

**ПОЛИТИКА И ПРАКТИКА
ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА
ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА**

СЪДЪРЖАНИЕ

1	ВЪВЕДЕНИЕ.....	5
1.1	ПРЕГЛЕД.....	5
1.1.1	НОРМАТИВНИ ПОЗОВАВАНИЯ.....	6
1.2	ИМЕ И ИДЕНТИФИКАТОР НА ДОКУМЕНТА.....	7
1.3	УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА.....	8
1.3.1	УДОСТОВЕРЯВАЩИ ОРГАНИ.....	8
1.3.2	РЕГИСТРИРАЩ ОРГАН.....	9
1.3.3	ПОТРЕБИТЕЛИ.....	10
1.3.4	ДОВЕРЯВАЩИ СЕ СТРАНИ.....	10
1.3.5	ДРУГИ УЧАСТНИЦИ.....	10
1.4	ПРИЛОЖЕНИЕ НА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА.....	10
1.5	УПРАВЛЕНИЕ НА ПОЛИТИКАТА И ПРАКТИКАТА.....	11
1.5.1	ОРГАНИЗАЦИЯ, УПРАВЛЯВАЩА ПОЛИТИКАТА.....	11
1.5.2	ЛИЦЕ ЗА КОНТАКТ.....	11
1.6	ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ.....	11
1.6.1	ОПРЕДЕЛЕНИЯ.....	11
1.6.2	СЪКРАЩЕНИЯ.....	13
2	ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И СЪХРАНЕНИЕ.....	13
3	ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ.....	14
3.1	ИМЕНА.....	14
3.2	ПЪРВОНАЧАЛНА ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ.....	14
3.2.1	УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ.....	15
3.2.2	УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ.....	17
3.2.3	УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ.....	18
3.3	АВТЕНТИФИКАЦИЯ.....	19
4	ПРОЦЕС НА ПРЕДОСТАВЯНЕ НА УСЛУГАТА.....	19
4.1	ИЗИСКВАНИЯ КЪМ КВАЛИФИЦИРАНАТА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА.....	20
4.2	ОПИСАНИЕ НА ТЕХНОЛОГИЯТА.....	22
4.3	СХЕМИ НА ПРОЦЕСА НА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА.....	23
4.4	ПРОЦЕС НА ПРЕДОСТАВЯНЕ НА УСЛУГАТА.....	25
4.5	ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ/ПОЛУЧАТЕЛ.....	27
4.5.1	ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ.....	27
4.5.2	ИДЕНТИФИКАЦИЯ НА ПОЛУЧАТЕЛ.....	28
4.6	СЪЗДАВАНЕ НА ДОКАЗАТЕЛСТВА.....	29
4.6.1	ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ИЗПРАЩАЧА (S-ERDS).....	29
4.6.2	ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ПОЛУЧАТЕЛЯ (R-ERDS).....	30
4.6.3	ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ПРЕДАВАНЕТО НА ПОТРЕБИТЕЛСКО СЪДЪРЖАНИЕ НА ПОЛУЧАТЕЛЯ.....	31
4.7	ЗАЩИТА НА ПРЕДАВАНИТЕ ДАННИ СРЕЩУ РИСК ОТ ЗАГУБА, КРАЖБА, ПОВРЕДА ИЛИ НЕПОЗВОЛЕНИ ИЗМЕНЕНИЯ.....	32
4.8	КРАЙ НА АБОНАМЕНТА НА УСЛУГАТА.....	32
4.9	ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ).....	33
5	КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ.....	33

5.1	ФИЗИЧЕСКИ КОНТРОЛИ ЗА СИГУРНОСТ	33
5.1.1	ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА.....	34
5.1.2	ФИЗИЧЕСКИ ДОСТЪП.....	34
5.1.3	КОНТРОЛ НА ДОСТЪПА	34
5.2	УПРАВЛЕНИЕ НА ИНЦИДЕНТИ	35
5.3	КОНТРОЛ НА ПЕРСОНАЛА	36
5.4	ПРОЦЕДУРА ЗА ОДИТ	36
5.5	АРХИВИРАНЕ	37
5.5.1	СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ	38
5.5.2	ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИ.....	39
5.5.3	УПРАВЛЕНИЕ НА АКТИВИ	39
5.5.4	ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ	40
5.6	СМЯНА НА КЛЮЧОВЕ.....	41
5.7	КОМПРОМИТИРАНЕ И ВЪЗСТАНОВЯВАНЕ ПРИ БЕДСТВИЯ.....	42
5.7.1	ПЛАН ЗА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА.....	42
5.8	ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА УДОСТОВЕРЯВАЩ ОРГАН	44
6	КОНТРОЛИ НА ТЕХНИЧЕСКА СИГУРНОСТ	45
6.1	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА КЛЮЧОВИ ДВОЙКИ	45
6.2	ЗАЩИТА НА ЧАСТНИ КЛЮЧОВЕ И НА КРИПТОГРАФСКИЯ МОДУЛ.....	45
6.3	ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА КЛЮЧОВИТЕ ДВОЙКИ	45
6.4	ДАННИ ЗА АКТИВИРАНЕ.....	46
6.5	КОМПЮТЪРНА СИГУРНОСТ	46
6.6	СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА.....	46
6.6.1	ОЦЕНКА НА УЯЗВИМОСТТА НА ИНФОРМАЦИОННАТА СИСТЕМА	46
6.7	МРЕЖОВА СИГУРНОСТ	47
7	ПРОФИЛИ НА УДОСТОВЕРЕНИЯ, CRL И OCSP	47
7.1	ПРОФИЛ НА БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT“	47
7.2	ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES CA“	47
7.3	ПРОФИЛ НА УСЛУГА ЗА ВАЛИДИРАНЕ НА СТАТУС НА УДОСТОВЕРЕНИЯ „EVROTRUST SERVICES OCSP“	49
7.4	ПРОФИЛ НА CRL НА „EVROTRUST SERVICES CA“	50
7.5	ПРОФИЛ НА „EVROTRUST QERDS SU“	51
8	ОДИТ НА СЪОТВЕТСТВИЕТО И ДРУГА ОЦЕНКА	52
8.1	ЗАСТРАХОВКА	52
9	ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ.....	53
9.1	ЦЕНИ.....	53
9.2	ФИНАНСОВА ОТГОВОРНОСТ	53
9.3	НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ.....	53
9.4	ПРАВАТА НА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ.....	54
9.5	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ.....	55
9.5.1	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТРЪСТ	55
9.5.2	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН	57
9.5.3	ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ (ИЗПРАЩАЧИ И ПОЛУЧАТЕЛИ)	57
9.5.4	ДЪЛЖИМА ГРИЖА НА ДОВЕРЯВАЩА СЕ СТРАНА	58
9.6	ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ.....	58
9.7	ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА	58
9.8	СРОК И ПРЕКРАТЯВАНЕ НА ПОЛИТИКАТА И ПРАКТИКАТА.....	58

9.9	ИНДИВИДУАЛНИ СЪОБЩЕНИЯ И СЪОБЩЕНИЯ С УЧАСТНИЦИТЕ	59
9.10	ИЗМЕНЕНИЯ НА ПОЛИКИТА И ПРАКТИКАТА.....	59
9.11	РАЗРЕШАВАНЕ НА СПОРОВЕ	60
9.12	ПРИЛОЖИМО ПРАВО.....	60
9.13	СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО	60
9.14	ОБЩИ РАЗПОРЕДБИ.....	61
9.15	ДРУГИ РАЗПОРЕДБИ.....	61

1 ВЪВЕДЕНИЕ

„Евротръст Технолъджис“ АД (Евротръст) е квалифициран доставчик на удостоверителни услуги, осъществяващ дейност съгласно изискванията на Регламент (ЕС) № 910/2014 г. на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (Регламент (ЕС) № 910/2014 г.) и Закона за електронния документ и електронните удостоверителни услуги и като такъв той е вписан в доверителния списък на европейските доставчици на удостоверителни услуги (<https://webgate.ec.europa.eu/tl-browser/#/tl/BG>), както и в регистъра на българските доставчици на удостоверителни услуги, поддържан от Комисията за регулиране на съобщенията (<https://crc.bg/bg/statii/1653/doveritelen-spisyk-trusted-list>).

Евротръст предоставя на своите потребители високо надеждна и сигурна квалифицирана услуга за електронна препоръчана поща в съответствие с Регламент (ЕС) № 910/2014 г.

1.1 ПРЕГЛЕД

„Политика и практика при предоставяне на квалифицирана услуга за електронна препоръчана поща“ (Политика и практика) е документ, който описва общите правила и норми, прилагани от „Евротръст Технолъджис“ АД (Евротръст) при предоставяне на квалифицирана услуга за електронна препоръчана поща (QERDS). Документът се отнася за удостоверителна услуга на Евротръст, съгласно раздел 7 от Регламент (ЕС) № 910/2014 г., и в съответствие с приложимото законодателство в Република България.

Настоящият документ определя общо приложимите изисквания към дейността на Евротръст в качеството му на квалифициран доставчик на електронна препоръчана поща (QERDSP). Политиката урежда разпоредбите, отнасящи се до персонала на дружеството (компетенции, отговорности, оправомощаване и задължения в зависимост от ролята, която има всеки един служител).

Квалифицираната услуга за електронна препоръчана поща (QERDS) е специфичен тип ERDS (услуга за препоръчана поща). При QERDS както услугата, така и доставчикът, който я

предоставя отговарят на определен брой допълнителни изисквания, на които не е необходимо да отговарят доставчиците на обикновената ERDS. QERDS позволява изпращане и/или получаване на потребителско съдържание (електронни документи) и сигурно, и дългосрочно съхраняване на доказателствата за този процес. Тази услуга е удобен инструмент за бърза и надеждна доставка на информация. Евротръст осигурява сигурност и защитеност на комуникацията с удостоверяване на времето на изпращане на документи и съобщения от изпращача и удостоверяване на времето на получаване на документи и съобщения от получателя, както и доказателства за комуникацията, които гарантират автентичност на обменените документи. Евротръст осигурява сигурна първоначална идентификация на получателя и изпращача и защита срещу загуба, кражба, повреда или неразрешена промяна на предаваните данни, с което гарантира целостта на съобщенията.

Услугата е предназначена за физически и юридически лица, за администрации, за лица, осъществяващи публични функции и за организации, предоставящи обществени услуги.

Запознаването с целите и ролята на Политиката и практиката е особено важно за потребителите на Евротръст от гледна точка на приложимостта на тази услуга.

Отношенията между Евротръст и потребителите се уреждат с „Договор за използване на услугите достъпен чрез приложението на „Евротръст Технолъджис“ АД.

Настоящият документ е в съответствие със стандарта с ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.

Настоящият документ е публичен. Той може да бъде променян по всяко време от Евротръст, като всяка нова редакция се одобрява от Борда на директорите и се съобщава на заинтересованите лица чрез сайта на дружеството в интернет.

Настоящият документ е неразделна част от политиките и практиките за предоставяне на квалифицирани услуги на Евротръст.

1.1.1 НОРМАТИВНИ ПОЗОВАВАНИЯ

Политиката е съобразена със следните документи:

➤ 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;

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1: Framework and Architecture;
- ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents;
- ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats;
- ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1: Message delivery bindings;
- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2: Evidence and identification bindings;
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-3 Capability and requirements bindings.

1.2 ИМЕ И ИДЕНТИФИКАТОР НА ДОКУМЕНТА

Настоящият документ е с пълно наименование „Политика и практика при предоставяне на квалифицирана услуга за електронна препоръчана поща“ от „Евротръст Технолъджис“ АД и идентификатор:

Наименование на политика	Идентификатор на обект (OID)
QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE POLICY AND PRACTICE	1.3.6.1.4.1.47272.2.10.1

Евротръст гарантира, че не променя обектния идентификатор на настоящия документ, както и обектните идентификатори на политиките, практиките и другите рефериращи документи. Ако има разширяване/промяна в политиката и практиката, която не засяга вече издадени удостоверения, Евротръст презентира нов обектен идентификатор, който описва новите удостоверения или разширените/променените такива. Евротръст следва вътрешна процедура за управление на OID.

1.3 УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА

1.3.1 УДОСТОВЕРЯВАЩИ ОРГАНИ

1.3.1.1 БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН („EVROTRUST RSA ROOT CA“)

Evrotrust RSA Root CA издава квалифицирани електронни удостоверения, които са йерархично зависими в инфраструктурно отношение в домейна на Евротръст. Базовото удостоверение на Евротръст е самоиздадено и самоподписано с базовия частен ключ на Евротръст. С базовия частен ключ доставчикът подписва удостоверения за публични ключове на свои оперативни Удостоверяващи органи.

1.3.1.2 ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН “EVROTRUST SERVICES CA”

„Evrotrust Services CA“ е удостоверяващ орган на квалифицираната услуга за електронна препоръчана поща, който чрез използване на модул за подписване/signing unit „Evrotrust QERDS SU“ електронно подписва доказателствата, които се издават съгласно настоящата политика.

1.3.1.3 ОРГАН ЗА ПРОВЕРКА НА СТАТУС НА УДОСТОВЕРЕНИЯ „EVROTRUST SERVICES OCSP“

„Evrotrust Services OCSP“ е валидиращ орган на удостоверяващия орган на квалифицираната услуга за електронна препоръчана поща, който подписва удостоверенията за статус на издаваните от „Evrotrust Services CA“ удостоверения. Услугата за проверка на статус се достъпва посредством OCSP протокол.

1.3.1.4 ОРГАН ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ („EVROTRUST TSA“)

„Evrotrust TSA“ е удостоверяващ орган в структурата на Евротръст, който предоставя квалифицирана услуга за удостоверяване на време TSS. „Evrotrust TSA“ приема заявки за издаване на квалифицирани електронни времеви печати за удостоверяване на точно време в генерираните доказателства.

Детайлно описание има в документа „Политика и практика на услуга за предоставяне на квалифицирани електронни времеви печати“.

1.3.2 РЕГИСТРИРАЩ ОРГАН

Потребителите на Евротръст първоначално се идентифицират през надеждна, сигурна и сертифицирана инфраструктура. Схемата за електронна видео идентификация на физически и юридически лица през мобилно устройство отговаря на изискванията на Регламент (ЕС) № 910/2014 г.

Регистриращият орган е обособена структура на Евротръст, но може да бъде и външно лице, на което Евротръст възлага осъществяване на услуги по проверка на регистрацията, идентификацията и удостоверяването на самоличността и идентичността на потребителите на QERDS.

Информация за контакт с Регистриращия орган на Евротръст е на разположение на интернет сайта на дружеството (e-mail: office@evrotrust.com, тел.: 02 448 58 58).

1.3.3 ПОТРЕБИТЕЛИ

Всяко физическо или юридическо лице, което има сключен договор с Евротръст за квалифицирана услуга за електронна препоръчана поща е потребител на QERDS. Потребителите може да използват квалифицираната услугата за препоръчана поща (електронна доставка/връчване) в ролята на изпращач и/или на получател.

Когато това е практически осъществимо, предоставяната удостоверителна услуга и използваните при предоставянето на QERDS продукти са достъпни и за хора с увреждания.

1.3.4 ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяващите се страни (трети страни) са физически или юридически лица, които разчитат на доказателствата предоставени от доставчика във връзка с QERDS. В конкретния случай те не са потребители на QERDS.

1.3.5 ДРУГИ УЧАСТНИЦИ

Евротръст запазва право при необходимост да сключва договори с външни лица за предоставяне на определени удостоверителни услуги.

1.4 ПРИЛОЖЕНИЕ НА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

QERDS се използва за изпращане и получаване на потребителско съдържание. Поради широко обхватния диапазон на приложение на услугата се забранява предоставянето ѝ в нарушение с разпоредбите на приложимите регламенти, стандарти и препоръки или извън обхвата на разрешена употреба, определена в настоящия документ. Електронната препоръчана поща не трябва да се използва по начин, несъвместим с обявената за нея цел, нейното приложно поле/Политика и за незаконосъобразни цели

Предоставяните продукти и услуги от Евротръст за крайни потребители са достъпни и за хората с увреждания.

1.5 УПРАВЛЕНИЕ НА ПОЛИТИКАТА И ПРАКТИКАТА

1.5.1 ОРГАНИЗАЦИЯ, УПРАВЛЯВАЩА ПОЛИТИКАТА

Евротръст отговаря за управлението на настоящата Политика и практика.

Всяка версия на Политиката и практиката е в сила до момента на одобрение и публикуване на нова версия. Всяка нова версия се разработва от служители на Евротръст и след одобрение от Борда на директорите на Евротръст се публикува.

Потребителите са длъжни да се съобразяват само с валидната версия на Политика и практика към момента на ползване на услугите на Евротръст.

1.5.2 ЛИЦЕ ЗА КОНТАКТ

Контактното лице за управление на документа „Политика и практика при предоставяне на квалифицирана услуга за електронна препоръчана поща от „Евротръст Технолъджис“ АД“ е изпълнителния директор на Евротръст.

Допълнителна информация може да бъде получена на следния адрес:

„Евротръст Технолъджис“ АД

1766 София, бул. „Околовръстен път“ № 251 Г

„ММ Бизнес център“, ет. 5

телефон за контакт: + 359 2 971 44 61 – информация/регистрация орган/техническа поддръжка

интернет страница: <http://www.evrotrust.com>

адрес на електронна поща: info@evrotrust.com

1.6 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

1.6.1 ОПРЕДЕЛЕНИЯ

Услуга за електронна препоръчана поща (Electronic Registered Delivery Service/ERDS) - услуга, която позволява предаването на данни между лица по електронен път, предоставя доказателство във връзка с обработката на предаваните данни, включително доказателство

за изпращането и получаването на данните, и защитава предаваните данни срещу риск от загуба, кражба, повреда или непозволенни изменения;

Квалифицирана услуга за електронна препоръчана поща (Qualified Electronic Registered Delivery Service/QERDS) - услуга за електронна препоръчана поща, която отговаря на изискванията, предвидени в член 44 на Регламент (ЕС) № 910/2014 г.;

Доставчик на услуга за електронна препоръчана поща - доставчик на квалифицирани удостоверителни услуги, който предоставя услуга за електронна препоръчана поща;

Квалифициран доставчик на квалифицирана услуга за електронна препоръчана поща (Qualified Electronic Registered Delivery Service Provider/ QERDSP) - квалифициран доставчик на квалифицирани удостоверителни услуги, който предоставя квалифицирана услуга за електронна препоръчана поща, в съответствие с Регламент (ЕС) № 910/2014 г.;

ERDS доказателства - данни, генерирани в рамките на услуга за електронна препоръчана поща, които имат за цел да докажат, че в даден момент е настъпило определено събитие;

Потребителско съдържание - оригинални данни, създадени от изпращача, които трябва да бъдат доставени на получателя;

Потребителски агент (UA/User Agent) - програми (приложения), през които изпращача и получателя комуникират със системата за електронна препоръчана поща;

Получател (Recipient) - физическо или юридическо лице, до което се адресира потребителско съдържание;

Изпращач (Sender) - физическо или юридическо лице, което предоставя потребителско съдържание;

Доставка (Consignment) - когато доставката на потребителско съдържание е пресякла

границата на електронната препоръчана поща, т.е. вече е на разположение на получателя;

Връчване (Handover) – когато потребителското съдържание успешно пресече границата на електронната препоръчана поща на получателя, т.е. към потребителския агент/приложението на ERD на получателя;

Оригинално съобщение (original message) – потребителско съдържание и метаданни за изпращане;

Пратка – изпратено/получено съдържание (документ/и).

1.6.2 СЪКРАЩЕНИЯ

ЗЕДЕУУ – Закон за електронния документ и електронните удостоверителни услуги;

КДУУ – Квалифициран доставчик на удостоверителни услуги;

ERD – електронна препоръчана поща;

ERDS – Услуга за електронна препоръчана поща;

QERDS – Квалифицирана услуга за електронна препоръчана поща;

ERDSP – Доставчик на услуга за електронна препоръчана поща;

QERDSP – Квалифициран доставчик на услуга за електронна препоръчана поща;

UA – потребителски агент, който изпращача/получателя използват, за да изпратят/получат потребителското съдържание;

R-ERDS – системата за квалифицирана услуга за електронна препоръчана поща на получателя;

S-ERDS – системата за квалифицирана услуга за електронна препоръчана поща на изпращача.

2 ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И СЪХРАНЕНИЕ

Публичният регистър е достъпен на адрес: <https://www.evrottrust.com/>.

Евротръст публикува на уебсайта си съобщения, свързани с неговата дейност и

всички важни документи от интерес за потребителите и доверяващите се страни.

Потребителите и доверяващите се страни се информират, относно Политиката и практиката и Общите условия за предоставяне на услугата за електронна препоръчана поща преди сключване на договор. Документацията, включваща Политика и практика, споразумения, образци, доклади от одити и др. се публикува на страницата на Евротръст в интернет незабавно при всяка актуализация. Оперативните удостоверения на удостоверяващия орган се публикуват незабавно при всяко издаване на нови удостоверения.

Евротръст предлага услуги, свързани с достъпа до информацията съхранявана в хранилището (публичния регистър), като осигурява HTTP/HTTPS базиран достъп до нея. Информацията, публикувана в хранилището на Евротръст, е достъпна постоянно (24/7/365), освен в случаите на събития, извън контрола на Евротръст.

3 ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ

3.1 ИМЕНА

Изискванията, които Евротръст прилага относно видовете имена са описани в т.3.1 от документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

3.2 ПЪРВОНАЧАЛНА ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ

Системата на Евротръст за QERDS позволява да се изпращат потребителски съобщения и прикачени документи/файлове (потребителско съдържание) като пратки. Разликата с обикновената електронна доставка се състои в това, че изпращачът и получателят трябва първо да преминат през процес на първоначална идентификация, преди да използват системата. В процеса на обслужване, изпращачът на електронни документи се автентифицира и едва тогава изпраща пратката, респективно получателя има достъп до съдържанието ѝ след като също се е автентифицирал.

Евротръст проверява самоличност/идентичност на изпращача и получателя пряко или чрез трета страна:

- а) дистанционно, използвайки средства за електронно идентифициране, което е

равносилно на физическото присъствие на физическото или юридическо лице. Средствата за електронно идентифициране отговарят на изискванията, посочени в член 8 от Регламент (ЕС) № 910/2014 по отношение на нивата на сигурност „значителни“ или „високи“.

За идентификация на клиентите Евротръст използва система за отдалечена видео идентификация, през мобилно устройство, която дава право на доставчика първоначално да идентифицира и да провери отдалечено самоличността/идентичността на едно лице. При тази система доставчика си комуникира с националните първични регистри (гражданска регистрация, лични документи, регистри на юридически лица и др.). След проверка на предоставената и проверена информация се създават данни за самоличността/идентичността на лицата, които данни се запазват в хранилището на Евротръст за срок от 10 години, включително и след преустановяване на дейността си. Евротръст изпълнява изискванията по чл. 24 от Регламент (ЕС) № 910/2014 като съхранява цялата имаща отношение информация с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата, срокът от 10 години е определен в съответствие с чл. 21(3) от Закона за електронния документ и електронните удостоверителни услуги.

б) при невъзможност за отдалечена идентификация Евротръст допуска физическото присъствие на физическото лице, негов упълномощен представител или на упълномощен представител на юридическото лице при Регистриращ орган на Евротръст.

3.2.1 УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ

Установяване и първоначална проверка на самоличността на физическо лице се осъществява автоматизирано чрез отдалечена проверка и/или от Регистриращ орган.

Минималният набор от данни за физическо лице трябва да съдържа изброените по-долу специфични данни:

а) фамилно име (или имена);

б) собствено име (или имена);

в) дата на раждане;

г) национален уникален идентификатор, ако има такъв, в съответствие с техническите спецификации за целите на трансграничната идентификация, който да остава непроменен,

колкото е възможно по-дълго време. За Република България това е единния граждански номер (ЕГН).

Минималният набор от данни за физическо лице може да съдържа и допълнителни специфични данни:

- а) собствено име (или имена) и фамилно име (или имена) по рождение;
- б) място на раждане;
- в) постоянен адрес;
- г) други данни.

За автоматизирано установяване и първоначална проверка на самоличността на физическо лице, чрез отдалечена проверка, е необходимо следното:

- изисква се физическото лице да е инсталирало мобилното приложение на Евротръст и да е иницирирало процес по регистрация и отдалечена електронна идентификация през мобилно устройство за нуждите на сключване на договор за удостоверителни услуги с Евротръст;
- лицето трябва да е сканирало с камерата на мобилно/смарт (смартфон, таблет) устройство валиден документ за самоличност;
- Евротръст иницирира процедура по проверка на валидността на документа за самоличност чрез национална база данни с документи за самоличност (при наличие на съответна интеграция) или използва услуга за проверката им;
- осъществява се процедура по автоматизиран анализ на биометрията на лицето чрез поредица от контроли, целящи да установят идентичност на лицето със снетата снимка, получена от достоверен източник, включително чрез проверки за 3D обект (в съответствие със сертифицирана методология);
- при неуспешна автоматизирана проверка се преминава към идентификация чрез видео конферентна връзка с оператор на Евротръст, съобразно сертифицирана методология за проверка на знание на определени лични данни и визуална идентификация на лицето спрямо снетите документи и получени данни от първични регистри;
- при успешна проверка на лицето, то подписва Договор за използване на услугите, достъпни чрез приложението на „Евротръст Технолъджис“ АД. При неуспешна проверка се указва на лицето да посети офис на Евротръст или негов Регистриращ орган за лично

явяване и персонална идентификация.

Евротръст извършва проверка на достоверността на информацията с всички законово позволени средства в съответните публични регистри.

3.2.2 УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ

Установяването на първоначална идентичност на юридическо лице, се осъществява от представител на Регистриращия орган, чрез автоматизирана проверка в първични регистри (Например: Търговски регистър), проверка в съответните регистри по предоставен национален идентификатор и/или други данни.

Минималният набор от данни за юридическо лице трябва да съдържа изброените по-долу специфични данни:

а) наименование на юридическото лице (фирма);

б) уникален национален идентификатор в съответствие с техническите спецификации за целите на трансграничната идентификация, който да остава непроменен, колкото е възможно по-дълго време. За Република България това е ЕИК/БУЛСТАТ.

Минималният набор от данни за юридическо лице може да съдържа допълнителни данни:

а) адрес на управление;

б) регистрационен номер по ДДС;

в) данъчен номер;

г) идентификационен код съгласно член 3, параграф 1 от Директива 2009/101/ЕО на Европейския парламент и на Съвета (1);

д) идентификационен код на правния субект (ИКПС), посочен в Регламент за изпълнение (ЕС) № 1247/2012 на Комисията (2);

е) идентификационен номер на икономически оператор (EORI номер), посочен в Регламент за изпълнение (ЕС) № 1352/2013 на Комисията (3);

ж) акцизен номер, предвиден в член 2, параграф 12 от Регламент № 389/2012 на Съвета (4);

з) други данни.

Евротръст предприема стъпки, за да се сведе до минимум рискът идентичността на

юридическото лице да не съответства на заявената такава.

3.2.3 УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ

Установяване на първоначална идентичност на физическо лице, което е упълномощено от юридическо лице се осъществява автоматизирано чрез отдалечена проверка и/или от Регистриращия орган. За установяване на първоначална идентичност на физическо лице, което е представител на юридическо лице (управители, членове на съвети, прокуристи и др.), когато представителната му власт произтича от закон, се прави проверка в съответните регистри при наличие на такава интеграция (Търговски регистър, Регистър на юридическите лица с нестопанска цел и др.).

Овластяването трябва да произтича от лице с представителна власт по закон. Когато представителната власт произтича от овластително изявление, то същото следва да бъде представено и проверено от Евротръст.

За всяко от физическите лица се прави първоначална проверка на самоличност по реда на предходните раздели. Когато представителната власт не може да се установи по реда на предходните правила, първоначалната идентичност на юридическото лице се проверява въз основа на представени документи от Регистриращия орган в офис на Евротръст.

В този случай се изискват следните документи:

- нотариално заверено пълномощно или документ за регистрация, от който произтича законна представителна власт (удостоверение за актуално състояние и др.);
- преглед и потвърждение на документ за самоличност на физическото лице, чрез проверка в национален регистър;
- проверка на вписванията на представителната власт на юридическото лице в официални регистри (към Агенцията по вписванията)
- други документи.

С първоначалната проверка на идентичността на юридическо лице се цели да се докаже, че по време на разглеждане на заявката юридическото лице съществува и че представляващото лице, което кандидатства за ползване на QERDS притежава

представителна власт.

3.3 АВТЕНТИФИКАЦИЯ

Ако се налага извършване на повторна заявка за ползване на услугата, в този случай не се извършва първоначална идентификация, а само проверка на актуалността на данните за самоличност/идентичност. Потребителят използва QERDS след като се автентифицира. В зависимост от използвания потребителски агент/програма (UA), през които изпращачът и получателят комуникират със системата за електронна препоръчана поща, те се автентифицират както следва:

1. Ако използва Мобилно приложение, лицето използва за автентификация криптографски ключове (secrets), които са интегрирани в мобилното приложение;
2. Ако лицето използва приложен програмен интерфейс (API), на него му се предоставя по сигурен канал криптографски ключ (secret), чрез който то се автентифицира пред системата. Допълнително лицето само генерира двойка криптографски ключове, като публичния ключ се използва за криптиране на данните към лицето;
3. Ако лицето използва уеб портал, то се автентифицира чрез Мобилно приложение по т.1. Допуска се на лицето да се предостави за целите на автентификацията и двойка криптографски ключове с приложено към тях удостоверение за квалифициран електронен подпис, които се генерират и издават по стандартна за Евротръст процедура.

Освен описаните начини за автентификация, Евротръст прилага допълнителни механизми с цел постигане на максимална сигурност и защита на процеса.

4 ПРОЦЕС НА ПРЕДОСТАВЯНЕ НА УСЛУГАТА

QERDS позволява прехвърляне на потребителско съдържание (например: документи) между потребители на Евротръст (изпращач и получател). Тази услуга предоставя доказателства за интегритета и времето на предадените данни, включително доказателства за изпращането и получаването им. Услугата защитава данните от загуба, кражба, нарушение на целостта им или неразрешена промяна и отговаря на изискванията на QERDS съгласно Регламент (ЕС) № 910/2014 г.

При използване на QERDS се спазва принципа, че правната сила на електронен документ не може да бъде оспорена на основанието, че той е в електронна форма, с цел да се гарантира, че електронна трансакция няма да бъде отхвърлена единствено на основанието, че даден документ е в електронна форма. В тази връзка се приема, че изпратените и получени електронни документи чрез QERDS са изчерпателни, изпратени са от изпращача и се получават от получателя, и че датата и часа на изпращане и получаване са точни.

4.1 ИЗИСКВАНИЯ КЪМ КВАЛИФИЦИРАНАТА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

Услугата за QERDS, предоставена от Евротръст, отговаря на всички изисквания в т. 6.1 на ETSI EN 319 401, както и на следните специфични изисквания:

- Политиките и практиките за ERDS се одобряват от ръководството на ERDSP и се съобщават на заинтересованите лица, като се публикуват на сайта на Евротръст (т.1.1);
- ERDSP има процедура за преразглеждане и актуализиране на практиките и процедура за уведомяване на направените промени на заинтересованите лица (т. 9.11);
- Услугата QERDS се предоставя от „Евротръст Технолъджис“ АД. Извън тази организация няма други външни организации, които да поддържат предоставянето на услугата;
- Комуникацията, по която текат данните е надеждно защитена с криптиран канал, с което се елиминира риска от всякакви изменения на потребителското съдържание преди изпращането/предаването. Доказателствата, свързани със събитията по изпращане/предаване на потребителско съдържание се съхраняват надеждно от последваща загуба и кражба в защитена среда под контрола на Евротръст за срок от 10 (десет) години (т.4.7).;
- В настоящия документ (т.3) е описан процесът по идентифициране на изпращача и получателя;
- Евротръст гарантира идентификацията/автентификацията на изпращача преди изпращане на потребителското съдържание;
- Евротръст гарантира идентификацията/автентификацията на получателя преди

доставянето на данните (пратката/потребителското съдържание);

- изпращането и получаването на данни е обезпечено чрез усъвършенстван електронен печат на Евротръст по начин, който изключва всякаква възможност за незабелязана промяна на данните;
- настоящият документ включва задълженията (т.9.5) на изпращача, получателя и доверяващите се страни;
- Настоящият документ посочва типовете събития, свързани с доставката и предоставя доказателства за този процес (т.4.6);
- всяка промяна на данните, необходима за целите на изпращането или получаването на данните, се обозначава ясно за изпращача и за получателя на данните;
- датата и часът на изпращане, получаване и промяна на потребителското съдържание се посочват с квалифициран електронен времеви печат;
- наличността, целостта и поверителността на потребителското съдържание е гарантирано от изпращането му до неговото приемане;
- интегритета на потребителското съдържание е защитено, особено когато се обменя между изпращача/получателя или между разпределените системни компоненти на услугата;
- доказателствата, свързани с действията по доставката на потребителското съдържание е защитено с усъвършенстван електронен печат, издаден от Евротръст, което изключва възможността данните да се променят;
- изпращачът задава предварително за какъв период от време системата за QERDS прави опити за доставяне на потребителското съдържание. Ако изпращача, не избере опция, то по подразбиране този срок е 3 дни;
- в случаите, при които се налага промяна на потребителското съдържание от ERDS, промените се указват ясно на изпращача, получателя и на третите страни;
- Датата и часът на изпращане, получаване и промяна на потребителското съдържание се посочват с квалифициран електронен времеви печат;
- QERDS използва квалифицирани услуги на Евротръст за издаване и управление на квалифицирани удостоверения (X.509) и квалифицирани удостоверения за време (Time Stamps);
- цялата информация по предоставяне на QERDS се съхранява за период от 10

години, съобразен с националното законодателство на Република България (ЗЕДЕУУ);

- Настоящият документ описва събитията, при които е невъзможна доставката до R-ERDS. В тези случаи системата автоматично генерира необходимите доказателства за това събитие и те се съхраняват 10 (десет) години (т.4.2);
- настоящият документ ясно и недвусмислено посочва, че политиката на ERDS е съгласно Регламент (ЕС) № 910/2014;
- настоящият документ включва пълния списък (т.1.3) на участващите QTSP предоставянето на QERDS;
- настоящият документ включва всички ограничения (т.9. 5 и 9.6) за използването на QERDS;
- Евротръст съхранява доказателствата надеждно от последваща загуба и кражба в защитена среда за срок от 10 години;
- Възможността за прекратяване на действието на услугата е на разположение денонощно (т.4.8).

4.2 ОПИСАНИЕ НА ТЕХНОЛОГИЯТА

QERDS използва технология, при която след първоначална идентификация на изпращача и текуща негова автентификация, потребителското съдържание се приема от S-ERDS по надеждно защитен и криптиран сигурен канал. В този момент S-ERDS генерира необходимите доказателства с включени в тях точни данни за вида на събитието, включително дата, час, контролна/хеш сума на потребителското съдържание, като те са електронно подписани от QERDS SUs, като част от QERDS, и подпечатани с квалифициран времеви печат. При невъзможност за приемане от страна на S-ERDS, отново тя автоматично генерира необходимите доказателства за отказа.

S-ERDS надеждно прехвърля пратката към R-ERDS. Отново автоматично се генерира необходимите доказателства с включени в тях точни данни за вида на събитието, включително дата, час, контролна/хеш сума на потребителското съдържание, като те са електронно подписани от QERDS SUs и подпечатани с квалифициран времеви печат. При невъзможност за доставка до R-ERDS, системата автоматично генерира необходимите доказателства за това събитие.

В момента, в който потребителското съдържание постъпи в системата на получателя, т.е. то е връчено на получателя, R-ERDS генерира необходимите доказателства с включени в тях точни данни за събитието, включително дата, час, контролна/хеш сума на потребителското съдържание, като те са електронно подписани от QERDS SUs и подпечатани с квалифициран времеви печат. Подписващият орган QERDS SUs използва удостоверение, издадено от удостоверяващ орган, който в случая е „Evrotrust Service CA“ с OID: 1.3.6.1.4.1.47272.2.14 в архитектурата на Евротръст. При невъзможност за връчване, отново R-ERDS автоматично генерира необходимите доказателства за това събитие.

4.3 СХЕМИ НА ПРОЦЕСА НА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

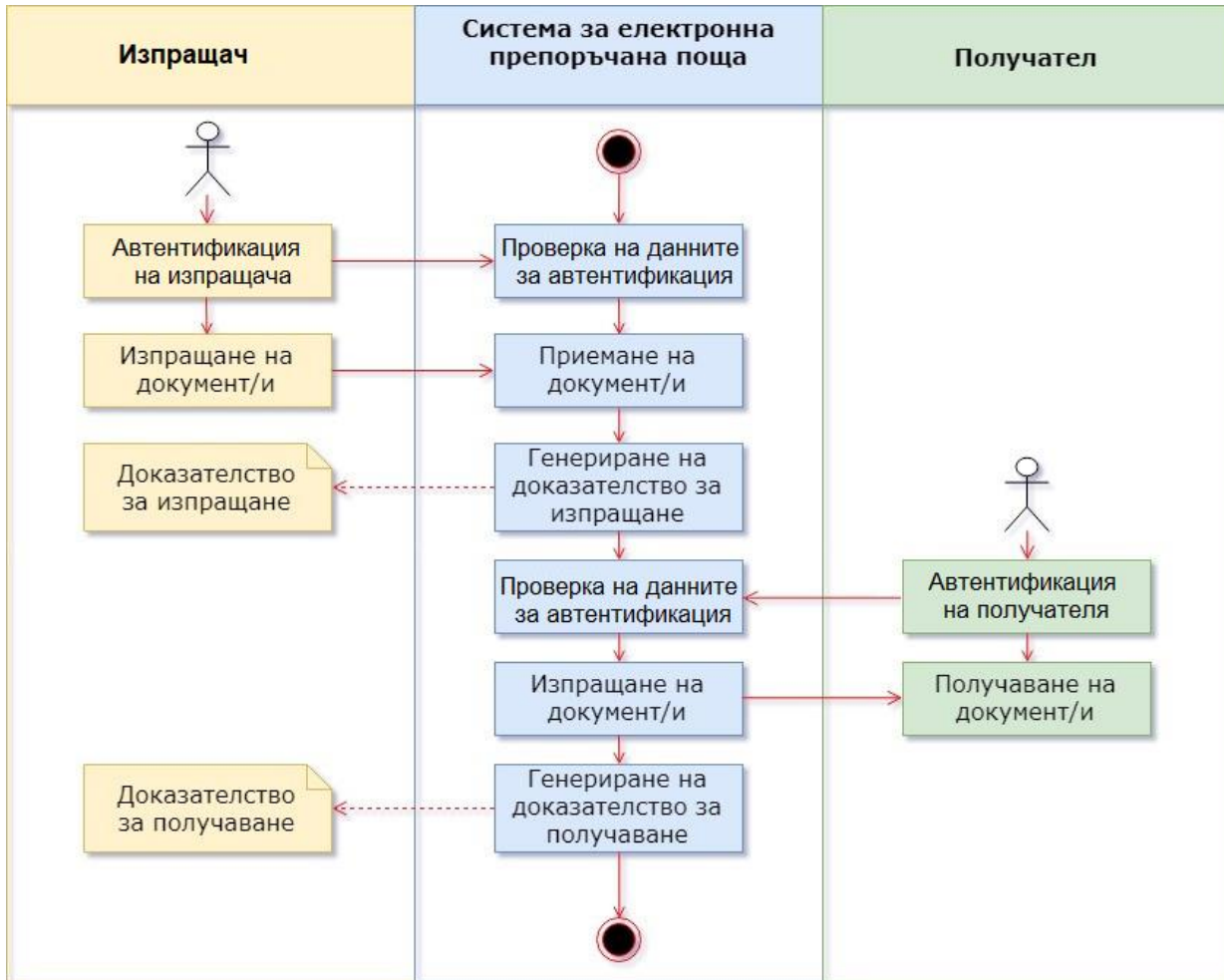
QERDS предоставя доказателства за събития, които се случват по време на предаването на потребителско съдържание (съобщения, документи, файлове и др. обекти) между страните (например информация, че данните са били изпратени от изпращача или че са доставени на получателя). Тези доказателства могат да се използват, за да се докаже пред трети лица, ако е необходимо и в съдебни производства, че размяната на съобщения или документи е била извършена в точен времеви момент, което се потвърждава с квалифициран времеви печат.

Доказателството за QERDS е удостоверение, подписано с усъвършенстван електронен печат на Евротръст от QERDS SUs с обектен идентификатор: 1.3.6.1.4.1.47272.2.10.1 . Удостоверяващият орган на квалифицирана услуга за електронна препоръчана поща „Evrotrust Services CA“ подписва удостоверението на подписващия орган QERDS SUs. Доказателството съдържа информация, че конкретно събитие, свързано с процеса на предаване на данни между изпращача и получателя (например изпращане на съобщение или получаване на съобщение) се е случило в точно определен момент. Едно доказателство за QERDS може незабавно да бъде предадено на изпращача/получателя, но също така, то се съхранява за срок от 10 години, съобразно националното законодателство на Република България (ЗЕДЕУУ) в хранилището на Евротръст, за по-късен достъп от заинтересованите страни.

За сигурна и надеждна доставка на данни между получателя и изпращача Евротръст

използва първоначална идентификация на участниците в процеса. Първоначалната идентификация се извършва чрез проверка на съвкупност от идентифициращи атрибути, които уникално идентифицират лицата.





4.4 ПРОЦЕС НА ПРЕДОСТАВЯНЕ НА УСЛУГАТА

QERDS на Евротръст се достъпва чрез използването на интернет портал (web portal/уеб портал), приложно-програмен интерфейс (Application Programming Interface/API) или мобилно приложение. Използването на услугата изисква осъществяването на първоначална идентификация на изпращача и получателя, която се осъществява отдалечено, чрез използване на мобилно приложение, или чрез лично явяване на лицата или техни представители пред някои от Регистриращите органи (РО) на Евротръст. Данните за изпращача и получателя, които Евротръст събира са лични данни, данни за контакт, данни от документ за самоличност и други.

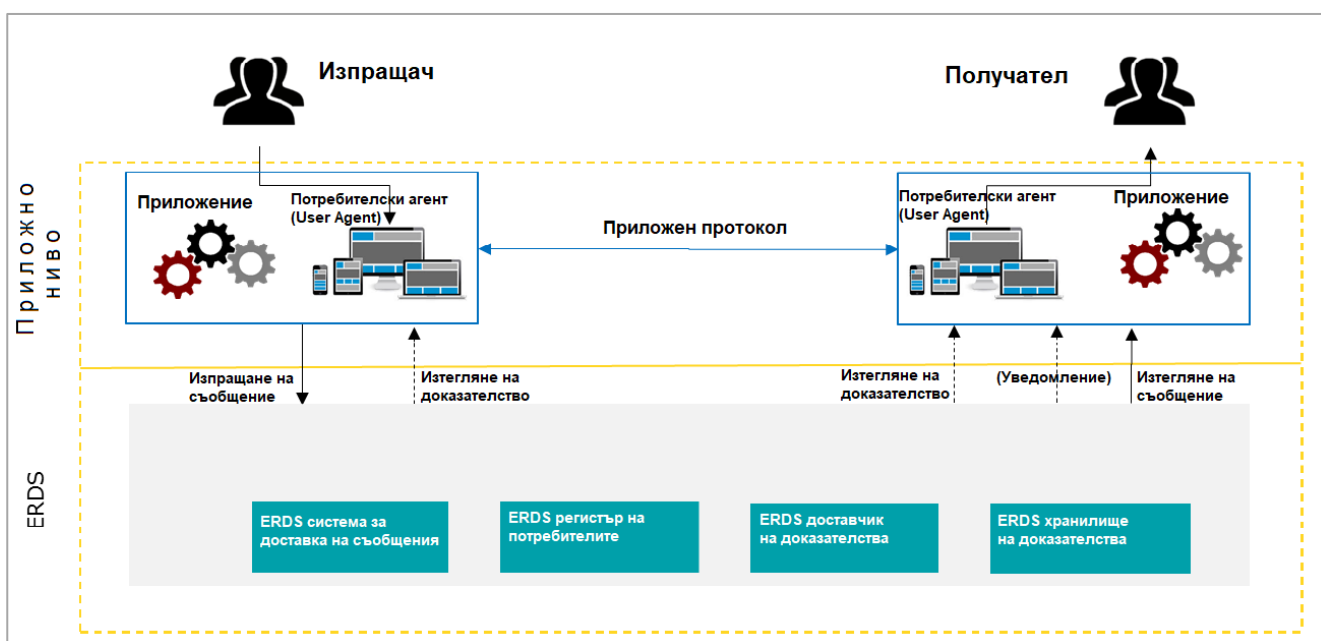
Потребителските агенти/програми (UA), през които изпращачът и получателят комуникират със системата за електронна препоръчана поща са:

1. Мобилно приложение, инсталирано на персонално мобилно устройство

(мобилен телефон, таблет и др.);

2. Приложен програмнен интерфейс (API), чрез който интегрираните външни системи използват услугата (компании, банки, дружества и др.);

3. Уеб портал, през който потребителите използват услугата.



Съобразявайки се с използваната терминология в ETSI EN 319 521 и терминологията използвана в националното законодателство (ЗЕУ и ЗЕДЕУУ), Политиката на Евротръст конкретизира момента на доставка/consignment и момента на връчване/handover на потребителско съдържание в зависимост от реализацията на услугата. Моментът на доставка/consignment е момента, в който ERDS направи пратката достъпна за получаване от получателя в рамките на ERDS. Моментът на връчване/handover е:

- при използване на мобилно приложение: момента на доставка/изтегляне на пратката в бекенда на мобилното приложение на получателя, който бекенд е част от потребителския агент/приложение на получателя;
- при използване на API интеграция: момента на доставка/изтегляне на пратката в/от информационната система на получателя, която използва API интеграция;
- при използване на уеб базиран портал: момента на доставка/изтегляне на пратката в бекенда, достъпен през уеб базиран портал, който бекенд е част от потребителския агент/приложение на получателя.

4.5 ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ/ПОЛУЧАТЕЛ

4.5.1 ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ

Евротръст извършва първоначална идентификация на изпращача по един от следните начини, в зависимост от използвания от него потребителски агент:

1. При използване на мобилно приложение - регистрираният орган на доставчика първоначално идентифицира изпращача чрез системата за видео идентификация, сертифицирана като сигурна електронна идентификация по смисъла на Регламент (ЕС) № 910/2014 г. Използвайки двуфакторна идентификация, изпращачът достъпва сигурна среда - електронно подписано специализирано мобилно приложение на Евротръст, чрез което той се автентифицира и подава документите за изпращане.

2. При използване на Приложен програмен интерфейс (API) - Евротръст първоначално идентифицира изпращача, чрез регистрирания си орган. След тази идентификация, изпращачът използва криптографски, сесийни и API ключове, чрез които се автентифицира и подава документите за изпращане.

3. При използване на уеб портал - Евротръст използва мобилно приложение и извършва първоначална идентификация на изпращача чрез системата за видео идентификация, сертифицирана като сигурна електронна идентификация по смисъла на Регламент (ЕС) № 910/2014 г. Използвайки двуфакторна идентификация, изпращачът достъпва сигурна среда - електронно подписано специализирано мобилно приложение на Евротръст, през която той се автентифицира за достъп и работа с уеб портала, чрез който подава документите за изпращане.

Само след успешна автентификация на изпращача, пратката се прехвърля от системата, която е под негов контрол към системата на QERDS.

Процесът на автентифициране се извършва в защитена и контролирана среда. Всички доказателства за автентификацията и изпращане на пратката се събират и съхраняват в защитена среда.

4.5.2 ИДЕНТИФИКАЦИЯ НА ПОЛУЧАТЕЛ

Евротръст извършва първоначална идентификация на получателя по един от следните начини, в зависимост от използвания потребителски агент:

1. При използване на мобилно приложение - регистриращият орган на доставчика първоначално идентифицира получателя чрез системата за видео идентификация, сертифицирана като сигурна електронна идентификация по смисъла на Регламент (ЕС) № 910/2014 г. Използвайки двуфакторна идентификация, получателят достъпва сигурна среда - електронно подписано специализирано мобилно приложение на Евротръст, чрез което той се автентифицира и подава документите за изпращане.

2. При използване на Приложен програмнен интерфейс (API) - Евротръст първоначално идентифицира получателя, чрез регистриращия си орган. След тази идентификация, получателят използва криптографски, сесийни и API ключове, чрез които се автентифицира и подава документите за изпращане.

3. При използване на уеб портал - Евротръст използва мобилно приложение и извършва първоначална идентификация на получателя чрез системата за видео идентификация, сертифицирана като сигурна електронна идентификация по смисъла на Регламент (ЕС) № 910/2014 г. Използвайки двуфакторна идентификация, получателят достъпва сигурна среда - електронно подписано специализирано мобилно приложение на Евротръст, през която той се автентифицира за достъп и работа с уеб портала, чрез който подава документите за изпращане.

Доказателството за получаване се предоставя като отделен електронен документ в строго определен формат, като в него е посочена точна дата и час на получаване на потребителското съдържание от получателя, чрез квалифициран времеви печат. Доказателството е електронно подписано от удостоверяващия орган на QERDS.

Само след успешно преминала автентификация на получателя, пратката се доставя от системата на QERDS до системата, която е под негов контрол, респ. до получателя.

Процесът на автентифициране се провежда в защитена и контролирана среда. Всички доказателства за автентификацията и получаването на пратката се събират и съхраняват в защитена среда.

4.6 СЪЗДАВАНЕ НА ДОКАЗАТЕЛСТВА

QERDS предоставя доказателства за изпращането и получаването на потребителско съдържание.

Евротръст събира и съхранява данни за:

1. Всички събития, свързани с първоначалната проверка на самоличността/идентичността на изпращача и идентификацията му;
2. Всички събития, свързани с първоначалната проверка на самоличността/идентичността на получателя и идентификацията му;
3. При първоначална проверка на самоличността/идентичността се проверяват данните от документа за самоличност на физическо лице (напр. лична карта или паспорт), данни за идентифициране на юридическо лице (напр. проверка в регистри, пълномощни и т.н.) и всички други данни, които са необходими за правилното му определяне;
4. Данни за първоначална идентификация на изпращача/получателя;
5. Ниво на автентификация на изпращача/получателя;
6. Доказателство, че изпращача е автентифициран правилно, преди приемане на пратката;
7. Данни за експлоатацията на QERDS, потвърждаващи автентификацията на изпращача и получателя, както и на комуникацията между тях;
8. Доказателство, че потребителското съдържание е получено от получателя;
9. Доказателство, че потребителското съдържание не е променено по време на предаването.

4.6.1 ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ИЗПРАЩАЧА (S-ERDS)

След успешно първоначално идентифициране и автентифициране на изпращача и използване на QERDS чрез S-ERDS се създават доказателства за изпращане, които могат да се предоставят и на трета страна. В доказателствата е посочена точна дата и час на изпращане на потребителското съдържание от изпращача с точно калибровано време спрямо UTC (Coordinated Universal Time).

а. Приемане за изпращане (SubmissionAcceptance)

Изпращачът успешно предава потребителското съдържание към S-ERDS.

Генерира се доказателство с вписани дата и час, което показва, че изпращачът, който е първоначално идентифициран и надлежно автентифициран, е подал в ERDS системата пратка, която е била приета от доставчика и той ще предприеме всички необходими действия, за да я достави към съответния получател(и).

б. Отхвърляне за изпращане (SubmissionRejection)

Потребителското съдържание, което е било изпратено към S-ERDS от изпращача не е било прието от S-ERDS. Генерираното доказателство свидетелства, че изпращачът, който е първоначално идентифициран и надлежно автентифициран, е предал потребителското съдържание в конкретни дата и час на ERDS, и че ERDS системата е отказала да изпълни необходимите действия.

4.6.2 ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ПОЛУЧАТЕЛЯ (R-ERDS)

След успешно първоначално идентифициране и автентифициране на получателя и използване на QERDS чрез R-ERDS се създава доказателство за получаване, което може да се предоставя и на трета страна. В доказателствата е посочена точна дата и час на изпращане на потребителското съдържание от изпращача с точно калибровано време спрямо UTC (Coordinated Universal Time).

а. Доказателства, свързани с доставката на съдържание (ContentConsignment)

Потребителското съдържание е предоставено на получателя.

Свързаните с това доказателства свидетелстват, че пратката е била предоставена на получателя в рамките на предварително указаното време, след като получателят е бил първоначално идентифициран и правилно автентифициран.

б. Невъзможност за доставка на съдържание (ContentConsignmentFailure)

Потребителското съдържание не може да бъде доставено на получателя в рамките на определен период от време поради технически грешки и/или поради други причини.

Възможно е да липсва доказателство за доставка в рамките на предварително посочения период от време.

Невъзможността за доставка на съдържание може да бъде предизвикано от различни събития, например:

- ERDS системата не е могла да изпрати съдържанието от изпращача до получателя.

В този случай доказателствата се изготвят от R-ERDS.

- По време на престоя на съобщението в ERDS системата не е получено доказателство за успешна доставка в рамките на определен период от време. В този случай ERDS създава доказателствата с подходящия код на причина за невъзможността за доставка.

4.6.3 ДОКАЗАТЕЛСТВА, СВЪРЗАНИ С ПРЕДАВАНЕТО НА ПОТРЕБИТЕЛСКО СЪДЪРЖАНИЕ НА ПОЛУЧАТЕЛЯ

а. Връчване на съдържание (ContentHandover)

Потребителското съдържание успешно е преминало от R-ERDS към приложението на получателя/потребителския агент (UA). Събитията могат да са: „pull“ (т.е. UA/приложението на получателя извлича автоматично потребителското съдържание от R-ERDS – при получатели, свързани с API или чрез портал) или „push“ (потребителското съдържание е успешно доставено в системата на получателя чрез директно доставяне на съобщението в системата на получателя – мобилно приложение, API или уеб портал).

Свързаните с това доказателства свидетелстват, че потребителското съдържание в точно определена дата и час е предадено от R-ERDS, чрез UA/приложението на получателя и след неговото правилно удостоверяване.

б. Грешка при връчване на съдържание (ContentHandoverFailure)

Потребителското съдържание не може да бъде предадено от R-ERDS към потребителския агент (UA)/приложението на получателя. В случай „pull“ (т.е. UA/приложението на получателя автоматично извлича съобщението от ERDS), съобщението не може да бъде изтеглено в рамките на даден период поради технически грешки и/или други причини.

Свързаните с това доказателства свидетелстват, че съдържанието не може да бъде

пренесено от R-ERDS към UA/приложението на получателя след определен брой опити или определено време на изчакване. Тези параметри са специфични и конфигурирани за конкретната система.

4.7 ЗАЩИТА НА ПРЕДАВАНИТЕ ДАННИ СРЕЩУ РИСК ОТ ЗАГУБА, КРАЖБА, ПОВРЕДА ИЛИ НЕПОЗВОЛЕНИ ИЗМЕНЕНИЯ

Всички носители съдържащи софтуер, архиви на данни или одитна информация се съхраняват безопасно в специално архивно помещение с въведен контрол на достъп. В помещението с архива на Евротръст има изградена система на физическа и логическа защита.

Поверителността и целостта на данните са важни за дейността на Евротръст и по тази причина се използват криптографски техники за защита на данните на сменяеми носители. За да се смекчи рискът от остаряване на носителите, докато съхраняваните данни са все още необходими, данните се прехвърлят на нови носители, преди да станат нечетливи. Евротръст съхранява по няколко копия на ценните данни на различни носители, за да намали още повече рискът от случайно повреждане или загуба на данните. Комуникацията, по която текат данните е надеждно защитена с криптиран канал, с което се елиминира риска от загуба, кражба, повреда или непозволені изменения на данни. Доказателствата се съхраняват надеждно от последваща загуба и кражба в защитена среда под контрола на Евротръст за срок от 10 години.

4.8 КРАЙ НА АБОНАМЕНТА НА УСЛУГАТА

Договорът за предоставяне на квалифицирана услуга за електронна препоръчана поща се прекратява при едно от следните обстоятелства:

- a) закриване на профил от мобилното приложение на Евротръст с активиране на съответната функционалност. Прекратяването се извършва незабавно;
- b) други обстоятелства, посочени в „Практиката при предоставяне на квалифицирани удостоверителни услуги на Евротръст.

Възможността за прекратяване на действието на услугата е на разположение

денонощно, 7 дни в седмицата. Времето в системите, свързани с прекратяване на договор за услуга за предоставяне на електронна препоръчана поща се синхронизира спрямо UTC поне веднъж на 24 часа.

4.9 ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)

Частните ключове на удостоверяващия орган на Евротръст, които са включени в удостоверителната йерархия на Евротръст са персонализирани върху преносими носители и не подлежат на доверително съхранение от Евротръст (ЕСКРОУ).

Частните ключове на потребителите, които са заявили издаване на удостоверения отдалечено, чрез мобилното приложение на Евротръст, подлежат на доверително съхранение от Евротръст (ЕСКРОУ) и се съхраняват в криптиран в надеждна криптографска система (Hardware Security Module/HSM), сертифицирана за ниво на сигурност FIPS 140-2 Level 3.

5 КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ

5.1 ФИЗИЧЕСКИ КОНТРОЛИ ЗА СИГУРНОСТ

Мерките предприети по отношение на физическата защита на Евротръст са елемент от разработената и внедрена в Евротръст Система за информационна сигурност, съответстваща на изискванията на стандарта ISO/IEC 27001.

Мерките свързани с физическата защита на информационните данни, технологичните системи, помещенията и свързаните с тях поддържащи системи са насочени към предотвратяване на:

- неразрешен достъп, нанасяне на щети и намеса в условията на работа;
- загуба, вреди или компрометиране на ресурси;
- компрометиране или кражба на информация или средства за обработка на информацията.

Инфраструктурата на Евротръст е физически и логически обособена и не се използва за други дейности, които Евротръст осъществява.

5.1.1 ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА

Евротръст разполага със специално конструирано и оборудвано помещение с най-висока степен на контрол на физически достъп, в което се помещават удостоверяващ орган и всичките централни компоненти на инфраструктурата.

5.1.2 ФИЗИЧЕСКИ ДОСТЪП

Физическата сигурност на системите е съобразена с изискванията на международни стандарти и препоръки. За оборудването в защитеното и изолирано помещение на Евротръст е осигурена физическа неприкосновеност. Има двуфакторен контрол на достъпа и денонощна въоръжена физическа охрана. Не е позволен физически достъп до критичното оборудване за повече от 30 (тридесет) минути на посещение. Не е позволен достъп до шкафа с оборудването на по-малко от 2 (две) оторизирани лица на Евротръст. Всеки достъп до помещенията с критична инфраструктура се документира в специални журналы.

Защитата на сградата на Евротръст е реализирана от невъоръжена 24-часова охрана. В помещенията на Евротръст има Система за алармена сигнализация, Система за видеонаблюдение, Пожароизвестителна система и Система за контрол на достъпа.

В Евротръст офисите на Регистриращите органи са обособени и отделени от останалите помещения. Съоръжени са с техника, позволяваща безопасно съхранение на данни и документи. Достъпът до всички зони се следи и ограничава до оторизирани лица в съответствие с тяхната дейност.

В сградите на доставчика има изградени системи за електрозахранване и вентилация, защита срещу наводнения и пожар.

5.1.3 КОНТРОЛ НА ДОСТЪПА

Достъпът до системата на Евротръст е ограничен до упълномощени лица:

- контролите (например защитни стени) защитават вътрешните мрежови домейни на Евротръст от неразрешен достъп, включително достъп на клиенти и трети страни;
- доставчикът предоставя администраторски достъп на операторите,

администраторите и системните одитори. Ръководството управлява потребителските акаунти, навременната промяна или премахване на достъпа.

- достъпът до информацията и системата се ограничава в съответствие с разделянето на доверените роли;
- служителите на Евротръст се идентифицират и удостоверяват преди да използват критични приложения, свързани с услугата;

Евротръст е предприело мерки да защити чувствителните данни на дружеството срещу разкриване и неоторизиран достъп

5.2 УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Евротръст класифицира инцидентите със сигурността в две категории:

- които застрашават целостта на удостоверителните услуги (напр. проникване или промяна в местоположението на доставката, грешки в поддържането на системата, които застрашават целостта на системите/сървърите, физически достъп от неупълномощени лица);
- които не застрашават целостта на удостоверителните услуги (напр. загуба на електрозахранването, повреда в комуникационните линии, злоупотреба с правомощия, опити за проникване в системата).

Ако има съмнение при определяне на коя категория е класифициран инцидента по сигурността, инцидентът се счита за класифициран от най-висока степен.

Всяко лице, което вижда или подозира за инцидент по сигурността е задължено да информира ръководството. Докладването на инцидентите по сигурността се извършва по какъвто и да е начин (лично, по телефон или по имейл), който дава възможност за най-бързо уведомяване на съответните ръководни лица.

Ръководството е задължено да разследва докладвания инцидент и да приеме или предложи подходящи мерки за предотвратяване на повторение от подобен инцидент.

Всеки инцидент свързан със сигурността се записва в протокол.

Евротръст установява процедури за уведомяване на съответните засегнати страни в съответствие с приложимите регулаторни правила за всяко нарушаване на сигурността или загуба на неприкосновеност, което оказва значително въздействие върху доверието на

предоставената удостоверяваща услуга и върху личните данни, поддържани в нея, в рамките на 24 часа от идентифицирането на нарушението. Когато нарушаването на сигурността или загубата на данни може да се отрази неблагоприятно на физическо или юридическо лице, което използва услугата, доставчикът уведомява лицето за инцидента.

Евротръст разглежда всяка критична уязвимост в рамките на 48 часа след откриването ѝ.

5.3 КОНТРОЛ НА ПЕРСОНАЛА

Евротръст гарантира, че служителите изпълняват административни и управленски процедури и процедури, които са в съответствие с управление на информационната сигурност, като по този начин осигуряват надеждност и сигурност на своята дейност. Евротръст наема персонал и, ако е приложимо, подизпълнители, които притежават необходимия опит, надеждност и квалификация и които са преминали обучение по отношение на сигурността и защитата на личните данни. Евротръст прилага подходящи дисциплинарни наказания за служители, които нарушават политиките или процедурите на дружеството.

Ролите и отговорностите по информационна сигурност са документирани в длъжностните характеристики на персонала. Ръководният персонал притежава необходимия опит и знания по отношение на предоставяната услуга QERDS, запознати са с процедурите за сигурност и оценка на риска, достатъчни за осъществяване на управленски функции.

Целият персонал на доставчика няма конфликт на интереси, който би могъл да накърни безпристрастността на дейността на Евротръст.

Организационния контрол, който осъществява Евротръст е описан в т. 5.2 на документа „Практиката при предоставяне на квалифицирани удостоверяващи услуги“.

5.4 ПРОЦЕДУРА ЗА ОДИТ

Проверките (одитите), извършвани в Евротръст се отнасят до обработката на

информационните данни и управление на ключовите процедури. Евротръст ежегодно извършва най-малко един вътрешен одит. Доставчикът е преминал успешно одит от външна фирма и е сертифициран по следните ISO стандарти: ISO 9001, ISO 22301, ISO/IEC 27001 и ISO/IEC 20000-1.

Предметът на дейност, проверяван по време на одитите за всеки от стандартите е:

- ISO 9001, ISO 22301 - Предоставяне на услуги, свързани с електронна идентификация и услуги по Регламент (ЕС) № 910/2014;
- ISO/IEC 27001 - Система за управление на информационната сигурност за обработка на лични данни на клиенти, корпоративни данни и информационни системи за предоставяне на електронна идентификация и удостоверителни услуги в съответствие с Декларация за приложимост версия 1.0.;
- ISO/IEC 20000-1 - Система за управление на ИТ услуги за предоставяне на услуги, свързани с електронна идентификация и удостоверителни услуги на външни клиенти в съответствие с каталог на услугите.

Евротръст е обект на одит най-малко веднъж на 24 месеца от Орган за оценяване на съответствието. Целта на одита е да се потвърди, че Доставчика на квалифицирани удостоверителни услуги и предоставяните от него удостоверителни услуги отговарят на изискванията, посочени в Регламент (ЕС) № 910/2014.

Докладите от вътрешни и външни одити се предават на ръководството на Евротръст.

Докладът от Органа за оценяване на съответствието се предава на Органа по надзор в рамките на 3 (три) дни след връчването му на ръководството на Евротръст. Органа по надзор, разглежда доклада и решава дали да предостави или отнеме квалифицирания статут на доставчика.

Въз основа на направените оценки от докладите, ръководство на Евротръст набелязва мерки и срокове за отстраняване на констатираните пропуски и несъответствия.

5.5 АРХИВИРАНЕ

Информацията за значимите събития се архивира в електронен вид периодично.

Евротръст архивира всички данни и файлове, свързани с: информацията при регистрация; със сигурността на системата; всички искания, подадени от клиентите; цялата

информация за клиентите; всички ключове, използвани от Удостоверяващите органи и от Регистриращия орган; и цялата кореспонденция между Евротръст и клиентите. На архивиране са подложени всички документи и данни, използвани в процеса на проверка на самоличността.

Информацията по чл. 24, параграф 2, буква „з“ от Регламент (ЕС) № 910/2014 г.(цялата имаща отношение информация във връзка с данните, издадени и получени от Евротръст, и по-специално с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата) се съхранява за срок 10 години, включително и след преустановяване на дейността на Евротръст.

Дългосрочното съхраняване на данни се прави в сигурно и защитено помещение. Конкретните условия са в съответствие с приложимите стандарти, препоръки и регламенти, посочени в областта на информационната сигурност.

Данните се събират по начин, съответстващ на вида на документа.

Достъпът до съхраняваните дългосрочно данни е възможен само от упълномощени лица.

5.5.1 СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ

Всички носители съдържащи софтуер, архиви на данни или одитна информация се съхраняват безопасно в специално архивно помещение с въведен контрол на достъп. В помещението с архива на Евротръст има изградена система на физическа и логическа защита.

Когато поверителността или целостта на данните са важни за дейността на Евротръст се използват криптографски техники за защита на данните на сменяеми носители. За да се смекчи рискът от остаряване на носителите, докато съхраняваните данни са все още необходими, данните се прехвърлят на нови носители, преди да станат нечетливи.

Евротръст съхранява по няколко копия на ценните данни на различни носители, за да намали още повече рискът от случайно повреждане или загуба на данните.

5.5.2 ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИ

Създадени са процедури за сигурно унищожаване на носители, за да се намали до минимум рискът от изтичане на поверителна информация към неоторизирани лица. Процедурите за сигурно унищожаване на носители, съдържащи поверителна информация, съответстват на чувствителността на тази информация.

Носителите, съдържащи поверителна информация, се съхраняват и унищожават по сигурен начин, чрез изгаряне или нарязване, или изтриване на данни при използване от друго приложение. Унищожаването на чувствителни обекти се записва в дневник, за да се поддържа история за одита.

За повредените устройства, съдържащи чувствителни данни се оценява риска дали обектите трябва да бъдат физически унищожени или изпратени за поправка.

Хартиените носители, съдържащи значима информация за сигурността на Евротръст, след изтичане на определения съгласно вътрешните правила период на съхранение, се унищожават в специални устройства за нарязване.

Носителите на информация за криптографските ключове и кодове за достъп до тях, използвани за тяхното съхранение, се раздробяват с подходящи устройства. Това се отнася за носителите, които не позволяват окончателно заличаване на съхранени данни и тяхното повторно използване.

В определени случаи, информацията от преносими носители се унищожават, чрез изтриване или форматиране на устройството без възможност за възстановяване.

5.5.3 УПРАВЛЕНИЕ НА АКТИВИ

Евротръст осигурява подходящо ниво на защита на своите активи, включително информационни активи. Доставчикът поддържа списък на всички информационни активи и прави оценка на риска.

Евротръст идентифицира активите, съответстващи на жизнения цикъл на информацията и ги документира по тяхната важност. Жизненият цикъл на информацията включва създаване, обработване, съхранение, обмен/предаване, изтриване и унищожаване. Документацията се поддържа в специални описи. Описът на активите е точен,

актуален и последователен.

Информацията е класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране.

Разработени са процедури за работа с активи в съответствие с класификационната схема на информацията, приета от Евротръст.

5.5.4 ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ

Евротръст прави записи на:

- събития, свързани с първоначалната проверка на самоличността/идентичността на изпращача и/или с допълнителната автентификация;
- събития, свързани с първоначалната проверка на самоличността/идентичността на получателя и/или с допълнителна автентификация;

Записите съдържат описание на документите, представени от лицето, което желае да бъде идентифицирано (напр. документ за самоличност, пълномощно и т.н.), както и данни, отнасящ се до уникални идентификационни данни, номера или комбинация от тях или екземпляри от заявления и документи за самоличност, включително подписан договор, съгласие с Политиката и практиката на Евротръст и предоставянето на лични данни.

- събития, свързани с изпращането и получаването на потребителското съдържание;
- събития за сигурност, включително промени, свързани с политиката за сигурност, стартиране и изключване на системата, системни сризове и откази на хардуер, защитна стена и маршрутизатор и опитите за достъп до PKI система;
- записите, свързани с експлоатацията на услугата QERDS, са надеждно и поверително архивирани в съответствие с бизнес практиките на дружеството;
- точното време на значимите събития за управлението на ключовете и синхронизацията на часовника. Времето в системите се синхронизира спрямо UTC поне веднъж на 24 часа;
- събитията се записват по начин, по който не може лесно да бъдат изтрети или унищожени;

➤ събития, имащи съществено значение върху сигурността и надеждността на технологичната система, контрола върху персонала и клиентите, и въздействието върху сигурността на предоставяната QERDS се записват.

Събраните документи, свързани с предоставянето на услугата, се предоставят като доказателства, например за целите на съдебно производство. Евротръст осигурява поверителността, целостта и наличността на журналите. Информацията за електронните журнали се генерира автоматично. Журнали на записи на регистрирани събития се съхраняват във файлове за най-малко 6 (шест) месеца. През това време те са достъпни онлайн или в процес на търсене от оторизиран служител на Евротръст. След този период, записите се архивират. Архивирани журнали се запазват в продължение на 10 (десет) години. Архивът се подписва с усъвършенстван електронен подпис и квалифициран електронен времеви печат. Информацията от записите в логовете периодично се записва на физически носители, които се съхраняват в специален сейф, намиращ се в помещение с висока степен на физическа защита и контрол на достъпа.

5.6 СМЯНА НА КЛЮЧОВЕ

Доставчикът може да смени ключовете на удостоверяващия орган „Evrotrust Services CA“ и на подписващия „QERDS SU“, в случай на:

- изтичане на срока на валидност на съпътстващото му удостоверение;
- при промени в характеристиките на частния ключ, свързани със сигурността и изискване за нови приложими криптографски комбинации и алгоритми;
- при съмнения за компрометиране.

При смяна на частните ключове Евротръст се спазват следните правила:

- „ QERDS SU “, с чийто ключ се подписват доказателствата, и чийто ключ ще бъде променен, спира издаването на удостоверения 60 (шестдесет) дни преди момента, в който оставащия период на валидност на частния ключ се изравни с периодът на валидност на последното подписано доказателство;
- Удостоверяващият орган „Evrotrust Services CA“, с чийто частен ключ се подписва удостоверението на „ QERDS SU“ и Списъка със спрени и прекратени удостоверения (CRL) и чийто частен ключ ще бъде сменен, продължава да публикува списъци, подписани със

стария частен ключ до момента, в който изтече срокът на валидност на последното подписано удостоверение.

➤ Евротръст не подновяване потребителско квалифицирано удостоверение, заявено отдалечено през мобилното приложение. След изтичането му се издава ново удостоверение, с нова двойка ключове.

5.7 КОМПРОМИТИРАНЕ И ВЪЗСТАНОВЯВАНЕ ПРИ БЕДСТВИЯ

Процедурите, които следва Евротръст при компрометиране и възстановяване при бедствия са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“

В случай на компрометиране на услугите на ERDSP, Евротръст уведомява за това всички свои клиенти, както и доверяващите се страни и други образувания, с които ERDSP има споразумения или друга форма на установени отношения за предоставяне на ERDS. Информацията, която се предоставя, показва, че доказателствата, издадени чрез компрометирания ключ, може да не са вече валидни от времето на компрометирането.

Ако някой от алгоритмите или свързаните параметри, използвани от ERDSP, станат недостатъчни за оставащото им предназначение, тогава Евротръст:

- информира всички свои потребители и доверяващи се страни, с които ERDSP има споразумение или друга форма на установени отношения за предоставянето на ERDS;
- и
- осигурява съществуващия доказателствен материал с нови времеви печати.

5.7.1 ПЛАН ЗА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА

Дружеството е създадо, документирало, осъществило и поддържа планове, процедури и механизми за контрол в съответствие с международния стандарт ISO 22301, за да осигури необходимото ниво на непрекъснатост на дейността и сигурността на информацията по време на неблагоприятни случаи.

Евротръст осигурява:

а) наличие на адекватна структура на управление, за да се подготви, смекчи и реагира на разрушаващо събитие, използвайки персонал с необходимите пълномощия, опит и компетентност;

б) разработва и одобрява планове и процедури за реакция и възстановяване, подробно описвайки как дружеството ще управлява разрушаващо събитие и ще поддържа непрекъснатостта на сигурността на информацията;

в) механизми за контрол на сигурността на информацията в рамките на процедурите и поддържащите системи и инструменти за непрекъснатост на дейността и възстановяване след бедствие;

г) компенсирани механизми за контрол на механизмите за контрол на сигурността на информацията, които не могат да бъдат поддържани по време на неблагоприятен случай.

Осигурен е план за непрекъснатост, който включва дублиране на критичните системи. Ваксип се съхранява на географски отдалечени места. Конкретните условия са в съответствие с приложимите стандарти, препоръки и регламенти, посочени в областта на информационната сигурност.

Дружеството проверява през редовни интервали от време създадените механизми за контрол на непрекъснатостта на сигурността на информацията, така че да осигури тяхното действие и ефикасност по време на неблагоприятни случаи.

Евротръст редовно прави резервни копия на важна информация и софтуер, и гарантира, че цялата основна информация и софтуера могат да бъдат възстановени след бедствие или при загуба на архива.

Механизмите за възстановяване се проверяват редовно, за да се гарантира, че те отговарят на изискванията на плана за непрекъснатост на работата.

Базата от данни на доставчика, необходима за възстановяване на дейността по QERDS в случай на инцидент или бедствие се поддържа и съхранява на безопасни и сигурни места. Евротръст има задължението да информира изпращачи, получатели и трети страни при настъпили инциденти в дейността по предоставяне на услугата.

5.8 ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА УДОСТОВЕРЯВАЩ ОРГАН

При прекратяване на дейността на удостоверяващия орган „Evrotrust Services SA“ Евротръст извършва следното:

- Следва актуализиран и одобрен от ръководството план и сценарий за прекратяване на дейността на удостоверяващ орган. Информиранието може да се извърши чрез имейл или чрез публикуване;

- уведомява потребителите, Органа по надзор и третите страни за прекратяването на дейността на своя удостоверяващ орган. Информацията се предоставя чрез имейл или чрез публикуване на сайта на Евротръст;

- прекратява разрешението на всички лица, които имат договорни отношения да извършват дейности, свързани конкретния удостоверяващ орган;

- преди прекратяване на дейността на удостоверяващия орган, в разумен срок, прехвърля задълженията си по поддържане на цялата информация, необходима за предоставяне на доказателства на надеждна страна;

- преди да прекрати дейността, частните ключове, включително резервните копия, биват унищожени или изтеглени от употреба по такъв начин, че личните ключове да не могат да бъдат извлечени;

- при възможност прехвърля дейността си на друг квалифициран доставчик;

- Евротръст прилага мерки за покриване на разходите в случай на банкрут или поради други причини за прекратяване на действието на удостоверяващ орган. В случай, че не е в състояние да покрие разходите сам е предвидил мерки в рамките на приложимото законодателство;

- променя статуса на оперативното удостоверение;

- прекратява издаването нови удостоверения, но продължава да управлява активните удостоверения до края на тяхното действие;

- прави търговски разумни усилия, за да се сведе до минимум нарушаването на интересите на потребителите;

- ERDSP съхранява събраните доказателства за националното законоустановеното време.

Евротръст следи и не допуска издаване на удостоверение за срок, по-дълъг от

валидността на удостоверяващия орган, който го е издал.

6 КОНТРОЛИ НА ТЕХНИЧЕСКА СИГУРНОСТ

6.1 ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА КЛЮЧОВИ ДВОЙКИ

Процедурата по генериране и инсталиране на ключовите двойки на удостоверяващия орган „Evrotrust Services SA“ и на подписващия доказателствата „QERDS SU“ следва процедурите, описани в т. 6 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.2 ЗАЩИТА НА ЧАСТНИ КЛЮЧОВЕ И НА КРИПТОГРАФСКИЯ МОДУЛ

Евротръст има изградени контроли за сигурност за управлението на всички криптографски ключове и криптографски устройства през целия им жизнен цикъл.

Евротръст, в качеството си на доставчик на QERDS генерира квалифицирано удостоверение за електронен печат, което използва за дейността си по предоставяне на QERDS. Частният ключ на удостоверението за електронен печат се съхраняват във физически изолирано помещение и единствено оторизиран доверен персонал има достъп до ключовете. Частният ключ се съхранява и използва в рамките на сигурна среда за извършване на криптографски операции. Този ключ се архивира, съхранява и възстановява само от служители с доверени роли във физически обезопасена среда. Броят на персонала оправомощен да изпълнява тази функция, се свеждат до минимум и съответства на практиката на QERDS. Частният ключ за подпечатване от QERDS, съхраняван в сигурна защитена среда на ERDSP и не се извежда извън нея в незащитен вид.

QERDSP използва съвременни протоколи и алгоритми за криптиране на пренасяните данни.

6.3 ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА КЛЮЧОВИТЕ ДВОЙКИ

Процедурата по управление на ключовите двойки на удостоверяващия орган „Evrotrust Services SA“ и на подписващия доказателствата „QERDS SU“ е описана в т. 6.2 на документа

„Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.4 ДАННИ ЗА АКТИВИРАНЕ

Процедурата по активиране на ключовите двойки на удостоверяващия орган „Evrotrust Services SA“ и на подписващия доказателствата „QERDS SU“ е описана в т. 6.2 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.5 КОМПЮТЪРНА СИГУРНОСТ

Процедурата по сигурност на компютърните системи е описана в т. 6.5 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.6 СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА

Процедурата по сигурност на компютърните системи е описана в т. 6.6 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.6.1 ОЦЕНКА НА УЯЗВИМОСТТА НА ИНФОРМАЦИОННАТА СИСТЕМА

Евротръст класифицира и поддържа регистри на всички активи в съответствие с изискванията на ISO/IEC 27001. Съгласно Политиката по сигурност на Евротръст се извършва анализ на оценката за уязвимост по всички вътрешни процедури, приложения и информационни системи. Изисквания за анализ могат, също така, да бъдат определени от външна институция, упълномощена да извършва одит на Евротръст.

Анализът на дейностите и надзорът на изпълнението на всички процедури се извършва редовно от упълномощени лица на Евротръст или автоматично от системите за сигурност на всички информационни и комуникационни устройства на Евротръст. Оценката на уязвимостта се извършва въз основа на анализа на дневниците, събитията в областта на сигурността и други важни данни.

6.7 МРЕЖОВА СИГУРНОСТ

Процедурата за мрежова сигурност е описана в т. 6.7 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

Евротръст изпълнява и следните специфични изисквания:

- следи изискванията за капацитет;
- прогнозира бъдещи изисквания за капацитет, които да гарантират наличието на адекватна мощност и съхранение на процесорите;
- използва най-съвременните протоколи и алгоритми за криптиране на ниво транспортен слой;
- използва удостоверения за уебсайтове за сигурност на транспортния слой, в случаите, когато данните се изпращат извън вътрешните мрежи.

7 ПРОФИЛИ НА УДОСТОВЕРЕНИЯ, CRL И OCSP

7.1 ПРОФИЛ НА БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT“

Профил на Базовия удостоверяващ орган има в документа: „Практика при предоставяне на квалифицирани удостоверителни услуги“

7.2 ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES CA“

„Evrotrust Services CA“ с OID: 1.3.6.1.4.1.47272.2.14 е удостоверяващ орган на квалифицирана услуга за електронна препоръчана поща, който удостоверява генерираните доказателства по настоящата политика.

Version	V3	
Serial number	38 00 00 00 07 58 f6 72 2b 87 3d 45 0d 00 00 00 00 00 07	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC

	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	10 July 2019, 12:50:59 UTC	
Valid to	10 July 2029, 13:00:59 UTC	
Subject	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
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	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=servicesca@evrotrust.com URL= http://www.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	
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0	

Thumbprint (SHA1): 7448b95dc14ff7127af731c580e0d6ca74f3fe10

Thumbprint

(SHA256):

5c7ac0f5ada82e251b4cb8d701a43a4a5baf369289d4f29e27ab2690a88162ec

7.3 ПРОФИЛ НА УСЛУГА ЗА ВАЛИДИРАНЕ НА СТАТУС НА УДОСТОВЕРЕНИЯ „EVROTRUST SERVICES OCSP“

Квалифицираното удостоверение за квалифициран електронен печат на „Evrotrust Services OCSP“ е:

Version	V3	
Serial number	1e 80 a0 58 1d 28 ed 88 a9 f6 3c a2 a7 5f ec 99 66 d8 4b e2	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	13 July 2019, 15:32:03 UTC	
Validit to	11 July 2024, 15:32:03 UTC	
Subject	CN=	Evrotrust Services OCSP
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.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://services.evrotrust.com/ocsp	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.14.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
OCSP Revocation Checking	No	NULL (05 00)

Extended Usage	Key	OCSP Signing (1.3.6.1.5.5.7.3.9)
CRL Points	Distribution	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.crl
Subject Identifier	Key	85 16 bd dc e2 1e 90 80 c0 66 9a 92 db 28 7d a9 dd 7f 76 14
Basic (critical)	Constrains	Subject Type=End Entity Path Length Constraint=None
Key Usage (critical)		Digital Signature, Non-Repudiation (c0)

Thumbprint (SHA1): b791d5fcd076c1c3722b7ee17b7b16ba2cff9e00

Thumbprint (SHA256):

49f0685953e721a913494bb825833f0ef9e250d6516f0f6f338a790fec1b9e29

7.4 ПРОФИЛ НА CRL НА „EVROTRUST SERVICES CA“

Списъкът със спрени и прекратени удостоверения (CRL) на удостоверяващия орган на квалифицираната услуга за електронна препоръчана поща „Evrotrust Services CA“ има следния профил:

Version	V2	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
CRL Number	[пореден номер на CRL]	
ExpiredCertsOnCRL	[начална дата за включена информация за прекратен статус на удостоверения с изтекъл срок на действие]	

7.5 ПРОФИЛ НА „EVROTRUST QERDS SU“

„Evrotrust QERDS SU“ е квалифицирано удостоверение за квалифициран електронен печат на квалифицираната услуга за електронна препоръчана поща. Чрез него електронно се подписват доказателствата, чрез използване на модул за подписване/signing unit (SU), които се издават съгласно настоящата политика. Квалифицираното удостоверение за електронен печат на „Evrotrust QERDS SU“ е:

Version	V3	
Serial number	37 4a c1 13 27 89 ce e2 b6 0e 7d 35 34 fc bf 4b b0 73 56 8b	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	13 July 2019, 15:36:24 UTC	
Valid to	11 July 2024, 15:36:24 UTC	
Subject	CN=	Evrotrust QERDS SU
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://services.evrotrust.com/EvrotrustServicesCA.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://services.evrotrust.com/ocsp	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	

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- QcSSCD (oid=0.4.0.1862.1.4)	
	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
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.crl	
Subject Key Identifier	43 d9 b3 d7 d8 ae fd a8 75 5a cf b8 60 33 ef 6d b4 51 86 3e	
Basic Constrains (critical)	Subject Type=End Entity Path Length Constraint=None	
Key Usage (critical)	Digital Signature, Non-Repudiation (c0)	

Thumbprint (SHA1): *fda618da1eff89e74409aef09e780ba3473ce0c3*

Thumbprint (SHA256):

0479822a7d7985a1aa159090d5948aede330866f16eb50db3c2c94651c3fd7a4

8 ОДИТ НА СЪОТВЕТСТВИЕТО И ДРУГА ОЦЕНКА

Процедурата по извършване на одит на съответствието е описана в т. 8 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.1 ЗАСТРАХОВКА

Евротръст сключва задължителна застраховка на дейността си като квалифициран доставчик на удостоверителни услуги.

9 ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ

9.1 ЦЕНИ

Евротръст поддържа документ „Ценова тарифа за предоставяни удостоверителни, информационни, криптографски и консултантски услуги“ на интернет страницата си: <https://www.evrotrust.com>.

9.2 ФИНАНСОВА ОТГОВОРНОСТ

Евротръст е финансово отговорен пред клиенти на QERDS, които разчитат на неговата дейност. Финансовата отговорност се отнася само, ако щетите са по вина на Евротръст или на страните, с които е сключил споразумение. Ако Евротръст потвърди и приеме, че са настъпили вреди, той се ангажира да плати щетите. Максималната граница на плащане не надвишава размера на щетите.

Финансовата отговорност на всяко лице, участник в дейността по предоставяне и ползване на QERDS се посочва, чрез взаимни споразумения.

9.3 НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ

Евротръст е регистриран като администратор на лични данни по реда на Закона за защита на лични данни.

В качеството си на администратор на лични данни, Евротръст строго съблюдава изискванията за поверителност и неразпространение на личните данни на физическите и юридически лица, станали му известни при изпълнение на дейността му като квалифициран доставчик на удостоверителни услуги.

1) Дружеството използва в своята дейност:

- единствено информация за дейността и бизнеса на клиентите и партньорите си, която е необходима за предоставянето на QERDS;
- конфиденциална информация като търговски, финансови и технически документи (софтуер, анализи, таблици, данни, проучвания, цени, договори и други документи).

2) Евротръст информира своите служители:

- със задължението, че интереса на дружеството трябва да бъде приоритет пред личните интереси и че служителите трябва да направят всичко възможно за да избягват причиняването на щети;
- относно разпоредбите на Закона за защита на личните данни и европейското законодателството в областта на защитата на личните данни, както и мерките, и процедурите за защита на личните данни в дружеството;
- че всички данни и информация, които се дефинират като търговска тайна, трябва да бъдат внимателно съхранявани, за да се предпазят от разкриване без изричното разрешение на доставчика;
- че те са задължени да събират лични данни, независимо от етническата принадлежност на лицето, за което се отнасят, и независимо от тяхната форма и местоположение. Дължни са да предпазят данните от умишлено или случайно унищожаване, заличаване, предаване на трети страни или друга обработка на такива данни;
- обработката на лични данни (събиране, съхранение, модификация, предаване, заличаване и всяка обработка във връзка с тях) е разрешена само в случаите, когато за обработването съществува правно основание в съответствие със националното законодателство, уреждащо защитата на личните данни и че всяка друга обработка е незаконна;
- неоторизираното разкриване на поверителна информация е в основата на прекратяването на сътрудничеството;
- издаването и неоправданото придобиване на професионална тайна представлява престъпление;
- злоупотребата с лични данни представлява престъпление.

9.4 ПРАВТА НА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

Различни данни, включени в оперираната от Евротръст QERDS система са обект на права върху интелектуалната собственост и други имуществени и неимуществени права.

9.5 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ

9.5.1 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТРЪСТ

Евротръст гарантира, че осъществява дейността си като:

- спазва точно условията в настоящия документ, изискванията на Регламент (ЕС) № 910/2014 и националното законодателство;
- предоставената услуга QERDS не нарушава авторските права и лицензирани права на трети страни;
- използва техническо оборудване и технологии, които осигуряват надеждност на системите и техническата и криптографска сигурност при осъществяване на процесите, в това число и сигурен и защитен механизъм/устройство за генериране на ключове в своята инфраструктура;
- предоставя QERDS след като провери с допустими от закона средства предоставената информация;
- сигурно съхранява и поддържа информация, свързана с предоставяната QERDS и оперативната работа на системите;
- спазва установените процедури за работа и правила за технически и физически контрол, в съответствие с условията в настоящата Политика и „Практика при предоставяне на квалифицирани удостоверителни услуги“;
- осигурява условия за точно определяне на времето на изпращане и получаване на данни;
- изпълнява процедури по идентификация и установяване на автентичност на физически и юридически лица или на упълномощени представители на юридически лица;
- взема незабавни мерки при възникване на технически проблеми във връзка със сигурността;
- информира клиентите за техните задължения и дължимата грижа на поведение при използването на предоставяната от Евротръст удостоверителна услуга QERDS;
- използва и съхранява събраната лична и друга информация само за целите на своята дейност в съответствие с националното законодателство;
- поддържа разполагаеми средства, които осигуряват възможност за извършване на дейността му;

- сключва застраховка за времето на своята дейност;
- поддържа доверен персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността;
- поддържа Публичен регистър, в който публикува електронни документи, свързани с дейността си;
- осигурява постоянен достъп до Публичния регистър по електронен път (24/7/365);
- осигурява защита срещу внасяне на промени в поддържания Публичен регистър от нерегламентиран и неправомерен достъп или поради случайно събитие;
- извършва периодични вътрешни одити на дейността на Удостоверяващия орган и Регистриращия орган;
- извършва външни одити от независими одитори и публикува на сайта си резултатите от проверката;
- използва в дейността си сертифициран софтуер и хардуер, както и сигурни и надеждни технологични системи;
- поддържа на сайта на Евротръст списък с Регистриращи органи, списък с препоръчителен софтуер и хардуер за използване от клиентите, бланки, формуляри, типов Договор и други документи в полза на клиентите;
- осигурява максимален достъп до своите услуги (365/24/7), с изключение на следните случаи:
 - планирани и предварително обявени технически ремонти по инфраструктурата;
 - непланирани технически ремонти по инфраструктурата в резултат на непредвидени повреди;
 - техническо обслужване, дължащо се на повреди по инфраструктурата извън юрисдикцията на доставчика;
 - недостъпност на услугата в резултат на непреодолима сила или извънредни събития.
- обявява поддържането или модернизирането на инфраструктурата си най-малко три (3) дни преди началото на ремонта.

Евротръст носи отговорност пред клиентите за причинени вреди от груба небрежност

или умисъл:

- от неизпълнение на изискванията от Регламент (ЕС) № 910/2014 при осъществяване на дейността си по предоставяне на QERDS;
- от неспазване на задълженията си по предоставяне на QERDS;
- от пропуски в установяване на първоначалната самоличност/идентичност на клиентите.

9.5.2 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН

Евротръст гарантира, че Регистриращия орган изпълнява своите функции и задължения в пълно съответствие с условията в този документ, с изискванията и процедурите в Политиката и издадените вътрешни оперативни инструкции.

Евротръст отговаря за действията на Регистриращия орган в инфраструктурата си.

Евротръст гарантира, че Регистриращия орган:

- изпълнява своята дейност, като използва надеждни и сигурни устройства и софтуер;
- предоставя услуги, които са в съответствие със националното законодателство и не нарушава авторските права и лицензирани права на клиентите;
- полага нужните усилия, за да извършва при необходимост правилна идентификация на клиентите.

9.5.3 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ (ИЗПРАЩАЧИ И ПОЛУЧАТЕЛИ)

Физическите и юридически лица имат следните задължения:

- да се запознаят и да спазват условията на Договора, Общите условия, Политиките и Практиките при използване на QERDS, както и изискванията в останалите документи, публикувани в Публичния регистър на Евротръст;
- да използват квалифицираната електронна препоръчана поща само за законни цели и в съответствие с указаната за нея Политика и практика;
- да одобряват условията, посочени в Договора между тях и Евротръст.

9.5.4 ДЪЛЖИМА ГРИЖА НА ДОВЕРЯВАЩА СЕ СТРАНА

Доверяващата се страна следва да положи дължима грижа, която е описана в т. 9.6.4 на документа: „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.6 ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ

Евротръст не носи отговорност за щети, произтичащи от:

- използване на QERDS извън пределите на вписаните в нея предназначения и ограничения на нейното действие;
- незаконни действия от страна на клиенти;
- случайни събития, имащи характера на непреодолима сила, включително злоумишлени действия на трети лица (хакерски атаки, отнемане на устройството за използване на електронна препоръчана поща, на начина на идентифициране и др.);
- използване на електронна препоръчана поща в несъответствие с изискванията и процедурите на Политиката и практиката на Евротръст;
- лошо качество и функционалност на софтуерните продукти и хардуерни устройства използвани от клиентите;
- неправилна и неадекватна защита с парола;
- издаване на поверителни данни и безотговорно поведение на клиентите;
- повреди в инфраструктурата, която не е в областта на управление на Евротръст;
- неадекватно поведение на клиентите при използване на услугата QERDS.

9.7 ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА

За предоставяната квалифицирана услуга за електронна препоръчана поща, Евротръст поставя ограничение на отговорността в рамките на 5 000 евро.

9.8 СРОК И ПРЕКРАТЯВАНЕ НА ПОЛИТИКАТА И ПРАКТИКАТА

Настоящият документ влиза в сила от момента на неговото одобрение от Борда на

директорите на Евротръст и публикуването му в Публичния му регистър на Евротръст. Допълнения към този Политиката и практиката влизат в сила след публикуването им.

Разпоредбите в настоящия документ са валидни до издаване и публикуване на следваща версия на „Политика и практика при предоставяне на квалифицирана услуга за електронна препоръчана поща“ на сайта на Евротръст.

С прекратяване на дейността на Евротръст, се прекратява актуалността на Политиката и практиката, както и на съдържащи се в този документ разпоредби.

Доставчикът съхранява надлежно и сигурно всички предишни версии/редакции на този документ.

9.9 ИНДИВИДУАЛНИ СЪОБЩЕНИЯ И СЪОБЩЕНИЯ С УЧАСТНИЦИТЕ

Лицата, посочени в настоящата Политика и практика могат да извършват изявления и да обменят информация с помощта на обикновена поща, електронна поща, факс, телефон и мрежови протоколи (например TCP/IP, HTTP), както и чрез мобилното приложение на Евротръст.

Изборът на средствата може да бъде избран в зависимост от типа на информацията и начина на използване на услугата.

9.10 ИЗМЕНЕНИЯ НА ПОЛИКИТА И ПРАКТИКАТА

Измененията в настоящия документ може да бъдат резултат от наблюдавани грешки, актуализации и предложения от засегнатите страни. В случай на недействителна клауза от Политиката и Практиката, валидността на целия документ се запазва и не се нарушава договора с потребителя. Недействителната клауза се замества със законосъобразна норма.

Евротръст може да прави редакционни промени в този документ, които не засягат съдържанието на правата и задълженията в него. В случаи на промени в Политиката и практиката обектния идентификатор на документа (OID) се запазва и не се променя. Промени, които водят до нова версия на документа се публикуват на интернет страницата на Евротръст.

9.11 РАЗРЕШАВАНЕ НА СПОРОВЕ

Спорове или жалби относно използване на QERDS, предоставяна от Евротръст, се решават чрез посредничество въз основа на писмено подадена информация. Жалбите се разглеждат от юриста на Евротръст. Жалбоподателят получава отговор в рамките на 2 (два) работни дни след подаване на жалбата. В случай, че не се намери решение на спора в рамките на 30 (тридесет) дни от началото на процедурата по споразумение, страните могат да предадат решаването на спора от българския съд.

9.12 ПРИЛОЖИМО ПРАВО

За всички въпроси, неуредени в настоящия документ се прилагат разпоредбите на българското законодателство.

9.13 СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО

Евротръст гарантира, че услугата работи по правен и надежден начин. Тя се предлага в съответствие с приложимите законови изисквания. За всички въпроси, неуредени в настоящия документ се прилагат разпоредбите на българското законодателство. В случай, че националното законодателство се променя, то до хармонизирането на настоящата политика важат законовите правила.

Евротръст гарантира, че личните данни се обработват в съответствие с РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните/GDPR).

Когато е възможно, услугата за електронна препоръчана поща и продуктите на крайните клиенти, използвани при предоставянето на услугата, са достъпни за хора с увреждания.

9.14 ОБЩИ РАЗПОРЕДБИ

Задълженията и отговорността на потребителите и Евротръст се уреждат чрез договорни споразумения. Отношенията с доверяващи се страни се уреждат по реда на общото деликтно право. Договорите за предоставяне на квалифицирани услуги за електронна препоръчана поща следва да бъдат сключвани в писмена или електронна форма, при спазване на разпоредбите на Регламент (ЕС) № 910/2014, РЕГЛАМЕНТ (ЕС) 2016/679 и приложимото законодателство в Република България.

9.15 ДРУГИ РАЗПОРЕДБИ

Практиката не посочва никакви други разпоредби.

Настоящият документ е публикуван на уебсайта на Евротръст в интернет на български и английски език. В случай на несъответствие между текстовете на български и английски език, приоритет има българския текст.