# НАРЪЧНИК ЗА ПОТРЕБИТЕЛЯ
# ПРИ ПРЕДОСТАВЯНЕ НА
# УДОСТОВЕРИТЕЛНИ УСЛУГИ

**Версия: 1.1**

## СЪДЪРЖАНИЕ

## I. ОБЩИ ПОЛОЖЕНИЯ

1. Наръчник на потребителя

Настоящият Наръчник за потребителя (Наръчника) съдържа Практиката при предоставяне на удостоверителни услуги (“Certification Practice Statement”, “CPS”) и Политиката за предоставяне на удостоверителни услуги (“Certificate Policy”, “CP”), разработени и поддържани от “ЕВРОТРЪСТ ТЕХНОЛЪДЖИС” АД (по-надолу за краткост “ЕВРОТРЪСТ” или “Доставчика”) и определя правилата, съгласно които дружеството осъществява дейността си на доставчик на удостоверителни услуги.

2. Нормативно съответствие

Наръчникът за потребителя е разработен съгласно изискванията на действащото законодателство и на общоприетите препоръки, спецификации и стандарти за предоставяне на удстоверителни услуги.

Наръчникът за потребителя има характер на общи условия за предоставяне на удостоверителни услуги от ЕВРОТРЪСТ. Той може да бъде променян по всяко време при спазване изискванията на действащото законодателство. Всяка нова редакция се публикува на уебсайта на ЕВРОТРЪСТ.

3. Използвани термини и съкращения

а) На български език

| | |
|---|---|
| **Автор** | Авторът (“Signatory”) е физическото лице, което в електронното изявление се сочи като негов извършител. Авторът е физическо лице, което осъществява от името на Титуляря (там където е наличен) електронни изявления и ги подписва, в съответствие с предоставената му представителна власт и е посочено в издаденото удостоверение като такъв. |
| **Доверяващи се лица** | Доверяващи се лица (“Relying Parties”) са физически или юридически лица-адресати на електронни изявления, подписани с електронни подписи, за които има издадени удостоверения за електронен подпис от ЕВРОТРЪСТ или на преобразувана електронна информация или данни, посредством PKI технологии, базирани на предоставяните от ЕВРОТРЪСТ удостоверителни или други информационни и криптографски услуги |
| **ЕВРОТРЪСТ** | Доставчик на удостоверителни услуги. В настоящия документ - “ЕВРОТРЪСТ технолоджис” АД, осъществяващ дейността си по предоставяне на удостоверителни услуги чрез физически и функционално обособената си вътрешна организационна структура - Звено за |

| | |
|---|---|
| | удостоверителни услуги. |
| **ЕГН** | Единен граждански номер |
| **Електронен подпис, ЕП** | Всяка информация в електронна форма, добавена или логически свързана с електронното изявление, за установяване на неговото авторство |
| **ЗУУ** | Звено за удостоверителни услуги |
| **ИАБСА** | Изпълнителна агенция "Българска служба за акредитация" |
| **ЗЕДЕП** | Закон за електронния документ и електронния подпис |
| **Квалифициран електронен подпис, КЕП** | Квалифициран електронен подпис е усъвършенстван електронен подпис, който:<br>1. е придружен от издадено от ЕВРОТРЪСТ удостоверение за квалифициран електронен подпис, отговарящо на изискванията на чл. 24 от ЗЕДЕП и удостоверяващо връзката между Автора и публичния ключ за проверка на подписа, и<br>2. е създаден посредством устройство за сигурно създаване на подписа.<br>КЕП има значението на саморъчен подпис. |
| **КРС** | Комисия за регулиране на съобщенията |
| **МОЛ** | Материално отговорно лице |
| **НДЕВРОТРЪСТ** | Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията при предоставяне на удостоверителни услуги |
| **НИАСПКЕП** | Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис |
| **Наръчник** | Наръчник за потребителя за предоставяните от ЕВРОТРЪСТ удостоверителни, информационни, криптографски и консултантски услуги<br>Наръчникът има характер на общи условия и обединява следните документи:<br>1. Практика при предоставяне на удостоверителни услуги (“Certification Practice Statement”, “CPS”) и<br>2. Политика за предоставяне на удостоверителни услуги (“Certificate Policy”, “CP”) |
| **ПИН** | Персонален идентификационен номер |
| **Практика** | Практика при предоставяне на удостоверителни услуги е документ-неделима част от Наръчника за потребителя, съдържащ правила относно издаване, спиране, възобновяване и прекратяване действието на удостоверенията, условията за предоставянето на достъп до удостоверенията. |
| **Политика** | Политика за предоставяне на удостоверителни услуги е документ, |

| | |
|---|---|
| | неделима част от Наръчника за потребителя, описващ политиката, която доставчикът следва при издаване на удостоверения, както и за всички предоставяни услуги |
| **Регистриращ Орган, РО** | Регистриращ орган (“Registration Authority”, “RA”) е обособено подзвено на ЗУУ в структурата на ЕВРОТРЪСТ, което осъществява дейностите по: приемане, проверка, одобряване или отхвърляне на искания за издаване на удостоверения, регистриране на подадените искания до Удостоверяващия орган за издаване и внасяне на промени в статуса на удостоверения, осъществяване на съответни проверки за установяване на самоличността, съответно идентичността на Титуляря и автора, както и на специфични данни за тях, с допустимите от закона средства и в съответствие с Политиката и Практиката при предоставяне на съответната удостоверителна услуга, уведомяване на Удостоверяващият орган за издаване удостоверение след успешна идентификация и сключване на договори за предоставяне на удостоверителни услуги с титулярите, от името на доставчика.<br>Регистриращият орган може да бъде обособено подзвено в рамките на доставчика (ЕВРОТРЪСТ-РО или “RA”) или да бъде юридическо лице, различно от доставчика, на което са делегирани права да осъществява дейностите по предоставяне на удостоверителни услуги от името на доставчика съгласно действащия Наръчник. |
| **Титуляр** | Титулярът (“Signature Owner”) е физическо или юридическо лице, от името, на което се осъществяват подписвани електронни изявления. Титулярът може да е посочен в издаденото удостоверение за електронен подпис като такъв |
| **Удостоверение за време** | Удостоверението за време (“Time Stamp Certificate”) е подписан от ЕВРОТРЪСТ електронен документ, който съдържа минимум:<br>1. идентификатора на политиката за издаване на удостоверения за време, съдържаща се в Наръчника на потребителя;<br>2. представения на ЕВРОТРЪСТ електронен подпис на подписания електронен документ;<br>3. идентификаторите на алгоритмите, използвани за създаването на електронния подпис;<br>4. времето на представяне на електронния подпис;<br>5. уникалния идентификационен номер на удостоверението за време;<br>6. удостоверението за квалифицирания електронен подпис на ЕВРОТРЪСТ, или съответна препратка към него. |
| **Удостоверение за квалифициран** | Удостоверението за КЕП е електронен документ, издаден и подписан от ЕВРОТРЪСТ, който съдържа: |

| | |
|---|---|
| **електронен подпис, Удостоверение за КЕП** | 1. указание, че удостоверението е издадено за квалифициран електронен подпис;<br>2. наименованието и адреса на доставчика ЕВРОТРЪСТ;<br>3. името или псевдонима на Автора на електронния подпис;<br>4. особени атрибути, свързани с Автора, когато удостоверението се издава за конкретна цел, както и когато ЕВРОТРЪСТ поддържа политика за издаване на удостоверения с вписване на такива атрибути;<br>5. публичния ключ, съответстващ на държания от автора частен ключ за създаване на квалифицирания електронен подпис;<br>6. усъвършенстваният електронен подпис на ЕВРОТРЪСТ;<br>7. срока на действие на удостоверението;<br>8. ограниченията на действието на подписа по отношение на целите и/или на стойността на сделките, когато удостоверението е издадено с ограничения на удостоверителното действие;<br>9. уникалния идентификационен код на удостоверението; |
| **Удостоверение за усъвършенстван електронен подпис** | Удостоверението е подписан от ЕВРОТРЪСТ електронен документ, съдържащ определени от закона реквизити, удостоверяващ връзката между автора и публичния му ключ за проверка на подписани документи и обекти, и предоставящ възможност за установяване идентичността на Титуляря и автора, а при провеждане на съответна политика от ЕВРОТРЪСТ – и тяхната самоличност. |
| **Удостоверяващ Орган, УО** | Удостоверяващ орган (“Certification Authority”, “CA”) е обособено подзвено на ЗУУ в структурата на ЕВРОТРЪСТ, което осъществява дейностите по предоставяне на удостоверителни услуги. Удостоверяващият орган няма самостоятелна правосубектност и всички осъществени действия и актове на служителите му се извършват в качеството им на служители на ЕВРОТРЪСТ, в рамките на предоставените им правомощия |
| **Усъвършенстван електронен подпис, УЕП** | Усъвършенстван електронен подпис е електронен подпис, който:<br>1. дава възможност за идентифициране на Автора;<br>2. е свързан по уникален начин с Автора;<br>3. е създаден със средства, които са под контрола единствено на Автора, и<br>4. е свързан с електронното изявление по начин, който осигурява установяването на всякакви последващи промени |
| **УУ** | Удостоверителни услуги |

б) На английски език

| | |
|---|---|
| **ASN.1** Abstract Syntax | Абстрактен език за описание на обекти в удостоверенията |

| | |
|---|---|
| Notation One | |
| **A** Actuality | Актуалност |
| **BG** Bulgaria | България |
| **C** Country | Страна |
| **CA** Certification Authority | Удостоверяващ орган |
| **CC** Common Criteria | Общи критерии |
| **CN** Common Name | Публично име |
| **CP** Certificate Policy | Политика за предоставяне на удостоверителни услуги |
| **CSP** Cryptograph Services Provider | Криптографски модул към четящо устройство и смарт карта |
| **CPS** Certification Practice Statement | Практика при предоставяне на удостоверителни услуги |
| **CRL,** Certificate Revocation List | Списък с прекратени удостоверения |
| **DSA,** Digital Signature Algorithm | Вид криптографски алгоритъм за създаване на електронен подпис |
| **DN,** Distinguished Name | Отличително име на субект, вписан удостоверението |
| **E** E-mail | Електронна поща |
| **Enhanced key usage** | Разширени цели за използването на ключа |
| **FIPS,** Federal Information Processing Standard | Федерален стандарт за обработка на информация |
| **HSM,** Hardware Security Module | Хардуерен криптографски модул |
| **ISO,** International Standardization Organization | Международна организация за стандартизация |
| **Issuer** | Издател |
| **IP,** Internet Protocol | Интернет протокол |
| **LDAP,** Lightweight Directory Access Protocol | Протокол за опростен достъп до регистър |
| **L,** Location | Местонахождение |
| **N,** Number | Номер |
| **O,** Organization | Пълното наименование на юридическото лице по регистрация или акт на вписване. |
| **OU,** Organization Unit | Организационна единица, към която субект, вписан в удостоверението е свързан |
| **OID,** Object Identifier | Идентификатор на обект |
| **OCSP,** Online Certificate Status Protocol | Протокол за он-лайн проверка на статуса на удостоверение |
| **PKCS,** Public Key | Криптографски стандарт за пренос на публичен ключ |

| | |
|---|---|
| Cryptography Standards | |
| **PKI,** Public Key Infrastructure | Инфраструктура на публичния ключ е съвкупността от хардуера, софтуера, персонала, документацията в ЕВРОТРЪСТ за създаване, използване, управление и проверка на издавани от последния удостоверения за електронни подписи и удостоверителни услуги, включваща различни звена и лица, участващи в предоставянето и използването на удостоверителни услуги– удостоверяващи органи, регистриращи органи, титуляри, автори и доверяващи се лица. |
| **JSC,** Joint Stock Company | Акционерно дружество |
| **PSE,** Personal Security Environment | Надеждна среда за генериране на двойка ключове при автора |
| **RA,** Registration Authority | Регистриращ орган |
| **RSA,** Rivest-Shamir-Adelman | Вид асиметричен криптографски алгоритъм за създаване на електронен подпис |
| **SSCD,** Secure Signature Creation Device | Устройство за сигурно създаване на подписа със защитен профил |
| **SHA,** Secure Hash Algorithm | Сугурен хеш-алгоритъм за извличане на хеш-идентификатор |
| **SSL,** Secure Socket Layer | Сигурен канал за предаване на данни |
| **SMIME,** Secure Multipurpose Internet Mail Extensions | Протокол за сигурно предаване на електронна поща през Интернет |
| **S** Street | Улица |
| **T** Title | Професионално качество на автора. |
| **URL,** Uniform Resource Locator | Единен ресурсен локатор |

## II ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

1. Общи положения

Практиката при предоставяне на удостоверителни услуги съдържа:

- публичните мерки за сигурност при предоставяне на услугите;
- процедурите при издаване, спиране, възобновяване и прекратяване действието на удостоверения за квалифициран електронен подпис (КЕП), в съответствие с конкретните изисквания на политиките на отделните удостоверения;
- процедури при предоставяне достъп за проверка на удостоверенията.

2. Данни за ЕВРОТРЪСТ

“ЕВРОТРЪСТ ТЕХНОЛЪДЖИС” АД (ЕВРОТРЪСТ) е българско юридическо лице, акционерно дружество,: вписано в Търговския регистър при Агенцията по вписванията под ЕИК 203397356, със седалище и адрес на управление: гр. София, район Изгрев, жк Изток, ул. „Николай Хайтов“ 2, вх. Д, ет. 2

**Адрес за кореспонденция:**
“ЕВРОТРЪСТ ТЕХНОЛЪДЖИС” АД
ул. „Николай Хайтов“ 2, вх. Д, ет. 2
1113 София, България

**Телефони за контакт:**

+ 359 2 971 44 61 – информация
+ 359 2 971 44 61 – регистриращ орган
+ 359 2 971 44 61 – техническа поддръжка

**Уебсайт:**

http://www.evrotrust.com

**Адреси на електронна поща:**

info@evrotrust.com
delovodstvo@evrotrust.com

ЕВРОТРЪСТ е доставчик на удостоверителни услуги, осъществяващ дейността си по предоставяне на удостоверителни и други доверителни услуги чрез специално обособена в рамките на юридическото лице организационно обособено звено.

ЕВРОТРЪСТ е юридическо лице, осъществяващо публични функции по смисъла на Закона за електронното управление. Дейността по издаване и управление на удостоверения и водене на

регистър за тях обхваща:

- издаване на удостоверения за публични ключове съгласно изискванията на закона;
- водене и поддържане на регистър за издадените удостоверения;
- предоставяне на всяко трето лице достъп до регистъра;
- управление на издадените удостоверения, в това число спиране, възобновяване, продължаване и прекратяване на действието на удостоверения;
- предоставяне на услуги по създаване на двойки криптографски ключове - частен и публичен ключ;
- сигурна проверка (валидиране) на електронни подписи, електронни печати и други информационни обекти, за които има издадени удостоверения;
- сигурно съхраняване на частни ключове, електронни подписи и друг криптографски материал.

3. Страни ангажирани при издаване и използване на удостоверение

3.1. Удостоверяващ орган

Функциите на Удостоверяващ орган се извършват от обособено подзвено в организационната структура на ЕВРОТРЪСТ. В рамките на разрешеното от закона, техническото осъществяване на тази дейност може да се възлага на външни лица.

В инфраструктурата на ЕВРОТРЪСТ са обособени следните Удостоверяващи органи:

- Evrotrust RSA Root CA– издава електронни удостоверения на йерархично зависими в инфраструктурно отношение Удостоверяващи органи в домейна „Evrotrust“;
- Evrotrust RSA Operational CA – издава потребителски електронни удостоверения за електронни подписи и електронни печати, съгласно Политиката за предоставяне на удостоверителни услуги;
- Evrotrust TSA – издава потребителски електронни удостоверения за време.

3.2. Регистриращ орган

Функциите на Регистриращ орган се извършват от обособено подзвено в организационната структура на ЕВРОТРЪСТ. В рамките на разрешеното от закона, на външни лица може да се възлага на осъществяването на следните функции:

- проверка на идентичност и самоличност на авторите и титулярите при искания за издаване на електронни удостоверения;
- удостоверяване валидността на подадена електронна заявка за удостоверение;
- иницииране и предаване на Удостоверяващия орган искания за спиране, възобновяване или прекратяване на издадени удостоверения;
- извършване на одобрение на заявки за продължаване действието на удостоверения от името на ЕВРОТРЪСТ.

Функциите на Регистриращ орган се извършват от обособено подзвено в организационната структура на ЕВРОТРЪСТ или от юридически лица, с които ЕВРОТРЪСТ влиза в договорни

отношения, при спазване на всички условия на Практиката при предоставяне на удостоверителни услуги и Политиката за предоставяне на удостоверителни услуги.

### **3.3.** Титуляр

Титуляр на електронното изявление е физическото или юридическото лице, от името на което е извършено електронното изявление. Може да бъде вписано като такъв в удостоверението за КЕП, когато е необходимо за неговите цели и ако ЕВРОТРЪСТ поддържа съответната политика.

### **3.4.** Автор

Автор на електронното изявление е физическото лице, което в изявлението се сочи като негов извършител.

Авторът е физическо лице, което осъществява от името на Титуляря, когато такъв е вписан в удостоверението, електронни изявления и ги подписва, в съответствие с предоставената му представителна власт. Средствата за създаване на електронния подпис са под контрола единствено на Автора и само той има право на достъп до частния ключ за подписване на електронни изявления.

### **3.5.** Адресати

Адресат на електронното изявление може да бъде лице, което по силата на закон е длъжно да получава електронни изявления или за което въз основа на недвусмислени обстоятелства може да се смята, че се е съгласило да получи изявлението в електронна форма.

Адресатът на електронно изявление, придружено с удостоверение за квалифициран електронен подпис (КЕП) на Автора, следва да се довери и да приеме, че подписът има правна стойност на саморъчен, след като е проверил всички обстоятелства относно валидността на подписа съгласно правилата посочени в този Наръчник.

Доверяващи се страни са физически или юридически лица – адресати на електронни изявления, подписани с електронни подписи, за които има издадени удостоверения за електронен подпис от ЕВРОТРЪСТ.

### **3.6.** Използване на удостоверение за квалифициран електронен подпис

Удостоверението за КЕП се използва при идентифициране на Автора, в случаи като подписване на електронни документи и осъществяване на електронни транзакции, достъп до информационни системи или криптиране на информация.

### **3.7.** Съдържание на удостоверение за квалифициран електронен подпис

Удостоверение за КЕП, издадено и подписано от ЕВРОТРЪСТ, съдържа следните минимални атрибути:

- указание, че удостоверението е издадено за квалифициран електронен подпис;
- наименованието и адреса на ЕВРОТРЪСТ и указание, че е регистриран в Република България;

- името или алтеренативно - псевдонима на автора на електронния подпис;
- особени атрибути, свързани с автора, когато удостоверението се издава за конкретна цел, доколкото ЕВРОТРЪСТ поддържа политика за издаване на удостоверения с вписване на такива атрибути (личен идентификатор, идентификатор за професионална принадлежност, друга информация)
- публичния ключ, съответстващ на държания от автора частен ключ за създаване на квалифицирания електронен подпис;
- КЕП на ЕВРОТРЪСТ;
- срок на действие на удостоверението;
- дата и час на издаването;
- ограниченията на действието на подписа по отношение на целите и/или на стойността на сделките, ако удостоверението е издадено с ограничения на удостоверителното действие;
- уникалния идентификационен код (серийния номер) на удостоверението;
- идентификатор на алгоритъма за създаване на електронния подпис и на допустимостта на използваните хеш-алгоритми.

Съдържанието на всяко конкретно удостоверение се описва от неговия профил. Информация за профилите на издаваните от ЕВРОТРЪСТ удостоверения има в настоящия документ в съответната политика на издаване, по-долу.

### **3.8.** Приложение на удостоверение за КЕП

Според спецификацията X.509, удостоверението и кореспондиращата с него двойка частен-публичен ключ могат да имат различни приложения, част от които са:

- създаване на електронен подпис (Digital Signature) – за установяване на авторството на електронни изявления, ненарушимост на интегритета на подписания електронен документ и съгласието на автора с извършеното изявление;
- неотменимост (Non-repudiation) – за юридическо привързване на електронния подпис към извършеното изявление и невъзможността за отмяна на волята на Автора след полагането на подписа;
- криптиране на ключове (Key encipherment) – за криптиране при размяна на ключове използвани за шифриране на данни;

Приложението на всяко конкретно удостоверение, издавано от ЕВРОТРЪСТ, е описано в съответната политика, по-долу.

### **3.9.** Използване на удостоверение извън зададените му ограничения

Когато удостоверението е издадено с вписани ограничения по отношение на приложението си или стойността на транзакциите, то не може да се използва извън рамките на тези ограничения. Такъв електронен подпис загубва стойността си на квалифициран и ЕВРОТРЪСТ не отговаря за такава употреба.

## 4. Общи положения

### 4.3. Права и задължения

#### 4.3.1. Права и задължения на ЕВРОТРЪСТ

ЕВРОТРЪСТ е уведомило Комисия за регулиране на съобщенията (КРС) за започване на дейността си по предоставяне на удостоверителни услуги, в съответствие с изискванията на действащото законодателство.

Еротръст е предоставило на КРС изискваните данни за задължителни обстоятелства, подлежащи на вписване в регистъра по чл. 38, ал. 4 от ЗЕДЕП, съгласно който Комисията води публичен регистър на всички доставчици, установили се на територията на Република България, които са я уведомили за започване на дейността си по чл. 19, ал. 1 и за акредитираните доставчици.

ЕВРОТРЪСТ има следните задължения:

- да издава удостоверение по искане на всяко лице, като предварително го информира дали е акредитиран;
- да информира лицата, желаещи да им бъде издадено удостоверение, за условията за издаване и използване на удостоверението, включително за ограниченията на неговото действие, както и за процедурите за подаване на жалби и за решаване на спорове;
- когато издава удостоверения, да проверява чрез допустимите средства самоличността, съответно идентичността, на Автора и на Титуляря на КЕП и ако е необходимо – други данни за тези лица, включени в удостоверението;
- да публикува издаденото удостоверение, така че трети лица да имат достъп до него съгласно указанията на Автора, съответно на Титуляря;
- да не съхранява или копира данни за създаване на частни ключове;
- да предприема незабавни действия във връзка със спирането, възобновяването и прекратяването на действието на удостоверението при установяване на съответните основания за това;
- незабавно да уведомява Автора и Титуляря за обстоятелства относно валидността или надеждността на издаденото удостоверение;
- да уведомява Автора, съответно Титуляря и всички заинтересовани страни за своята акредитация при предоставяне на удостоверения и УУ;
- да спазва своите вътрешни и публични политики и процедури;
- да спазва приложимото законодателство.

#### 4.3.2. Задължения на Автора и Титуляря

Авторът и Титулярят, посочени в удостоверения за КЕП, издадени от ЕВРОТРЪСТ, имат следните задължения:

- да са запознати и да спазват условията и правилата при предоставяне на удостоверителни услуги от ЕВРОТРЪСТ, съдържащи се в настоящия документ и останалите документи публикувани в електронния регистър;

- да предоставят вярна, точна и пълна информация, която ЕВРОТРЪСТ изисква съгласно нормативните изисквания и този документ и съответните политики, при подаване на заявки за издаване и управление на удостоверения;
- да генерират двойката ключове използвайки сигурен метод и алгоритъм, съобразно изискванията на Наредба за изискванията към алгоритмите за създаване и проверка на ЕВРОТРЪСТ;
- да проверят пълнотата и верността на съдържанието на DN (предоставената от него информация за удостоверяване). В случай на несъответствие между представената информация и съдържанието да уведомят незабавно ЕВРОТРЪСТ;
- да преустановят използването на удостоверението в случай на съмнение за компрометиране на частния ключ и да подадат заявка за неговото спиране в ЕВРОТРЪСТ;
- да преустановят използването на удостоверението в случай на загуба или компрометиране на частния ключ на издадено удостоверение и незабавно да уведомят ЕВРОТРЪСТ за настъпилите обстоятелства;
- да преустановят използването на удостоверението при наличие на остаряла, променена, неточна и/или невярна информация, включена в издадено удостоверение и да подадат заявка за прекратяване действието на удостоверението;
- да сменят своя ПИН за достъп до устройството за сигурно създаване на подписа (Secure Signature Creation Device, SSCD) , където се съхранява частния ключ преди да използва удостоверението;
- да предприемат необходимите предпазни мерки за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неразрешено използване на частния ключ, кореспондиращ на публичния ключ, който е публикуван в удостоверението;
- да използват издаденото от ЕВРОТРЪСТ удостоверение само за законни цели и в съответствие на политиката и практиката за предоставяне на удостоверителни услуги.

### 4.3.3. Дължима грижа на доверяващата се страна

Дължимата грижа на доверяващата се страна се изразява в извършване на надлежна проверка на предназначението и валидността на удостоверението, което съпровожда електронния подпис върху електронното изявление на Автора, а от там и на електронния подпис.

За да провери валидността на удостоверението и на електронния подпис, Доверяващата се страна е длъжна:

- да направи справка в списъците с прекратени удостоверения (CRL), публикувани в електронния регистър на ЕВРОТРЪСТ съгласно правилата от настоящия документ;
- да провери дали издаденото удостоверение не е изтекъл срок на валидност;
- да провери дали подписът, придружен от удостоверението не е използван цели и за стойност на транзакциите, извън вписаните в удостоверението лимити;

- да направи справка за валидност на цялата верига от удостоверения до базовото удостоверение на ЕВРОТРЪСТ.
- че дължината на използваните ключове отговаря на изискванията за сигурност на Доверяващата се страна;
- че удостоверението е било валидно към момента на създаване на електронния подпис под конкретното подписано удостоверение.

Проверката за предназначението на удостоверението се извършва по следните данни, съдържащи се в профила на удостоверението за КЕП:

- политика, в съответствие на която се издава и управлява удостоверение за КЕП, посочена в поле “Certificate Policies”;
- предназначението и ограниченията на действието на удостоверението за КЕП, описани в поле “Key Usage” и “ExtendedKey Usage”;
- данни за Автора, респективно Титуляря на удостоверението за КЕП, посочени в поле “Subject”.

ЕВРОТРЪСТ не носи отговорност за настъпили вреди за Доверяващата се страна вследствие на неизвършване на описаните проверки или доверяване на електронен подпис, придружен от удостоверение за нужди на доверяващата се страна извън политиките, при които удостоверението е издадено, извън ограниченията и цели, вписани в него или при установяване на невалидност на подписа или удостоверението.

### 4.4. Отговорност

#### 4.4.1. Отговорност на ЕВРОТРЪСТ

ЕВРОТРЪСТ отговаря пред Автора, съответно пред Титуляря на КЕП и пред всички трети лица за причинените вреди от груба небрежност или умисъл:

- от неизпълнение на изискванията по чл. 21 и на задълженията по чл. 22 и 25 от ЗЕДЕП при осъществяване на дейността си по предоставяне на удостоверителни услуги;;
- от неверни или липсващи данни в удостоверението към момента на издаването му;
- които са им причинени в случай, че по време на издаването на удостоверението лицето, посочено като Автор, не е разполагало с частния ключ, съответстващ на публичния ключ;
- от алгоритмичното несъответствие между частния ключ и публичния ключ, вписван в удостоверението.

ЕВРОТРЪСТ носи отговорност всички процедури по предоставяне на удостоверителни услуги да се изпълняват в съответствие с правилата в „Практика при предоставяне на удостоверителни услуги“ и „Политика за предоставяне на удостоверителни услуги“.

#### 4.4.2. Освобождаване от отговорност

ЕВРОТРЪСТ не носи отговорност в случаите, когато настъпилите вреди са следствие от неполагане на дълкжима грижа, неизпълнение на задълженията или липса на познания в областта

на PKI технологиите от страна на Авторите, Титулярите или Доверяващите се страни.

ЕВРОТРЪСТ не носи отговорност и в случаи на вреди причинени от:

- използване на удостоверение извън пределите на вписаните в него предназначения и ограничения на неговото действие по отношение на целите за използване и ограничения за стойността на трансакциите;
- незаконни действия от страна на Титуляря, Автора и трети страни;
- използване на удостоверение, който не е издадено или използвано в съответствие с изискванията и процедурите на „Практика при предоставяне на удостоверителни услуги" и „Политика за предоставяне на удостоверителни услуги";
- използване на невалидно удостоверение – удостоверение, което е спряно, прекратено или с изтекъл срок на валидност;
- несвоевременно прекратяване или спиране на удостоверение, което е следствие от забавена от страна на Титуляря или Автора заявка или поради причини извън контрола на ЕВРОТРЪСТ (природни бедствия, аварии и всякакви събития, причинени от непреодолима сила или случайни събития);
- компрометиран частен ключ, кореспондиращ на публичния ключ в удостоверението;
- качеството и функционалност на софтуерните продукти и хардуерни устройства използувани от Автора, Титуляря и Доверяващи се страни.

### 4.4.3. Отговорност на Автора

Авторът отговаря спрямо третите лица ако:

- при създаването на двойката частен-публичен ключ е използвал алгоритъм, който не отговаря на изискванията на Наредбата за изискванията към алгоритмите за създаване и проверка на квалифицирания електронен подпис;
- не изпълнява точно изискванията за сигурност, определени от ЕВРОТРЪСТ;
- не поиска от ЕВРОТРЪСТ прекратяване действието на удостоверението, когато е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерното му използване;
- е извършил неверни изявления, направени пред ЕВРОТРЪСТ и имащи отношение към съдържанието или към издаването на удостоверението;

Когато удостоверението е издадено с вписан Титуляр, той отговаря за неизпълнението от страна на Автора на задълженията му.

### 4.4.4. Отговорност на Титуляря и на Автора към ЕВРОТРЪСТ

Авторът, съответно Титулярят, отговаря спрямо ЕВРОТРЪСТ, ако Авторът е предоставил неверни данни, съответно е премълчал данни, имащи отношение към съдържанието или към издаването на удостоверението, и когато не е държал частния ключ, съответстващ на посочения в удостоверението публичен ключ.

### 4.5. Електронен регистър

#### 4.5.1. Публикувани удостоверения и списъци

Съгласно изискванията на дйстващото законодателство, ЕВРОТРЪСТ води електронен регистър, в който публикува:

- базовото си удостоверение (Evrotrust RSA Root CA);
- оперативните удостоверения на Удостоверяващите органи (Evrotrust RSA Operational CA);
- всички издадени от ЕВРОТРЪСТ удостоверения;
- списъкът на прекратените и временно спрени удостоверения (CRL), издадени от ЕВРОТРЪСТ;
- удостоверенията за време;

#### 4.5.2. Публикувана информация

ЕВРОТРЪСТ публикува в електронния си регистър и информация за:

- условията и реда за издаване на удостоверение, включително за правилата за установяване идентичността на Титуляря на КЕП;
- процедурите за сигурност при издаване и управление на удостоверения за КЕП;
- начина на използване на КЕП;
- условията и реда за използване на КЕП, включително изискванията за съхраняване на частния ключ;
- условията за достъп до удостоверението и начина на проверка на КЕП;
- цената за получаване и използване на удостоверение, както и цените на останалите предоставяни услуги;
- отговорността на ЕВРОТРЪСТ и на Титуляря на КЕП;
- условията и реда, по които Авторът, съответно Титулярят прави искане за прекратяване действието на КЕП.
-

#### 4.5.3. Достъп до информацията в електронния регистър

ЕВРОТРЪСТ предлага директорийни услуги за информацията съхранявана в електронния регистър, като осигурява X.500, HTTP/HTTPS и OCS1P базиран достъп.

Електронният регистър е публичен и ЕВРОТРЪСТ не може да ограничава достъпа до информацията в него, освен по писмено искане на Автора и само по отношение на негово валидно издадено удостоверение.

Информацията публикувана в електронния регистър на ЕВРОТРЪСТ е достъпна постоянно, освен в случаите на събития, извън контрола на Доставчика и при настъпили събития вследствие на непреодолима сила.

#### 4.5.4. Актуализация на информацията в регистъра

Издадените от ЕВРОТРЪСТ удостоверения се публикуват в електронния регистър веднага

след тяхното подписване на Удостоверяващия орган.

Актуализирането на списъците на действащите и прекратените удостоверения за КЕП се извършва през интервал от 3 /три/ часа. Списъците се публикуват веднага след всяка актуализация.

Публикуването на изменени ревизии на "Наръчника за потребителя" се осъществява съгласно вътрешните правила и процедури на ЕВРОТРЪСТ.

### 4.6. Защита на личните данни

Личните данни на Титуляря и Автора на удостоверение, които се събират в процеса на заявяване, издаване и управление на удостоверение и не се съдържат в издавания удостоверение са конфиденциални. Информацията се съхранява в бази данни на ЕВРОТРЪСТ и не се предоставя на трети лица без изричното писмено съгласие на Титуляря съответно Автора, освен в предвидените от закона случаи.

ЕВРОТРЪСТ възприема като конфиденциална и информацията, която се съдържа в:

- договора за удостоверителни услуги;
- заявките за издаване на удостоверение;
- журналите от оперативната дейност на информационните системи на ЕВРОТРЪСТ;
- записи за извършени плащания;
- вътрешни правила и процедури от системата за информационна сигурност на ЕВРОТРЪСТ;
- планове за действие при непредвидени случаи и възстановяване след бедствия.

### 4.7. Публична информация

Личните данни за Титуляря и Автора, които се съдържат в полетата на издаваните удостоверения са публични.

При сключване на договор за предоставяне на удостоверителни услуги с ЕВРОТРЪСТ, Титулярът и Авторът се съгласяват личните данни, необходими за издаването на удостоверението да бъдат достъпни за трети лица чрез публикуването им в електронния регистър на доставчика.

Общодостъпна е и всяка информация, съдържаща се в електронния регистър по отношение на:

- издадените от ЕВРОТРЪСТ удостоверения;
- списъците с прекратените удостоверения;
- Наръчника за потребителя;
- други документи като правила за използване на КЕП, цени на предоставяните от ЕВРОТРЪСТ услуги и др.

### 4.8. Разкриване на информация

Събираната и съхранявана конфиденциална информация от ЕВРОТРЪСТ, може да бъде разкривана в следните случаи:

- Титуляр или Автор на удостоверение могат да дадат писмено съгласие на ЕВРОТРЪСТ

да бъдат предоставени на трети страни техни лични данни, събрани в процеса на издаване и управление на удостоверението;

- пред лица и организации, които по силата на правомощия дадени им от закона имат право на достъп до съответната информация.

### 4.9. Права на интелектуалната собственост

ЕВРОТРЪСТ притежава правата на интелектуална собственост върху издаваните удостоверения и публикуваните списъци с прекратени удостоверения. На Титулярите и Авторите се предоставя възможност да използват и възпроизвеждат предоставените им удостоверения при условие че:

- се запазва цялостта на информацията, съдържаща се в удостоверението;
- удостоверенията се използват според приложението им, описано в политиката на ЕВРОТРЪСТ по издаването им.

ЕВРОТРЪСТ притежава правата на интелектуална собственост върху документе „Политика за предоставяне на удостоверителни услуги“ и „Практика при предоставяне на удостоверителни услуги“, публикувани в електронния регистър на доставчика и образуващи „Наръчник за потребителя“.

ЕВРОТРЪСТ си запазва всички права върху притежавани търговските марки и имена, съдържащи се в полетата на издадените удостоверения.

Титулярите/Авторите си запазват всички права върху притежавани търговски марки и имена съдържащи се в полетата на издадените удостоверения.

Титулярът/Авторът притежава правата върху двойката частен-публичен ключ, която кореспондира с издаденото удостоверение.

Титулярът/Авторът притежава правата върху средствата за активиране на частния ключ.

### 4.10. Прекратяване на дейността

В случай, че желае ЕВРОТРЪСТ преустанови дейността си на ЕВРОТРЪСТ, той ще уведоми КРС и потребителите си своевременно за своето намерение. Преди да прекрати своята дейност и да прехвърли отговорностите си по поддръжката на архивите на приемните страни, ЕВРОТРЪСТ изпълнява следната процедура:

- уведомява писмено КРС и потребителите на неговите УУ, които имат валидни удостоверения за КЕП за намеренията си, най-късно 4 (четири) месеца преди датата на прекратяване на дейността си;
- предава цялата си документация, свързана с дейността по предоставяне на УУ на друг доставчик, на когото прехвърля тази дейност или на КРС, в случай че не реализира прехвърляне;
- полага необходимата грижа, за да осигури продължаване на действието на издадените от него удостоверения;
- уведомява потребителите относно условията по поддръжка на прехвърлените техни удостоверения към Доставчика-приемник и неговото име;

- в случай че прехвърля дейността си на друг доставчик, ЕВРОТРЪСТ предоставя правото на приемника да използва инфраструктурата на публичния ключ на ЕВРОТРЪСТ, с оглед управление на вече издадените удостоверения за КЕП, за срок не по-дълъг от 6(шест) месеца;

или

- прекратява всички удостоверения за КЕП, които все още са валидни в края на четиримесечния период от време, в случай че дейността няма да бъде прехвърлена на друг доставчик;
- извършва всички необходими действия за съхранение на архивите на електронните и хартиени регистри в съответствие с нормативните изисквания, в случай че дейността няма да бъде прехвърлена на друг доставчик.

## 5. Идентификация и удостоверяване на достоверност на информацията

Електронната идентификация на Автор, съответно Титуляр на издадено от ЕВРОТРЪСТ удостоверение, се вписва в полето “Subject”.

Информацията за Автора/Титуляря, която се предоставя подписана от заявителя или от упълномощен представител при регистрация на първоначално искане за издаване на удостоверение и която се проверява в Регистриращия орган въз основа на представените документи и със законово допустими средства за справка, е базата за формиране на полето "Subject" в удостоверението.

Серийният номер (SerialNumber) на всяко издадено удостоверение е уникален в домейна на ЕВРОТРЪСТ.

Информацията от полето за серийния номер съвместно с тази от полето Issuer, е гаранция за уникалност на издаденото удостоверение в публичен домейн.

### 5.1. Уникалност и използване на имена

Удостоверенията на базовия и удостоверяващите органи на ЕВРОТРЪСТ съдържат уникални имена с общоразбираема семантика, което позволява еднозначното определяне на идентичността на ЕВРОТРЪСТ, като субект на удостоверението.

Удостоверенията за КЕП на клиентите на ЕВРОТРЪСТ могат да съдържат имена, съвпадащи с установените имена/псевдоними на Авторите и идентифицираните имена на Титулярите - субекти на вече издадени удостоверения.

#### 5.1.1. Типове имена

Името и белезите, по които се индивидуализират Автора, съответно Титуляря когато е вписан, в съответните полета за всеки тип удостоверение се формират съобразно препоръки X.500 и политиките за издаване на съответният тип удостоверение за КЕП, включително отдалечено.

#### 5.1.2. Правила за вписване на имената

Удостоверенията съдържат имената на Авторите - субекти на издадените удостоверения.

ЕВРОТРЪСТ не гарантира, че имената записани в полето Subject за даден Автор/Титуляр са уникални, доколкото може да има повече от едно лице с едно и също име. Уникалната

идентификация на вписаните в удостоверенията лица се осъществява посредством съвкупност от вписани в удостоверенията атрибути (адрес на електронна поща, телефонен номер, уникален индентификатор (ако лицето е избрало да се вписва такъв), професионален идентификатор и др.).

ЕВРОТРЪСТ допуска издаване на повече от едно удостоверение с една и съща стойност във всички подполета на цялото поле Subject, когато се издава повече от едно удостоверение на едно и също лице.

#### 5.1.3. Правила за интерпретация на имената

Полето за обичайно име (Common Name, CN) съдържа име на физическото, съответно наименование на юридическото лице, с което то е обичайно обозначавано в дейността му. Когато не е избрано вписване на обичайно име, в полето се вписва пълното името на физическото лице, ако такова е вписвано в удостоверението или алтернативно - псевдонима, ако такъв е избран от Автора за вписване в удостоверението, вместо име. Когато удостоверението се издава на юридическо лице и не е избрано обичайно име, в полето се вписва наименованието на юридическото лице.

#### 5.1.4. Процедура по решаване на спор за използване на имена

Титулярите и Авторите нямат право да заявяват издаване на удостоверение с използване на имена, които нарушават чужди имуществени или неимуществени права.

ЕВРОТРЪСТ не носи отговорност, когато използвани имена в удостоверение, нарушават чужди права върху търговско име, търговска марка, домейни, авторски права и др.

В случай на възникнал спор по отношение на използвани имена, ЕВРОТРЪСТ си запазва правото да не издаде удостоверение или едностранно и без предизвестие да прекрати договора за поддържане на такова.

### 5.2. Идентификация и проверка за самоличност на физическо лице

Установяването и проверката на самоличността на физическото лице – Автор, Титуляр или представител на Автора или Титуляря, се осъществява от Регистриращия орган или чрез отдалечена проверка, включително автоматизирано.

За установяване и проверка на самоличността на физическо лице се изисква то да представи документ за самоличност. Когато същото е овластено от Автора/Титуляря или е законен представител на Титуляря - следва да представи и документ, доказващ представителната власт или овластяване. В случаите на правоприемство, физическото лице следва да представи документ, с който да удостовери качеството си на правоприемник. Тези проверки могат да се правят автоматизирано, при наличие на технологично решение за това.

Физическото лице, което заявява издаване на удостоверение или извършва действия по управление на издадено удостоверение, надлежно попълва и предава на ЕВРОТРЪСТ доказателства и данни, в съответствие с политиките на ЕВРОТРЪСТ за издаване и управление на различните типове удостоверения. Попълнените документи съдържат данни за лицето, в това число данни за контакт, адрес по местоживеене и адрес за електронна поща. Физическото лице потвърждава достоверността на данните в попълнените документи, чрез:

- саморъчно поставен подпис върху документите пред упълномощен служител на Регистриращия орган, в случай на лично предаване на документите;
- нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;
- подписване на приложените електронни документите с валидно удостоверение за КЕП по смисъла на ЗЕДЕП;
- подписване с усъвършенстван електронен подпис на документите чрез съответно мобилно или друго приложение и след извършена надлежна идентификация на физическото лице – заявител и юридическото лице – титуляр, от служител на ЕВРОТРЪСТ.

ЕВРОТРЪСТ извършва проверки за достоверността на информацията в попълнените документи, с всички законово позволени средства и във всички публични регистри.

Списък с изискуемите документи за физическо лице при издаване и управление на удостоверение се поддържа на уеб-сайта на ЕВРОТРЪСТ и от специализирано приложение.

При наличие на технологична и организационна готовност, ЕВРОТРЪСТ осигурява набавянето на необходимите документи и друга информация, необходима за издаването и управлението на удостоверение, в качеството му на лице, осъществяване публични функции по реда на Закона за електронното управление, за което с подаването на заявлението се счита, че заявителят е дал съгласие.

### **5.3.** Идентифициране на юридическо лице

Установяване на идентичността на българско юридическо лице – Титуляр, се осъществява от Регистриращия орган чрез автоматизирана проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ по реда на Закона за електронното управление. За български юридически лица, които не са търговци, както и за чуждестранни юридически лица, за които не може да се извърши автоматизирана проверка се представят:

- съдебно решение или друг документ, удостоверяващи възникването на юридическото лице;
- документ, удостоверяващ актуалното състояние на лицето;
- Уникален национален идентификатор.

Списък с изискуеми документи се поддържа на уеб-сайта на ЕВРОТРЪСТ и в специализираните приложения за достъп до услугите. След заснемане на Копия от всички изискуеми документи остават в архива на ЕВРОТРЪСТ.

Лицето представляващо юридическото лице удостоверява достоверността на информацията, която се съдържа в документи чрез:

- Заверка „Вярно с оригинала“ и саморъчен подпис върху документите пред упълномощен служител на Регистриращия орган, в случай на лично предаване на документите;
- нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;

- подписване на приложените електронни формати на документите с валидно удостоверение за КЕП;
- подписване с усъвършенстван електронен подпис на документите чрез съответно мобилно или друго приложение и след извършена надлежна идентификация на физическото лице – заявител (автор) и юридическото лице – титуляр, от служител на ЕВРОТРЪСТ и наличието на представителната власт на заявителя спрямо титуляря.

ЕВРОТРЪСТ извършва проверки за достоверността на информацията в попълнените документи, като това включва:

- справка при нотариус;
- справка в публични електронни регистри;
- справка от съдебни и административни органи.

**5.4.** Проверка за притежаването на частния ключ

За издаването или продължаване на удостоверение е необходимо ЕВРОТРЪСТ да получи електронна заявка във формат PKCS#10. Спецификацията на този формат на заявка за издаване на удостоверение изисква заявката да бъде подписана от Автора, притежаващ частния ключ.

ЕВРОТРЪСТ извършва проверка на валидността на електронния подпис придружаващ заявката. Проверката на валидността на подписа се извършва в съответствие с чл. 17 от ЗЕДЕП.

Установяването на валидност на поставения електронен подпис е достатъчно основание да се счита, че Авторът подал електронната заявка, притежава частния ключ, който е технически годен и кореспондира на публичния ключ, съдържащ се в заявката.

С помощта на разработен в ЕВРОТРЪСТ специализиран софтуерен продукт, се прави проверка за притежанието на частния ключ и в случаите, когато Авторът изтегля издадено или продължено удостоверение отдалечено. Механизмът на проверката се основава на електронно подписване на документи. Проверката на валидността на подписите и в този случай се извършва в съответствие с чл.17 от ЗЕДЕП и НЕВРОТРЪСТ.

ЕВРОТРЪСТ може да предоставя услугата по генериране на двойката ключове на автора.

**5.5.** Потвърждаване на представителна власт

В случай, че заявката за издаване или управление на удостоверение не е подадена от Автора и е налице овластяване, се изисква нотариално заверено пълномощно от Титуляря, с което упълномощеното лице получава правото:

- да представлява Титуляря, респ. Автора пред ЕВРОТРЪСТ във връзка с дейността на последното като доставчик на удостоверителни услуги;
- да извърши всички необходими действия за издаване и управление на удостоверение за квалифициран електронен подпис по смисъла на чл.24 и чл.33 от ЗЕДЕП.

При наличие на регистър на овластяванията, упълномощаването може да се извърши и чрез нарочно вписване. В този случай нотариална заверка не се изисква.

**5.6.** Идентификация и установяване на достоверност на информацията при подмяна на

двойката частен-публичен ключ

Подмяна на двойката частен-публичен ключ може да се извърши в случаи, че Авторът/Титулярят желае да продължи действието на удостоверението и подаде заявка за това преди изтичането на срока му на валидност. В такива случай, ЕВРОТРЪСТ препоръчва да се генерира нова двойка ключове, с цел да се избегне риска от компрометиране на старата двойка.

Заявката може да се подаде по електронен път, подписана с квалифициран електронен подпис. Когато заявката се подава пред Регистриращ орган, процедурата по идентификация и установяване на самоличност става по реда за издаване на удостоверение.

### 5.7. Идентификация и установяване на достоверност на информацията при заявка за прекратяване на удостоверение

В съответствие с чл. 27, ал.2 от ЗЕДЕП, ЕВРОТРЪСТ е се уверява в самоличността и представителната власт на лицето, което заявява прекратяването на удостоверение.

За установяване на самоличността на лицето заявило прекратяване на удостоверение се прилагат правилата описани в Наръчника.

## 6. Оперативни правила при издаване и управление на удостоверенията

### 6.1. Подаване на заявка за издаване на удостоверение

Заявка (искане) за издаване на удостоверение може да се подаде:

- всяко физическо лице, което желае да подписва електронни документи от свое име;
- всяко лице (Автор), което ще подписва от името на друго физическо или юридическо лице (Титуляр), след като докаже представителната си власт спрямо Титуляря. Представителната власт не се доказва, когато произтича от закон. В този случай ЕВРОТРЪСТ осъществява автоматизирани проверки за наличието й от съответните публични регистри, по реда на Закона за елекронното управление.

Заявката се подава в писмена форма, когато е пред Регистриращ орган. Заявката може да се подаде в електронна форма пред интернет-страницата на ЕВРОТРЪСТ или чрез съответно софтуерно приложение. В този случай писмената форма се смята спазена на основание чл. 3, ал. 2 ЗЕДЕП.

Въз основа на подадената заявка се сключва договор за удостоверителни услуги, при наличие на следните предпоставки:

- надлежно попълнени данни и представитени документи, в съответствие с Политиката на ЕВРОТРЪСТ за издаване на конкретното удостоверение. Изискуемата информация трябва да е точна, пълна и вярна;
- генерирани от Автора двойка ключове, при съблюдава изискванията за сигурност, регламентирани в закона и политиката на ЕВРОТРЪСТ за издаване на съответното удостоверение;
- предоставяне от страна на Автора на ЕВРОТРЪСТ на публичния му ключ, чрез електронна заявка във формат PKCS#10;

- установяване на алготритмично съответствие на частния ключ с публичния ключ.

### 6.2. Издаване на удостоверение

#### 6.2.1. Условия за издаване на удостоверение

ЕВРОТРЪСТ издава удостоверението, когато:

- информацията относно Автора и Титуляря, когато такъв е вписан, предоставена за включване в удостоверението, е вярна и пълна;
- частния ключ се държи от Автора, технически е годен да бъде използван за създаване на КЕП и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен КЕП е създаден със съответния му частен ключ.

#### 6.2.2. Ред за подаване на заявка за издаване на удостоверение

Редът за подаване на заявка за издаване на удостоверение от ЕВРОТРЪСТ и процедурата по издаване са описани в политиката за издаване и управление на конкретния тип удостоверение, която е част от „Политика за предоставяне на удостоверителни услуги“.

#### 6.2.3. Издаване на удостоверение

ЕВРОТРЪСТ издава незабавно удостоверението посредством публикуването му в регистъра на удостоверенията.

### 6.3. Приемане на удостоверение

Авторът, съответно Титулярят, може да възрази, ако издаденото удостоверение съдържа грешки или непълноти, в 3 (тридневен) срок от публикуването му в регистъра. ЕВРОТРЪСТ ги отстранява чрез издаване на ново удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на неверни данни. При липса на възражение се смята, че съдържанието на удостоверението е прието.

Правилата в настоящата точка са в сила както при издаване на удостоверение така и при подновяване на удостоверение.

### 6.4. Спиране на удостоверение

#### 6.4.1. Основания за спиране на удостоверение

ЕВРОТРЪСТ спира действието на издадено удостоверение за необходимия според обстоятелствата срок, но за не повече от 48 часа от момента на спирането, ако съществува основание да се предполага, че действието на удостоверението трябва да бъде спряно.

ЕВРОТРЪСТ приема за основания за спиране:

- изгубено/откраднато устройство за сигурно създаване на подписа, когато частният ключ е записан на такова устройство (Secure Signature Creation Device, SSCD);
- напуснал служител (Автора), когато удостоверението му е издадено по искане на Титуляря в качеството му на служител и за осъществяване на функции, присъщи на съответната длъжност;
- промяна на представителната власт на Автора спрямо Титуляря, когато

удостоверението е издадено с вписан Титуляр;

- промяна на трудовото правоотношение между Автора и Титуляря, когато удостоверението е издадено с вписан Титуляр;
- прекратяване на професионалната правоспособност на лицето, когато същата е удостоверена в издаденото удостоверение;
- смяна на идентифициращи данни на Автора, съответно на Титуляря в удостоверението;
- съмнение, че частният ключ е компрометиран;
- други.

При възможност проверките на горните обстоятелства може да се извършва автоматимизирано по реда на Закона за електронното управление (смърт, поставяне под запрещение, прекратяване на законово представителство между Автора и Титуляря, прекратяване на трудовото правоотношение между тях, прекратяване на професионалната правоспособност на Автора и др.).

#### 6.4.2. Заявяване на спиране на удостоверение

ЕВРОТРЪСТ спира действието на издадено от него удостоверение за необходимия според обстоятелствата срок, но за не повече от 48 часа от момента на спирането:

- по искане на Титуляря или Автора, без да е длъжен да се увери в самоличността или представителната му власт;
- по искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, член на семейството и други;
- по искане на КРС;

При непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона, председателя на КРС може да задължи ЕВРОТРЪСТ да спре действието на удостоверението за необходимия според обстоятелствата срок, но за не повече от 48 часа от момента на спирането.

#### 6.4.3. Ред за подаване на заявка за спиране на удостоверение

Редът за подаване на заявка за спиране на издадено от ЕВРОТРЪСТ удостоверение е описан в кореспондираща му политиката за издаване и управление, която е част от „Политика за предоставяне на удостоверителни услуги“.

Спирането на действието на удостоверение се реализира чрез включването му в списъка с прекратени удостоверения и публикуване на актуализирания списък в електронния регистър на доставчика, съгласно Секция 2.4.

#### 6.4.4. Уведомяване на Титуляря и Автора

ЕВРОТРЪСТ незабавно уведомява Титуляря и Автора за спиране на действието на удостоверението.

### 6.5. Възобновяване на удостоверение

#### 6.5.1. Основание за възобновяване на удостоверение

Действието на спряно удостоверение се възобновява:

- с изтичане на максималния срок на спиране от 48 часа, ако междувременно не е постъпила заявка за прекратяване на удостоверението;
- преди изтичане на максималния срок на спиране от 48 часа, ако междувременно е отпаднало основанието за спиране, или Авторът/Титулярът подаде искане за възобновяване, след като ЕВРОТРЪСТ или Комисията за регулиране на съобщенията се е уверил/а, че Авторът/Титулярът е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.

#### 6.5.2. Заявяване на възобновяване на удостоверение

Титулярът/Авторът на удостоверението могат да подават заявка за възобновяване на спряно удостоверение.

#### 6.5.3. Ред за подаване на заявка за възобновяване на удостоверение

Редът за подаване на заявка за възобновяване на спряно удостоверение е описан в кореспондираща му политиката за издаване и управление, която е част от „Политика за предоставяне на удостоверителни услуги“.

### 6.6. Подновяване на удостоверение

Удостоверения, които не са прекратени, могат да бъдат подновени преди изтичане на срока им на валидност без да е необходимо генериране на нова двойка ключове.

При подновяване на удостоверение е възможно да се прегенерира двойката частен-публичен ключ („re-key“) или удостоверението да бъде издадено за съществуващата към момента двойка („renew“).

ЕВРОТРЪСТ като доставчик на удостоверителни услуги препоръчва да се запазва първоначалната двойка ключове само при първо заявяване за подновяване, с цел да се намали риска от компрометирането на ключовете.

#### 6.6.1. Условия за подновяване на удостоверение

Удостоверение издадено от ЕВРОТРЪСТ може да бъде подновено в случай че:

- няма промяна в първоначално предоставената информация за Титуляря и Автора, удостоверена с действащото към момента удостоверение;
- срокът на валидност на удостоверението не е изтекъл;
- удостоверението не е прекратено;
- има подадена заявка за подновяване не по-рано от 30 /тридесет/ дни и не по-късно от 10 /десет/ дни преди изтичане срока на валидност на действащото удостоверение;
- заплатена е цената за подновяване.

Ако някое от условията изредени по-горе не е изпълнено, се следват:

- спиране на текущото удостоверение и поставянето му в CRL със статус HOLD в рамките регламентираните 48 часа до изясняване и отстраняване на несъответствията;
- правилата за издаване на ново удостоверение съгласно този Наръчник.

#### 6.6.2. Подаване на заявка за подновяване на удостоверение

Авторът, съответно Титулярът на удостоверението или надлежно овластено лице, могат да подават заявка за подновяване на удостоверение.

#### 6.6.3. Ред на подаване на заявка за подновяване на удостоверение

Редът за подаване на заявка за подновяване на издадено от ЕВРОТРЪСТ удостоверение и процедурата по подновяване са описани в политиката за издаване и управление на конкретния тип удостоверение, която е част от „Политика за предоставяне на удостоверителни услуги“.

Кореспондиращата политика съдържа и описание на процедурата за подновяване на удостоверението.

### 6.7. Прекратяване действието на удостоверение

#### 6.7.1. Основание за прекратяване на удостоверение

Действието на удостоверение се прекратява:

- с изтичане на срокът му на валидност и при неподадена заявка за подновяване;
- при прекратяване на юридическото лице на ЕВРОТРЪСТ, без прехвърляне на дейността на друг доставчик на удостоверителни услуги.

ЕВРОТРЪСТ е длъжен да прекрати действието на удостоверение по искане на Титуляря/Автора след като се увери в самоличността и представителната власт на Титуляря, съответно на Автора.

ЕВРОТРЪСТ прекратява действието на удостоверение при:

- смърт или поставяне под запрещение на Титуляря/Автора;
- прекратяване на юридическото лице на Титуляря;
- прекратяване на представителната власт на Автора по отношение на Титуляря;
- прекратяване на трудовото правоотношение между Автора и Титуляря;
- прекратяване на професионалната правоспособност на лицето, когато същата е удостоверена в издаденото удостоверение;
- установяване, че удостоверението е издадено въз основа на неверни данни.

При установяване чрез автоматизирани проверки настъпването на фактите, които са основание за прекратяване и удостоверението е било спряно на това основание и след уведомяване на Титуляря и Автора, не е поискано възобновяване.

#### 6.7.2. Заявяване на прекратяване на удостоверение

Титулярът/Авторът, техни универсални правоприемници или надлежно овластени лица могат да подадат заявка за прекратяване на удостоверение.

### 6.7.3. Ред за подаване на заявка за прекратяване на удостоверение

Редът за подаване на заявка за прекратяване на издадено от ЕВРОТРЪСТ удостоверение и процедурата по прекратяване са описани в политиката за издаване и управление на съответния тип удостоверение, която е част от „Политика за предоставяне на удостоверителни услуги“.

### 6.8. Проверка в списъка на прекратени удостоверения

ЕВРОТРЪСТ поддържа и актуализира на всеки 3 (три) часа публичен списък на прекратените и спрени удостоверения (CRL, Certificate Revocation List). За тази цел ЕВРОТРЪСТ публикува данните от удостоверенията и CRL в собствен, достъпен за всеки електронен архив. Достъпът до архива се извършва по протокол LDAP (Lightweight Directory Application Protocol).

Всяка доверяваща се страна е необходимо да направи проверка на статуса на удостоверението в Списъка на прекратените удостоверения всеки път, когато и предстои да вземе решение дали да се довери на електронния подпис, придружен с издадено от ЕВРОТРЪСТ удостоверение. ЕВРОТРЪСТ не носи отговорност за настъпили вреди за доверяващите се страни при липса на извършена проверка на статуса на удостоверенията.

Списъка с прекратените удостоверения е достъпен 24 часа в денонощието на следния адрес: **http://www.evrotrust.com.**

### 6.9. Онлайн проверка на статуса на удостоверение (OCSP)

ЕВРОТРЪСТ предоставя за ползване възможността за проверка на статуса на издадените удостоверения в реално време, като използва необходимата техника и технологии. Тази услуга позволява на Доверяващите се лица да получават информация за статуса на удостоверението към в реално време.

За онлайн проверка на данни от регистъра е необходимо използуването на подходящ софтуер (OCSP-клиент или интеграция със специализирано приложение).

## 7. Удостоверения за време

Удостоверението за време е подписан от ЕВРОТРЪСТ формализиран електронен документ, който съдържа идентификатора на политиката за издаване на удостоверения за време, представения електронен подпис на подписания електронния документ, идентификатор на алгоритмите за създаване на електронния подпис, времето на представяне на електронния подпис, уникалния идентификационен номер на удостоверението за време и удостоверението за квалифициран електронен подпис на ЕВРОТРЪСТ.

Удостоверението за време се издава на физически и на юридически лица, които са Автори на подписани електронни изявления или са доверяваща се страна спрямо използваните УЕП.

## 8. Профил на издаваните удостоверения и на Списъка с прекратени

**удостоверения (CRL)**

### 8.1. Профил на издаваните удостоверения

Удостоверенията издавани от ЕВРОТРЪСТ са в съответствие с:

- ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework;
- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Издадените удостоверения съдържат задължително основните полета описани в таблицата по-долу:

| | |
|---|---|
| Serial Number | Сериен номер на удостоверението |
| Signature Algorithm | Алгоритъм използван при подписване на удостоверението от Доставчика на удостоверителни услуги |
| Issuer | Данни за ЕВРОТРЪСТ |
| Valid From | Дата, от която е валидно удостоверението |
| Valid To | Дата, до която е валидно удостоверението |
| Subject DN | Данни за Автора и Титуляря на удостоверението (ако има вписан такъв). |
| Subject Public Key | Публичния ключ на Титуляря/Автора |
| Signature | Подпис на ЕВРОТРЪСТ, генериран и кодиран в съответствие с RFC 3280. |

Точното съдържание на профила на всяко конкретно удостоверение се съдържа в политиката, в съответствие с която е издадено.

#### 8.1.1. Версия на издаваните удостоверения

Версията на издаваните от ЕВРОТРЪСТ удостоверения е X.509 Version 3.

#### 8.1.2. Разширения на издаваните удостоверения

Използваният от ЕВРОТРЪСТ X.509 Version 3 формат за издаваните удостоверения позволява дефиниране на разширения и/или ограничения в приложението на удостоверението, в съответствие с възприетия профил. Полета, които дефинират тези разширения и/или ограничения са:

8.1.2.1 “Key Usage” - дефинира целите, за които може да се използва частния ключ за създаване на електронен подпис, в рамките на които подписът ще има правна стойност като такъв. Според препоръки X.509 v3 са възможни следните предназначения на удостоверението:

- Digital Signature (електронен подпис) - за подписване на електронни изявления и доказване на тяхното авторство и интегритет;
- Non-repudiation (неотменяемост) - за доказване на факта на изявлението и съгласието на автора с извършеното изявление към момента на подписването, както и на

невъзможността да се отметне от извършеното изявление.

- Key encipherment (криптиране на ключ) - за криптиранена ключове, както и при обмен на такива през незащитена преносна среда;
- Data encipherment (криптиране на данни) - за криптиранена данни, които се архивират или предават;
- Key Certificate Signing (електронно подписване на удостоверение) - използва се само за подписване на други операционни удостоверения на Удостоверяващи органи на ЕВРОТРЪСТ;
- CRL Signing (електронно подписване на Списък на прекратени удостоверения) - използва се само при удостоверения на Удостоверяващ органи, за подписване на Списъка на прекратените удостоверения.

8.1.2.2 “Certificate Policies” - указва политиките, която доставчикът на удостоверителни услуги е следвал при издаване на съответното удостоверение. Политиката се идентифицира с уникален идентификатор.

8.1.2.3 “Basic Constraints” - дефинира дали издаденото удостоверение е на Удостоверяващ орган на ЕВРОТРЪСТ или е удостоверение на краен потребител.

8.1.2.4 ”Enhanced Key Usage” - указва приложението, политиката на издаване и характера на съответното удостоверение.

### 8.1.3. Алгоритми за създаване и проверка на КЕП

ЕВРОТРЪСТ използва SHA2RSA алгоритъм за подписване на издаваните от него удостоверения, чрез прилагане на:

- хеш-функция – SHA2 (Secure Hash Algorithm);
- алгоритъм за криптиране – RSA (Rivest-Shamir-Adelman).

Издадените от ЕВРОТРЪСТ удостоверения и подписани с алгоритъм SHA2RSA отговарят на изискванията на препоръки RFC3279.

Информация за използвания алгоритъм при подписване на удостоверението се съдържа в поле „Signature Algorithm“ от неговия профил.

### 8.1.4. Форма и ограничения при използване на имена

Имената в полетата на удостоверението се записват в съответствие с изискванията и ограниченията според препоръките X.501.

Прилагат се правилата за използване на имена и разрешаване на конфликти с имена са описани в Секция 8.1.

### 8.1.5. Идентификация на политиките за издаване на удостоверение

На всяка от политиките, в съответствие с които се издават удостоверения от ЕВРОТРЪСТ се присвоява идентификатор на обект (OID – Object Identifier). Идентификаторът на обект е уникална поредица от цели числа.

### 8.2. Профил на списъка с прекратени удостоверения (CRL)

Публикувания от ЕВРОТРЪСТ списък с прекратени удостоверения съответства на изискванията на препоръки RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

#### 8.2.1. CRL профил на базовия удостоверяващ орган Evrotrust RSA Root CA

| | | |
|---|---|---|
| Version | 2 | |
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Effective date | Дата на публикуване на списъка във формат: [dd Month gggg hh:mm:ss] | |
| Next update | Дата към която ще бъде публикувана следващата актуализация на списъка [dd Month gggg hh:mm:ss] | |
| Signature algorithm | SHA256RSA | |
| Authority Key Identifier | KeyID=74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70 | |
| CRL Number | [XXX…] | |
| Next CRL Publish | Day, Month, dd, gggg hh:mm:ss | |
| Revocation List | Списък на прекратените и спрени удостоверение, който съдържа следната информация за всеки от удостоверенията в списъка:<br>сериен номер на удостоверение;<br>дата на прекратяване или спиране. | |

#### 8.2.2. CRL профил на оперативния орган за КЕП - Evrotrust RSA Operational CA

| | | |
|---|---|---|
| Version | 2 | |
| Issuer | CN= | Evrotrust RSA Operational CA |
| | OU= | Qualified Operational CA |
| | O= | Evrotrust Technologies JSC |
| | oganizationIdentifier (2.5.4.97) | NTRBG-203397356 |
| | CN= | BG |
| Effective date | Дата на публикуване на списъка във формат: [dd Month gggg hh:mm:ss] | |
| Next update | Дата към която ще бъде публикувана следващата актуализация на списъка [dd Month gggg hh:mm:ss] | |
| Signature algorithm | SHA256RSA | |

| | |
|---|---|
| Authority Key Identifier | KeyID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08 |
| CRL Number | [XXX…] |
| Next CRL Publish | Day, Month, dd, gggg hh:mm:ss |
| Revocation List | Списък на прекратените и спрени удостоверение, който съдържа следната информация за всеки от удостоверенията в списъка:<br>сериен номер на удостоверение;<br>дата на прекратяване или спиране. |

#### 8.2.3. Версия на профила

Списъкът с прекратени удостоверения (CRL), публикуван в електронния регистър на ЕВРОТРЪСТ е Version 2.

#### 8.2.4. Кодове за прекратяване и спиране на удостоверение

Кодът посочва причината поради която даден удостоверение е поставен в Списъка с прекратени удостоверения (CRL) на ЕВРОТРЪСТ и може да му бъде присвоена някоя от следните стойности:

- “Key Compromised” – компрометиран частен ключ на Автора;
- “CA Compromised” – компрометиран частен ключ на Удостоверяващия орган, с който се подписват удостоверенията на потребителите;
- “Affiliation Changed” – променена връзка между Автора и Титуляря - промяна в дружеството, промяна в представителната власт, отнемане на представителната власт, прекратяване на трудово правоотношение и т.н.;
- “Superseded” – удостоверението е заместено с друго удостоверение;
- “Certificate Hold” – действието на удостоверението е спряно;
- “Unspecified“ – удостоверението е прекратено без посочване на причина, когато е налично валидно искане за прекратяване.

## 9. Мерки за сигурност във връзка с предосавяните услуги

### 9.1. Мерки за физическа сигурност

Защитните мерки предприети по отношение на физическата защита са елемент от разработената и внедрена ЕВРОТРЪСТ система за информационна сигурност, съответстваща на изискванията на стандарта ISO/IEC 27001:2013 и ISO/IEC 19011:2011.

Мерките свързани с физическата защита на данните, системите, 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 ресурсите;
- компрометиране или кражба на информацията или средствата за обработка на информацията.

**9.1.1.** Физически достъп

Системите на ЕВРОТРЪСТ са защитени на няколко нива на физическа сигурност, изискваща първоначален достъп на по-долно ниво преди получаването на достъп до по-високо ниво. За всяко ниво се прилагат прогресивно намаляващи права за достъп. Ключовата дейност на Удостоверяващия орган протича на максимално защитеното ниво.

**9.1.2.** Електрозахранване и вентилация

Структурите на ЕВРОТРЪСТ са оборудвани с основни и резервни захранващи системи, осигуряващи непрекъснато захранване с електрическа енергия, които са защитени срещу външни интервенции

Електрозахранването на всички централни компоненти на инфраструктурата на ЕВРОТРЪСТ е защитено срещу прекъсване на електроснабдяването.

Вентилационната система е специално предназначена за такъв клас помещения, не допускаща компрометиране на физическата и електромагнитната защита на това помещение, както и нормалната работа на инсталираните компютърни компоненти.

**9.1.3.** Мерки срещу наводнение

ЕВРОТРЪСТ предприема необходимите мерки да ограничи опасността от наводняване.

**9.1.4.** Противопожарни мерки

ЕВРОТРЪСТ предприема необходимите мерки за предпазване и минимизиране на опасността от пожар. Тези мерки са проектирани по начин, че да отговарят на приложимите законови и стандартизационни актове, регулиращи противопожарната охрана.

**9.1.5.** Резервно съхраняване на критична информация

Всички носители съдържащи софтуер, архиви на данни или одитна информация се съхраняват в структурите на ЕВРОТРЪСТ или в обезопасена зона за съхранение с подходяща система на физическа и логическа защита, ограничаващи достъпа и защитаващи носителите от случайно увреждане (излагане на електромагнитно увреждане и други).

Копия на съхраняваната информация, квалифицирана като критична и конфиденциална (журналната информация от работата на системите, активиращите данни за криптоустройствата/модулите, системна архивна информация (back-up), др.) се съхранява в специални помещения. В определени случай, определени от вътрешните правила за съхранение на информацията, същата може да бъде съхранявана в специализирани помещения извън сградата на ЕВРОТРЪСТ .

**9.2. Процедурни мерки за сигурност**

**9.2.1.** Общи организационни правила

Всички процедури, касаещи сигурността при издаването, администрирането и използването на удостоверения за електронен подпис, се изпълняват от персонал на ЕВРОТРЪСТ.

ЕВРОТРЪСТ поддържа достатъчен брой квалифицирани служители, които във всеки момент от осъществяването на дейността му да осигурят дейността в съответствие с действащото законодателство и вътрешните правила и норми на организацията.

**9.2.2.** Разпределяне на функциите

Подробно разпределение на функциите и отговорностите на персонала е разписано във вътрешни документи (длъжностни характеристики, щатно разписание) и съответни вътрешни оперативни процедури.

Разпределянето на функциите се осъществява по такъв начин, че да бъде сведена до възможен минимум опасността от компрометиране, изтичане на конфиденциална информация или на лични данни или конфликт на интереси.

### 9.3. Мерки за сигурност по отношение на персонала

**9.3.1.** Квалификация на персонала

Подборът на персонал се прави, съгласно вътрешните документи и щатното разписание на ЕВРОТРЪСТ и в съответствие със изискванията за съответната длъжност по отношение на теоретични и практически умения и квалификация, личностни характеристики и др.

**9.3.2.** Подготовка на персонала

ЕВРОТРЪСТ осигурява подготовка на персонала, която да осигурява успешното изпълнение на техните служебни задължения, свързани с:

- PKI-технология;
- функции, задължения и отговорности свързани с конкретни операции и процеси;
- политики и процедури на ЕВРОТРЪСТ;
- използване на софтуер и хардуер;
- справяне с кризи;
- възстановяване и поддържане на нормален работен процес.

**9.3.3.** Документация предоставяна на персонала

ЕВРОТРЪСТ предоставя на служителите си съответната документация, необходима им с оглед нормално изпълнение на задълженията и осъществяване на функциите, произтичащи от заеманата длъжност.

### 9.4. Процедури по проверка на сигурността

**9.4.1.** Записвани видове събития

ЕВРОТРЪСТ води автоматизиран отчет, на следните събития:

- събития относно периода на валидност на ключовете на удостоверяващите органи;

- събития от периода на валидност на удостоверенията на удостоверяващите органи и потребителите:
  - заявки за удостоверение, обновяване, прекодиране, прекратяване и спиране;
  - успешно или неуспешно обработване на заявките;
  - създаване и издаване на удостоверение и Списъците с прекратени и спрени удостоверение.
- събития свързани със сигурността.

**9.4.2.** Честота на извършване на записите

Отчетите от оценките на сигурността се преглеждат най-малко веднъж седмично за значителни събития по сигурността и дейността. Допълнително ЕВРОТРЪСТ преглежда своите отчети за необичайна активност в отговор на изпратени предупреждения, основаващи се на нередности или инциденти с регистриращите и удостоверяващи органи на ЕВРОТРЪСТ .

В отчетите от оценката на сигурността се съдържа удостоверение, че отчетът не е фалшифициран посредством преглеждането на всички данни в отчета и на разследване на всички нередности в отчетите. Предприетите в тази връзка действия също се документират.

**9.4.3.** Период на съхранение на отчетите

Отчетите се съхраняват най-малко два месеца след обработването им и след това се архивират.

### 9.5. Архивиране на записи от дейността на ЕВРОТРЪСТ

#### 9.5.1. Видове записвани събития

В допълнение към отчетите на оценките на сигурността ЕВРОТРЪСТ поддържа записи, които включват документация за:

- съвместимостта на ЕВРОТРЪСТ с политиката за предоставяне на удостоверителни услуги и други задължения произтичащи от споразуменията с потребителите;
- действие и информация от значителна важност за всяка заявка за удостоверение и на създаването, издаването, използването, спирането, прекратяването, възобновяването, продължаването, изтичането на всички удостоверения, издадени от Удостоверяващия орган на ЕВРОТРЪСТ.

Записите на ЕВРОТРЪСТ относно периода на валидност на удостоверенията включва:

- самоличността на потребителя на всяко удостоверение;
- самоличността на лицата подали заявка за спиране или прекратяване на удостоверение;

- други факти от удостоверението, времеви записи;
- някои предвидими факти отнасящи се към издаването на удостоверенията включващи, но неограничаващи се до информация относно успешното приключване на оценка за съвместимост.

Записите се съхраняват в електронен вид, с оглед точното и пълно индексиране, съхраняване, запазване и възпроизвеждане.

### 9.5.2. Период на съхранение на архивите

Записите свързани с удостоверенията се съхраняват докато ЕВРОТРЪСТ изпълнява функциите на доставчик на удостоверителни услуги.

Ако е необходимо ЕВРОТРЪСТ може да съхранява записите и за по-дълъг период от време с оглед спазването на приложимите закони.

### 9.5.3. Защита на архивите

ЕВРОТРЪСТ съхранява архивираните си записи, така че само оторизирани и доверени лица имат достъп до тях. Информацията архивирана по електронен път, е защитена срещу неоторизирано разглеждане модифициране, изтриване или фалшифициране чрез внедряването на подходящ логически и физически контрол на достъпа. Носителят съхраняващ записаната информация и приложенията за нейната обработка се поддържат с цел осигуряването на достъп до информацията за периода.

### 9.5.4. Процедури по съхраняване на архивите

ЕВРОТРЪСТ изготвя копия на електронните си архиви съхраняващи информация за издадените удостоверения ежедневно и осъществяват пълно копиране седмично. Копие на информацията съхранявани на хартиен носител се съхраняват в структура защитена от бедствия в съответствие с предвидените действия за възстановяване от кризи.

Планът на ЕВРОТРЪСТ за възстановяване от кризи е създаден с цел да осигури пълно възстановяване на всички функции на ЕВРОТРЪСТ в рамките на една седмица след криза, засегнала главните структури. ЕВРОТРЪСТ изпробва своето оборудване в структурата си, за да поддържа функциите на Удостоверяващ и Регистриращ органи след значима криза, която би спряла функционирането на цялата структура. Резултатите от тези проверки служат за оценъчни и планиращи цели. Когато е възможно дейността на структурата на ЕВРОТРЪСТ се възстановява колкото се може по-скоро след значима криза.

Поддържат се копия на важна информация от удостоверяващия орган на ЕВРОТРЪСТ. Тази информация включва, но не е ограничена до: информацията за заявките за удостоверение, информация относно оценките на сигурността съгласно Процедури по оценка на сигурността и база данни за всички издадени удостоверения.

### 9.6. Подмяна на ключовете на Удостоверяващ орган

Двойката частен-публичен ключ на Удостоверяващ орган може да бъде подновена в случай на:

- изтичане на срока на валидност на двойката частен-публичен ключ;
- въвеждане на нови услуги от ЕВРОТРЪСТ, които налагат променени характеристики на двойката частен-публичен ключ (например по-голяма дължина на ключа).

При подмяна на двойката частен-публичен ключ на Удостоверяващ орган на ЕВРОТРЪСТ се спазват следните правила:

- Удостоверяващият орган, чиято двойка публичен и частен ключ ще бъде подменена, спира издаването на удостоверение на подчинени Удостоверяващи органи (ако има такива) 60 /шестдесет/ дни преди момента, в който оставащия период на валидност на двойката му ключове се изравни с периодът на валидност на издаваните от подчинените му Удостоверяващи органи удостоверение;
- Удостоверяващият орган, чиято двойка ключове е подменена, продължава да публикува списък с прекратени и спрени удостоверение, който е подписан със старата двойка ключове до момента, в който изтече срокът на валидност на последния удостоверение издадено:
  - със старата двойка публичен и частен ключ на Удостоверяващия орган;
  - от подчинен Удостоверяващ орган, чиито удостоверение е подписан със старата двойка публичен и частен ключ.

## 10. Технически мерки за сигурност

Генерирането на двойката частен-публичен ключ на Удостоверяващите органи и Регистриращия орган, се осъществява от ЕВРОТРЪСТ, като се използва защитен механизъм за създаване на подпис със защитен профил определен в съответствие със спецификации, определящи нива на сигурността.

### 10.1. Генериране на двойката частен-публичен ключ на потребителски удостоверения

В случаите, когато генериране на двойката частен-публичен ключ се осъществява при Титуляря или Автора, същият носи пълната отговорност по защитата на частния ключ, с цел предотвратяване на неговото компрометиране, разкриване, модифициране, загуба или неразрешено ползване. Титуляря/Автора носи отговорност за пропуски или действия на упълномощени от тях лица, които са делегирани да генерират, пазят или съхраняват техните частни ключове.

#### 10.1.1. Отдалечено генериране на двойката ключове.

Авторът зарежда персоналната си форма за генериране на двойката ключове към системата на доставчика.

Специално разработения за дейността на доставчика софтуер, съвместно със съответния CSP за управление на потребителското четящо устройство и смарт карта, реализира процеса по генериране на двойката ключове.

Записването и съхраняването на частния ключ е с високо ниво на сигурност, което е гарантирано от самия носител(смарт карта), защитен посредством ПИН, който е известен само на Титуляря или Автора(надлежно овластен съгласно съответната приложена бланка-образец).

Авторът генерира електронната заявка за удостоверение в PKCS#10 формат и я изпраща на ЕВРОТРЪСТ. Според препоръки RFC 2314, PKCS#10 форматът за електронна заявка съдържа DN, публичния ключ и други атрибути, като всички те са подписани с частния ключ и са пакетирани в ASN.1 формат.

#### 10.1.2. Генериране на двойката ключове в ЕВРОТРЪСТ

Авторът в присъствието на надлежно овластен служител на Регистриращия орган на ЕВРОТРЪСТ, зарежда персонализираната си форма за генериране на двойката ключове към системата на доставчика.

Специално разработения за дейността на доставчика софтуер, съвместно със съответния CSP за управление на потребителското четящо устройство и смарт карта, реализира процеса по генериране на двойката ключове.

След генериране на двойката ключове, Авторът сам сменя ПИН-кода за достъп до смарт картата.

Записването и съхраняването на частния ключ е с високо ниво на сигурност, което е гарантирано от самия носител(смарт карта), защитен посредством ПИН, който е известен само на Титуляря или Автора(надлежно овластен съгласно съответната предоставена бланка-образец).

Надлежно овластеното лице от структурата на Регистриращ орган на ЕВРОТРЪСТ пред Автора генерира електронната заявка за удостоверение в PKCS#10 формат.

### 10.2. Предаване на частен ключ

Двойката частен-публичен ключове се генерира и съхранява от Автора.

### 10.3. Предоставяне на публичен ключ от Автора на ЕВРОТРЪСТ

Тази процедура се изпълнява само от Автора.

Авторът изпраща електронна заявка във формат PKCS#10. Заявката съдържа публичния ключ на Титуляря/Автора и е подписана електронно с кореспондиращия частен ключ.

Чрез проверка на достоверността на подписа ЕВРОТРЪСТ може установи и достоверността на изпратения публичен ключ.

### 10.4. Предоставяне на публични ключове на Удостоверяващи органи на заинтересованите лица

Публичните ключове на доставчика (Базовият - Evrotrust RSA Root CA и оперативните –

Evrotrust RSA Operational CA) са публично достъпни в Интернет страницата на ЕВРОТРЪСТ на адрес: http://www.evrotrust.com

### 10.5. Защита на частния ключ

#### 10.5.1. Стандарт за криптографски модул

Частните ключове кореспондиращи на Базовия и Оперативните удостоверения на ЕВРОТРЪСТ се съхраняват в сигурни криптографски модули, удовлетворяващи нормативните изисквания.

Инсталираните криптомодули са най-висока степен на сигурност, съгласно изискванията на международните стандарти и тези поставени от българското законодателство.

#### 10.5.2. Съхраняване и контрол върху частен ключ

Единствено Авторът има право на достъп до частния ключ, кореспондиращ с публичния ключ в издаваното удостоверение. ЕВРОТРЪСТ предоставя услуга по генериране на двойката частен-публичен ключ, като ключовете се генерират върху смарт карта, без възможност за извличане на частния ключ. Смарт картата се предава на Автора.

Авторът е задължен да съхранява и пази от компрометиране персоналните данни за активация на своята смарт карта или ключов файл (своя ПИН или парола).

#### 10.5.3. Архив на публичните ключове

Публичните ключове се съхраняват в база данни на ЕВРОТРЪСТ и се архивират периодично за период съответстващ на срокът на валидност на оперативния удостоверение на Удостоверяващия орган.

Удостоверенията, които съдържат публичните ключове на Авторите, се съхраняват в Електронния регистър на ЕВРОТРЪСТ.

## 11. Защита на компютърните системи

В ЕВРОТРЪСТ са разработени и се спазват политики, процедури и методи за администриране и управление на сигурността на използваната инфраструктура, в съответствие с общоприети в международната практика стандарти за управление на информационната сигурност.

Защитните мерки предприети по отношение на компютърните системи са елемент от разработената и внедрена ЕВРОТРЪСТ система за информационна сигурност и са насочени към редуциране на идентифицираните и оценени рискове на приемливо ниво.

Възприетите мерки по отношения на защита на компютърните системи са предназначени за защита, възпиране, откриване, ответни действия и възстановяване, като те могат да се използват едновременно за няколко от посочените функции.

Надеждността на използваните системи и техническата и криптографската сигурност на осъществяваните чрез тях процеси се осигуряват посредством провеждане на изпитвания и проверки на компютърните информационни системи.

В ЕВРОТРЪСТ са установени практики, мерки и принципи по отношение на сигурността в

мрежовата среда, осъществяваният контрол и даване на права до мрежови информационни ресурси. ЕВРОТРЪСТ използва най-съвременни мрежови технически средства (хардуер и софтуер) за защита на достъпа и обмен на информация в рамките на своята инфраструктура.

## 12. Други условия

### 12.1. Възнаграждения

ЕВРОТРЪСТ предоставя удостоверителни и други услуги срещу заплащане на възнаграждение или безплатно, съобразно търговската си политика.

Възнаграждението за удостоверителните и други услуги, които ще бъдат предоставени на Титуляря, се определя при сключване на договора за удостоверителни услуги, съобразно Ценовата тарифа за предоставяни услуги, публикувана на уеб-сайта на ЕВРОТРЪСТ.

ЕВРОТРЪСТ си запазва правото едностранно да променя обявените цени, при спазване изискванията на действащото законодателство. Промяната на възнагражденията не може да засегне вече заплатено възнаграждение.

ЕВРОТРЪСТ определя цени на следните услуги:

- издаване и поддържане на удостоверение;
- подновяване на удостоверение;
- подновяване на удостоверение след промени в публичната част от страна на Титуляря/Автора;
- технологична помощ и консултации;
- плащане при подписване.

ЕВРОТРЪСТ предоставя безплатно следните услуги:

- TimeStamp достъп;
- достъп до CRL;
- OCSP достъп;

Възнаграждението за предоставяне на удостоверителни услуги се заплаща еднократно, преди издаване на удостоверение на Титуляря, съответно Автора. Такова може да не се заплаща, когато за определени приложения ще се събира такса за подписване (плащане при използване).

Възнаграждението за извършена технологична помощ и консултации се заплаща еднократно, след извършване на технологична помощ и консултации и установяване на тяхната продължителност.

Заплащането на дължими суми може да се осъществи с банков превод по посочена от ЕВРОТРЪСТ банкова сметка, с банкова карта през интернет-страницата или съответно приложение, или в брой при Регистриращ орган. Когато възнаграждение се дължи при използване, то се заплаща чрез електронно протмоне, депозитни суми, банкови карти, електронни пари или чрез други достъпни методи, в съответствие с действащото законодателство.

Всички разноски по преводи са за сметка на клиента.

### 12.2. Застрахователна политика

#### 12.2.1. Застраховка

ЕВРОТРЪСТ сключва договор за задължителна застраховка, който му осигурява възможност за осъществяване на дейността му по предоставяне на УУ, включително покрива вредите в случай на неизпълнение на задълженията му.

#### 12.2.2. Застрахователно покритие

Задължителната застраховка покрива отговорността на ЕВРОТРЪСТ за причинените на Автора, съответно Титуляря на КЕП и на всички трети лица неимуществени и имуществени вреди, за които застрахованите отговарят съгласно българското законодателство или законодателството на страната, в която е настъпила вредата. Застраховката е за застрахователна сума в размерите, посочени в чл.14 от НЕВРОТРЪСТ.

### 12.3. Приложимо законодателство. Решаване на спорове и юрисдикция

За всички нерегламентирани в настоящия документ въпроси се прилага действащото в Република България законодателство.

Всички възникнали спорове при предоставянето на удостоверителни услуги се уреждат с преговори, а когато това се окаже невъзможно – по съдебен ред.

Жалби относно дейността на ЕВРОТРЪСТ могат да бъдат подадени:

- по електронен път, на e-mail: delovodstvo@evrotrust.com;
- в деловодството на “Регистриращ орган” на “ЕВРОТРЪСТ технолоджис” АД , гр.София.

Жалбите се разглеждат в двуседмичен срок от получаването им. Ръководителят на Звеното за удостоверителни услуги се произнася с мотивиран отговор, който се довежда до знанието на жалбоподателя, чрез осъществяване на контакт по предварително уточнен с жалбоподателя начин.

В случай, че доброволното уреждане на отношенията е невъзможно, спорът се отнася пред компетентния съд.

За имуществени спорове, възникнали след сключване на договора за удостоверителни услуги, компетентен е съответният съд в град София.

# III. ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

### 13. Въведение

Настоящият част от „Наръчник за потребителя” съдържа политиките, които следва “ЕВРОТРЪСТ технолоджис” АД, в качеството си на доставчик на удостоверителни услуги (наричан за краткост ЕВРОТРЪСТ) при издаване и управление на удостоверения за КЕП

Документът описва предоставяните от ЕВРОТРЪСТ услуги, както и прилаганите процедури при издаване, спиране, продължаване и прекратяване на удостоверенията. ЕВРОТРЪСТ прилага отделна политика за всеки от предлаганите типове удостоверения. Политиката отразява различните процедури следвани при издаване и поддръжка на удостоверенията, приложимостта им, мерките за сигурност при идентификация на Авторите, респективно Титулярите и генерирането на двойката частен-публичен ключ.

### 14. Идентификация на политиките за издаване на удостоверения за ЕП

На всяка от политиките, в съответствие с които се издават удостоверения за ЕП от ЕВРОТРЪСТ се присвоява идентификатор на обект (OID – Object Identifier). Стойностите на идентификаторите на обекти са:

| Тип удостоверение за електронен подпис | Идентификатор на обект |
|---|---|
| Evrotrust RSA Root CA | 1.3.6.1.4.1.47272.1 |
| Evrotrust RSA Validation | 1.3.6.1.4.1.47272.1.1 |
| Evrotrust TSA | 1.3.6.1.4.1.47272.1.2 |
| Evrotrust RSA Operational CA | 1.3.6.1.4.1.47272.2 |
| Evrotrust RSA QS Validation | 1.3.6.1.4.1.47272.2.1 |
| Evrotrust Qualified Natural Person Certificate | 1.3.6.1.4.1.47272.2.2 |

### 15. Базово удостоверение на ЕВРОТРЪСТ

Базовото удостоверение Evrotrust RSA Root CA на доставчика на удостоверителни услуги “ЕВРОТРЪСТ технолоджис” АД е самоподписано и издадено удостоверение за КЕП с валидност 20 години.

С базовия частен ключ на Evrotrust RSA Root CA се подписва оперативното удостоверение Evrotrust RSA Operational CA, удостоверението на органа за валидация Evrotrust RSA Validation и удостоверението на органа за удостоверяване на време Evrotrust TSA.

**Профил на базовото удостоверение Evrotrust RSA Root CA на ЕВРОТРЪСТ:**

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 6c:6e:c9:bf:48:51:72:a5:4b:d4:0f:27:78:62:52:45 | |
| Signature Algorithm | SHA384RSA | |
| Valid from | 160520153919Z | |
| Validit to | 360520154919Z | |
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Subject | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | E= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Public Key | RSA(4096 Bits) | |
| Key Usage (critical) | keyCertSign and cRLSign | |
| Subject Key Identifier | 74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70 | |
| Basic Constraints (critical) | Subject type = CA, Path Length Constraint=None | |

## 16. Оперативни удостоверения за КЕП на ЕВРОТРЪСТ Evrotrust RSA Operational CA

Оперативното удостоверение за КЕП на Удостоверяващия орган Evrotrust RSA Operational CA е подписано с базовия частен ключ на ЕВРОТРЪСТ и е с валидност 10 години.

С частния оперативен ключ на ключ на Evrotrust RSA Operational CA се подписват всички издавани от ЕВРОТРЪСТ удостоверения за КЕП от типове: Evrotrust Qualified Natural Person Certificate, както и на органа за валидация Evrotrust RSA QS Validation.

**Профил на оперативното удостоверение Evrotrust RSA Operational CA на ЕВРОТРЪСТ:**

| | |
|---|---|
| Version | V3 |
| Serial number | 38:00:00:00:03:4e:8e:cb:48:09:25:01:bc:00:00:00:00:00:03 |
| Signature Algorithm | SHA256RSA |
| Valid from | 160521003435Z |
| Validit to | 260521004435Z |

| | | |
|---|---|---|
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Subject | CN= | Evrotrust RSA Operational CA |
| | OU= | Qualified Operational CA |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Public Key | RSA(2048 Bits) | |
| Subject Key Identifier | 7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08 | |
| Key Usage (critical) | Certificate Signing, keyCertSign and cRLSign | |
| Extended keyUsage | serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning | |
| Certificate Policies | [[1]Certificate Policy:<br>Policy Identifier=All issuance policies<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.evrotrust.com/cps | |
| Authority Key Identifier | 74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70 | |
| Subject alternative name (not critical) | URL=http://www.evrotrust.com RFC822 Name=ca@evrotrust.com | |
| CRL Distribution Points | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl | |
| Authority Information Access | [[1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/ocsp | |

| | |
|---|---|
| Basic Constraints (critical) | Subject Type=CA<br>Path Length Constraint=0 |

## 17. Оперативни правила при издаване и управление на удостоверение за КЕП

### 17.1. Заявки за издаване на удостоверението

#### 17.1.1. Документи, идентифициращи Автора/Титуляря – физическо лице

Лицето, което желае да му бъде издадено удостоверение за КЕП (наричано по-долу за краткост Заявител), надлежно попълва и предава на Регистриращия орган доказателства и данни за формиране на съответните формуляри или попълнени такива по пощa.

Попълнените документи съдържат данни за лицето, в това число данни за контакт, адрес по местоживеене и адрес за електронна поща. Физическото лице потвърждава достоверността на данните в попълнените документи, чрез:

- саморъчно поставен подпис върху документите пред упълномощен служител на Регистриращия орган, в случай на лично предаване на документите;
- нотариална заверка на документите, които се изпращат по пощa до Регистриращия орган;
- подписване на приложените електронни документите с валидно удостоверение за КЕП по смисъла на ЗЕДЕП;
- подписване с усъвършенстван електронен подпис на документите чрез съответно мобилно или друго приложение и след извършена надлежна идентификация на физическото лице – заявител и юридическото лице – титуляр, от служител на ЕВРОТРЪСТ.
- саморъчно подписано копие от лична карта или паспорт на Титуляря/Автора и изписан текст „Съгласен съм да се ползва копието на личната ми карта за целите на предоставяните удостоверителни услуги от ЕВРОТРЪСТ ”;
- заявка за издаване на удостоверение за КЕП;
- договор за удостоверителни услуги (2 екземпляра);

Съгласието се изисква във връзка със Закона за защита на личните данни.

Заявителят може да изтегли посочените по-горе образци на документи от уеб-сайта на ЕВРОТРЪСТ (http://www.evrotrust.com) или чрез специализирано приложение.

#### 17.1.2. Документи, идентифициращи Титуляря – юридическо лице:

Установяване на идентичността на българско юридическо лице – Титуляр, се осъществява от Регистриращия орган чрез автоматизирана проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ по реда на Закона за електронното управление. За български юридически лица, които не са търговци, както и за чуждестранни юридически лица, за които не може да се извърши автоматизирана проверка, се представят:

- съдебно решение или друг документ, удостоверяващи възникването на

юридическото лице;

- документ, удостоверяващ актуалното състояние на лицето;
- Уникален национален идентификатор.

Списък с изискуеми документи се поддържа на уеб-сайта на ЕВРОТРЪСТ и в специализираните приложения за достъп до услугите. След заснемане на Копия от всички изискуеми документи остават в архива на ЕВРОТРЪСТ.

Лицето представляващо юридическото лице удостоверява достоверността на информацията, която се съдържа в документи чрез:

- Заверка „Вярно с оригинала“ и саморъчен подпис върху документите пред упълномощен служител на Регистриращия орган, в случай на лично предаване на документите;
- нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;
- подписване на приложените електронни формати на документите с валидно удостоверение за КЕП;
- подписване с усъвършенстван електронен подпис на документите чрез съответно мобилно или друго приложение и след извършена надлежна идентификация на физическото лице – заявител (автор) и юридическото лице – титуляр, от служител на ЕВРОТРЪСТ и наличието на представителната власт на заявителя спрямо титуляря.

Регистриращият орган извършва проверки за достоверност на подадената информация от Заявителя. Тези проверки могат да се правят автоматизирано, при наличие на технологично решение за това. Проверката включва:

- проверка за липса на изисквани документи и коректност на попълването на документите;
- идентификация на Титуляря/Автора на удостоверението;
- достоверност на попълнените данни.

В случай на отказ за издаване на удостоверение за КЕП, Регистриращият орган уведомява Заявителя чрез избран от посочените от него начини за комуникация и посочва причината за отхвърляне на заявката.

Посредством уеб- базиран интерфейс Авторът има възможност да проследява и управлява процесите по издаване и управление на удостоверението за КЕП.

### **17.2.** Издаване на удостоверението

След като Авторът е потвърдил съгласието си със съдържанието на DN(предоставената от него информация за удостоверяване), като по този начин приема съдържанието на публичната част от полето “Subject” от удостоверението, процесът преминава към процедурата по генериране на двойката частен-публичен ключ и подаване на електронна заявка. Всички електронни заявки за издаване на удостоверения за КЕП, когато двойката ключове се генерира при Автора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната

заявка е в PKCS#10 формат, което позволява на Регистриращия орган на ЕВРОТРЪСТ да се увери, че Авторът държи частния ключ.

ЕВРОТРЪСТ, чрез Регистриращия си орган, реализира мерки за автентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи от Автора, в съответствие със заявения тип удостоверение за КЕП.

Мерките за идентификация и установяване притежаването на частен ключ са описани в този документ.

При констатирано съответствие Регистриращият орган на ЕВРОТРЪСТ одобрява заявката за удостоверение за КЕП. Удостоверяващият орган потвърждава и издава удостоверението.

При констатирано несъответствие се уведомява Заявителя по избран подходящ начин, предоставен от него за контакт.

Удостоверението не се издава преди потребителят да извърши заплащане на услугата.

След издаване на удостоверението ЕВРОТРЪСТ уведомява Титуляря/Автора и му предоставя начин за получаване. Достъпът до удостоверението за КЕП може да бъде осъществен чрез зареждането му през уеб-сайта на ЕВРОТРЪСТ http://www.evrotrust.com .

### **17.3.** Публикуване на удостоверението

Издаденото от Удостоверяващия орган на ЕВРОТРЪСТ удостоверение за КЕП се публикува веднага след генерирането му в електронния регистър на доставчика.

Електронният регистър на ЕВРОТРЪСТ е публичен и начините за достъп до него са описани в настоящият документ.

### **17.4.** Приемане на удостоверението

Титулярът или Авторът могат в 3/три/ дневен срок след зареждане и инсталиране на удостоверението за КЕП да направят рекламация за коректността на съдържанието му.

Ако след изтичане на този срок Титулярът/Авторът не е направил рекламации относно коректността на съдържанието, удостоверението се счита за окончателно прието.

Удостоверението за КЕП се счита за окончателно прието от Титуляря/Автора, ако преди изтичане на 3 /три/ дневния срок след издаването му бъде използвано поне веднъж.

### **17.5.** Спиране и възобновяване действието на удостоверението

#### **17.5.1. Спиране на удостоверение**

Спиране на действието на издадени от ЕВРОТРЪСТ удостоверения за КЕП се предприема при наличие на определени основания, като срокът за който е спряно действието на удостоверението зависи от обстоятелствата довели до спиране. Този срок не може да надвишава 48 часа от момента на спирането.

Искане за спиране на удостоверение за КЕП може да бъде отправено до ЕВРОТРЪСТ по някой от следните начини:

- на телефонни номера +359 2 9699200/ 252

лицето, което иска спирането, трябва да съобщи:

- трите си имена;
- телефонният номер, от който се обажда за спиране на удостоверение за КЕП; /този телефонен номер се използва за обратна контрола/;
  удостоверението за КЕП, за което се иска спиране;
- причините, поради които иска спиране на съответното удостоверение.

Когато Титулярът/Авторът е поискал спиране, се изисква да съобщи и паролата за идентификация, която е попълнил в заявката за удостоверение за КЕП.

- електронна поща

  лицето, което иска спиране, изтегля от уеб-сайта на ЕВРОТРЪСТ „Заявка за спиране на действието на удостоверение за КЕП“;

  попълва изтеглената форма и я изпраща като прикачен файл в електронна поща на адрес: delovodstvo@evrotrust.com .

Когато лицето е Титуляр/Автор, той съобщава и паролата за идентификация, която е попълнил в заявката за удостоверение за КЕП.

- през Интернет сайта на ЕВРОТРЪСТ - заявителят попълва и изпраща електронна форма „Заявка за спиране на действието на удостоверение за КЕП“.
- лично при доставчика на Удостоверителни услуги - лицето, което иска спиране лично при Доставчика на Удостоверителни услуги ЕВРОТРЪСТ, попълва „Заявка за спиране на действието на удостоверение за КЕП.

ЕВРОТРЪСТ спира действието на удостоверение за КЕП като го поставя в списъка с прекратени удостоверения със статус „HOLD“.

ЕВРОТРЪСТ идентифицира, но не удостоверява самоличността на лицето, поискало спиране на удостоверение.

ЕВРОТРЪСТ незабавно уведомява Титуляря/Автора за спирането на удостоверението.

### 17.5.2. Възобновяване на удостоверение

Спряно удостоверение за КЕП се възобновява, ако в рамките на законово регламентирания максимално допустим 48-часов срок Титулярят предостави надлежно попълнена и подписана „Заявка за възобновяване на удостоверение за КЕП.

„Заявка за възобновяване на удостоверение за КЕП се попълва от Титуляря при отпадане на основанието за спиране, и с която уверява Доставчика на удостоверителни услуги, че е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.

В случаите, когато искането за спиране произхожда от Комисията за регулиране на съобщенията, ЕВРОТРЪСТ предоставя на комисията копие от писмената заявка за възобновяване.

Възобновяването се извършва чрез изваждането на удостоверението със статус “HOLD” от списъка с прекратени удостоверения (CRL) в електронния регистър на ЕВРОТРЪСТ.

Ако след изтичане на максимално регламентираният 48 /четиридесет и осем/ часов срок от спиране на удостоверение не е налице основание за неговото прекратяване, ЕВРОТРЪСТ

автоматично възобновява удостоверението.

### **17.6.** Подновяване на удостоверение

Удостоверения за КЕП, които не са прекратени, могат да бъдат подновени преди изтичане на срока им на валидност, без да е необходимо генериране на нова двойка ключове.

ЕВРОТРЪСТ като доставчик на удостоверителни услуги допуска подновяване на удостоверение за КЕП чрез използване на съществуващата двойка ключове само еднократно, с цел да се намали риска от компрометирането й.

#### **17.6.1. Процедурата по подновяване действието на удостоверение без да се генерира нова двойка ключове**

Процедурата включва следните стъпки:

- предоставяне на Регистриращия орган лично или по пощата на заявка за подновяване на удостоверение , подписана от Титуляря/Автора. В случай, че заявката не се предава лично на представител на Регистриращия орган, се изисква нотариална заверка на подписа;
- предоставяне на електронно подписана заявка за подновяване по електронна поща до Регистриращия орган или чрез специализирано приложение.

Регистриращият орган извършва проверка за достоверност на подадената информация от Титуляря/Автора. Проверката включва:

- проверка за коректност на съдържанието на предоставената заявка;
- идентификация на Автора и респ. на Титуляря на удостоверението;
- достоверност на попълнените данни;
- в случай, че заявката е изпратена по електронен път, Регистриращият орган да поиска персонална идентификация на Титуляря/Автора за удостоверяване на идентичността му и държането на частния ключ.

След установяване на достоверност на информацията, Регистриращият орган пристъпва към подновяване на удостоверението.

След извършване на горните процедури, се преминава към процедура по генериране и подаване на електронна заявка. Всички електронни заявки за подновяване на удостоверения за КЕП, когато двойката ключове се генерира при Титуляря/Автора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка е в PKCS#10 формат, което позволява на Регистриращият орган на ЕВРОТРЪСТ да провери притежанието на частния ключ.

ЕВРОТРЪСТ, чрез Регистриращия си орган, реализира мерки за идентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи от Автора, в съответствие със заявения тип удостоверение.

При констатирано съответствие, Регистриращият орган на ЕВРОТРЪСТ одобрява заявката за подновяване на удостоверението. Удостоверяващият орган подновява заявеното

удостоверение за КЕП .

При констатирано несъответствие се уведомява Автора, по избран подходящ начин, предоставен от него за контакт.

Удостоверение за КЕП не се подновява преди потребителят да извърши заплащане на услугата.

След подновяване на удостоверението, ЕВРОТРЪСТ уведомява Титуляря/Автора, че достъпът до подновеното удостоверение е осигурен и предоставя начин за получаването му. Достъпът до удостоверението може да бъде осъществен чрез зареждането му през уеб-базирания интерфейс на доставчика на удостоверителни услуги ЕВРОТРЪСТ http://www.evrotrust.com .

#### 17.6.2. Процедурата по подновяване действието на удостоверение с генериране на нова двойка ключове

Процедурата включва следните стъпки:

- предоставяне на Регистриращия орган лично или по пощата на заявка за подновяване на удостоверение , подписана от Титуляря/Автора. В случай, че заявката не се предава лично на представител на Регистриращия орган, се изисква нотариална заверка на подписа;
- предоставяне на електронно подписана заявка за подновяване по електронна поща до Регистриращия орган или чрез специализирано приложение.

Регистриращият орган извършва проверка за достоверност на подадената информация от Титуляря/Автора. Проверката включва:

- проверка за коректност на съдържанието на предоставената заявка;
- идентификация на Автора и респ. на Титуляря на удостоверението;
- достоверност на попълнените данни;
- в случай, че заявката е изпратена по електронен път, Регистриращият орган да поиска персонална идентификация на Титуляря/Автора за удостоверяване на идентичността му и държането на частния ключ.

След установяване на достоверност на информацията, Регистриращият орган пристъпва към подновяване на удостоверението.

След извършване на горните процедури, се преминава към процедура по генериране и подаване на електронна заявка. Всички електронни заявки за подновяване на удостоверения за КЕП, когато двойката ключове се генерира при Титуляря/Автора, са подписани от потребителя с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка е в PKCS#10 формат, което позволява на Регистриращият орган на ЕВРОТРЪСТ да провери притежанието на частния ключ.

ЕВРОТРЪСТ, чрез Регистриращия си орган, реализира мерки за идентификация на притежателя на частния ключ и установяване на факта, че този частен ключ се държи от Автора, в съответствие със заявения тип удостоверение.

При констатирано съответствие, Регистриращият орган на ЕВРОТРЪСТ одобрява заявката за подновяване на удостоверението. Удостоверяващият орган подновява заявеното

удостоверение за КЕП .

При констатирано несъответствие се уведомява Автора, по избран подходящ начин, предоставен от него за контакт.

Удостоверение за КЕП не се подновява преди потребителят да извърши заплащане на услугата.

След подновяване на удостоверението, ЕВРОТРЪСТ уведомява Титуляря/Автора, че достъпът до подновеното удостоверение е осигурен и предоставя начин за получаването му. Достъпът до удостоверението може да бъде осъществен чрез зареждането му през уеб-базирания интерфейс на доставчика на удостоверителни услуги ЕВРОТРЪСТ http://www.evrotrust.com .

### 17.7. Прекратяване на удостоверение

#### 17.7.1. Прекратяване действието на удостоверение за КЕП с изтичане срока на валидност

При неподадена заявка за подновяване от страна на Титуляря/Автора преди изтичане на срока на действието на удостоверението за КЕП, действието на удостоверението се прекратява автоматично, с изтичане срокът му на валидност.

#### 17.7.2. Прекратяване действието на удостоверение за КЕП преди изтичане срока на валидност

Действието на удостоверението се прекратява при прекратяване на юридическото лице на доставчика на удостоверителни услуги без прехвърляне на дейността на друг доставчик на удостоверителни услуги.

Доставчикът на удостоверителни услуги прекратява действието на удостоверението при смърт или поставяне под запрещение на Титуляря/Автора.

Доставчикът на удостоверителни услуги прекратява действието на удостоверението при установяване, че удостоверението е издадено въз основа на неверни данни.

Действието на удостоверението предсрочно се прекратява при изразено желание от страна на Титуляря/Автора, заявено лично или по пощата. Необходимо е представяне на заявка за прекратяване на удостоверение.

В случай, че заявката не се предава лично на представител на Регистриращия орган, се изисква нотариална заверка.

След като се увери в самоличността и извърши допълнителна проверка за достоверност на подадената информация, Регистриращият орган въвежда електронна заявка за промяна в статуса на удостоверението на потребителя. Удостоверяващият орган реализира прекратяването като включва удостоверението за КЕП в CRL.

Всички изискуеми от ЕВРОТРЪСТ формуляри се намират на уеб-сайта http://www.evrotrust.com

## 18. Характеристика и приложение на удостоверения за КЕП за физически и юридически лица тип Evrotrust Qualified Natural Personal Certificate

Удостоверения за квалифицирани електронни подписи се издават на физически лица

Титуляр и Автор. Същите се използват за да удостоверяват връзката между публичния ключ и Автора и дават възможност за установяване на това дали Авторът е подписал съответно електронно изявление.

Всеки електронен подпис, който е придружен от това удостоверение, има характера на саморъчно поставен подпис и осигурява увереност по отношение на автентичност, интегритет, съгласие и неотменимост на подписаните съобщения.

Двойката частен-публичен ключ, която кореспондира с издаденото удостоверение за КЕП, се създава и съхранява на SSCD, без възможност за извличане на частния ключ от устройството.

Обичайните приложения за използване на удостоверения за квалифицирани електронни подписи са при подписване на електронна поща, достъп до защитени информационни системи, електронния търговия и др. С кореспондиращата двойка ключове може да се поставя електронен подпис и да се криптира информация.

За физически лица, които са асоциирани с юридическо лице, например служители, управители, счетоводители и т.н., се издават удостоверения за КЕП с попълнени атрибути O(organizationName) и 2.5.4.97=(organizationIdentifier) с данните на асоциираното юридическо лице. За физически лица, които упражняват свободна професия, също се попълват тези атрибути.

**18.1.** ЕВРОТРЪСТ може да вписва и други атрибути, които не са описани в текущия профил на удостоверението.Удостоверение за КЕП на физически лица - Evrotrust Qualified Natural Personal Certificate

Издаденото удостоверение за КЕП е с валидност 2 /две/ години.

**Профил на удостоверение за КЕП Evrotrust Qualified Natural Personal Certificate**

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | [сериен номер] | |
| Signature Algorithm | SHA256RSA | |
| Issuer | CN= | Evrotrust RSA Operational CA |
| | OU= | Qualified Operational CA |
| | O= | Evrotrust Technologies JSC |
| | oganizationIdentifier (2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Valid from | [начална дата и час по UTC на валидност на удостоверението] | |
| Validit to | [крайна дата и час по UTC на валидност на удостоверението] | |
| Subject | C= (countryName) | Държава: Двубуквен код на държавата според ISO 3166 |

| | |
|---|---|
| CN=<br>(commonName) | Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице. |
| G=<br>(givenName) | Собствено име: Име на физическото лице според документ за самоличност |
| S=<br>(surname) | Фамилно име: Фамилия на физическото лице според документ за самоличност |
| Или | |
| 2.5.4.65=<br>(pseudonym) | Псевдоним: Псевдоним, избран от физическото лице |
| SERIALNUMBER=<br>(serialNumber) | Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например:<br>- PNOBG-8310257645 за ЕГН;<br>- PASSBG-12345678 за номер на паспорт;<br>- IDCBG-195416023 за номер на лична карта;<br>- TINBG-123434341 за ДДС номер.<br>Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генериран от доставчика, с цел идентифициране на физическото лице при необходимост. |
| O*=<br>(organizationName) | Наименование на юридическо лице: Пълно наименованието по регистрация или акт на вписване на юридическото лице, с което физическото лице е асоциирано. |
| 2.5.4.97*=<br>(organizationIdentifier) | Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например:<br>- VARBG-123456789 – ДДС;<br>- NTRBG-123456789 - ЕИК (БУЛСТАТ).<br>Вписва се националния идентификатор според местното законодателство на юридическото лице, с което физическото лице е асоциирано. |

<table>
<tr><td></td><td>E=<br>(e-mailAddress)</td><td>Имейл адрес на физическото лице</td></tr>
<tr><td>Public Key Type/Length</td><td colspan="2">RSA (2048 Bits)</td></tr>
<tr><td>Subject Key Identifier</td><td colspan="2">[Изчислена стойност за издаденото удотоверение]</td></tr>
<tr><td>Authority Key Identifier</td><td colspan="2">Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="2">1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</td></tr>
<tr><td>Authority Information Access</td><td colspan="2">1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/ocsp</td></tr>
<tr><td>Enhanced Key Usage</td><td colspan="2">Client Authentication (1.3.6.1.5.5.7.3.2)<br>Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td colspan="2">[1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.47272.2.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.evrotrust.com/cps<br>[2]Certificate Policy:<br>Policy Identifier=0.4.0.1456.1.1</td></tr>
<tr><td>Key Usage (critical)</td><td colspan="2">Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)</td></tr>
<tr><td>QCStatements</td><td colspan="2"><table><tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1)<br>id-etsi-qcs-SemanticsId-Legal* (oid=0.4.0.194121.1.2)</td></tr><tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr></table></td></tr>
</table>

| | | |
|---|---|---|
| | 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-**esign** (oid=0.4.0.1862.1.6.1) |
| | id-etsi-qcs-**QcPDS** (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf<br>language=en |

*Полетата маркирани с* ***** *са опционални .*

### 19. Удостоверение за време

Удостоверението за време удостоверява със стойността на официално удостоверяване на точната дата и час, в който клиентският електронен документ е регистриран в TimeStamp сървъра на ЕВРОТРЪСТ. TimeStamp сървърът на ЕВРОТРЪСТ издава сериен номер и електронно подписва удостоверението за време. ЕВРОТРЪСТ предоставя услугата по удостоверяване на време съобразно относимите международни препоръки и спецификации, посочени в „Наръчника". Предоставеното точно време е калибровано спрямо Coordinated Universal Time (UTC) с точност до 0.5 сек. Сертификатът на удостоверяващият за времеме орган **Evrotrust TSA** е подписан с базовия частен ключ на ЕВРОТРЪСТ и е с валидност 5 години.

Достъпът за получаване и проверка на издадените удостоверения за време е публичен през уеб-сайта на ЕВРОТРЪСТ http://www.evrotrust.com.

**Профил на удостоверение за Удостоверяване на време - Evrotrust TSA**

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 38:00:00:00:03:4e:8e:cb:48:09:25:01:bc:00:00:00:00:00:03 | |
| Signature Algorithm | SHA256RSA | |
| Valid from | 160521004013Z | |
| Validit to | 210521005013Z | |
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Subject | CN= | Evrotrust TSA |
| | OU= | Time Stamping Authority TSS/TSU |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Public Key | RSA(2048 Bits) | |
| Subject Key Identifier | 03:BB:3B:42:27:8E:B8:80:90:1B:51:05:DF:52:C4:4B:0F:34:85:B9 | |

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

20. **Проверка на статуса на удостоверение в реално време (OCSP)** - Доверяващите се страни могат да използват за проверка на статуса на издадените удостоверения посредством OCSP протокол на адрес – http://ca.evrotrust.com/ocsp Услугата по валидация е основана на препоръките на (IETF) Public Key Infrastructure X.509 (PKIX) "Lightweight OCSP Profile for High Volume Environment".

### 20.1. Профил на валидиращия сертификат (OCSP) за базовия удостоверителен орган (Evrotrust RSA Root CA).

Издава се за срок от 5 г.

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 38:00:00:00:02:46:4e:fc:a4:9d:94:68:e3:00:00:00:00:00:02 | |
| Signature Algorithm | SHA256RSA | |
| Valid from | 160520154459Z | |
| Validit to | 210521155459Z | |
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Subject | CN= | Evrotrust RSA Validation |
| | OU= | OCSP Signing |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Public Key | RSA(2048 Bits) | |
| Subject Key Identifier | DA:40:9F:0A:F0:65:11:77:52:14:65:5F:AF:00:CA:D5:6E:D9:DC:2C | |
| Key Usage (critical) | OCSP Signing | |
| Extended keyUsage | OCSP Signing (1.3.6.1.5.5.7.3.9) | |
| Authority Key Identifier | 74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70 | |
| OCSP No Revocation Checking | NULL | |
| Application policies | [1]Application Certificate Policy:<br>Policy Identifier=OCSP Signing | |

**20.2.** Профил на валидиращия сертификат за Оперативния удостоверяващ орган (Evrotrust RSA OperationalCA). Издава се за срок от 5 г.

| | |
|---|---|
| Version | V3 |
| Serial number | 2b:00:00:00:03:c3:3b:19:4b:08:91:37:24:00:00:00:00:00:03 |
| Signature Algorithm | SHA256RSA |
| Valid from | 160521014614Z |
| Validit to | 210520014614Z |

| | | |
|---|---|---|
| Issuer | CN= | Evrotrust RSA Operational CA |
| | OU= | Qualified Operational CA |
| | O= | Evrotrust Technologies JSC |
| | oganizationIdentifier (2.5.4.97) | NTRBG-203397356 |
| | C= | BG |
| Subject | CN= | Evrotrust RSA QS Validation |
| | OU= | OCSP QS Signer |
| | O= | Evrotrust Technologies JSC |
| | OrganizationIdentifier(2.5.4.97)= | NTRBG-203397356 |
| | C= | BG |
| Public Key | RSA(2048 Bits) | |
| Subject Key Identifier | 17:A2:1D:16:B0:BF:89:1F:A2:C5:86:BF:CB:DF:77:9F:35:76:7B:66 | |
| Key Usage (critical) | OCSP Signing | |
| Extended keyUsage | OCSP Signing (1.3.6.1.5.5.7.3.9) | |
| Authority Key Identifier | 7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08 | |
| OCSP No Revocation Checking | NULL | |
| Application policies | [1]Application Certificate Policy:<br>Policy Identifier=OCSP Signing | |