359 2 448 58 58

website: http://www.evrotrust.com

email: office@evrotrust.com

*This document is published on the web page of Evrotrust in Bulgarian and English. In the event of a discrepancy between the texts in Bulgarian and English, the Bulgarian text has priority.*