НАРЪЧНИК НА ПОТРЕБИТЕЛЯ

ЗА ПРЕДОСТАВЯНИТЕ ОТ "БОРИКА - БАНКСЕРВИЗ" АД B-TRUST® УДОСТОВЕРИТЕЛНИ, ИНФОРМАЦИОННИ, КРИПТОГРАФСКИ И КОНСУЛТАНТСКИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

Версия 2.3

21 Март 2016 г.

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК

АД	Акционерно дружество
ДВ	Държавен вестник
ЕГН	Единен граждански номер
ЗД	Закон за далекосъобщенията
ЗЕДЕП	Закон за електронния документ и електронния подпис
КЕП	Квалифициран Електронен Подпис
КРС	Комисия за регулиране на съобщенията
МТС	Министерство на транспорта и съобщенията
НДДУУ	Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията при предоставяне на удостоверителни услуги
НИАКЕП	Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис
Наръчник	Наръчник на потребителя за предоставяните от “БОРИКА - БАНКСЕРВИЗ” АД B-Trust® удостоверителни, информационни, криптографски и консултантски услуги
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на удостоверителни услуги
Политика	Политика за предоставяне на удостоверителни услуги

СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК

ASN.1	Abstract Syntax Notation One – Абстрактен език за описание на обекти в сертификатите
BG	Bulgaria – България
CA	Certification Authority – Удостоверяващ орган
CC	Common Criteria for Information Technology Security Evaluation - Международен стандарт (ISO/IEC 15408) за информационна сигурност
CD	Compact Disk – Компакт диск
CEN	European Committee for Standardization - Европейски стандартизационен комитет
CENELEC	European Committee for Electrotechnical Standardization - Европейски комитет за електротехническа стандартизация
CP	Certificate Policy – Политика за предоставяне на удостоверителни услуги
CPS	Certification Practice Statement – Практика при предоставяне на удостоверителни услуги
CRL	Certificate Revocation List – Списък с прекратени и спрени сертификати
DSA	Digital Signature Algorithm – Вид криптографски алгоритъм за създаване на подпис
DN	Distinguished Name – Уникално име
ECDSA	Elliptic Curve Digital Signature Algorithm – Вид криптографски алгоритъм за създаване на подпис
ETSI	European Telecommunications Standards Institute - Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз
FIPS	Federal Information Processing Standard – Федерален стандарт за обработка на информация
IEC	International Electrotechnical Commission - Международна електротехническа комисия
ISO	International Standardization Organization - Международна организация за стандартизация
IP	Internet Protocol – Интернет протокол
LDAP	Lightweight Directory Access Protocol – Протокол за опростен достъп до регистър
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за он-лайн проверка на статуса на сертификати
PKCS	Public Key Cryptography Standards – Криптографски стандарт за публичен ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
PSE	Personal Security Environment – Надеждна среда за генериране на двойка
QES	Qualified Electronic Signature – Квалифициран електронен подпис
RA	Registration Authority – Регистриращ орган
RSA	Rivest – Shamir - Adelman – Криптографски алгоритъм за създаване на подпис
SSCD	Secure Signature Creation Device – Устройство за сигурно създаване на подписа
B-Trust SSCD	SSCD със защитен профил, отговарящ на изискванията за ниво на сигурност EAL 4 или по-високо, съгласно CC или друга спецификация, определяща еквивалентни нива на сигурността
SHA	Secure Hash Algorithm – Хеш-алгоритъм за извличане на хеш-идентификатор
SSL	Secure Socket Layer – Сигурен канал за предаване на данни
S/MIME	Secure/Multipurpose Internet Mail Extensions – Протокол за сигурно предаване на електронна поща през Интернет
TRM	Tamper Resistant Module – Хардуерен модул неподатлив на интервенция
URL	Uniform Resource Locator – Единен ресурсен локатор

СЪОТВЕТСТВИЕ И УПОТРЕБА

Този „Наръчник на Потребителя":

- е разработен от „БОРИКА - БАНКСЕРВИЗ" АД, юридическото лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 201230426;
- подменя изцяло всички досегашни редакции на документа „Наръчник на потребителя за предоставяните удостоверителни, информационни, криптографски и консултантски услуги за универсален електронен подпис";
- влиза в сила на 21.03.2016г. ;
- съдържа условията, съгласно които Доставчикът на Удостоверителни слуги „БОРИКА - БАНКСЕРВИЗ" АД (Доставчик) предоставя на Потребители срещу възнаграждение удостоверения за квалифициран електронен подпис и свързаните с тях удостоверителни услуги, както и други удостоверителни, информационни, криптографски и консултантски услуги под запазената търговска марка B-Trust, чрез организационно обособено звено - Удостоверяващ орган B-Trust®, в съответствие с изискванията на Закона за Електронния Документ и Електронния Подпис (ЗЕДЕП);
- има характер на общи условия на основание чл. 33, ал. 2 Наредбата за Дейността на Доставчиците на Удостоверителни Услуги (НДДУУ) и по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД). Тези условия са част от писмен Договор за удостоверителни услуги, който се сключва между Доставчика и Потребителите на основание чл.23 от ЗЕДЕП. Договорът може да съдържа специални условия, които се ползват с предимство пред общите условия в Наръчника;
- включва подробно описание на практиката и политиките при предоставяне на удостоверителни услуги на Доставчика и е публичен документ с цел установяване на съответствие на дейността на Доставчика със ЗЕДЕП и нормативната уредба;
- може да бъде променян от ДУУ и всяка нова редакция на Наръчника се публикува на интернет-страницата на Доставчика;
- включва две части:
  - **ЧАСТ I:** Практика при предоставяне на удостоверения и удостоверителни услуги за квалифициран електронен подпис (Certification Practice Statement, CPS);
  - **ЧАСТ II:** Политика при предоставяне на удостоверения и удостоверителни услуги за квалифициран електронен подпис (Certificate Policy, CP);

Настоящият документ е изготвен в съответствие с:

- Закона за електронния документ и електронния подпис (ЗЕДЕП);
- Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията при предоставяне на удостоверителни услуги (НДДУУ);
- Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис (НИАКЕП);

Съдържанието и структурата на документа е в съответствие с общоприетата международна препоръка RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework и се позовава на информация, съдържаща се в следните утвърдени международни препоръки, спецификации и стандарти:

- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 2560: Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- ETSI TS 101 456: Policy requirement for certification authorities issuing qualified certificates;
- ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 101 862: Qualified certificate profile.

Всякаква информация, свързана с този документ, може да се получи от Доставчика на адрес:

бул. „Цар Борис III" № 41
София 1612
„БОРИКА - БАНКСЕРВИЗ" АД

ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

Практиката при предоставяне на удостоверения и удостоверителни услуги за квалифициран електронен подпис (КЕП):

- е неделима част от този документ и съдържа общите процедури по издаване, спиране, възобновяване и прекратяване действието на удостоверенията за КЕП, мерките за сигурност при предоставяне на удостоверителните услуги, изискванията към персонала, профила на издаваните и поддържани удостоверения, както и условията за достъп до издадените и прекратени удостоверения;
- се осъществява чрез работата на оперативните Удостоверяващи органи на Доставчика и се означава със следните идентификатори:

Практика на Доставчика	**Идентификатор (OID)**
B-Trust CPS QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1

- използва следните алгоритми за електронен подпис и защита на данните:

Алгоритъм	**Наименование**
Хеш-алгоритми:	SHA1, SHA256
Асиметрични алгоритми:	RSA

ПОЛИТИКА НА ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

Политиката на предоставяне на удостоверения и удостоверителни услуги за квалифициран електронен подпис:

- описва условията, които Доставчикът спазва и следва при издаване на удостоверения за КЕП, както и приложимостта на тези удостоверения с оглед на нивото на сигурност и ограниченията при използването им;
- е съвкупност от конкретни процедури, които се спазват в процеса на издаване и поддържане на удостоверенията за КЕП, от изискванията при идентификация, условията и изискванията за ниво на сигурност при създаване на електронния подпис и съхраняване на частния ключ;
- определя приложимостта и степента на доверие в удостоверените факти в тези удостоверения.

1. Доставчикът прилага обща Политика за всички типове удостоверения за КЕП, която се означава със следните идентификатори на политика в съответните удостоверения:

Политика на Доставчика	**Идентификатор (OID)**
B-Trust CP QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1

Съгласно тази Политика Доставчикът издава и поддържа следните типове удостоверения за КЕП:

- персонално удостоверение за КЕП на физическо лице „B-Trust Personal certificate QES";
- професионално удостоверение за КЕП на физическо лице „B-Trust Professional certificate QES";

2. Доставчикът си запазва правото да разшири поддържаните Политики на издавани удостоверения чрез оперативните Удостоверяващи органи.

НАРЪЧНИК НА ПОТРЕБИТЕЛЯ - ЧАСТ I:

ПРАКТИКА

ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

ВЪВЕДЕНИЕ

Практиката при предоставяне на удостоверителни услуги за КЕП е съставна част на този документ, разработен от ДУУ „БОРИКА - БАНКСЕРВИЗ" АД и одобрен от КРС.

Тази част на документа съдържа описание на участниците в инфраструктурата на публични ключове B-Trust® и на нейните компоненти, чрез които Доставчика издава, поддържа, публикува и управлява удостоверенията за КЕП.

Описани са общите оперативни процедури при заявяване на удостоверения, идентифициране на заявители, издаване и публикуване, доставяне и приемане на удостоверенията, поддръжка и управление на тези удостоверения.

Практиката включва още мерките и следваните технически процедури от страна на Доставчика, които гарантират сигурността и надеждността на предоставяните удостоверителни услуги чрез инфраструктурата на B-Trust® в съответствие със ЗЕДЕП и нормативната уредба.

Документът е разработен в съответствие с формалните изисквания за съдържание, структура и обхват, посочени в международната препоръка RFC 3647, доколкото тя отговаря на управленската политика на Доставчика.

Документът включва и допълнителна информация с оглед на изискванията в нормативната уредба по ЗЕДЕП.

1 ОСНОВНИ ПОЛОЖЕНИЯ

1.1 Доставчик на удостоверителни услуги

1. „БОРИКА - БАНКСЕРВИЗ" АД е юридическо лице - търговец, осъществяващо дейност на ДУУ съгласно ЗЕДЕП и нормативната уредба.
2. В качеството си на регистриран ДУУ, „БОРИКА - БАНКСЕРВИЗ" АД осъществява следните правно-регламентирани дейности по:
   - издаване на удостоверения:
     - приемане на искане за първоначално издаване;
     - установяване на идентичност и валидни данни за Автора/Титуляря;
     - подписване на удостоверение;
     - запис на издадено удостоверение на SSCD.
   - поддръжка и управление на удостоверения:
     - подновяване на издадено валидно удостоверение;
     - промяна в статуса на валидно удостоверение - спиране, възобновяване и прекратяване;
     - проверка на статуса на удостоверение;
     - проверка на статуса на удостоверение в реално време (OCSP статус).
   - водене на регистри:
     - водене на публичен регистър на всички издадени удостоверения;
     - публикуване на издадено удостоверение в публичния регистър;
     - водене на списък на всички прекратени удостоверения;
     - незабавно публикуване на прекратено удостоверение в списъка с прекратени удостоверения;
     - постоянен достъп на трети лица до публичния регистър и до списъка на прекратени удостоверения.
   - удостоверяване на време:
     - удостоверяване на точно време на представено съдържание на електронно подписан документ (време на подписване);
     - удостоверяване на съдържане в даден момент и непроменимост на съдържанието след този момент;
     - доказателствена проверка на издадените удостоверения за време.
   - предоставяне на SSCD за генериране и съхранение на криптографски ключове и за създаване на електронен подпис.
3. Доставчикът предоставя посочените удостоверителни услуги в съответствие с настоящата Практика на Удостоверяващия орган и посочената в удостоверението Политика.
4. Доставчикът може да предоставя и други удостоверителни, криптографски, информационни и консултантски услуги, свързани с приложимостта на КЕП, следвайки общоприетите препоръки, спецификации и стандарти.
5. Доставчикът може да публикува отделно общи условия за тези услуги.

1.2 Регулация и контрол

1. „БОРИКА - БАНКСЕРВИЗ" АД е уведомило КРС за започване на дейност като ДУУ по реда на ЗЕДЕП и действащата нормативна уредба.
2. Акредитацията на "БОРИКА - БАНКСЕРВИЗ" АД като ДУУ по ЗЕДЕП цели най-високо ниво на сигурност на предоставяните удостоверителни услуги и по-добро хармонизиране на тази дейност със съответната такава в страните-членки на Европейския съюз.
3. Доставчикът уведомява Потребителите за своята акредитация при предоставяне на удостоверенията за КЕП и на удостоверителни услуги за тях.

1.3 Идентификатори в документа

1. Практиката на Доставчика при издаване и поддържане на удостоверения за КЕП се осъществява посредством оперативен Удостоверяващ орган B-Trust Operational CA QES и се означава в удостоверението на този Орган със следния идентификатор:

O.I.D. = 1.3.6.1.4.1.15862.1.5.1

2. Политиката на Доставчика относно удостоверенията за КЕП и предоставяните за тях удостоверителни услуги се означава в издаваните удостоверения със следния идентификатор:

   O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1

3. Доставчикът следва посочените означения на Политика за издаваните и поддържани типове удостоверения за КЕП:

Тип на Удостоверение	Наименование на удостоверение	Политика	Идентификатор на Политика (OID)
Персонално удостоверение за КЕП на физическо лице	B-Trust Personal Certificate QES	B-Trust CP QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1
Професионално удостоверение за КЕП на физическо лице	B-Trust Professional Certificate QES	B-Trust CP QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1

1.4 Участници в инфраструктурата на B-Trust®

1.4.1 Удостоверяващ орган

1. „Удостоверяващия орган" на B-Trust® на ДУУ "БОРИКА - БАНКСЕРВИЗ" АД е организационно обособено звено, което осъществява дейността му по издаване на удостоверения за КЕП, по предоставяне и по поддържане на удостоверителни услуги за тях. Удостоверяващият орган няма самостоятелна правосубектност и всички осъществени действия и актове на служителите му се извършват в качеството им на служители на Доставчика, в рамките на предоставените им правомощия.
2. Инфраструктурата на B-Trust® има двустепенна йерархия на Удостоверяващи органи за издаване и поддръжка на удостоверения за КЕП, както следва:
   - Базов Удостоверяващ орган ***„B-Trust Root CA"*** - издава удостоверения на подчинените оперативни удостоверяващи органи на Доставчика и такива на други Доставчици. Той издава и удостоверенията за поддържащите оперативни органи на ДУУ;
   - Оперативен Удостоверяващ орган ***„B-Trust Operational CA QES"*** - издава удостоверения за КЕП на Потребители;
3. ДУУ си запазва правото да разшири инфраструктурата на B-Trust® с друга йерархия от Удостоверяващи органи, различна от тази за КЕП (например, за приложно ориентирани удостоверения).

1.4.2 Регистриращ орган

1. „Регистриращият орган" е звено, което осъществява дейности на Доставчика, както следва:
   - приема, проверява, одобрява или отхвърля искания за издаване на удостоверения;
   - регистрира подадени искания до Удостоверяващия орган за издаване и внася промени в статуса на удостоверенията;
   - осъществява съответни проверки за установяване на самоличността на Автора и идентичността на Титуляря, както и на специфични данни за тях с допустимите средства, и в съответствие с Политиката и Практиката при предоставяне на съответната удостоверителна услуга;
   - уведомява Удостоверяващия орган да издаде удостоверение след успешна идентификация и заплатена услуга;
   - предава на Автора /Титуляря издаденото удостоверение за КЕП, съответстващо на генерираната двойка ключове;
   - приема или отхвърля регистрирани искания за поддръжка и управление на удостоверения в съответствие с утвърдената Практика и Политика;
   - сключва договори за предоставяне на удостоверителни и други криптографски, информационни и консултантски услуги с титулярите от името на Доставчика.
2. Регистриращият орган може да бъде обособено звено в рамките на юридическо лице, различно от Доставчика, на което са делегирани права да осъществява тези дейности или на част от тях от името на Доставчика.
3. Регистриращият орган на Доставчика може да разкрива и да предоставя удостоверителни услуги на Потребители чрез Местни Регистриращи Служби (МРС).
4. Когато Регистриращият орган/МРС е самостоятелно юридическо лице, правомощието да осъществява тази

дейност може да бъде ограничено за определена територия, срок, удостоверителни услуги или за определена категория Автори/Титуляри. Правомощието се удостоверява пред заявителите и всички трети лица с писмено или електронно удостоверение за Регистриращия орган/МРС.

5. В случаите, когато Регистриращият орган е самостоятелно юридическо лице, МРС към този орган се разкриват само след изрично одобрение от страна на Доставчика.
6. Отношенията между Доставчика и Регистриращия орган/МРС по т.4 се уреждат с договор.
7. Доставчикът гарантира, че дейността на Регистриращия орган/МРС ще бъде съобразена с условията на настоящия Наръчник.

1.4.3 Орган за удостоверяване на време

1. „Орган за удостоверяване на време" е обособено и неделимо звено към Удостоверяващия орган, което осъществява дейности на Доставчика, както следва:
   - приема заявки за удостоверяване на време на представено съдържание на електронен документ от Автор/Титуляр или Доверяваща се страна;
   - изготвя удостоверение за време на представения електронен документ;
   - осигурява възможност за последващо (след периода на валидност на удостоверението) доказване спрямо Автора на факта на подписването на изявление или на електронен документ.
2. „B-Trust TSA" е Органът за удостоверяване на време на Доставчика.
3. Електронният подпис на удостоверението за време е със статус на квалифициран електронен подпис на Доставчика.
4. Удостоверенията за време се издават на физически и на юридически лица, които са Автори/Титуляри или са Доверяваща се страна спрямо използваните удостоверения за електронен подпис.
5. Удостоверенията за време могат да се интегрират в процеса на създаване или приемане на КЕП, на електронно подписани документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и други.
6. Доставчикът разработва и публикува отделна Политика на Органа за удостоверяване на време.

1.4.4 Орган за валидация

1. „Орган за валидация" е обособено и неделимо звено на Удостоверяващия орган, което осъществява дейности на Доставчика както следва:
   - приема заявки от Автор/Титуляр или Доверяваща се страна за проверка в реално време на статуса на представено удостоверение, издадено от Доставчика;
   - изготвя автоматично в реално време електронно подписан отговор за статуса на представено удостоверение.
2. „B-Trust VA" и „B-Trust VA QES" са Органите за валидация на Доставчика.
3. Електронният подпис на получения отговор е със статус на КЕП на Доставчика.
4. Всяка доверяващата се страна, когато приема удостоверения за електронен подпис, може да заяви проверка на статуса на удостоверенията в реално време.
5. Проверката на статуса на удостоверения в реално време не е задължителна за Доверяващите се страни, но Доставчикът препоръчва да се използва тази услуга и нейното интегриране в процеса на създаване или приемане на КЕП, при проверка и приемане на електронни транзакции и други.

1.4.5 Абонати

1. „Абонат" е физическо или юридическо лице, което има сключен писмен договор с Доставчика за предоставяне на удостоверителни услуги.
2. Абонат, заявил пред Доставчика издаването на удостоверение за КЕП, е Автор/Титуляр на електронния подпис и се вписва като такъв в издаденото от Доставчика удостоверение.

1.4.6 Титуляр

1. „Титуляр" в удостоверение за КЕП е физическо или юридическо лице, от името на което Авторът подписва електронни изявления, и е посочено като такъв в издаденото удостоверение.

1.4.7 Автор

1. „Автор" в удостоверение за КЕП е физическо лице, което осъществява от свое име или от името на Титуляря, ако такъв е вписан в удостоверението, електронни изявления и ги подписва в съответствие с предоставената му представителна власт, и е посочено в издаденото удостоверение като Автор.

2. В удостоверението за КЕП може се посочи основанието за овластяване на Автора.
3. Единствено Авторът като Потребител на удостоверението за КЕП, има право на достъп до частния ключ за подписване на електронни изявления (създаване на електронен подпис).

1.4.8 Доверяващи се страни

1. „Доверяващи се страни" са адресатите на подписани електронни изявления, Авторите на които притежават издадени от Доставчика удостоверения за КЕП.
2. Доверяващите се страни следва да имат познания и умения относно използването на удостоверения за електронен подпис и се доверяват на удостоверените обстоятелства в тях само с оглед на приложимата Политика, особено по отношение на нивото на сигурност при проверка на самоличността на Авторите и идентичността на Титулярите на тези удостоверения.
3. Доверяващите се страни имат постоянен достъп до регистрите на Доставчика за проверка на валидността на удостоверенията за КЕП, за установяване на електронната идентичност/автентичност на Авторите/Титулярите или на други обстоятелства и данни, отразени в удостоверенията или вписани в тези регистри.

1.5 Удостоверения и употреба

1.5.1 Определение

1. "Удостоверение за публичен ключ" (накратко „удостоверение") е подписан от Доставчика електронен документ, съдържащ определени реквизити, удостоверяващи връзката между Автора/Титуляря и публичния му ключ, съответстващ на частния ключ, с който Автора е създал електронния подпис и служи за проверка на подписа в електронни документи и обекти.
2. Удостоверенията могат да се използват за дейности, които изискват електронна идентификация, подписване, автентификация и криптиране на електронни документи и обекти.
3. Само удостоверенията с означените в този документ политики, които издава Доставчикът, имат характер на удостоверения за КЕП и съдържат предвидените в чл. 24 от ЗЕДЕП реквизити.

1.5.2 Удостоверения на Доставчика

Базово удостоверение

1. Базово удостоверение на Доставчика е самоиздадено и самоподписано с базовия частен ключ на Доставчика удостоверение за неговия базов публичен ключ. С базовия частен ключ Доставчикът подписва удостоверения за публични ключове на свои оперативни Удостоверяващи органи, както и удостоверения на други (под)доставчици на удостоверителни услуги в инфраструктурата на B-Trust.
2. В съответствие със ЗЕДЕП и йерархията от Удостоверяващи органи в инфраструктурата на B-Trust, Доставчикът предоставя на КРС валидното удостоверение на базовия Удостоверяващ орган.
3. Основните реквизити на базовото удостоверение на Удостоверяващия орган „B-Trust Root CA" на Доставчика са:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	01
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 април 2015 09:25:01 UTC
Validity to	-	16 април 2035 09:25:01 UTC
Subject	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d

Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path Length Constraint =	CA 4
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=All issuance polices [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	70 01 49 a2 e6 3c 21 ac d0 54 9f 87 de 8c df aa c9 93 f1 b0
Thumbprint (Sha256)	-	1f b2 11 4a 2c e4 bc 4d 56 b1 7b 03 a4 55 18 3b 31 65 40 b2 a0 fa d5 ce c2 b2 5a 84 eb 83 d5 29

4. На основание чл. 16, ал. 3, т. 2 на ЗЕДЕП подписите на Доставчика, които са придружени от базовото удостоверение са КЕП.
5. Доставчикът може да инсталира и поддържа други базови удостоверения в инфраструктурата на B-Trust.

Оперативно удостоверение за издаване на удостоверения за КЕП

1. Удостоверение на оперативен Удостоверяващ орган на Доставчика за издаване на удостоверения за КЕП е удостоверението за публичния ключ на оперативния Удостоверяващ орган „B-Trust Operational CA QES", подписано с базовия частен ключ на Доставчика. С частният ключ, съответстващ на този публичен ключ, оперативния Удостоверяващ орган подписва издаваните от Доставчика удостоверения за КЕП на Потребителите.
2. В съответствие със ЗЕДЕП и йерархията от Удостоверяващи органи в инфраструктурата на B-Trust, Доставчикът предоставя на КРС валидните удостоверения на оперативните Удостоверяващи органи.

Основните реквизити на оперативното удостоверение на Удостоверяващия орган „B-Trust Operational CA QES" на Доставчика са:

Поле	**Атрибути**	**Значение/Стойност**
Version	-	V3
Serial number	-	02
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 април 2015 09:29:53 UTC
Validity to	-	16 април 2030 09:29:53 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org

	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a
Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate Serial Number=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path length Constrain =	CA 3
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.2 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	91 ab 04 6d 20 c6 ac 63 57 6d 69 d8 7c 2b 9f 3b 40 3d ef c2
Thumbprint (Sha256)	-	f3 b7 0a 38 f7 83 36 b5 97 b7 72 e7 85 24 85 44 ce 1b fc ee 28 15 3b 87 07 f7 e2 1f 2a 33 45 3d

3. На основание чл. 16, ал. 3, т. 2 на ЗЕДЕП подписите на Доставчика, които са придружени от това оперативно удостоверение са КЕП.
4. Доставчикът може да инсталира и поддържа други оперативни удостоверения в инфраструктурата на B-Trust.

Удостоверение на Орган за удостоверяване на време

1. Удостоверение на Органа за удостоверяване на време на Доставчика е удостоверение за публичния ключ, подписано с базовия частен ключ на Доставчика. С частния ключ на Органа за удостоверяване на време на Доставчика се подписват удостоверенията за време на представяне на съдържание на електронен документ от Потребител и/или Доверяваща се страна.
2. Реквизитите на служебното удостоверение на Органа за удостоверяване на време „B-Trust TSA" на Доставчика са:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	0b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 април 2015 09:34:16 UTC
Validity to	-	15 април 2020 09:34:16 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5tss@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117.
	CN =	B-Trust Time Stamp Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2d 79 0e 96 e8 dc 9d c2 40 fd 08 71 da ae 06 67 4e 49 e6 2e
Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d
		Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://tss.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.crl
Authority Information Access		[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage (critical)	-	Time Stamping (1.3.6.1.5.5.7.3.8)
Thumbprint (Sha1)		17 8e 35 12 63 06 b2 eb 74 a9 e5 c7 72 e6 9d 7a ee a8 0a 8c
Thumbprint (Sha256)		4f a4 8f 10 1b a9 69 db 32 b3 1f d9 00 3b 74 4a fa 97 91 c2 20 5a 37 10 a4 94 5b 94 a7 7b e7 0d

3. Подписите на Доставчика, които са придружени от служебното удостоверение на Органа за удостоверяване на време "B-Trust TSA" са КЕП.
4. Доставчикът публикува отделна Политика, включваща условията и процедурите по издаване на удостоверения за време от Органа за удостоверяване на време.

Удостоверения на Органа за валидация

1. Удостоверенията на Органа за валидация на Доставчика са удостоверения на публичния ключ, подписани съответно с базовия частен ключ на Доставчика и оперативния ключ на Доставчика. С частните ключове на двойките ключове на Органите за валидация „B-Trust VA" и „B-Trust VA QES" Доставчикът подписва резултатът/отговорът от проверката в реално време на статуса на представени удостоверения за електронен подпис.
2. Реквизитите на служебното удостоверение на Органа „B-Trust VA" на Доставчика са:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	0c
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 април 2015 10:34:53 UTC
Validity to	-	15 април 2020 10:34:53 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5va@b-trust.org
	PostalCode =	1784
	STREET =	bul. Tsarigradsko shose No 117
	CN =	B-Trust Validation Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	14 e9 ea 3d 65 1c cc 97 e9 c6 7b 98 f2 02 11 18 c4 d7 a7 34
Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type =	End Entity
	Path length Constrain =	None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.crl
Authority Information Access		[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation	-	05 00

Checking		
Thumbprint (Sha1)		66 7a 4d 10 e5 2d e2 df bb 89 b9 d3 01 bb 9d a1 97 1d 7c 2a
Thumbprint (Sha256)		ba e0 56 2a cf 8d 57 de f9 8e db 2d fc 03 f7 fe b0 20 bf f0 c6 77 dd 72 13 24 47 42 25 d7 ae ac

3. Реквизитите на служебното удостоверение на Органа „B-Trust VA QES" на Доставчика са:

Поле	**Атрибути**	**Значение/Стойност**
Version	-	V3
Serial number	-	10
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	07 май 2015 10:51:30 UTC
Validity to	-	06 май 2020 10:51:30 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5va@b-trust.org
	PostalCode =	1784
	STREET =	bul. Tsarigradsko shose No 117
	CN =	B-Trust Validation Authority QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2c 36 5a f3 2a db c1 a0 e8 f6 5e ae 95 25 94 d2 e3 4d 5a 0a
Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		2a 58 a0 7e 93 ab ea 40 79 9e 03 08 ba a4 26 80 89 3e 1c 6c
Thumbprint (Sha256)		7d f3 55 fc 8f 61 78 d9 ad a9 87 43 89 ab 47 05 91 d5 a5 e0 fa aa ac b9 4a 4c bc af d1 37 3a ca

4. Подписите на Доставчика, които са придружени от служебните удостоверения на „B-Trust VA" или „B-Trust VA QES" са КЕП.

1.5.3 Удостоверения на други оперативни органи

1. Доставчикът може да издава оперативни удостоверения на други удостоверяващи органи в инфраструктурата на B-Trust, както и на други Доставчици, когато последните:
   - осъществяват дейност извън правно регламентираната в ЗЕДЕП, с цел функциониране като доставчик;
   - взаимно удостоверяват публичните оперативни ключове с оглед повишаване на доверието в предоставяните удостоверителни услуги (крос-сертифициране);
   - осъществяват правно регламентирана дейност на ДУУ съгласно ЗЕДЕП.
2. Издаването на тези удостоверения се осъществява на базата на конкретна договореност със съответните доставчици.

1.5.4 Удостоверение за квалифициран електронен подпис

1. Доставчикът издава на Потребители удостоверения за КЕП в зависимост от заявителите, приложното поле и предназначение на електронния подпис:
   - персонално удостоверение за КЕП „B-Trust Personal Certificate QES";
   - професионално удостоверение за КЕП „B-Trust Professional Certificate QES";
2. Практиката и Политиката на Доставчика, съгласно този документ, определят правилата и изискванията за сигурност, приложими при издаване и използване на удостоверенията за КЕП.
3. Доставчикът издава удостоверение за КЕП по смисъла на чл. 24 на ЗЕДЕП само на физическо лице.
4. Персонално удостоверение за КЕП „B-Trust Personal Certificate QES" се издава персонално на физическо лице - Автор. Искането за издаване на това удостоверение се прави отдалечено (по електронен способ) или локално (на място) в Регистриращ орган/МРС, като процедурата по идентификация чрез установяване на самоличността на Автора/Титуляря изисква лично присъствие или изрично упълномощаване от страна на автора. Идентификационната процедура и процедурите по генериране на двойката ключове, по издаване и по предоставяне на удостоверението на Автора гарантират най-високо ниво на сигурност на данните за Автора в удостоверението и връзката им с публичния ключ.
5. Професионално удостоверение за КЕП „B-Trust Professional Certificate QES" се издава на физическо лице - Автор, представляващо Титуляря по силата на закона или упълномощаване.
6. Искане за регистрация и издаване на съответното квалифицирано удостоверение се прави онлайн или локално (на място) в Регистриращ орган/МРС като процедурата по идентификация чрез установяване на самоличността на Автора и идентичността на Титуляря изисква лично присъствие на Автора или изрично упълномощено от него лице, респективно на физическо лице упълномощено от Титуляря. Идентификационната процедура и процедурите при генериране на двойката ключове, при издаване и предоставяне на удостоверението на Автора/Титуляря гарантират най-високо ниво на сигурност на данните за Автора/Титуляря в удостоверението и връзката им с публичния ключ.
7. Удостоверенията „B-Trust Personal Certificate QES" и „B-Trust Professional Certificate QES" и съответстващите им частни ключове се съхраняват и предоставят на Потребителите задължително на SSCD.
8. Удостоверенията за КЕП имат значението на саморъчен подпис спрямо всички по смисъла на чл.13, ал.4 на ЗЕДЕП.

1.5.5 Предназначение на удостоверенията за КЕП

1. Издадено удостоверение за КЕП от Удостоверяващ орган на Доставчика може да се използва по предназначение съобразно Политиката за това удостоверение.
2. Всяко удостоверение съдържа като реквизит поле за предназначение на удостоверението. Реквизитът е от категорията "критични" и се идентифицира като "Key Usage".
3. Издаваните от Доставчика удостоверения могат да се използват с едно или едновременно с няколко от следните предназначения:
   - автентификация (authentication) - да установи авторството на направени електронни изявления;
   - конфиденциалност (confidentiality) - да криптира и декриптира направени електронни изявления или информационни обекти;
   - цялостност (integrity) - да запази целостта и непроменимостта на направени електронни изявления или на информационни обекти;
   - неотменимост (non-repudiation) - да осигури възможност за последващо доказване спрямо Автора, на факта на подписване на електронно изявление или на съдържание и на невъзможност за отказ от положения подпис.

4. Чрез реквизит „Extended Key Usage", който също се съдържа в издаваните от Доставчика удостоверения за КЕП и е от категорията "некритични", се детайлизира приложимостта на удостоверението с оглед предназначението му.
5. Приложното поле на издаваните типове удостоверения за КЕП е както следва:

Тип на удостоверение	Приложимост
Персонално удостоверение за КЕП „B-Trust Personal Certificate QES"	Персонална електронна идентичност в приложения, изискващи най-високо ниво на сигурност - уеб-базирани приложения за електронна търговия, електронно подписване на документи, електронно подписване на договори, банкови транзакции, водене на кореспонденция и извършване на изявления от и до държавни органи и органи на местното самоуправление по смисъла на ЗЕДЕП.
Професионално удостоверение за КЕП „B-Trust Professional Certificate QES"	Електронна професионална идентичност в приложения, изискващи най-високо ниво на сигурност - уеб-базирана електронна търговия, електронно подписване на документи, банкови транзакции, водене на кореспонденция и извършване на изявления от и до държавни органи и органи на местното самоуправление по смисъла на ЗЕДЕП.

1.5.6 Ограничение на удостоверителното действие

1. Ако удостоверението за КЕП се издава с ограничение на удостоверителното действие и в съответствие с чл.24, ал.1, т.8 на ЗЕДЕП, Практиката на Доставчика допуска да се вписва в удостоверението ограничение на електронния подпис по отношение на цели и/или стойност на сделки между Титулярите при използване на подписа.
2. По преценка, Доставчикът може да използва реквизита "Qualified Statements" или друг подходящ такъв в профила X.509, v.3 на удостоверенията за КЕП.
3. Ограничителното действие на издадени удостоверения за КЕП по отношение на стойността на сделките, които Титулярите сключват посредством използване на електронен подпис, се съгласува между тях и всяка Доверяваща се страна и е извън обхвата на настоящия Наръчник.

1.5.7 Употреба на удостоверения извън приложното поле и ограниченията

1. Когато Автор/Титуляр или Доверяваща се страна използват и се доверяват на удостоверение за КЕП с предназначение, различно от указаните в реквизити "Key Usage", "Extended Key Usage", „Certificate Policy" или „Qualified Statements", отговорността е изцяло тяхна и не ангажира с отговорност Доставчика по никакъв начин.

1.6 Управление на Практиката и Политиката на Доставчика

1. Практиката и Политиката на Доставчика подлежат на административно управление и контрол от страна на Съвета на директорите на „БОРИКА - БАНКСЕРВИЗ" АД.
2. Допускат се промени, редакции и допълнения, които не засягат правата и задължения, произтичащи от този документ и стандартния договор между Доставчика и Потребителите след съгласуване и утвърждаване от Съвета на директорите.
3. Всяка представена и одобрена нова версия или редакция на този документ незабавно се публикува на сайта на Доставчика.
4. Коментари, запитвания и разяснения по този документ могат да се отправят на:
   - електронен адрес на Удостоверяващ орган: info@b-trust.org;
   - електронен адрес на Доставчика: info@bobs.bg;
   - тел.: (02) 9215 100 и факс: (02) 981 45 18

2 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР

2.1 Публичен регистър

1. Доставчикът води електронен Публичен регистър, в който публикува:
    - всички издадени удостоверения за КЕП на Потребители и актуален Списък на прекратените удостоверения (CRL) за КЕП, както и своите служебни удостоверения;
2. Публичният регистър на всички издадени удостоверения и актуалните CRL са постоянно достъпни, освен в случаите на събития, извън контрола на Доставчика и при настъпили форсмажорни обстоятелства.
3. Автор/Титуляр на издадено от Доставчика удостоверение е длъжен да провери верността и пълнотата на информацията в удостоверението, независимо, че то е прието.
4. Доставчикът предоставя на всяко трето лице при поискване информацията касаеща статуса на издадено удостоверение. Доставчикът предоставя информацията, съдържаща се в издаденото удостоверение, при наличие на нормативно установено задължение да я предостави и при надлежно искане от оправомощен орган или лице.
5. Актуалният CRL съдържа информация за всички прекратени и спрени удостоверения до момента на публикуването му в регистъра. Спряно удостоверение се поддържа в CRL за период от време, регламентиран от ЗЕДЕП и предвиден в Наръчника. Ако удостоверението бъде възобновено или след регламентирания период от време, то се отстранява и актуализираният CRL се публикува без него.

2.2 Публично хранилище на документи

1. Доставчикът публикува и поддържа в електронно хранилище актуални и предишни версии на:
    - Общи положения и условия, съдържащи се в Наръчника;
    - Практиката при предоставяне на удостоверителни услуги;
    - Политиката при предоставяне на удостоверителни услуги;
    - Договор за удостоверителни услуги;
    - Тарифа на предоставяните удостоверителни услуги;
    - Правила за издаване на удостоверения за КЕП, включително правилата за установяване на идентичността на Титуляря на КЕП;
    - Условия и ред за използване на КЕП, включително изискванията за съхраняване на частния ключ;
    - Документи, изискуеми при първоначално издаване на удостоверения за КЕП, при подновяване и спиране/прекратяване на удостоверенията;
    - Други документи, изискуеми по ЗЕДЕП и нормативната уредба

2.3 Публикуване на информация за удостоверенията

1. Доставчикът незабавно публикува в Регистъра издадено валидно удостоверение след подписването му от оперативните Удостоверяващи органи „B-Trust Operational QES".
2. Доставчикът незабавно публикува актуален CRL, подписан от оперативен Удостоверяващ орган след прекратяване/спиране на всяко валидно удостоверение за КЕП. Актуалният CRL включва и прекратеното и/или спряно удостоверение.
3. Ефективният период на валидност на публикувания актуален CRL е 30 дни, освен ако не се извърши актуализацията му.

2.4 Честота на публикуване

1. Актуализация на публичния Регистър на издадените удостоверения се осъществява автоматично и незабавно след публикуване на всяко новоиздадено валидно удостоверение.
2. Актуализация на текущия CRL се осъществява автоматично на не повече от 3 (три) часа или незабавно след прекратяване или спиране/възобновяване на валидно удостоверение. Във всички CRL ДУУ указва времето за следващото издание на CRL.
3. Публикуване на нова редакция или версия на Наръчника, както и на други съпътстващи документи по ЗЕДЕП, се осъществява незабавно.

2.5 Достъп до Регистъра и до хранилището

1. Доставчикът води Публичен регистър на издадените удостоверения за КЕП, който е он-лайн публично достъпен.

2. Доставчикът не може да ограничи достъпа до Публичния регистър. С оглед защита на личните данни на Потребителите достъпът на трети лица за изтегляне на публикуваните удостоверения е ограничен, освен ако съответният Потребител изрично не е поискал достъпът да бъде свободен.
3. Няма ограничение до Наръчника и на съдържащите се в него условия, Практика и Политики. Всяко заинтересовано лице има право на достъп до публикуваните документи.
4. Няма ограничение на достъпа за търсене на издадено и публикувано удостоверение с цел проверка на статуса му. Всяко заинтересовано лице може да търси публикувано удостоверение (валидно или с изтекъл срок на валидност) по определени атрибути.
5. Всяко заинтересовано лице има право на свободен достъп за четене и изтегляне по електронен път на CRL.
6. Всяко заинтересовано лице има право на свободен достъп до служебните удостоверения на Доставчика.
7. Доставчикът осигурява свободен достъп до всички базови и оперативни удостоверения на своите активни удостоверителни органи, както и свободен достъп до тези на всички неактивни такива за срок не по-малък от 2 (две) години след изтичане на срока на валидност на тези удостоверения.

3 ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ

1. Доставчикът, чрез свой Регистриращ орган/МРС:
   - приема искания за издаване на удостоверения;
   - осъществява проверка за установяване на самоличността на Автора, съответно идентичността на Титуляря и на специфични данни за тях с допустими средства;
   - утвърждава след успешна проверка или отхвърля регистрираните искания;
   - уведомява Удостоверяващия орган да издаде исканото удостоверение.
2. Регистриращият орган/МРС събира и получава необходимата информация за идентификация и автентификация на Автора/Титуляря.
3. Автентификацията/идентификацията на Автора/Титуляря след регистрация и преди да бъде издадено удостоверение за КЕП, изисква негово лично присъствие или присъствие на упълномощен представител на заявителя в Регистриращия орган/МРС.
4. Доставчикът гарантира, че физическите и юридическите лица са правилно идентифицирани, автентифицирани и че заявките за издаване на удостоверения за КЕП са напълно, акуратно и надлежно проверени и одобрени, включително: пълното име/наименование и правния статус на съответното физическо/юридическо лице; доказателства за връзката между удостоверените данни и физическото/юридическото лице.

3.1 Именуване

3.1.1 Използване на имена

1. Удостоверенията за КЕП са с формат, съответстващ на стандарта X.509. Регистриращ орган/МРС, работещ от името на Доставчика утвърждават, че имената в заявките за удостоверения съблюдават стандарта X.509.
2. Полето „Subject" в удостоверението електронно идентифицира Автора/Титуляря свързан с публичния ключ в удостоверението за КЕП.
3. Името и други индивидуализиращи белези на Автора/Титуляря в съответните полета за всеки тип удостоверение са в съответствие с DN (Distinguished Name), формиращо се съобразно стандарта X.500 и X.520.
4. Служебните удостоверения на Доставчика съдържат в полето "Subject" и поле "Issuer" атрибут DN формиращ неговото уникалното име.
5. Детайлна спецификация на издаваните от Доставчика удостоверения за КЕП се съдържа в съответните глави на настоящия документ.

3.1.2 Използване на псевдоним

1. Доставчикът може да издава удостоверение за КЕП като използва „псевдоним" за да именува Автора само след като Регистриращият орган/МРС събере необходимата информация за самоличността му и успешно го идентифицира.

3.1.3 Значимост на имената при вписване

1. Удостоверенията на удостоверяващите органи на Доставчика съдържат уникални имена с общоразбираема семантика, позволяваща определянето на идентичността на Доставчика, субект на удостоверението.
2. Удостоверенията за КЕП на Потребители съдържат имена, съвпадащи с автентифицираните идентификационни имена на Титуляри/Автори, субекти на издадените удостоверения.
3. За по-удобна електронна комуникация с Автора/Титуляря, Доставчикът изисква и удостоверява в удостоверението за КЕП имейл адрес на Автора. В случай, че последният не разполага с такъв, Доставчикът може да му предостави имейл адрес в домейна B-Trust.

3.1.4 Правила за интерпретация на имената

1. Доставчикът включва в удостоверенията за КЕП на Потребители информация за електронна идентификация на Автора/Титуляря, която е успешно проверена и потвърдена от Регистриращия орган/МРС, въз основа на представените документи за самоличност на Автора и идентичност на Титуляря.
2. Във всички удостоверения, в които се вписва Автор, полето за име (Common Name, CN) съдържа пълното име на физическото лице/Автор или неговия псевдоним.

3. В професионалното удостоверение, атрибутът за уникално име (DN) съдържа информация за идентичността на юридическото лице/Титуляр на удостоверението.

3.1.5 Уникалност на имената

1. Електронната идентификация на Автор/Титуляр на издадено от Доставчика удостоверение за КЕП е на базата на DN.
2. Полето "Subject" в удостоверението се формира от информацията за Автора/Титуляря, която се предоставя он-лайн или на хартия от заявителя или от упълномощен представител при регистрация на първоначално искане за издаване на удостоверение и която се проверява в Регистриращия орган/МРС на базата на представените документи.
3. Доставчикът гарантира уникалност на „DN" на Автора/Титуляря в домейна B-Trust чрез добавяне на реквизит, който гарантира такава уникалност.
4. Автор/Титуляр с уникален DN в домейна B-Trust може да има повече от едно издадени действителни удостоверения за КЕП.
5. Всяко издадено удостоверение има уникален сериен номер ("SerialNumber") в домейна на Доставчика (B-Trust). Комбинацията на полета „Issuer", "SerialNumber" и „Validity from“ гарантира уникалността на издаденото удостоверение в публичния домейн.

3.1.6 Признаване, автентичност и роля на търговските марки

1. Титуляри/Автори нямат право да заявяват издаване на удостоверения с използване на имена, които нарушават чужди имуществени или неимуществени права.
2. Притежатели на такива права удостоверяват това свое право с официален документ пред Регистриращия орган/МРС при искането за издаване на удостоверението.
3. Доставчикът не носи отговорност, когато използвани имена в удостоверения нарушават чужди права върху търговско име, търговска марка, домейни, авторски права и др.
4. В случай на възникнал спор по отношение на използвани имена, Доставчикът си запазва правото да не издаде удостоверение или ако такова е издадено, да го прекрати.
5. Доставчикът не включва търговски марки, запазени знаци или друг графичен материал в удостоверенията, които издава.

3.2 Първоначална идентификация и установяване на идентичност

1. За първоначална идентификация/установяване идентичността на Титуляр и самоличността на Автор на удостоверение за КЕП, Доставчикът изисква да бъде регистрирано искане за първоначално издаване на удостоверение.
2. Искане за първоначално издаване на удостоверение пред Регистриращ орган/МРС на Доставчика е процедура, чрез която Доставчикът изисква, събира и получава необходима информация за идентификация на Автора/Титуляря на удостоверението.
3. Процедурата по регистрация включва:
   - попълване на регистрационна форма за издаване на удостоверение;
   - генериране на двойка ключове;
   - подготвяне на електронна заявка, съдържаща публичния ключ, за който се издава удостоверението;
   - представяне на изискуемите документи в Регистриращия орган/МРС съгласно Политиката при издаване на удостоверението;
   - възможност за заявяване на други услуги, свързани с издаваното удостоверение.
4. Установяване на самоличността на Автора/идентичността на Титуляря след регистрация и преди издаване на заявеното удостоверение за КЕП изисква тяхно лично присъствие или на упълномощен представител в Регистриращия орган/МРС.
5. Първоначалната идентификация и потвърждаване на самоличността включва:
   - държането на частния ключ от Автора или изрично упълномощено от него лице, съответстващ на публичния ключ, представен на Доставчика за издаване на удостоверението;
   - проверка и потвърждаване на самоличността на Автора и идентичността на Титуляря на издаваното удостоверение.
6. След успешна проверка на самоличността на Автора/идентичността на Титуляря, оторизираният оператор в Регистриращия орган/МРС:

- предлага договор за удостоверителни услуги подписан от името на Доставчика и съхранява всички представени документи към договора;
- потвърждава искането за издаване и изпраща електронна заявка за издаване на удостоверение до оперативния Удостоверяващ орган на Доставчика;
- може да запише издаденото удостоверение на SSCD и да го предаде на Автора/Титуляря или на упълномощеното лице.

3.2.1 Доказване държането на частния ключ

1. Регистриращият орган/МРС извършва проверка за съответствие на представения публичен ключ, който се удостоверява в издаваното удостоверение от Доставчика с частния ключ на Автора.
2. Електронната заявка с публичния ключ, която се генерира за издаване на удостоверение за КЕП от заявителя, следва да бъде подписана с частния ключ, който кореспондира с публичния ключ в заявката. Електронната заявка следва да е във формат, който позволява на Доставчика, чрез Регистриращия орган/МРС, да провери държането на частния ключ.
3. Он-лайн исканията за администриране на удостоверения следва да бъдат подписвани от заявителя с частния ключ, кореспондиращ с публичния ключ в удостоверението, обект на заявката. Доставчикът, чрез Регистриращия орган/МРС, проверява положения електронен подпис.
4. Регистриращият орган/МРС предприема допълнителни стъпки за автентификация на държателя на частния ключ и факта на държането на ключа, в зависимост от заявения тип удостоверение съгласно прилаганата Политика.
5. Двойката ключове, съответстваща на издаваното от Доставчика удостоверение, задължително се генерира в SSCD и контролът на достъпа до частния ключ в SSCD се държи само от Автора.

3.2.2 Установяване на идентичност на юридическо лице или едноличен търговец като Титуляр

1. Установяване и проверката на идентичността на юридическото лице или едноличен търговец като Титуляр на удостоверение се осъществява от Регистриращия орган/МРС на Доставчика съгласно съответната Политика при издаване на удостоверение и другите вътрешни документи на Доставчика.
2. Установяването на идентичността на юридическо лице или едноличен търговец като Титуляр на професионално удостоверение за КЕП „B-Trust Professional Certificate QES" изисква в Регистриращия орган/МРС да се яви упълномощен представител на Титуляря и да представи изискуемите документи, доказващи правния статус на Титуляря.

3.2.3 Установяване самоличността на физическо лице като Автор, Титуляр или представител на Титуляря

1. Установяване и проверка на самоличността на физическото лице като Автор, Титуляр или представител на Титуляря, както и овластяването на Автора, се осъществява от Регистриращия орган/МРС на Доставчика при следване на процедурните правила стъпки, посочени в съответната Политика и другите вътрешни документи на Доставчика.
2. Установяването на самоличността на физическо лице, като Автор/Титуляр или представител на Титуляря, изисква лицето или упълномощен негов представител лично да представи в Регистриращия орган/МРС следните документи:

Тип на удостоверение за КЕП	Необходими документи
Персонално удостоверение за КЕП „B-Trust Personal Certificate QES"	Документи, доказващи самоличността на Автора - при лично явяване на Автора Документи, доказващи самоличността на упълномощеното лице и пълномощно – при явяване на упълномощено лице
Професионално удостоверение за КЕП „B-Trust Professional Certificate QES"	Документи, доказващи самоличността на Автора, идентичността на Титуляря и представителната власт на Автора спрямо Титуляря.

3.2.4 Особени атрибути

1. Доставчикът може да включва в издаваното удостоверение особени атрибути, свързани с Автора/Титуляря, ако удостоверението се издава за конкретна цел по съответната политика.
2. Тази информация подлежи на проверка от Регистриращия орган или служба за регистрация.

3.2.5 Непотвърдена информация

1. Непотвърдена информация е всяка информация, извън обхвата на проверяваната задължителна

информация, която следва да бъде включена в удостоверението съгласно чл. 24 на ЗЕДЕП.

2. Доставчикът може да включва в издаваното удостоверение и непотвърдена информация за Автора/Титуляря, която не подлежи на проверка от Регистриращия орган или служба за регистрация.
3. Доставчикът не носи никаква отговорност за включената в удостоверението непотвърдена информация.

3.3 Идентификация и установяване на идентичност при подновяване

1. Доставчикът може да поднови валидно удостоверение за КЕП, което не е прекратено в срока му на валидност, по два начина:
    - като запази генерираната двойка ключове за текущото удостоверение (Renew);
    - като генерира нова двойка ключове (Re-key).
2. Удостоверение се подновява за същата двойка асиметрични ключове (Renew) на текущото удостоверение на Автора/Титуляря ако информацията за Автора/Титуляря в удостоверението, което се подновява, е идентична с тази в текущото. Само периодът на валидност в подновеното удостоверение е различен от този в текущото.
3. Доставчикът допуска многократно подновяване на удостоверение за КЕП, като запазва текущата двойка ключове (Renew), но препоръчва тази практика да се ограничава с цел да се намали риска от компрометиране на частния ключ.
4. Доставчикът ще поднови текущо удостоверение на Автор/Титуляр с нова двойка ключове (Re-key), само ако той заяви искане за това и декларира, че няма настъпили промени в удостоверената информация в текущото удостоверение. Подновеното удостоверение има различен публичен ключ и нов период на валидност, като удостоверената информация за Автора/Титуляря се запазва.
5. След подновяване текущото удостоверение не се прекратява и остава валидно в срока му на валидност.
6. За идентификация, установяване на идентичност и самоличност на Автора/Титуляря на удостоверение, което се подновява, не се изисква тяхното лично присъствие в Регистриращия орган/МРС на Доставчика.
7. При настъпили промени в информацията за Автора/Титуляря на удостоверение, текущото удостоверение не се подновява. Доставчикът издава ново удостоверение, като следва първоначална идентификация и установяване на идентичността му, съответно самоличността му и прекратява незабавно текущото удостоверение.
8. Подновяване на удостоверение на Удостоверяващ орган на Доставчика „БОРИКА - БАНКСЕРВИЗ" АД не се допуска. При всички обстоятелства, които налагат подмяна на удостоверението, винаги се издава ново удостоверение на Удостоверяващия орган.
9. Доставчикът съблюдава следните времеви ограничения и изисквания за идентификация при подновяване на удостоверение за КЕП:

Времеви интервал	Подновяване	Изискване
До 30 дни преди изтичане срока на валидност на удостоверение, което не е прекратено и което няма промяна в удостоверената в него информация	- чрез Renew - чрез Re-key	1. Да няма промяна в „DN" на удостоверението 2. Удостоверението да е било издадено на SSCD 3. Заявката за подновяване може да бъде извършена отдалечено
До 30 дни след изтичане срока на валидност на удостоверение, което не е прекратено и което няма промяна в удостоверената в него информация	- чрез Renew - чрез Re-key	1. Да няма промяна в „DN" на удостоверението 2. Удостоверението да е било издадено на SSCD 3. Заявката за подновяване се подава на място (Регистриращ орган/МРС)
Повече от 30 дни след срока на валидност на удостоверение	Не се подновява	

3.4 Идентификация и автентификация при спиране

1. Доставчикът е длъжен, чрез Регистриращия орган/МРС, да спре действието на валидно удостоверение при постъпило искане за спиране, но не за повече от 48 часа (ЗЕДЕП, чл. 26).
2. Доставчикът, чрез Регистриращия орган/МРС, не извършва идентификация и автентификация на заявителя и спира незабавно действието на удостоверение.
3. Доставчикът, чрез Регистриращия орган/МРС, възобновява действието на спряно удостоверение в съответствие с чл. 26, ал. 6 на ЗЕДЕП.

3.5 Идентификация и автентификация при прекратяване

1. Доставчикът, чрез Регистриращия орган/МРС, прекратява действието на валидно удостоверение при

постъпило искане за прекратяване в съответствие с чл. 27 на ЗЕДЕП.

2. Доставчикът, чрез Регистриращия орган или службата за регистрация незабавно спира действието на удостоверението и извършва последваща идентификация и автентификация на заявителя.
3. Доставчикът, чрез Регистриращия орган или службата за регистрация, следва да извърши идентификацията и автентификация на заявителя в рамките на допустимия срок за спиране на действието на удостоверението, който е 48 часа.
4. Доставчикът, чрез Регистриращия орган/МРС, прекратява действието на удостоверение само след успешна идентификация и автентификация на заявителя и уточнена причина за прекратяване. В противен случай удостоверението се възобновява.

3.6 Идентификация и автентификация след прекратяване

1. Не се допуска подновяване на удостоверение чрез „Renew" или „Re-key“ след прекратяването му.
2. Автор/Титуляр на прекратено удостоверение може да заяви издаване на ново удостоверение.
3. Доставчикът, чрез Регистриращия орган/МРС изпълнява първоначална идентификация, установяване на идентичност на Автора/Титуляря, ако той заяви ново удостоверение.

4 ОПЕРАТИВНИ ИЗИСКВАНИЯ И ПРОЦЕДУРИ

1. Доставчикът, чрез Регистрираща орган/МРС, в рамките на сключен Договор за удостоверителни услуги, предоставя следните операционни процедури за удостоверителни услуги, приложими към удостоверения за КЕП:
   - регистрация на искане за издаване на удостоверение;
   - обработка на искане за издаване;
   - издаване на удостоверение;
   - предаване на издадено удостоверение;
   - употреба на двойката ключове и на удостоверението;
   - подновяване на удостоверение чрез “Renew”;
   - подновяване на удостоверение чрез “Re-key”;
   - спиране/възобновяване действие на удостоверение;
   - прекратяване на удостоверение;
   - статус на удостоверение.
2. Доставчикът, чрез Регистрираща орган/МРС, допуска Автор/Титуляр да прекрати Договора за удостоверителни услуги между тях.

4.1 Искане за издаване на удостоверение

1. Издаването на удостоверение се предхожда от регистриране на искане от страна на заявителя пред Регистрираща орган/МРС на Доставчика.
2. Искане за издаване на удостоверение може да направи лично от Автора/Титуляря или упълномощен представител на Титуляря (упълномощено лице).
3. Заявителят регистрира искане за издаване на удостоверение в онлайн режим или чрез оператор в Регистрираща орган/МРС на Доставчика.
4. Оператор на Регистрираща орган/МРС, като оторизиран представител на Доставчика, може да изпълнява роля на заявител, като регистрира онлайн искане за издаване на удостоверение в присъствието на заявителя.

4.1.1 Процес на заявяване

1. Искането за издаване включва цялата изискуема информация по чл. 24 на ЗЕДЕП, за Автора/Титуляря и типа на удостоверението, което се заявява. Искането може да включва и допълнителна, непроверяема информация, част от която се удостоверява, а друга част улеснява контакта на Доставчика с Титуляря.
2. Процесът на заявяване предоставя възможност на оператор на Регистрираща орган/МРС или на Автор/Титуляр да генерира двойката криптографски (RSA) ключове и да включи публичния ключ в информацията за издаване на удостоверението.
3. Двойката криптографски ключове за издаване на удостоверение за КЕП задължително се генерира в SSCD, отговарящо на изискванията за ниво на сигурност за създаване подписа.
4. Електронният формат на искането за издаване на удостоверение с информацията, която ще се включи в удостоверението е структура, подписана с частния ключ от генерираната двойка ключове в SSCD.
5. В случаите, когато е необходимо, Регистриращият орган/МРС предоставя на Автора/Титуляря или на упълномощено от него лице в защитен вид информация/код за достъп до частния ключ в SSCD.
6. Ако заявителят не притежава SSCD, когато представя искане за издаване на удостоверение на Регистрираща орган/МРС на Доставчика, той само въвежда информацията за идентифициране на Автора/Титуляря, както и друга допълнителна такава, без да генерира криптографската двойка ключове (RSA) за исканото удостоверение.
7. Комуникациите между Потребителите и защитени Интернет страници на Доставчика се базират на HTTPS протокол.
8. Одобрените заявки за издаване и управление на КЕП са подписани от Доставчика.

4.2 Процедура на издаване

4.2.1 Функции по идентификация и автентификация

1. Регистриращият орган/МРС извършва идентификация и автентификация на заявителя на искането за издаване на удостоверение - Автор/Титуляр или упълномощено от него лице.

2. След първоначална идентификация и утвърдени вътрешни процедури на Доставчика, на база постъпило искане за издаване на удостоверение и представени документи, в личното присъствие на заявителя - Автор/Титуляр или упълномощено от него лице, Регистриращият орган/МРС проверява и потвърждава пред Доставчика:
   - самоличността на Автора/идентичността на Титуляря, респективно или упълномощеното лице;
   - представителната власт на Автора спрямо Титуляря и на упълномощеното лице на Титуляря;
   - проверява упълномощаването;
   - държането на частния ключ, съответстващ на публичния ключ;
   - допълнителна информация, заявена за включване в удостоверението, както и допустима непотвърдена такава;
   - подписване на Договор за удостоверителни услуги и съгласие с условията в настоящия Наръчник.
3. Ако двойката ключове е генерирана при Автора/Титуляря, Регистриращият орган/МРС следва да провери предоставената електронна заявка и изискванията за нивото на сигурност на SSCD.

4.2.2 Потвърждаване или отхвърляне на искане за издаване

1. След успешно направените проверки, оторизиран оператор на Регистриращият орган/МРС утвърждава пред Доставчика искането за издаване на удостоверение.
2. Регистриращият орган/МРС отхвърля искането за издаване на удостоверение ако потвърждаването е неуспешно.
3. Регистриращият орган/МРС незабавно уведомява заявителя и посочва причините за отхвърляне.
4. Заявител с отхвърлено искане за издаване на удостоверение може отново да направи искане след като е отстранил посочените причини за отхвърляне.
5. Регистриращият орган/МРС надлежно съхранява и архивира представените документи и потвърдената електронна заявка за издаване на удостоверение.
6. Регистриращият орган/МРС контролира и утвърждава пред Доставчика верността и точността на включената информация в удостоверението само към момента на издаването му.
7. Автор/Титуляр на удостоверение за КЕП има задължението незабавно да информира Доставчика за настъпили промени в удостоверената информация след издаването му.

4.2.3 Срок за обработка на искане за издаване на удостоверение

1. Регистриращият орган/МРС на Доставчика незабавно, в присъствието на заявителя - Автор/Титуляр или упълномощено от него лице, изпълнява всички функции по проверка, след като заявителя е представил необходимите за това документи и утвърждава представената информация чрез направеното искане за издаване на удостоверение.
2. Удостоверяващият орган на Доставчика издава незабавно удостоверението след утвърждаване от Регистриращия орган/МРС на електронната заявка за издаване.

4.3 Издаване на удостоверение

4.3.1 Действие на Удостоверяващия орган

1. Удостоверяващият орган на Доставчика електронно идентифицира Регистриращия орган/МРС , утвърдил електронната заявка за издаване на удостоверение за КЕП.
2. Удостоверяващият орган генерира заявеното удостоверение съгласно избрания профил, подписва го с електронния подпис на Доставчика и го публикува незабавно в Публичния си регистър.

4.3.2 Известяване на Автора/Титуляря на удостоверение от Доставчика

1. Доставчикът, чрез Службата за известяване на Потребители на удостоверителни услуги, незабавно известява Автора/Титуляря на издаденото и публикувано удостоверение.
2. Службата за известяване изпраща до Автора/Титуляря електронно известие по имейл с информация за името на Автора, вида на издаденото удостоверение за КЕП, уникалния сериен номер на удостоверението и периода му на валидност, освен в случаите, когато липсва имейл адрес.
3. Доставчикът доставя издаденото удостоверение на Автора/Титуляря, респективно на упълномощеното от него лице, чрез Регистриращия орган/МРС.
4. Оторизиран оператор на Регистриращия орган/МРС записва удостоверението на SSCD, където е била генерирана двойката криптографски ключове (RSA) за това удостоверение.

4.4 Приемане и публикуване на удостоверението

1. Доставчикът, чрез оперативния Удостоверяващ орган публикува незабавно издаденото удостоверение в Публичния регистър на издадените удостоверения.
2. Авторът/Титулярят, може да възрази пред Доставчика или чрез Регистриращия орган/МРС, ако издаденото удостоверение съдържа грешки или непълноти, в 3(три) дневен срок от публикуването му в Публичния регистър. Те се отстраняват незабавно от Доставчика чрез издаване на ново удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на неверни данни.
3. При липса на възражение от страна на Автора/Титуляря в посочения по-горе срок се смята, че съдържанието на удостоверението е прието.

4.5 Употреба на двойката ключове и на удостоверението

4.5.1 От Автора

1. Частният ключ, съответстващ на удостоверения публичен ключ, се контролира от Автора. Отговорността за използването на частния ключ е на Автора.
2. Авторът/Титулярят употребява удостоверението и съответстващата двойка ключове на удостоверението, както следва:
   - в съответствие с означената в удостоверението Политика "Certificate Policy" и съгласно атрибутите „keyUsage" и „extendedKeyUsage";
   - за полагане на електронен подпис в рамките на срока на валидност на удостоверението;
   - проверка на положен електронен подпис;
   - до момента на прекратяване на удостоверението;
   - когато удостоверението е спряно, да не използва частния ключ, в частност за създаване на електронен подпис;
   - съгласно Договора за удостоверителни услуги между него и Доставчика.

4.5.2 От доверяваща се страна

1. Публичният ключ в удостоверението, съответстващ на държания от Автора частен ключ, е публично достъпен за всички.
2. Всяка доверяваща се страна, включително оператор в Регистриращ орган/МРС следва да използва публичния ключ и удостоверението на Автора/Титуляря, както следва:
   - в съответствие с означената в удостоверението политика "Certificate Policy" и съгласно атрибутите „keyUsage" и „extendedKeyUsage;
   - само след проверка на статуса на удостоверението и проверка на електронния подпис на Доставчика;
   - до прекратяване на удостоверението;
   - когато удостоверението е спряно, публичният ключ не трябва да се използва.

4.6 Подновяване на удостоверение

1. Подновяването на удостоверение за КЕП запазва информацията за Автора/Титуляря от текущото удостоверение, като в подновеното удостоверение се променя периода на валидност.
2. Подновяване на удостоверение за КЕП, което не е било прекратено в периода му на валидност, може да се изпълни по два начина:
   - запазва се генерираната двойка ключове за текущото удостоверение (Renew);
   - генерира се нова двойка ключове (Re-key).
3. Подновяването на удостоверение за КЕП се предхожда от регистриране на искане за подновяване пред Регистриращия орган/МРС.
4. Искането за подновяване на удостоверение се регистрира онлайн, когато Авторът/Титулярят има валидно удостоверение за КЕП, което трябва да поднови.
5. Когато удостоверението е с изтекъл срок на валидност и искането за подновяване е съгласно посочените времеви ограничения и изисквания за идентификация при подновяване, Авторът/Титулярят или упълномощено от него лице трябва лично да посети Регистриращия орган/МРС на Доставчика.
6. Автор/Титуляр или упълномощено от него лице може да поднови многократно свое удостоверение за КЕП при съблюдаване на посочените по-долу условия за подновяване.
7. Доставчикът не допуска използване на двойка ключове за КЕП за период, по-голям от 3 (три) години.
8. Доставчикът не препоръчва многократното подновяване на удостоверение за КЕП, чрез „Renew" с цел да се

намали риска от компрометиране на частния ключ.

9. Доставчикът препоръчва на Автор, респективно Титуляр или упълномощено от него физическо лице да поднови свое удостоверение чрез „Re-key".

4.6.1 Условия за подновяване на удостоверение

1. Регистриращият орган/МРС ще поднови едно удостоверение за КЕП чрез „Renew" при съблюдаване на следните условия:
   - удостоверението не е прекратено в периода му на валидност;
   - Автор/Титуляр или упълномощен от него лице декларира, че няма промяна в удостоверената информация в текущото му удостоверение;
   - искане за подновяване е направено до 30 дни преди или след изтичане на периода на валидност на удостоверението;
   - строго изпълнява идентификацията и установява идентичността, съответно самоличността на заявителя и посочените времеви ограничения при подновяване.
2. Регистриращият орган/МРС ще поднови едно удостоверение за КЕП чрез „Re-key" при съблюдаване на следните условия:
   - удостоверението не е прекратено в срока му на валидност;
   - Автор/Титуляр или упълномощен от него лице декларира, че няма промяна в удостоверената информация в текущото му удостоверение;
   - искане за подновяване е направена до 30 дни преди или след изтичане на срока на валидност на удостоверението;
   - строго изпълнява идентификацията и установяване на идентичността, съответно самоличността на заявителя и посочените времеви ограничения при подновяване;
3. Във всички случаи, когато има промяна в удостоверената информация за Автора/Титуляря на текущото удостоверение, последното не подлежи на подновяване, а Доставчикът издава ново удостоверение.

4.6.2 Кой може да заяви подновяване на удостоверение

1. Автор/Титуляр или упълномощен от него лице може да заяви подновяване на удостоверението при съблюдаване на времевите ограничения, изисквания и условия за подновяване.

4.6.3 Процедура по подновяване на удостоверение

1. Подновяването на удостоверение за КЕП се предхожда от регистриране на искане за подновяване пред Регистриращия орган/МРС на Доставчика.
2. Искането за подновяване на удостоверение чрез електронна заявка се удостоверява с електронен подпис, съответстващ на валидното удостоверение на Автора/Титуляря, което се подновява.
   В случай, че удостоверението, което се подновява е с изтекъл срок на валидност, Авторът/Титулярят или упълномощено от него лице трябва да посети лично Регистриращия орган/МРС на Доставчика. орган/МРС строго следва изискванията за идентификация и установяване на идентичност, респективно самоличност на заявителя и на условията за подновяване.
3. След успешна идентификация и проверка на условията за подновяване, Регистриращият орган/МРС потвърждава искането за подновяване пред оперативния Удостоверяващ орган на Доставчика.
4. След успешна електронна автентификация на Регистриращия орган/МРС чрез оторизирания оператор, оперативния Удостоверяващ орган изпълнява потвърденото искане за подновяване на удостоверението.
5. При неуспешна идентификация и проверка на условията за подновяване, Регистриращият орган/МРС отхвърля искането за подновяване на удостоверението и незабавно известява заявителя за причината.
6. Заявител с отхвърлено искане за подновяване, може да заяви издаване на ново удостоверение за КЕП.

4.6.4 Известяване на Автора/Титуляря след подновяване на удостоверение

1. Доставчикът, чрез Службата за известяване на Потребители на удостоверителни услуги, незабавно известява Автора/Титуляря на подновеното и публикувано удостоверение.
2. Службата за известяване изпраща до Автора/Титуляря електронно известие/имейл с името на Автора/Титуляря, типа на удостоверението за КЕП, уникалния сериен номер и срока на валидност на подновеното удостоверение и адреса (URL), от който може да достави подновеното удостоверение.
3. Когато заявителят за подновяване на удостоверение посещава Регистриращия орган/МРС, Авторът/Титулярят получава подновеното удостоверение чрез оторизирания оператор, който го записва на SSCD, в което е генерирана двойката криптографски ключове (RSA) за удостоверението.

4.6.5 Публикуване на подновено удостоверение

1. Доставчикът, чрез оперативния Удостоверяващ орган публикува незабавно подновеното удостоверение в Публичния регистър.

4.7 Подмяна на двойка криптографски ключове в удостоверение

1. Доставчикът допуска подмяна на криптографска двойка ключове в удостоверение за КЕП чрез „Re-key", само при спазване на изискванията и на условията за подновяване на удостоверение или като издаде ново удостоверение.

4.8 Промяна в удостоверение

1. Доставчикът допуска промени в съдържанието на информация в издадено и публикувано удостоверение за КЕП само при спазване на изискванията и на условията за издаване на ново удостоверение.
2. Доставчикът не допуска промяна в профила на удостоверенията за КЕП, специфициран в Част II на този документ.

4.9 Прекратяване и спиране на удостоверение

1. На прекратяване подлежат само валидни удостоверения, т.е. удостоверения, чийто срок на валидност не е изтекъл.
2. При прекратяване на удостоверението на оперативния Удостоверяващ орган за издаване и поддържане на удостоверения за КЕП, действието на всички издадени от него и валидни удостоверения се прекратява.
3. Само оперативният Удостоверяващ орган, издал удостоверение за КЕП, може да прекрати действието на това удостоверение.
4. Ако прекратяването е следствие от операторска грешка или следствие от компрометиране на оперативен частен ключ на Доставчика, довели до прекратяване на удостоверението на оперативния Удостоверяващ орган, Доставчикът ще издаде за своя сметка еквивалентно удостоверение.
5. Услугите по управление на прекратяване и спиране на действието на удостоверение са на разположение денонощно, 7 дни в седмицата.
6. При срив в системата, услугите или други фактори, които са извън контрола на Удостоверяващия орган, ДУУ полага максимални усилия, за да гарантира, че услугата не липсва за период, по-дълъг от максималния период от време, който в случая е 3 (три) часа.

4.9.1 Условия за прекратяване на удостоверение

1. Доставчикът прекратява издадено от него удостоверение при:
    - смърт или поставяне под запрещение на Автора/Титуляря с прекратяване на юридическо лице на Титуляря;
    - прекратяване на представителната власт на Автора спрямо Титуляря;
    - установяване на неверни данни при издаване на удостоверението;
    - станала впоследствие невярна удостоверена информация;
    - при промяна в удостоверена вече информация на Автора/Титуляря;
    - компрометиране на частния ключ;
    - забава в заплащането на дължимо възнаграждение;
    - искане за прекратяване от страна на Автора/Титуляря, след като се увери в самоличността им и в представителната власт на Автора.
2. Доставчикът предприема незабавно прекратяване на действието на издаденото удостоверение при всяко едно от посочените по-горе обстоятелства.
3. Доставчикът прекратява издадените от него удостоверения, ако прекрати дейността си без да я прехвърлил на друг доставчик.
4. Доставчикът може да спре и прекрати удостоверение на Удостоверяващ орган от инфраструктурата, ако са налице основателни съмнения за компрометиране на частния ключ на този орган.

4.9.2 Процедура за прекратяване на удостоверение

1. Прекратяване действието на удостоверение се предхожда от регистриране на искане за прекратяване пред Регистриращия орган/МРС на Доставчика.
2. Искането за прекратяване на удостоверение може да се регистрира електронно, само когато Автора/Титуляря има (друго) валидно и достъпно за ползване удостоверение за КЕП. В противен случай се

прави искане на място пред оторизиран оператор в МРС.

3. Прекратяването на удостоверение чрез искане по електронен способ се удостоверява с КЕП, съответстващ на валидно удостоверение на Автора/Титуляря.
4. Оторизираният оператор в Регистриращия орган/МРС незабавно, без да идентифицира заявителя, спира действието на удостоверението за не повече от 48 часа.
5. Във всички случаи, Авторът/Титулярят или упълномощено от него лице трябва да посети лично Регистриращия орган/МРС на Доставчика за последваща проверка на идентичността, респективно самоличността на заявителя.
6. Регистриращият орган/МРС строго следва изискванията за идентификация и установяване на идентичност, респективно самоличност на заявителя и причините за прекратяване.
7. След успешна електронна автентификация на Регистриращия орган/МРС чрез оторизирания оператор, оперативния Удостоверяващ орган изпълнява потвърдената заявка за прекратяване на удостоверението.
8. При неуспешна идентификация и проверка на условията за прекратяване, Регистриращият орган/МРС отхвърля искането за прекратяване на удостоверението и незабавно известява заявителя за причините за това.
9. Заявител, с отхвърлено искане за прекратяване на удостоверение, може да подаде ново искане за прекратяване на удостоверението, след като отстрани посочените причини за отказа.
10. След прекратяване на удостоверението, Доставчикът, чрез своя оперативен Удостоверяващ орган, незабавно публикува прекратеното удостоверение в CRL, като издава нов.
11. След прекратяване на удостоверението, Доставчикът, чрез Службата за известяване незабавно уведомява Автора и Титуляря на прекратеното удостоверение.
12. Прекратено удостоверение на Автор/Титуляр не подлежи на възобновяване или на подновяване.
13. Достъп до искането за прекратяване и отчетите от изпълнението на прекратяване на удостоверение имат оторизирани лица от персонала на Доставчика.

4.9.3 Гратисен период преди прекратяване на удостоверение

1. Преди да прекрати действието на валидно удостоверение, Доставчикът чрез своя Регистриращ орган/МРС спира действието на удостоверението за не повече от 48 часа.
2. В рамките на този гратисен период Доставчикът, чрез своя Регистриращ орган/МРС, трябва да извърши всички проверки за установяване на идентичността/самоличността на заявителя и на причините за прекратяване.
3. При неуспешна проверка или след изтичане на гратисния период, Доставчикът възобновява действието на удостоверението.
4. Доставчикът възобновява действието на удостоверението по изрично искане на Автора/Титуляря или упълномощено от него лице преди да изтече гратисния период.

4.9.4 Време, за което Удостоверяващ орган трябва да изпълни искане за прекратяване

1. Доставчикът трябва да изпълни искане за прекратяване на удостоверение за период от време, не по-голям от посочения гратисен период и само след успешно завършена проверка на условията и на причините за прекратяване.

4.9.5 Изисквания към Доверяващи се страни за проверка на прекратено удостоверение

1. Всяка Доверяваща се страна приема издадено от Доставчика удостоверение за КЕП само след успешна проверка на статуса на удостоверението чрез актуалния CRL или чрез проверка на текущия статус на удостоверението в реално време чрез Органа за валидация „B-Trust VA" или „B-Trust VA QES".
2. Доставчикът не носи отговорност за настъпили вреди и последствия от неизпълнение на посочените изисквания.

4.9.6 Честота на публикуване на актуален Списък на прекратени удостоверения

1. Доставчикът, чрез своя оперативен Удостоверяващ орган, публикува незабавно нов актуален CRL, всеки път когато се прекрати действието на валидно удостоверение, издадено от този орган.
2. Доставчикът, чрез своя оперативен Удостоверяващ орган, публикува периодично актуален нов CRL със срок на валидност 1 месец.
3. Срокът на валидност 1 месец важи за всеки публикуван нов актуален CRL на оперативния Удостоверяващ орган.

4.9.7 Публикуване на актуален Списък на прекратени удостоверения

1. Доставчикът своевременно публикува актуален CRL след автоматичен запис на прекратено или спряно удостоверение.
2. Публикуването на актуалния CRL е автоматично.

4.9.8 Възможност за проверка на статус на удостоверение в реално време

1. Доставчикът предоставя онлайн проверка в реално време по OCSP протокол на статуса на издадените удостоверения за КЕП.

4.9.9 Изисквания за ползване на OCSP

1. Проверка на статус на удостоверение в реално време (по OCSP протокол) изисква софтуерен клиент (OCSP-клиент) и онлайн достъп през Интернет до Органите за валидация „ B-Trust VA" и „ B-Trust VA QES".
2. Проверка на статус на удостоверение в реално време (по OCSP протокол) може да се изпълни и през Интернет страницата на Доставчика.

4.9.10 Условия за спиране на удостоверение

1. Доставчикът, чрез своя оперативен Удостоверяващ орган, спира действието на валидно удостоверение при определени условия и за срок до 48 часа.
2. Доставчикът предприема незабавни действия по искането за спиране на удостоверение.
3. За времето, през което удостоверението е спряно, то се счита за невалидно и всички електронни подписи, проверявани с това удостоверение са недействителни (невалидни).

4.9.11 Кой може да заяви искане за спиране на удостоверение

1. Доставчикът спира издадено от него валидно удостоверение ако:
   - постъпи искане на Автора/Титуляря или упълномощено от него лице, без да е длъжен да се увери в самоличността или в представителната му власт;
   - постъпи искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, др.;
   - постъпи искане на КРС;
   - има решение на председателя на КРС, когато е налице непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на ЗЕДЕП.

4.9.12 Процедура за спиране на удостоверение

1. Спиране действието на удостоверение се предхожда от регистриране на искане за спиране пред Регистриращия орган/МРС.
2. Искането за спиране на удостоверение може да се регистрира чрез електронна заявка или се прави искане пред оторизиран оператор в МРС на Доставчика.
3. Искането за спиране на удостоверение чрез електронна заявка се удостоверява с електронен подпис, съответстващ на валидното удостоверение на Автора/Титуляря.
4. Оторизираният оператор в Регистриращия орган/МРС незабавно, без да идентифицира заявителя, спира действието на удостоверението. Спирането на удостоверението се извършва чрез временното му вписване в списъка на прекратените удостоверения, съгласно чл. 26, ал. 5 от ЗЕДЕП.
5. След успешна електронна автентификация на оторизирания оператор в Регистриращия орган/МРС, оперативния Удостоверяващ орган изпълнява потвърдената заявка за спиране на удостоверението.
6. Регистриращият орган/МРС не може да отхвърля искането за спиране.
7. След спиране на удостоверението, Доставчикът чрез своя оперативен Удостоверяващ орган незабавно публикува спряното удостоверение в CRL чрез издаване на нов.
8. След спиране на удостоверението, Доставчикът чрез своята Служба за известяване незабавно уведомява Автора/Титуляря на спряното удостоверение.

4.9.13 Ограничение на периода на спиране на удостоверение

1. Доставчикът спира действието на удостоверение за КЕП за период до 48 часа от получаване на искането за спиране.
2. Доставчикът временно спира до 48 часа действието на удостоверение, преди прекратяването му.

4.9.14 Възобновяване действието на спряно удостоверение

1. Доставчикът възобновява действието на спряно удостоверение:
   - до 48 часа след неговото спиране;
   - след като изтече срока за спиране (48 часа) и не е постъпило искане за възобновяване;
   - след като отпадане основанието за спиране, преди да изтече периода на спиране;
   - по искане на Титуляря, след като Доставчикът, съответно КРС се увери, че той е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.
2. След възобновяване на удостоверение, последното се счита за действително.

4.9.15 Процедура за възобновяване на действието на удостоверение

1. Регистриращият орган/МРС възобновява спряно удостоверение след като получи искане за възобновяване от Автора/Титуляря и след успешна проверка за идентификация (идентичност, самоличност).
2. Регистриращият орган/МРС възобновява спряно удостоверение след като получи писмено разпореждане или писмена заповед от КРС, съответно на председателя на КРС за възобновяване на удостоверението.
3. Регистриращият орган/МРС незабавно възобновява спряно удостоверение след като изтече нормативния период на спиране (48 часа).
4. Във всички случаи, процедурата по възобновяване изважда спряното удостоверение от текущия CRL и публикува нов.

4.10 Статус на удостоверение

1. Всички действителни удостоверения за КЕП, които Доставчикът издава чрез оперативния Удостоверяващ орган „B-Trust Operational CA QES", се публикуват в Публичния регистър.
2. Всяко публикувано удостоверение в Регистъра е:
   - със статус „валидно" - периодът на валидност, посочен в удостоверението не е изтекъл към момента на проверка на статуса;
   - със статус „невалидно" - периодът на валидност, посочен в удостоверението е изтекъл към момента на проверка на статуса.
3. Всички прекратени удостоверения се включват в CRL, който се публикува периодично или незабавно след промяна на статус на удостоверение.
4. Елементът в CRL, съответстващ на спряно/прекратено удостоверение съдържа атрибут, който указва причината за прекратяване на удостоверението („CRL Reason").
5. Спряно удостоверение се включва в CRL до неговото възобновяване и атрибутът „CRL Rason" в съответстващия му елемент от Списъка е със значение „certificate Hold".
6. Статус на удостоверение, проверяван чрез CRL-механизъм (чрез Списък на прекратени удостоверения), се определя от значението на атрибута „CRL Reason".
7. Статус на удостоверение, проверяван чрез OCSP-механизъм (чрез OCSP протокол), се определя от значението „response Status" в отговора, получен от Органите за валидация, както следва:
   - „good"- удостоверението не е спряно/прекратено, но не утвърждава, че времето на отговора е в рамките на периода на валидност на това удостоверение;
   - „revoked"- удостоверението е прекратено или временно спряно (on hold);
   - „unknown"- Органът за валидация няма информация за това удостоверение (най-вероятно удостоверението е издадено от друг Доставчик).

4.11 Прекратяване на договор за удостоверителни услуги

1. Договорът за удостоверителни услуги между Доставчика и Потребителя се прекратява след изтичане на срока на валидност на последното издадено удостоверение, прекратяване на всички валидни удостоверения по този договор, или на друго основание, посочено в договора.

5 СРЕДСТВА, УПРАВЛЕНИЕ И ОПЕРАТИВЕН КОНТРОЛ

5.1 Физически контрол

1. Доставчикът осигурява физическа защита и контрол на достъпа на помещенията, където има инсталирани критични компоненти на инфраструктурата на B-Trust.
2. Критични компоненти на инфраструктурата B-Trust на Доставчика са:
   - Базов Удостоверяващ орган „B-Trust Root CA";
   - Оперативен Удостоверяващ орган „B-Trust CA QES";
   - Оперативен Удостоверяващ орган „B-Trust CA AES";
   - Регистриращ орган;
   - Публичен регистър;
   - Орган за удостоверяване на време „B-Trust TSA";
   - Орган за валидация „B-Trust VA";
   - Орган за валидация „B-Trust VA QES";

3. Инфраструктурата B-Trust на Доставчика е физически и логически обособена и не се използва при други дейности, които „БОРИКА - БАНКСЕРВИЗ" АД осъществява.

5.1.1 Помещения и конструкция на помещенията

1. Доставчикът разполага със специално конструирано и оборудвано помещение с електромагнитна защита и най-висока степен на контрол на физически достъп, в което се помещават удостоверяващите органи на Доставчика и всичките централни компоненти на инфраструктурата – „B-Trust Root CA“, „B-Trust CA QES”, „B-Trust CA AES”.

5.1.2 Физически достъп

1. Физическият достъп до специализираното помещение се контролира от системи за контрол на достъпа, видеонаблюдение, сигнално-известителни системи, климатик, др.
2. Системите за контрол на физическия достъп се инспектират периодично и се поддържат необходимите журнали.
3. Овластените лица от персонала на Доставчика строго спазват и следват разработени вътрешни процедури за достъп до различните зони на помещението с ограничен физически достъп.
4. Всяко лице от персонала на Доставчика е персонифицирано в системите за контролиране на достъпа до помещението и се изисква строга верификация.

5.1.3 Електрическо захранване и климатични условия

1. Електрозахранването на всички критични компоненти на инфраструктурата B-Trust на Доставчика са защитени срещу прекъсване на електроснабдяването. Електрозахранването на помещението е с висока степен на защита и е екранирано срещу външни интервенции.
2. Вентилационната система е специално предназначена за такъв клас помещения, като не допуска компрометиране на физическата и електромагнитната защита на това помещение, както и нормалната работа на инсталираните компютърни компоненти.

5.1.4 Наводнение

1. Предвидени са специални мерки срещу наводнение на помещението.

5.1.5 Предотвратяване на пожар и защита от пожар

1. Доставчикът спазва въведените нормативни и стандартизационни противопожарни изисквания за такъв клас помещения.

5.1.6 Съхранение на носители на данни

1. В помещението са разположени сейфове с различна степен на физическа защита срещу отваряне, в които се съхранява информацията, квалифицирана като конфиденциална.

5.1.7 Срок на употреба на технически компоненти

1. Експлоатационният срок на физическите елементи в състава на всички критични компоненти на инфраструктурата на B-Trust се съблюдава и след предвидения период на работа, те се извеждат от употреба.

5.1.8 Дублиране на техническите компоненти

1. Всички критични компоненти в инфраструктурата B-Trust на Доставчика са дублирани.
2. Компонентите в инфраструктурата, които предоставят услуги в реално време, свързани с издадените удостоверения, са изпълнени по схема за непрекъсваемост на услугите.

5.2 Процедурен контрол

1. Оперативните процедури в настоящия Наръчник, относно инфраструктурата на B-Trust, се изпълняват в пълно съответствие с разработени вътрешни правила, указания и Политика за сигурност на Доставчика.

5.2.1 Длъжности и дейности

1. Доставчикът поддържа квалифицирани служители на длъжности, които осигуряват изпълнението на задълженията му във всеки момент при осъществяването на дейността по издаване, поддръжка и управление на удостоверенията за КЕП, в съответствие с нормативната уредба.
2. Доставчикът осигурява дейността си със собствен персонал.
3. За определени дейности в чл. 5 в НДДУУ, Доставчикът може да привлича и външни лица.

5.2.2 Брой на служители за определена задача

1. За всяка от посочените дейности в нормативната уредба, Доставчикът поддържа поне по едно лице, което да изпълнява поставените задачи.

5.2.3 Идентификация на длъжност

1. Доставчикът е разработил длъжностни характеристики за всяка една от длъжностите на персонала, който изпълнява дейността му.
2. Длъжностите от персонала на Доставчика включват дейности по:
   - генериране и поддържане на инфраструктурата на публичния ключ на доставчика на удостоверителни услуги;
   - администриране и осигуряване сигурност на системите;
   - създаване и управление на удостоверения за квалифициран електронен подпис, включително създаване на двойка ключове - частен и публичен, за квалифициран електронен подпис;
   - съхранение на данни и архивиране.

5.2.4 Изисквания за разделяне на отговорностите

1. Дейностите на персонала на Доставчика се изпълняват от различни лица.

5.3 Квалификация и обучение на персонал

1. Персоналът на Доставчика притежава необходимата квалификация, професионални познания и опит в следните области: технологии за сигурност, криптография, PKI - технология, технически норми за оценка на сигурността, информационни системи, комуникации и др.
2. Лицата от персонала на Доставчика преминават начално и последващо квалификационно обучение по експлоатация на компонентите на инфраструктурата B-Trust.
3. Изискванията за допълнителна квалификация, опреснителни и други мероприятия са разписани във вътрешни документи на Доставчика.
4. Доставчикът подготвя и актуализира вътрешни инструкции за работа, които предоставя на персонала за целите на самообучение и повишаване на квалификацията при работа.

5.4 Изготвяне и поддържане на журнали

5.4.1 Записи на значими събития

1. Доставчикът съхранява записи, създавани от операционните системи на компютърните платформи в инфраструктурата B-Trust, както следва:
   - при инсталиране на нов и/или допълнителен софтуер;

- при спиране и стартиране на системите и приложенията в тях (дата, време);
- при успешни и неуспешни опити за стартиране на и достъп до хардуерни и софтуерни PKI-компоненти на системите;
- при системни софтуерни и хардуерни сривове на системите и други аномалии в платформите.

2. Доставчикът съхранява записи, създавани от компонентите (софтуер и хардуер) в инфраструктурата на B-Trust относно:
   - генериране и управление на двойките ключове и удостоверения за удостоверяващите органи и компоненти в инфраструктурата на B-Trust;
   - управление на криптомодулите (HSM) на „B-Trust Root CA”, „B-Trust CA QES“ и „B-Trust CA AES“;
   - съдържание на издадените удостоверения;
   - генериране и управление на двойките ключове и удостоверения на Потребителите;
   - успешна или неуспешна обработка на заявки за издаване и/или поддръжка на удостоверения;
   - генериране на CRL;
   - публикуване на издадени валидни удостоверения в Публичния регистър;
   - конфигуриране на профили на удостоверения;
   - статус на удостоверение в реално време;
   - удостоверяване на време на представено съдържание.
3. Достъп до информацията на записите имат само овластени лица от персонала по поддръжка на системите.
4. Доставчикът съхранява записи, които се създават в Регистриращ орган/МРС относно:
   - постъпили документи за регистриране с цел установяване на идентичност/самоличност и на искания за издаване, подновяване, спиране/възобновяване и прекратяване на удостоверения;
   - вътрешни процедури за идентификация и регистрация.
5. Съхраняват се записи, създадени от комуникационните компоненти в инфраструктурата.
6. Съхраняват се записи в документалния архив - стари и актуални версии на Наръчника на потребителя, заявки-формуляри, инструкции за работа и др.

5.4.2 Честота на създаване на записи

1. Информацията за електронните журнали се генерира автоматично.
2. Записите и логовете периодично се анализират от овластени служители на Доставчика.

5.4.3 Период на съхранение на записи

1. Журналите се съхраняват за период от 1 (една) година.

5.4.4 Защита на записите

1. Информацията от записите в логовете периодично се записва на физически носители, които се съхраняват в специален сейф, намиращ се в помещение с висока степен на физическа защита и контрол на достъпа.
2. Само квалифицирани овластени лица от персонала на Доставчика имат право на достъп и работа с тези записи и логове.

5.4.5 Поддържане на резервни копия

1. Поддържат се резервни копия от записите в логовете на системите, които се съхраняват надеждно.

5.4.6 Уведомяване след анализ на записи в журнала

1. Периодично се анализират записите в журнала по отношение на уязвимост и надеждност на системите и се уведомяват компетентните органи на Доставчика за вземане на мерки по управление на сигурността, ако е необходимо.

5.5 Архив и поддържане на архива

1. Информацията за значими събития се архивира в електронен вид периодично.
2. На хартиен носител или в електронен вид се архивира и цялата информация, свързана със искането за издаване, подновяване, спиране/възобновяване и прекратяване на удостоверения и пълния документооборот между Доставчика и Потребителите.
3. Доставчикът съхранява архива във формат, позволяващ възпроизвеждане и възстановяване.

5.5.1 Видове архиви

1. Доставчикът поддържа хартиени и електронни архиви.

5.5.2 Период на съхранение

1. Архивът се съхранява за срок от 10 (десет) години.

5.5.3 Защита на архивна информация

1. Сигурността на архива се обезпечава, както следва:
   - архивните файлове в електронна форма са електронно подписани;
   - специфичните събития и данни, които се записват в архива са определени и документирани от Доставчика;
   - съхранява се на надеждни електронни носители, които не могат да бъдат лесно унищожени или изтрити през периода на съхранение на архива;
   - Удостоверяващият орган електронно подписва всички удостоверения и списъци на прекратени и спрени удостоверения;
   - само овластени лица от персонала по поддръжка на системите работят със защитената архивна информация;
   - електронните комуникации между локалните компоненти на инфраструктурата са защитени на база стандарта PKIX;
   - отдалечените електронни комуникации са защитени и са базирани на стандарта PKIX;
2. Доставчикът преценява използването на пощенски и куриерски услуги и факс с Потребителите.

5.5.4 Възстановяване на архивна информация

1. При необходимост Доставчикът възстановява информация от архива.

5.5.5 Изискване за удостоверяване на дата и на час

1. Отделните архиви се обезпечават с удостоверяване на точното време на подписването им.

5.5.6 Съхраняване на архива

1. Вътрешна (журнална) и външна (документална) информация се съхранява надлежно в специален сейф в помещение с висока степен на физическа защита.

5.5.7 Придобиване и проверка на информация в архива

1. Публичната архивна информация на Доставчика се публикува и е достъпна в Публичния регистър и CRL и в документалния регистър. Друга информация, която се събира при искане за издаване или управление на удостоверение е достъпна само за лицата, подали искането или за съответно упълномощени от тях лица.
2. Наръчникът, Политиките, Договорът за удостоверителни услуги и инструкциите за обслужване/работа на Потребителите са публично достъпни в документалния регистър на Доставчика и могат да се получат и изтеглят от Интернет страницата на Доставчика.
3. Доставчикът осигурява публичната архивна информация в четим вид.

5.6 Промяна на ключ

1. Доставчикът може да промени ключа, съответстващ на издадено удостоверение, само като издаде ново удостоверение или поднови текущото с „Re-Key”.

5.7 Компрометиране на ключове и възстановяване след аварии

1. Доставчикът полага дължимата грижа, за да поддържа непрекъсваемост и цялостност на удостоверителните услуги, свързани с удостоверенията, които издава, поддържа и управлява.
2. Доставчикът полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на ключовете на Удостоверяващите си органи вследствие от природни бедствия или аварии.
3. В случай на сривове в компютърен ресурс, в софтуер или в информацията, Доставчикът уведомява Авторите/Титулярите, възстановява компонентите на инфраструктурата и приоритетно възобновява достъпа до Публичния регистър и CRL.

5.8 Компрометиране на частен ключ

5.8.1 На Удостоверяващ орган

1. Доставчикът предприема следните действия при компрометиране на частния ключ на оперативния Удостоверяващ орган:
   - прекратява незабавно удостоверението на оперативния орган;
   - издава и публикува нов CRL от базовия орган;
   - уведомява Потребителите и Доверяващите се страни;
   - спира оперативния Удостоверяващ орган;
   - уведомява КРС;
   - извършва незабавен анализ и изготвя доклад за причината за компрометирането;
   - инициира процедура по генериране на нова двойка оперативни ключове;
   - издава ново удостоверение на органа от Базовия орган.
2. Доставчикът предприема следните действия при компрометиране на частния ключ на базовия Удостоверяващ орган:
   - прекратява незабавно удостоверението на базовия орган;
   - следва всички стъпки по предходната точка;
   - уведомява КРС и акредитира/регистрира нов(и) удостоверяващ(и) орган(и).

5.8.2 На Автор

1. При компрометиране на частен ключ на Автора, същият или Титулярят, в случай, че удостоверението е издадено с вписан Титуляр, е задължен незабавно да уведоми Доставчика, за да инициира процедура по прекратяване на удостоверението.

5.9 Прекратяване на дейността на Доставчика

1. Дейността на Доставчика се прекратява по реда на НДДУУ.
2. При прекратяването на дейността си Доставчикът:
   - уведомява КРС за намерението си, не по-късно от 4 месеца преди датата на прекратяване;
   - независимо от изискването по предходната точка, Доставчикът уведомява КРС в случай на иск за обявяване на дружеството в несъстоятелност, за обявяване на дружеството за недействително или за друго искане за прекратяване или за започване на процедура по ликвидация;
   - полага всички усилия и грижи, за да продължи действието на издадените удостоверения;
   - уведомява писмено КРС и Потребителите дали дейността на Доставчика се поема от друг регистриран доставчик, както и относно името му, най-късно към момента на прекратяване на дейността. Уведомление се публикува и в Интернет страницата на Доставчика;
   - уведомява Потребителите относно условията по поддръжка на прехвърлените удостоверения към Доставчика-приемник;
   - ДУУ променя статуса на своите удостоверения и надлежно предава цялата документация, свързана с дейността му на приемащия Доставчик, заедно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени);
   - извършва необходимите действия за прехвърляне на задълженията за поддръжка на информацията към приемащия Доставчик, включително архив на събитията за промяна на статус на издадените удостоверения за съответния период. Тази информация се предава на приемащия Доставчик при същите условия, като тези описани в настоящата политика;
   - управлението на вече издадените удостоверения за крайни клиенти преминава към приемащия Доставчик;
   - в случай, че Доставчикът не успее да прехвърли дейността си на друг регистриран доставчик, той прекратява действието на всички издадени удостоверения и предава цялата документация на КРС;
   - КРС поддържа регистър със CRL.

6 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

6.1 Генериране и инсталиране на двойка ключове

1. Криптографските (RSA) двойки ключове за служебните удостоверения на Доставчика се генерират и инсталират съгласно инструкциите и процедурите в този документ.
2. Доставчикът използва своите частни ключове само за целите на дейността си както следва:
   - да подписва издадени служебни удостоверения на оперативни органи в своята инфраструктура;
   - да подписва издаваните и публикувани CRL;
   - да подписва всички издавани и публикувани удостоверения за КЕП на Потребителите.
3. Криптографската (RSA) двойка ключове (частен и публичен) на издаваните удостоверения за КЕП в инфраструктурата на Доставчика се генерира както следва:
   - от Автора/Титуляря - с хардуер и софтуер, който е под негов контрол, но е одобрен от Доставчика;
   - от оператор на Регистриращия орган/МРС на Доставчика - с хардуер и софтуер, който е под контрола на инфраструктурата на B-Trust.
4. Генерацията на двойка ключове на удостоверение за КЕП винаги използва SSCD, със защитен профил съгласно нормативната уредба по ЗЕДЕП.
5. Доставчикът може на базата на договорни отношения да предостави на Авторите/Титулярите одобрени от него технически средства, които отговарят на изискванията за ниво на сигурност.
6. Само електронни подписи, създадени с частен ключ на двойка ключове генерирани в SSCD имат характера на КЕП.
7. Авторът/Титулярят се задължава да използва лицензиран софтуер на даден производител за работа с SSCD.

6.2 Процедура по генериране

6.2.1 На Удостоверяващ орган на Доставчика

1. Доставчикът генерира двойки криптографски (RSA) ключове на базовия и на оперативен Удостоверяващи органи като използва хардуерна криптосистема (HSM, Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо.
2. Оторизирани лица от персонала на Доставчика изпълняват стъпките по генериране, инсталиране и съхраняване на двойките ключове на Базовия и на Оперативните удостоверяващи органи, съответно „B-Trust Root CA" и „B-Trust Operational CA QES" съгласно документирана вътрешна процедура, съгласувана и утвърдена от ръководството на Доставчика.
3. Процедурата се изпълнява в присъствие на член на Съвета на директорите на „БОРИКА - БАНКСЕРВИЗ" АД и на нотариус.
4. Двойка ключове на Удостоверяващ орган на Доставчика се генерира само след инициализация на съответния слот в хардуерната криптосистема, обслужваща този Орган.
5. При инициализация на всеки слот се въвеждат предварително подготвени кодове за контрол на достъпа до частния ключ на Органа в този слот.
6. Кодовете за достъп до частния ключ са независимо поделени между поне две оторизирани лица от персонала на Доставчика, с оглед на невъзможност за персонална активация на достъпа до съответния частен ключ.
7. Създадените частни ключове на Удостоверяващите органи се съхраняват разделно върху отделни SSCD, всяко от които е под контрола на повече от едно оторизирано лице от персонала на Доставчика.
8. Разделното съхранение на частните ключове и индивидуалния контрол на достъп до съхраняваните части на частни ключове на Удостоверяващите органи в отделните SSCD не позволява тези ключове да бъдат компрометирани и/или нерегламентирано репродуцирани извън Доставчика.

6.2.2 На Автора/Титуляря

1. Двойката ключове на Автор/Титуляр на удостоверение за КЕП се генерира само в одобрен от Доставчика SSCD, проверени за нивото на сигурност и за успешна работа през интерфейсите на инфраструктурата на B-Trust.
2. Когато двойката ключове се генерира при Доставчика, винаги се използва B-Trust SSCD. Частният ключ на генерираната двойка ключове не може да бъде изведен от SSCD.
3. Контролът на частния ключ е чрез код за достъп, а дължината на ключа за КЕП е поне 2048 бита. Авторът

използва частния ключ да създаде подписа като въвежда кода за достъп на SSCD.

4. Когато двойката ключове се генерира при Автор/Титуляр, Доставчикът препоръчва последният да използва в инфраструктурата на B-Trust одобрено SSCD или еквивалентно такова.
5. Доставчикът препоръчва Потребителят да използва B-Trust SSCD или друго SSCD, съвместимо в инфраструктурата на B-Trust.

6.2.3 Доставка на частния ключ

1. Когато двойката ключове се генерира при Доставчика, Авторът/Титулярят или изрично упълномощено от него лице получава частния ключ и издаденото удостоверение върху B-Trust SSCD в МРС на Доставчика.
2. SSCD гарантира най-високо ниво на сигурност и защита на частния ключ и се предоставя заедно с начален код за достъп.
3. Авторът/Титулярят е задължен да смени предоставения начален код за достъп и въведе свой личен.
4. Когато Автор/Титуляр генерира двойката ключове в друго SSCD, частният ключ е в това SSCD, но чрез Регистриращия орган/МРС Доставчикът проверя държането на този ключ от Автора/Титуляря.

6.2.4 Доставка на публичния ключ при Доставчика

1. Изпълнява се само от Автора/Титуляря, при който се генерира двойка ключове и който следва да достави своя публичен ключ на Доставчика за нуждите на процеса на издаване на удостоверението.
2. Авторът/Титулярят доставя чрез Регистриращия орган/МРС на Доставчика публичния ключ от генерираната двойка ключове, чрез заявка в електронен форма.
3. Авторът/Титулярят може да предостави електронната заявка на носител, лично в Регистриращия орган/МРС, заедно с другите документи съгласно Политиката на Доставчика или през Интернет-страницата на Доставчика.
4. Регистриращият орган/МРС на Доставчика задължително прави проверка на държането на частния ключ от Автора/Титуляря.

6.2.5 Доставка на публичния ключ на Доставчика на Доверяващи се страни

1. Публичните ключове на Доставчика са публично достъпни в Интернет страницата Доставчика, където са публикувани неговите служебни удостоверения.
2. Всяка Доверяваща се страна изгражда доверие към Доставчика, като приеме и зареди в системите под неин контрол служебните удостоверения на Доставчика.

6.2.6 Дължина на ключове

1. Дължината на базовия RSA-ключ на Доставчика е 4096 бита.
2. Дължината на двойката RSA-ключове на оперативния Удостоверяващ орган „B-Trust Operational CA QES" е 4096 бита.
3. Дължината на двойката RSA-ключове на оперативните органи „B-Trust TSA", „B-Trust VA" и „B-Trust VA QES" е не по-малка от 2048 бита.
4. Дължината на двойка ключове (RSA) за КЕП на Автор/Титуляр, генерирана чрез инфраструктурата на Доставчика (B-Trust SSCD) е поне 2048 бита.
5. Дължината на двойка ключове (RSA) за КЕП на Автор/Титуляр, генерирана извън инфраструктурата на Доставчика е поне 2048 бита.
6. Независимо къде е генерирана двойката ключове за издаване на удостоверение за КЕП, ключът трябва да е с дължина най-малко 1024 бита за алгоритми RSA и DSA и 160 бита за алгоритми ECDSA.

6.2.7 Параметри на публичен ключ

1. Параметрите на публичния ключ са посочени и удостоверени в удостоверението, което Доставчикът издава за този публичен ключ, съответстващ на частния ключ в SSCD.

6.2.8 Използване на ключа

1. Параметрите на използване на двойката ключове, съответно на частния ключ, се съдържат в удостоверението, което издава Доставчика чрез атрибутите "keyUsage" и „extended keyUsage".

6.3 Защита на частен ключ и контрол на криптографския модул

6.3.1 Стандарти

1. Основните компоненти в инфраструктурата на B-Trust „B-Trust Root CA" и „B-Trust CA QES" използват

високо-надеждна криптографска система (Hardware Security Module, HSM), сертифицирана за ниво на сигурност FIPS 140-2 Level 3, която удовлетворява нормативните изисквания.

2. B-Trust SSCD, в което се генерира и съхранява частния ключ на Автора/Титуляря е с ниво на сигурност CC EAL 4+/FIPS 140-1 Level 2.
3. Всички SSCD извън инфраструктурата на B-Trust, които Потребителят може да ползва за да генерира двойка ключове и да съхранява частния ключ, трябва да са сертифицирани за ниво на сигурност CC EAL 4 и по-високо еквивалентно.

6.3.2 Контрол на използване и съхранение на частен ключ

1. Частните ключове на Удостоверяващите органи на Доставчика се използват само в криптосистемата (HSM) и са достъпни посредством кодове за достъп, разделени на няколко части, които са известни на оторизирани лица от персонала на Доставчика.
2. Едновременно с генериране на двойка ключове на Удостоверяващ орган се изпълнява и процедурата по съхраняване на частния ключ (или двойката ключове) в съответствие с утвърдена вътрешна процедура.
3. Частният ключ на Автор/Титуляр се използват само в B-Trust SSCD или в SSCD с еквивалентно ниво на сигурност и е достъпен посредством личен код за достъп.
4. Едновременно с генериране на двойка ключове на Автор/Титуляр се изпълнява съхраняване на частния ключ в SSCD.
5. Доставчикът по никакъв начин не съхранява и не архивира частен ключ на Автор/Титуляр за създаване на КЕП, независимо къде се генерира двойката.

6.3.3 Съхранение и архивиране на частния ключ

1. Частните ключове на Удостоверяващите органи се съхраняват на части разделно върху отделни SSCD със защитен профил CC EAL 4+ или по-висок, като достъпът до всяко SSCD се контролира чрез код за достъп от съответното оторизирано лице от персонала на Доставчика.
2. Кодът за достъп до всяко SSCD е личен за всяко отделно оторизирано лице от персонала на Доставчика.
3. Разделното съхранение на частните ключове на Удостоверяващите органи върху няколко SSCD и личния контрол на достъп до тези SSCD не позволява ключовете да бъдат компрометирани или нерегламентирано репродуцирани извън Доставчика.
4. Репродуцирането на частни ключове на Доставчика върху резервна криптографска система (HSM) след дефектиране на оперативната такава, се изпълнява само в присъствие на поне 2 оторизирани лица, всяко от които контролира достъпа до неговото SSCD.
5. Частният ключ на Автор/Титуляр се съхранява само на SSCD и не може да се репродуцира на друго SSCD.
6. При дефектиране на SSCD, Потребителят трябва да го подмени и да заяви издаване на ново удостоверение.

6.3.4 Трансфер на частен ключ в и от криптографски модул

1. Трансфер на частен ключ на Удостоверяващ орган на Доставчика от криптосистемата (HSM) с цел съхранение и възстановяване в резервна такава се изпълнява под изключителен контрол и само при Доставчика съгласно документираните и утвърдени вътрешни процедури за генериране и съхранение и за възстановяване на ключовете на Удостоверяващ орган.
2. Трансфер на частен ключ на Автор/Титуляр към и от Доставчика с цел съответно съхранение и възстановяване в друго SSCD не се поддържа.
3. Частният ключ на Автор/Титуляр се съхранява само на SSCD, в което се генерира двойката ключове и не може да се трансферира/репродуцира на друго.

6.3.5 Метод на активация на частен ключ

1. Частен ключ на Доставчика се активира посредством поделен системен код за достъп, отделните части на който са известни на повече от едно оторизирано лице от персонала на Доставчика.
2. Само в присъствие на тези лица, след въвеждане на всички части на кода за достъп, се разрешава достъпът до слота в криптосистемата (HSM) и се активира частния ключ.
3. Частен ключ на Автор/Титуляр се активира чрез въвеждане на потребителския код за достъп на SSCD, където се съхранява ключа или се използва друг способ на идентификация.

6.3.6 Метод на де-активация на частен ключ

1. Частен ключ на Доставчика в криптосистемата на Удостоверяващите органи се деактивира (прекратява се възможността за използване/достъп на частния ключ) посредством преустановяване на логическия достъп до съответния ключ в нея.

2. Частен ключ на Автор/Титуляр се деактивира (прекратява се възможността за използване/достъп на частния ключ) посредством преустановяване на логическия достъп до SSCD или физическо му унищожаване.

6.3.7 Унищожаване на частен ключ

1. Частен ключ на Доставчика в криптосистемата на Удостоверяващите органи се унищожава посредством изтриване на ключа или съответния слот. При необходимост се изтриват и съхраняваните в архива носители (SSCD) за възстановяване.
2. Частен ключ на Автор/Титуляр се унищожава посредством изтриването му от SSCD или цялостното изтриване/инициализация на SSCD.

6.4 Други аспекти на управление на двойка ключове

6.4.1 Архивиране на публичния ключ

1. Публичните ключове на Удостоверяващите органи се съдържат в издадените служебни удостоверения на Доставчика и се съхраняват във вътрешен регистър. Същите са публично достъпни чрез публикуване на удостоверенията на Доставчика.
2. Публичните ключове на Удостоверяващите органи се архивират и съхраняват за период от 10 години след изтичане на периода на валидност или прекратяването на съответните удостоверения.
3. Публичните ключове на Автори/Титуляри се съдържат в издадените за тях удостоверения, които са публикувани в Публичен регистър и се съхраняват във вътрешен регистър.
4. Публичните ключове на Автори/Титуляри се съхраняват и архивират чрез периодично архивиране на вътрешния регистър.

6.4.2 Период на валидност на удостоверение и употреба на двойка ключове

1. Удостоверенията за КЕП имат следните срокове на действие:
   - на базовия Удостоверяващ орган „B-Trust Root CA" - 20 (двадесет) години;
   - на оперативния Удостоверяващ орган „B-Trust CA QES" - 15 (петнадесет) години;
   - на Автор/Титуляр – съгласно договора между Доставчика и Автора/Титуляря, но не повече от 3 (три) години.
2. Когато се използва ключа за подписване след изтекъл период на валидност на удостоверението, подписът е невалиден и съответния подписан обект или изявление следва да се счита недействително.
3. Шест месеца преди изтичането на периода на валидност на Удостоверяващ орган, Доставчикът генерира нова двойка ключове и прилага всички необходими действия за ненарушаване на работата на Доверяващите се страни, които разчитат на старата двойка ключове. Новата двойка ключове на Удостоверяващия орган се генерира и публичната ѝ част се разпространява съгласно политиката в този документ.

6.5 Данни за активация

6.5.1 Генериране и инсталиране на данни за активация

1. При първоначално издаване на удостоверение върху B-Trust SSCD, преди генериране на двойка ключове, SSCD се инициализира и се създават следните кодове за достъп/активация: Потребителски ("User") и Административен ("SO") и съответно, за персонален достъп до частния ключ в SSCD и за деблокиране на блокирано SSCD.
2. Началният Потребителски и Административен код за достъп и за деблокиране на B-Trust SSCD се предоставят на Автора/Титуляря или на упълномощеното от него лице в запечатен, непрозрачен хартиен плик.
3. Авторът е задължен на смени първоначалния Потребителски код за достъп посредством софтуера, който се предоставя с B-Trust SSCD.
4. Доставчикът препоръчва Авторът да сменя периодично своя Потребителски код за достъп до SSCD.
5. Авторът/Титуляря следва да използва предоставеният Административен код за достъп да деблокира блокирано B-Trust SSCD.

6.5.2 Защита на данни за активация

1. Авторът е задължен да съхранява и пази от компрометиране кодовете за достъп на своето SSCD.

6.5.3 Други аспекти на данните за активация

1. След определен брой неуспешни опити за въвеждане на коректен код за достъп до частния ключ на Автора, SSCD се блокира.
2. Авторът трябва да използва предоставеният му Административен код за достъп за да деблокира блокирано B-Trust SSCD.

6.6 Сигурност на компютърните системи

6.6.1 Изисквания за сигурност

1. Компютърните платформи, на които работят всички критични компоненти на инфраструктурата на B-Trust, са оборудвани и конфигурирани със средства за локална защита на достъпа до софтуера и информацията.
2. Доставчикът осигурява методи и използва процедури за администриране и управление на сигурността на цялата инфраструктура на B-Trust, в съответствие с общоприети в международната практика стандарти за управление на информационната сигурност.
3. Надеждността на използваните системи, техническата и криптографска сигурност на осъществяваните чрез тях процеси, се осигурява чрез тестове и проверки на техническото оборудване и технологиите съгласно методика за оценка на сигурността.
4. Проверки и тестове се извършват периодично, както и при всяка промяна, която засяга сигурността на инфраструктурата.

6.6.2 Степен на сигурност

1. Степента на сигурност на използваните системи в инфраструктурата на B-Trust отговаря на нормативните изисквания за изпълнение на дейността на Доставчика и се определя чрез документа Политика за сигурност на Доставчика.

6.7 Развой и експлоатация (жизнен цикъл)

6.7.1 Развой

1. Развоят на продукти и удостоверителни услуги, свързани с издаваните и поддържани удостоверения от Доставчика, се осъществява на отделни системи, напълно независими от тези в редовна експлоатация.
2. Продукти, софтуер и услуги, които се предлагат от Доставчика, се тестват първоначално на развойните системи, преди да бъдат въведени в експлоатация.
3. Новите продукти и удостоверителни услуги, които Доставчикът предлага, се съпровождат от процедури по експлоатация и инструкции за ползване.

6.7.2 Експлоатация

1. Въведените в експлоатация удостоверителни услуги и продукти от Доставчика се поддържат посредством обособените за тази цел експлоатационни компютърни системи.
2. Чрез експлоатационните системи Доставчикът предоставя всички удостоверителни услуги.
3. Продуктите и услугите на Доставчика са тествани в условия на реална работа.

6.8 Мрежова сигурност

1. Доставчикът използва съвременни технически средства за обмен и защита на информация в инфраструктурата на B-Trust, за да гарантира мрежовата сигурност на системите срещу външни интервенции и заплахи.

6.9 Удостоверяване на време

1. Доставчикът публикува в отделен документ Политиката и практиката на Органа за удостоверяване на време.

7 ПРОФИЛИ НА УДОСТОВЕРЕНИЯ ЗА КЕП, НА CRL И НА OCSP

7.1 Профил на удостоверения за КЕП

1. Пълното съдържание (профил) на удостоверенията за КЕП се съдържа в Наръчник на потребителя, Част II: Политика на предоставяне на удостоверения и удостоверителни услуги.

7.1.1 Номер на версия

1. Доставчикът издава удостоверения за КЕП във формат X.509, v3.
2. Версията се вписва в издаваното удостоверение.

7.1.2 Разширения във формата на удостоверение

1. Атрибут „Subject Key Identifier"- формира се от публичния ключ, удостоверен в удостоверението като хеш-стойност на публичния ключ.
2. Атрибут „Authority Key Identifier"- формира се като хеш-стойност на публичния ключ на оперативния Удостоверяващ орган на Доставчика.
3. Атрибут „Issuer Alternative Name"- съдържа URL-стринг като алтернативно име на Доставчика.
4. Атрибут „Basic Constrains"- определя типа на удостоверението и има стойност „End entity" в удостоверението на Потребителя.
5. Атрибут „Certificate Policy" - има две политики: 1.3.6.1.4.1.15862.1.5.1.1 определя идентификатора на Политиката за удостоверенията за КЕП, които издава Доставчика; 0.4.0.1456.1.1 определя удостоверението като КЕП, издадено върху крипографско устройство за сигурно създаване на подписа (SSCD).
6. Атрибут „Key Usage" - критичен атрибут, който определя ограниченията в употреба на удостоверението.
7. Атрибут „Extehanced Key Usage" - допълва значението на атрибут "Key Usage" и указва допълнителните и специфични приложения на удостоверението.
8. Атрибут „CRL Distribution Point" - съдържа линк към актуалния CRL на оперативния Удостоверяващ орган на Доставчика.
9. Атрибут „Authority Information Access" - съдържа URL-адреса на Органите за валидация „B-Trust VA" и „B-Trust VA QES".
10. Атрибут „Qualified Statements" - атрибутът съдържа указание, че удостоверението е за КЕП (qualified electronic signature) и частния ключ е генериран и се съхранява в SSCD.

7.1.3 Идентификатори на алгоритмите на електронен подпис

1. Атрибутът „Signature algorithm" идентифицира алгоритмите (криптографския механизъм), които се използват за КЕП.

7.1.4 Форми на именуване

Виж секция „Именуване" от този документ.

7.1.5 Ограничения на имената

Виж секция „Именуване" от този документ.

7.1.6 Идентификатор на Политика

1. Удостоверенията за КЕП се издават съгласно Политика на Доставчика, която се вписва в атрибута „Certificate Policy" на удостоверението.

7.1.7 Означение на удостоверение за КЕП

1. Доставчикът използва в удостоверението с профил X.509 v.3 атрибута „Qualified Statements" с идентификатора (OID) 0.4.0.1862.1, съгласно спецификацията ETSI TS 101 862.
2. Удостоверението за КЕП се означава явно чрез атрибута "Certificate Policy", на който се присвоява идентификатора (OID) със значение 1.3.6.1.4.1.15862.1.5.1.1.

7.2 Профил на Списъка на прекратени удостоверения

7.2.1 Версия

1. Доставчикът, чрез своите Удостоверяващи органи издава, публикува и поддържа Списъци на прекратени удостоверения (CRL) във формата X.509 v.2.
2. Версията се вписва в издадения CRL.

7.2.2 Формат

1. Доставчикът издава, публикува и поддържа CRL, чийто формат е в съответствие с изискванията в международната препоръка RFC 3280 Internet PKI Certificate and Certificate Revocation List (CRL) Profile.
2. Удостоверяващите органи на Доставчика издават, публикуват и поддържат самостоятелни пълни CRL-и като в тях записват само прекратени удостоверения, които са издадени от съответния Орган.
3. Доставчикът не издава и не поддържа схема на „частичен" (delta) CRL, но запазва право при необходимост да въведе такава схема.
4. Основните CRL-атрибути са:
   - „Version"- версия;
   - „Issuer Name" - идентифицира Удостоверяващия орган, издал и подписал Списъка;
   - „Effective Date"/"This update" - време на издаване на Списъка;
   - „Next Update"- времето на валидност на Списъка. След посоченото време, Органът издава периодично нов Списък. През периода на валидност, в случай на прекратяване/спиране на удостоверение, Органът издава незабавно нов CRL;
   - "Signature algorithm" - означава криптографския механизъм/алгоритъма за електронен подпис на CRL;
   - "Signature hash algorithm" - хеш-функцията в механизма на електронния подпис.
5. Допълнителни CRL-атрибути са:
   - „Authority Key Identifier"- идентификатора на Органа, който издава и подписва Списъка. Съдържа значението на „subjectKeyIdentifier" от удостоверението на Органа, който подписва Списъка;

7.2.3 Формат на елемент в CRL

1. CRL на Удостоверяващ орган съдържа елементи за всички прекратени удостоверения от Органа. Тези елементи са постоянни в Списъка.
2. CRL на Удостоверяващ орган съдържа елемент за всяко спряно удостоверение от Органа.Такъв елемент е временен в Списъка до момента на възобновяване на удостоверението.
3. Атрибутите на елемент в CRL са:
   - "Serial number" - серийният номер на прекратено/спряно удостоверение;
   - "Revocation date"- време на прекратяване/спиране на удостоверение;
   - "CRL Reason Code" - код идентифициращ причината на прекратяване/спиране.
4. Значенията на причината за прекратяване/спиране на удостоверение са както следва:
   - "keyCompromise" - компрометиран частен ключ на Автора;
   - "ACompromise" - компрометиран частен ключ на оперативен Удостоверяващ орган на Доставчика;
   - "affiliationChange" - променен статус на Автора спрямо Титуляря - промяна в представителната власт, отнемане на представителната власт, прекратяване на трудово правоотношение и т.н;
   - "superseded" - удостоверението е заместено с друго;
   - "certificateHold" - действието на удостоверението временно е спряно.

7.3 Профил на OCSP

1. Органите за „B-Trust VA" и „B-Trust VA QES" на Доставчика работят и предоставят услугата „онлайн проверка на статус на удостоверение в реално време" в съответствие с международно утвърдената препоръка IETF RFC 2560 Internet PKI On-line Cerificate Status Protocol.
2. Информация за профила на заявка и на отговор при работа с „B-Trust VA" и „B-Trust VA QES" се съдържа в горепосочената техническа препоръка, публично достъпна от сайта на IETF.

8 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

8.1 Периодична и обстоятелствена проверка

1. Контрол на правно-регламентираната дейност на Доставчика, свързана с удостоверенията за електронен подпис и нейната съобразност с изискванията на ЗЕДЕП и нормативната уредба се осъществява от Комисията за регулиране на съобщенията, в рамките на нейните компетенции.
2. Вътрешен контрол на дейността на Доставчика се назначава от оперативното ръководство и/или Съвета на директорите на юридическото лице на Доставчика като редът и обхватът на проверките е съобразен с вътрешни документи на юридическото лице.
3. Ръководството на Доставчика осъществява постоянен оперативен контрол за точното изпълнение на инструкциите при работа от персонала на Доставчика.
4. Ръководството на „БОРИКА - БАНКСЕРВИЗ" АД назначава периодични проверки за съответствие на текущата дейност с утвърдените Практика и Политиката относно дейността на Доставчика.
5. Доставчикът изпълнява постоянен контрол върху дейността на Регистриращ орган/МРС.

8.2 Квалификация на проверяващите лица

1. Проверяващи лица могат да бъдат само лица, които имат право да изпълняват такива функции в съответствие с възприети в международната практика изисквания и документи.
2. Проверяващите лица следва да отговарят на изискванията по чл.32, ал.2, т.4 на ЗЕДЕП и Глава пета от НДДУУ или са акредитирани от международна акредитационна организация да изпълняват такива проверки.
3. Вътрешните проверки на работата на Регистриращ орган/МРС се изпълняват от служители на Доставчика, които са оторизирани за тази дейност.
4. Проверяващи лица не могат да упълномощават други лица да извършват част или цялата проверка, освен с изричното съгласие на Доставчика.
5. Проверяващите лица носят отговорност за проверените факти и обстоятелства, независимо дали са превъзложили част или цялата проверка на други лица със съгласието на Доставчика.

8.3 Отношения на проверяващите лица с Доставчика

1. Проверяващите лица трябва да бъдат независими, да не са свързани (пряко или косвено) и да нямат конфликт на интереси с Доставчика.
2. Отношенията между Доставчика и проверяващо външно лице се уреждат с договор.

8.4 Обхват на проверката

1. Проверката от страна на КРС обхваща нормативно регламентираните изисквания към дейността на Доставчика съгласно ЗЕДЕП.
2. Вътрешната проверка може да обхваща всяко обстоятелство или дейност, посочени в този документ, както и:
   - съпоставка на практики и процедури посочени в този Наръчник с тяхната практическа реализация при изпълнение на дейността на Доставчика;
   - проверка на дейността на подизпълнители (външни Регистриращи органи/МРС;
   - други обстоятелства, факти и дейности, свързани с инфраструктурата B-Trust, по преценка на Ръководството на Доставчика.

8.5 Обсъждане на резултатите и действия с оглед извършената проверка

1. Въз основа на направените оценки и доклада от проверката, Ръководство на Доставчика набелязва мерки и срокове за отстраняване на констатираните пропуски и несъответствия.
2. Персоналът на Доставчика предприема конкретни действия за тяхното отстраняване в посочените срокове.
3. Резултатите от извършената проверка се съхраняват надлежно в архива на Доставчика.

9 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

9.1 Цени и такси

1. Доставчикът поддържа документ "Тарифа за предоставяните удостоверителни, информационни, криптографски и консултантски услуги".
2. Доставчикът има право да променя едностранно Тарифата по всяко време от действието на Договора, като уведомява за това Титуляря посредством публикуване на промените на Интернет страницата.
3. Промяната има действие спрямо Титуляря от деня, следващ деня на публикацията.
4. В 5 (пет) дневен срок от датата на промяната и доколкото е налице увеличение на цените, Титулярят има право да прекрати едностранно договора с отправяне на писмено известие до Доставчика, считано от датата на изтичане на срока на последното удостоверение. В този случай договорът се счита прекратен от датата на промяната, като платените по договора възнаграждения за ползване на услуги не подлежат на възстановяване.
5. При липса на известие за прекратяване се счита, че Титулярят е съгласен с промяната.
6. Промяната на възнагражденията не може да засегне вече заплатени възнаграждения.

9.1.1 Възнаграждения

1. Стойността на договора включва едно или няколко от следните възнаграждения:
   - възнаграждение за издаване и поддържане на удостоверение;
   - възнаграждение за подновяване на удостоверение;
   - възнаграждение за извършени по искане на Титуляря консултации и технологична помощ;
   - цена за закупено или предоставено под наем от Доставчика оборудване;
   - възнаграждение за персонализиране на физически носител.
2. Дължимите възнаграждения и суми се заплащат на Доставчика в размери, съгласно Тарифата за предоставяните от „БОРИКА - БАНКСЕРВИЗ" АД удостоверителни, информационни, криптографски и консултантски услуги и в срокове и по начини, посочени в Договора и приложенията към него.
3. Доколкото има уговорено авансово или абонаментно възнаграждение за използване на услуга, същото не подлежи на възстановяване, ако Титулярят не е консумирал предоставяната услуга през съответния срок, за който се отнася авансовото или абонаментното възнаграждение.
4. Цената не включва начислените от телекомуникационните компании суми във връзка с ползвани от Автора/Титуляря услуги от тях за целите на предоставяните услуги от Доставчика. Те се дължат изцяло от Титуляря на съответната телекомуникационна компания. Доставчикът не дължи и не носи отговорност за заплащането на тези суми.
5. Всички разходи и такси за превеждане на дължимите суми по сметката на Доставчика, включително и тези кореспондентски банки, са за сметка на Клиента.

9.1.2 Възнаграждения за удостоверителни, криптографски, информационни и консултантски услуги

1. За услугите по предоставяне и използване на удостоверения за електронен подпис и свързаните с тях услуги се заплаща дължима сума при заявяване на услугата. В останалите случаи плащането се извършва в 10-дневен срок от получаване на фактурата или съгласно сключения договор.
2. Услугите свързани с осъществяване на технологична помощ и предоставяне на консултации за изграждане и поддържане на инфраструктура и решения за информационна сигурност са на база "човекочас" и се заплащат въз основа на двустранно подписан протокол за извършена работа. Цените на часовата ставка в приложената Тарифа са валидни в рамките на установеното работно време. При работа в извън установеното работно време, цените се увеличават със съответен процент, съгласно Тарифата.
3. За услуга „Удостоверяване на време" при съгласувано ниво на обслужване (SLA, Service Level Agreement) се заплаща съгласно договорните условия за доставка и ползване на услугата.
4. Цената на закупено или предоставено под наем от Доставчика оборудване се уговаря и се дължи съгласно условията на договора. Правоотношенията между Доставчика и Титуляря се уреждат съгласно общите правила на договора за продажба, респ. договора за наем.
5. При забавяне на плащанията след договорения срок Клиента дължи на Доставчика законовата лихва за периода до окончателното изплащане на дължимите суми.
6. Ползването на публикувани документи в Интернет страницата на Доставчика е безплатно. За запис и

предоставяне на тези документи върху физически носител се заплаща себестойността на този носител и куриерските разноски.

9.1.3 Фактуриране

1. Доставчикът издава на Потребителя фактура за предоставяните услуги.
2. Неполучаването на фактура не освобождава Потребителя от задължението му да заплати дължимите възнаграждения в уговорените срокове.
3. Всички дължими по договора суми се заплащат от Потребителя в брой или по банков път. Плащането по банков път се счита извършено със заверяването на банковата сметка на Доставчика с пълния размер на дължимите суми.
4. Всички банкови комисионни, такси и разноски във връзка с банковите преводи са за сметка на Потребителя.

9.1.4 Връщане на удостоверение и възстановяване на плащане

1. Автор/Титуляр може да възрази относно неточност или непълнота в съдържанието на издадено удостоверение в 3-дневен срок след публикуването му в Публичния регистър.
2. Ако причина за невярното съдържание на удостоверението е в Регистриращия орган/МРС, Доставчикът прекратява удостоверението и издава ново с вярно съдържание за своя сметка или възстановява направеното плащане за прекратеното удостоверение с невярно съдържание.
3. Ако причина за невярното съдържание на удостоверението е по вина на Автора/Титуляря, Доставчикът прекратява удостоверението и не възстановява направеното плащане. Доставчикът може да издаде ново с вярно съдържание за сметка на Потребителя.
4. Потребителят може да откаже издадено удостоверение за КЕП с вярно съдържание, което Доставчикът ще прекрати незабавно без да възстанови направеното плащане за прекратеното удостоверение.

9.1.5 Безплатни услуги

1. Доставчикът предоставя безплатно регистърни и информационни услуги, свързани с ползване на Публичния регистър, както следва:
   - проверка на публикувано в регистъра удостоверение на Автор/Титуляр;
   - проверка за валидност на издадено удостоверение в Публичния регистър;
   - проверка на статус на удостоверение в реално време;
   - удостоверение за време на представено съдържание/електронно изявление без SLA;
   - изтегляне на актуален CRL и достъп до архива със CRL-и;
   - изтегляне на служебните удостоверения на Доставчика;
   - изтегляне на публични документи на Доставчика;
   - други услуги.

9.2 Финансови отговорности

9.2.1 Застраховка на дейността

1. Доставчикът сключва задължителна застраховка на дейността си като регистриран ДУУ от КРС;
2. Задължителната застраховка е с непрекъсваем срок и се подновява периодично.
3. Предмет на застраховката е отговорността на Доставчика за осъществяваната от него дейност съгласно изискванията на ЗЕДЕП и НДДУУ.
4. Доставчикът има задължителна застраховка в размер на застрахователни суми посочени в чл. 14, ал.1 на НДДУУ:
5. Задължителната застраховка покрива отговорността на Доставчика към Титуляри, съответно Доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в ЗЕДЕП и НДДУУ.
6. След настъпване на събитие, което може да позволи предявяване на иск покрит от застраховката, засегнатото лице трябва да уведоми писмено Доставчика и Застрахователя в срок от 7 дни след като събитието му стане известно.

9.2.2 Застрахователно покритие

1. Застрахователното покритие за нанесени неимуществени и/или имуществени вреди на Автор/Титуляр не надхвърля размера установен от НДДУУ.
2. Застраховката не покрива случаите по отказ на отговорност, в частност за вреди причинени от:
   - неспазване на задълженията на Автори/Титуляри на удостоверения;

- компрометиране или загуба на частен ключ на Автор поради неполагане на дължимата грижа за опазване или при използване;
- неспазване на изискванията за проверка на валидността на електронния подпис и на удостоверението от Доверяваща се страна;
- форсмажорни и други обстоятелства, извън контрола на Доставчика.

9.3 Конфиденциалност на бизнес информация

9.3.1 Обхват на конфиденциалната информация

1. Информация за Автори/Титуляри, която не е включена в издадените удостоверения и в CRL съставлява лични данни по смисъла на Закона за защита на личните данни (ЗЗЛД), се счита за конфиденциална.
2. Информацията по предходната точка се събира от Доставчика само доколкото е необходима за нуждите на издаване и поддържане на удостоверенията.
3. Считаната за конфиденциална информация не може да бъде предоставяна на трети лица, без изрично съгласие на предоставилите я лица с изключение на случаите, при които Доставчикът е задължен по силата на закон.
4. Доставчикът може да събира допълнителна информация, която също не се включва в удостоверение, но се използва за целите на качественото поддържане на удостоверителните услуги.
5. Конфиденциалната информация се съхранява на място, достъпът до което е ограничен само за лица от персонала на Доставчика, овластени да оперират с данните и се разкрива само след изрично съгласие на Автора/Титуляря с изключение на случаите, при които Доставчикът е задължен по силата на закон.
6. Никой освен Автора, включително и Доставчика, няма право да използва частния ключ за създаване на електронен подпис. Доставчикът препоръчва Автора да не излага потребителския код за достъп на B-Trust SSCD, дори ако той е шифрован.
7. Всички частни ключове на лица от персонала и звена в инфраструктурата на Доставчика са надеждно защитени срещу компрометиране и разпространение.
8. Записи в журналите и логовете от системите на Доставчика се разглеждат като конфиденциална информация и са защитени от неправомерен достъп и въздействие.

9.3.2 Неконфиденциална информация

1. Общодостъпна е всяка информация, съдържаща се в Публичния регистър по отношение на издадените удостоверения, както и в публикувания актуален CRL и в архивните копия на този списък.

9.3.3 Защита на конфиденциалната информация

1. Доставчикът и Авторите/Титулярите нямат право да разпространяват или да допускат разпространяване на информация, станала им известна при или по повод изпълнение на задълженията им по Договора, включително относно плащания, без предварително изрично писмено разрешение от другата страна.

9.4 Поверителност на лични данни

1. Доставчикът е регистриран като администратор на лични данни по реда на ЗЗЛД.
2. В качеството си на Администратор на лични данни, Доставчикът строго съблюдава изискванията за поверителност и неразпространение на личните данни на Автори/Титуляри, станали му известни при изпълнение на дейността си като ДУУ.
3. Съгласно утвърдената Политика на удостоверенията за КЕП елементи на информацията в тях могат да съдържат лични данни на Автори и Титуляри. С оглед осъществяването на дейността си и на определени изисквания на публичните електронни услуги към удостоверената информация, Доставчикът я прави достъпна за трети лица чрез издадените удостоверения, освен ако в искането за издаване на удостоверение не е посочена опцията „забрана на достъпа".
4. Във връзка с чл. 22, т.4 от ЗЕДЕП, Доставчикът публикува всяко издадено удостоверение и осигурява достъп на трети лица, съгласно указанията на Автора/Титуляря.

9.5 Права върху интелектуална собственост

1. Различни данни, включени в издавани удостоверения или публикувани в Публичния регистър са обект на права върху интелектуалната собственост и други имуществени и неимуществени права.
2. Отношенията по повод на тези права между Доставчика и другите участници в инфраструктурата на B-Trust, като външни Регистриращи органи, МРС и др. се уреждат с договор.
3. Всички издадени удостоверения от Доставчика са обект на авторско право на Доставчика.

4. Всички права върху използвани от Доставчика бизнес марки (напр., B-Trust®), както и съдържащи се в удостоверенията търговски наименования използвани от Титулярите, се запазват от титулярите им и се използват само за нуждите на предоставяните удостоверителни услуги.
5. Двойките ключове, кореспондиращи на удостоверенията на Доставчика и на Другите участници в инфраструктурата на B-Trust както и съответния секретен материал, са обект на права на Доставчика и на съответните участници, независимо от собствеността върху физическия носител на ключовете.

9.6 Отговорност и гаранции

9.6.1 Отговорност и гаранции на Доставчика

1. Доставчикът отговоря и гарантира, че спазва точно условията в настоящия документ, изискванията на ЗЕДЕП и на нормативната уредба при осъществяване на дейността на регистриран ДУУ.
2. Доставчикът осъществява дейността на регистриран ДУУ като:
   - използва техническо оборудване и технологии, които осигуряват надеждност на системи и техническата и криптографска сигурност при осъществяване на процесите, в това число и сигурен и защитен механизъм/устройство за генериране на ключове и за създаване на електронен подпис в своята инфраструктура;
   - издава удостоверения след като провери с допустими от закона средства представената информация;
   - съхранява и поддържа информация, свързана с издаваните удостоверения и оперативната работа на системите;
   - спазва установените процедури за работа и правила за технически и физически контрол, в съответствие с условията в този документ;
   - при искане издава съответните типове удостоверения, спазвайки условията и процедурите в този документ и съответните Политики;
   - уведомява Потребителите за факта на акредитацията си;
   - създава възможност за незабавно спиране и прекратяване на действието на удостоверение;
   - прекратява и спира действието на удостоверения при условията и по реда на съответната Политика;
   - уведомява незабавно след спиране на удостоверение Автора и Титуляря;
   - осигурява условия за точно определяне на времето на издаване, спиране, възобновяване и прекратяване на действието на удостоверенията;
   - осигурява мерки срещу подправяне на удостоверенията и поверителността на данните, до които има достъп в процеса на създаването на подписа;
   - използва надеждни системи за съхраняване и управление на удостоверенията;
   - осигурява само надлежно овластени служители да имат достъп за внасяне на промени, установяване на автентичността и валидността на удостоверенията;
   - при възникване на технически проблеми във връзка със сигурността, това да става незабавно достояние на обслужващия персонал;
   - с изтичане на срока на валидност на удостоверение да отмени валидността му;
   - информира Авторите, Титулярите и трети доверяващи се страни за техните задължения и дължимата грижа на поведение при използването и доверяването на предоставяните от Доставчика удостоверителни услуги, както и относно правилното и сигурно използване на издадените удостоверения и удостоверителните услуги, свързани с тях;
   - използва и съхранява събраната лична и друга информация само за целите на своята дейност по предоставяне на удостоверителни услуги по смисъла на ЗЕДЕП и в съответствие с разпоредбите на ЗЗЛД и другите относими правни норми;
   - не съхранява или не копира данни за създаване на частни ключове;
   - поддържа разполагаеми средства, които осигуряват възможност за извършване на дейността му;
   - застрахова за времето на своята дейност за вредите от неизпълнение на задълженията му по ЗЕДЕП, в съответствие със Застрахователната политика;
   - поддържа персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността;
   - поддържа Регистър, в който публикува издадените удостоверения, актуален CRL, други обстоятелства и електронни документи, съгласно този документ и ЗЕДЕП;
   - осигурява достъп до Регистъра по електронен път 24 часа в денонощието;
   - осигурява защита срещу внасяне на промени в поддържания Регистър от нерегламентиран и неправомерен достъп или поради случайно събитие;

- публикува в публичния Регистър на удостоверенията незабавно издадените и подписани удостоверения;
- създава условия на всяка доверяваща се страна да провери статуса на издадено и публикувано удостоверение в публичния Регистър на удостоверения.

3. Доставчикът отговаря пред Автор/Титуляр и Доверяваща се страна за:
   - задълженията си по предходната точка;
   - неверни или липсващи данни в удостоверение по негова вина;
   - пропуски в установяване на идентичността, съответно самоличността на заявителя.

9.6.2 Отговорност и гаранции на Регистриращ орган/МРС

1. Доставчикът гарантира, че Регистриращ орган/МРС изпълнява своите функции и задължения в пълно съответствие с условията в този документ, с изискванията и процедурите в Политиката и издадените вътрешни оперативни инструкции.
2. Доставчикът отговаря за действията на Регистриращ орган/МРС в инфраструктурата на B-Trust.

9.6.3 Отговорност на Автора/Титуляря

1. Автор/Титуляр трябва да:
   - спазва точно условията и процедурите на тази документ и съответната Политика при искане за издаване на удостоверения и ползването на другите удостоверителни услуги;
   - заплаща дължимото възнаграждение към Доставчика съгласно Договора и приложенията към него;
   - има основни познания относно използването на удостоверения за електронен подпис и PKI технологии;
   - предоставя вярна, точна и пълна информация, която Доставчикът изисква съгласно закона и този документ при подаване на искане за издаване и управление на удостоверение;
   - осигурява сигурна и надеждна среда и процедура (надеждни технически средства и софтуер), когато генерира двойката ключове извън инфраструктурата на Доставчика, с оглед опазване тайната на частния ключ;
   - използва алгоритми, съобразно изискванията на НИАКЕП при генериране на двойката ключове;
   - уведоми незабавно Доставчика, в случай на компрометиране или съмнения за компрометиране на частния ключ като изпрати заявка за спиране или прекратяване действието на удостоверението;
   - съхранява и защитава надеждно своя частен ключ през цялото време на валидност на удостоверението срещу загуба и компрометиране в съответствие на изискванията на Наръчника. Всяко използване на частния ключ се приема като извършено от Титуляря действие;
   - приеме издадено удостоверение за електронен подпис незабавно след неговото представяне от страна на Доставчика;
   - провери пълнотата и верността на съдържанието на удостоверение в срок от 3 (три) дни от публикуването му. В случай на несъответствие между предстaвената информация по силата на договора и съдържанието на удостоверението, да уведоми незабавно Доставчика;
   - извести за настъпила промяна в удостоверената информация и да поиска прекратяване на удостоверението;
   - уведоми Доставчика за всяка промяна в информацията, която не е включена в издадено негово удостоверение, но която е предоставена в процеса на издаване на удостоверението;
   - смени своя първоначален код за достъп до SSCD, преди да използва удостоверението;
   - използва издадените му удостоверения само с лицензиран криптографски софтуер;
   - използва издадено удостоверение само в съответствие с отбелязаното в него предназначение и съгласно приложимата Политика, както и с оглед ограниченията при които е издадено;
   - не използва частния ключ за създаване на електронен подпис след изтичане срока на валидност на удостоверение или след спиране или прекратяване действието му;
   - информира всяка Доверяваща се страна относно нейната грижа и отговорност при доверяване на удостоверението за КЕП;
   - приема условията за грижата и отговорността при доверяване на удостоверение за КЕП, в случай че действа като Доверяваща се страна.
2. Авторът/Титулярят е отговорен ако е приел удостоверение, издадено от Доставчика въз основа на предоставени от него неверни данни, съответно въз основа на премълчани или липсващи данни.
3. Доставчикът ще регресира спрямо Автора/Титуляря претенция за всички претърпени вреди, вследствие от реализирана отговорност на Доставчика, поради неизпълнение на произтичащи от този документ или договора задължения, когато:

- е използвал алгоритъм, който не отговаря на изискванията на НИАКЕП;
- не изпълнява точно изискванията за сигурност, определени от Доставчика;
- не поиска прекратяване действието на удостоверение, когато е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерното му използване;
- е приел удостоверението при неговото издаване, когато Авторът не е бил овластен да държи частния ключ, съответстващ на посочения в удостоверението публичен ключ;
- е приел удостоверението при неговото издаване, като е направил неверни изявления пред Доставчика, имащи отношение към съдържанието на удостоверението;
- е приел удостоверението, когато Авторът не е бил овластен да поиска издаването на удостоверението.

9.6.4 Грижа и отговорност на Доверяваща се страна

1. Лицата, които се доверяват на удостоверенията за електронен подпис трябва да притежават основни познания относно принципите на използване и приложимост на електронния подпис и на услугите, свързани с употреба на удостоверение за електронен подпис.
2. Доверяващата се страна следва да положи дължима грижа, като:
    - се доверява на удостоверенията само с оглед на Политиката относно предназначението и на ограниченията и условията, при които е издадено;
    - извърши проверка на статуса на удостоверението в поддържания от Доставчика Публичен регистър. Проверката на електронната автентичност и на интегритета на удостоверението извън Публичния Регистър или в неактуален CRL-списък не осигурява проверка за неговата валидност и всички настъпили вреди от предприети действия, след осъществяване единствено на такава проверка, са за сметка на Доверяващата страна;
    - проверява валидността на електронния подпис на електронно подписани изявления, както и валидността на електронния подпис на Доставчика по веригата от удостоверения до базовото удостоверение;
    - се увери, че приложенията, с които се използва удостоверението са функционално приложими за предназначението, за които е издадено, както и с оглед нивото на сигурност, посочени в съответната Политика.
3. Дължима грижа на Доверяващата се страна е да използва механизъм за сигурна проверка на подписа, който гарантира, че:
    - публичният ключ, който се използва за проверка на подписа съответства на този, който се представя пред него;
    - проверката за използване на частния ключ е надеждно потвърдена и резултатите от тази проверка коректно се представят;
    - при необходимост може да се установи съдържанието на подписания електронен документ;
    - автентичността и валидността на удостоверението към момента на подписването надеждно се проверяват;
    - резултатите от проверката и електронната идентичност на Автора/Титуляря правилно се представят;
    - всякакви промени, релевантни за сигурността са установими.
4. Доставчикът не носи отговорност за настъпили вреди на Доверяващата се страна от неполагане на дължимата грижа.

9.7 Отказ от отговорност

1. С изключение на случаите на претърпени вреди от използване и доверяване на удостоверения за КЕП, Доставчикът не отговаря за своите небрежни действия.
2. Доставчикът не отговаря в случаите, когато настъпилите вреди са следствие от небрежност, отсъствие на положена грижа или липса на основни познания относно технологиите на електронен подпис от страна на Автори/Титуляри или Доверяващи се страни.
3. Доставчикът по никакъв начин не може да отговаря за случаите, в които подписани и придружени с валидни удостоверения изявления са били оттеглени.
4. Доставчикът не отговаря в случаите, когато е подписан софтуер или информационни обекти и същите са причинили вреди на Доверяваща се страна.
5. Доставчикът не проверява и не следи за нарушаване на права на трети лица по отношение на техни търговски марки, търговски наименования или други имуществени или неимуществени права, когато информация, съдържаща се в издадени удостоверения е довела до такива нарушения. В случай на претърпени вреди от страна на Доставчика поради такива нарушения, същият може да ги претендира от

Титуляря.

6. Доставчикът не отговоря за преки или косвени, предвидими или непредвидими вреди, настъпили вследствие от използване или доверяване на спрени, прекратени или с изтекъл срок на валидност удостоверения.
7. Извън случаите по предходните точки, Доставчикът не носи отговорност за:
   - точността, автентичността, пълнотата или съответствието на информация, която е включена в тестови, безплатни или демонстрационни удостоверения;
   - качеството, функциите или технологията на софтуерните продукти и хардуерни устройства в инфраструктурата на B-Trust, използвани от Автори, Титуляри или Доверяващи се страни;
   - за своевременно прекратяване и спиране на удостоверения и/или проверка на статуса на удостоверения поради причини, които са извън неговия контрол (напр. неполагане на дължима грижа от страна на Доверяваща се страна, недобросъвестни действия от страна на Автори или Титуляри, телекомуникационни и енергийни смущения и др.).
8. Доставчикът не отговаря за вреди, причинени от използване на удостоверение за КЕП извън обхвата на вписаните в него ограничения и предназначения.

9.8 Ограничение на отговорност на Доставчика

1. За издавани удостоверения за КЕП, Доставчикът отговаря в рамките на следните лимити:

Типове удостоверения	Максимален лимит на отговорност /лв./
B-Trust Personal Certificate QES	40 000
B-Trust Professional Certificate QES	40 000

2. Посочените лимити на отговорност се считат за ограничения на отговорността на Доставчика по смисъла на чл. 24, във връзка с чл. 29, ал. 3 на ЗЕДЕП.

9.9 Компенсации за Доставчика

1. За всички случаи на неизпълнение на задълженията от страна на Автора/Титуляря, Доставчикът ще ангажира отговорността на Автора/Титуляря за вреди и ще има правото да прекрати незабавно издадено удостоверение.

9.10 Срок и прекратяване

1. Разпоредбите в настоящия документ, както и включените в него Практика и Политика на предоставяне на удостоверителни услуги от Доставчика са валидни до издаване и публикуване на следваща тяхна версия/редакция в публичния документален регистър.
2. Договорът за удостоверителни услуги между Доставчика и Потребител е със срок три години или до изтичане на срока на валидност на последното издадено удостоверение по договора.
3. С прекратяване на дейността на Доставчика се прекратяват разпоредбите, Практиката и Политиката съдържащи се в този документ.
4. В случай на недействителност на отделна клауза от този документ, валидността на целия документ се запазва и не се нарушава договора с Потребителя. Недействителната клауза се замества от повелителните норми на закона.
5. Договорът за удостоверителни услуги между Доставчика и Потребител се прекратява с изтичане на срока на валидност на последното издадено удостоверение по договора или с прекратяване на всички издадени удостоверения по договора.
6. Доставчикът съхранява надлежно и сигурно всички предишни версии/редакции на този документ, на Практиките и на Политиките.

9.11 Уведомяване и комуникация между страните

1. Доставчикът използва изявления, писма и съобщения на Регистриращия орган/МРС както и електронни уведомления, които публикува на своята Интернет-страница.
2. Клиентите на инфраструктурата на B-Trust могат да изпращат съобщения, писма, препоръки, въпроси и жалби до Доставчика като използват следния адрес за контакти:

пощенски адрес: София 1612, бул. „Цар Борис III" 41

телефон: 02/ 92 15 100
факс: 02/ 981 45 18
имейл адрес: info@b-trust.org

3. В случай на получаване на жалба, Доставчикът извършва незабавна проверка и изпраща отговор до жалбоподателя в срок от 2 работни дни.

9.12 Промени в Документа

1. Доставчикът може да прави редакционни промени в този документ, които не засягат съдържанието на правата и задълженията в него.
2. Промени, които водят до нова версия/редакция на документа се публикуват на Интернет-страницата на Доставчика.
3. Промените се съобщават на КРС и заинтересуваните лица.
4. Всяко лице може да отправя предложения за промени (структурни и съдържателни) и отстраняване на допуснати грешки, като използва посочените по-горе контакти с Доставчика.

9.13 Решаване на спорове и място (подсъдност)

1. Всички възникнали спорове между страните по договора за удостоверителни услуги се уреждат по споразумение между страните, чрез разбирателство и в дух на добра воля, а ако такова не бъде постигнато, се решават от компетентния български съд.

9.14 Приложимо право

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

9.15 Съответствие с приложимото право

1. Настоящият документ е разработен в съответствие със ЗЕДЕП и действащата нормативна уредба.

НАРЪЧНИК НА ПОТРЕБИТЕЛЯ - ЧАСТ II:

ПОЛИТИКА

ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

1. Политиката на предоставяне на удостоверения и удостоверителни услуги е документ, неделима част от Наръчника на потребителя, описващ политиката и процедурите, които Доставчикът следва при издаване на удостоверения за КЕП, видовете удостоверителни услуги приложими за тези удостоверения както и тяхното приложно поле.
2. Политиката определя начина и нивото на сигурност при идентификация на Автора/Титуляря, следваните процедури при издаване, поддръжка и управление на удостоверението, изискването за ниво на сигурност на SSCD за създаване на подписа и съхранение на частния ключ, определя степента на доверие в удостоверените данни и употребата му в различните приложения.
3. Доставчикът поддържа и прилага Политики за следните типове удостоверения за КЕП, които издава, поддържа и управлява „БОРИКА - БАНКСЕРВИЗ" АД като регистриран ДУУ:
    - удостоверения за КЕП с идентификатор на политика OID = 1.3.6.1.4.1.15862.1.5.1.1;
4. Общите изисквания и отговорности на Доставчика, Автора/Титуляря и дължимата грижа на всяка Доверяваща се страна при използване на удостоверения за КЕП са посочени в Част I (ПРАКТИКА) на Наръчника.
5. Общите процедури на спиране, възобновяване и прекратяване действието на издадено валидно удостоверение за КЕП се съдържат в Част I (ПРАКТИКА) на Наръчника.
6. Цените на удостоверенията и на услугите по издаване и поддържане на удостоверения за КЕП се съдържат в Ценоразписа на Доставчика, достъпен на неговата Интернет-страница.

10 ПОЛИТИКА НА ИЗДАВАНЕ, ПОДДРЪЖКА И УПРАВЛЕНИЕ НА ПЕРСОНАЛНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

10.1 Обща характеристика на удостоверението

1. Персонално удостоверение „B-Trust Personal Certificate QES" се издава на Автор/Титуляр - физическо лице и удостоверява електронната идентичност и връзката на Автора/Титуляря с публичния му ключ.
2. „B-Trust Personal Certificate QES" има характер на удостоверение за КЕП по смисъла на чл. 16, ал. 1 от ЗЕДЕП.
3. За издаването на удостоверение „B-Trust Personal Certificate QES" се изисква лично присъствие, пред Регистриращия орган/МРС на Доставчика, на Автора/Титуляр или упълномощено от него лице при проверка на неговата самоличност, респ. идентичност.
4. Процедурата по идентификация включва представяне на доказателство за самоличността на Автора и идентичността на Титуляря.
5. Проверката на искането за издаване на персонално удостоверение по реда на точки 3 и 4 осигурява високо ниво на сигурност по отношение на идентичността на Автора/Титуляря и връзката му с публичния ключ.
6. Авторът/Титулярят може сам да генерира двойката ключове, като използва B-Trust SSCD и съответен софтуер за него или друго еквивалентно SSCD, което е съвместимо в инфраструктурата на Доставчика.
7. Частният ключ за създаване на КЕП задължително се генерира в SSCD и не може да бъде изведен навън от него.
8. Издаденото персонално удостоверение за КЕП, удостоверяващо публичен ключ съответстващ на частния такъв, задължително се записва в SSCD, което се предоставя на Автора/Титуляря.
9. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към персоналното удостоверение за КЕП.

10.2 Предназначение и приложимост на удостоверението

1. Персоналното удостоверение може да се използва при създаване/полагане на КЕП на физическото лице посочено като Автор в удостоверението, към електронни документи и в приложения, които изискват високо ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в удостоверението за КЕП обозначената политиката, приложима към това удостоверение (атрибут "Certificate Policy") и предназначението и ограниченията на действието на удостоверението, описани в атрибутите "Key Usage" и "Extended Key Usage", преди да се довери на положения електронен подпис.

10.3 Обозначение на политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в персоналното удостоверение „B-Trust Personal Certificate QES" за КЕП с идентификатор на политика OID = 1.3.6.1.4.1.15862.1.5.1.1.

10.4 Профил на удостоверението

1. Доставчикът издава персонално удостоверение за КЕП с посочения по-долу профил:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha1RSA / Sha256RSA
Signature hash algorithm	-	Sha1 / Sha256
Issuer	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784

	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN =	[Пълно име на Автора]
	E =	[Имейл адрес]
	OU =	EGN/PID: [ЕГН/ЛНЧ на Автора] (ако има такова)
	OU =	Personal certificate – UES
	S =	[[Адрес на Автора], PK:[пощенски код],]* EGN/PID:[ЕГН/ПИД на Автора] (ако има такъв)
	C=	BG
Subject Alternative Name*	CN =	FID: [номер на документ за самоличност на чуждестранно лице - Автор]
	C =	[код на държава на документ за самоличност на чуждестранно лице - Автор]
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[хеш на „Subject"]
Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1]*
Enhanced Key Usage	-	Client Authentication, Secure Email, IP security (end system, tunnel termination, end user, IKE)
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment, Data Encipherment, Key Agreement
Qualified Statement	QStatement:	StatementId = (1) statementInfo = 0.4.0.1862.1 StatementId =(4) StatementInfo=qcSSCD (0.4.0.1862.1.4)

* Маркираните със звездичка полета може да не присъстват в удостоверението

10.5 Оперативни процедури по издаване, подновяване и управление на

удостоверението

1. Оперативните процедури по издаване, подновяване и управление на персонално удостоверение за КЕП „B-Trust Personal Certificate QES" са описани в Глава 12 на документа.

11 ПОЛИТИКА НА ИЗДАВАНЕ, ПОДДРЪЖКА И УПРАВЛЕНИЕ НА ПРОФЕСИОНАЛНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

11.1 Обща характеристика на удостоверението

1. Професионалното удостоверение „B-Trust Professionall Certificate QES" се издава на Титуляр, респективно на физическо лице Автор, упълномощено като такова от Титуляря и удостоверява електронната идентичност на Титуляря и на Автора и връзката на Автор/Титуляр с публичния му ключ, за който се издава удостоверението.
2. „B-Trust Professional Certificate QES" има характер на удостоверение за КЕП по смисъла на чл. 16, ал.1 от ЗЕДЕП и всеки електронен подпис.
3. За издаването на удостоверение „B-Trust Professional Certificate QES" се изисква личното присъствие при проверка на идентичността, респективно самоличността на Автора/Титуляр пред Регистриращия орган/МРС на Доставчика.
4. Процедурата по идентификация включва представяне на доказателство за самоличността на Автора и идентичността на Титуляря.
5. Проверката на искането за издаване на професионално удостоверение по реда на точки 3 и 4 осигурява високо ниво на сигурност по отношение на идентичността на Автора/Титуляря и връзката му с публичния ключ.
6. Авторът/Титулярят може сам да генерира двойката ключове, като използва B-Trust SSCD и съответен софтуер за него или друго еквивалентно SSCD, което е съвместимо в инфраструктурата на Доставчика.
7. Частният ключ за създаване на КЕП задължително се генерира в SSCD и не може да бъде изведен навън от него.
8. Издаденото професионално удостоверение за КЕП, удостоверяващо публичен ключ съответстващ на частния такъв, задължително се записва в SSCD, което се предоставя на Автора/Титуляря.
9. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към професионалното удостоверение за КЕП.

11.2 Предназначение и приложимост на удостоверението

1. Професионалното удостоверение може да се използва при създаване/полагане на КЕП на физическото лице, посочено като Автор в удостоверението и упълномощено да подписва от името на Титуляря електронни документи и да работи с приложения, които изискват високо ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в удостоверението за КЕП обозначената политиката, приложима към това удостоверение (атрибут "Certificate Policy") и предназначението и ограниченията на действието на удостоверението, описани в атрибутите "Key Usage" и "Extended Key Usage", преди да се довери на положения електронен подпис.

11.3 Обозначение на политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в професионалното удостоверение „B-Trust Professionall Certificate QES" за КЕП с идентификатор на политика OID = 1.3.6.1.4.1.15862.1.5.1.1.

11.4 Профил на удостоверението

1. Доставчикът издава професионално удостоверение за КЕП с посочения по-долу профил:

Поле	Атрибути	Meaning/Value
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha1RSA / Sha256RSA
Signature hash algorithm	-	Sha1 / Sha256
Issuer	Phone =	+359 2 9 215 100

	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	Bul. Tsarigradsko shoes No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN =	[Пълно има на Автора]
	O =	[Наименование/пълно име на Титуляря]
	OU =	BULSTAT: [ЕИК(БУЛСТАТ) на Титуляря] (ако има такъв)
	OU* =	EGN/PID: [ЕГН/ЛНЧ на Титуляря] (ако има такъв)
	S =	[[Служебен адрес на Автора при Титуляря], PK:[пощенски код],]* EGN/PID:[ЕГН/ПИД на Автора] (ако има такъв)
	OU =	Professional certificate – UES
	E =	[Имейл адрес]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Alternative Name*	CN* =	FID: [номер на документ за самоличност на чуждестранно лице - Автор]
	C* =	[код на държава на документ за самоличност на чуждестранно лице - Автор]
	OU* =	C:[код на държава на регистрация на чуждестранно лице - Титуляр]
	OU* =	SR:[номер на съдебна регистрация на чуждестранно лице - Титуляр]
Subject Key Identifier	-	[хеш на „Subject"]
Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [[2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1]*
Enhanced Key Usage	-	Client Authentication, Secure Email, IP security (end system, tunnel termination, end user, IKE)
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment, Data Encipherment, Key Agreement
Qualified Statement	QStatement:	statementId = (1) statementInfo = 0.4.0.1862.1 StatementId =(4)

		StatementInfo=qcSSCD (0.4.0.1862.1.4)

* Маркираните със звездичка полета може да не присъстват в удостоверението

11.5 Оперативни процедури по издаване, подновяване и поддържане на удостоверението

1. Оперативните процедури по издаване, подновяване и управление на професионално удостоверение за КЕП „B-Trust Professional Certificate QES" са описани в Глава 12 на документа.

12 ОПЕРАТИВНИ ПРОЦЕДУРИ ЗА ИЗДАВАНЕ, ПОДНОВЯВАНЕ И ПОДДРЪЖКА/УПРАВЛЕНИЕ НА УДОСТОВЕРЕНИЯТА ЗА КЕП

1. Оперативните процедури на Доставчика за издаване, подновяване и поддръжка/управление на персонално и на професионално удостоверение за КЕП са общи за трите типа удостоверения.

12.1 Регистрация на искане за издаване на удостоверението

1. Заявителят на удостоверение за КЕП прави искане пред Регистриращия орган/МРС на Доставчика чрез оператор на МРС по място за издаване на удостоверението.
2. Искането за издаване включва изискуемата информация по чл. 24 на ЗЕДЕП, индивидуализираща Автора/Титуляря и типа на удостоверението, което се заявява. Искането може да включва и допълнителна, непроверяема информация, част от която се удостоверява, а друга част се изисква за да улесни контакта на Доставчика с Автора/Титуляря.
3. Процесът на заявяване предоставя на заявителя (Автор/Титуляр или упълномощено от него лице) или на оператора на Регистриращия орган/МРС да генерира двойката криптографски (RSA) ключове и да включи публичния ключ в информацията за издаване на удостоверението.
4. Двойката криптографски ключове задължително се генерира в B-Trust SSCD или друго еквивалентно на него SSCD, отговарящо на изискванията за ниво на сигурност EAL 4 или по-високо, съгласно CC или друга спецификация, определяща еквивалентни нива на сигурността.
5. Електронният формат на заявката за издаване на удостоверение с информацията, която ще се включи в удостоверението е структура, подписана с частния ключ от генерираната двойка ключове в SSCD.
6. Когато заявителят не притежава B-Trust SSCD, процесът на заявяване на удостоверение изисква само информацията, идентифицираща Автора/Титуляря, типа на удостоверението (персонално или професионално), както и друга допълнителна такава, без да включва генериране на криптографската двойка ключове (RSA) за удостоверението. Генерацията на двойката ключове като стъпка от искането за издаване на удостоверението се изпълнява от оператор в МРС.
7. След успешна регистрация на искане за издаване на удостоверение, операторът в МРС трябва да установи идентичността на заявителя.

12.2 Идентификация и приемане/отхвърляне на искането

1. Заявителят следва да се запознае със списъка изисквани документи, необходими за издаване на избраното от него удостоверение за КЕП, в това число и с предлагания типов Договор за удостоверителни услуги.
2. Заявителят надлежно подготвя изискуемите документи от списъка.
3. Заявителят следва лично да се яви в избрана и удобна за него МРС на Доставчика и да представи подготвените документи.
4. Операторът в Регистриращия орган/МРС изпълнява процедурата по идентификация и автентификация на заявителя за издаване на удостоверение - Автор/Титуляр или упълномощено от него физическо лице.
5. В съответствие с Наръчника - Част I (ПРАКТИКА) и утвърдени вътрешни процедури на Доставчика, на база постъпило и регистрирано искане за издаване на удостоверение за КЕП и представени документи, в личното присъствие на заявителя - Автор/Титуляр или упълномощено от него лице, Регистриращият орган/МРС потвърждава пред Доставчика:
    - идентичността на Титуляря, респективно самоличността на Автора;
    - представителната власт на Автора спрямо Титуляря и на упълномощеното лице на Титуляря;
    - държането на частния ключ, съответстващ на публичния ключ, представен в процеса;
    - на искането за издаване на удостоверението;
    - допълнителна информация, заявена за включване в удостоверението, без непотвърдената такава;
    - приема Договор за удостоверителни услуги и условията в настоящия Наръчник.
6. Регистриращият орган/МРС на Доставчика незабавно, в присъствието на заявителя - Автор/Титуляр или упълномощено от него лице, след успешна проверка по идентификация и съгласие с информацията, която се включва в удостоверението, утвърждава представената информация, чрез направеното искане за издаване на удостоверение.
7. Въз основа на утвърденото искане за издаване, Удостоверяващият орган на Доставчика издава заявения тип удостоверение.
8. При отхвърлено искане за издаване на удостоверение, заявителят се уведомява с посочване на причините за

отказа на искането.

12.3 Издаване и публикуване на удостоверението

1. Удостоверяващият орган на Доставчика електронно идентифицира Регистриращия орган/МРС, който е утвърдил електронната заявка от искането за издаване на удостоверение за КЕП.
2. Удостоверяващият орган генерира заявеното удостоверение, подписва го с електронния подпис на Доставчика и го публикува в Публичния си регистър.
3. Службата за известяване на Доставчика изпраща до Автора/Титуляря известие за името на Автора/Титуляря, вида на удостоверението за КЕП, уникалния сериен номер и срока на валидност на издаденото удостоверение.

12.4 Приемане на удостоверението

1. Приемането на съдържанието на удостоверение е акт, който се изпълнява преди издаването и публикуването му от Доставчика чрез оперативния Удостоверяващ орган.
2. Доставчикът, чрез оперативния Удостоверяващ орган публикува издаденото удостоверение в Публичния регистър на издадените удостоверения.
3. След публикуване на удостоверението Авторът/Титулярят е длъжен в срок до 3 (три) дни от публикуването да прегледа отново съдържанието на удостоверението и при необходимост да направи възражения пред Доставчика или Регистриращия орган/МРС относно верността и пълнотата на съдържанието му.
4. При направени възражения по реда на предходната точка, Доставчикът незабавно прекратява това удостоверение и предприема последващи действия за повторно издаване на удостоверението с коректни и пълни данни.

12.5 Предоставяне на удостоверението

1. След успешно издаване на удостоверението, оператор в Регистриращия орган/МРС на Доставчика може незабавно да го запише върху B-Trust SSCD, което предоставя на Автора/Титуляря (или упълномощеното от него лице). Ако двойката ключове е генерирана в SSCD при заявителя, го уведомява чрез електронния пощенски адрес, съдържащ се в неговото удостоверение като посочва Интернет-страницата, от където той може да зареди издаденото удостоверение.
2. Срещу представяне на документ за самоличност, Авторът/Титулярят (или упълномощеното лице) получава комплекта за КЕП, издаден на B-Trust SSCD.

12.6 Подновяване на удостоверението

1. Подновяване на удостоверението за КЕП се изпълнява от Доставчика в съответствие с общата оперативна процедура за Подновяване на удостоверение, представена в Наръчника - Част I (ПРАКТИКА).

12.7 Спиране/възобновяване на удостоверението

1. Спиране/възобновяване на удостоверението за КЕП се изпълнява от Доставчика в съответствие с общите оперативни процедури за Спиране/Възобновяване на удостоверение, представени в Наръчника - Част I (ПРАКТИКА).

12.8 Прекратяване на удостоверението

1. Прекратяване на удостоверението за КЕП се изпълнява от Доставчика в съответствие с общата оперативна процедура за Прекратяване на удостоверение, представена в Наръчника - Част I(ПРАКТИКА).