

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018



POLICY

FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL

Version: 2.4

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

CONTENTS

1	INTRODUCTION	5
1.1	REVIEW	5
1.2	NAME AND IDENTIFIER THE POLICY	6
1.3	PARTICIPANTS IN THE INFRASTRUCTURE	7
1.3.1	CERTIFYING AUTHORITY	7
1.3.2	REGISTERING AUTHORITY	9
1.3.3	USERS	9
1.3.4	RELYING PARTIES	10
1.3.5	OTHER PARTICIPANTS	10
1.4	USE AND APPLICABILITY OF QUALIFIED CERTIFICATES	10
1.4.1	APPLICABILITY OF QUALIFIED CERTIFICATES	10
1.4.2	PROHIBITION OF USE OF QUALIFIED CERTIFICATES	10
1.5	POLICY MANAGEMENT	10
1.5.1	POLICY MANAGEMENT ORGANIZATION	10
1.5.2	CONTACT PERSON	11
1.5.3	RELATIONSHIP BETWEEN POLICY AND PRACTICE	11
1.5.4	CONTACT PERSON AND PRACTICE APPROVAL PROCEDURES	11
1.6	DEFINITIONS AND ABBREVIATIONS	12
1.6.1	DEFINITIONS	12
1.6.2	ABBREVIATIONS	15
2	RESPONSIBILITY FOR PUBLISHING AND STORAGE	16
2.1	REPOSITORY	16
2.2	PUBLISHED INFORMATION	17
2.3	FREQUENCY OF PUBLICATION	17
2.4	ACCESS TO PUBLICATIONS	17
3	IDENTIFICATION AND VERIFICATION OF IDENTITY	18
3.1	NAMES	18
3.2	INITIAL REGISTRATION	19
3.2.1	CHECK FOR PRIVATE KEY OWNERSHIP	19
3.2.2	CHECKING THE IDENTITY OF A LEGAL ENTITY	20
3.2.3	ESTABLISHING AN IDENTITY OF A NATURAL PERSON, AN AUTHORIZED REPRESENTATIVE OF A LEGAL ENTITY	20
3.2.4	ESTABLISHING IDENTITY OF A NATURAL PERSON	20
3.2.5	VERIFICATION BY THE CERTIFYING AUTHORITY	21
3.3	IDENTIFICATION AND IDENTITY VERIFICATION UPON RENEWAL A QUALIFIED CERTIFICATE	21
3.4	IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS SUSPENDED	22
3.5	IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS TERMINATED	22
3.6	IDENTIFICATION AND IDENTITY VERIFICATION AFTER A QUALIFIED CERTIFICATE IS TERMINATED	22
4	OPERATIONAL REQUIREMENTS	23
4.1	USE OF QUALIFIED CERTIFICATE AND KEY PAIR	24
4.1.1	BY USERS	24
4.1.2	FROM RELYING PARTIES	24
4.2	RENEWAL OF QUALIFIED CERTIFICATE	25
4.3	ISSUING A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR (RE-KEY)	25
4.4	CHANGE IN QUALIFIED CERTIFICATE	26
4.5	SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE	26
4.5.1	CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE	26

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

4.5.2	PROCEDURE FOR TERMINATION OF QUALIFIED CERTIFICATE.....	27
4.5.3	GRACE PERIOD FOR TERMINATION OF QUALIFIED CERTIFICATE	28
4.5.4	ONLINE CHECK OF A CERTIFICATE STATUS.....	28
4.5.5	CIRCUMSTANCES FOR SUSPENSION OF A QUALIFIED CERTIFICATE	28
4.5.6	PROCEDURE FOR SUSPENDING AND RESUMING A QUALIFIED CERTIFICATE.....	28
4.5.7	GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE	29
4.5.8	RESUMING SUSPENDED CERTIFICATE	29
4.6	CHECKING THE STATE OF PLAY (STATUS) OF A QUALIFIED CERTIFICATE	29
4.7	TERMINATION OF A QUALIFIED CERTIFICATION SERVICES AGREEMENT BY USER.....	30
5	CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY	30
5.1	CONTROL OF PHYSICAL SECURITY	30
5.1.1	PREMISES AND THEIR STRUCTURE	30
5.1.2	THE PHYSICAL ACCESS	30
5.1.3	STORAGE OF DATA CARRIERS.....	31
5.1.4	WASTE DISPOSAL	31
5.2	ORGANIZATIONAL CONTROL.....	31
5.2.1	TRUSTED ROLES.....	32
5.2.2	REQUIREMENTS FOR DIVISION OF RESPONSIBILITIES.....	32
5.3	STAFF CONTROL.....	32
5.3.1	REQUIREMENTS FOR THE TRAINING OF EVROTRUST STAFF	32
5.4	EVENT LOGS AND JOURNAL MAINTENANCE	33
5.4.1	VULNERABILITY AND EVALUATION	33
5.5	ARCHIVING.....	33
5.6	TERMINATION OF EVROTRUST OPERATION.....	34
5.6.1	REQUIREMENTS RELATING TO THE TRANSITION TO THE TERMINATION OF THE SUPPLIER'S BUSINESS.....	34
5.6.2	TRANSFER OF BUSINESS TO ANOTHER QUALIFIED SERVICE PROVIDER	34
5.6.3	DISQUALIFICATION OF QUALIFIED PROVIDER OR QUALIFIED SERVICE STATUS	35
6	MANAGEMENT AND CONTROL OF THE TECHNICAL SECURITY.....	35
6.1	GENERATING AND INSTALLING A PAIR OF KEYS OF A CERTIFICATION AUTHORITY.....	35
6.1.1	GENERATING PAIR OF KEYS TO SIGNATORY/CREATOR.....	36
6.1.2	DELIVERY OF A PUBLIC KEY FROM A VENDOR USER	37
6.1.3	KEY LENGTH.....	38
6.1.4	PUBLIC KEY PARAMETERS	38
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROL.....	38
6.2.1	CONTROLLING OF USE AND STORAGE OF A PRIVATE KEY.....	38
6.2.2	PRIVATE KEY STORAGE	39
6.2.3	PRIVATE KEY ACTIVATION METHOD	39
6.2.4	METHOD FOR DISABLING A PRIVATE KEY	39
6.2.5	PRIVATE KEY DESTROYING METHOD.....	39
6.3	OTHER ASPECTS OF PAIR KEY MANAGEMENT	39
6.3.1	PUBLIC KEY ARCHIVING	39
6.3.2	PERIOD OF VALIDITY OF QUALIFIED CERTIFICATE AND USE OF KEYS.....	40
6.4	ACTIVATION DATA.....	40
6.4.1	GENERATING AND INSTALLING ACTIVATION DATA.....	40
6.4.2	PROTECTION OF ACTIVATION DATA.....	40
6.5	COMPUTER SYSTEMS SECURITY.....	41
6.6	LIFE CYCLE SECURITY OF THE TECHNOLOGY SYSTEM	41
6.7	NETWORK SECURITY.....	41
7	PROFILES OF QUALIFIED CERTIFICATES FOR ADVANCED ELECTRONIC SIGNATURES/SEALS	41
7.1	QUALIFIED CERTIFICATE PROFILE FOR THE EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR AES:.....	41
7.2	QUALIFIED CERTIFICATE PROFILE FOR EVROTRUST QUALIFIED LEGAL PERSON	

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

	CERTIFICATE FOR AESEAL:	44
7.3	EVROTRUST QUALIFIED PSD2 LEGAL PERSON CERTIFICATE FOR AESEAL:	46
7.4	PROFILE OF A QUALIFIED EVROTRUST SERVER CERTIFICATE	49
8	VERIFICATION AND CONTROL OF SUPPLIER'S ACTIVITY	51
8.1	ACTIONS TAKEN AS A RESULT OF AN AUDIT	51
9	OTHER BUSINESS AND LEGAL ISSUES.....	52
9.1	PRICES AND FEES.....	52
9.1.1	RETURN OF A CERTIFICATE AND REIMBURSEMENT OF PAYMENT	52
9.2	FINANCIAL RESPONSIBILITIES.....	52
9.2.1	ACTIVITY INSURANCE.....	52
9.3	PRIVACY OF PERSONAL DATA	53
9.4	INTELLECTUAL PROPERTY RIGHTS.....	53
9.4.1	OWNERSHIP OF A PAIR OF KEYS.....	53
9.5	OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST	53
9.5.1	OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF THE REGISTRATION AUTHORITY	55
9.6	OBLIGATIONS OF USERS	56
9.7	DISCLAIMER	57
9.8	SIGNATORY'S/CREATOR'S RESPONSIBILITY	57

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

1 INTRODUCTION

“Policy for qualified certification for advanced electronic signature/seal” (Policy/CP/Certificate Policy) is a document describing the general rules and regulations applied by “Evrotrust TECHNOLOGIES” AD (Evrotrust) in the creation and management of qualified certificates for advanced electronic signatures/seals, the types of qualified certification services applicable for those certificates, as well as their scope of application.

Upon issuance of qualified certificate for advanced electronic signature/seal from Evrotrust, procedures are in place to ensure a high level of reliability and security of the authenticated information identifying the Users. Procedures are in place to ensure reliability and security when issuing, publishing and managing (stopping, resuming, terminating and renewing) qualified certificates, signing/printing, storing a private key and using it in a variety of applications.

Introduction to the objectives and role of the “Policy for qualified certification for advanced electronic signature/seal” is particularly important for Users (Signatories/Creators) and Relying Parties in terms of the feasibility of these services.

The relations between Evrotrust and the User are governed by a contract for qualified certification services.

The prices of certificates and services for issuing and managing qualified certificates are contained in the Evrotrust Tariff, available on the Evrotrust web site.

1.1 REVIEW

The “Policy for qualified certification for advanced electronic signature/seal” document refers to qualified certificates issued by Evrotrust pursuant to 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) No 910/2014) and in accordance with the applicable legislation in the Republic of Bulgaria.

This document is structured in accordance with the framework defined by IETF RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

The policy complies with the following documents:

- ETSI EN 319 411-2 v2.1.1 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates”;
- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”;
- ETSI EN 319 412-1: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures”;

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЕ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

- ETSI EN 319 412-2: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“;
- ETSI EN 319 412-3: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons“;
- ETSI EN 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“;
- ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates“.
- ETSI TS 119 495: „Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366“;
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

The issue of Qualified Certificates for Advanced Electronic Signatures/Seals is associated with:

- issuance of a qualified certificate to a natural person (Signatory) – has the character of a Qualified Certificate for Advanced Electronic Signature;
- advanced electronic seal of a legal entity (Creator of a seal) – Has the character of a Qualified Certificate for Advanced Electronic Seal.

“Policy for qualified certification for advanced electronic signature/seal” to Evrotrust TECHNOLOGIES AD is a public document. It may be amended at any time by Evrotrust and any new revision shall be notified to the interested parties by publishing on the Evrotrust website: <https://www.evrotrust.com>.

1.2 NAME AND IDENTIFIER THE POLICY

This document is entitled “Policy for Qualified certification for Advanced Electronic Signature/Seal” by Evrotrust Technologies AD.

The certificates contain a policy identifier that can be used by the Relying parties to determine their applicability to an application as described in IETF RFC 3647 recommendation [1.4], section 3.3.

The policy identifiers of Qualified Certificates specified in this document are:

QCP-n:

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

policy-identifiers(1) qcp-natural (0)

QCP-I:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

policy-identifiers(1) qcp-legal (1)

The Provider supports and applies a Qualified Certification Policy based on the rules defined in ETSI EN 319 411-1 [2] with Object Identifier (OID) as follows:

Certificate type	Object Identifier
Evrotrust Qualified Natural Person Certificate for AES QCP-n, NCP+	1.3.6.1.4.1.47272.2.7 <i>(relevant to policy with O.I.D. = 0.4.0.194112.1.0)</i>
Evrotrust Qualified Legal Person Certificate for AESeal QCP-I, NCP+	1.3.6.1.4.1.47272.2.8 <i>(relevant to policy with O.I.D. = 0.4.0.194112.1.1)</i>
Evrotrust Qualified PSD2 Legal Person Certificate for AESeal QCP-I, NCP+	1.3.6.1.4.1.47272.2.8.1 <i>(relevant to policy with O.I.D. = 0.4.0.194112.1.1)</i>
Evrotrust Server Certificate QCP-I, NCP+	1.3.6.1.4.1.47272.2.6 <i>(relevant to policy with O.I.D. = 0.4.0.194112.1.1)</i>

1.3 PARTICIPANTS IN THE INFRASTRUCTURE

Evrotrust, as a qualified provider of qualified certification services, provides generation and management services (suspension, resumption and termination) of Qualified Certificates through the Authentication Body “Evrotrust RSA Operational CA” and Services for Identity and Authentication of Users through the Registration Authority. Other participants in the Evrotrust infrastructure are Users and Relying Parties.

1.3.1 CERTIFYING AUTHORITY

“Evrotrust RSA Operational CA” is a certifying authority that issues qualified certificates for advanced electronic signatures/seals that are managed under this policy.

Version	V3
Serial number	38 00 00 00 03 4e 8e cb 48 09 25 01 bc 00 00 00 00 00 03
Signature Algorithm	SHA256RSA

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Valid from	21 May 2016 00:34:35 UTC	
Valid to	21 May 2016 00:34:35 UTC	
	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	7f 3e 64 59 85 2b dd 23 29 c2 01 e7 cb c3 69 c0 87 93 2b 08	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)	
Subject Alternative Name	URL= http://www.evrotrust.com RFC822 Name=ca@evrotrust.com	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name:	

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

	URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

1.3.2 REGISTERING AUTHORITY

The registration authority is a separate structure of Evrotrust but may also be an external legal entity to which Evrotrust assigns services of registration, identification and authentication of Evrotrust users.

The Registration authority performs the following activities:

- accepts requests for qualified certificates, approves or rejects these requests in accordance with Evrotrust's internal rules of approval;
- verifies the identity of the persons applying for certificates;
- verifies that the issued certificate is handed to the User (Signatory/Creator);
- terminates qualified certificates on the basis of the Evrotrust termination rules.

Contact details of the Evrotrust Registration Authority are available on the Evrotrust web site.

1.3.3 USERS

Any natural person or legal entity who has a written contract with Evrotrust is a user of a qualified certification service provided by Evrotrust.

Users are:

- natural person (Signatory) who creates an advanced electronic signature;
- natural person (Signatory) who is the authorized representative of a legal entity and creates an advanced electronic signature;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

- legal entity (Creator of a seal), which creates an advanced electronic seal.

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

1.3.4 RELYING PARTIES

Relying Party is a natural or legal person accepting a qualified certificate issued by the Evrotrust infrastructure after having verified the advanced electronic signature/seal of a User of Qualified Certification Services to the Provider.

1.3.5 OTHER PARTICIPANTS

Evrotrust reserves the right, if necessary, to conclude contracts with outside persons for the provision of certain certification services.

1.4 USE AND APPLICABILITY OF QUALIFIED CERTIFICATES

1.4.1 APPLICABILITY OF QUALIFIED CERTIFICATES

Qualified Certificate of natural person (Signatory)/Legal Entity (Creator) or authorized representative of a legal entity named as Signatory in the certificate may be used to create an advanced electronic signature/seal in electronic documents and attachments/transactions that require high level of information security.

1.4.2 PROHIBITION OF USE OF QUALIFIED CERTIFICATES

Qualified Evrotrust certificates should not be used in a manner inconsistent with their stated purpose and scope/Policy.

Qualified certificates issued in accordance with this Policy must not be used for unlawful purposes.

1.5 POLICY MANAGEMENT

1.5.1 POLICY MANAGEMENT ORGANIZATION

Evrotrust is responsible for the management of this Policy.

Each version of the Policy is in force until the approval and publication of a new version. Each new

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

version is developed by Evrotrust employees and is published after approval by the Evrotrust Board of Directors.

Users are required to comply only with the valid version of the Policy at the time of use of Evrotrust services.

1.5.2 CONTACT PERSON

The contact person for the document “Policy for the award of a qualified certificate for advanced electronic signature/seal” by Evrotrust TECHNOLOGIES AD is the Executive Director of Evrotrust.

Further information can be obtained at the following address:

Evrotrust Technologies AD
 Sofia, 101 Tsarigradsko Shose Blvd.
 Business Centre “AKTIV”, floor 6
 Phone, fax: + 359 2 448 58 58
 Email: office@evrotrust.com

1.5.3 RELATIONSHIP BETWEEN POLICY AND PRACTICE

The “Policy for qualified certification for advanced electronic signature/seal” (CP/Policy) and the “Practice for providing qualified certifying services” (CPS/Practice) cover the same set of topics which serve the Users and the interests of the Relying Parties, so as to allow them to rely on the secure and reliable application of qualified certificates for advanced electronic signature/seal issued by Evrotrust.

The main difference between both documents is the focus of their provisions and their intended purpose. The policy examines the requirements and the implementation of the standards imposed by Evrotrust’s created infrastructure and identifies the participants in the certification services activities. Practice, on the other hand, indicates how the Certification Authority and other infrastructure participants apply procedures and controls to meet the requirements of the Policy. In other words, the purpose of both documents is to ensure the unity of rules and procedures how the participants in the Evrotrust infrastructure perform their duties and responsibilities.

The main difference between Policy and Practice is that with a Practice Certification Authority can support several Policies used for different applications or with different scope for different Relying Parties.

1.5.4 CONTACT PERSON AND PRACTICE APPROVAL PROCEDURES

The person who takes decisions on the performance of the “Practice for Providing Qualified Certification Services” (CPS) and is responsible for its management is the Executive Director of Evrotrust TECHNOLOGIES AD.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

“Practice for Providing Qualified Certification Services” (CPS) has been developed by the Evrotrust team and has been approved by the Board of Directors of Evrotrust.

Each version of “Practice for Providing Qualified Certification Services” is in effect until the approval and publication of a new version.

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Certification – A certification services provider may be granted a “qualified” status for a specified period in accordance with Regulation (EU) No 910/2014 after passing a successful audit of compliance by accredited auditors;

Validation data - Data that is used to validate an electronic signature or an electronic seal;

Validation - The process of verifying and confirming that an electronic signature or a seal is valid.

Person identification data - A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

Data for the creation of an electronic signature - Unique data which is used by the Signatory to create an electronic signature;

Relying Parties – Natural persons or legal entities who are the addressees of electronic statements or other information sites and trust the certification services of Evrotrust;

Qualified trust service provider - A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body;

Electronic time stamp - Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time and is issued in accordance with Regulation (EU) No. 910/2014;

Electronic seal - Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity; The electronic seal should serve as evidence that an electronic document was issued by a legal entity, ensuring certainty of the document’s

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

origin and integrity.

Electronic signature - Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the Signatory to sign;

Qualified trust service - A trust service that meets the applicable requirements laid down in Regulation (EU) No. 910/2014;

Qualified certificate for electronic signature - A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Regulation (EU) No. 910/2014;

Qualified electronic time stamp - An electronic time stamp which meets the requirements laid down in Regulation (EU) No. 910/2014;

Advanced electronic seal - An advanced electronic seal, which is created by an advanced electronic seal creation application/system, and that is based on a qualified certificate for electronic stamp;

Advanced electronic signature - An advanced electronic signature that is created by an advanced electronic signature creation application/system, and which is based on a qualified certificate for electronic signatures;

Coordinated Universal Time (UTC) – Time to which the time is calculated in different time zones. It uses the International Atomic Time (TAI) as a basis;

Policy Approval Authority (PAA) – Body authorized to approve, monitor, and maintain the Certification Policy;

Compliance assessment body – A body that is accredited in accordance with Regulation (EC) No. 765/2008 as competent to assess the compliance of a qualified certification service provider and the qualified certification services provided by that provider with the requirements of Regulation (EU) No. 910/2014;

Practice (CPS) - Practice in the provision of Qualified Certification Services is a document containing rules on the issuance, suspension, revocation and revocation of certificates as well as the conditions for granting access to certificates;

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

CRL/Certificate Revocation List – The list containing certificates that may no longer be considered valid. The CRL is digitally signed by the issuer of the certificates – the Certifying Authority;

Creator of a seal means a legal entity who creates an electronic seal;

Private key – A string of symbols that is used in an algorithm to convert information from a readable encrypted form or vice versa – encrypted in a readable form (decryption);

Public Key – One of the key pairs used in an asymmetric cryptosystem that is accessible and can be used to verify electronic signature/seal;

Signatory of an electronic signature - A natural person who creates an electronic signature;

Certification service - An electronic service which is usually provided in return for payment consisting in: the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, registered email services, as well as certificates related to those services; or the creation, verification and validation of certificates of authenticity of a website; or the storage of electronic signatures, seals or certificates related to those services;

Electronic seal certificate - Legal entity certificate by terms of Regulation (EU) No 910/2014;

Time stamp certificate - Data in electronic form linking other electronic data to a certain point in time, providing evidence that these data exist at that time;

Certificate for electronic signature - An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

Environment for creating an advanced electronic seal – An environment for creating an advanced electronic seal is an application or system that complies with the requirements of Regulation (EU) No 910/2014;

Environment for the creation of an advanced electronic signature – An advanced electronic signature enrichment environment is an electronic signature application or system that complies with the requirements of Regulation (EU) No 910/2014;

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Electronic signature creation environment - Application or system used to create an electronic signature is a configured software or hardware used for the creation of an electronic signature;

1.6.2 ABBREVIATIONS

QCP-I – Qualified certificate policy issued to a legal entity when the private key of the associated certificate is generated in a secure environment;

QCP-n - Qualified certificate policy issued to a natural person when the private key of the associated certificate is generated in a secure environment;

NCP + – Enhanced normalized certification policy that includes additional requirements for Qualified Certificates in accordance with Regulation (EU) No. 910/2014

CA Certification Authority – Certifying Authority;

CN Common Name – Common name;

CP Certificate Policy – Policies to provide qualified certificate for advanced electronic signature/seal;

CPS Certification Practice Statement – Certification services provision practice;

CRL, Certificate Revocation List – List of suspended and terminated certificates;

PSD2 (Payment Services Directive 2) - Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

PSP (Payment Service Provider) - Payment Service Provider;

DN, Distinguished Name – Distinct name of subject, entered in the certificate;

Enhanced key usage – Expanded key usage goals

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

FIPS, Federal Information Processing Standard – Federal standard for information processing;

HSM, Hardware Security Module – Hardware Cryptographic Module;

Issuer – Publisher;

LDAP, Lightweight Directory Access Protocol – Protocol for Simple Registry Access;

OID, Object Identifier – Object Identifier;

PKCS, Public Key Cryptography Standards – Cryptographic standard for public key transfer;

PKI, Public Key Infrastructure – Public Key Infrastructure – aggregate of hardware, software, staff, Evrotrust documentation for creating, using, managing and verifying issued electronic signatures/stamps;

RA, Registration Authority – Registration Authority;

RSA, Rivest-Shamir-Adelman – Type of asymmetric cryptographic algorithm for creation of an electronic signature;

SHA, Secure Hash Algorithm – A sure hash algorithm to extract a hash-identifier;

SSL, Secure Socket Layer – Secure data transmission channel;

SMIME, Secure Multipurpose Internet Mail Extensions – A secure e-mail protocol over the Internet;

2 RESPONSIBILITY FOR PUBLISHING AND STORAGE

2.1 REPOSITORY

The Evrotrust Public Register is a repository of current and previous versions of electronic documents (including up-to-date versions of the “Qualified Certificate for Advanced Electronic Signature/Seal Certificate” and “Practice for Qualified Certification Services”), intended for Users, Certificates of the Certifying Authority, User Certificates, CRLs and other information.

The repository is managed and controlled by Evrotrust.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

All users and trustees have permanent access to all information in the repository at: <https://www.evrotrust.com>. Restrictions have the relying parties, but they are related to accessing only user certificates for which public access is restricted.

2.2 PUBLISHED INFORMATION

The public registry could be accessed at: <https://www.evrotrust.com/>.

Qualified certificates issued are stored in a Evrotrust database. Access to these certificates can be accomplished through an online protocol to verify the status of the issued OCSP (Online Certificate Status Protocol).

For online verification of registry data, it is necessary to use appropriate software (OCSP client or access through the supplier's website).

Verification of qualified certificates issued may also be made on the CRL, which is published on the Evrotrust website and updated every 3 hours.

2.3 FREQUENCY OF PUBLICATION

The documentation, including Policy and Practice in the provision of Qualified Certification Services, Agreements, Patterns, Electronic Signature/Seal Manuals, Audit Reports, etc. issued by Evrotrust, is published on the Evrotrust web site immediately upon each update.

The Operating Certificates of the Certifying Authority are published immediately upon each issue of new certificates.

An update of the Public Register with the issued user qualified certificates shall be made automatically and immediately after the publication of each newly issued valid certificate.

An update of the current CRL is automatically made no more than 3 (three) hours or immediately after the revocation/termination or suspension/resumption of a valid certificate.

2.4 ACCESS TO PUBLICATIONS

Evrotrust offers directory services for information stored in the repository (public register), providing HTTP/HTTPS and OCSP-based access.

Access to repository information is not limited by Evrotrust, except upon request of the Signatory/Creator and only in respect of a validly issued Qualified Certificate.

The information published in Evrotrust's repository is permanently accessible (24/7/365), except in the event of events beyond Evrotrust's control.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

3 IDENTIFICATION AND VERIFICATION OF IDENTITY

3.1 NAMES

Qualified certificates use all applicable names or other identifiers, including ASN.1 object identifiers.

The certificate names requirements are as stated in Recommendation ITU-T X.509 or IETF RFC 5280 and ETSI EN 319 412. The names may be in accordance with the Domain Name Service (DNS) described in RFC 2247.

The Subject field on the certificate contains the Signatory/Creator name.

The name and other distinguishing marks of the Signatory/Creator in the appropriate fields for each type of certificate are in accordance with the DN (Distinguished Name) formed according to the standard X.500 and X.520.

Evrotrust may issue a qualified certificate using a “nickname” to name the User only after the Registration Authority has collected the necessary identification information and has successfully identified it.

The names included in the Distinguished Name (DN) of the user have their meaning in Bulgarian or in another foreign language. The DN structure is approved by the Registration Authority and depends on the type of Qualified Certificate and the User. DN consists of the following areas (the descriptions are in accordance with RFC 3280 and X.520):

- field C – international country name abbreviation (BG for Bulgaria),
- field CN – full/common name of the natural person or organization,
- field GN – name of the natural person,
- field SN – surname of the natural person,
- field O – name of the organization that the person represents,
- field E – user email address,
- field SerialNumber – unique identifier of the natural person,
- Other fields, which are detailed in the policies for the Qualified Certificates’ profiles.

Signatory/Creator with a unique DN in the Evrotrust domain may have more than one issued valid Qualified Certificates.

Each issued certificate has a unique serial number (“SerialNumber”) in the Evrotrust domain. The combination of “Issuer” and “SerialNumber” fields ensures the uniqueness of the issued certificate in the public domain.

Verification of identity, or identity of:

- A legal entity (Creator of a seal) shall be carried out by checking in the relevant registers under

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

the provided UIC, respectively BULSTAT by the order of the Electronic Management Act (EMA). A list of required documents is supported on the Evrotrust website;

➤ An authorized representative of a legal entity (Signatory), shall be carried out by means of an authentication and authentication and a handwritten signature on the required documents;

When documents are sent by post or electronically, the documents are authenticated.

➤ A natural person (Signatory), shall be carried out by personal presence with an identification document or by remote verification by means of authentication of the documents.

➤ When using the Evrotrust mobile application, physical identification is carried out through an automated video identification system by checking a scanned identity document and obtaining data on its validity from a national database of Bulgarian identity documents as well as by biometric analysis of the person with picture material obtained from the national database. In the event of a failure, identification is performed by an operator using a special methodology via videoconference. The verification of the representative power of a natural person in relation to the legal entity is carried out by checking the data for the entries in the respective registers with the Registry Agency.

Evrotrust performs verification of the authenticity of the information in the filled in documents, with all legally allowed funds in the respective public registers.

A list of the required documents for a natural person for issuing and managing a qualified certificate is maintained on the Evrotrust website.

3.2 INITIAL REGISTRATION

Initial registration includes a number of procedures that allow identification to be collected before a User certificate is issued. Confirmation of these data requires face-to-face contact with a representative of the Registration Authority, notary or other authorized person confirming his/her identity. This procedure may be carried out remotely through a remote identification system via the Evrotrust mobile application.

After verification of the data provided and a contract for a qualified certification service, the requesting person is included as a User of the services of Evrotrust.

3.2.1 CHECK FOR PRIVATE KEY OWNERSHIP

Evrotrust may provide the Signatory/Creator with a service locally or by remotely generating the key pair.

For issuance or continuation of a qualified certificate, Evrotrust must receive an electronic request in PKCS # 10 format. The specification of this request form for a qualified certificate requires that the request be signed by the Signatory/Creator holding the private key.

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

3.2.2 CHECKING THE IDENTITY OF A LEGAL ENTITY

The establishment of the identity of a Bulgarian legal entity (Creator of a stamp) shall be carried out by a representative of the Registration Authority, by checking in the respective registers under UIC provided, respectively BULSTAT by the order of the E-government Act. For non-business, Bulgarian legal entities as well as for foreign legal entities for which an automated check cannot be performed shall be provided:

- court decision or other document certifying the occurrence of the legal entity;
- document certifying the state of play of the person;
- unique national identifier.

A list of required documents is supported on the Evrotrust website.

3.2.3 ESTABLISHING AN IDENTITY OF A NATURAL PERSON, AN AUTHORIZED REPRESENTATIVE OF A LEGAL ENTITY

For the issuance of a qualified certificate to a natural person (Signatory), which is authorized by a legal person, the authorized representative shall appear before the Registration Authority. Validation of the information contained in the submitted documents is done by:

- “True copy” validation and a handwritten signature on the documents before an employee of the Registrar in case of personal transmission of the documents;
- signing of the attached electronic formats of the documents with a valid certificate for advanced electronic signature/seal;
- examination and confirmation by using a specialized mobile or other application and after proper identification of the representative and/or legal entity by an employee of Evrotrust and by checking the registrations of the representative authority in the official registers (to the Registry Agency).

The verification of the identity of a legal entity seeks to prove that during the examination of the application the legal person exists and that the representative who applies for a qualified certificate has the power to request the issue.

3.2.4 ESTABLISHING IDENTITY OF A NATURAL PERSON

Identification and verification of the identity of a natural person (Signatory) is carried out by a representative of the Registration Authority. Identification can also be done automated by remote verification.

To identify and verify the identity of a natural person, it is required to produce an identity document.

The natural person confirms the authenticity of the data by:

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЕ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

- a handwritten signature on the documents before an employee of the Registrar in case of personal transmission of the documents;
- signing the attached electronic documents with a valid electronic signature certificate within the meaning of Regulation (EU) No. 910/2014;
- review and confirmation by using a specialized mobile or other application and upon proper identification of the natural person automated or by an employee of Evrotrust.

A list of the required documents for a natural person (Signatory) for issuing and managing a qualified certificate is maintained on the Evrotrust website.

3.2.5 VERIFICATION BY THE CERTIFYING AUTHORITY

Upon successful identification and verification by the Registration Authority of the conditions for the issuance or management of a qualified certificate, a representative of the Registration Authority confirms the data to the Certifying Authority. The Certifying Authority shall immediately publish the Qualified Certificate issued in the Public Register/Issued Certificates repository or CRL.

In Evrotrust, only the operational Certifying Authority that has issued an advanced electronic signature/seal certificate may terminate this certificate.

3.3 IDENTIFICATION AND IDENTITY VERIFICATION UPON RENEWAL A QUALIFIED CERTIFICATE

Evrotrust may renew a validly qualified certificate which has not been terminated within its term of validity generating a new key pair (“Re-key”).

Evrotrust does not maintain the option for Renewal with preservation of the existing key pair (Renewal) or with preservation of the serial number.

Evrotrust renews current Signatory/Creator certificates with a new key pair (Re-key) only if there have been no changes in the verified information. Renewed certificates contain new serial numbers, new public keys, new validity periods and new electronic signatures/seals of the Certification Body, whereby the verified information therein remains the same.

Upon renewal, the current qualified certificate shall not be terminated and shall remain valid within its period of validity.

His/her personal attendance is not required before the Evrotrust Registration Authority for identification and identity verification of Signatory/Creator of the qualified certificate, which is renewed,

In the event of changes of the information about the Signatory/Creator of qualified certificate, the current certificate is not renewed. The provider issues a new qualified certificate following the initial identification and identity verification and terminates the current qualified certificate immediately.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

3.4 IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS SUSPENDED

Suspending the validity of a qualified certificate is an established practice of Evrotrust and differs from a termination in that it leads to the temporary suspension of the certification power of a certificate. For reasons of legal certainty, Evrotrust always makes clear the status of suspension of certificates.

Evrotrust is obliged, through the Registration Authority, to suspend the validity of a valid certificate upon request for suspension.

Evrotrust, through the Registration Authority, automatically resumes the operation of a suspended certificate.

The time in the systems associated with stopping and terminating certificates is synchronized to UTC at least once every 24 hours.

Suspension of a certificate issued from a remote location is not allowed.

3.5 IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS TERMINATED

When Evrotrust, through the Registration Authority or itself, ceases a qualified certificate, it shall record this in the databases it holds with qualified certificates and publish the revoked status of the certificate in due time but not later than 24 hours after the request is received. The revocation shall become effective immediately upon its publication.

Upon termination through the Evrotrust mobile application, identity verification is not performed due to the Signatory's access to the appropriate functionality.

3.6 IDENTIFICATION AND IDENTITY VERIFICATION AFTER A QUALIFIED CERTIFICATE IS TERMINATED

The policy and practice of providing qualified certification services to Evrotrust does not allow the renewal of a qualified certificate through Renewal or Re-key after termination.

The Signatory/Creator of a terminated Qualified Certificate may request the issuance of a new certificate.

Evrotrust, through the Registration Authority, performs initial identification and identity verification of the Signatory/Creator if he/she requests a new certificate. Such a check is not performed if the user requests the issue of a new qualified certificate from the mobile application in which there is an active account.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

4 OPERATIONAL REQUIREMENTS

Evrotrust, through the Registration Authority, within the framework of a Qualified Certification Services Agreement, provides the following operating procedures for Qualified Certification Services applicable to Advanced Electronic Signatures/Seals:

- registration of a request for a qualified certificate;
- processing a request for a qualified certificate;
- issuing a qualified certificate;
- handing over to the User of the Qualified Certificate issued;
- renewing a qualified certificate;
- suspension/resumption of a qualified certificate;
- termination of a qualified certificate;

The request for registration of Qualified Certification Services Users shall be filed with the Registration Authority by natural, legal or authorized persons and shall include the following information:

- full name of the Signatory/Creator or an authorized representative of the legal entity;
- evidence of the Representative authority of the Signatory against the Creator;
- identifiers: UIC (Personal Identification Number), etc.;
- postal address of the person (country, district, postal code, city or village, building number, street or neighbourhood name, telephone, fax number);
- e-mail address;
- type of qualified certificate requested, taking into account its purpose;
- the identifier of the authentication policy on the basis of which the certificate is issued;
- presence of a private key corresponding to a public key;
- public key;
- additional information requested to be included in the certificate as well as an admissible unconfirmed one;
- signing a Qualified Certification Services Agreement and agreeing to the terms and conditions of the Policy and Practice for the provision of qualified certification services by Evrotrust.

An application for a qualified certificate may also be filed through the Evrotrust mobile application. In this case, the above requirements do not apply.

Signatory/Creator or authorized representative of the legal entity may request the renewal of a qualified certificate, subject to the time limits, requirements and conditions for renewal.

Renewal of a Qualified Certificate keeps the Signatory/Creator or Authorized Person information

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЕ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

from the current certificate, and the validity period is changed in the renewed certificate. Certificates that have been terminated during their period of validity shall not be renewed.

Renewal is not allowed for qualified certificates issued remotely through the Evrotrust mobile application.

A request for termination of a qualified certificate is filed by the Signatory/Creator or an authorized representative of the legal person on site at the Registration Authority or by electronic means.

Evrotrust **terminates** a certificate issued upon:

- death or incapacity of the Signatory/Creator;
- termination of the Representative authority of the Signatory against the Creator;
- detecting false data when issuing the certificate;
- subsequently became false certified information;
- in case of change in already certified information of Signatory/Creator;
- compromise of a private key;
- delay in payment of due remuneration;
- request for termination by the Signatory/Creator, after Evrotrust has ascertained their identity and the representative power of the Creator.

➤ Upon termination by the mobile application, it is assumed that the request is made by activating the appropriate functionality. In this case, the termination is done immediately.

Termination and Suspension Management Services are available 24 hours a day, 7 days a week.

The time in the systems associated with stopping and terminating certificates is synchronized to UTC at least once every 24 hours.

4.1 USE OF QUALIFIED CERTIFICATE AND KEY PAIR

4.1.1 BY USERS

Users must use the private keys and their respective qualified certificates:

- in accordance with their intended purpose;
- only within the period of their validity;
- when the certificate is suspended, the user should not use the private key, especially for creating an electronic signature/seal.

Responsibility for using the private key is at the Signatory.

4.1.2 FROM RELYING PARTIES

Relying parties, including operators in the Registration Authority, must use the public keys and

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

their respective certificates:

- in accordance with their intended purpose;
- only after checking their status and checking the electronic signature of the Certification

Authority that issued the certificate;

- until the validity of a key is revoked/terminated;
- when the certificate is suspended, the relying party should not accept the public key.

4.2 RENEWAL OF QUALIFIED CERTIFICATE

Renewal of a qualified certificate means replacing a valid certificate with a new one without changing the existing information in it, except for a new serial number and a new validity period.

Renewal is only performed within the validity period of a current certificate. It must be preceded by the registration of a renewal application in an appropriate form accepted and approved by an operator in the Registration Authority, verified identity and correctness of the submitted application.

Renewal of a remote certificate issued through the mobile application is not allowed.

4.3 ISSUING A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR (RE-KEY)

A new pair of keys is generated by Evrotrust, in cases where an already registered user requests to generate a new key pair or a new user requests to generate a pair of keys. The generation of a new pair of keys is accompanied by the issue of a new qualified certificate confirming ownership of the newly created key pair.

Evrotrust shall inform users in advance by email at least 14 days before the expiration of the validity of the issued certificate, whenever possible.

The request for renewal of a qualified certificate by electronic application is certified by an electronic signature/seal corresponding to a valid Signatory/Creator's certificate or an authorized representative of the legal entity.

In the event that the renewal certificate has expired, the Signatory/Creator or the person authorized by him/her has to personally visit the Evrotrust Registration Authority.

Renewal of certificates issued remotely through the Evrotrust mobile application is not allowed.

The Signatory/Creator or the person authorized by him/her may object if the issued certificate contains errors or incompleteness within 3 (three days) of its publication in the register. Evrotrust removes them by issuing a new qualified certificate without payment of remuneration, unless they are due to the provision of false data. In the absence of objection, the content of the Qualified Certificate is deemed to have been accepted.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

4.4 CHANGE IN QUALIFIED CERTIFICATE

Changing a qualified certificate means a change in the content of the data in a previously issued and published advanced electronic signature/seal certificate. Upon changing a qualified certificate, a new pair of keys is required to be generated.

The change is treated in the same way as issuing a new qualified certificate.

4.5 SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE

Suspension and termination of a qualified certificate is only valid during the period of validity of the certificate. Suspensions causes temporary suspension of the validity of certificate. Termination results in the irreversible suspension of the validity of the certificate.

If a certificate is terminated after the initial activation, it will lose its validity from the moment of termination and its status cannot be restored under any circumstances.

If Evrotrust suspends or terminates a qualified certificate, it registers this change in its qualified certificate database and publishes the revoked status of the certificate in due time. Suspension or termination becomes effective as soon as the certificate is published in the repository.

Termination and suspension management services for a qualified certificate are available 24 hours a day, 7 days a week.

Suspension of certificates issued remotely through the Evrotrust mobile application is not allowed.

4.5.1 CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE

Evrotrust terminates a qualified certificate issued by it, subject to the following hypotheses:

- when the information entered in the certificate has changed;
- when there is a suspicion that the private key associated with the public key contained in the certificate is compromised;
 - the user decides to terminate the contract with Evrotrust;
 - death or incapacity of the Signatory/Creator;
 - termination of the Representative authority of the Signatory against the Creator;
 - when the User does not meet the requirements of the Certification Policy;
 - if the Certifying Authority ceases its activity;
 - if the User owes outstanding fees for the provision of Qualified Certification Services;
 - when the reliability and security of the Certification Authority private key is compromised;
 - when User who is an employee of an organization terminates his or her contract of employment

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЕ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

and does not delete a private key corresponding to the qualified certificate issued.

4.5.2 PROCEDURE FOR TERMINATION OF QUALIFIED CERTIFICATE

4.5.2.1 Qualified end-user certificate termination procedure

Termination of a qualified end-user certificate is preceded by a request for termination before the Evrotrust Registration Authority. A request for termination of a certificate may be registered electronically only when the Signatory/Creator has (another) valid and available for use Advanced Electronic Signature/Seal Certificate. Otherwise, an on-site request is made to an Authorized Operator at the Registration Authority.

Any request for termination of a certificate must contain irrefutable proof of confirmation of termination.

The procedure for terminating a qualified certificate is as follows:

- The Authorized Operator at the Registration Authority immediately suspends the certificate without identifying the user;
- The registration authority strictly follows the requirements for identification and authentication of the Signatory/Creator or an authorized representative of the legal entity and the reasons for termination. If necessary, the Signatory/Creator or the authorized representative of the legal entity shall visit the Evrotrust Registration Authority personally for subsequent verification of the identity or identity of the consumer;
- Upon successful authentication of the Signatory/Creator or the authorized representative of the legal entity, the Registration Authority applies to the Operational Certification Authority for termination of the certificate. Upon confirmation by the Certifying Authority, the request for termination of the certificate is executed;
- In the event of failure to identify and verify the conditions for termination, the Registration Authority shall reject the request for termination of the certificate and immediately notify the Signatory/Creator or the authorized representative of the legal entity of the reasons for doing so;
- User with a rejected request for termination of a Qualified Certificate may file a new request for termination of the certificate after removing the reasons for the refusal;
- Upon termination of the certificate, Evrotrust, through its Certifying Authority, immediately issues the suspended certificate on the CRL by issuing a new List;
- Upon termination of the qualified certificate, Evrotrust shall notify the Signatory/Creator about the cancelled certificate.

Terminated Signatory/Creator's Certificate is not subject to resumption or renewal.

When using a mobile application, it is assumed that the termination request is present when the User has activated the appropriate functionality set forth in the app. In this case, the above procedures do

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

not apply.

4.5.3 GRACE PERIOD FOR TERMINATION OF QUALIFIED CERTIFICATE

Before suspending the validity of a validated certificate, Evrotrust, through its Registration Authority, shall suspend the certificate validity for a grace period until the reasons for the suspension have been specified, but not longer than 72 hours. Within this period Evrotrust handles the request for termination of the Qualified Certificate.

Grace period is not allowed for remote certificates issued. They are terminated immediately.

4.5.4 ONLINE CHECK OF A CERTIFICATE STATUS

Evrotrust provides a qualified service to check the status of issued certificates in real time. This service is based on a Protocol for Online Certificate Verification of the Status (OCSP) described in RFC 2560. Using OCSP makes it possible to obtain status information for certificates without requiring verification in the CRL.

The OCSP service generates a database-based response. The OCSP response is valid for up to 7 days. To maintain the proper system performance, OCSP responses are cached for a predetermined time (typically not more than a few hours).

Verification in real-time certificate status under the OCSP protocol can be performed via Internet at the Evrotrust website: <https://www.evrotrust.com>.

4.5.5 CIRCUMSTANCES FOR SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust, through its Operator Certification Authority (“Evrotrust RSA Operational CA”), suspends a valid certificate under certain conditions.

Evrotrust takes immediate action on the request to suspend a certificate.

The time during which the certificate was suspended is deemed invalid and all electronic signatures/stamps checked with this certificate are null and void.

4.5.6 PROCEDURE FOR SUSPENDING AND RESUMING A QUALIFIED CERTIFICATE

Suspension of a qualified certificate is preceded by the registration of a request for suspension before the Registration Authority.

- The request for suspension of a certificate may be registered electronically or submitted on

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

paper to an authorized operator of the Evrotrust Registration Authority.

- The request for suspension of a certificate is electronically certified by an electronic signature/seal corresponding to a valid Signatory/Creator's certificate.
- The Authorized Operator at the Registration Authority immediately suspends the Qualified Certificate without identifying the user. Suspension of the certificate is made by its temporary entry in the CRL.
- The registration authority may not reject a suspension request.
- Upon termination of a certificate, Evrotrust, through its Operational Certifying Authority, immediately publishes the suspended certificate on the CRL by issuing a new List.
- Upon termination of a certificate, Evrotrust shall immediately notify the Signatory/Creator of the suspended Qualified Certificate.
- Stopping and resuming qualified certificates issued remotely through the mobile application is not allowed.

4.5.7 GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust suspends a Qualified Electronic Signature/Seal Certificate for a grace period until the reasons for the suspension are specified, but not longer than 72 hours.

Grace period of suspension of qualified certificates issued remotely through the mobile application is not allowed.

4.5.8 RESUMING SUSPENDED CERTIFICATE

Evrotrust resumes the operation of a suspended certificate:

- after dropping the ground for stopping before the end of the suspension;
- upon request of the Signatory, after clarifying the reasons for the suspension requested;

Upon renewal of the certificate, the latter is considered to be valid.

4.6 CHECKING THE STATE OF PLAY (STATUS) OF A QUALIFIED CERTIFICATE

Information on the status of certificates issued by Evrotrust may be obtained from the CRL, published on the Evrotrust website and through the OCSP Online Certificate Verification Protocol.

Authentication services for status verification of Qualified Certificates are available 24/7/365 (continuously operating).

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЩ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

4.7 TERMINATION OF A QUALIFIED CERTIFICATION SERVICES AGREEMENT BY USER

The Contract for Qualified Certification Services between Evrotrust and User is terminated:

- after expiry of the last issued qualified certificate, and the user has not taken any action to update his/her qualified certificate;
- when the qualified certificate has been terminated and the user has not taken action to issue another certificate.
- when User profile is closed from the Evrotrust mobile application. In this case, all qualified certificates issued shall be terminated.

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 CONTROL OF PHYSICAL SECURITY

The measures taken with regard to the physical protection of Evrotrust are an element of the Evrotrust Information Security System, which complies with the requirements of ISO/IEC 27001:2013, ISO 9001:2015, ISO 22301: 2012, и ISO/IEC 1901120000-1:2011.

Measures related to the physical protection of information data, technological systems, premises and related support systems are aimed at preventing:

- unauthorized access, damage and interference in working conditions;
- loss, damage or compromise of resources;
- compromising or stealing information or means of processing the information.

Infrastructure of the provider is physically and logically distinct and is not used in other activities, which Evrotrust Technologies AD implements.

5.1.1 PREMISES AND THEIR STRUCTURE

Evrotrust has a specially designed and equipped room with the highest degree of physical access control, which houses the Certification Authority of the supplier and all the central components of the infrastructure.

5.1.2 THE PHYSICAL ACCESS

The physical security of certificate issuing and management systems is consistent with the requirements of international standards and recommendations.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

For the equipment in the protected and isolated room of Evrotrust, physical integrity is ensured. There is two-factor access control and 24-hour armed physical security. Physical access to critical equipment is not allowed for more than 30 (thirty) minutes per visit. No access to the cabinet is permitted with the equipment of more than 2 (two) authorized Evrotrust technicians. Every access to critical infrastructure premises is documented in special journals.

The protection of the Evrotrust building is performed by unarmed 24-hour security. Evrotrust has an Alarm System, Video Surveillance System, Signal-Alarm System and Access Control System.

In Evrotrust the offices of the Registration Authorities are detached and separated from the other premises. They are equipped with a technique for safe storage of data and documents. Access to these areas is monitored and limited to authorized persons related to the activity of the Registration Authority (operators of the Registration Authority, System Administrators) and their clients.

5.1.3 STORAGE OF DATA CARRIERS

All media containing software, data archives, or audit information are stored in a firebox in a special archive room with access control. There is a system of physical and logical protection in the room with Evrotrust's archive.

5.1.4 WASTE DISPOSAL

Paper and electronic media containing potentially significant security information for Evrotrust shall be destroyed in special shredding devices after the storage period specified in the internal rules.

The data carriers for the cryptographic keys used for their storage and the access codes are fragmented with appropriate devices. This applies to carriers that do not allow the permanent deletion of stored data and its reuse.

In certain cases, information from portable media is destroyed by deleting or formatting the non-recoverable environment.

5.2 ORGANIZATIONAL CONTROL

All security procedures for issuing, administering, and using Qualified Certificates for Advanced Electronic Signature/Seal are performed by trusted Evrotrust staff.

Evrotrust maintains a sufficient number of qualified employees who, at every moment of its activity, ensure compliance with the applicable legislation and the company's internal rules and regulations.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

5.2.1 TRUSTED ROLES

A detailed distribution of the functions and responsibilities of the staff is written in Evrotrust's internal documents: job descriptions, establishment plan and relevant internal operational procedures.

The allocation of functions is done in such a way as to minimize the risk of compromise, leakage of confidential information or the occurrence of a conflict of interest.

5.2.2 REQUIREMENTS FOR DIVISION OF RESPONSIBILITIES

The trusted activities of Evrotrust personnel are performed by different persons.

5.3 STAFF CONTROL

The staff of Evrotrust consists of a sufficient number of highly qualified employees. Trusted persons have the necessary professional background and experience to ensure that security requirements and technical security assessment standards are respected. Professional knowledge of information systems, cryptography and public key infrastructure enables employees with trusted roles to perform their duties properly.

Evrotrust employees periodically attend further training courses in accordance with the current requirements in Evrotrust's fields of activity.

5.3.1 REQUIREMENTS FOR THE TRAINING OF EVROTRUST STAFF

Personnel performing functions and tasks arising from their employment in Evrotrust or employment in the Registration Authority (with the presence of an external Registration Authority) must undergo the following training:

- “Practice in Providing Qualified Certification Services” by Evrotrust TECHNOLOGIES AD;
- “Policy for Providing Qualified Certificate for Advanced Electronic Signature/Seal” by Evrotrust TECHNOLOGIES AD;
- Provisions, procedures and documentation relating to the role played;
- Security Technologies and security procedures used by the Certifying Authority and the Registration Authority;
- System software of the Certifying Authority and the Registration Authority;
- Responsibilities arising from roles and tasks performed in the system;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

➤ Procedures performed in case of system failure or interruption of the activities of the Certification Authority.

5.4 EVENT LOGS AND JOURNAL MAINTENANCE

For the efficient management and operation of Evrotrust, all events having a significant impact on the security and reliability of the technology system, personnel and user control and the security impact of the qualified certification services provided are recorded.

Electronic journal information is generated automatically.

Recordings journals of recorded events are stored in files on the system disk for at least 6 (six) months. During this time, they are available online or in the process of searching by any authorized Evrotrust employee. After this period, the records are stored in the archives.

Archived journals are kept for at least 20 (twenty) years.

The archive is signed with an electronic signature/electronic time stamp. Information from the log entries is periodically recorded on physical media stored in a special safe located in a room with a high degree of physical protection and access control.

5.4.1 VULNERABILITY AND EVALUATION

Evrotrust classifies and maintains registers of all assets in accordance with ISO/IEC 27001: 20013. According to the “Security Policy” of EVOTRUST, an analysis is carried out for the vulnerability assessment of all internal procedures, applications and information systems. Analytical requirements may also be determined by an external institution authorized to audit Evrotrust.

The risk analysis shall be carried out at least once a year. The decision to proceed with the analysis is done by the Board of Directors.

5.5 ARCHIVING

Information about significant events is archived in electronic form periodically.

Evrotrust backs up all data and files related to: registration information; system security; all requests submitted by users; all consumer information; all keys used by the Certifying Authorities and the Registration Authority; and all correspondence between Evrotrust and users. All documents and data used in the identity verification process are subject to backup.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

5.6 TERMINATION OF EVROTRUST OPERATION

5.6.1 REQUIREMENTS RELATING TO THE TRANSITION TO THE TERMINATION OF THE SUPPLIER'S BUSINESS

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

➤ notify the Supervisory Authority of its intention to terminate its services in the event of an action for declaring the company bankrupt, declaring the company invalid or otherwise requesting termination or initiating winding-up proceedings. The notification should be made 4 (four) months before the agreed date of termination;

- notify (at least 4 months before) its users of the decision to terminate the services it provides;
- changes the status of their certificates;
- terminate all user certificates within the announced end-of-service period;
- notify all its users of termination of services;
- makes commercial reasonable efforts to minimize distortion of consumer interests;
- pays compensation to consumers (compensation must be proportional to the remaining period of validity of the certificates);
- carries out the necessary action to enable the Supervisory Authority to maintain the CRL.

If the decision to terminate the certification service only concerns the Registration Authority, it shall be obliged to:

- notify Evrotrust about its intention to terminate the registration activity. The notification should be made 4 (four) months before the agreed date of termination;
- transmit to the receiving Provider the complete documentation related to the users, including the archive and the audit data.

5.6.2 TRANSFER OF BUSINESS TO ANOTHER QUALIFIED SERVICE PROVIDER

In order to ensure the continuity of the issuance of qualified authentication services to consumers, Evrotrust may sign an agreement with another qualified certification service provider. In this case, Evrotrust shall:

- notify the Supervisory Authority of its intention no later than 4 months before the date of termination and transfer of the business;
- make every effort and care to continue the validity of issued user certificates;
- notify the Surveillance Authority and Consumers in writing that its activity is being undertaken by another registered supplier as well as its name. The notification shall be published on the Evrotrust

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

website;

- notify Users of the Conditions of Maintenance of Transferred Certificates to the Receiving Provider;
 - modify the status of the operating certificates and duly transmit all documentation relating to its activity to the receiving Provider, together with all records and all certificates issued (valid, suspended and discontinued);
 - perform the necessary actions to transfer the maintenance of the information to the receiving Provider;
 - transfer the management of the already issued end-user certificates to the receiving Provider;
- The Receiving Provider assumes the rights and obligations of Evrotrust with terminated activity and continues to manage the active Qualified Certificates until the end of their operation.

The Evrotrust Archive with terminated status must be delivered to the Provider accepting the activity.

5.6.3 DISQUALIFICATION OF QUALIFIED PROVIDER OR QUALIFIED SERVICE STATUS

In the event of the revocation of the qualified Evrotrust status or of any of its certification services, it shall:

- notify its users of the changed status of its services;
- change the status of their certificates;
- terminates issuance of new qualified certificates but continues to support and maintain the already active certificates until they expire;
- make commercial reasonable efforts to minimize distortion of consumer interests;

6 MANAGEMENT AND CONTROL OF THE TECHNICAL SECURITY

6.1 GENERATING AND INSTALLING A PAIR OF KEYS OF A CERTIFICATION AUTHORITY

Evrotrust generates pairs of cryptographic (RSA) keys on the base and on the Operations Certification Authorities using an HSM/Hardware Security Module at FIPS 140-2 Level 3 or above, or CC EAL 4+ or higher respectively.

Evrotrust uses its private keys only for its business purposes as follows:

- to sign the operating certificates issued to the Certification Authorities on its infrastructure;
- to sign CRLs issued and published;
- to sign all issued and published Advanced Electronic Signature/Seal Certificates to Users.

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

6.1.1 GENERATING PAIR OF KEYS TO SIGNATORY/CREATOR

The Signatory/Creator's keys of a Qualified Certificate for Advanced Electronic Signature/Seal are generated in a secure environment as required by Regulation (EU) No. 910/2014.

The control of the private key is through an access code. The Signatory uses the private key to create a signature/seal by entering the code in the secure environment to create an advanced electronic signature/seal.

When the key pair is generated by the Signatory/Creator, Evrotrust recommends that the latter use an approved environment in the Evrotrust infrastructure to create an advanced electronic signature/seal or equivalent that complies with the requirements of Regulation (EU) No. 910/2014 and is compatible with the Evrotrust infrastructure.

In cases where the pair of keys is generated by the Signatory or the Creator, the latter bears full responsibility for the protection of the private key in order to prevent its compromise, disclosure, modification, loss or unauthorized use. The Signatory/Creator is responsible for omissions or actions by authorized persons who are authorized to generate, keep or store their private keys.

The Signatory/Creator undertakes to use licensed software to work with the environment to create an advanced electronic signature/seal.

6.1.1.1 REQUIREMENTS TO THE ENVIRONMENT FOR CREATION OF UPDATED ELECTRONIC SIGNATURE/SEAL

The environment for the creation of an advanced electronic signature/seal shall ensure, by appropriate technical and procedural means, at least that:

- the confidentiality of electronic signature/seal creation data used for the creation of the electronic signature/seal is reasonably guaranteed;
- the data for creating an electronic signature/seal are practically only once met;
- the electronic signature/seal creation data are sufficiently secured and cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
- the electronic signature creation data may be reliably protected by the legitimate Signatory/Creator of the signature/seal against use by others.

Advanced electronic signature/seal creation environment shall not alter the data to be signed or prevent such data from being presented to the Signatory/Creator prior to signing.

Generating or management of data for creating an electronic signature/seal on behalf of the Signatory/Creator of the electronic signature/seal can only be carried out by Evrotrust.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЩ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

6.1.1.2 Remote generation of a pair of keys

The Creator/Signatory uses specialized software provided by Evrotrust, which implements the process of generating and managing the cryptographic pair of keys.

The generation, use, and storage of the private key has a high level of security that is guaranteed by the environment where it is created. It is securely protected and accessed only by the Signatory/Creator or an authorized representative of the legal entity.

The Creator/Signatory or Authorized Representative of the legal entity generates an electronic application for a Qualified Certificate in PKCS # 10 format and sends it to Evrotrust. According to the recommendations of RFC 2314 - PKCS # 10, ASN.1, the electronic request form contains a DN, a public key and other attributes, all of which are signed with the private key.

When remote generation of the key pair is performed where requested by the Evrotrust mobile application, it is generated in a reliable Evrotrust environment that meets the requirements of the Advanced Electronic Signature Environment Regulation.

6.1.1.3 Delivery of a private key to a user

When the key pair is generated at Evrotrust, the Signatory/Creator or the authorized representative of the legal entity receives the private key and the qualified certificate issued at the supplier's Registration Authority or electronically.

The initial User and Administrative Access Code is provided to the Signatory/Creator or the authorized representative of the legal entity in a stamped, opaque paper envelope or alternative electronic channel.

When remote generation of the key pair takes place, the private key is generated and stored encrypted in a reliable Evrotrust environment. The key encryption is a PIN-code created by the Signatory/Creator, which ensures that only he can be accessed to activate the key.

6.1.2 DELIVERY OF A PUBLIC KEY FROM A VENDOR USER

It is executed only by the Signatory/Creator or an authorized representative of a legal entity in which a pair of keys is generated and who is to deliver its public key to Evrotrust for the purposes of the process of issuing a qualified certificate.

The Signatory/Creator or authorized representative of the legal entity delivers, via the Evrotrust registration authority, the public key of the generated pair of keys, by means of a request in electronic form, whose format is PKCS # 10. The request contains a public key and is signed electronically with the corresponding private key.

The user may submit the electronic application on a medium or electronically to the Registration

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

Authority together with the other documents under the Evrotrust Policy or through the Evrotrust webpage.

The registration authority of Evrotrust must verify the holding of the private key by the Signatory/Creator or the authorized representative of the legal entity and confirm the request for a qualified certificate.

This procedure is not implemented when remote certificates are applied through the Evrotrust mobile application.

6.1.3 KEY LENGTH

The length of a pair of keys for Enhanced Electronic Signature/Seal of a User Generated through the Evrotrust infrastructure is 2048 bits, with an applicable combination of asymmetric and hash algorithms: sha256-with-RSA.

Regardless of where the pair of keys for certificate issuance for advanced electronic signature/seal is generated, the key must be at least 1024 bits long for RSA and DSA algorithms and 160 bit for ECDSA algorithms.

6.1.4 PUBLIC KEY PARAMETERS

The Signatory/Creator or Authorized Representative of the legal entity of a key pair is responsible for verifying the quality of the generated private key parameters. It is required to verify the ability of the key to encrypt and decrypt, including creating an electronic signature and performing a check.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROL

Each User creates and stores a private key using a reliable system for its security. The Certification Authority generates a pair of keys upon request from the User and transmits it to a secured state by notifying him of the rules for storing and protecting his private key.

6.2.1 CONTROLLING OF USE AND STORAGE OF A PRIVATE KEY

The private key of the Signatory/Creator or the authorized representative of the legal entity is only used in a secure environment to create an advanced electronic signature/seal, as required by Regulation (EU) No. 910/2014.

Evrotrust does not in any way store or archive a private key of a User to create an electronic signature/seal, except in the case of remote certification of a qualified certificate through the Evrotrust mobile application. In this case, the private key is generated and stored encrypted in a reliable Evrotrust

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

environment. The key encryption is a PIN-code created by the Signatory/Creator, which ensures that only he can be accessed to activate the key.

6.2.2 PRIVATE KEY STORAGE

Evrotrust does not create copies of users' private keys except in the case of the previous paragraph. If the private key is deleted or lost, the user must replace it and request the issuance of a new qualified certificate.

6.2.3 PRIVATE KEY ACTIVATION METHOD

The private key of the Signatory/Creator or an authorized representative of the legal entity is activated by entering the user code to access where the key is stored securely or using another means of identification with the same or higher security level.

6.2.4 METHOD FOR DISABLING A PRIVATE KEY

A private key of Signatory/Creator or an authorized representative of the legal entity is deactivated by deleting the private key or destroying the environment where it is stored. This will permanently disable the access and use of the private key.

6.2.5 PRIVATE KEY DESTROYING METHOD

The private key of a Qualified User Certificate is destroyed by deleting it from the environment where it is stored or by physical destruction.

6.3 OTHER ASPECTS OF PAIR KEY MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVING

Public Keys of Signatories/Creators or authorized representatives of legal entities are contained in the Qualified Certificates issued to them, which are published in the Public Register of the Evrotrust Web site and stored in a repository.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

6.3.2 PERIOD OF VALIDITY OF QUALIFIED CERTIFICATE AND USE OF KEYS

The period of use of public keys is determined by the value of the field in the certificate describing the validity of the public key. The validity of the certificates and their respective private keys may be curtailed in the event of termination of the certificates.

6.4 ACTIVATION DATA

When the User is personally present at the Registration Authority, the activation data of a private key are primarily used by the operator of the Registration Authority. Users use authentication and control access to their private key.

In cases where the Signatory/Creator or the authorized representative of a legal entity generates a pair of Qualified Certificate Keys, they create and manage the activation data themselves.

6.4.1 GENERATING AND INSTALLING ACTIVATION DATA

Activation data is used during initial issuance of a certificate in an environment to create an advanced electronic signature/seal before generating a pair of keys.

Access codes and environment unblocking to create an advanced electronic signature/seal are provided to the Signatory/Creator or the authorized representative of the legal entity in a stamped, opaque paper envelope or in an electronic form on an alternative channel.

When using a mobile application of Evrotrust, the access code is generated by the Signatory/Creator. The code is not stored by Evrotrust and can only be accessed by the user while the mobile application is activated. To recover the personal code, the Signatory/Creator creates a special crypto-key that is generated by answers to three secret questions asked by the user at the time of registration via the mobile application. The answers to the questions are not kept by Evrotrust.

6.4.2 PROTECTION OF ACTIVATION DATA

The Signatory/Creator or Authorized Representative of the legal entity is required to store and protect from compromising the access codes to the environment to create an advanced electronic signature/seal.

Evrotrust recommends that environment activation data never be stored in the environment itself.

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

6.5 COMPUTER SYSTEMS SECURITY

Evrotrust only uses reliable and secure hardware and software that are part of the Evrotrust computer system.

The computer systems that operate all critical components of the Evrotrust infrastructure are equipped and configured with means of locally protecting software and information data access.

Evrotrust uses procedures to manage the information security of the entire Evrotrust infrastructure in accordance with generally accepted international practice standards.

6.6 LIFE CYCLE SECURITY OF THE TECHNOLOGY SYSTEM

All hardware changes are monitored and registered by authorized Evrotrust staff. When purchasing new technical equipment, it is supplied with the necessary operating procedures and instructions for use.

Supervision of the functionality of the technological system is ensured and it is ensured that it functions properly and in accordance with the delivered manufacturing configuration.

6.7 NETWORK SECURITY

Evrotrust infrastructure utilizes modern technical means of information exchange and protection to ensure the network security of systems against external interventions and threats.

7 PROFILES OF QUALIFIED CERTIFICATES FOR ADVANCED ELECTRONIC SIGNATURES/SEALS

User Qualified Certificates profiles comply with the format described in ITU-T X.509 v.3 standard. A certificate of type X.509 v.3 is a data set that uniquely authenticates the public key to the author of the advanced electronic signature/seal.

7.1 QUALIFIED CERTIFICATE PROFILE FOR THE EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR AES:

Version	V3
Serial number	[serial number]
Signature Algorithm	SHA256RSA

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
	C= (countryName)	Country: Two-letter country code according to ISO 3166
Subject	CN= (commonName)	Usual name: A name chosen by the natural person, with which it is usually presented. When not selected, enter the full name of the natural person.
	G= (givenName)	Forename: Name of natural person according to ID
	S= (surname)	Surname: Surname of the natural person according to ID
	Or	
	2.5.4.65= (pseudonym)	Nickname: Nickname chosen by the natural person
Subject	SERIALNUMBER= (serialNumber)	Identifier of the natural person (ETSI EN 319 412-1 p.5.1.3), for example: - PNOBG-8310257645 for PIN; - PASSBG-12345678 for passport number; - IDCBG-195416023 for an ID card number; - TINBG-123434341 for VAT number. If the person does not wish to enter his/her national identifier, a client number shall be entered, generated by the provider, to identify the natural person if necessary.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

	<p style="text-align: center;">Oⁱ = (OrganizationName)</p>	<p>Legal entity name: Full name under the registration or act of registration of the legal entity with which the natural person is associated.</p>
	<p style="text-align: center;">2.5.4.97ⁱ = (OrganizationIdentifier)</p>	<p>Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example:</p> <ul style="list-style-type: none"> - VARBG-123456789 - VAT; - NTRBG-123456789 - UIC (BULSTAT). <p>Enter the national identifier according to the local law of the legal entity with which the natural person is associated.</p>
	<p style="text-align: center;">E= (e-mailAddress)</p>	<p>E-mail of the natural person</p>
<p>Public Key Type/Length</p>	<p>RSA (2048 Bits)</p>	
<p>Subject Key Identifier</p>	<p>[Calculated value for issued certificate]</p>	
<p>Authority Key Identifier</p>	<p>Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</p>	
<p>CRL Distribution Points</p>	<p>1]CRL Distribution Point</p> <p style="padding-left: 40px;">Distribution Point Name:</p> <p style="padding-left: 80px;">Full Name:</p> <p style="padding-left: 120px;">URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</p>	
<p>Authority Information Access</p>	<p>[1]Authority Info Access</p> <p style="padding-left: 40px;">Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)</p> <p style="padding-left: 40px;">Alternative Name:</p> <p style="padding-left: 80px;">URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt</p> <p>[2]Authority Info Access</p> <p style="padding-left: 40px;">Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)</p> <p style="padding-left: 40px;">Alternative Name:</p> <p style="padding-left: 80px;">URL=http://ca.evrotrust.com/ocsp</p>	
<p>Enhanced Key</p>	<p>Client Authentication (1.3.6.1.5.5.7.3.2)</p>	

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Usage	Secure Email (1.3.6.1.5.5.7.3.4)										
Certificate Policies	<p>[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0</p> <p>[2]Certificate Policy: Policy Identifier=0.4.0.1456.1.2</p> <p>[3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.7</p> <p>[3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps</p>										
Key Usage (critical)	Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)										
QCStatements	<table border="1"> <tr> <td>id-qcs-pkixQCSyntax-v2ⁱ (oid=1.3.6.1.5.5.7.11.2)</td> <td>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId-Legal (oid=0.4.0.194121.1.2)</td> </tr> <tr> <td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td> </tr> <tr> <td>id-etsi-qcs-QcLimitValueⁱⁱ (0.4.0.1862.1.2)</td> <td>[Amount in BGN or EUR]</td> </tr> <tr> <td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td> <td>id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)</td> </tr> <tr> <td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td> <td>PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en</td> </tr> </table>	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱ (0.4.0.1862.1.2)	[Amount in BGN or EUR]	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en
id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)										
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)											
id-etsi-qcs- QcLimitValue ⁱⁱ (0.4.0.1862.1.2)	[Amount in BGN or EUR]										
id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)										
id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en										

7.2 QUALIFIED CERTIFICATE PROFILE FOR EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR AESEAL:

Version	V3
Serial number	[serial number]
Signature Algorithm	SHA256RSA
Issuer	CN= Evrotrust RSA Operational CA
	OU= Qualified Operational CA
	O= Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= NTRBG-203397356
	C= BG

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Valid from	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166
	CN= (commonName)	Legal entity/organisation name:
	O= (organizationName)	Legal entity/organisation name: Full name under the registration or act of registration of the legal entity.
	2.5.4.97= (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 - VAT; - NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity with which the natural person is associated.
	E= (e-mailAddress)	E-mail of the legal entity
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority	1]Authority Info Access	

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Information Access	<p>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)</p> <p>Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt</p> <p>[2]Authority Info Access</p> <p>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)</p> <p>Alternative Name: URL=http://ca.evrotrust.com/ocsp</p>										
Enhanced Key Usage	<p>Client Authentication (1.3.6.1.5.5.7.3.2)</p> <p>Secure Email (1.3.6.1.5.5.7.3.4)</p>										
Certificate Policies	<p>[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1</p> <p>[2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.8</p> <p>[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps</p>										
Key Usage (critical)	Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)										
QCStatements	<table border="1"> <tr> <td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td> <td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td> </tr> <tr> <td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td> </tr> <tr> <td>id-etsi-qcs-QcLimitValueⁱⁱ (0.4.0.1862.1.2)</td> <td>[Amount in BGN or EUR]</td> </tr> <tr> <td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td> <td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td> </tr> <tr> <td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td> <td>PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en</td> </tr> </table>	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱ (0.4.0.1862.1.2)	[Amount in BGN or EUR]	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)										
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)											
id-etsi-qcs- QcLimitValue ⁱⁱ (0.4.0.1862.1.2)	[Amount in BGN or EUR]										
id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)										
id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en										

7.3 EVROTRUST QUALIFIED PSD2 LEGAL PERSON CERTIFICATE FOR AESEAL:

The certificate is issued for the purpose of authenticating a PSD2 related PSP2 website. Used to meet PSD2 requirements. It has the character of a qualified website certificate within the meaning of Regulation (EU) No 910/2014 and is used to create a confident visitor that the website is a real and legitimate subject. Through technology, reliable connectivity is secured through a secure data exchange protocol.

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
	C= (countryName)	Country: Two-letter country code according to ISO 3166
	CN= (commonName)	Legal entity/organisation name:
	O= (organizationName)	Legal entity/organisation name: Full name under the registration or act of registration of the legal entity.
	2.5.4.97= (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 - VAT; - NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity with which the natural person is associated.
	E= (e-mail Address)	E-mail of the legal entity
Public Key Type/Length	RSA (2048 Bits)	

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

Subject Key Identifier	[Calculated value for issued certificate]						
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08						
CRL Distribution Points	<p>1]CRL Distribution Point</p> <p style="padding-left: 40px;">Distribution Point Name:</p> <p style="padding-left: 80px;">Full Name:</p> <p style="padding-left: 80px;">URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</p>						
Authority Information Access	<p>1]Authority Info Access</p> <p style="padding-left: 40px;">Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)</p> <p style="padding-left: 40px;">Alternative Name:</p> <p style="padding-left: 80px;">URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt</p> <p>2]Authority Info Access</p> <p style="padding-left: 40px;">Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)</p> <p style="padding-left: 40px;">Alternative Name:</p> <p style="padding-left: 80px;">URL=http://ca.evrotrust.com/ocsp</p>						
Enhanced Key Usage	<p>Client Authentication (1.3.6.1.5.5.7.3.2)</p> <p>Secure Email (1.3.6.1.5.5.7.3.4)</p>						
Certificate Policies	<p>[1]Certificate Policy:</p> <p style="padding-left: 40px;">Policy Identifier=0.4.0.194112.1.1</p> <p>[2]Certificate Policy:</p> <p style="padding-left: 40px;">Policy Identifier=1.3.6.1.4.1.47272.2.8.1</p> <p>[1,1]Policy Qualifier Info:</p> <p style="padding-left: 40px;">Policy Qualifier Id=CPS</p> <p style="padding-left: 40px;">Qualifier:</p> <p style="padding-left: 80px;">http://www.evrotrust.com/cps</p>						
Key Usage (critical)	Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)						
QCStatements	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 2px;">id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td> <td style="width: 50%; padding: 2px;">id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td> </tr> <tr> <td colspan="2" style="padding: 2px;">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td> </tr> <tr> <td style="padding: 2px;">id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td> <td style="padding: 2px;">id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td> </tr> </table>	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)						
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)							
id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)						

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

	id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en
	id-etsi-psd2-qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAId= NCA abbreviated unique identifier

7.4 PROFILE OF A QUALIFIED EVROTRUST SERVER CERTIFICATE

A qualified server certificate is issued under the same terms as the Qualified certificate for advanced electronic seal for legal person, but it differs according to the type and volume of the information verified in it. It is used to authenticate digital asset of type “server” of the legal person. It is used to identify and sign data on behalf of a server that is under the control of the legal entity.

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
	C= (countryName)	Country: Two-letter country code according to ISO 3166
	CN= (commonName)	Name of the legal entity/organization server
	O = (organizationName)	Name of the legal entity/organization

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

	<p style="text-align: center;">2.5.4.97 = (organizationIdentifier)</p>	<p>Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity with which the natural person is associated.</p>
	<p style="text-align: center;">L= (Locality)</p>	<p>The location where the server of the legal entity is located</p>
<p>Public Key Type/Length</p>	<p>RSA (2048 Bits)</p>	
<p>Subject Key Identifier</p>	<p>[Calculated value for issued certificate]</p>	
<p>Authority Key Identifier</p>	<p>Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</p>	
<p>CRL Distribution Points</p>	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</p>	
<p>Authority Information Access</p>	<p>[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp</p>	
<p>Enhanced Key Usage</p>	<p>Secure Email (1.3.6.1.5.5.7.3.4) Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)</p>	
<p>Subject Alternative Name</p>	<p>DNS Name=[Domain name or IP]</p>	
<p>Certificate Policies</p>	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.6</p>	

	ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	eIDAS-CP-AES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL	Version – 2.4 10.09.2018

	[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
	[2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4	
	[3]Certificate Policy: Policy Identifier=0.4.0.2042.1.7	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	
QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱ (0.4.0.1862.1.2)	[Amount in BGN or EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en

8 VERIFICATION AND CONTROL OF SUPPLIER'S ACTIVITY

The audits carried out at Evrotrust concerns the processing of information data and management of key procedures.

Evrotrust annually performs at least one internal audit.

Evrotrust is audited at least once every 24 months by a Compliance Assessment Body. The purpose of the audit is to confirm that the Qualified Certification Services Provider and the Qualified Certification Services Providers comply with the requirements set out in Regulation (EU) No. 910/2014.

8.1 ACTIONS TAKEN AS A RESULT OF AN AUDIT

Reports of internal and external audits are transmitted to Evrotrust.

The report of the Compliance Assessment Body shall be transmitted to the Supervisory Body within 3 (three) days of its handing over to the Evrotrust management. The Supervisory Authority examines the report and decides whether to leave or take the qualified Evrotrust status.

On the basis of the assessments made in the report, Evrotrust's Guide sets out measures and deadlines for remedying the identified gaps and inconsistencies.

Evrotrust staff undertake specific actions for their removal within the specified deadlines.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 PRICES AND FEES

Evrotrust maintains the document “Pricing for certification, information, cryptographic and consultancy services” on its website: <https://www.evrotrust.com/blanki/tarifa.pdf>.

9.1.1 RETURN OF A CERTIFICATE AND REIMBURSEMENT OF PAYMENT

Signatory/Creator or authorized representative of a legal entity may object to an inaccuracy or incompleteness in the content of a qualified certificate issued within 3 days after its publication in the Public Register.

If the reason for the false content of a qualified certificate is in the Registration Authority, Evrotrust terminates the certificate and issues a new one with true content on its own account or refunds the payment for the revoked certificate with false content.

If the reason for the false content of a qualified certificate is due to the Signatory/Creator or the authorized representative of a legal entity, Evrotrust shall terminate the certificate and shall not reimburse the payment made. Evrotrust may issue a new one with true content at the expense of the User.

The user may refuse to issue a qualified certificate of true content that Evrotrust will terminate immediately without reimbursing the payment for the revoked certificate.

9.2 FINANCIAL RESPONSIBILITIES

Evrotrust is responsible for the certification services provided to the users who rely on the certificates.

Evrotrust shall be liable if the damage is due to his fault or fault of the persons to whom he has assigned the job.

If Evrotrust confirms and accepts that damage has occurred, it undertakes to pay the remedy. The maximum payment limit may not exceed the amount of the damage.

9.2.1 ACTIVITY INSURANCE

Evrotrust undertakes compulsory insurance of its activity as a registered Provider of Qualified Certification Services.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

9.3 PRIVACY OF PERSONAL DATA

Evrotrust is registered as an administrator of personal data under the terms of the Personal Data Protection Act.

As a Personal Data Administrator, Evrotrust strictly observes the requirements of confidentiality and non-dissemination of the personal data of Signatory/Creator or authorized representatives of legal entities that have become known to it in its capacity of Qualified Certification Services Provider.

9.4 INTELLECTUAL PROPERTY RIGHTS

Various data included in the Evrotrust qualified certificates or published in the Public Register/Repository are subject to intellectual property rights and other proprietary and non-material rights.

9.4.1 OWNERSHIP OF A PAIR OF KEYS

The user key pair and the associated public key certificate issued by Evrotrust, as well as the relevant secret material, are owned by Evrotrust, regardless of the ownership of the physical environment in which the keys are stored and protected.

9.5 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST

Evrotrust ensures that it carries out its activities as:

- strictly complies with the terms of this document, the requirements of Regulation (EU) No. 910/2014 and the national legislation in the performance of its activity as Qualified Certification Services Provider;
- the services provided do not infringe the copyrights and licensed rights of third parties;
- uses technical equipment and Technologies that ensure system reliability and technical and cryptographic security in the process, including a secure and secure mechanism/environment for generating keys and for creating an advanced electronic signature/seal in its infrastructure;
- issues qualified certificates for electronic signatures/seal after verifying the information provided by law;
- securely stores and maintains information related to the certificates issued and the systems operation;
- complies with the established operating procedures and technical and physical control rules, in accordance with the terms of this Policy and “Practice in Providing Qualified Certification Services”;
- creates an opportunity for immediate suspension and termination of a qualified certificate;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

- terminates and suspends the performance of certificates under the terms and conditions of the relevant Policy;
- immediately informs the interested parties after the suspension of a qualified certificate;
- provides conditions for accurately determining the timing of issuance, suspension, resumption and termination of Qualified Certificates;
- performs procedures for identification and authentication of the Signatory/Creator or the authorized representative of a legal entity;
- provides measures against tampering with qualified certificates and the confidentiality of the data accessed in the process of creating the advanced electronic signature/seal;
- uses reliable systems for storing and managing certificates;
- only duly empowered employees have access to make changes to the data, establish the authenticity and validity of the certificates;
- takes immediate action in the event of technical security issues;
- upon expiration of the validity of a qualified certificate, cancels its validity;
- informs the Signatories/Creators or authorized representatives of legal entities as well as the Relying Parties about their obligations and due diligence in the use and trust of the qualified certification services provided by Evrotrust as well as the correct and safe use of the issued Qualified Certificates and the Certification Related services;
- uses and stores the collected personal and other information solely for the purposes of its activity of providing qualified certification services in accordance with national law;
- does not store or copy data to create custom private keys except for remotely requesting Qualified Certificates through the Evrotrust mobile application;
- maintains disposable means that enable it to carry out its activities;
- concludes insurance policy for the time of its activity;
- maintains trusted staff with the necessary expertise, experience and qualification to perform the activity;
- maintains a public register/repository in which it publishes the issued Qualified Certificates, a current CRL, other circumstances and electronic documents under this Policy and national legislation;
- provides permanent access to the Public Register electronically (24/7/365);
- provides protection against making changes to the maintained Public Register from unauthorized or unauthorized access or due to a random event;
- immediately publishes in the Public Register the certificates issued and signed;
- creates the conditions for each relying party to verify the status of issued and published qualified certificate in the Public Register of Certificates;
- performs periodic internal audits of the activity of the Certifying Authority and the Registration Authority;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

- performs external audits by independent auditors and publishes the results of the audit on its site;
- uses certified software and hardware in its business as well as secure and reliable technology systems;
- maintains on the Evrotrust website a list of Registration Authorities, a list of recommended software and user hardware, forms, Forms, Types of Contract and other documents for the benefit of users;

Evrotrust is liable to Users and Trustees for damages caused by gross negligence or intent:

- by failure to meet the requirements of Regulation (EU) No. 910/2014 in the performance of its activity of providing qualified certification services;
 - from false or missing data in the Qualified Certificate at the time of issue;
 - from damages caused if, during the issuance of the Qualified Certificate, the person named as Signatory/Creator or authorized representative of a legal entity did not have the private key corresponding to the public key;
 - from algorithmic discrepancy between the private key and the public key entered in the Qualified Certificate;
 - from non-compliance with its obligations to issue and manage qualified certificates;
 - From omissions in establishing the identity of the Signatory/Creator or the authorized representative of a legal entity.

9.5.1 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF THE REGISTRATION AUTHORITY

Evrotrust ensures that the Registration Authority performs its functions and duties in full compliance with the terms of this document, the requirements and procedures in the Policy and the issued internal operational instructions.

Evrotrust is responsible for the actions of the Registration Authority in the Evrotrust infrastructure.

Evrotrust ensures that the Registration Authority:

- performs its business using reliable and secure devices and software;
- provides services that are in accordance with national law and does not infringe the copyrights and licensed rights of Users;
 - makes the necessary efforts to perform correct User identification, correctly and accurately inputs the data in the Evrotrust database and updates this information at the time of validation of the data;
 - does not make any deliberate mistakes or misinterpret the information contained in Qualified Certificates;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЩ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

➤ its services comply with generally accepted standards: X.509, PKCS # 10, PKCS # 7, PKCS # 12.

9.6 OBLIGATIONS OF USERS

The Signatory/Creator or authorized representative of a legal person specified in the issued qualified certificate as Signatory has the following obligations:

➤ to become aware with and comply with the terms of the Contract, the Policies and Practices in the provision of qualified certification services by Evrotrust, as well as the requirements in the other documents published in the Public Register of Evrotrust;

➤ when submitting requests for the issuance and management of qualified certificates, to provide true, accurate and complete information that Evrotrust requires under the Contract, the regulatory requirements, the applicable Policies and Practices;

➤ to generate cryptographic keys using a secure method and algorithm in accordance with the requirements of Regulation (EU) No 910/2014 and to use a secure environment for creating an advanced electronic signature/seal;

➤ to verify the completeness and authenticity of the content of the authentication information provided by it in the Distinguished Name (DN) field of the Qualified Certificates issued. In case of a discrepancy between the submitted information and the certified content, the user must immediately notify Evrotrust;

➤ to discontinue the use of a qualified certificate in the event of any doubt about the loss or compromise of the private key and to file an application for termination with Evrotrust;

➤ to discontinue the use of a qualified certificate in the presence of obsolete, altered, inaccurate and / or incorrect information in it and to file a request for suspension of the certificate;

➤ to apply due diligence and to take the necessary measures to prevent the private key from compromising, loss, disclosure, modification or other unauthorized action;

➤ to use the qualified certificate issued by Evrotrust for legitimate purposes only and in accordance with the policy and practice specified therein;

➤ to approve the conditions specified in the Agreement between him and Evrotrust (this approval must be a handwritten signature on the Contract);

➤ to approve the qualified certificate issued to him/her;

➤ not to disclose the password to access the environment to create an advanced electronic signature/seal to unauthorized persons;

➤ not make his/her private key available to others.

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАЩ ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

9.7 DISCLAIMER

Evrotrust is not responsible for any damages caused by:

- use of a qualified certificate outside the limits of the intended purposes and limitations of its validity;
- Illegal actions by Consumers and Leading Parties;
- providing method for identification of the environment for creating advanced electronic signature/seal and private key access by Third Party Users;
- incidental events of a force majeure, including malicious actions of third parties (hacker attacks, removal of the environment for creating an advanced electronic signature/seal, access to the private key, knowing without the Signatory/Creator of the identification method, etc.)
- use of a qualified certificate that has not been issued or used in accordance with the requirements and procedures of Evrotrust's Practice and Policy;
- use of an invalid certificate (certificate that has been suspended or terminated);
- not timely action to terminate or suspend a certificate (due to a delay by the Signatory/Creator's request or for reasons beyond the control of Evrotrust);
- compromised private key corresponding to the public key in the qualified certificate by fault of the Signatory/Creator;
- poor quality and functionality of the software products and hardware devices used by Signatory/Creator and Relying parties.
- Evrotrust is not responsible for using the certificate beyond the limits of the transaction value limits and usage goals.
- EUROTRAST is not responsible for the attachment contents. All the risks that may occur when downloading the attachments are responsibility of the users who exchange them.

9.8 SIGNATORY'S/CREATOR'S RESPONSIBILITY

The responsibility of the Signatory/Creator or the authorized representative of a legal entity results from the performance of his/her duties. The terms of liability are governed by a Contract with Evrotrust.

The Signatory/Creator or Authorized Representative of a Legal Person is liable to Evrotrust and to the Relying parties if:

- in creating the private-public key pair used an algorithm and environment to create an advanced electronic signature/seal that does not comply with the requirements of Regulation (EU) No. 910/2014;
- does not exactly comply with the security requirements set by Evrotrust;
- does not request Evrotrust to suspend or terminate the Qualified Certificate after learning that the private key has been misused or threatened by improper use;

	<p style="text-align: center;">ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ</p>	<p style="text-align: center;">eIDAS-CP-AES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL</p>	<p style="text-align: center;">Version – 2.4 10.09.2018</p>

- has made false statements made to Evrotrust relating to the content or issuance of the Qualified Certificate;
- when the qualified certificate is issued with a registered Creator and his authorized person (Signatory), he is responsible for the failure of the authorized person to fulfil his obligations.

Subscriber, Titular/Creator or the representative of the legal entity is responsible for the content of the attachments and the consequences of their use.

ⁱ If there are no included attributes for **organizationName** and **organizationIdentifier** the attribute **id-etsi-qcs-SemanticsId-Legal** is also not included.

ⁱⁱ If the attribute **id-etsi-qcs-QcLimitValue** is included in the certificate it specifies the limitation on the value of transaction for which this certificate can be used to.