ISO 9001:2015 ISO 27001:2022
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

POLICY AND PRACTICE

FOR PROVIDING REMOTE ELECTRONIC SIGNATURE / SEAL SERVICE

TABLE OF CONTENTS

1 INTRODUCTION

The European Union has introduced the concept of electronic signature which is created by a "remote signature creation device", which means that the signature device is no longer a personal device under the user's physical control, but is rather replaced by services offered and managed by a certification service provider. Regulation (EU) No. 910/2014 has allowed the signatory of electronic signature to entrust the service of qualified electronic signature creation devices to a third party, provided that appropriate mechanisms and procedures are in place to ensure that the signatory has sole control over the use of the data related to the creation of its electronic signature, and that the requirements with regard to qualified electronic signatures are met when using the device. In this sense, Evrotrust Technologies AD (Evrotrust), as a certification service provider, provides a remote electronic signature/seal service, whereby it manages the electronic signature creation environment on behalf of the signatory of the electronic signature. In this service, in order to ensure that electronic signatures receive the same legal recognition as electronic signatures created in a fully user-managed environment, Evrotrust applies specific procedures for managing physical and administrative security, makes use of reliable systems and products, including secure electronic communication channels, a reliable electronic signature creation environment, and makes sure that this environment is used under the sole control of the signatory of the electronic signature. The provision of a qualified electronic signature created by a remote electronic signature creation device shall comply with the requirements applicable to qualified certification service providers as described in Regulation (EU) No. 910/2014.

Regulation (EU) No. 910/2014 allows for all requirements for electronic signatures to be also applied mutatis mutandis to electronic seals. Pursuant to Regulation (EU) No. 910/2014, Evrotrust provides its service both for remote electronic signature creation and for remote electronic seal creation for users. Users of the service can be both individuals and legal entities who own a smartphone, tablet or other mobile device.

1.1 REVIEW

This document (Policy and Practice) covers the security policy, practice and requirements of Evrotrust, in its capacity as a qualified certification service provider providing a Remote Electronic Signature Service (RESS). The Policy and Practice describes the fulfilment of the requirements of technical specifications ETSI TS 119 431-1, ETSI TS 119 431-2 and standard CEN EN 419 241-1.

Components controlling remote electronic signature creation devices (QSCD/SCDev) and components supporting the AdES digital signature creation service (SCASC) are used to provide the remote electronic signature/seal service. The AdES digital signature creation service component relies on remote server signing or creation of a signature in a user environment by a signature creation device. The use of this component and the components of the QSCD control device shall comply with the requirements of Regulation (EU) No. 910/2014 on the creation of an electronic signature on behalf of a remote signer. Those requirements are based on the general policy and practice requirements set out in ETSI EN 319 401, taking into account the related certification requirements in ETSI EN 319 411-1, as well as the requirements set out in CEN EN 419 241-1.

Evrotrust, by providing a remote electronic signature service, acts as a service provider providing a server signing/remote signing application (SSASP), and a service provider providing a signature creation/remote signature creation application (SCASP).

The requirements fulfilled by the server signing application service component (SSASC) are in line with the organizational structure, operating procedures, facilities and communication environment of Evrotrust. In addition to the generally applicable Evrotrust security policy requirements when using a SSASC controlling a remote signature creation device (SCDev), Evrotrust also applies specific requirements associated with the fact that it uses a device that is compliant with Regulation (EU) No. 910/2014 (QSCD). The service component includes a signing application (SSA) and a QSCD/SCDev. The security policy requirements are described with regard to the requirements for the creation, maintenance and management of the lifecycle of the signing keys used to create electronic signatures/seals.

The requirements fulfilled by the electronic signature creation application service component (SCASC) are in line with the requirements of the Evrotrust security policy when using a component supporting the AdES digital signature creation service that serves a signature creation application. In this case, it is a Signature Creation Application (SCA). SCASC has connections with external (certification) services that it can connect to, for example for the purpose of provision of information that needs to be included in the signature. SCASC connects to a server signing application service component (SSASC) using access protocols. Evrotrust uses

SCASC or SSASC connection protocols in accordance with ETSI TS 119 432. This document describes the specific controls that are required to address specific risks associated with the provision of AdES signature creation services.

Evrotrust provides a remote electronic signature creation service in accordance with the requirements of Regulation (EU) No. 910/2014 on electronic signatures and electronic seals, based on X.509 certificates. The service can be used to create advanced and qualified electronic signatures, advanced and qualified electronic seals.

Evrotrust develops, implements, imposes and regularly updates the Policy and Practice. This document is intended for auditors, users and relying parties. It is of utmost importance for users and relying parties to get acquainted with the goals and role of the Policy and Practice in terms of the applicability of this service, and so that users of the service gain more confidence. The relationship between Evrotrust and the end-user are governed by the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services, or, where applicable, by a contract for provision of the respective service, the General Terms being an inseparable part thereof, and the price of the service is contained in the Evrotrust tariff which is available on the website. This document is structured in accordance with the framework defined by IETF RFC Recommendation 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.2 REGULATORY REFERENCES

The Policy and Practice is in line with the following documents:

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- CEN EN 419 241-1 "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements";

- CEN EN 419 241-2 "Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing";
- ETSI TS 119 431-1 "Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev (remote signing)";
- ETSI TS 119 431-2 "Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation";
- ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements";
- ETSI EN 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
- ETSI TS 119 101 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation";
- ETSI TS 119 102-1 "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation";
- ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects";
- IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.3 NAME AND IDENTIFICATION OF THE RESS POLICY

The full title of this document is "Certificate Policy and Practice for Providing Remote Electronic Signature Service". The policies applicable to the remote electronic signature/seal service include the policies applicable to all trust services remotely provided by Evrotrust. Evrotrust makes sure that it does not change the object identifiers of the applicable policies, as well as the object identifiers of the policies and practices, and of other reference documents as well. If there is any extension/change in the Policy and Practice which affects certificates already issued, Evrotrust will represent a new object identifier describing the new certificates or the extended/changed ones. Evrotrust follows an internal OID management procedure. The RESS policy describes the application of the remote electronic signature/seal service and contains additional information related to its use. This document is intended for auditors, users and relying parties.

The level of service provision (SLA/Service Level Agreement) is guaranteed by Evrotrust and is described in the General Terms and Conditions and the individual agreements with clients. Evrotrust shall not be held liable for the inability to cover the level of service availability caused by a system beyond its control, except in cases where it could have ensured an alternative provision, but in accordance with the requirements of the applicable standards. Evrotrust shall not be held liable for any losses or damages resulting from force majeure events.

Evrotrust, as a provider of a remote electronic signature/seal service, shall fulfill both the requirements of the ETSI standards related to the service provided, and more specifically ETSI TS 119 431-1, 2 and CEN EN 419 241-1, and the specific requirements related to Regulation (EU) No. 910/2014, Regulation (EU) 2016/679 and the national legislation.

1.3.1 IDENTIFICATION OF THE SSASC POLICY

The SSASC policy describes the applicability of the service and is determined independently of the details of the specific SSASP operating environment. Evrotrust applies an EU SSASC policy (EUSCP) that provides for the same quality as that provided for by the normalized SSASC policy (NSCP), fulfilling the requirements of ETSI TS 119 431-1, but in accordance with the specific requirements of Regulation (EU) No. 910/2014 related to the QSCD management. The NSCP shall comply with the generally recognized best practices for TSPs that provide a remote SCDev management service in support of all types of transactions and justified risk assessment.

Evrotrust, as a SSASP, applies the following SSASC certification service policies:

- Light SSASC policy (LSCP) with **OID**: itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) lightweight (1);
- Normalized SSASC policy (NSCP) with **OID**: itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1) policy-identifiers(1) normalized (2).

SSASP manages the server signing application service component (SSASC) service or the remote signature creation device (SCDev/QSCD) service. SSASC is part of a remote electronic signature/seal certification service which is provided by Evrotrust in accordance with Art. 3, para. 16 of Regulation (EU) No. 910/2014.

Evrotrust, as a SSASP, applies the following specific EUSCP policy of the EU SSASC certification service with **OID**: itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3).

Evrotrust defines the EUSCP policy by applying all requirements set out for a normalized NSCP policy.

1.3.2 IDENTIFICATION OF THE SCASC POLICY

The SCASC policy describes the remote electronic signature/seal creation service application and contains additional information related to its use. Evrotrust, as a SCASP, fulfills both the requirements of ETSI TS 119 431-2 and the specific requirements related to Regulation (EU) No. 910/2014 on the creation of electronic signatures/seals based on X.509 certificates. Evrotrust uses in its documentation the following specific object identifiers:

- **OID:** itu-t (0) identified-organization (4) etsi (0) SERVICE CREATION-policies (19431) ades (2) policy-identifiers (1) main (1); and
- **OID:** itu-t(0) identified-organization(4) etsi(0) SERVICE CREATION-policies(19431) ades (2) policy-identifiers(1) eu-advancedx509 (2).

The policy of the service offered by Evrotrust is in line with the requirements of the European Union (EU) and provides for the same quality as a normalized policy (NSCP) which meets the generally recognized best practices for TSPs operating with a remote SCDev used to support any type of transaction offered by the NSCP, but with the specific requirements of Regulation (EU) No. 910/2014 related to the QSCD management. Where the SCASC is used for the creation of an electronic signature, the signing certificate identifies the signer, and where the SCASC is used for the creation of an electronic seal, the signing certificate identifies the creator of the seal. The signing certificate is contained in the created AdES signature.

1.4 PARTICIPANTS IN RESS

Evrotrust, as a qualified provider of qualified trust services, provides services of generation and management (cancellation, renewal and revocation) of qualified certificates, through the "Evrotrust RSA Operational CA" Certification Authority, and services of user identification and authentication, through a Registration Authority (RO). Other participants in the Evrotrust infrastructure are users and relying parties.

Under this policy, the signer associated with the signing key may be:

- an individual;
- an individual associated with a legal entity;

- a legal entity (which may be an organization, unit or department associated with the organization); or
- a device or system operated by or on behalf of an individual or legal entity.

The relationship between the user signing an agreement with Evrotrust for the use of a certification service and the signer holding a private key is equivalent to the relationship between a "subscriber" and a "subject", as described in ETSI EN 319 411-1. These relations are regulated both in the General Terms and Conditions and in an Agreement.

Evrotrust, as a SSASP and SCASP, may use other parties to provide parts of the service, however Evrotrust shall always bear full liability and ensure that the requirements of this document have been fulfilled. If the external party uses electronic means of identification issued under a notified scheme which is included in the list published by the European Commission, Evrotrust will not require any evidence of the required level of compliance.

1.4.1 CERTIFICATION AUTHORITIES

- **"Evrotrust RSA Operational CA"** is a certification authority that issues qualified certificates of qualified electronic signatures/seals;

The activities of the "Evrotrust RSA Operational CA" Certification Authority are described in the document entitled "Practice in the Provision of Qualified Trust services".

- **"Evrotrust TSA"** is a certification authority issuing qualified electronic time stamps. It accepts requests for the issuance of qualified electronic time stamps of submitted content of an electronic document by a user or a relying party. The Certification Authority prepares a qualified electronic time stamp of the submitted hash value of an electronic document and provides an opportunity for subsequent (after the period of validity of the qualified electronic signature/seal certificate) proof before the receiving party of the fact that a statement or electronic document has been signed. Qualified electronic time stamps can be integrated in the process of creating or accepting a qualified electronic signature/seal, electronically signed documents and electronic transactions, when archiving electronic data and others.

The activities of the "Evrotrust TSA" Certification Authority are described in the document entitled

"Policy and Practice of a Qualified Electronic Time Stamps Provision Service".

1.4.2 REGISTRATION AUTHORITIES

The Registration Authority is a separate structure of Evrotrust, but it can also be an external legal entity to which Evrotrust assigns the provision of services of registration, identification and authentication of users of Evrotrust. External registration authorities represent an established network of registration authorities that perform their activities of provision of trust services on behalf of Evrotrust. A complete and up-to-date list of registration authorities and information on their contact details is available on the Evrotrust website: https://www.evrotrust.com.

The registration authorities which provide trust services and which are not within the organizational structure of Evrotrust (external RAs) shall, before carrying out such activities, enter into an agreement with Evrotrust. In addition to the rights and obligations of both parties, the agreement shall also include information on the identity of the persons participating in the registration authority and their authorization to represent the two parties during the performance of the agreement.

The operators from the registration authority shall be responsible for one or more of the following functions: identification and authentication of persons for the purpose of issuance of certificates, approval or rejection of applications for issuance of certificates, initiation of revocation or cancellation of certificates in certain circumstances, processing of user requests to withdraw or cancel their certificates, and approval or rejection of requests by users to renew their certificates.

1.4.3 USERS

Any individual (signatory) or legal entity (creator) who has a written agreement entered into with Evrotrust is a user of the remote electronic signature/seal service provided by Evrotrust. In the event that the signatory of an electronic signature assigns the service of the qualified electronic signature creation devices to Evrotrust, Evrotrust will ensure that appropriate mechanisms and procedures have been implemented, the signatory has sole control over the use of the data related to the creation of its electronic signature in accordance with this document, and that the requirements with regard to qualified electronic signatures are met when using the device. Only the signatory of the qualified certificate shall have the right to access the private key

for signing electronic statements through which it creates an electronic signature.

A user may be:

- an individual who creates an electronic signature;
- an individual who is an authorized representative of a legal entity and creates an electronic signature;
- a legal entity which creates an electronic seal.

Where practicable, the trust services provided and the products used in the provision of those services will also be made accessible to persons with disabilities.

1.4.4 RELYING PARTIES

A Relying Party means an individual or legal entity who relies on the remote electronic signature/seal certification service provided by Evrotrust. Relying Parties shall have knowledge and skills regarding the use of a qualified certificate and shall rely on the circumstances certified therein only in view of the applicable Policy and Practice, especially with regard to the level of security when verifying the identity of signatorys and the identity of creators, as well as with regard to the restrictions for its use as entered in the certificate. Relying Parties shall have permanent access to the Evrotrust registers to verify the validity of the qualified certificates. Relying Parties established outside the territory of the Republic of Bulgaria can rely on reliable, secure, easy and convenient qualified validation, in an automated manner, of qualified electronic signatures/seals the certificates for which have been issued by Evrotrust.

1.4.5 OTHER PARTICIPANTS

For certain activities, pursuant to Regulation (EU) No. 910/2014, Evrotrust may involve external parties. The relations regarding such activities shall be regulated in an agreement. Such agreement shall set out the rights and obligations of the external parties involved in the certification service provision activities. Evrotrust uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation of server and network equipment, providers of cloud systems and services, providers of automated identification services, IT services and others. When working with subcontractors and providers, Evrotrust requires them to strictly follow its procedures, in accordance with this Policy and Practice.

1.5 USE AND APPLICATION OF RESS

Evrotrust, as a qualified certification service provider, offers its users a service that replaces the use of flash drives and smart cards for the creation of electronic signatures. The service provides for fast, easy, reliable and secure remote signature creation, where the electronic signature creation environment is managed by Evrotrust, on behalf of the user, as the signatory of the electronic signature and by using its own smart device. The provided service can be used extremely easily and quickly at any place and at any time. Evrotrust provides this service in full compliance with the applicable law. Access to it is provided without geographical boundaries to all persons holding a valid identity document.

1.5.1 PROHIBITION ON THE USE OF RESS

The remote electronic signature/seal service must not be used for illegal purposes and in a way incompatible with the announced Policy and Practice.

1.6 POLICY AND PRACTICE MANAGEMENT

1.6.1 ORGANIZATION, MANAGEMENT DOCUMENTATION OF EVROTRUST

Evrotrust is responsible for the management of this Policy and Practice. Each version of this document shall be valid until a new version has been approved and published. Each new version is developed by Evrotrust personnel and published after approval by the Board of Directors of Evrotrust. Users shall be obliged to comply only with the version of the Policy and Practice which is valid at the time of using the services of Evrotrust.

1.6.2 CONTACT PERSON

The contact person for the management of the document entitled "Policy and Practice for Providing Remote Electronic Signature Service" shall be the Executive Director of Evrotrust.

Further information can be obtained at the following address:

Evrotrust Technologies AD

1766 Sofia

251 G Okolovrasten Pat Av, MM Business Center, fl. 5

telephone number/fax: + 359 2 448 58 58

e-mail: office@evrotrust.com

1.6.3 POLICY AND PRACTICE APPROVAL PROCEDURES

Evrotrust follows the following procedure for the approval of this document:

- Each version of the Policy and Practice is developed by qualified Evrotrust personnel. This document shall become effective upon its approval by the management of Evrotrust and its publication on the Evrotrust website (https://www.evrotrust.com/landing/bg/a/tsp-documents). The provisions contained in the Policy and Practice shall be valid until the issuance and publication of a new version of the document;
- This document and any update (new version) thereof will be immediately communicated to the Evrotrust employees and to all interested parties;
- Evrotrust has a management body that specifies and finally approves the Policy and Practice document and each update (new version) thereof based on the requirements for the provision of the service before it is published on the company's website;
- The RESS policy is approved and updated in accordance with a specific review procedure, including the responsibilities for its maintenance, in order to ensure that the policy is supported by practice;
- The management of Evrotrust reviews the practices, including the responsibilities for maintaining this document, at least once a year;
- For the RESS policy, which includes SCASC based on the requirements set out in ETSI TS 119 431-2 and SSASC based on the requirements set out in ETSI TS 119 431-1, Evrotrust performs a risk assessment to assess the business requirements and define the security requirements as described in this document;
- Evrotrust describes in the RESS policy all deviations that it decides to apply;
- Evrotrust will inform users in cases where it supplements or further restricts the requirements of the RESS policy by publishing, without delay, an updated version of this document on the Evrotrust website.

1.6.4 APPLICABILITY OF PUBLIC DOCUMENTATION

RESS is related to a set of documents which can be both documentation internal for Evrotrust and public documentation. The Risk Assessment and the Information Security Policy are both internal documents and are subject to annual update and verification. The documentation

intended for users, relying parties and all other interested parties is distributed 7/24/365 on the company's website. The General Terms and Conditions of RESS and, in particular of SCASC and SSASC, are part of the document entitled "General Terms and Conditions of the Agreement for the Provision of Certification, Information, Cryptographic and Consulting Services" which is published on the Evrotrust website and forms an integral part of the agreement entered into between a user and Evrotrust.

1.7 DEFINITIONS AND ABBREVIATIONS

AdES (Digital) Signature – an electronic signature which is a CAdES, PAdES or XAdES;

Electronic Signature Creation Data - unique data used by the Electronic Signature Signatory for the creation of an electronic signature;

Electronic Signature - data in electronic form which is added to other data in electronic form or is logically associated with it, and which the Electronic Signature Signatory uses to sign;

Electronic Seal - data in electronic form, which is added to other data in electronic form or is logically associated with it, in order to guarantee the origin and integrity of the latter. An electronic seal serves as proof that an electronic document has been issued by a legal entity and guarantees the reliable origin and integrity of the data;

Qualified Electronic Signature/Seal Creation Device (QSCD) - an electronic signature/seal creation device that meets the requirements laid down in Regulation (EU) No. 910/2014;

Signer Interaction Component (SIC) – a component for interaction with the signer;

Signature Activation Module (SAM) – a signature activation module which represents configured software executed in an environment protected against unauthorized use;

Signature Activation Data (SAD) – signature activation data;

Signature Activation Protocol (SAP) – signature activation protocol;

Trustworthy System Supporting Server Signing (TW4S) - a trustworthy system supporting server signing/client-server system for the creation of electronic signatures, using signing keys under the sole control of the signer;

Data to be Signed Representation (DTBS/R) – formatted data used to calculate the electronic

signature value (e.g. hash value);

Remote Signature Creation Device (SCDev) - a remote electronic signature/seal creation device which ensures that the signing operation is under the sole control of the signer – it represents configured software or hardware for the creation of an electronic signature/seal;

Server Signing Application (SSA) - a server signing application/application using a remote signature creation device;

Signature Creation Application (SCA) – a remote signature creation application;

Driving Application (DA)/Digital Identity Solution (DIS) – a management / controlling application for creating, validating and extending electronic signatures. Organizes all processes and interactions with end users/signers and integrated third parties for the provision of qualified trust services. The application also integrates the functionalities of electronic identification and generation of the electronic identification means (eID means);

Signature Creation System (SCS) – a signature creation system;

Signature Creation Application Service Component (SCASC) – a signature creation application service component;

Server Signing Application Service Component (SSASC) - a component of the remote electronic signature creation service using a server signing application for the creation of digital signature values on behalf of the signer;

Server Signing Application Service Provider (SSASP) – a provider of a service providing a server signing/remote signing application;

Signature Creation Application Service Provider (SCASP) – a provider of a service providing a signature creation/remote signature creation application;

Relying Parties - individuals or legal entities who are addressees of electronic statements or other information objects and rely on the trust services of Evrotrust;

Qualified Certification Service Provider – a certification service provider that provides one or more qualified trust services and has obtained its qualified status from the Supervisory Authority;

Qualified Certification Service - a certification service that meets the applicable requirements set out in Regulation (EU) No. 910/2014;

Qualified Electronic Signature Certificate – an electronic signature certificate issued by a qualified certification service provider and meeting the requirements laid down in Regulation (EU) No. 910/2014;

Qualified Electronic Seal - a qualified electronic seal is an advanced electronic seal created by a qualified electronic seal creation device and based on a qualified electronic seal certificate;

Qualified Electronic Signature - an advanced electronic signature created by a qualified electronic signature creation device and based on a qualified electronic signature certificate;

Practice (CPS) - practice in the provision of qualified trust services is a document containing rules on the issuance, cancellation, renewal and revocation of certificates, as well as the conditions for granting access to certificates;

Seal Creator - a legal entity that creates an electronic seal;

Private Key – a string of characters used in an algorithm for converting information from intelligible to encrypted form or vice versa - from encrypted to intelligible form (decryption);

Public Key – one of a pair of keys used in an asymmetric cryptosystem that is accessible and can be used to verify an electronic signature/seal;

Electronic Signature Signatory - an individual who creates an electronic signature;

Certification Service - an electronic service, usually provided for a fee, which consists of: the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered mail services, as well as certificates related to the said services; or the creation, verification and validation of certificates of authenticity on a website; or the storage of electronic signatures, seals or certificates relating to the above listed services;

Electronic Seal Certificate – a legal entity certificate pursuant to Regulation (EU) No. 910/2014;

Electronic Signature Certificate - an electronic certificate which associates the electronic signature validation data with an individual and confirms at least the name or pseudonym of that individual;

Qualified Electronic Seal Creation Device - a qualified electronic seal creation device is an electronic seal creation device that meets the requirements of Regulation (EU) No.

910/2014;

Qualified Electronic Signature Creation Device - a qualified electronic signature creation device is an electronic signature creation device that meets the requirements of Regulation (EU) No. 910/2014;

Authentication – an electronic process that enables the electronic identification of an individual or legal entity or the confirmation of the origin and integrity of data in electronic form;

Electronic Signature Value - the result of cryptographic processing of data in electronic form which enables the data recipient to prove the source and integrity of such data;

Electronic Identification (eID) - a process of using data in electronic form to identify persons whose data uniquely represent an individual or legal entity, or an individual representing a legal entity;

Means of Electronic Identification – a tangible and/or intangible unit which contains personal identification data and which is used for authentication in an online service;

Reference to Means of Electronic Identification - data used in SSASC as a reference to a means of electronic identification with the purpose of authentication of the signer (for example, where a signed certificate is generated after successful authentication of the signer, the signer identification number and the user identifier may be the reference);

Personal Identification Data - a set of data that allows to establish the identity of an individual or legal entity, or of an individual representing a legal entity;

2 PUBLICATION RESPONSIBILITY AND REPOSITORY

2.1 PUBLIC REGISTER

The Evrotrust Public Register is a repository containing current and previous versions of electronic documents (including current versions of this document, "Policy for Providing Qualified Remote Electronic Signature/Seal Certificate Service" and "Practice for Providing Qualified Trust Services"), Agreement for the use of electronic signatures intended for users, certificates of the Certification Authority, Certificate Revocation List (CRL) and other information on the use of signing keys and their related certificates. The Evrotrust Public Register provides users and relying parties with a current version of the General Terms and Conditions, which document contains

information on the use of signing keys. In the applicable General Terms and Conditions, the methods of using a signing key and its related certificate are easily recognizable.

All users and relying parties are provided with permanent access 24/7/365 to the information contained in the repository at: https://www.evrotrust.com. Access to this information has no geographical restrictions.

In the event of a system failure, service failure or any other factors beyond the control of Evrotrust, the best practices will be applied to ensure that the RESS service is not available for longer than the maximum period allowed, as defined in the User Agreement and/or in the General Terms and Conditions (incl. SSASC and SCASC).

Immediately after their issuance, user certificates are published in the Evrotrust Register of Certificates (database). Access to them is restricted to relying parties without the users' express consent.

2.2 PUBLIC INFORMATION

The Public Register is available to all interested parties without any national boundaries at: https://www.evrotrust.com/. The qualified certificates issued are stored in an Evrotrust database. Verification of issued qualified certificates can be performed through a service of qualified and unqualified validation of all types of electronic signatures according to Regulation (EU) 910/2014 and in the Certificate Revocation List (CRL) which is published on the Evrotrust website and is updated every 3 (three) hours. Evrotrust provides a service of checking the status of issued certificates in real time based on an online certificate status verification protocol (OCSP). The use of OCSP makes it possible to obtain information about the status of certificates without being necessary to make a reference to the CRL. The OCSP service generates a database-based response. To maintain proper system performance, OCSP responses can be cached for a predetermined time (usually no more than a few hours).

2.3 PUBLICATION FREQUENCY

The documentation containing Policy and Practice for providing qualified trust services, agreements, templates, electronic signature/seal operating manuals, audit reports, etc. issued by Evrotrust will be published on the Evrotrust website immediately upon each update. The operating certificates of the Certification Authority will be published immediately upon each

issuance of new certificates. Update of the Register with the issued user qualified certificates will be performed automatically and immediately upon the publication of each newly issued valid certificate and it may be accessed through the OCSP protocol. The current CRL will be automatically updated every 3 (three) hours at the most or immediately upon the cancellation or revocation/renewal of a valid certificate.

2.4 ACCESS TO PUBLICATIONS

Evrotrust offers services of access to the information stored in the repository (public register), by providing HTTP/HTTPS and OCSP based access.

Access to the information in the repository is not restricted by Evrotrust, except at the request of the signatory/creator and only in respect of its validly issued qualified certificate.

The information published in the Evrotrust repository is available at all times (24/7/365), except in cases of events beyond the control of Evrotrust.

3 REQUIREMENTS TO RESS

3.1 GENERAL REQUIREMENTS

Evrotrust applies the following general requirements for RESS:

a) Evrotrust applies a set of policies and practices appropriate to the remote electronic signature/seal service. The applicable policies and practices are listed, together with their object identifiers, in the issued certificates when using the service. For each certification service provided and each certificate issued, Evrotrust has published on its website a policy and practice with included object identifiers;

b) The management of Evrotrust approves the set of policies and practices and they are thereafter published and communicated to the employees and relying parties, where appropriate;

c) This document describes the practices and procedures used to address all requirements identified for the applicable Evrotrust policy;

d) This document, in item 1.4.5 thereof, refers to the possibility of involving external organizations supporting the services of Evrotrust. In the case of external organizations, their obligations and applicable policies and practices shall be described in contractual agreements;

e) Evrotrust provides users and relying parties with the policy, practice and other

relevant documentation through the company's website: https://www.evrotrust.com/landing/bg/a/tsp-documents;

f) Evrotrust has a management body that finally approves this document;

g) The management of Evrotrust manages the implementation of the applicable policies and practices;

h) Evrotrust defines the practices review process which takes place at least once a year, and defines the responsibilities for their maintenance which it assigns to authorized personnel;

i) Evrotrust promptly updates the practices and policies, with each new version of the documents being approved by the management and published on the company's website;

j) Evrotrust publishes each new edition of its applicable practices and policies without delay;

k) Termination of the service may occur upon termination or expiration of the trust services agreement entered into between a user and Evrotrust. An agreement may be terminated upon closing a user profile. Item 13 of this document stipulates the provisions for termination of an agreement upon termination of the business of Evrotrust.

3.2 SPECIFIC REQUIREMENTS TO SSASC

Evrotrust applies the following specific requirements when providing the server signing application server component (SSASC) service:

a) the length of the keys and the cryptographic algorithms used by Evrotrust, which are crucial for the security of the SSASC service, have been complied with the technical specification ETSI TS 119 312 and are as follows:

- The length of the Evrotrust RSA Root CA is 4096 bits, with an applicable combination of asymmetric and hash algorithms: sha384-with-RSA;
- The length of the key pair of the Evrotrust RSA Operational CA is 2048 bits, with an applicable combination of asymmetric and hash algorithms: sha256-with-RSA;
- The length of the key pair of the operational authorities "Evrotrust TSA", "Evrotrust RSA QS Validation" and "Evrotrust RSA Validation" is 2048 bits, with an applicable combination of asymmetric and hash algorithms: sha256-with-RSA;
- The length of a key pair for qualified and advanced electronic signature / seal

of the Signatory/Creator generated through the Evrotrust infrastructure can be 2048, 3072 or 4096 bits, with an applicable combination of asymmetric and hash algorithms: sha256-with-RSA;

b) all policies and practices applied are available 24/7/365 to all interested parties in the public register on the Evrotrust website. Documents containing sensitive information, such as information security procedures, are internal to Evrotrust and are not published.

3.3 SPECIFIC REQUIREMENTS TO SCASC

Evrotrust applies the following specific requirements when providing the electronic signature creation application service component (SCASC) service in accordance with ETSI TS 119 431-2:

a) SCASC supports the inclusion of timestamping in the digital AdES signature, which is described in item 5.3 of this document;

b) The applicable signature creation policies are described in item 1.3 of this document;

c) This document indicates all supported signature formats in item 5.4 there of;

d) This document indicates all supported signature classes in item 5.2 there of;

e) This document describes the possibility for the involvement of external organizations in the provision of the service in item 1.4.5 thereof.

4 ARCHITECTURES

4.1 BASIC INFORMATION

There are two different architectures wherein SCASC and SSASC apply different certification and authorization mechanisms according to the level of reliance on the signing keys control, given that Evrotrust, which controls SCASC and SSASC, may delegate certification and authorization processes to an external party (e.g. identity and/or certification provider).

The architectures include two main environments: the signer environment and the Evrotrust protected environment. The Evrotrust protected environment includes a tamper protected device (cryptographic module) certified according to the requirements of CEN EN 419 221-5. The Evrotrust protected environment is managed in accordance with the security policy and keeps in a secure form both the signing keys and evidence of the connection between the private keys and the signers' identity. The signer environment is local to the signer (own device)

and its protection is the signer's responsibility.

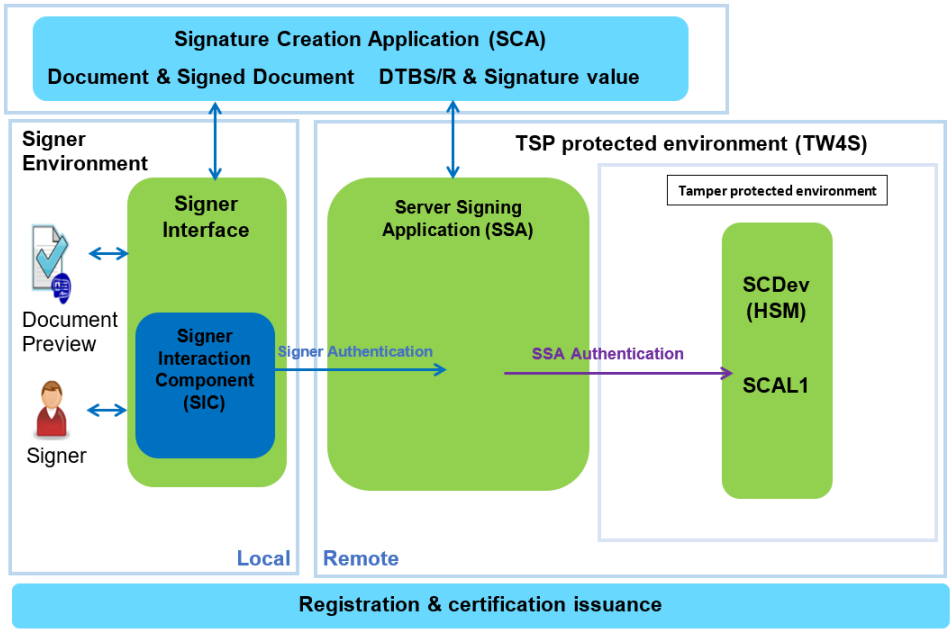
4.2 BLOCK SCHEME

Evrotrust provides a remote electronic signature/seal service by having built a reliable server signing support system (TW4S) in accordance with the general security requirements of Standard EN 419 241-1. The reliable system is located in a secure environment that covers personnel physical security requirements, procedures and documentation providing a remote electronic signature creation service. The reliable system aims to create a digital signature under the sole control of an individual or legal entity which may be included in an electronic signature or electronic seal, as defined in Regulation (EU) No. 910/2014. The level of reliance on the signing key control, where the digital signature is a seal, does not necessarily have to be the same as where it is used to represent an electronic signature.

The Evrotrust reliable server signing support system (TW4S) is a system that offers remote electronic signatures/seals as a service. It ensures that the signer's signing key or keys is/are used for its/their intended purpose under its sole control.

Evrotrust supports two levels of sole control provision, SCAL1 and SCAL2:

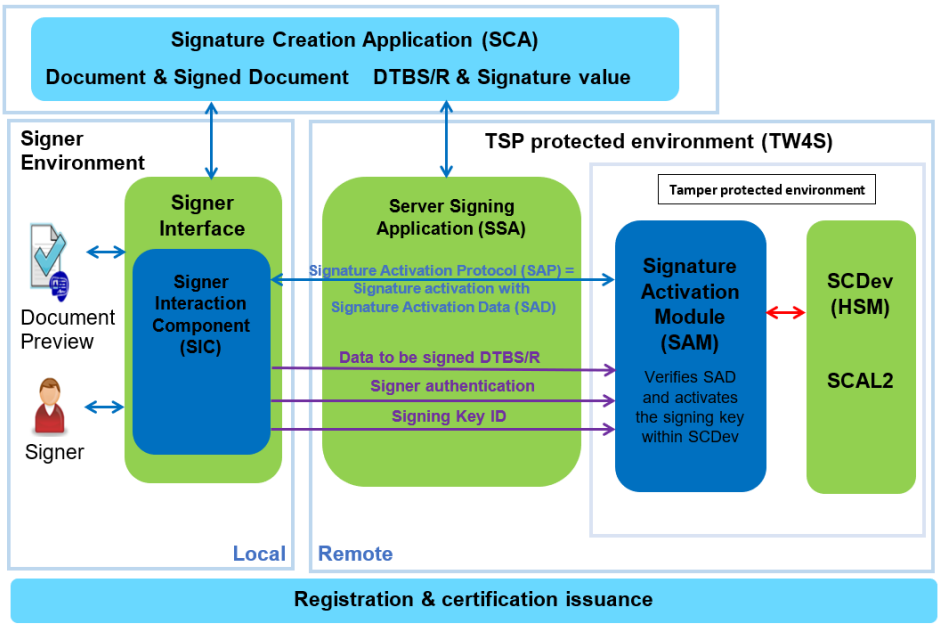
a) In SCAL1 sole control, the signing keys are used with a low level of reliance under the sole control of the signer.



To generate a digital signature in SCAL1, the signing key (the private key of the asymmetric

key pair) does not necessarily have to be generated, stored and used in a cryptographic module. The signing key may be stored in a file, and the SCDev may be software using such file. At the users' request, files can be used, but Evrotrust applies specific external security measures in addition to the protection of the files themselves from tamper (deletion, modification). To generate a digital signature in SCAL1, the TW4S uses signing keys in a tamper protected environment. The environment is provided by SCDev which is a hardware security device meeting the standards EN 419 211 or EN 419 221. In SCAL1, the signer successfully certifies in the server signing application (SSA) and then provides access to the signing operation. The signer's signing key is linked by the SSA to its certification factor. Evrotrust allows the authentication of the signer to be performed by an external party, such as an electronic identity provider. If such external party uses electronic means of identification issued under a notified scheme which is included in the list published by the European Commission in accordance with Article 9 of Regulation (EU) No. 910/2014, there is no need to prove compliance with the required level and Evrotrust accepts compliance with the regulatory requirements.

b) In SCAL2 sole control, the signing keys are used with a high level of reliance under the sole control of the signer.



As a result of the interaction of the signature activation module (SAM) and the signer interaction component (SIC), through a server signing application (SSA), the signature activation data (SAD) is calculated and set to enable the signing operation in SCDev for specific DTBS/R signing data. To reach SCAL2, SAM manages the use of SAD to provide "sole control". The

authorized signer key is managed by SAM using a signature activation protocol (SAP). Through the protocol, the same level of security for "sole control" is achieved as that which would be achieved through a stand-alone QSCD, as defined in Regulation (EU) No. 910/2014. Activation of a signature in SCAL2 requires authentication of the signer and authenticity of the request for the signing operation. In SCAL2, Evrotrust allows for the authentication of the signer to be performed by an external party, such as an electronic identity provider. In this case, Evrotrust makes sure that the authentication process delegated to the external party makes use of electronic identification means issued under a notified scheme in accordance with the applicable regulatory requirements and that the external party complies with all the requirements of EN 419241-1.

Evrotrust provides the service using level SCAL1 or SCAL2 to ensure sole control in accordance with the applicable signing policy and applicable legal requirements.

The main functionalities of TW4S are the following:

- generation of signing keys in SCDev and their provision for use by authorized signers;
- management of signing keys - deletion, backup and recovery in SCDev;
- signer authentication in order for it to be allowed to use the signing key;
- creation of a digital signature within the SCDev, after interaction with the authorized signer.

To increase the level of security in SCAL2, there are additional mandatory functionalities:

- use of the SIC component to establish a connection between the signer and the signing operation in the SAP (signature activation protocol);
- use of a SAM (signature activation module) which is located in a tamper protected environment and which is responsible for the implementation of the SAP protocol. The SAM provides a set of functional components:
  - for generation of data for the activation of the SAD signature in a tamper protected environment where the SAD is not generated by the SIC;
  - for management of the SAD verification and for the activation of the signing keys;
  - for management of the signers' authentication factors associated with the

signing keys and generation of the signing keys.

TW4S uses the SAM cryptographic module to generate the signing key and create a digital signature value. TW4S consists of at least one server signing application (SSA) and one remote signature creation device (SCDev). A SCDev is a device that is remotely controlled by a signature activation module (SAM) implemented in a tamper protected environment. This module uses signature activation data (SAD) collected through a signature activation protocol (SAP) to ensure with a high degree of certainty that the signing keys are used under the sole control of the signer. SSA uses the remote SCDev to generate, maintain, and use the signing keys under the sole control of their authorized signer. So when the SSA uses a remote SCDev, the authorized signer remotely manages the signing key with a high level of reliance. TW4S is intended to provide the signer or other application with an electronic signature created on the basis of the data to be signed.

The Evrotrust service is applicable for **Batch Server Signing**. The Evrotrust service allows the signer to sign a batch of documents without explicitly verifying and approving each document. In this case, the signatory applies controls to the batch signing process, and not to each individual document. Since the applicability of batch signing depends on the legal environment and the application environment, TW4S can support configuration profiles that enable or disable batch signing with electronic signatures.

TW4S consists of **local and remote environments**. The signer is in the local environment and interacts via its device (laptop, tablet or mobile phone) with the server signing application (SSA) in the remote environment. The purpose of the interaction between the device and the SSA is to use the SSA signing service. The signing operation is performed through a signature activation protocol (SAP), which requires that the signature activation data (SAD) is provided in the local environment. SAD connects three elements: the signer authentication data using the signing key and the data to be signed (DTBS/R(s)). To ensure that the signer has "sole control" on its signing keys, an authorization operation is performed. This is done by a signature activation module (SAM) which, by processing a SAP endpoint, verifies the SAD and activates the signing key in the cryptographic module. Evrotrust has placed the cryptographic module and SAM in a secure environment. SAD verification means that the SAM verifies the connection between the three SAD elements and whether the signer has been authenticated. Evrotrust uses a certified cryptographic module according to standard EN 419221-5, which is in line with QSCD. The signer

is in the local environment with a device user interface which displays the documents to be signed. The device uses a signer interaction component (SIC) with the SSA. The SSA forwards the communication from the SIC or from the SSA to the QSCD. Inside the QSCD, the SAM receives the messages and optionally communicates with the SSA to receive relevant data. Once the SAM has verified SAD, it can allow the activation of the signing key in the cryptographic module and create a digital signature value. The value is returned to the SSA and can be further delivered to a remote signature creation application (SCA) or SIC. The SSA and the user interface act as support modules that display documents and forward messages. TW4S relies on the following three services: authentication of individuals; certified signing keys; signature creation application that is responsible for creating the signed document by using the signature values provided by TW4S.

SAD contributes, either directly or indirectly, to the authentication of the signer. It is possible for the authentication to be performed before the collection of SAD or the information to come from an electronic identity provider. The confidentiality and integrity of the key signing is ensured by the remote SCDev. SAP allows secure use of the signing key by the cryptographic module. SAP is a protocol in which the signer (via SIC) and TW4S communicate to generate SAD. SAP authenticates the signer, certifies the authenticity of the signature request with specific SAD, the validity of the selected signing key, and ensures the secure transfer of all SAD elements. The remote SCDev is under the control of the SIC. The remote SCDev is managed through SAP and ensures that the signing operation is under the sole control of the signer. SSA interfaces enable, through a secure channel between the SAM and the remote SCDev, for the SAM to verify the SAD to enable the activation of the corresponding signing key. The system allows for the use of SSA for the purpose of group/batch signing, by using more than one DTBS/R within a single SAD. The sole responsibility for the proper handling of SAD lies with SAM.

SIC is a component managed by the signer's mobile application and is entirely under its control. The component is needed to provide "sole control" for security level 2 (SCAL2), which ensures that the signing keys are used with a high level of reliance under the sole control of the signer. The SIC component is essential in the SAP process and for the creation of a digital signature by the signing server application (SSA). The SIC imposes the connection between the signer and the signing operation in SAP. The SIC participates in SAP at all times to authenticate the signer and directly generate SAD. The SAD is then used by the SSA to enable signing using

an X.509 Qualified Electronic Signature Qualified Certificate (QESQC). SIC relies on the security of the mobile phone's built-in security chip. SIC generates SAD and uses a cryptographic asymmetric key for digital signing of the final SAD request.

SAM is specialized software that uses SAD to ensure with a high degree of certainty that signing keys are used under the sole control of the signer for the SCAL2 level. Evrotrust has fulfilled the requirement that SAM be used in a tamper protected environment by using a module certified for this purpose. SAM is responsible for the implementation of SAP. It provides a set of components: generation of SAD, generation and activation of the signing key.

SCA is a software application component that creates a signed document using the digital signature generated by the server signing service (SSASC) component. The SCA manages the document to be signed and submits the part to be signed to the SSA. SCASC is the component that supports Advanced Electronic Signatures (AdES)/Qualified Electronic Signatures (QES), digital signature creation, and the performance of several specific parts of the signature creation process. The SCA is able to interact with SSASC to request the creation of digital signature values. The SCA interface receives the document(s) to be signed and other parameters, including the X.509 Qualified Electronic Signature Qualified Certificate (QESQC) of the end user as the primary input and the signed document(s) as the primary output.

The use of the authorized signer's key is made by the **SSA** which authenticates the signer. The signer must be successfully authenticated in the SSA to provide access to the signing operation. The signer's signing key is connected by the SSA to the signer's authentication factor. The confidentiality and integrity of the key signing is ensured by SCDev. SCDev may be activated by the SSA. The activation of the signing key requires that the signer be authenticated by the SSA. Only after successful authentication of the signer is it possible to use the relevant key on behalf of the signer.

Evrotrust has built a **Tamper Protected Environment** to provide its service which is protected against direct internet access. Evrotrust ensures the integrity of the code implemented in this environment. The code protects the use of signing keys and fulfills the requirement that the signature activation be under the control of the signer. The tamper protected environment protects the connection between the signing keys and the signer (when creating a signature, the connection is created and verified).

The **TSP protected environment** is checked in accordance with the requirements for

secure operation of the server signing system. It protects against internet attacks and processes internet connections to/from the external environment (e.g. with the signer, SCA, RO (RA)). The signer environment is local to it and the signer shall be responsible for its protection. Where the signer uses an environment provided by a third party, then such third party shall be responsible for protecting the signer environment. The signing environment consists of elements that can be used to prepare the document for signing, signature formatting and SIC. The SIC is used by the signer to create a connection between itself and the entire signing operation activated through SAP.

4.3 CRYPTOGRAPHIC KEYS

TW4S uses and manages cryptographic keys to ensure the integrity, confidentiality, and certification/authentication functions within its own subsystems and between subsystems. Unauthorized use, disclosure, modification or replacement of these keys would result in a loss of security in TW4S. Evrotrust fulfills the requirement that these keys be managed securely throughout their lifecycle. The keys are:

- user signing keys – as regards security requirements, these keys are considered highly sensitive;
- infrastructure keys used by TW4S - these keys are considered highly sensitive too, but due to their distributed characteristics they are less sensitive as compared to the signers' signing keys;
- control keys used by the TW4S management personnel - these are the least sensitive keys used by Evrotrust, since they are used by TW4S management personnel. These keys are used by trusted parties and have a shorter life;
- session keys that are used for single/short transactions - these keys are treated as sensitive information, but with lower security requirements.

Private keys are generated and used in a certified SCDev. The SCDev used by Evrotrust is a reliable system with a security level of EAL 4 or higher, in accordance with ISO/IEC 15408, or equivalent nationally or internationally recognized security assessment criteria. The security profile for the cryptographic module shall meet the requirements specified in EN 419 221-5. SCDev supports cryptographic algorithms and key lengths in line with ETSI TS 119 312. Within TW4S, Evrotrust does not use any private keys that are not protected by SCDev. If it is necessary

to use private or secret keys (e.g. infrastructure, control) to be used outside the SCDev, Evrotrust will apply safeguards to ensure their integrity. The SCDev is initialized before a signing key is generated, with technical mechanisms requiring at least two operators.

All private keys (incl. signers', infrastructure and control keys) are stored securely, in a protected state. In cases where it is necessary to export a private key from SCDev, Evrotrust will apply encryption protection to ensure its confidentiality and integrity, up to the same or higher level of security like the one within SCDev. TW4S ensures that backups, storage and recovery of private keys (including the signer's signing key, infrastructure and control keys) are performed by authorized personnel only. Master cryptographic keys used to protect both user and operating keys are archived, stored and recovered by at least double control. Such keys are kept outside the SCDev in a protected form.

Evrotrust ensures that all private cryptographic keys (incl. user, infrastructure and control ones) are used only for their intended purpose, are not shared, unless their intended purpose requires it and they have access controls available.

When keys are distributed, Evrotrust ensures that all private cryptographic keys (incl. user, infrastructure and control ones) are transmitted in a secure manner. All keys used to protect other private keys during transmission are at least as reliable as the transmitted keys. Infrastructure and control keys are changed periodically, with a frequency complied with the risk assessment. The keys are changed immediately in case an algorithm or length is considered inappropriate or in case they are compromised or suspectedly compromised.

Signing keys are not archived, but are destroyed securely after the expiration of the validity of the certificates associated therewith or in case they become unnecessary for the signers. In the event that the connection between the signing key and the signer is not maintained after the signing operation session, the signing key will be destroyed at the end of the signing operation session. The signing key destruction mechanism and procedure ensure that all backups of the destroyed key are destroyed too and that no residual information can be used to recover the signing key.

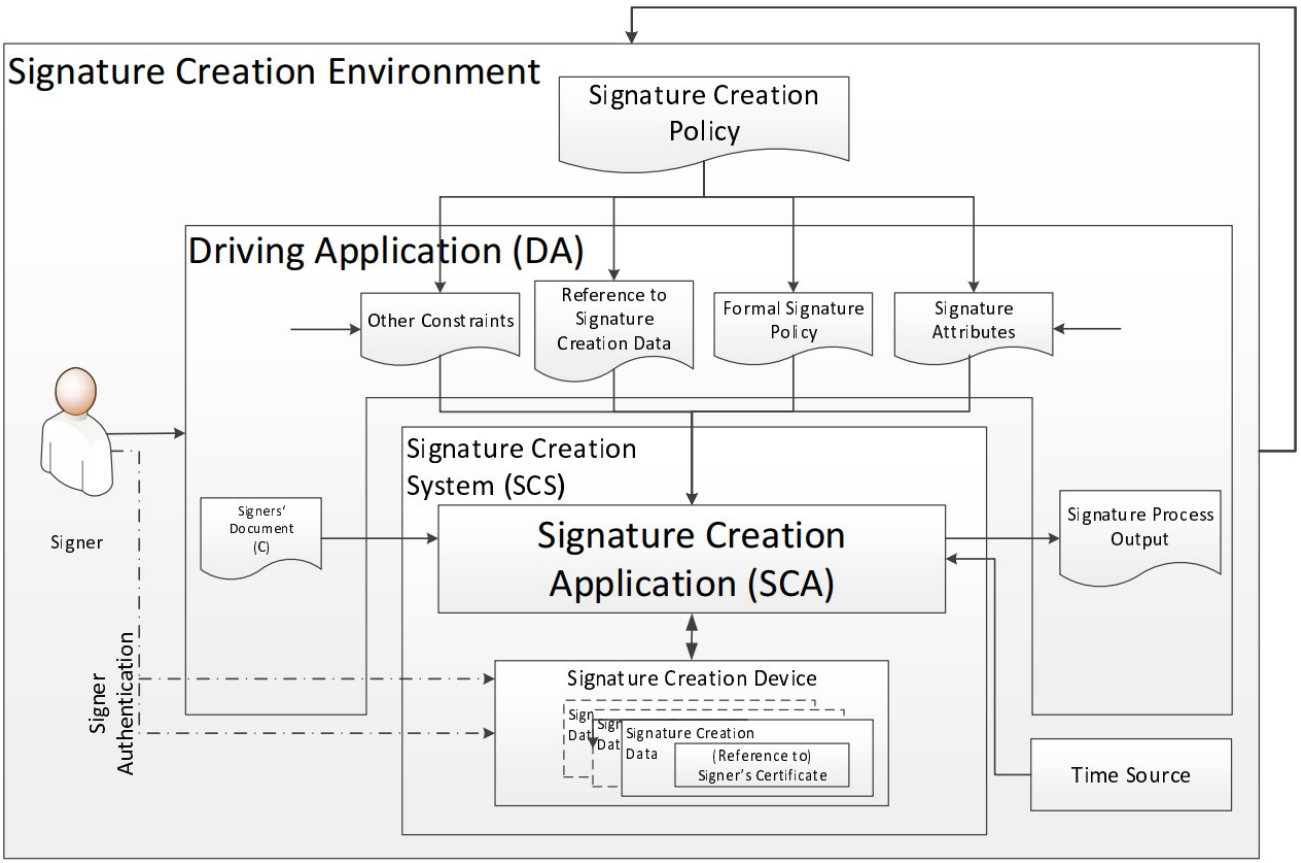
4.4 REQUIREMENTS TO IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Evrotrust applies the following requirements to the identification and authentication functions:

- The identification and authentication functions restrict the access and use of TW4S to authorized persons only. Evrotrust applies this rule to all management components;
- TW4S requires that each user identifies itself and be successfully authenticated before authorizing any action on behalf of such user or the role assumed by the user;
- Re-authentication is mandatory after logging out of the system;
- Evrotrust uses a combination of authentication data that is unpredictable;
- There are mechanisms in place for privileged users which reduce the risk during a certified user session and if the user's input device is left unattended, after a certain period of inactivity the user session will be terminated;
- Where the number of failed authentication attempts by the same user reaches the maximum number of allowed attempts, TW4S will prevent further user authentication attempts until administrative intervention to unblock the user (or within a certain period of time).

5 SIGNATURE CREATION FUNCTIONAL MODEL

The purpose of creating a signature is to generate a signature that covers the signer's document (SD), the signing certificate or a reference thereto, and a number of attributes that support the signature. The functional model used by Evrotrust is consistent with the requirements of ETSI TS 119 102-1. The signature creation environment consists of a user, who wants to create a signature (signer), a driving application (DA/DIS) (organizes all processes and interactions with end users / signers and integrated third parties) and a signature creation system (SCS), which implements the remote signing functionality.



The signature creation system (SCS) contains a signature creation application (SCA) and a signature creation device (SCDev). The SCA is serviced by SCASC. The SCS receives the document to be signed, along with other data from the DA. It composes the data to be signed (DTBS) and formats it (DTBSF). It creates a signature on the DTBSF and formats the result in the signed data object (SDO) corresponding to the desired signature format (CAdES, XAdES and PAdES). Finally, it returns the SDO and a status indication to the DA.

The signature creation device (SCDev) has a signing certificate, stores the relevant signature creation data, authenticates the signer and creates the signature value using the signer's signature creation data. Evrotrust uses various ways to implement signature creation procedures, as part of application software on a computer with a graphical user interface, as a web service or web application and others.

The signature creation process is controlled by a set of **constraints**. Evrotrust uses a formal signature creation policy and applies specific controls which are described in internal documents of the organization. DAs provide additional constraints to the SCA through parameters selected by the application or the signer. Such constraints affect the signature creation process and the

creation result, regardless of where they are defined:

- by using a signature creation policy (machine processed);
- explicitly in system-specific control data: e.g. in conventional configuration files as a property (.ini/.config files) or stored in a register or database;
- implicitly in the performance itself;
- additional constraints may be given by the SCA DA through parameters selected by the application or the signer.

The document to be signed (SD) is the document whereon the signature is generated or whereto the signature is connected. SD is selected or composed by the signer or by the DA. It may be in a revisionable format, such as a word processing document, message or file, which can be edited and where its performance depends on the current configuration of the viewing device. It can be in an unambiguous form (e.g. .pdf, .xml, etc.). These formats contain complete submission rules that ensure that the signed document is the same one that was submitted for signing. The document may be in a form that is not normally represented directly to the signer or certifier, or it may be in a form that is inherently represented to the signer and verifier in different ways. Evrotrust supports different electronic formats of input files, such as TXT, DOC, ZIP, AVI, MP3 and other computer files.

Signer's document representation (SDR) is used in the calculation of the signature as an SD representation. SDR can be provided by the DA to the SCA. Each time the DA does not provide a SDR, the SCA will calculate the SDR from the SD applying the algorithm specified in the signature creation policy used. It is not possible to find another SD that is represented by the same SDR. Some signature formats do not include SD directly in the signature. The SDR is usually built on an SD cryptographic hash.

The data to be signed (DTBS) is made up of the information objects that will be covered by the signature. These are: SD (or SDR) and the signature attributes selected for signing along with the SD. The DTBS construction may include form-specific pre-processing. Data to be signed formatted (DTBSF) is created by DTBS objects, it is formatted, hashed, and the result of this process (DTBSR) is used in the signature creation process. The SCDev takes the DTBSR and applies an algorithm in accordance with ETSI TS 119 312. The signed data object (SDO) contains the signature value and the signed attributes. It may also contain additional unsigned attributes.

5.1 SIGNATURE ATTRIBUTES

Signature attributes are information elements that support the AdES signature and its intended purpose, and can be covered by the signature along with the SD. Signature attributes can be selected via DA or automatically inserted into the signature by the SCS.

Attributes are either signed attributes, i.e. attributes that are covered by the signature, or unsigned attributes, i.e. attributes that are not protected by the signature. Unsigned attributes can also be added to the signature at a later stage. The set of attributes included in the signature is determined by the signature creation policy used or, where a signature is supplemented, by the signature extension policy used, in accordance with the requirements of ETSI TS 119 172-1 and may also depend on the specifics of the form.

The main signature attributes, in accordance with ETSI TS 119 102-1, are:

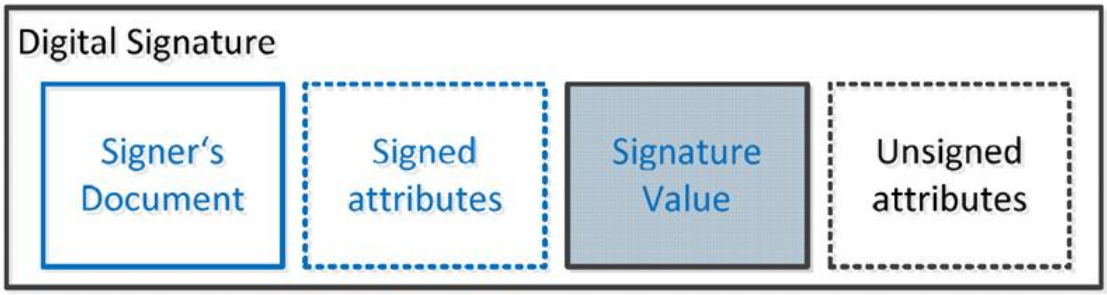
- **Signing Certificate Identifier** - This signed attribute contains a reference to the signing certificate. It prevents the reference certificate from being replaced by another, with different semantics, but with the same public key. If the signer holds different certificates related to different signature creation data, it shall show the verifier the correct data for the purpose of verifying the signature. This attribute may also contain references to some or all certificates in the Evrotrust certification hierarchy. For each certificate, the attribute contains a calculated checksum (message digest) along with a unique identifier of the algorithm that was used to calculate such checksum. That algorithm is a cryptographic hash function.
- **Signature Policy Identifier** – This signed attribute contains a unique identifier of the signature creation policy that is applied during signature creation;
- **Data Content Type -** This signed attribute indicates the data content type (SD);
- **Commitment type indication –** This signed attribute indicates the type of commitment taken by the signer when signing certain documents. The indicated type of commitment is expressed in the form of an OID or URI. It may contain a sequence of qualifiers providing further information about the commitment. If there is a reference to the signature creation policy and the said policy lists a set of permitted types of commitments, the content of this attribute is selected from the set defined by that policy. If the AdES signature does not contain any recognized type of commitment, then the semantics of the AdES signature will depend on the semantics of the document being signed and the context in which it is used;
- **Counter Signatures –** This unsigned attribute is a signature counter. This attribute

contains at least one signature;

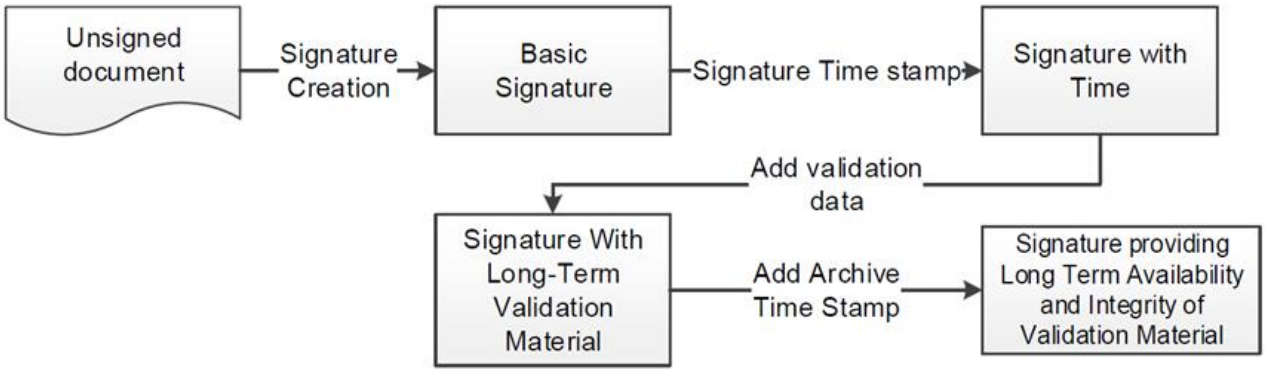
- **Claimed Signing Time** - This signed attribute represents the requested signing time. This attribute contains the time for which the signer claims to have completed the signing process;
- **Claimed Signer Location** - This signed attribute represents the requested location of the signer. This attribute indicates the address associated with the signer in a specific geographical (e.g. city) location where the signer claims to have submitted the signature;
- **Signer's Attributes** - This signed attribute contains signed certificates that the signer claims to have held when the signature was generated. It is applied when the signer's position within a company or organization is important, or when the signer is authorized to do so.

5.2 SUPPORTED SIGNATURE CLASSES

The signature structure common to all signature classes consists of the signer's document, the signed attributes that are included in the calculation of the signature value, the signature value, and all unsigned attributes that are also included in the signature.



The steps in the signature lifecycle have been defined as signature classes that have common properties. The process of creating a type of signature class based on the signature of another class following this lifecycle is also called signature extension and is governed by a signature extension policy. The diagram that illustrates the signature lifecycle is as follows:



Each signature class corresponds to a combination of attributes added to the signature with the purpose of improving the ability to validate the signature in the future, when the relevant certificate required for successful validation may have expired, have been revoked or the algorithms used are no longer strong enough to be reliable. The types of signatures are:

- the main signature is the one that can be validated, as long as the relevant certificates have neither been revoked nor expired;
- a signature with time is a signature that proves that the signature already existed at a certain point in time;
- a signature with long-term validation material is a signature that ensures the long-term availability of the verification material, by including all materials or references to materials required for signature validation;
- a signature providing the long-term availability and integrity of the digital signature validation material can help validate the signature outside of events limiting its validity (e.g. weakness of cryptographic algorithms used, certificate expiration, or key sizes used are no longer relevant).

Evrotrust maintains signature classes in accordance with ETSI TS 119 102-1 which are summarized in the below table:

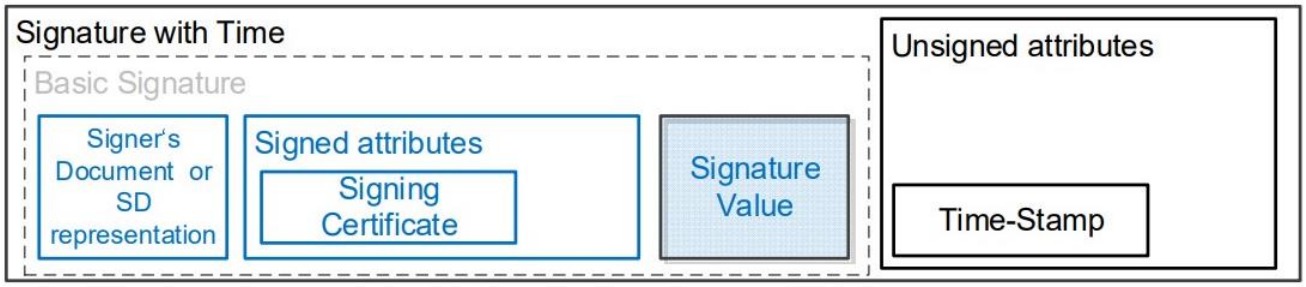
AdES-Level **Baseline**	**Basic Signature**	**Signature With Time**	**Signatures with Long-Term Validation Material**	**Signatures providing Long Term Availability and Integrity of Validation Material**
CAdES-B-B, XAdES-B-B, PAdES-B-B	×			
CAdES-B-T, XAdES-B-T, PAdES-B-T		×		

CAdES-B-LT, XAdES-B-LT, PAdES-B-LT			×	
CAdES-B-LTA, XAdES-B-LTA, PAdES-B-LTA				×

5.3 SIGNATURE EXTENSION

5.3.1 CREATION OF A SIGNATURE WITH TIME

The SCASC supports the inclusion of timestamping in the digital AdES signature, as a result of which it is proved that the signature already existed at a certain point in time. The time is provided by time-assertions/time stamp token of the signature as an unsigned property (unsigned attribute) added to the main signature as a result of extension (enhancement) of the signature.



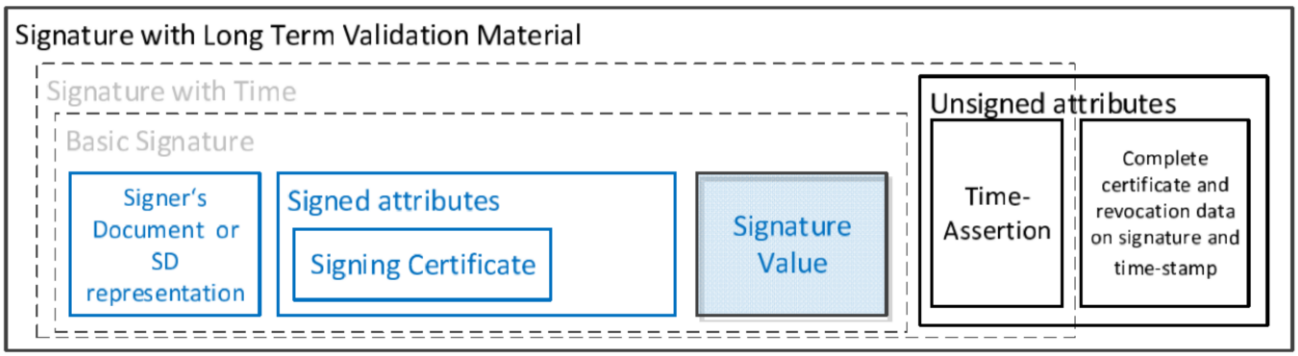
The "Evrotrust TSA" Time Certification Authority, through its "Evrotrust TSS" (Timestamping service) is provided by Evrotrust in accordance with ETSI EN 319 422. By including an object identifier: 1.3.6.1.4.1.47272.1.2.1 in the time-assertions/TST issued, Evrotrust confirms compliance with the "Policy and Practice for a Qualified Electronic Time Stamps Provision Service". For the purpose of signing user certificates with included time stamp, SCASC uses the length of the signing key and the signing algorithm according to ETSI TS 119 312.

5.3.2 CREATION OF A SIGNATURE WITH LONG-TERM VALIDATION MATERIAL

The validation algorithm can evaluate the validity of a signature with time, which can be supplemented to form a signature with a long-term validation material (LTV) by adding unsigned attributes. Such extension may be performed by a SCA, a third party, or a verifier using SVA.

Signature validation can be performed while the validation data is accessible online for verifiers and the Proof of Existence (POE), i.e. the attributes are available. In case it is not certain

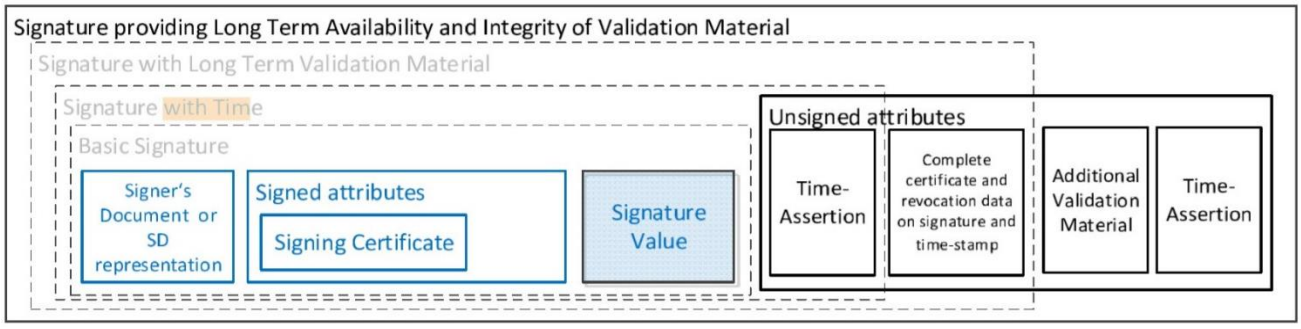
that the validation data will be accessible online or the verifiers cannot access that data, then it is necessary to take that data from the signature.



When creating a signature, an attribute is added containing long-term validation data, which enables the verification of the signature after the expiration of the validity of the signing certificate.

5.3.3 CREATION OF A SIGNATURE WITH LONG-TERM AVAILABILITY AND INTEGRITY OF THE VALIDATION MATERIAL

Before the algorithms, keys, and other cryptographic data used during signature creation become weak and the cryptographic features become vulnerable, or the certificates supporting previous time-assertions expire or are revoked, the signer's document, the signature, as well as all attributes contained in the signature with long-term validation material must be protected by applying one or more time-assertions. Such time-assertions link the data to a specific period, establishing evidence that the latest data existed at that time. Such additional time-assertions are added to the signature as unsigned attributes to ensure the long-term availability and integrity of the validation material and are thus called attributes for long-term availability and integrity of the validation material. The creation of time-assertions is repeated in time before the protection provided by previous time-assertions becomes weak. The security uses stronger algorithms or longer key lengths than those used in the original signatures or in previous time-assertions.



The signature creation process providing long-term availability and integrity of the validation material returns the signature provided as an input, supplemented by an unsigned attribute for long-term availability and integrity of the validation material, i.e. timestamp marker or evidence of signature. Also, additional validation material can be included in the signature as an unsigned attribute.

5.4 SUPPORTED SIGNATURE FORMATS

CARRIER (CONTAINER)	SIGNATURE FORMATS	SIGNATURE PACKAGING	LEVEL OF SERVICE
-	CAdES	Enveloping	BASELINE_B BASELINE_T BASELINE_LT BASELINE_LTA
-	CAdES	Detached	
-	PAdES	Enveloped	
-	XAdES	Enveloped	
-	XAdES	Enveloping	
-	XAdES	Detached	
ASiC-S	CAdES	Detached	
ASiC-S	XAdES	Detached	
ASiC-E	CAdES	Detached	
ASiC-E	XAdES	Detached	

1) Evrotrust supports the following signature formats:

CAdES - defines an advanced electronic signature format based on Cryptographic Message Syntax (CMS). The format allows electronic signing of random files. The extensions of the final signed files are .p7m (for enveloping signature type) or .p7s (for detached signature type). A .pkcs extension is also allowed.

PAdES - defines an advanced electronic signature format based on PDF (Portable Document Format). The format allows electronic signing of PDF files only. Only the enveloped signature type is supported. The allowed file extension after signing is .pdf.

XAdES - defines an advanced electronic signature format based on XML (Extensible Markup Language). The format allows electronic signing of XML files only. The enveloped, enveloping and detached signature types are supported. The extension of the signed file is .xml.

ASiC-S - using a single signature-related carrier (ASiC-S) to cover the file. The name of the final signed file has the .asics extension.

ASiC-E - using extended signature-related carrier (ASiC-E) to cover the file. The name of the final signed file has the .asice extension.

2) **Applicable types of signing indicating the location of the signature itself:**

Enveloped - an electronic signature built into the file which complements the original file.

Enveloping - an electronic signature built into the file which as a package envelops the entire original file.

Detached - an external electronic signature wherein the signature and the document are located in separate files.

3) **Level of service –** different levels of service are applied to each signature format by adding different attributes ensuring the long-term validation of the signature:

BASELINE_B - basic electronic signature/seal profile

BASELINE_T - basic electronic signature/seal profile with certified timestamping

BASELINE_LT - basic electronic signature/seal profile with certified timestamping and enabled status (CRL/OCSP) of the used certificate

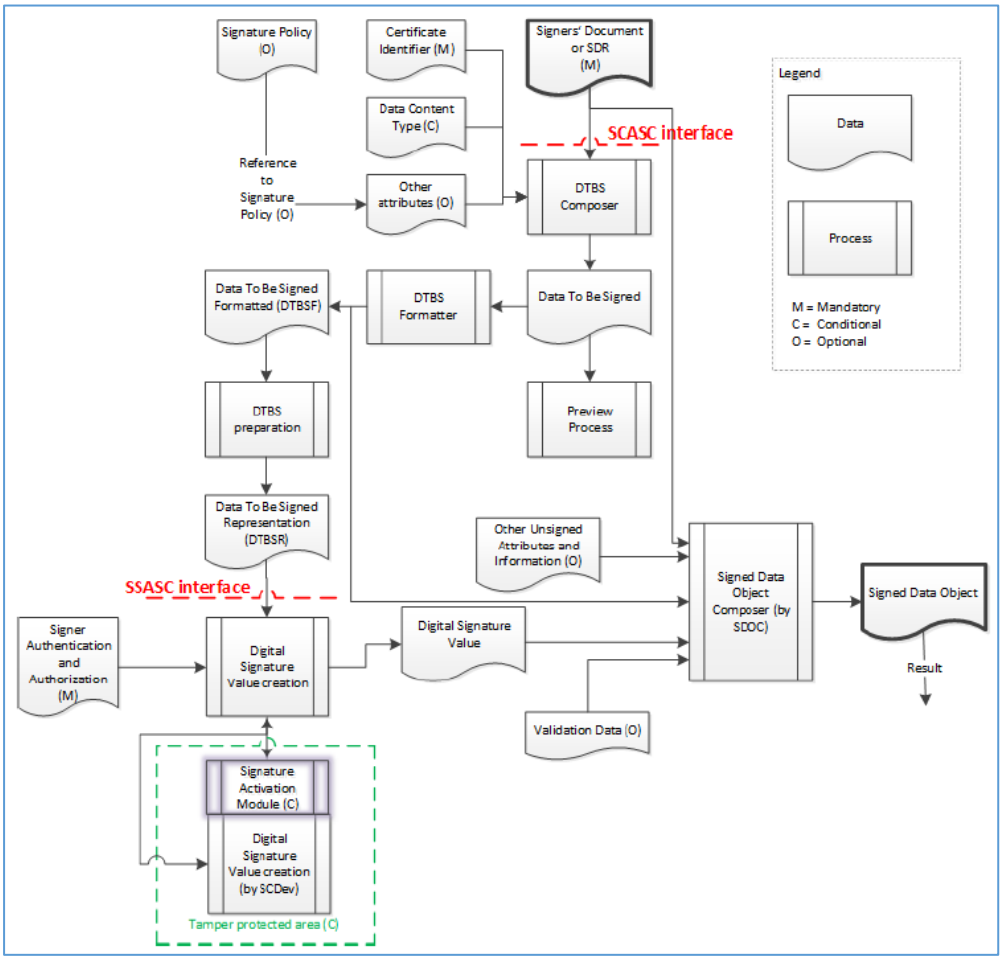
BASELINE_LTA - basic electronic signature/seal profile with certified timestamping, enabled status (CRL/OCSP) of the used certificate, as well as additional certified time for long-term storage (LTA)

6 COMPONENTS, PROTOCOLS AND INTERFACES OF THE REMOTE SIGNATURE CREATION SERVICE

For the components providing specific functionalities of the remote AdES signature creation service, Evrotrust applies protocols and interfaces in accordance with the requirements of ETSI TS 119 102-1 and ETSI TS 119 432.

6.1 MAIN COMPONENTS AND INTERFACES OF THE SERVICE

The schematic diagram that illustrates the signature creation process and shows the different steps and their related data elements in the remote signature creation process is shown below. The process is limited to the building blocks and information required to create a signature, without taking into account issues such as signer's authentication, authorization to use the signing key, or the availability of a signing certificate. The signature activation module in the tamper protected area is only required when the signature creation service complies with the Level 2 signature activation mechanism (SCAL2).



AdES and/or digital signature value (DSV) is created through the use of a private key held

in a cryptographic security module called a signature creation device (SCDev) managed by Evrotrust (SCSP/Signature Creation Service Provider). Based on the different types of data managed in the requests and responses, two main components have been identified providing different signature management interfaces: the electronic signature application service component (SCASC) and the server signing application service component (SSASC). SSASC is the component that supports the creation of digital signature values. SSASC interacts with the SCDev which holds the signer's private key. When SSASC uses SCDev, the signer is able to control the signing key with a certain level of reliance.

The SSASC interface contains Data To Be Signed Representation (DTBSR) and other parameters as the main input and the digital signature value as the main output. SCASC is the component that supports the creation of an AdES digital signature and implements several specific parts of the signature creation process. SCASC interacts with SSASC on a request to create digital signature values.

The SCASC interface contains the document to be signed (SD) or its representation (SDR/Signer's Document Representation), as well as other parameters as the main input and the signed document or digital signature as the main output. Evrotrust plans to build such interface in case of need for integration with third party services.

SCS is a service of Evrotrust that implements a signature creation application (SCA) and a server signing application (SSA). The signature is created by a SCA which creates a signed document using a digital signature generated by SSASC. The SCA manages the document to be signed and transfers it to a server signing application (SSA). The SCA is able to interact with SSASC on a request for the creation of digital signature values. The SCA interface receives the document to be signed and other parameters, including an X.509 certificate for the signer's electronic signature as the main input and the signed document as the main output. Several options of these interfaces are possible depending on the functional split between the SCS and the local signing system.

6.2 SIGNATURE CREATION APPLICATION (SCA)

The signature creation process commences with the signer's document (SD) to be signed. The SD document is represented (SDR) with its hash value in the Data To Be Signed (DTBS). The creation of SDR (hashing) can be done where the SD is stored or by SCASC. In the first case, the

SDR is transferred to the SCASC, while in the second case, the SD is transferred to the SCASC. The SD is part of the final signed data object (SDO). Part of the Signed Data Object Composer (SDOC) function (building the final AdES format) is to link the digital signature value to the SD.

The creation and formatting of the DTBS, the hash of the document to be signed (SDR), and the hashes of all signed attributes are collected in the Data To Be Signed Formatted (DTBSF). In addition to the certificate ID (the signing certificate hash, and possibly the additional certificates from the certification chain), the standard ETSI signature formats (C/X/PAdES) may require or allow additional signed attributes. For example, all baseline CAdES and XAdES require the presence of the signed "document type" (on a SD) and "requested signing time" attributes. The signed attributes or their hash values whose presence is required in the DTBS are accessible for the SCASC when the DTBSF is created by the SCASC.

SCASC prepares the entire DTBSF, calculates the hash, and sends the value (DTBSR) as input to SSASC.

The construction of SDO (AdES format) consists in combining the digital signature value with other parameters in the required format. Depending on the format, the digital signature provided for SD is:

- Enveloped, when the signature is added to the SD (e.g. PAdES format);
- Enveloping, when the signature envelops the SD (e.g. some CAdES formats);
- Detached, when the signature is a separate object linked to the SD.

SDO creation is performed by a separate service component or integrated with other functions in the SCASC.

6.3 SERVER SIGNING APPLICATION (SSA)

The purpose of the signature creation process is to take the DTBSR and create a digital signature value under the signer's control. The creation of the digital signature value is controlled by SSASC which uses a signing key stored in a cryptographic module (SCDev). Signers can activate the key by means of a secure authorization and activation process. SSASC uses a remote SCDev to generate, maintain, and use signing keys under the signers' control. The signer remotely controls the signing key with a certain level of security using the signature activation module (SAM). SAM is a software component that uses signature activation data (SAD) to authenticate the signer and obtain permission to activate its signing key for DTBSR signing purposes. This process

gives certainty that the signing keys are under the signer's control. Evrotrust can apply two different levels of reliance in the control of the signing key in its activities. In "sole control" level 1 (SCAL1), the signing keys are used with a low level of reliance, under the sole control of the signer. The use of the signing key is made by the SSASC which authenticates the signer. The activation of the signing key may remain for a certain period and/or for a certain number of signatures. In the provision of "sole control" level 2 (SCAL2), the signing keys are used with a high degree of reliance, under the sole control of the signer. The use of the signing key is made by the signature activation module (SAM) by means of signature activation data (SAD) provided by the signer, using a signature activation protocol (SAP) and enabling the use of a specific key for the signing of specific documents.

The signature creation process is performed by a remote SCDev. The signing key can be used to generate the digital signature value after successful authentication of the signer by SSASC (SCAL1) or after successful verification of SAD by SAM (SCAL2).

6.4 INTERACTION OF SCASC AND SSASC

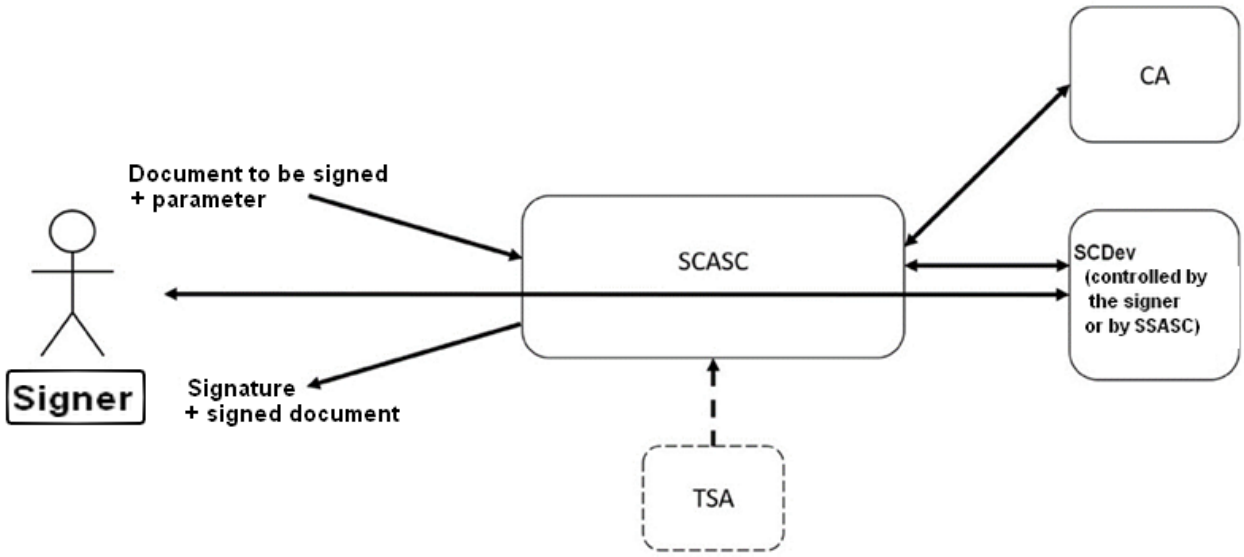
The system architecture supporting remote server signing includes the interaction of SCASC and SSASC with other parties involved in the remote signature creation process, and takes into account the level of reliance in the control of signing keys (SCAL1 and SCAL2).

The system supporting remote server signing (applies to both AdES and QES) includes SCASC which is linked to the SSASC hosting the remote SCDev. Services such as CA, RA, OCSP and CRL, TSA and authentication and/or authorization servers are considered external to the scheme.

Evrotrust applies protocols that enable both SCASC and SSASC to apply group signing for documents, document hashes and DTBSR. In such batch document signature processes, the signer is not required to explicitly approve each document signature.

7 COMPONENTS OF THE EVROTRUST SERVICE SUPPORTING THE CREATION OF ADES DIGITAL SIGNATURE

7.1 SCASC SERVICE ARCHITECTURE



The electronic signature creation application service component (SCASC) receives the document(s) and/or hash(es) of document(s) to be signed and optionally some signature parameters, collects all the information required for the creation of the signature, prepares the formatted data that is used to calculate the digital signature value (e.g. hash value) (Data To Be Signed Representation/DTBSR) and sends it to a signature creation device (SCDev). The digital signature is used to represent an electronic signature or electronic seal. A digital signature can be created under the control of an individual or legal entity. The term signer covers an individual or legal entity. The term SCDev is used for a device creating a signature or a seal. The SCDev is controlled by the SSASC. The SCDev, controlled by the signer (SCAL2) or by SSASC (SCAL1), monitors the authentication and signing process and returns the digital signature value. The digital signature value is included by the SCASC in the electronic signature. The SCDev is a hardware security device complying with the EN 419 211 series or the CEN TS 419 221 series. In its protected environment, data tampering for the purpose of creating a digital signature is not permitted. SCASC is the signature creation application (SCA) described in EN 419 241-1. The SCA creates a signed document using the digital signature generated by the remote SCDev, whereby the authorized signer remotely controls the signature key with a high level of reliance.

7.2 TECHNICAL REQUIREMENTS OF THE ELECTRONIC SIGNATURE CREATION APPLICATION SERVICE COMPONENT (SCASC)

Evrotrust performs its activity of providing a remote electronic signature/seal service, fulfilling the following technical requirements for the SCASC interface:

- When SCASC has a machine-accessible interface to connect to its service, it uses a protocol defined in ETSI TS 119 432. Evrotrust applies the requirements of the Standard on the semantics of protocols on requests for digital signature creation to a remote server and for the purpose of obtaining the related response. For the semantics of the protocols, Evrotrust applies a link in XML and/or JSON formats;
- Evrotrust uses a secure and safe connection between SCASC and SCDev to create the digital signature value;
- Evrotrust makes sure that when SCASC submits, either directly or indirectly, a document to be signed, what the signer sees is what it actually signs (WYSIWYS). Evrotrust, as the owner of the digital signing system, makes sure that the semantic content of the signed documents cannot be changed, either accidentally or intentionally. When digitally signing a document, the integrity of the signature is ensured by the reliability of the digital signing algorithms (algorithms in accordance with ETSI TS 119 312 are used, which are also used to maintain the security of the computer system used to sign the document). In order to achieve a high degree of certainty in the signer that the files are not tampered, Evrotrust uses cryptographic algorithms that provide checksums SHA256, SHA384 and SHA512. Evrotrust provides an opportunity for the visual representation of the digital document and the possibility to verify the digital signature;
- As a signature creation application (SCA), Evrotrust uses the Digital Signature Services (DSS) in accordance with the eIDAS, ETSI and CEN remote signing requirements. It includes specific recommendations and know-how that have been developed in previous installations and maintenance of the DSS library;
- When SCASC provides the signer with the document to be signed, the user shall keep in mind that the types of content that can be properly represented are: PDF and XML and random files with a built-in electronic signature, XML and random files with external electronic signature, as well as single and extended signature-related carriers (containers) to cover the

original file and its signature;

- Evrotrust makes sure that the SCASC correctly represents to the signer all types of content of digital signature documents, which can also be signed on paper. Their representation is done through intermediate components (DA/DIS, Mobile Application) which are located between the signer and the SCASC, but it is also possible for them to be directly provided by the SCASC;
- when SCASC/intermediate component represents the document to the signer, the interface warns the signer if it cannot accurately represent all parts of the document to be signed (SD/Signer's Document) according to the type of data content;
- when SCASC/intermediate component represents the document to the signer, Evrotrust provides a workflow wherein the signer agrees to the signing of the document;
- when SCASC/intermediate component represents the document to the signer, the SCA ensures that when the SD is represented to the signer, it is the same data that will be signed in the signing process. The SCA calculates the signature after representing the DTBS (Data To Be Signed)/SD to the signer. In the case of a group signing, the signer may not receive all submitted DTBS/SD;
- when SCASC/intermediate component represents a document to the signer, the SCASC/intermediate component or intermediate component enables the downloading by the user of the document to be signed;
- when SCASC/intermediate component represents a document to the signer, the SCASC/intermediate component records how long the document has been represented to the signer;
- when SCASC/intermediate component represents a document to the signer and the document has been downloaded, the SCASC/intermediate component records this event.

7.3 REQUIREMENTS TO THE CREATION OF ADES DIGITAL SIGNATURE

Evrotrust performs its activity of providing a remote electronic signature/seal creation service, fulfilling the requirements as follows:

- SCASC guarantees the integrity and confidentiality of the information received.
- Evrotrust uses only cryptographic algorithms recommended by ETSI TS 119 312;
- All used cryptographic RSA and DSA and ECDSA algorithms have been complied

with the technical specification ETSI TS 119 312. Evrotrust regularly monitors the security and applicability of the hash algorithm used. All algorithms used are verified once a year or upon the occurrence of any changes. In case an algorithm is compromised or becomes inappropriate, for this purpose it is proceeded to the re-generation of all keys affected (a description of the algorithms used and the length of the keys can be found in item 3.2 (a) of this document). For each supported profile, Evrotrust monitors the strength of each cryptographic algorithm used in connection with such profile. In case any of the used algorithms or parameters is considered less secure or the validity of the respective certificate is expiring, it will be updated or a new profile will be created;

- Evrotrust applies the following specific requirements:
  - DA/DIS ensures that the SD selected by the user for signing is the same as that provided by the SCA for signing;
  - when the signer has more than one signing certificate, DA allows the signer to select the certificate to be used to create the signature or to use a default certificate. If only one choice is possible, this step can be skipped;
  - SCA protects the link to the certificate or a copy of the signing certificate within the signature from undetected replacement after the signature is created. Evrotrust shall ensure that the signer is familiar with the scope of application of the signature and that the signature contains all the attributes necessary for the purposes of application;
  - When the signer's authentication data is passing through the SCA, the SCA maintains the confidentiality and integrity of such data and securely deletes it as soon as it is no longer needed;
- Evrotrust will inform the signer about all its obligations before entering into a contractual relationship. All documents are publicly available on the company's website;
- SCASC includes in the signature the chain of signing certificates;
- the signer has the opportunity to find out in advance which signature creation policy will be applied;
- the signer has the opportunity to find out which signature creation policy has been applied in the creation of the specific signature. Information on which signature creation policy will be or has been applied to a particular signature can be added as a signed attribute to the signature. If no specific policy is specified, the current version of the policy is considered to have

been used;

- SCASC provides the signature to the signer;
- If SCASC has access to the signed data, it provides the signed data together with the signature to the signer; This happens in cases where the signature is used to sign part of the its containing document (enveloped) or if it contains the signed data in itself (enveloping).

8 SERVICE COMPONENTS OPERATING WITH REMOTE QSCD/SCDEV

Evrotrust provides a service where digital signatures are entirely created in an environment operated by the user. In this case it is assumed that the data for the signature creation are under the control of the signer, who physically owns the private key access control device and, respectively, the electronic signature/seal placed. For creation of a remote digital signature, the data about the signature creation are stored and operated by Evrotrust on behalf of the signer. In order to guarantee the reliability of the signature creation environment and that the data about the signature creation are used under the signer's control, Evrotrust applies specific procedures for security management in accordance with the requirements of ETSI TS 119 431-1.

8.1 SSASC SUBCOMPONENTS

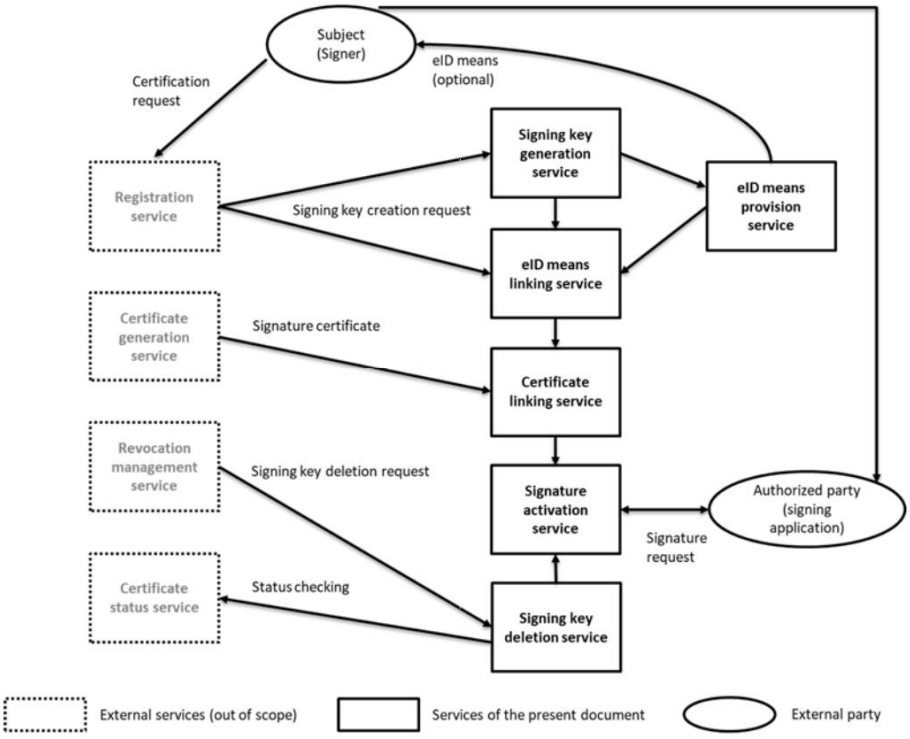
The server signing application service component (SSASC) contains the following subcomponent services:

- generation of signature keys: generates keys for signing on a remote device. The proof of ownership of generated signature keys is transferred to the registration system of Evrotrust that issues the respective certificate;
- provision of eID means: The Evrotrust electronic identification means (eID means) is generated by DIS and is a JSON Web Token (JWT) claim containing a unique signer identifier linked to an extension which includes the signatory's identification data tailored to a specific use of the means. eID means is provided by DIS to SSA. eID means is not provided to the signer;
- linking the electronic identification means (eID means): The eID means is linked to the corresponding signing keys to provide "sole control". The signer's key pair is not generated by the CA. The process of requesting an electronic signature certificate verifies whether the signer owns or controls the private key associated with the public key submitted for the issuance of the

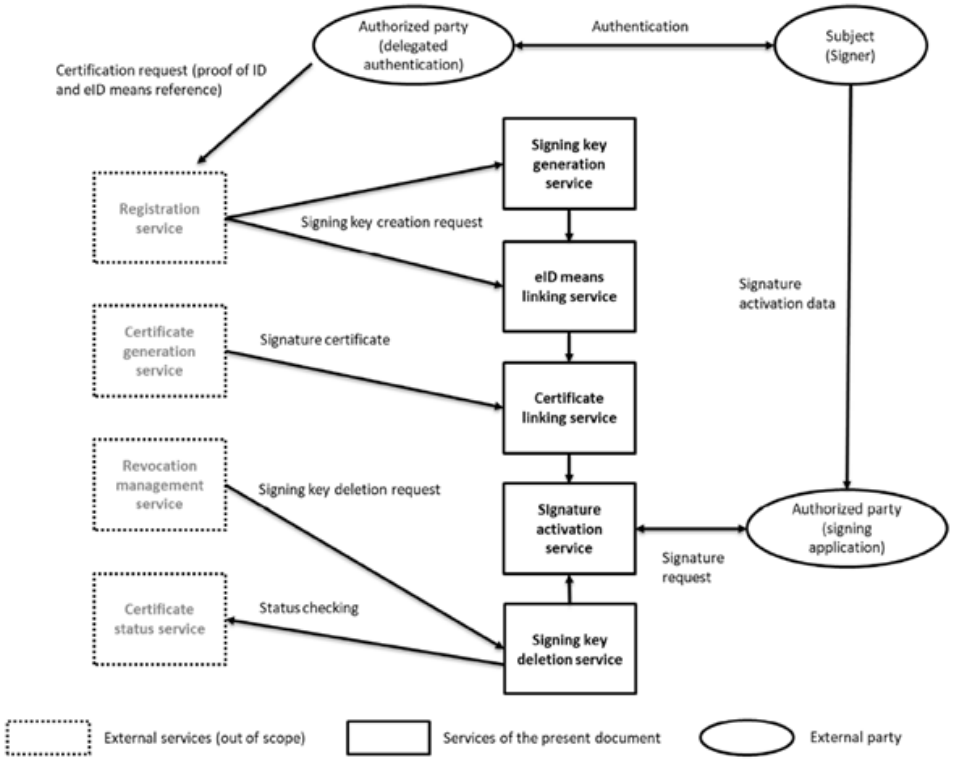
specific certificate;

- linking certificates: links the certificates issued to the respective signature keys generated and the eID means;
- signature activation: checks the signature activation data and activates the respective key in order to create a digital signature. Confirmation by the signer is required.
- deletion of signature keys: destroys the signature keys in a way that ensures that the signature keys may no longer be used.

A diagram presenting the links between the service subcomponents of the SSASC service and the external component services of Evrotrust issuing signing certificates:



A diagram showing the interrelation between Evrotrust's service for remote signing with an electronic signature and the link to the certification process delegated to an external party. The scheme will be applied after Evrotrust's integration with such a party:



The scheme illustrates the subdivision of the SSASC subcomponents with certification delegated by an external party.

8.2 INITIALISATION OF THE SIGNING KEY

8.2.1 GENERATION OF SIGNING KEYS

Evrotrust applies requirements for EUSCP (EU SSASC policy, which is in accordance with Regulation (EU) No. 910/2014), in the generation of signing keys:

- the signing key of the user is generated in QSCD;
- the qualified signature creation device (QSCD) operates in its configuration as described in the documentation accompanying its certification. QSCD that use Evrotrust are certified in accordance with the requirements of Regulation (EU) No. 910/2014, Annex II. The QSCD used by Evrotrust ensure the confidentiality of the data for creation of an electronic signature. These data are available only once and may not be subject to unauthorised extraction. Evrotrust uses a technology that provides reliable protection of the signature against forgery.

Evrotrust applies the following requirements in the generation of signing keys:

a) the private or secret keys and generated and used in SCDev. SCDev is a reliable system with EAL 4 or higher level of security or, respectively, CC EAL 4+ or higher, with protection

profiles in accordance with EN 419221–5;

b) the signers' signing keys are generated and used in SCDev. SCDev is a reliable system with EAL 4 or higher level of security or, respectively, CC EAL 4+ or higher, with protection profiles in accordance with EN 419221–5;

c) all algorithms are in line with the technical specification ETSI TS 119 312. Evrotrust regularly monitors the security and applicability of the hash algorithm used. All algorithms used are checked once a year or when changes occur. If the algorithm is compromised or becomes inappropriate, re-generation of all affected keys is undertaken for this purpose. Evrotrust monitors the strength of each cryptographic algorithm used in relation to this profile for each profile maintained. If one of the algorithms or parameters used is considered less secure or if the validity of the respective certificate expires, it is updated or a new profile is created. (*For description of the algorithms used and the length of the keys, see section 3.2 (a) of this document.)*

d) the private keys (including the signer's signing key, the infrastructure and control keys) are not held outside SCDev and in this way they are protected and their confidentiality and integrity is ensured;

e) SCDev is initialised before generating any signing key by technical mechanisms that require at least two operators;

f) the reliable system creates signatures by using algorithms that will survive the lifecycle of the signer's certificate;

g) the signing key can be generated in advance (i.e. it may not be linked to the public key certificate);

h) in case of SCAL2, the pair of keys is generated by using SAM, which ensures the ownership and control on the private key by the signer. The remote SCDev is a remotely controlled secure signature creation device provided by a signature activation module (SAM) and executed in an environment protected from forgery. This module uses the signature activation data (SAD) collected via a signature activation protocol (SAP) to ensure with a high level of confidence that the signing keys are used under the sole control of the signer.

8.2.2 LINKING THE EID MEANS

Evrotrust fulfils the following requirements for linking eID means:

- Evrotrust fulfils the requirements for SCAL1, where the level of security in case of a

request and registration is either low or higher. The characteristics and design of the eID means of Evrotrust correspond to a "low" or higher level of security. The certification mechanism corresponds to a "low" or higher level of security. Evrotrust provides high level of reliability of the signer's environment, thereby ensuring the lack of identity alteration misuse;

- Evrotrust fulfils the requirements for SCAL2, thereby ensuring resilience against threats for the signature activation protocol and the signature activation data, by applying "significant" or higher level of security for the requests and registration. The characteristics and design of the eID means of Evrotrust correspond to a "significant" or higher level of security. The certification mechanism corresponds to a "significant" or higher level of security;
- SSASP links the signing keys to a reference eID means of the signer;
- SSASP can generate a reference to a eID means and provide the corresponding eID means to the signer;
- SSASP guarantees that the identification data of the person in an eID means is the same as the data linked to the person by the associated certificate;
- if a reference to the eID means of the signer exists it may be provided by an authorized (external) party;
- if the entire or part of the certification process is delegated to an external party, SSASP guarantees that the external party meets the requirements for the respective level of security. If the external party uses electronic identification means issued under a notified scheme included in the list published by the Commission under Article 9 of Regulation (EU) No. 910/2014 for compliance with the regulatory requirements, Evrotrust does not require compliance with the necessary level;
- if the entire or part of the certification process is delegated to an external party, SSASP guarantees that:
  - the external party meets all requirements of this document and the requirements for registration in accordance with the applicable regulatory requirements, or
  - the certification process delegated to the external party uses eID means issued under a notified scheme in accordance with the applicable regulatory requirements;
- SSASP protects the integrity of the links between the signing key of the signer and their eID means.

8.2.3 LINKING A CERTIFICATE

The following requirements are applied for SSASC:

- a reliable system supporting server signing (TW4S) links the signing keys of the signer to the respective certificate accompanying the public key;
- the signing key is not used before TW4S links it to its certificate;
- TW4S protects the integrity of the links between the signing key and the certificate accompanying the public key.

8.2.4 DELIVERY OF EID MEANS

Evrotrust as SSASP securely and reliably delivers the eID means to the services that needs it in order for them to be able to correctly identify the signer, including the SSA, without the signer himself receiving it.

SSASP personalizes the signer's eID means with the user activation data (e.g. public part of the "sole control" key), whereby activation data (e.g. password for the private key usage) is securely prepared by the SIC and registered, separate from the signer's eID means.

8.3 OPERATIONAL REQUIREMENTS FOR THE SIGNING KEYS LIFECYCLE

8.3.1 SIGNATURE ACTIVATION

Evrotrust performs its signature activation service by fulfilling the requirements for EUSCP as follows:

- the signing key of the user is used in QSCD;
- QSCD operates in its configuration as described in the relevant documentation for certification or in an equivalent configuration that achieves the same security objective;
- Evrotrust uses a signature activation protocol (SAP), which provides cryptographically strong mechanisms that protect the certification factors from protocol compromising threats as well as from secure attacks to someone else's identity by third parties;
- Evrotrust has mitigated the threats for SAP and has undertaken measures for protection of SAP from secondary reproduction, measures against bypass, as well as continuous monitoring for false attacks between the signer and the remote SCDev;
- the signature activation module (SAM), which constitutes a configured software, uses the set of the signature activation data (SAD) to guarantee with a high level of confidence

that the signer's key is used solely under their control. SAM is used in an environment that is protected against unauthorised use. Based on a risk analysis and considering the physical and other non-technical security measures, Evrotrust uses a reliable system, whose security or protection profile corresponds to level EAL 4 or higher in accordance with ISO/IEC 15408 or equivalent national or internationally recognised evaluation criteria for the security of information technologies;

- Evrotrust has designed SAP so that SAD are always reliably protected against copying or forgery by an attacker with a high attack potential;
- SAP is designed so that the signer can always reliably protect the signing key activation via SAD against an attacker with a high attack potential.

Evrotrust performs its signature activation activity by fulfilling the following additional specific requirements:

- SSA requires successful identification and certification of every signature before allowing the performance of any actions that could affect the "sole control" on each signing key;
- Evrotrust uses secure protocols that prevent human attacks in the environment and generally prevent any form of attack where a malicious user could use identification data that do not belong to them;
- Evrotrust applies strict access control requirements so that the access controls ensure that the signer will not have access to sensitive system sites or any functions that could give them control on the signing key of another user;
- Evrotrust applies strict control on the signing key, where TW4S guarantees that DTBS/R provided under the control of the signer will be only signed by the signing key belonging to that signer;
- TW4S requires the signer to present the SAD to the SAM so that it can be certified and activate the signing key;
- Evrotrust provides protocols with high level of security by using controls corresponding to the level of risk in order to counteract the following threats to the use of the SAD: online or off-line speculations, duplication of identification data, fishing, wiretapping, replacement, session highjacking, attacks from a human in the environment, theft of identification data, frauds and mask attacks;

- the activated signing key is used only for signing DTBS/R allowed by SAP;
- SSASP guarantees that the certificate for the public key is valid (not expired, revoked or suspended) before using the respective signing key;
- the signing keys are only used in the cases where the consent of the signer is obtained;
- the parameters of the cryptographic algorithms used for creation of a signature by the secure systems are selected so that they can survive the validity of the signers' certificates and are in line with the recommendations of ETSI TS 119 312.

8.3.2 SAD MANAGEMENT

Evrotrust performs signature activation data (SAD) management by fulfilling the requirements for EUSCP as follows:

- The SAD (signature activation data) is a dataset or a result of cryptographic operations using the mandatory parameters (listed below);
- SAD is generated in the signer's environment by SIC, however, realisation where this happens remotely by SIC under the signer's control is also allowed;
- SAD links the following parameters as a minimum with a high level of confidence:
  - represented data to be signed DTBS/R or a set of DTBS/R,
  - identification elements of the certified signer, and
  - a selected signing key, if there is no such default key.
- SAD is used for activation of the signing key only if the signer's certification is successful, which is checked by the SAM;
- Evrotrust's system indicates the SAD destination and the signature activation data are transferred to the SAM in the SAP;
- if the signer is a natural person, the collection and protection of the signature activation data are defined as follows:
  - SAD are collected in a manner that is under the control of the signer with a high level of confidence,
  - SAD are protected so that all keys held in the devices are protected,
  - SAD protect any secret used (single use or long-term). For this purpose, SAP is protected against secondary reproduction, bypass and false attacks between the signer and the

remote SCDev.

- when the signer is a natural person, Evrotrust's system is developed in such a way, so that the data are under the sole control of the signer during the submission of the signature activation data. SAP is designed so that the SAD are received from the SAM and so that it can be assumed that the SAD have been submitted under the sole control of the signer via the means owned by the signer;
- SAD are protected and checked after activation so that it is very unlikely for actions, such as guessing, wiretapping, repeating or manipulation of communication by an attacker with a high attack potential, to be able to hinder the authentication for the signature activation.

8.3.3 DELETION OF A SIGNING KEY

Evrotrust complies with the following requirements:

- the signing key is destroyed after revocation or expiration of the public key certificate or if the signing key is of no use for the signer;
- SSASP destroys the signing key upon request by the signer;
- Evrotrust securely operates the signing session and guarantees that the signing key will be destroyed after the signing session in the cases where the link between the signing key and the signer is not maintained after the signing operation;
- Evrotrust does not store any backup copies of the signing keys and guarantees that it is not possible to use any residual information to recover the signing keys.

8.3.4 KEY MANAGEMENT

Together with the generation of a pair of keys **of the certification authority**, the private key (or pair of keys) storage procedure is implemented in an encrypted manner and in accordance with an established internal procedure. For management of the private keys stored in the hardware security module (HSM) two persons with the respective passwords for access are necessary. A backup of the keys is created at the beginning – after the creation of all keys, as well as subsequently, after some of them are re-generated. The backup of private keys located in a HSM with level of security FIPS 140-2 Level 3 or higher is performed in accordance with the requirements of the HSM specification. In order to make a backup copy of the keys, two persons with trusted roles are necessary, who shall have the respective HSM access rights. Backup is

performed in a protected environment. After the creation of the backup, it is put in a vault at a remote location with the necessary security measures.

Together with the remote generation of the pair of keys **of the users** via the mobile application of Evrotrust, they are also stored in the HSM (in accordance with the requirements of Regulation (EU) No. 910/2014) in an encrypted manner and they are accessible through a password for access to the private key by the signer by observing the requirements for SCAL1 and SCAL2.

The private key of the certification authority used for creation of qualified electronic signatures/seals is backed up for at least 10 years after expiration of its validity period or after its termination. The same applies to the certificate of the public key corresponding to the private key after expiration of its validity period or after its termination.

Transfer of a private key in a hardware security module is performed in the following cases:

- for protection in case of creation of backup copies of private keys stored in a hardware security module (e.g. in case of compromising or malfunction of the hardware security module);
- when the private key needs to be transferred from the operating module of another hardware security module (in case of a failure of the operating hardware security module or if it needs to be destroyed).

The transfer of a private key to a hardware security module is a critical operation. Such operation requires suitable measures and procedures that prevent the disclosure of the private key or its alteration and falsification during the performance of the operation. The transfer of a private key to a hardware security module requires recovery of the key from the cards of two out of four authorised officers in the presence of a member of the management.

The private key of the provider **is activated** via a shared system access code, the components of which are known by more than one authorised persons from Evrotrust. The access to the slot in the HSM and the activation of the private key is allowed only in the presence of these persons after entering all parts of the access code.

Evrotrust complies with the following requirements related to the management of keys:

- all private keys (including the signer's signing key, the infrastructure and control keys) are never held in an unprotected state. They are securely and reliably stored in an encrypted form in an HSM with level of security FIPS 140-2 Level 3 or higher, corresponding to the requirements of Regulation (EU) No. 910/2014;
- private keys of signers are not exported from HSM. If a private infrastructure or control key needs to be exported from SCDev, this is done in a secure manner in order to guarantee its confidentiality and integrity up to the same or higher level of protection as in SCDev. When the private key is protected via encryption, Evrotrust uses only cryptographic algorithms of equivalent or higher level of security;
- TW4S guarantees that the backup, storage and recovery of private keys (including signing keys of users, infrastructure and control keys) is only performed by authorised officers. The master cryptographic keys used for protection of both user and operating keys are backed up, stored and recovered based on two-factor control. Such keys are held outside SCDev in a protected form;
- the management of Evrotrust controls the number of duplicated datasets so that it does not exceed the minimum necessary for ensuring the continuity of the service.

8.3.5 KEY CHANGEOVER

The policy for provision of the remote signature service with an electronic signature/seal does not have any requirements regarding the replacement of keys according to ETSI TS 119 431-1. The practice of Evrotrust is to provide generation of a new private key for each certification and issuance of a new qualified certificate of the user.

9 PHYSICAL SECURITY AND SAFETY OF THE ENVIRONMENT

9.1 PREMISES AND PREMISE CONSTRUCTION

The measures undertaken with respect to Evrotrust's physical protection constitute an element of the Information Security System developed and implemented at Evrotrust, which complies with the requirements of ISO/IEC 27001. Evrotrust has premises that are specially constructed and equipped with the highest level of physical access control, where the basic authority, the certifying authorities and all central components of the infrastructure are located.

9.2 PHYSICAL SECURITY

The measures applied by Evrotrust with respect to the control on physical security are as follows:

- Evrotrust controls the physical access to the facilities, the security of which is essential for the provision of trust services, and minimises any risks related to the physical security. The security of the systems for issuing and management of certificates is in line with the requirements of international standards and recommendations;
- the physical access to components of Evrotrust's system, the security of which is essential for the provision of trust services, is limited to authorised persons only. The criticality of the components is identified by risk assessment. Physical integrity is ensured with respect to the equipment located in the protected and isolated premises of Evrotrust. A two-factor control on the access and 24/7 armed physical security guarding has been implemented. No physical access to critical equipment is allowed for more than 30 (thirty) minutes per visit. The equipment cabinet may not be accessed by more than 2 (two) authorised technical staff members of Evrotrust. Any access to the premises with critical infrastructure is documented in special journals;
- control is applied for the purpose of preventing losses, damages or compromising of assets and interruption of the business operations. The authorised persons from Evrotrust's staff strictly observe the internal procedures for access to the different zones with restricted physical access;
- control is applied for the purpose of preventing compromising of data or theft of information processing tools. The physical protection of the premises where Evrotrust is located is ensured by their massive and stable construction with strong doors and keylocks. Protection is ensured by 24-hour non-armed security guarding. There is an Alarm System, a Video Surveillance System, a Signalling Alert System and an Access Control System in the premises of Evrotrust;
- the components that are critical for the secure operation of the trust services are located in a protected area, with physical security guarding against trespassing, with access control and trespassing detection systems;

In addition, Evrotrust applies the special requirement to only use reputable cryptographic libraries tested under the applicable standard in its operations with respect to the signature creation application (SCA).

Furthermore, the following specific requirements are applied (they are applied "mutatis mutandis" both for generation services and for signing key activation and management services):

- the facilities related to the generation of certificates and management of Certificate Revocation Lists (CRL) are operated in an environment that ensures physical protection of the services from compromising via unauthorised access to the systems or data;
- any intrusion on the physically protected zone is subject to independent control and no unauthorised persons are allowed unaccompanied;
- any entry in and exit from the protected zone is registered in journals;
- the physical protection is achieved by creating clearly defined perimeters of security (i.e. physical barriers) around the facilities related to the certificate generation services and CRL;
- all parts of the premises shared with other organisations are outside the perimeter of the facilities related to the certificate generation services and CRL;
- physical and environmental control on security is applied with respect to the technological system, the system resources themselves and the facilities supporting their operation;
- the policy for physical security and safety of the environment at Evrotrust for systems related to the generation of certificates and CRLs deals with the physical access control, protection from natural disasters, fire safety, failure of supporting utility services (e.g. power supply and telecommunications), breakdown of premises, water leaks, protection against theft, breaking in and intrusion and recovery from disasters;
- Evrotrust applies controls for protection against unauthorised removal of equipment, information, data media or software outside the company building (including outside the protected premises);
- access to the protected zones is restricted to authorised officers only;
- the private root key (Root CA) is stored and used only in HSM. It is in an "Offline" mode. Only certain reliable staff members have access to the private keys of Evrotrust.

9.3 ACCESS CONTROL

Evrotrust has an Access Control Policy in place, which is in line with the following

requirements:

- access to the system is restricted to authorised persons only. TW4S ensures control on the access to sensitive information. The access rights for specific TW4S sites are defined by the privileges and roles of the employees;
- controls (firewalls) have been introduced to protect the internal network domains from unauthorised access, including access by users and third parties;
- the firewalls are configured to prevent all protocols and access that are not required for the operation of Evrotrust;
- Evrotrust administers the access of the users, administrators and system auditors;
- the system administrator manages the user accounts and ensures timely modification or removal of access;
- access to the information and the applications is restricted in accordance with the Access Control Policy;
- Evrotrust's technological system ensures sufficient control on the computer security with respect to the administration and activities of the employees in accordance with their roles;
- Evrotrust controls the software use and the employees need to prove their identity before using critical applications related to the service;
- the employees of Evrotrust are responsible for their actions which is certified by journals of the events;
- TW4S ensures control on the access to sensitive information. The sensitive data are protected from disclosure by unauthorised users;
- TW4S provides an opportunity for control and restriction of access for identified persons to the system and user sites they own or they are responsible for. TW4S requires each user to prove their identity and to be successfully authenticated before allowing any actions on behalf of the respective user or role undertaken by the user. Second authentication is mandatory after logging off from the system. There are implemented mechanisms for privileged users, which reduce the risk during a certified user session and if the input device of the user is left unattended, the user session is terminated after a certain idle period. When the number of unsuccessful attempts for authentication by one and the same user reaches the maximum possible number of attempts, TW4S prevents any further attempts for authentication of the user until the administrator undertakes actions for unblocking the user (or within a certain period of time).

9.4 POWER SUPPLY AND AIR-CONDITIONING

The server racks with critical equipment are supplied by at least two independent UPS systems and are screened for prevention against external interventions. The air-conditioning systems in the isolated premises maintain a constant air temperature to ensure the normal operation of the technological system.

External power supply from a diesel generator is maintained, which is backed up. In case of a failure of the main power line, the system shifts to an emergency power source (UPS and/or electricity). The working environment in the area of the computer systems is continuously monitored independently from the other working areas.

The ventilation systems are specially designed for such class of premises and they do not allow compromising of the physical and electromagnetic protection of these premises or of the normal operation of the installed computer components.

The offices of Evrotrust are connected to the emergency power system of the building.

9.5 FLOOD

Sensors for detection of the level of humidity have been installed in the premises of the computer systems, as well as the entire building of Evrotrust, in order to monitor the humidity. These sensors are integrated in the building security system. The security guards and the employees of Evrotrust have been instructed and are obliged to immediately notify the relevant offices, the security administrator and the system administrator in case of eventual threats.

9.6 PREVENTION OF FIRE AND FIRE PROTECTION

Evrotrust complies with all fire safety provisions by performing the required activities in accordance with all the legal and standardisation requirements.

The protected premises with critical infrastructure are located in buildings where the following are installed: sound and light fire alert system, active fire alert system with gas and a stop gas button in case of complicated circumstances and evacuation. In case of a fire, interruption of the power supply to the facilities and extinguishing of the fire with gas are planned.

10 INTERNAL ORGANISATION

10.1 ORGANISATIONAL CONTROL

The following requirements are applied with respect to the management of Evrotrust's operations in the provision of the remote signature service with an electronic signature/seal:

- Evrotrust, in its capacity as SCASP and SSASP, ensures the security and reliability of the trust services provided via regular internal and external audits performed by independent organisations;
- Evrotrust guarantees that the policy and practice applied in its operations is non-discriminatory;
- the trust services are available for all entities whose operations fall within the scope of applicability of the services and who agree to fulfil their obligations as specified in the policies, practices, the contract and the general terms of Evrotrust;
- in relation to the risk of liability for damages caused under Article 13 of Regulation (EU) No. 910/2014, Evrotrust concludes a suitable insurance policy for third party liability in accordance with the national law;
- Evrotrust has the necessary financial stability and resources for operation in accordance with this document;
- Evrotrust has policies and procedures for resolution of claims and disputes raised by users or relying parties in relation to the provision of the services or other activities related to the services;
- where the provision of trust services involves subcontractors, Evrotrust always signs a contract.

10.2 HUMAN RESOURCES

Evrotrust complies with the following requirements:

- Evrotrust guarantees that the employees and contractors observe the requirements for reliability of the operation;
- Evrotrust hires employees and, if applicable, subcontractors, that have the necessary expertise, reliability, experience and qualification and that have undergone a training on security and personal data protection rules relevant to the operations they perform;
- the employees of Evrotrust undergo periodical (at least every 12 months) training

for increasing their expertise, experience and qualification. The trainings include courses in information security, potential threats and good security practices;

- proper disciplinary sanctions are imposed on employees who violate the policies of Evrotrust;
- the roles and responsibilities related to information security are documented in job descriptions;
- Evrotrust defines reliable roles which the security of the signatures/seals validation service is based on.
- the management of Evrotrust defines the responsibilities of the trusted roles;
- the trusted roles are approved and adopted by the management;
- Evrotrust's employees (both temporary and permanent) have job descriptions written with respect to the roles they perform, with division of the duties in accordance with the "least number of privileges" rule. The sensitivity of the position is defined based on the responsibilities, access levels, qualification and diploma;
- the job descriptions include requirements for skills and experience. A distinction is made in them between the general and specific duties;
- the employees apply administrative and operational procedures and processes that are part of the information security management procedures of Evrotrust;
- the management has the necessary knowledge with respect to the trust services provided, knowledge of the security procedures and experience in the field of information security and risk assessment sufficient for fulfilment of their management functions;
- all employees of Evrotrust with trusted roles are free of any conflicts of interest that could affect the objectiveness of the operations of Evrotrust;
- the trusted roles are described in section 10.2.3 of this document;
- the personnel of Evrotrust is assigned trusted roles by the senior management based on the "lowest privilege" principle with respect to access or during the configuration of the access privileges;
- the personnel is not given access to trusted functions before the necessary verifications take place. Evrotrust requires a certificate of criminal record.

10.2.1 PROCEDURES FOR EMPLOYEE BACKGROUND CHECKS

Evrotrust performs background checks with respect to all job applicants in accordance with the legal framework, the regulations and ethics and in line with the requirements related to the activity, the classification of information they have access to and the presumed risks. The background checks include: references, curriculum vitae, qualification, certificate of criminal record and other documents depending on the job the person applies for.

10.2.2 REQUIREMENTS FOR STAFF QUALIFICATION

Evrotrust hires employees and, if applicable, subcontractors, that have the necessary qualification, reliability and experience and that have undergone a training on security and personal data protection, as well as other trainings suitable for the trust services and activities of the company. The staff of Evrotrust fulfils the "expertise, experience and qualification" requirement via actual experience gained, trainings after being hired on a certain position or a combination of the two. Evrotrust's employees undergo regular trainings (at least every 12 months) on information security. The trainings cover security aspects related to new threats and good security practices.

10.2.3 TRUSTED ROLES

The management of Evrotrust has divided the duties and fields of responsibilities of the employees in order to reduce any possibilities for unauthorised or unintentional modification or misuse of the organisation's assets. All procedures related to the security in the creation and administration of electronic signatures are implemented by trusted staff. Evrotrust maintains a sufficient number of qualified employees to ensure compliance with the current legislation and the internal rules and regulations of the company at any time of the company's operation. The detailed division of the staff functions and responsibilities is presented in the internal documentation of Evrotrust: job descriptions, employment contract and the relevant internal operational procedures. The functions are divided in a way so as to minimise as far as possible the threat of any corruption, leakage of confidential information or occurrence of conflicts of interest.

Evrotrust complies with the following requirements for division of duties and fields of responsibility:

- the roles and responsibilities, as described in the information security policy of Evrotrust, are indicated in the employees' job descriptions;
- the trusted roles which Evrotrust's security of operations is based on, are clearly established;
- the trusted roles are determined by the management;
- the trusted roles are approved by the management and by the employee that will fulfil the role;
- the trusted roles are fulfilled by different employees;
- Evrotrust ensures that all employees with trusted roles are free of any conflicts of interest that could undermine their impartiality;
- the trusted roles and responsibilities included are:

a) security officers – overall responsibility for the administration of the application of the security policies and practices and access to information; The security officers are privileged system users;

b) system administrators - they are authorised to install, configure and support the reliable systems of Evrotrust for operation of the services. Their responsibilities include system recovery. The system administrators are privileged system users;

c) system operators – they are responsible for the daily operation of the reliable systems of Evrotrust. They are authorised to perform system backup and recovery. The system operators have privileged roles but may not administer or configure TW4S;

d) system auditors – they are authorised to review backups and audit journals of the reliable systems of Evrotrust. The system auditors have privileged roles but may not administer or configure TW4S.

- The employees of Evrotrust are assigned trusted roles by the senior management based on the "lowest privilege" principle during the configuration of the access privileges.

Certain trust services may require application of additional specific roles.

10.2.4 IDENTIFICATION AND VERIFICATION OF IDENTITY FOR EACH ROLE

The staff of Evrotrust is subject to identification and verification of identity in the following situations:

- when they are included in the list of persons with restricted access to buildings of Evrotrust;
- when they are included in the list of persons with physical access to the technological system and network resources of Evrotrust;
- when they are authorised to fulfil a specific assigned role;
- creation and assignment of an account and password in Evrotrust's information system.

Each authorisation for fulfilment of a certain role is subject to the following requirements:

- the role shall be unique and directly related to the respective person;
- it may not be shared with another person;
- it shall be limited to the function arising from the role and shall be fulfilled by a particular individual. The role is fulfilled by providing a certain software, technological system and access to the operational system of Evrotrust. The proper fulfilment of the role requires direct control on the job position.

Operations performed by Evrotrust that require access to shared network resources are protected via implemented mechanisms for strong authentication and encryption of the data transmitted.

10.2.5 STAFF TRAINING REQUIREMENTS

The staff that fulfils the functions and tasks associated with their occupation at Evrotrust or employment at the registration authority (including an external registration authority) shall attend the following trainings:

- „Policy and practice for providing remote electronic signature/seal service";
- Policies and practices for all trust services provided;
- provisions, procedures and documentation related to the relevant role;
- security technologies and procedures related to security used by the certification authority and the registration authority;
- system software of the certification authority and the registration authority;
- responsibilities arising from the roles and tasks implemented in the system;
- procedures implemented in case of a system breakdown or interruption of the activities of the certification authority;
- internal workplace and security regulations of the organisation.

10.2.6 FREQUENCY OF THE TRAININGS AND REQUIREMENTS FOR UPDATING THE EMPLOYEES' QUALIFICATION

Based on their work functions all employees of Evrotrust and, where appropriate, all subcontractors, undergo suitable training for performing their activities and regularly update their knowledge about the organisation's policies and procedures. The trainings are regularly planned and conducted by taking due account of the employees' roles. The trainings are internal and external and are conducted both by physical attendance and remotely.

10.2.7 CONTROL AND SANCTIONS FOR COMMITTING UNAUTHORISED ACTIVITIES

Proper disciplinary sanctions and procedures are applied with respect to the staff that violates the policies.

The management of Evrotrust requires its employees and subcontractors to apply the security measures in accordance with the organisation's established policies and procedures. Immediate measures for imposing a disciplinary sanction procedure are undertaken with respect to employees who have breached the information security.

10.3 RISK ASSESSMENT

Evrotrust classifies and maintains registers of all assets in accordance with the requirements of ISO/IEC 27001. According to Evrotrust's Security Policy, analysis for vulnerability assessment is conducted with respect to all internal procedures, applications and information systems. The analysis requirements may also be defined by an external institution authorised to audit Evrotrust.

Risk management is a structured, consistent and continuous process integrated in Evrotrust's operations, where decisions for response are identified, evaluated and taken and possible events are reported that could adversely or positively impact the accomplishment of the company objectives. Evrotrust determines the security requirements and operational procedures that are necessary for implementation of the selected measures for prevention of risky operations, which is documented in the Information Security Policy and in the Practice for provision of qualified trust services. Risk assessment is performed and reviewed at least once a year. The management of Evrotrust approves the risk assessment and accepts the residual risk identified.

Evrotrust complies with the following requirements related to the risk assessment:

- Evrotrust performs risk assessment in order to identify, analyse and evaluate the risks associated with the provision of trust services by taking due account of the business and technical issues;
- Evrotrust selects appropriate risk treatment measures, by taking due account of the risk assessment results. The risk treatment measures ensure that the level of security is commensurate to the level of risk;
- Evrotrust determines all security requirements and operational procedures that are necessary for implementation of the selected measures for risk treatment, as documented in the Information Security Policy and in the Practice for provision of qualified trust services;
- the management of Evrotrust regularly reviews and revises the risk assessment;
- the management of Evrotrust shall approve the risk assessment and accept the residual risk identified.

10.4 INCIDENT MANAGEMENT AND MONITORING

Evrotrust performs monitoring and incident management by applying the following requirements:

- Evrotrust has created and introduced strict procedures for monitoring of the technological system operation, the access to the information system, as well as the requests for trust services;
- the monitoring activities analyse and report the sensibility of each piece of information collected;
- cases of unavailable service or abnormal system operations that show a potential breach of security, including intrusion into Evrotrust's network, are detected and reported;
- authorised employees of Evrotrust monitor the following events:
  - ✓ starting and suspension of the registration operations;
  - ✓ availability and use of the necessary services via Evrotrust's network;
- in the cases of breaches of Evrotrust's security, there are procedures in place for timely, rapid and coordinated response in order to limit the breaches of security;
- the security incidents alerts are tracked and reported by employees with trusted

roles in accordance with the company procedures;

- Evrotrust has established a procedure to notify the relevant supervisory authorities in line with the applicable regulatory rules about any breach of the information security or loss of integrity that has a significant impact on the trust service provided, within 24 hours after detection of the breach;
- where the information security breach or loss of integrity is likely to adversely affect any natural or legal person that was provided with a trust service, Evrotrust notifies the respective natural or legal person without undue delay;
- Evrotrust monitors its technological system and regularly reviews the audit journals in order to identify evidence for any misconduct. The company has developed automated mechanisms for processing of the audit journals and for alerting the staff for possible critical events related to security;
- TW4S generates warnings in a timely manner that alert for unusual events that could influence the system capability for server signing in accordance with the security requirements (e.g. user operations outside the standard working hours; actions caused by a non-human intervention; user operations beyond the standard regulated operations);
- for each newly detected critical vulnerability a plan for its resolution is developed within 48 hours after its detection;
- for each hazard, based on its potential impact, Evrotrust:
  - ✓ develops a plan for minimising the damages;
  - ✓ documents the facts and reports to the management.
- The procedures for incident reporting to the management and the response from the decisions taken are used so that the measures undertaken could minimise any damages and so that future measures are undertaken to prevent such incidents.

10.5 INFORMATION SECURITY POLICY

The Information Security Policy focuses on the requirements related to the strategy for operations, the regulations, the legislations and contracts, as well as on the current and possible environment of any threat to information security. The security policy contains statements, objectives and principles that shall govern all actions in the assignment of general and specific responsibilities related to the management of security to certain roles and processes for

overcoming any deviations, breaches and emergency situations. More particularly, the Information Security Policy includes procedures that describe the mechanisms for control on the information security: access control, classification of information, physical security and security of the surrounding environment, assets, information exchange, remote work, software used, cryptographic mechanisms for control, security of communications, personal data protection and relationships with providers.

Evrotrust has an Information Security Policy in place, that has been developed and approved by the management, which includes the following:

- The Information Security Policy defines the approach of Evrotrust to the management of its operations.
- Any changes to the Information Security Policy are communicated to third parties (users, relying parties, supervisory or other regulatory bodies, compliance assessment bodies), where applicable.
- Evrotrust's information security policy is documented, implemented and maintained up-to-date.
- All employees of Evrotrust have been familiarised with the Information Security Policy.
- Evrotrust is responsible for compliance with the procedures described in the Information Security Policy in the cases where it subcontracts part of its operations. If there are subcontractors, Evrotrust defines their liability and ensures that they are bound to strictly apply all information security controls required by Evrotrust.
- The Information Security Policy of Evrotrust and the inventory of information security assets are reviewed at planned intervals from time to time or in the case of significant changes, in order to ensure their continued suitability, adequacy and effectiveness.
- Any changes that will impact the level of security provided are approved by an information security management body.
- The configuration of the systems of Evrotrust is regularly checked for changes which violate the information security rules. The maximum interval between two validations is based on the internal procedures of Evrotrust.

In addition, the following specific requirements are applied:

The Information Security Policy documents the security controls introduced for personal data protection. During the processing of personal data, Evrotrust complies with all personal data protection regulations applicable to its operations, including, but not limited to Regulation (EU) 2016/679. The Personal Data Protection Policy is an integral part of the Contract for use of the services. In case of any change to the Personal Data Protection Policy, changes are published on Evrotrust's website: www.evrotrust.com. Evrotrust undertakes all the necessary steps, including technical and organisational measures, based on the risk level of the personal data processing performed, in order to ensure the data security so that no accidental or unauthorised destruction, loss, alteration, unauthorised disclosure, access or other illegal or unwanted event can be allowed that could compromise the security of the personal data processed. Evrotrust collects information the amount of which is proportionate to its purpose and use. Each user gives their consent to the processing of personal data. This consent is declared by signing the Contract for trust services. The personal data are only used in relation to the provision of the specific trust service.

10.6 ASSET MANAGEMENT

Evrotrust manages its assets by applying the following requirements:

- Evrotrust has provided a proper level of protection of its assets, including its information assets.
- Evrotrust maintains an inventory list of all information assets and classifies them based on the risk assessment.

In addition, Evrotrust applies the special requirement of the signature creation application (SCA) by using only standard and tested cryptographic libraries in its operations.

10.6.1 BACKUP

Evrotrust backs up electronically both all significant events and all data and files related to the user registration and identification, the system security, contracts with third parties and providers and other essential information related to the lawful provision of trust services. The electronic backup is securely managed and stored and the access thereto is limited to authorised officers only. The electronic backup is signed with an electronic timestamp. The information from

the records in the logs is periodically written on physical media, which are stored in a special safe deposit box located in a premise with high level of physical protection and access control. The long-term backup copies on paper are stored in a special premise designated only for this purpose, in compliance with all requirements for secure and reliable storage of documents.

The data backed up collected by Evrotrust in accordance with the requirements of Art. 24, paragraph 2, letter "h" of Regulation (EU) No. 910/2014 for the purpose of provision of evidence in the case of court proceedings and ensuring continuity in the provision of the service are stored for a period of 10 years inclusive after termination of the respective activity. After expiration of this period the backed up data are destroyed.

10.6.2 OPERATION WITH DIFFERENT MEDIA

All media are securely processed in accordance with the requirements of the scheme for classification of information. The media that contain sensitive data that cease to be necessary are disposed of in a safe manner. All media containing software, data backups or auditing information are stored in a fireproof case in a special premise for backups with implemented access control. A system for physical and logical protection has been developed for the premise where the backup copies of Evrotrust are located. Evrotrust has undertaken serious measures against accidental or intentional damage to the data media. The registration authorities are obliged to keep and store the up-to-date information, including the users' documents on paper in a safe deposit box.

10.6.3 WASTE DISPOSAL

All paper and electronic media that contain potentially critical information about the security of Evrotrust are destroyed in special shredding devices after expiration of the storage period defined by the internal regulations.

The media with information about cryptographic keys and PIN/PUK codes used for their storage are crushed by using suitable devices. This applies to media where permanent deletion of the data stored and reuse is not possible.

In certain cases information from portable media will be destroyed by deletion or formatting of the device with no possibility for recovery.

11 MANAGEMENT AND CONTROL OF THE TECHNICAL SECURITY

Evrotrust uses only reliable and secure hardware and software, which are part of the company computer system. The computer systems where all critical components of Evrotrust's infrastructure operate are equipped and configured with tools for local protection of access to the software and information data. Evrotrust applies procedures for information security management for the entire infrastructure of Evrotrust in line with the generally accepted and international practices and standards.

In order to ensure the reliable operation and security of the computer systems lifecycle, Evrotrust performs activities in accordance with the following requirements:

- During the development of new systems, Evrotrust performs analysis on the security requirements as early as during the design and specification stage and thus guarantees the integration of security in the IT systems.
- Evrotrust applies a security policy and a procedure for control on alterations during updates, modifications of emergency and operating software and changes in the configuration.
- The procedures include documenting the changes.
- Evrotrust protects the integrity of the systems and information from viruses, malware and unauthorised software.
- The media used within the systems of Evrotrust are securely handled to protect them from damage, theft, unauthorised access or obsolescence.
- The procedures for management of the different media should prevent their obsolescence and deterioration during the period where records need to be stored.
- Evrotrust develops and applies procedures for all trusted and administrative roles that have impact on the provision of services.
- Evrotrust specifies and applies procedures for ensuring that:

a) any available software protective and functional updates (security patches) are applied within a reasonable period after becoming available;

b) the protective and functional updates are not applied if they are likely to introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them;

c) the justification for refusing to apply any protective or functional updates are documented.

In addition, the following specific requirements for SCA are applied:

- Evrotrust uses the latest version of the signature creation application, including the one as of the date of the security patch.
- Evrotrust uses signature creation applications of standardised protocols and libraries that have been successfully tested and reviewed.
- Evrotrust uses cryptographic libraries tested against the applied standard.
- The SCA maintains the integrity and confidentiality of the entire information provided by any user, as well as of any data transmitted between the application and the user, even in the case of public access to the application environment.
- SCASC applies all the mandatory requirements under ETSI TS 119 101 with respect to DA/SCA.

11.1 SECURITY MANAGEMENT

Regarding the security management during the provision of trust services, Evrotrust fulfils the following requirements:

- Evrotrust controls its security in order to manage TW4S that provides signature creation services.
- TW4S supports roles with different privileges:
  - ✓ as a minimum, TW4S supports the following privileged roles: security officers; system administrators; system operators and system auditors;
  - ✓ as a minimum, TW4S supports the following non-privileged roles:
    - signer: they are authorised to use TW4S by submitting SAD as part of SAP in order to sign the document or DTBS/R that could be potentially submitted via SAP;
    - SCA: it is authorised to send a DTBS/R request to TW4S so that it can be signed by the signer;
    - RA: the registration authority has the right to send the certificate with the public key to TW4S in response to a request for signing a certificate.
- One privileged user may not assume more than one of the privileged roles.
- Users linked to privileged roles are not associated with a non-privileged role. Users linked to non-privileged roles are not associated with a privileged role.

- TW4S guarantees that a user authorised to assume the role of a security officer does not have the right to play the role of a system auditor.
- TW4S guarantees that a user authorised to assume the role of a system administrator and/or the role of a system operator does not have the right to play the role of a system auditor and/or the role of a security officer.
- Persons who are part of a group of privileged system users are named according to the role fulfilled by them, which is described in their job descriptions and for which they are trained.
- Only privileged users of the system have physical access to the hardware and are able to administrate TW4S.
- Only privileged users of the system have broad rights to administer TW4S via all respective applications and interfaces.

11.2 OPERATION MANAGEMENT

Evrotrust, which operates TW4S, guarantees that the operation management functions are adequately protected and that it fulfils its activity in a manner so as:

- to guarantee that TW4S has documentation in place that contains the following: instructions that allow proper and secure operation; procedures that allow the risk of system failure to be minimised; and procedures ensuring the integrity of the systems and protecting the information they process from viruses and malware;
- which guarantees that TW4S has system documentation that covers the responsibilities of the four privileged roles and includes: an installation manual; an administration manual and a user manual.

11.3 TIME SYNCHRONISATION

The signature creation and subsequent verification are time-related. Evrotrust guarantees that that TW4S is properly synchronised with a source of standard time.

Evrotrust manages the operations by fulfilling the following requirements:

- TW4S uses a hardware source of high-precision coordinated time. The synchronisation of UTC with the source of time is automated, based on an NTP protocol after establishing any difference between the source and the system time. In case of a problem in the

hardware source of time and need to replace the latter with a backup, internet-based time servers are used as a source of exact time. The synchronisation is based on at least two sources of time via an NTP protocol. The exact coordinated time with respect to UTC (Coordinated Universal Time) is with up to 0.05 seconds precision. Evrotrust guarantees public access for receipt and verification of the issued qualified timestamp certificates.

- In order to guarantee the precision of the events verified, Evrotrust uses a source of time that is properly synchronised with a standard source of time.
- In order to check whether a given certificate validity period has expired, a source of time properly synchronised with UTC is used.

11.4 COMPUTER SECURITY CONTROLS

In order to achieve security in the trust service provision activity, Evrotrust applies specific requirements related to the access control. Their fulfilment is described in section 9.3 of this document.

Evrotrust uses reliable systems for its activities, which operate in accordance with the following requirements:

- TW4S generates a warning for timely notification about any unusual events that could influence the system capability for server signing.
- TW4S meets the security requirements set out in CEN EN 419 241-1.
- TW4S applies a mechanism for issuing a warning in case of detection of an unusual event. The warning triggers a notification to the administrator. The warning may also trigger further actions for response to possible attacks, such as interrupting the path of the potential attack.
- the unusual events related to user operations may include (but are not limited to):
  - ✓ user actions outside the standard working hours;
  - ✓ user actions implemented with an unusual speed (for detection of non-human submission);
  - ✓ user actions skipping the standard operations within certain processes;
  - ✓ duplicated user sessions.

11.5 NETWORK SECURITY

Evrotrust's infrastructure uses modern technical tools for information exchange and protection in order to guarantee the network security of the systems against any external interventions or threats.

Evrotrust protects its network and systems from attacks by applying the following requirements:

- Evrotrust divides its systems into networks or zones to a functional, a logical and a physical zone (including by location) based on the risk assessment and the link between the reliable systems and services. Detailed description of the network configuration and the means for protection are presented in the infrastructure technical documentation. This documentation has an "internal" status and is only accessible for authorised persons.
- Evrotrust applies one and the same security controls for all systems located within the same zone.
- Evrotrust limits the access and communication between the zones to those that are necessary for performing the relevant operations. Any attempts for unauthorised access to the system are documented via an Intrusion Prevention System (IPS).
- Evrotrust expressly bans or deactivates the unnecessary links and services.
- Evrotrust regularly reviews the established set of rules.
- Evrotrust maintains all systems that are essential for its operations in two protected zones. The servers and critical technological system of Evrotrust are connected to an internal LAN network. The remote access to the infrastructure (PKI) network of Evrotrust takes place via a designated VPN server that has been installed and configured, which accepts authentication through a special name and password issued solely for this purpose to authorised persons involved in the issuance of an electronic signature/seal and the administration of the infrastructure (Public Key Infrastructure/ PKI).
- Evrotrust has a separate special network for administration of the IT systems and the operational network.
- Evrotrust does not use systems that are used for administration of the security policy for other purposes.
- Evrotrust separates the systems servicing the trust services from the systems used for development and testing.

- Evrotrust establishes communication between individual secure systems only via reliable channels that differ logically from the other communication channels and ensure secure identification of the endpoints and protection of the channel data from modification or disclosure. The servers and critical technological system of Evrotrust are connected to an internal LAN network. The remote access to the infrastructure (PKI) network of Evrotrust takes place via a designated VPN server that has been installed and configured, which accepts authentication through a special name and password issued solely for this purpose to authorised persons involved in the issuance of an electronic signature/seal and the administration of the infrastructure (PKI).

- If an external service with High Availability requirements needs to use a trust service, the external network connectivity thereto will also take place based on the High Availability requirements, which guarantee accessibility of the trust service in case of a failure of one of its components.

- Evrotrust performs regular scanning of the vulnerability of the identified public and private IP addresses and records the evidence from this process. In order to ensure reliable reports, each vulnerability scan is performed by an authorised person with the necessary skills, qualifications and tools and in compliance with the code of conduct and the requirement for lack of conflict of interests.

- After each update, modification or upgrade of critical applications, Evrotrust performs systems intrusion tests.

- Evrotrust records the evidence that each intrusion test has been performed by an authorised person with the necessary skills and tools, who complies with the code of conduct and has no conflict of interests, in order to ensure a reliable report.

11.6 CRYPTOGRAPHIC CONTROLS

Evrotrust has introduced proper security controls for management of the cryptographic keys and all cryptographic devices during their entire lifecycle. Hash algorithms and asymmetric algorithms that meet the requirements set out in ETSI TS 119 312 are used for the generation of a cryptographic pair of keys (private and public). The applicable combinations of asymmetric and hash algorithms by duration with respect to the qualified electronic signature is as described in ETSI TS 119 312. A key length that meets the requirements of ETSI TS 119 312 is used: the length

of the pair of keys for qualified electronic signature / seal of a user can be 2048, 3072 or 4096 bits, with the applicable combination of asymmetric and hash algorithms: sha256-with-RSA. The key shall have a length of at least 1024 bits for RSA and DSA algorithms and 160 bits for ECDSA algorithms.

Evrotrust generates pairs of cryptographic (RSA) keys of the basic and the operational certification authority by using a hardware security system (HSM/Hardware Security Module) with level of security FIPS 140-2 Level 3 or higher, or, respectively CC EAL 4+ or higher. Evrotrust uses all its private keys solely for the purpose of its activities as follows:

- to sign the operational certificates issued to the certification authorities in its infrastructure;
- to sign the Certificate Revocation Lists (CRL) that have been issued and published;
- to sign all qualified certificates for electronic signature/seal of the users that have been issued and published.

In case of provision of a remote signing service with an electronic signature/seal and a requested issuance of certificate from Evrotrust's mobile application, the private key is generated and stored in an encrypted form in the hardware security module of Evrotrust, which meets the requirements of Regulation (EU) No. 910/2014 for a qualified signature creation device (QSCD). The key encryption takes place through a PIN code created by the user, which ensures that he is the sole person with access for activation of the key. The qualified electronic signature/seal creation devices guarantee that by using proper technical means and procedures, the following will be achieved as a minimum:

- the confidentiality of the data used for creation of an electronic signature/seal is reasonably guaranteed;
- the date for creation of an electronic signature/seal will be practically seen only once;
- the data for creation of an electronic signature/seal are sufficiently secured and may not be extracted and the electronic signature/seal is reliably protected against forgery by using the currently available technology;
- the data for creation of an electronic signature can be reliably protected by the legal Signatory/Creator of the electronic signature/seal against use by third parties.

12 CONTINUITY OF BUSINESS AND RECOVERY AFTER ACCIDENTS

Evrotrust manages the continuity of its business by applying the following requirements in its operations:

- Evrotrust has developed an Operation Continuity Plan which is periodically tested and maintained up-to-date and which shall be adopted in case of an accident.
- In case of an accident and failure of critical components of the technological system, including hardware, software or compromising of a private key of Evrotrust, the operations are resumed within the delay period established in the continuity plan. The reasons for the accident are analysed, suitable measures for its elimination are undertaken and measures are defined to prevent its recurrence.

In addition to the above requirements, in order to ensure continuity of business, Evrotrust, in its capacity as a SCASP, fulfils the following specific requirements:

- Evrotrust applies measures to avoid interruptions of SCASP due to intentional or unintentional conduct on the part of users or third parties.
- Evrotrust adds a timestamp to the signature and thus the service level agreement (SLA) of SCASP takes SLA of TSA into account. Evrotrust has the obligation to provide the user with availability and functionality of the service as described in the Contract and the General Terms. Evrotrust reports the level of the service availability on a monthly basis. The time of lack of availability is tracked at incident level in the support system. If the agreed level of service availability is not achieved, Evrotrust is liable for compensation, except for the cases that are beyond the control of Evrotrust.

13 OPERATION TERMINATION PLAN

Evrotrust (in its capacity as QTSP, SCASP and SSASP) has developed an Operation Termination Plan for ensuring continuity of service and specific scenarios thereto in accordance with the requirements of the *Regulation on the liability and for termination of the operation of trust service providers* and applies the following requirements:

- Evrotrust has adopted measures for minimising any potential interruptions of the trust services used by users and relying parties as a result of termination of the company operations. Particularly, Evrotrust ensures continuous maintenance of the information necessary

for validation of the trust services correctness.

- Evrotrust has an updated Termination Plan.
- Before terminating its services Evrotrust informs all stakesignatorys, users, relying parties, providers, subcontractors or other parties it has agreements with and the respective supervisory bodies.
- Before terminating its services, Evrotrust terminates the authorisation of all subcontractors (if any) to act on their behalf in carrying out any functions related to the process of issuing trust service certification tokens.
- Before terminating its services, Evrotrust transfers its obligations to a reliable party for maintaining all the information necessary to provide evidence for its operation for a reasonable period, unless it can be proven that it does not hold any such information.
- Before terminating its services, Evrotrust destroys or withdraws its private keys, including backup copies (if any) from use in a way that prevents their retrieval.
- Before terminating its services, where possible, Evrotrust undertakes measures for transferring the trust services provided for its existing users to another qualified trust service provider.
- Evrotrust has an insurance for covering the costs, as far as possible, in case of bankruptcy or if it is otherwise unable to cover the costs, however, within the limits of the applicable legislation with respect to insolvency.
- Evrotrust maintains or transfers its obligations to make its public or certification tokens available to relying parties for a reasonable period of time to a reliable party.

13.1 TERMINATION OF THE OPERATIONS OF THE CERTIFICATION AUTHORITY

In case of termination of the operation of a certification authority, Evrotrust implements the following procedure:

- It follows a plan and scenario for termination of the operation of the certification authority that is updated and approved by the management.
- It notifies the users, the Supervisory Body and the third parties for the termination of the operation of their certification authority. The information is provided via e-mail or by publication on the website of Evrotrust.
- It terminates the authorisation of all parties that have contractual activities to perform

operations related to the specific certification authority.

- Before the certification authority termination of operation, it transfers its obligations related to maintaining the entire information necessary to provide evidence to a reliable party within a reasonable period.
- It changes the status of its operational certificates.
- It terminates the issue of new certificates but continues to manage the active certificates until the expiration of their validity.
- Before terminating the activity, the private keys, including the backup copies, are destroyed or withdrawn from use so that the personal keys may not be retrieved.
- It exercises all reasonable economic efforts to minimise any breach of the users' interests.
- Evrotrust applies measures for covering the costs in case of bankruptcy or other reasons for termination of its operations as a certification authority. If it is not able to cover the costs by itself, it has foreseen measures in line with the applicable legislation.

13.2 TRANSFER OF OPERATIONS TO ANOTHER QUALIFIED TRUST SERVICE PROVIDER

If Evrotrust decides to transfer its operations to another qualified trust service provider, the company implements a plan and scenario preliminary created and approved by the management for continued provision of qualified trust services. In this case Evrotrust implements the following steps:

- It notifies the Supervisory Body about its intention no later than 4 months before the date of termination and transfer of operations.
- It exercises all the necessary efforts and due care to continue the validity of the user certificates issued.
- It notifies the Supervisory Authority and the users in writing that their operations are taken over by another qualified provider and about the name of that provider. The notification is published on Evrotrust's website.
- It notifies the users on the terms for supporting the transferred certificates with the provider taking over the operations.
- It changes the status of its operational certificates and duly transfers the entire documentation related to its operations to the provider taking over the operations, together with

all backups, as well as all certificates issued.

- It performs the necessary actions for transferring the obligations related to maintenance of the information to the provider taking over the operations.
- It transfers the management of the end user certificates already issued to the provider taking over the operations.

Evrotrust concludes a suitable contract by virtue of which the qualified provider taking over the operations assumes the rights and obligations of Evrotrust and continues to manage the active certificates until their expiration. The backup copies of Evrotrust with a terminated status shall be transfer to the provider taking over the operations.

13.3 WITHDRAWAL OF THE QUALIFIED STATUS OF EVROTRUST OR THE CERTIFICATION SERVICE

In case of withdrawal of the qualified status of Evrotrust or one or more of the trust services provided by the company, the following procedure shall be implemented:

- The company will notify its users about their changed status or the changed status of their services.
- It will change the status of their certificates.
- It will terminate the issue of new qualified certificates but will continue to manage the active certificates until the expiration of their validity.
- It will exercises all reasonable economic efforts to minimise any breach of the users' interests.

14 AUDIT AND ACTIVITY CONTROL

The audits carried out in Evrotrust are related to the data processing and management of key procedures. They aim to control the practices when providing qualified trust services insofar as they are compatible with the integrated management system implemented which includes the requirements of standards ISO/IEC 27001, ISO 9001, ISO 22301, and ISO/IEC 20000-1, Regulation (EU) No. 910/2014, GDPR and the internal management decisions and measures. The audits carried out by Evrotrust refer to all certification authorities belonging to the basic certification authority, the registration authority and other elements of the public key infrastructure.

Evrotrust carries out at least one internal audit every year.

Evrotrust is subject to audit at least once every 24 months by a conformity assessment body. The purpose of the audit is to confirm that Evrotrust, as a qualified certification service provider and the qualified trust services provided by it, comply with the requirements set out in Regulation (EU) No. 910/2014. The conformity assessment reports of the successfully completed audits should be submitted to the supervisory body to confirm the qualified status of the trust services in the trusted list.

The supervisory body may at any time carry out an audit or request a conformity assessment body to perform a conformity assessment of Evrotrust with Regulation (EU) No. 910/2014.

14.1 AUDIT FREQUENCY

The management of Evrotrust schedules periodic inspections on the conformity of current activity to the established policies and practices for providing qualified trust services. The management carries out constant operational control for the accurate execution of the instructions by Evrotrust personnel.

14.2 QUALIFICATION OF AUDITORS

An external audit shall be carried out by an accredited and independent conformity assessment body. The auditor's system of accreditation and competence are specified in Regulation (EC) No. 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No. 339/93 and is regulated by ISO/IEC 17065:2012: Conformity assessment - Requirements for bodies certifying products, processes and services.

An external inspection by a supervisory body is carried out at any time by authorised employees of the supervisory body - the Communications Regulation Commission.

The internal audit is carried out by Evrotrust employees with the necessary experience and qualification. For the purposes of auditing, Evrotrust has hired and authorised employees who have the necessary technical knowledge related to public key infrastructure, the reliable and secure operation of the technological system, information security, as well as extensive practical experience in auditing.

14.3 RELATIONS BETWEEN AUDITORS AND EVROTRUST

External auditors shall be independent, not directly or indirectly related to Evrotrust and shall have no conflict of interest with Evrotrust. The relations between Evrotrust and the auditing external person are regulated by a contract.

14.4 SCOPE OF AUDIT

The inspection carried out by the supervisory body covers the statutory requirements for the activities of Evrotrust according to the applicable legislation in the sector of qualified trust services. The audit carried out by the conformity assessment body covers the entire activity of Evrotrust regarding the provision of qualified trust services and implementation of all standards and standardisation documents related to Regulation (EU) No 910/2014: documentation; archives; information regarding the issuance and management of qualified certificates; physical and information security and reliability of the technological system and management; certification bodies. The conformity assessment body shall ensure that the scope and limits of applicability of the trust services provided by Evrotrust are clearly defined in terms of characteristics of the business, organisation, facilities, assets and technology. The conformity assessment body shall ensure that information security risk assessment and risk treatment are properly reflected in the activities of Evrotrust, that interfaces with services or activities that are not entirely within the scope of trust services are included in the information security risk assessment of Evrotrust.

The scope of internal audits includes: inspection of the provider's activity and its compliance with the policies and practices for providing qualified trust services; comparison of the practices and procedures outlined in this document with their practical implementation when carrying out the activity of Evrotrust; inspection of the activity of the registration authority; other circumstances, facts and activities related to the infrastructure of Evrotrust, at the discretion of the Evrotrust management.

14.5 ACTIONS UNDERTAKEN AS A RESULT OF THE AUDIT

External and internal audit reports shall be submitted to Evrotrust. The report from the conformity assessment body shall be submitted to the supervisory body within 3 (three) days of its delivery to the management of Evrotrust. The audit report includes findings of the examination

of Evrotrust's documentation, compliance with the requirements of applicable standards and regulatory requirements, report of information security risk analysis, fields covered by the audit and time of the audit, any observations made and all established non-conformities. The report shall examine the adequacy of Evrotrust's internal organisation and procedures to enhance trust in the trust services provided. Based on the assessments of the report, the management of Evrotrust shall identify measures and deadlines to remedy the established deficiencies and non-conformities. Evrotrust's personnel shall undertake specific actions to remedy them within the specified deadlines.

14.6 STORAGE OF AUDIT RESULTS

The results of internal and external audits conducted are duly stored in the archive of Evrotrust. The certification document received from the conformity assessment body shall be published on Evrotrust website.

14.7 COLLECTION OF EVIDENCE

Evrotrust has a procedure of evidence collection which includes:

- Evrotrust records and keeps accessible for an appropriate period of time, including after its activities have ceased, all relevant information concerning data issued and received during its activity, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service;
- Evrotrust has undertaken appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage of personal data;
- Evrotrust is a company registered in the Republic of Bulgaria, within Europe, and as such, while complying with the European and national legislation, it ensures that ensures that personal data are processed in accordance with Regulation (EU) 2016/679. In this respect, by providing trust services remotely, Evrotrust provides access to its services by processing only those identification data that are adequate, relevant and not excessive;
- maintains the confidentiality and integrity of current and archived records concerning operation of services;
- records concerning the operation of services are completely and confidentially

archived in accordance with good business practices;

- records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings;
- the precise time of significant operation management events, such as key management and clock synchronisation, are recorded;
- the time used to record events as required in the audit log is synchronised with UTC at least once a day;
- records concerning services are held for a period of time as appropriate for providing necessary legal evidence and as notified in the General Terms and Conditions and the contract;
- the events are logged in a way that they cannot be easily deleted or destroyed, except if reliably transferred to long-term media, within the period of time that they are required to be held.

Evrotrust applies the following additional requirement for audit logs:

SSASP stores audit logs in accordance with applicable legislation for a period of 10 (ten) years after any certification based on those logs ceases to be valid.

Evrotrust records all security-related events, including changes related to security policy, system startup and shutdown, system failures and hardware failures, firewall and router activities, and attempts to access the SSASC system.

Evrotrust generates audit data when registering: significant events for TW4S related to the environment, as well as events related to key management (generation, use and destruction; all attempts to access TW4S); user signing events (e.g. successful user signing, DTBS/R request management and issuance of certificates); user authentication via SAP; signer's SAD management by TW4S; turning on and turning off the function for generating audit data; changes in audit parameters.

Evrotrust guarantees the availability of audit logs. For this purpose, the audit function only adds information. Evrotrust undertakes actions in case of failure to transmit audit information to any external repository. Until the audit information is recovered, it is collected locally. TW4S

protects stored records from unauthorized deletion. Audit logs can be deleted when archived in an external repository. All audit logs contain: date and time of event, type of event, subject identity (user, administrator, process), successful or unsuccessful event, person responsible for the action. TW4S allows searching for events in the audit log based on the date of the event, the type of event and / or the user identity. Audit logs are in a format that can be processed and is suitable for system auditors to interpret the information. By default, TW4S denies all users read access to audit logs, except for users who are granted explicit read access (e.g. system auditor).

Evrotrust guarantees the integrity of audit logs, as TW4S ensures the integrity of audit logs with electronic signature and electronic timestamp. TW4S provides a function to verify the integrity of audit data. TW4S ensures the accurate timing of the audited events by using a time source that is properly synchronised with a standard time source. Sensitive information is stored in a secure manner to ensure its integrity and confidentiality.

Evrotrust generates archive on external storage. External storage devices are suitable for storage and further processing and can provide the necessary legal evidence to support electronic signatures. All audit logs are archived. Each record in the archive includes the time of archiving. The archive does not include sensitive information (e.g. TW4S user passwords). Evrotrust guarantees the integrity of the archived data and prevents unauthorised modifications of the records. It has a mechanism to check the integrity. Evrotrust archives system information needed to restore the system after a failure or disaster. If necessary, TW4S includes a system state restore function from a backup. A user associated with a role with sufficient privileges can call the restore function upon request of a backup.

In addition, Evrotrust applies the following specific requirements for the service of creation of remote electronic signature/seal:

- each operation to create a digital AdES signature is registered, together with the user identification, in cases where such information is known;
- event logs are signed with a timestamp;
- the strictest confidentiality measures are applied when collecting evidence;
- logs include the type of event, information about the success or failure of the event and an identifier of the person and/or component that caused the event;
- For the efficient management and operation of Evrotrust, all events which are

significant for the security and reliability of the technological system, the control of staff and users, and the impact on the security of the qualified trust services provided shall be recorded;

- information about electronic logs is generated automatically. Record logs of registered events are stored in files on the system drive for at least 6 (six) months. In this period, they are available online or upon search by any authorised employee of Evrotrust. After this period, records are stored in the archives.

15 OTHER BUSINESS AND LEGAL ASPECTS

15.1 PRICES AND FEES

Evrotrust provides trust services to users as follows:

а) provides the services free of charge or for a fee, in accordance with the prices specified in the tariff for the use of services available through the application of Evrotrust (the Tariff). The tariff is available in mobile applications and on: http://tariff.evrotrust.com;

б) reserves the right to unilaterally change the prices specified in the Tariff in compliance with the requirements of the of current legislation. Any change in prices does not affect the use of services already paid for by users;

в) the prices for the use of services shall be paid to Evrotrust by the users or by relying parties, according to the agreements between them;

- the prices for the use of services are due in accordance with the use of a service provided for in the Tariff or in another way specified in the Tariff.

г) when the price for the respective service is due by the user, the mobile application visualises accurate information about its amount including all due taxes and other costs and indicates when the payment due date.

15.2 INSURANCE OF ACTIVITIES

Evrotrust conclude compulsory insurance of its activity as a provider of qualified trust services. With regard to the risk of liability for damages in accordance with Article 13 of Regulation (EU) No. 910/2014, Evrotrust shall conclude appropriate liability insurance, in accordance with national law. The compulsory insurance shall be concluded for a continuous period and renewed annually. Subject of the insurance shall be the liability of Evrotrust to perform its activity according to the requirements of the applicable legislation. The compulsory insurance shall cover the

liability of Evrotrust to users and relying parties for material and non-material damage within the limits specified in the applicable legislation. Upon occurrence of an event that may result in claiming damage covered by the insurance, the person concerned must notify Evrotrust and the insurer in writing within 7 days after becoming aware of the event. The insurance coverage for non-material and/or material damage suffered by a signature owner/creator shall not exceed the amount established by the national legislation.

15.3 DATA PRIVACY

Evrotrust takes appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of personal data. As a data controller, Evrotrust strictly observes the requirements for confidentiality and non-disclosure of personal data of signature owners/creators, which became known to it during the performance of its activity as a provider of qualified trust services. Evrotrust ensures that personal data are collected, stored and processed in accordance with the Personal Data Protection Act and REGULATION (EU) 2016/679 General Data Protection Regulation (GDPR). Evrotrust collects such amount of information that is proportionate to its purpose and use. Every user gives their content to the processing of their personal data. This consent is declared by signing a trust services Agreement. Personal data are used only in relation to the provision of trust services which means that only data that are adequate, relevant and not excessive for providing online access to the services are collected. Personal data are protected in accordance with the confidentiality rules contained in the Privacy Policy of Evrotrust.

15.4 PRIVACY OF BUSINESS INFORMATION

This document does not set any requirements.

15.5 INTELLECTUAL PROPERTY RIGHTS

The relations between Evrotrust and users regarding intellectual property rights are regulated as follows:

a) Intellectual property rights over the mobile applications and over all other software applications and products, databases and other materials and resources in connection with the provision of the services are subject to protection under the Bulgarian Copyright and Related

Rights Act; they belong to Evrotrust or to the designated person who has transferred the right to use to Evrotrust and cannot be used in violation of the current legislation;

b) The user's right of access to the services does not include the right to copy or reproduce information and to use intellectual property rights, unless it is an insignificant amount of information intended for personal use, provided that legitimate interests of the authors or other signatorys of intellectual property rights are not unduly violated and in the event that the copying or reproduction is carried out for non-commercial purposes. Notwithstanding the above, the user has no right to remove the trademark signs and ownership of other intellectual property rights from the available materials, regardless of whether the signatory of the respective rights is a Evrotrust or a third party.

16 OBLIGATIONS, LIABILITIES AND GUARANTEES

16.1 OBLIGATIONS, LIABILITIES AND GUARANTEES OF THE REGISTRATION AUTHORITY

Evrotrust shall ensure that the registration authority performs its functions and obligations in full compliance with the requirements and procedures of this document, the General Terms and Conditions, the Trust services Agreement and the internal operational instructions. Evrotrust is responsible for the actions of the registration authority within the infrastructure of Evrotrust.

Evrotrust shall ensure that the registration authority:

- performs its activity using reliable and secure devices and software;
- provides services which comply with national law and does not infringe copyrights and licensed rights of the users;
- makes the necessary effort to properly identify and verify user data;
- does not make intentional mistakes or does not include inaccuracies in the information contained in the certificates;
- provides the services based on procedures that comply with applicable policies and practices; implements procedures for creating an archive and participates in external and internal audits of Evrotrust;
- provides Evrotrust with recommendations, especially those resulting from the audits;
- ensures personal data protection in accordance with the Personal Data Protection Act, GDPR and the relevant legislation;
- does not use private operator keys for purposes other than those specified in this

document.

16.2 OBLIGATIONS OF EVROTRUST

Evrotrust undertakes to:

- Provide the services to users in accordance with the General Terms and Conditions and the applicable legislation;
- take immediate actions in connection with the suspension, resumption and termination of certificates issued by it after establishing the relevant reasons to do it;
- immediately inform users about the circumstances regarding the validity or reliability of the certificates issued by it;
- publish and update electronically a publicly available list of the certificates terminated by it;
- have external audits carried out by independent auditors at least once every 2 years to verify the compliance of the certification service with the applied policy;
- to create digital signatures only from a QSCD device;
- the user's private key is maintained (or used accordingly) under the sole control of the user;
- the subject key pair should be used only for electronic signatures/seals.

16.3 GUARANTEES OF EVROTRUST

Evrotrust guarantees that when carrying out its activity, it:

- strictly complies with the conditions of this document, the General Terms and Conditions, the requirements of Regulation (EU) No. 910/2014, REGULATION (EU) 2016/679 and the applicable legislation in carrying out its activities as a qualified certification service provider;
- the services provided do not infringe copyrights and licensed rights of third parties;
- uses technical equipment and technologies that ensure reliability of the systems and the technical and cryptographic security in the implementation of processes, including a safe and secure mechanism/device for generating keys and creating an electronic signature/seal in its infrastructure;
- issues qualified certificates for electronic signatures/seals after verifying, by means permitted by law, the information provided;

- securely stores and maintains information related to the certificates issued and the operational performance of systems;
- observes the established operating procedures and rules for technical and physical control, in accordance with the conditions in the practices and policies for providing qualified trust services;
- upon request, issues the relevant types of certificates, complying with the terms and procedures in this document, the General Terms and Conditions, the relevant policies and practices and generally accepted standards
- notifies users of the qualified status;
- creates an opportunity for immediate suspension and termination of a qualified certificate;
- terminates and suspends certificates under the terms and conditions of the relevant policies and practices;
- immediately informs the interested parties (relying parties) after a suspension of a certificate;
- provides conditions for precise verification of the time of issuance, suspension, renewal and termination of certificates;
- performs identification and authentication procedures for the signature owner/creator;
- provides measures against forgery of certificates and for preserving the confidentiality of data which are accessible in the process of creating the signature / seal;
- uses reliable systems to store and manage certificates;
- ensures that only duly authorised employees have access to make changes to the data, and verify the authenticity and validity of the certificates;
- takes immediate actions in the event of security-related technical problems;
- upon expiry of the validity period of the qualified certificate, revoke its validity;
- informs the signature owners/creators and the relying parties of their obligations and due diligence in the use and trust of the trust services provided by Evrotrust, as well as about the proper and secure use of the certificates issued and the related trust services provided;
- uses and stores the collected personal and other information solely for the purposes of its activities of providing trust services in accordance with the applicable legislation;

- does not store or copy data to create user private keys;
- maintains available means that provide an opportunity to carry out its activities;
- concludes insurance for the time of its activity;
- maintains trusted staff with the necessary expertise, experience and qualification to perform the activity;
- maintains a registry/repository in which it publishes the issued Qualified Certificates, an updated Certificate Revocation List (CRL), other circumstances and electronic documents pursuant to this document and the applicable legislation;
- provides protection against any unauthorised changes to the maintained register, as a result of unauthorised and unlawful access or due to an accidental event;
- immediately publishes the certificates issued and signed in the register;
- carries out periodic internal audits of the activity of the certification authority and the registration authority;
- has external audits carried out by independent auditors and publishes the results of the audit on its website;
- uses certified software and hardware in its activity, as well as secure and reliable technological systems;
- maintains on the Evrotrust website a list of registration authorities, a list of recommended software and hardware to be used by users, forms, templates and other documents for the benefit of users.

Evrotrust, in its capacity as SSASP, is responsible for complying with the procedures described in this document, even if the functionality of SSASP is subcontracted as follows:

- Evrotrust retains overall responsibility for compliance with the procedures described in the information security policy, even if the functionality of Evrotrust is subcontracted;
- Evrotrust determines the responsibility of subcontractors and ensures that the contracting authority is obliged to fulfill the controls required by Evrotrust;
- Evrotrust describes in detail the assumption of guarantees or the waiver of guarantees in its contracts with subcontractors.

16.4 LIABILITY OF EVROTRUST

Evrotrust is liable to signature owners/creators/users and relying parties for any damage caused due to gross negligence or deliberately as a result of:

- failure to comply with the requirements of Regulation (EU) No. 910/2014 when carrying out its activity of providing qualified trust services;
- incorrect or missing data in the qualified certificate at the time of its issuance;
- damage caused in case the person indicated as the owner/creator did not have the private key corresponding to the public key at the time of issuing the certificate;
- the algorithmic mismatch between the private key and the public key stated in the certificate;
- failure to fulfill its obligations relating to the issuance and management of qualified certificates;
- failure to comply with the established policies for issuing a certificate regarding the verification of the identity of the owner/creator.

16.5 OBLIGATIONS OF USERS

Users have the following obligations:

a) the user agrees to comply with the conditions specified by Evrotrust in relation to the specificities of the services with regard to the type of provisioning regime and with regard to any policy adopted by Evrotrust and designed to protect or improve the quality and reliability of services;

б) the user himself/herself provides the technical equipment, software, access to mobile telephone services and data transmission services via a mobile network necessary for the use of the services;

в) when using the services, the user undertakes to:

- comply with the policies, practices, the General Terms and Conditions, the Contract and the applicable legislation;
- not to infringe others' property and non-property rights, including intellectual property rights;
- immediately notify Evrotrust of any case of a committed or established violation in the use of the services;

- not to impersonate another person or otherwise mislead Evrotrust or third parties about his/her identity;
- provide true, accurate and complete information required by Evrotrust, in accordance with the General Terms and Conditions, policies and practices and the current legislation, upon his/her registration and identification, as well as any other use of the application and/or services;
- check the completeness and accuracy of the content of the certificates issued to him/her and in case of discrepancy between the submitted information and the content of the respective certificate, the user must immediately notify Evrotrust;
- discontinue the use of the mobile application, the services and the certificates issued to him/her in case of suspicion of any compromise of the PIN, the identification method in the mobile application or in case of loss of its device where an application of Evrotrust is installed, taking immediate actions to stop/block/terminate these for Evrotrust;
- immediately notify Evrotrust in the event of any change in the information provided by him/her in relation to the use of the application and/or services, as well as to request immediate termination of the issued certificates in case of any change in the information included therein. When using a mobile application, the user is obliged, in case of any change in the information provided by him/her, to immediately update it through the relevant functionalities in the application. In case of any change of information provided by the user in the application, the certificates requested and issued through the mobile application, which include data that have been updated, are automatically terminated;
- use mobile applications, services and certificates issued by Evrotrust only for the intended purposes;
- not to commit malicious acts.

г) the user is obliged to take all due care, to take the necessary measures in order to protect the method of identification in the mobile application, as well as to protect its devices. For example, if the version of the mobile application requires a PIN, the user is obliged not to disclose it to third parties;

д) the owner/creator gives its consent for Evrotrust to process all data necessary for its successful identification and registration and for the verification of the data provided by the user,

as well as any additional information necessary for the provision of services, and to store such data in accordance with its applicable Personal Data Protection Policy and the current legislation.

16.6 RESPONSIBILITY OF USERS

Users shall be responsible for:

1) fulfilling the obligations provided for in this document and the General Terms and Conditions;

2) using their PINs or another method of identification, as well as for any use allowed by them to third parties. The user is solely responsible for the protection of his/her devices with a mobile application of Evrotrust installed thereon and for any use thereof allowed by him/her;

3) the user is obliged to indemnify Evrotrust for all damages and loss of profits, including for any financial penalties and attorney's fees paid and other expenses, as a result of any claims filed by and/or compensations paid to third parties in connection with his/her violating his/her obligations under the Contract, the policies and practices and all other documents forming an integral part of the Contract, as well as for any damage caused due to his/her failure to fulfill his/her obligations under current legislation;

4) the user declares and agrees that Evrotrust is not liable for any damages caused by him/her when using the mobile applications and services of Evrotrust, unless these are caused by Evrotrust intentionally or with gross negligence, or unless otherwise explicitly provided by law;

5) the owner/creator is liable to Evrotrust and all relying parties if:

- he/she fails to exactly meet the security requirements set by Evrotrust;
- he/she fails to request Evrotrust to suspend or terminate the certificate after becoming aware that the private key was misused or that there is a risk of misuse, including but not limited to the loss or theft of a device on which the mobile application is installed or if any unauthorised third party becomes aware of the PIN;
- has made false statements to Evrotrust which are also relevant to the content or to the issuance of the qualified certificate;
- when the certificate is issued with a registered Creator and a person authorised by him/her, the user is held responsible for any failure of the authorised person to fulfill his/her obligations.

6) the user is responsible for the content of the attachments and the consequences of their use.

16.7 DUE CARE OF A RELYING PARTY

Any relying party shall take all due care by:

- trusting certificates only in terms of the purpose and the limitations under which they are issued, in accordance with the applicable policies and practices of Evrotrust, the information stated in the certificate and the provisions of the General Terms and Conditions;
- verifying the status of the certificate. Any verification of the electronic authenticity and integrity of the certificate outside the public register or in an outdated Certificate Revocation List (CRL) does not provide verification of its validity and all damages incurred as a result of actions taken after such verification, shall be at the expense of the relying party;
- verifying the validity of the electronic signature/seal of electronically signed statements, as well as the validity of the electronic signature of Evrotrust along the chain of certificates to the basic certificate;
- ensuring that the applications using the certificate are functionally applicable to the purpose for which it is issued, as well as to the level of security specified in the relevant policies and practices;
- checking whether the signature/seal, accompanied by the certificate, has not been used for purposes and for value of transactions beyond the limitations and purposes stated in the certificate;
- making sure that the length of the keys used meets the security requirements of the relying party;
- making sure that the certificate was valid at the time of creating the electronic signature/seal;
- if necessary, the content of the signed electronic document can be established;
- the authenticity and validity of the certificate at the time of signing are reliably confirmed;
- the results of the verification and the electronic identity of the owner/creator are correctly presented;
- any security-relevant changes are identifiable.

Evrotrust is not liable for any damage suffered by the relying party due to its failure to take all due care.

16.7.1 VERIFICATION OF CERTIFICATES

The verification of electronic signature and electronic seal certificates issued by Evrotrust is performed by using the status verification services and the certificate revocation lists maintained by Evrotrust.

The verification of time certificates is performed by checking their compliance with the standard according to which they are issued, as well as in the public register. All electronically signed documents, including validation reports, can be verified using the validation service provided by Evrotrust (https://www.evrotrust.com/landing/bg/a/validation). The system used to validate the qualified electronic signature/seal provides the relying parties with the correct result of the validation process and allows them to detect any security-related issues.

Each relying party, upon receipt of an electronic document signed with a qualified electronic signature/seal by an owner/creator, shall verify the status of the qualified certificate either in the updated Certificate Revocation List (CRL), or by checking the current status of the certificate in real time through a qualified service for a qualified electronic signature/seal validation provided by Evrotrust. For the avoidance of doubt, the certificates issued by Evrotrust contain a period of validity which a relying party must always comply with before trusting it. The relying party should trust the certificates only until their termination. The relying party should not trust a certificate when the signature/seal was created at a time when the certificate was suspended. Any document with a defective or questionable electronic signature/seal should be rejected or possibly subjected to other procedures that allow the indication of its validity. The relying party shall also take any other precautionary measures provided for in this document, the General Terms and Conditions or any other applicable document of Evrotrust. Any person who approves such a document is held liable for any consequences thereof.

Evrotrust is not liable for any damage caused due to the failure of the relying party to comply with the requirements specified in this document.

16.8 EXEMPTION OF LIABILITY

Evrotrust shall not be held liable in the following cases:

a) to a user for any damage resulting from incorrect, incomplete or inaccurate data provided by the user;

б) for any damage caused:

- to the software, hardware, device or other telecommunications equipment, or for any loss of data resulting from materials or resources searched, downloaded or used in any way through the services provided;
- due to a user's untimely request or failure to request the suspension/blocking/termination of a mobile application, services and/or the user certificates issued;
- due to the user's failure to fulfill his/her obligations provided for in this document, the General Terms and Conditions or in all other documents forming an integral part of the Contract, as well as for any damage caused due to the user's failure to fulfill his/her obligations according to applicable policies and practices of Evrotrust and the current legislation;
- due to the use of a certificate beyond the purposes and limitations stated therein.

в) for the availability and quality of goods and/or content of services provided to the user by third parties, including by relying parties. Insofar as the actions of such third parties are not under the control of Evrotrust, it is not liable for any illegal nature of the activities of the third parties or for any incurrence, guarantee, performance, modification and termination of obligations and commitments assumed in relation to the goods or services offered by the third parties, nor is it liable for any damage and loss of profits arising from these relationships;

г) for any failure to provide the services in the event of circumstances beyond its control, such as force majeure, accidental events, problems in the global network or in the electronic communications network or in the provision of services outside the control of Evrotrust, as well as in case of third-party unauthorised access or intervention in the operation of the mobile application of Evrotrust through the user's device;

д) for any failure to provide the services or any poor-quality provision of the services as a result of tests or maintenance performed by Evrotrust for the purposes of testing equipment, connections, networks, etc., as well as tests aimed at improving or optimising the services provided. In such cases, Evrotrust notifies the user in advance of the possible temporary non-provision of services, respectively of their reduced quality, by sending an IM or a short message (SMS), or an e-mail to the registered e-mail.

f) any illegal actions of users or relying parties;

g) poor quality or functionality of software products and hardware devices used by the owner/creator and relying parties.

16.9 LIMITATION OF LIABILITY

The limitation of liability of Evrotrust is described in the General Terms and Conditions of Evrotrust which are provided to users and form an integral part of the service contract.

Evrotrust is liable for the qualified electronic signature/seal certificates within the limits of the transaction value stated in the certificates.

The liability, respectively the insurance, does not cover any damage caused due to:

- failure of the owner/creator to fulfill his/her obligations;
- compromising or losing a private key of an owner/creator due to failure to take due care to protect the key during use;
- failure of the relying party to comply with the requirements for verification of the validity of the electronic signature/seal and the qualified certificate;
- force majeure and other circumstances beyond the control of Evrotrust.

17 TERM AND TERMINATION OF THE CERTIFICATE POLICY AND PRACTICE FOR PROVIDING REMOTE ELECTRONIC SIGNATURE SERVICE

17.1 TERM

This document shall enter into force upon its approval by the Board of Directors of Evrotrust and its publication in the Public Register of Evrotrust. The provisions of this document are valid until the next version is published on the Evrotrust website.

17.2 TERMINATION

Upon termination of the activity of Evrotrust, the validity of the provisions contained herein shall be terminated.

17.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of the certification service contract, users and relying parties shall remain bound by this document in terms of issued user qualification certificates for the remainder

of the period of validity of these certificates.

18 NOTIFICATIONS AND COMMUNICATIONS BETWEEN THE PARTIES

The persons specified in this document can make statements and exchange information by ordinary mail, e-mail, telephone, network protocols (e.g. TCP/IP, HTTP) and via the Evrotrust mobile application.

19 AMENDMENTS TO THE CERTIFICATE POLICY AND PRACTICE FOR PROVIDING REMOTE ELECTRONIC SIGNATURE SERVICE

Amendments to this document may result from observed errors, updates and suggestions from affected parties. In the event of an invalid clause of this document, the entire document shall remain valid and the contract with the user is not violated. The invalid clause shall be replaced by a lawful provision. Evrotrust may revise this document without prejudice to the content of the rights and obligations therein. Any amendments that result in a new version of the document will be published on the Evrotrust website.

20 DISPUTE RESOLUTION

Evrotrust has a procedure for filing, examining and resolving suggestions, complaints, signals and claims received by users, clients or relying parties regarding the provision of services or other related issues.

Only discrepancies or disagreements between persons who are parties to the contract with Evrotrust may be subjects of disputes. Disputes or claims regarding the use of certificates and trust services provided by Evrotrust will be resolved through mediation based on information submitted in writing. Every claim must contain a description of the subject, cause or circumstances related to the problem being addressed, as well as the full name, address, e-mail and telephone number to contact the claimant. Copies of documents related to the described subject may be attached to the submitted complaints.

When filing a complaint, the user shall indicate the subject of the complaint, his/her preferred way to satisfy the complaint, respectively the amount of the claimed amount, and contact address. When filing a complaint, the user must also attach the documents on which the claim is based. When filing the complaint of the service, the user may claim for provision of the

services in accordance with the contract, a price discount or refund.

Claims, signals and complaints shall be filed as follows:

- Personally, in writing, on paper, and personally signed signed (by way of exception, only complaints are allowed to be made orally) in the office at the following address:

Evrotrust Technologies Inc.
1766 Sofia
251 G Okolovrasten Pat Av
MM Business Center, fl. 5
Tel./fax: + 359 2 448 58 58

- At the e-mail address of Evrotrust (office@evrotrust.com or dpo@evrotrust.com;), signed with a qualified electronic signature.

Evrotrust considers every claim or complaint received and prepares a written response with proposals for action to be taken (if applicable) within 7 days. When the decision of a specific claim or complaint requires the collection of additional information on the case, which requires more time, the claimant/complainant shall be notified in writing where the relevant reasons shall be specified. Evrotrust reviews a received claim or complaint and sends a final response to the claimant/complainant within 1 (one) month.

21 APPLICABLE LAW

The provisions of the applicable legislation shall apply to all issues not settled in this document.

21.1 COMPLIANCE WITH THE APPLICABLE LAW

Evrotrust applies the following requirements to ensure that it operates legally and reliably:

- Evrotrust provides users and all stakesignatorys with policies, practices, certificates and declarations for successfully performed inspections to prove how it meets the applicable legal requirements;
- Evrotrust provides trust services and products to end users - people with disabilities, where possible;

- Evrotrust provides trust services taking into consideration ETSI EN 301 549 relevant to the accessibility-related needs of ICT users in the products and services;
- Evrotrust guarantees that it has taken appropriate technical and organisational measures against unauthorised access to the information system, illegal processing of personal data or against accidental loss, destruction or damage of personal data. Evrotrust processes personal data in accordance with Regulation (EU) 2016/679. In this respect, the provision of an online service and the authentication of online data relates only to the processing of those identification data that are adequate, appropriate and not excessive in order to provide access to that service online.

In addition, Evrotrust applies the following specific requirements:

- where personal data are processed by a third party, an external registration authority, Evrotrust shall sign an appropriate agreement to ensure that subcontractors comply with legal requirements, including the application of technical, organisational and legal measures to protect personal data. The data to be signed are considered personal data;
- SCASC does not store SD after processing when it is not necessary. In cases where SCASP works in combination with a storage service of Evrotrust, users are given the opportunity to store such data for a long time.
- Evrotrust (SCASP) is fully responsible for meeting the requirements set out in this document, even if some or all of its functions are subcontracted.

This document is published on the website of Evrotrust in Bulgarian and English. In the event of any discrepancy between the texts in Bulgarian and English, the Bulgarian text shall prevail.