Гриф С1 (За общо ползване)

ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС
и
ПРАКТИКА ПРИ ПРЕДОСТАВЯНИТЕ ОТ „БОРИКА“ АД КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

Версия 3.2

1 Юли 2017 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
3.2	Димитър Николов	13.01.2017	Утвърден	Изменения на документа, свързани с прилагане на Регламент 910/2014.

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК

АД	Акционерно дружество
ДВ	Държавен вестник
ДКУУ	Доставчик на квалифицирани удостоверителни услуги
ЕГН	Единен граждански номер
ЕП	Електронен подпис
ЗД	Закон за далекосъобщенията
ЗЕДЕП	Закон за електронния документ и електронния подпис
КЕП	Квалифициран Електронен Подпис
КУ	Квалифицирано удостоверение
КУУ	Квалифицирани удостоверителни услуги
КУКЕП	Квалифицирано удостоверение за Квалифициран Електронен Подпис
КРС	Комисия за регулиране на съобщенията
МТС	Министерство на транспорта и съобщенията
МРС	Местна регистрираща служба
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
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на квалифицирани удостоверителни услуги
Политика	Политика за предоставяне на квалифицирани удостоверителни услуги
Регламент	Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно Електронната идентификация и Удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на директива 1999/93/ЕО
РО	Регистриращ орган
УО	Удостоверяващ орган

СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК

BG	Bulgaria – България
CA	Certification Authority – Удостоверяващ орган (УО)
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 удостоверения
DSA	Digital Signature Algorithm – Вид криптографски алгоритъм за създаване на подпис
DN	Distinguished Name – Уникално име
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
HSM	Hardware Security Module – специализирана хардуерна криптосистема за съхранение и работа с криптографски ключове
IEC	International Electrotechnical Commission - Международна електротехническа комисия
ISO	International Standardization Organization - Международна организация за стандартизация
IP	Internet Protocol – Интернет протокол
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за он-лайн проверка на статуса на удостоверения
PKCS	Public Key Cryptography Standards – Криптографски стандарт за публичен ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
QES	Qualified Electronic Signature – Квалифициран електронен подпис
RA	Registration Authority – Регистриращ орган
RSA	Rivest – Shamir - Adelman – Криптографски алгоритъм за създаване на подпис
QSCD	Qualified Signature Creation Device – Квалифицирано устройство за сигурно създаване на подписа
B-Trust QSCD	QSCDсъс 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 – Унифициран локатор на ресурс
QCP-n-qscd	certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD

СЪОТВЕТСТВИЕ И УПОТРЕБА

Този Документ:

- е разработен от „БОРИКА" АД, юридическото лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 201230426;
- подменя изцяло всички досегашни редакции на “Наръчник на Потребителя“ и/или „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА“ АД квалифицирани удостоверителни услуги“;
- влиза в сила на 01.07.2017г. ;
- съдържа условията, съгласно които Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД (Доставчик) предоставя на Потребители срещу възнаграждение квалифицирани удостоверения (КУ) и свързаните с тях квалифицирани удостоверителни услуги (КУУ), както и други 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 настоящия документ;
- включва подробно описание на практиката и политиките при предоставяне на КУУ на Доставчика и е публичен документ с цел установяване на съответствие на дейността на Доставчика със ЗЕДЕП и нормативната уредба;
- общодостъпен е по всяко време на интернет-страницата на Доставчика;
- може да бъде променян от ДКУУ и всяка нова редакция на „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА“ АД квалифицирани удостоверителни услуги“ се публикува на интернет-страницата на Доставчика;
- включва две части:
  - **ЧАСТ I:** Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги (Qualified Certification Practice Statement, QCPS);
  - **ЧАСТ II:** Политика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги (Qualified Certificate Policy, QCP);

Настоящият документ е изготвен в съответствие с:

- Закон 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);
- Регламент (ЕС) № 910/2014 на европейския парламент и на съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

Съдържанието и структурата на документа е в съответствие с Регламент (ЕС) № 910/2014 и се позовава на информация, съдържаща се в следните утвърдени международни препоръки, спецификации и стандарти:

- RFC 5280: 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 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411: Policy and security requirements for Trust Service Providers issuing certificates
- ETSI EN 319 412: Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

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

бул. „Цар Борис III" № 41
София 1612
„БОРИКА“ АД
телефон: 02/ 92 15 115
имейл адрес: info@b-trust.org
Официална страница на доставчика: www.b-trust.org

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

Практиката при предоставяне на КУКЕП и КУУ:

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

Наименование	Идентификатор (OID)
B-Trust Certification Practice Statement(CPS) for Qualified Certificates (Практика за предоставяне на КУКЕП)	O.I.D. = 1.3.6.1.4.1.15862.1.6

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

Алгоритъм	Наименование
Хеш-алгоритми:	SHA256
Асиметрични алгоритми:	RSA

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

Политиката на предоставяне на КУКЕП и КУУ:

- описва условията, които Доставчикът спазва и следва при издаване на КУКЕП , 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 КУКЕП, от изискванията при идентификация, условията и изискванията за ниво на сигурност при създаване на електронния подпис, както и съответното съхраняване на частния ключ;
- определя приложимостта и степента на доверие в удостоверените факти в тези КУКЕП.

1. Доставчикът прилага Политики за типовете КУКЕП, която се означава със следните идентификатори:

Политика на Доставчика	Идентификатор (OID)
B-Trust Personal Qualified Certificate Policy (QCP-n-qscd) (Политика за предоставяне на КУКЕП на физическо лице)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 (O.I.D. = 0.4.0.194112.1.2)
B-Trust Professional Qualified Certificate Policy (QCP-n-qscd) (Политика за предоставяне на КУКЕП на физическо лице, асоциирано с юридическо лице)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 (O.I.D. = 0.4.0.194112.1.2)

Съгласно тази Политика Доставчикът издава и поддържа следните типове КУКЕП:

- Персонално КУКЕП на физическо лице „B-Trust Personal qualified certificate QES";
- Професионално КУКЕП на физическо лице, асоциирано с юридическо лице „B-Trust Professional qualified certificate QES".

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

ЧАСТ I:

ПРАКТИКА

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

ВЪВЕДЕНИЕ

Практиката при предоставяне на КУУ е съставна част на този документ, разработен от ДКУУ „БОРИКА“ 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 КУКЕП. Описани са общите оперативни процедури при заявяване на КУКЕП, идентифициране на Заявители, издаване и публикуване, доставяне и приемане на КУКЕП, поддръжка и управление на тези удостоверения, както и процедури при предоставяне достъп за проверка на удостоверенията.

Практиката включва още мерките и следваните технически процедури от страна на Доставчика, които гарантират сигурността и надеждността на предоставяните КУУ 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 квалифицирани удостоверителни услуги

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

1.2 Регулация и контрол

1. „БОРИКА“ АД е уведомило КРС за започване на дейност като ДКУУ по реда на ЗЕДЕП и действащата нормативна уредба.
2. Акредитацията на „БОРИКА“ АД като ДКУУ по ЗЕДЕП цели най-високо ниво на сигурност на предоставяните КУУ 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 КУКЕП и на КУУ за тях.

1.3 Идентификатори в документа

1. Практиката на Доставчика при издаване и поддържане на КУ се осъществява посредством оперативен УО:

Оперативни УО	Идентификатор (OID)
B-Trust Operational Qualified CA (УО за КУКЕП)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1

2. Политиката на Доставчика относно КУКЕП и предоставяните за тях КУУ се означава в издаваните КУ със следните идентификатори:

Квалифицираното Удостоверение	Наименование	Вписани Политики (OID)
Персонално КУКЕП на физическо лице	B-Trust Personal qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2
Професионално КУКЕП на физическо лице, асоциирано с юридическо лице	B-Trust Professional qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2

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

Квалифицирано Удостоверение	Наименование	Политика
Персонално КУКЕП на физическо лице	B-Trust Personal qualified certificate QES	B-Trust Personal Qualified Certificate Policy
Професионално КУКЕП на физическо лице, асоциирано с юридическо лице	B-Trust Professional qualified certificate QES	B-Trust Professional Qualified Certificate Policy

1.4 Участници в инфраструктурата на B-Trust®

1.4.1 Удостоверяващ орган

1. „Удостоверяващия орган“ на B-Trust® на ДКУУ „БОРИКА“ АД е организационно обособено звено, което осъществява дейността му по издаване на КУКЕП, по предоставяне и по поддържане на КУУ за тях. УО нямат 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 УО за издаване и поддръжка на КУКЕП, както следва:
   - Базов УО ***„B-Trust Root Qualified CA"*** - издава удостоверения на подчинените в йерархично отношение оперативни УО на Доставчика и такива на други Доставчици;
   - Оперативен УО ***„B-Trust Operational Qualified CA"*** - издава КУКЕП, съгласно Политиката за предоставяне на КУУ;
3. ДКУУ си запазва правото да разшири инфраструктурата на B-Trust® с друга йерархия от УО.

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 КУКЕП;
   - регистрира подадени искания до УО за издаване и внася промени в статуса на КУКЕП;
   - осъществява съответни проверки за установяване на самоличността на физическите лица и идентичността на юридическите лица, както и на специфични данни за тях с допустимите средства и в съответствие с Политиката и Практиката при предоставяне на съответната КУУ;

- уведомява УО да издаде КУКЕП след успешна идентификация и заплатена услуга;
- предава на Титуляря издаденото КУКЕП , съответстващо на генерирана двойка ключове;
- приема или отхвърля регистрирани искания за поддръжка и управление на КУКЕП в съответствие с утвърдената Практика и Политика;
- сключва договори за предоставяне на удостоверителни и други криптографски, информационни и консултантски услуги със 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 (РО) на Доставчика може да предоставя удостоверителни услуги на Потребители чрез Местни Регистриращи Служби (МРС).
4. Когато РО/МРС е самостоятелно юридическо лице, правомощието да осъществява тази дейност може да бъде ограничено за определена територия, срок, удостоверителни услуги или за определена категория Титуляри. Правомощието се удостоверява пред Заявителите и всички трети лица с писмено или електронно удостоверение за РО/МРС.
5. В случаите, когато РО е самостоятелно юридическо лице, МРС към този орган се разкриват само след изрично одобрение от страна на Доставчика.
6. Отношенията между Доставчика и РО/МРС по т.4 се уреждат с договор.
7. Доставчикът гарантира, че дейността на РО/МРС ще бъде съобразена с условията на настоящия Документ.

1.4.3 Орган за издаване на квалифицирани електронни времеви печати

1. „Орган за издаване на квалифицирани електронни времеви печати" е обособено и неделимо звено към Удостоверяващия орган, което осъществява дейности на Доставчика, както следва:
   - приема заявки за издаване на квалифицирани електронни времеви печати на представено съдържание на електронен документ от Титуляря или Доверяваща се страна;
   - изготвя квалифициран електронен времеви печат на представения хеш-стойност на електронен документ;
   - осигурява възможност за последващо (след периода на валидност на КУКЕП) доказване спрямо приемащата страна на факта на подписването на изявление или на електронен документ.
2. „B-Trust Qualified Time Stamp Authority " е Органът за за издаване на квалифицирани електронни времеви печати на Доставчика.
3. Електронният подпис на удостоверението за време е със статус на квалифициран електронен печат на Доставчика.
4. Квалифицирани електронни времеви печати 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.
5. Доставчикът разработва и публикува отделна Политика на Органа за за издаване на квалифицирани електронни времеви печати.

1.4.4 OCSP сървър

1. „OCSP сървър" е обособено и неделимо звено на УО, което осъществява дейности на Доставчика както следва:
   - приема заявки от Титуляря 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. OCSP сървърите на Доставчика са: „B-Trust Root Qualified OCSP Authority" и „B-Trust Qualified OCSP Authority".

3. Всяка доверяващата се страна, когато приема КУКЕП, може да заяви проверка на статуса на удостоверенията в реално време.
4. Проверката на статуса на КУКЕП 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 електронно подписани документи, при проверка и приемане на електронни транзакции и други.

1.4.5 Титуляр

1. „Титуляр" на КУКЕП е физическо лице, което създава електронния подпис.
2. Титулярят осъществява от свое име или от името на друго лице, което той представлява, електронни изявления, които електронно подписва в съответствие с предоставената му представителна власт.
3. В КУКЕП може да се посочи и лицето, което Титулярят представлява.
4. Единствено Титулярят на КУКЕП , има право на достъп до частния ключ за подписване на електронни изявления (създаване на квалифициран електронен подпис).

1.4.6 Доверяващи се страни

1. „Доверяващи се страни" са адресатите на подписани електронни изявления, Титулярите на които притежават издадени от Доставчика КУКЕП.
2. Доверяващите се страни следва да имат познания и умения относно използването на КУКЕП и се доверяват на удостоверените обстоятелства в тях само с оглед на приложимата Политика, особено по отношение на нивото на сигурност при проверка на Титулярите на тези КУКЕП.
3. Доверяващите се страни имат постоянен достъп до регистрите на Доставчика за проверка на валидността на КУКЕП, за установяване на 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. "Квалифицирано удостоверение за публичен ключ" е подпечатан от Доставчика електронен документ, съдържащ определени реквизити, удостоверяващи връзката между Титуляря и публичния му ключ, съответстващ на частния ключ, с който Титуляря е създал електронния подпис и служи за проверка на подписа в електронни документи и обекти.
2. КУКЕП могат да се използват за дейности, които изискват подписване на електронни документи, осъществяване на електронни транзакции и автентификация.
3. Само удостоверенията с означените в този документ политики, които издава Доставчикът, имат характер на КУ 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 електронно самоподпечатано с базовия частен ключ на Доставчика КУ за неговия базов публичен ключ. С базовия частен ключ Доставчикът електронно подпечатва удостоверения за публични ключове на свои оперативни УО, както и удостоверения на други (под)доставчици на удостоверителни услуги в инфраструктурата на B-Trust.
2. В съответствие със ЗЕДЕП и йерархията от УО в инфраструктурата на B-Trust, Доставчикът предоставя на КРС валидното удостоверение на базовия УО. Основните реквизити на базовото удостоверение на УО „B-Trust Root Qualified 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 Qualified CA

	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-25T18:28:43Z
Validity to	-	2037-04-25T18:28:43Z
Subject	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path Length Constraint =	CA None
Certificate Policies	-	[1] Certificate Policy: Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.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 [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	c0 4d 7a 42 7f 5a 82 b1 2d a6 f0 94 88 11 66 8e 1a 67 0a f6
Thumbprint (Sha256)	-	d3 38 95 e1 d5 11 23 f9 48 c8 c9 99 f7 f7 26 40 fa 05 05 fb d1 5a b0 93 e8 98 db 27 dd 29 14 e8

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

Оперативни удостоверения за издаване на КУКЕП

1. Удостоверение на оперативен УО на Доставчика за издаване на КУКЕП е квалифицираното удостоверение за публичния ключ на оперативния УО „B-Trust Operational Qualified CA", електронно подпечатано с базовия частен ключ на Доставчика. С частният ключ, съответстващ на този публичен ключ, оперативния УО електронно подпечатва издаваните от Доставчика КУКЕП на Титулярите. Основните реквизити на оперативното удостоверение на УО „B-Trust Operational Qualified CA" на Доставчика са:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	02
Signature algorithm	-	Sha256RSA
Signature hash	-	Sha256

algorithm		
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-25T18:36:00Z
Validity to	-	2032-04-24T18:36:00Z
Subject	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path length Constraint =	CA 0
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.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 [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	51 96 52 17 9e 78 be e2 2e a8 13 14 72 7a 8f 60 67 17 2f 32
Thumbprint (Sha256)	-	64 fc 3f 77 db b8 3d a2 79 2a e4 cb 2c d0 ef 3d bb e7 92 7e 9b 80 74 54 de 14 f7 69 77 8d 34 8d

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

Удостоверения на OCSP сървър

1. Удостоверението на OCSP сървъра на Доставчика „B-Trust Root Qualified OCSP Authority" е КУ за публичния ключ на „B-Trust Root Qualified OCSP Authority", подпечатано с базовия частен ключ на УО „B-Trust Root Qualified CA“ на Доставчика. С частния ключ на двойката ключове на OCSP сървъра „B-Trust Root Qualified OCSP Authority" Доставчикът подпечатва резултата/отговора от проверката в реално време на статуса на представени КУКЕП, издадени от базовото удостоверение на УО „B-Trust Root Qualified CA". Реквизитите на служебното удостоверение на Органа „B-Trust Root Qualified OCSP Authority" на Доставчика са:

Поле	Атрибути	Значение/Стойност

Version	-	V3
Serial number	-	03
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:27:48Z
Validity to	-	2022-04-26T14:27:48Z
Subject	CN =	B-Trust Root Qualified OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	34 31 84 22 65 34 41 46 e0 0d 03 2a 9f a1 0a 29 4a 93 7b 5c
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.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 [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		64 ed 90 7c af 37 a0 f2 62 39 3a ce 7e 90 e1 a7 bd 45 af a1
Thumbprint (Sha256)		91 18 ce 2d 4b c0 dc d2 c0 b4 32 fc cb f7 04 4e 94 c0 53 e2 8e 92 93 21 88 5c d3 43 6b e2 69 d5

2. Удостоверението на OCSP сървъра на Доставчика „B-Trust Qualified OCSP Authority" е КУ за публичния ключ на „B-Trust Qualified OCSP Authority", подпечатано с частния ключ на оперативния УО “B-Trust Operational Qualified CA" на Доставчика. С частния ключ на двойката ключове на OCSP сървъра „B-Trust Qualified OCSP Authority" Доставчикът подпечатва резултата/отговора от проверката в реално време на статуса на представени КУКЕП, издадени от оперативния УО „B-Trust Operational Qualified CA". Реквизитите на служебното удостоверение на Органа „B-Trust Qualified OCSP Authority" на Доставчика са:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	23 C3 46 00
Signature algorithm	-	Sha256RSA

Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T15:26:25Z
Validity to	-	2022-04-26T14:35:30Z
Subject	CN =	B-Trust Qualified OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	be e5 83 42 fa 25 a5 58 4a 39 a5 0f 42 ea ef f4 42 05 95 2e
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.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 [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		53 a1 58 0e db 15 6c c0 1f f6 f4 a1 99 43 8d 5d 59 42 63 90
Thumbprint (Sha256)		c7 5f 3b 30 0c 54 62 ba 78 80 e9 ea 4b e3 96 35 e3 50 df 1a 92 e8 f4 53 5b 07 4a 6d 4a 02 d8 81

3. Електронните печати на Доставчика, които са придружени от служебните удостоверения на „B-Trust Root Qualified OCSP Authority“ и „B-Trust Qualified OCSP Authority“ са КУ за електронен печат.

1.5.3 Удостоверения на други оперативни органи

1. Доставчикът може да издава оперативни КУ на други УО 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 ДКУУ съгласно ЗЕДЕП .
2. Издаването на тези удостоверения се осъществява на базата на конкретна договореност със съответните доставчици.

1.5.4 Квалифицирани удостоверения за Потребители

1.5.4.1 Квалифицирани удостоверения за квалифициран електронен подпис (КУКЕП)

1. Доставчикът издава на Потребители КУКЕП в зависимост от Заявителите, приложното поле и предназначение на електронния подпис:
   - персонално КУКЕП „B-Trust Personal Qualified Certificate QES";
   - професионално КУКЕП „B-Trust Professional Qualified Certificate QES".
2. Практиката и Политиката на Доставчика, съгласно този документ, определят правилата и изискванията за сигурност, приложими при издаване и използване на КУКЕП.
3. Доставчикът издава КУКЕП само на физически лица.
4. Персонално КУКЕП „B-Trust Personal Qualified Certificate QES" се издава персонално на физическо лице - Титуляр.
5. Професионално КУКЕП „B-Trust Professional Qualified Certificate QES" се издава на физическо лице - Титуляр, представляващо друго юридическо лице по силата на закона или упълномощаване.
6. Искането за регистрация и издаване на тези КУКЕП се прави отдалечено (по електронен способ) или локално (на място) в РО/МРС, като процедурата по идентификация чрез установяване на самоличността на Титуляря изисква лично присъствие или изрично упълномощаване от страна на Титуляря. Проверява се и идентичността на представляваното лице, респективно на физическо лице упълномощено от Титуляря (ако има такива). Идентификационната процедура и процедурите при генериране на двойката ключове, при издаване и предоставяне на КУКЕП на Титуляря гарантират най-високо ниво на сигурност на данните за Титуляря в удостоверението и връзката им с публичния ключ.
7. КУКЕП „B-Trust Personal Qualified Certificate QES" и „B-Trust Professional Qualified Certificate QES" и съответстващите им частни ключове се съхраняват и предоставят на Титуляря задължително на QSCD.
8. КУКЕП имат значението на саморъчен подпис спрямо всички по смисъла на чл.13, ал.4 на ЗЕДЕП .

1.5.5 Предназначение на квалифицираните удостоверения за Потребители

1. Издадените КУКЕП за Потребители от УО на Доставчика може да се използват по предназначение съобразно Политиката за това удостоверение.
2. Всяко КУКЕП за Потребители съдържа като реквизит поле за предназначение на удостоверението. Реквизитът се идентифицира като "Key Usage" в съответствие с RFC 5280 и може да се използват с едно или едновременно с няколко от следните предназначения:
   - цифрово подписване (digitalSignature) - да осигури възможност за цифрово подписване на електронно изявление или на съдържание и неговата проверка;
   - неотменимост (nonRepudiation) - да осигури възможност за последващо доказване спрямо Титуляря на факта на подписване на електронно изявление или на съдържание и на невъзможност за отказ от положения електронен подпис;
   - криптиране на ключове (keyEncipherment) - да криптира и/или декриптира ключове, използвани при шифроване на данни;

3. Чрез реквизит „Extended Key Usage" в съответствие с RFC 5280, който също може да се съдържа в издаваните от Доставчика КУКЕП, се детайлизира приложимостта на удостоверението с оглед предназначението му.
4. Приложното поле на издаваните типове КУ е както следва:

Тип на удостоверение	Приложимост
Персонално КУКЕП на физическо лице „B-Trust Personal Qualified 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 КУКЕП на физическо лице „B-Trust Professional Qualified 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.

1.5.5.1 Ограничение на удостоверителното действие

1. Ако КУКЕП 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 по отношение на цели и/или стойност на сделки между Титулярите при използване на подписа.
2. Доставчикът задължително използва реквизит "Qualified Statements" в КУКЕП.
3. Ограничителното действие на издадени КУКЕП 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 документ.

1.5.5.2 Употреба на удостоверения извън приложното поле и ограниченията

1. Когато Титуляр или Доверяваща се страна използват и се доверяват на КУКЕП 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“ 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@borica.bg;
   - тел.: (02) 9215 115 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 КУКЕП на Потребители и актуален Списък на прекратените КУКЕП (CRL), както и на 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. Титуляр на издадено от Доставчика КУКЕП 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 КУКЕП . 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 КУКЕП до момента на публикуването му в регистъра. Спряно удостоверение се поддържа в CRL за период от време, регламентиран от ЗЕДЕП и предвиден в настоящия документ. Ако удостоверението бъде възобновено или изтече регламентирания период от време на спиране, 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 Политиката и Практиката;
   - Практиката при предоставяне на КУУ;
   - Политиката при предоставяне на КУУ;
   - Договор за КУУ;
   - Тарифа на предоставяните КУУ;
   - Правила за издаване на КУКЕП;
   - Условия и ред за използване на КУКЕП, включително изискванията за съхраняване на частния ключ;
   - Документи, изискуеми при първоначално издаване на КУКЕП, при подновяване и спиране/прекратяване на КУКЕП;
   - 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 издаването му от оперативен УО „B-Trust Operational Qualified CA".
2. Доставчикът незабавно публикува актуален CRL, подписан от оперативен УО след прекратяване/спиране на всяко валидно удостоверение. 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 ДКУУ указва времето за следващото издание на CRL.
3. Публикуване на нова редакция или версия на Политиката и Практиката, 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, 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 Политиката и Практиката и на съдържащите се в тях условия. 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 РО/МРС:
   - приема искания за издаване на КУКЕП;
   - осъществява проверка за установяване на самоличността на Титуляря и на специфични данни за него с допустими средства;
   - утвърждава след успешна проверка или отхвърля регистрираните искания;
   - уведомява УО да издаде исканото удостоверение.
2. РО/МРС събира и получава необходимата информация за идентификация и автентификация на Титуляря.
3. Автентификацията/идентификацията на Титуляря след регистрация и преди да бъде издадено КУКЕП, изисква негово лично присъствие или присъствие на упълномощен представител на Заявителя в РО/МРС.
4. Доставчикът гарантира, че физическите и юридическите лица са правилно идентифицирани, автентифицирани и че заявките за издаване на КУКЕП са напълно, внимателно 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. КУКЕП са с формат, съответстващ на стандарта X.509. РО/МРС, работещ от името на Доставчика утвърждават, че имената в заявките за удостоверения съблюдават стандарта X.509.
2. Полето „Subject" в удостоверението електронно идентифицира Титуляря, свързан с публичния ключ в КУКЕП.
3. Името и други индивидуализиращи белези на 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 КУКЕП се съдържа в съответните глави на настоящия документ.

3.1.2 Използване на псевдоним

1. Доставчикът може да издава КУКЕП като използва „псевдоним", за да именува Титуляря само след като РО/МРС събере необходимата информация за самоличността му и успешно го идентифицира.

3.1.3 Значимост на имената при вписване

1. Удостоверенията на УО на Доставчика съдържат уникални имена с общоразбираема семантика, позволяваща определянето на идентичността на Доставчика, субект на удостоверението.
2. КУКЕП на Потребители съдържат имена, съвпадащи с автентифицираните идентификационни имена на Титуляря, субекти на издадените удостоверения.
3. За по-удобна електронна комуникация с Титуляря, Доставчикът изисква и удостоверява в КУКЕП имейл адрес на Титуляря. 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 КУКЕП на Потребители информация за електронна идентификация на Титуляря, която е успешно проверена и потвърдена от РО/МРС, въз основа на представените документи за самоличност на Титуляря.
2. Във всички удостоверения, в които се вписва Титуляря, полето за обичайно име (Common

Name, CN) съдържа име на физическото лице, с което то е обичайно обозначавано в дейността му.
3. В професионалното удостоверение, атрибутът за уникално име (DN) съдържа информация и за идентичността на лицето, което Титуляря представлява.

3.1.5 Уникалност на имената

1. Електронната идентификация на Титуляря на издадено от Доставчика КУКЕП е на базата на DN.
2. Полето "Subject" в удостоверението се формира от информацията за 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 РО/МРС на базата на представените документи.
3. Доставчикът гарантира уникалност на „DN" на Титуляря в домейна B-Trust чрез добавяне на реквизит, който гарантира такава уникалност.
4. Титуляря с уникален DN в домейна B-Trust може да има повече от едно издадени действителни КУКЕП.
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. Титуляря няма право да заявява 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 РО/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 самоличността на Титуляря на КУКЕП, Доставчикът изисква да бъде регистрирано искане за първоначално издаване на удостоверението.
2. Искането за първоначално издаване на КУКЕП пред РО/МРС на Доставчика е процедура, чрез която Доставчикът изисква, събира и получава необходима информация за идентификация на Титуляря на удостоверението.
3. Процедурата по регистрация включва:
   - попълване на регистрационна форма за издаване на КУКЕП;
   - генериране на двойка ключове;
   - подготвяне на електронна заявка, съдържаща публичния ключ, за който се издава удостоверението;
   - представяне на изискуемите документи в РО/МРС съгласно Политиката при издаване на КУКЕП;
   - възможност за заявяване на други услуги, свързани с издаваното удостоверение.
4. Установяване на самоличността на Титуляря след регистрация и преди издаване на заявеното КУКЕП изисква тяхно лично присъствие или на упълномощен представител в РО/МРС.
5. Първоначалната идентификация и потвърждаване на самоличността включва:
   - държането на частния ключ от Титуляря или изрично упълномощено от него лице, съответстващ на публичния ключ, представен на Доставчика за издаване на удостоверението;

- проверка и потвърждаване на самоличността на Титуляря на издаваното удостоверение.

6. След успешна проверка на самоличността на Титуляря, оторизираният оператор в РО/МРС:
   - предлага договор за КУУ 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 УО на Доставчика;
   - може да запише издаденото удостоверение на QSCD и да го предаде на Титуляря или на упълномощеното лице.

3.2.1 Доказване държането на частния ключ

1. РО/МРС извършва проверка за съответствие на представения публичен ключ, който се удостоверява в издаваното удостоверение от Доставчика с частния ключ на Титуляря.
2. Електронната заявка с публичния ключ, която се генерира за издаване на КУКЕП 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 РО/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 РО/МРС, проверява положения електронен подпис.
4. РО/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 КУКЕП, задължително се генерира в QSCD.
6. Контролът на достъпа до частния ключ се държи само от Титуляря.

3.2.2 Установяване на идентичност на юридическо лице или едноличен търговец

1. Установяване и проверката на идентичността на юридическото лице или едноличен търговец се осъществява от РО/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 за професионално КУКЕП „B-Trust Professional Qualified Certificate QES" изисква в РО/МРС да се яви упълномощен представител на лицето и да представи изискуемите документи, доказващи правния му статус.

3.2.3 Установяване самоличността на физическо лице

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

Наименование на удостоверението	Необходими документи
Персонално КУКЕП „B-Trust Personal Qualified Certificate QES"	Документи, доказващи самоличността на Титуляря - при лично явяване на Титуляря. Документи, доказващи самоличността на упълномощеното лице и пълномощно – при явяване на упълномощено лице
Професионално КУКЕП „B-Trust Professional Qualified Certificate QES"	Документи, доказващи самоличността на Титуляря, идентичността на юридическото лице и представителната власт на Титуляря спрямо юридическото лице.

3.2.4 Особени атрибути

1. Доставчикът може да включва в издаваното удостоверение особени атрибути, свързани с

Титуляря, ако удостоверението се издава за конкретна цел по съответната политика.
2. Тази информация подлежи на проверка от РО/МРС.

3.2.5 Непотвърдена информация

1. Непотвърдена информация е всяка информация, извън обхвата на проверяваната задължителна информация, която следва да бъде включена в удостоверението.
2. Доставчикът може да включва в издаваното удостоверение и непотвърдена информация за Титуляря, която не подлежи на проверка от РО/МРС.
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 КУКЕП, 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 КУКЕП, ако информацията 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 КУКЕП, 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 КУКЕП с нова двойка ключове (Re-key), само ако Титуляря заяви искане за това и декларира, че няма настъпили промени в удостоверената информация в текущото удостоверение. Подновеното удостоверение има различен публичен ключ, нов период на валидност и нов сериен номер, като удостоверената информация 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 Титуляря на удостоверение, което се подновява, не се изисква тяхното лично присъствие в РО/МРС на Доставчика.
7. При настъпили промени в информацията за Титуляря на КУКЕП, текущото удостоверение не се подновява. Доставчикът издава ново КУКЕП, като следва първоначална идентификация и установяване на самоличността му и прекратява незабавно текущото удостоверение.
8. Подновяване на удостоверение на УО на Доставчика „БОРИКА“ АД не се допуска. При всички обстоятелства, които налагат подмяна на удостоверението, винаги се издава ново удостоверение на УО.
9. Доставчикът съблюдава следните времеви ограничения и изисквания за идентификация при подновяване на КУКЕП:

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 QSCD 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 QSCD 3. Заявката за подновяване се подава на място (РО/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 РО/МРС, да спре действието на валидно удостоверение при постъпило искане за спиране, но не за повече от 24 часа.
2. Доставчикът, чрез РО/МРС, не извършва идентификация и автентификация на Заявителя и спира незабавно действието на удостоверение.
3. Доставчикът, чрез РО/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 РО/МРС, прекратява действието на валидно удостоверение при постъпило искане за прекратяване в съответствие с чл. 27 на ЗЕДЕП .
2. Доставчикът, чрез РО/МРС незабавно спира действието на удостоверението и извършва последваща идентификация и автентификация на Заявителя.
3. Доставчикът, чрез РО/МРС, следва да извърши идентификацията и автентификация на Заявителя в рамките на допустимия срок за спиране на действието на удостоверението, който е 24 часа.
4. Доставчикът, чрез РО/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. Титуляр на прекратено удостоверение може да заяви издаване на ново удостоверение.
3. Доставчикът, чрез РО/МРС изпълнява първоначална идентификация, установяване на идентичност на Титуляря, ако той заяви ново удостоверение.

4 ОПЕРАТИВНИ ИЗИСКВАНИЯ И ПРОЦЕДУРИ

1. Доставчикът, чрез РО/МРС, в рамките на сключен Договор за КУУ, предоставя следните операционни процедури за КУУ, приложими към КУКЕП:
   - регистрация на искане за издаване на КУКЕП;
   - обработка на искане за издаване;
   - издаване на КУКЕП;
   - предаване на издадено КУКЕП;
   - употреба на двойката ключове и на КУКЕП;
   - подновяване на КУКЕП чрез “Renew”;
   - подновяване на КУКЕП чрез “Re-key”;
   - спиране/възобновяване действие на КУКЕП;
   - прекратяване на КУКЕП;
   - статус на КУКЕП.
2. Доставчикът, чрез РО/МРС, допуска 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 РО/МРС на Доставчика.
2. Искане за издаване на удостоверение може да направи лично от Титуляр или упълномощено лице.
3. Заявителят регистрира искане за издаване на удостоверение в онлайн режим или чрез оператор в РО/МРС на Доставчика.
4. Оператор на РО/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 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 лицето.
2. Процесът на заявяване предоставя възможност на оператор на РО/МРС или на Титуляр да генерира двойката криптографски ключове и да включи публичния ключ в информацията за издаване на удостоверението.
3. Двойката криптографски ключове за издаване на КУКЕП задължително се генерира в QSCD, 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.
5. В случаите, когато е необходимо, РО/МРС предоставя на Титуляря или на упълномощено от него лице в защитен вид информация/код за достъп до частния ключ.
6. Ако Заявителят не притежава QSCD, когато представя искане за издаване на КУ на РО/МРС на Доставчика, той само въвежда информацията за идентифициране на Титуляря, както и друга допълнителна такава, без да генерира криптографската двойка ключове 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 КУКЕП са подписани от Доставчика.

4.2 Процедура на издаване

4.2.1 Функции по идентификация и автентификация

1. РО/МРС извършва идентификация и автентификация на Заявителя на искането за издаване на удостоверение - Титуляр или упълномощено от него лице.
2. След първоначална идентификация и според утвърдени вътрешни процедури на Доставчика, на база постъпило искане за издаване на удостоверение и представени документи, РО/МРС проверява и потвърждава пред Доставчика:
   - самоличността на Титуляря или упълномощеното лице;
   - представителната власт на физическото спрямо юридическото лице и на упълномощеното лице;
   - 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 документ.
3. Ако двойката ключове е генерирана при Титуляря, РО/МРС следва да провери предоставената електронна заявка и изискванията за нивото на сигурност на QSCD.

4.2.2 Потвърждаване или отхвърляне на искане за издаване

1. След успешно направените проверки, оторизиран оператор на РО/МРС утвърждава пред Доставчика искането за издаване на удостоверение.
2. РО/МРС отхвърля искането за издаване на удостоверение, ако потвърждаването е неуспешно.
3. РО/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. РО/МРС надлежно съхранява и архивира представените документи и потвърдената електронна заявка за издаване на удостоверение.
6. РО/МРС контролира и утвърждава пред Доставчика верността и точността на включената информация в удостоверението само към момента на издаването му.
7. Титуляр на КУКЕП 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. РО/МРС на Доставчика незабавно, в присъствието на Заявителя - 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. УО на Доставчика издава незабавно удостоверението след утвърждаване от РО/МРС на електронната заявка за издаване.

4.3 Издаване на удостоверение

4.3.1 Действие на Удостоверяващия орган

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

4.3.2 Известяване на Титуляря на удостоверение от Доставчика

1. Доставчикът, чрез Службата за известяване на Потребители на КУУ, незабавно известява Титуляря на издаденото и публикувано удостоверение.
2. Службата за известяване изпраща до Титуляря електронно известие по имейл с

информация за издаденото КУКЕП, неговия сериен номер и периода му на валидност, освен в случаите, когато липсва имейл адрес.
3. Доставчикът доставя издаденото удостоверение на Титуляря, респективно на упълномощеното от него лице, чрез РО/МРС.
4. Оторизиран оператор на РО/МРС записва КУКЕП на QSCD, където е била генерирана двойката криптографски ключове за това удостоверение, когато това е възможно.

4.4 Приемане и публикуване на удостоверението

1. Доставчикът, чрез оперативния УО публикува незабавно издаденото удостоверение в Публичния регистър на издадените удостоверения.
2. Титулярят може да възрази пред Доставчика, 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 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 Титуляря

1. Частният ключ, съответстващ на удостоверения публичен ключ, се контролира от Титуляря. Отговорността за използването на частния ключ е на Титуляря.
2. 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 квалифициран електронен подпис в рамките на срока на валидност на удостоверението;
   - проверка на положен квалифициран електронен подпис;
   - до момента на прекратяване на удостоверението;
   - когато удостоверението е спряно, не използва частния ключ, в частност за създаване на квалифициран електронен подпис;
   - съгласно Договора за удостоверителни услуги между него и Доставчика.

4.5.2 От доверяваща се страна

1. Публичният ключ в КУКЕП, съответстващ на държания от Титуляря частен ключ, е публично достъпен за всички.
2. Всяка доверяваща се страна, включително оператор в РО/МРС следва да използва публичния ключ и КУКЕП на 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 усъвършенствания електронен печат 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 КУКЕП запазва информацията от текущото удостоверение, като в подновеното удостоверение се променя периода на валидност.
2. Подновяване на КУКЕП , 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 КУКЕП се предхожда от регистриране на искане за подновяване пред

РО/МРС.
4. Искането за подновяване на удостоверение се регистрира онлайн, когато Титулярят има валидно КУКЕП, 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, Титулярят или упълномощено от него лице трябва лично да посети РО/МРС на Доставчика.
6. Титуляр или упълномощено от него лице може да поднови многократно свое КУКЕП при съблюдаване на посочените по-долу условия за подновяване.
7. Доставчикът не допуска използване на двойка ключове за период, по-голям от 3 (три) години.
8. Доставчикът не препоръчва многократното подновяване на КУКЕП, чрез „Renew" с цел да се намали риска от компрометиране на частния ключ.
9. Доставчикът препоръчва на Титуляря да поднови свое удостоверение чрез „Re-key".

4.6.1 Условия за подновяване на удостоверение

1. РО/МРС ще поднови едно КУКЕП чрез „Renew" при съблюдаване на следните условия:
   - удостоверението не е прекратено в периода му на валидност;
   - 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 на Заявителя и съблюдава посочените времеви ограничения при подновяване.
2. РО/МРС ще поднови едно КУКЕП чрез „Re-key" при съблюдаване на следните условия:
   - удостоверението не е прекратено в срока му на валидност;
   - Титуляр или упълномощено 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 на Заявителя и съблюдава посочените времеви ограничения при подновяване;
3. Във всички случаи, когато има промяна в удостоверената информация за 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. Титуляр или упълномощено 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 КУКЕП се предхожда от регистриране на искане за подновяване пред РО/МРС на Доставчика.
2. Искането за подновяване на удостоверение чрез електронна заявка се удостоверява с КЕП. В случай, че удостоверението, което се подновява е с изтекъл срок на валидност, Титулярят или упълномощено от него лице трябва да посети лично РО/МРС на Доставчика. РО/МРС строго следва изискванията за идентификация и установяване на идентичност на Заявителя и на условията за подновяване.
3. След успешна идентификация и проверка на условията за подновяване, РО/МРС потвърждава искането за подновяване пред оперативния УО на Доставчика.
4. След успешна електронна автентификация на РО/МРС чрез оторизирания оператор, оперативния УО изпълнява потвърденото искане за подновяване на удостоверението.
5. При неуспешна идентификация и проверка на условията за подновяване, РО/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 КУКЕП.

4.6.4 Известяване на Титуляря след подновяване на удостоверение

1. Доставчикът, чрез Службата за известяване на Потребители на удостоверителни услуги, незабавно известява Титуляря на подновеното и публикувано удостоверение.
2. Службата за известяване изпраща до Титуляря електронно известие по имейл с информация за издаденото КУКЕП, неговия сериен номер и периода на валидност на подновеното удостоверение и адреса (URL), от който може да достави подновеното удостоверение.
3. Когато Заявителят за подновяване на удостоверение посещава РО/МРС, Титулярят получава подновеното удостоверение чрез оторизирания оператор, който при необходимост го записва на QSCD, в което е генерирана двойката криптографски ключове за удостоверението.

4.6.5 Публикуване на подновено удостоверение

1. Доставчикът, чрез оперативния УО 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 КУКЕП 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 КУКЕП само при спазване на изискванията и на условията за издаване на ново удостоверение.
2. Доставчикът не допуска промяна в профила на КУКЕП, специфициран в Част II на този документ.
3. Доставчикът не предлага услугата "Модификация на сертификат" (Certificate Modification).

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 УО за издаване и поддържане на КУКЕП, действието на всички издадени от него и валидни удостоверения се прекратява.
3. Само оперативният УО, издал удостоверение, 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 УО, 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. За спешно спиране на действието на удостоверение (при изгубено или откраднато QSCD устройство) е необходимо това да се заявяви на телефон: +359 2 97 13 461.
6. При срив в системата, услугите или други фактори, които са извън контрола на УО, ДКУУ 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.
7. Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

4.9.1 Условия за прекратяване на удостоверение

1. Доставчикът прекратява издадено от него КУКЕП при:

- смърт или поставяне под запрещение на Титуляря с прекратяване на юридическо лице на Титуляря;
- прекратяване на представителната власт на Титуляря спрямо юридическото лице, което представлява;
- установяване на неверни данни при издаване на удостоверението;
- станала впоследствие невярна удостоверена информация;
- при промяна в удостоверена вече информация на Титуляря;
- компрометиране на частния ключ;
- забава в заплащането на дължимо възнаграждение;
- искане за прекратяване от страна на Титуляря, след като се увери в самоличността им и в представителната власт на Титуляря.

2. Доставчикът предприема незабавно прекратяване на действието на издаденото КУКЕП 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 УО 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 РО/МРС на Доставчика.
2. Искането за прекратяване на удостоверение може да се регистрира електронно, само когато Титуляря има (друго) валидно и достъпно за ползване удостоверение. 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 полагане на валиден КЕП, съответстващ на валидно удостоверение на Титуляря.
4. Оторизираният оператор в РО/МРС незабавно, без да идентифицира Заявителя, спира действието на удостоверението за не повече от 24 часа.
5. Във всички случаи, Титулярят или упълномощено от него лице трябва да посети лично РО/МРС на Доставчика за последваща проверка на идентичността, респективно самоличността на Заявителя.
6. РО/МРС строго следва изискванията за идентификация и установяване на идентичност, респективно самоличност на Заявителя и причините за прекратяване.
7. След успешна електронна автентификация на РО/МРС чрез оторизирания оператор, оперативния УО изпълнява потвърдената заявка за прекратяване на удостоверението.
8. При неуспешна идентификация и проверка на условията за прекратяване, РО/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 УО, незабавно публикува прекратеното удостоверение в CRL, като издава нов списък.
11. След прекратяване на удостоверението, Доставчикът, чрез Службата за известяване незабавно уведомява Титуляря на прекратеното удостоверение.
12. Прекратено удостоверение на 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 КУКЕП, Доставчикът чрез своя РО/МРС спира действието на удостоверението за не повече от 24 часа.
2. В рамките на този гратисен период Доставчикът, чрез своя РО/МРС, трябва да извърши всички проверки за установяване на идентичността 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 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 КУКЕП само след успешна проверка на статуса на удостоверението чрез актуалния CRL или чрез проверка на текущия статус на удостоверението в реално време чрез OCSP сървъра на Доставчика.
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 УО, публикува незабавно нов актуален CRL, всеки път когато се прекрати действието на валидно КУКЕП, издадено от този орган.
2. Доставчикът, чрез своя оперативен УО, 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 УО.

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 КУ.

4.9.9 Изисквания за ползване на OCSP

1. Проверка на статус на КУКЕП в реално време (по OCSP протокол) изисква да се използва необходимата техника и технологии, както и онлайн достъп през Интернет до OCSP сървъра на Доставчика.
2. Проверка на статус на КУКЕП 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 УО, спира действието на валидно КУКЕП при определени условия и за срок до 24 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 Титуляря или упълномощено от него лице, без да е длъжен да се увери в идентичността 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 РО/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 КЕП.
4. Оторизираният оператор в РО/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 РО/МРС, оперативния УО изпълнява потвърдената заявка за спиране на удостоверението.
6. РО/МРС не може да отхвърля искането за спиране.
7. След спиране на удостоверението, Доставчикът чрез своя оперативен УО незабавно публикува спряното удостоверение в CRL чрез издаване на нов CRL.
8. След спиране на удостоверението, Доставчикът чрез своята Служба за известяване незабавно уведомява Титуляря на спряното удостоверение.

4.9.13 Ограничение на периода на спиране на удостоверение

1. Доставчикът спира действието на КУКЕП за период до 24 часа от получаване на искането за спиране.
2. Доставчикът временно спира до 24 часа действието на удостоверение, преди прекратяването му.

4.9.14 Възобновяване действието на спряно удостоверение

1. Доставчикът възобновява действието на спряно КУКЕП:
   - до 24 часа след неговото спиране;
   - след като изтече срока за спиране (24 часа) и не е постъпило искане за прекратяване;
   - 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. РО/МРС възобновява спряно КУКЕП след като получи искане за възобновяване от Титуляря и след успешна проверка за идентификация.
2. РО/МРС възобновява спряно удостоверение след като получи писмено разпореждане или писмена заповед от КРС, съответно на председателя на КРС за възобновяване на удостоверението.
3. РО/МРС незабавно възобновява спряно удостоверение след като изтече нормативния период на спиране (24 часа).
4. Във всички случаи, процедурата по възобновяване изважда спряното удостоверение от текущия CRL и публикува нов CRL.

4.10 Статус на удостоверение

1. Всички действителни КУКЕП, които Доставчикът издава 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 OCSP сървъра, 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"- OCSP сървъра 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.

4.12 Възстановяване на ключове

1. Доставчикът не предлага услугата "Ескортиране на ключ и възстановяване на ключ" (Key Escrow and Key Recovery).

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 УО „B-Trust Root Qualified CA";
   - Оперативен УО „B-Trust Operational Qualified CA";
   - Регистриращ орган;
   - Публичен регистър;
   - Орган за издаване на квалифицирани електронни времеви печати „B-Trust Qualified Time Stamp Authority";
   - OCSP сървър „B-Trust Root Qualified OCSP Authority";
   - OCSP сървър „B-Trust Qualified OCSP Authority".
3. Инфраструктурата B-Trust на Доставчика е физически и логически обособена и не се използва при други дейности, които „БОРИКА“ 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 УО на Доставчика и всичките централни компоненти на инфраструктурата – „B-Trust Root Qualified CA“, „B-Trust Operational Qualified CA”.

5.1.2 Физически достъп

1. Физическият достъп до специализираното помещение се контролира от системи за контрол на достъпа, видеонаблюдение, сигнално-известителни системи и 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 документ, 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 КУКЕП, 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 поне следните дейности:
   - генериране и поддържане на инфраструктурата на публичния ключ на доставчика на удостоверителни услуги;
   - администриране и осигуряване сигурност на системите;
   - създаване и управление на КУКЕП, включително създаване на двойка ключове - частен и публичен за КУКЕП;
   - 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 УО и компоненти в инфраструктурата на B-Trust;
   - управление на HSM на „B-Trust Root Qualified CA" и „B-Trust Operational Qualified CA";
   - 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.
   - издаване на квалифициран електронен времеви печат 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 РО/МРС относно:
   - постъпили документи за регистриране с цел установяване на идентичност 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 „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА" АД квалифицирани удостоверителни услуги", 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;
   - УО 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. „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА“ АД квалифицирани удостоверителни услуги“ и Договорът за удостоверителни услуги 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 КУКЕП, 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 УО вследствие от природни бедствия или аварии.
3. В случай на сривове в компютърен ресурс, в софтуер или в информацията, Доставчикът уведомява Титулярите, възстановява компонентите на инфраструктурата и приоритетно възобновява достъпа до Публичния регистър и CRL.
4. При компрометиране на използван криптографски алгоритъм, Доставчикът информира Потребителите и Доверяващите се страни със съобщение на официалния си уеб сайт.

5.8 Компрометиране на частен ключ

5.8.1 На Удостоверяващ орган

1. Доставчикът предприема следните действия при компрометиране на частния ключ на оперативния УО:
   - прекратява незабавно удостоверението на оперативния орган;
   - издава и публикува нов CRL от базовия орган;
   - уведомява Потребителите и Доверяващите се страни;
   - спира оперативния УО;
   - 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 УО:
   - прекратява незабавно удостоверението на базовия орган;
   - следва всички стъпки по предходната точка;
   - уведомява КРС и акредитира/регистрира нови удостоверяващи органи.

5.8.2 На частен ключ на Титуляр

1. При компрометиране на частен ключ на Титуляр , последният 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;
- ДКУУ 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 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 КУКЕП на Потребителите.
3. Криптографските (RSA) двойки ключове на издаваните КУКЕП в инфраструктурата на Доставчика се генерират, както следва:
   - от Титуляря - с хардуер и софтуер, който е под негов контрол;
   - от РО/МРС на Доставчика - с хардуер и софтуер, който е под контрола на Доставчика.
4. Доставчикът може на базата на договорни отношения да предостави на Титулярите одобрени от него технически средства, които отговарят на изискванията за ниво на сигурност.
5. Само електронни подписи, създадени с частен ключ на двойка ключове генерирани в QSCD имат характера на КУКЕП.
6. Титулярят се задължава да използва лицензиран софтуер за работа с КУКЕП и със QSCD.

6.2 Процедура по генериране

6.2.1 Генериране на криптографски ключове на Удостоверяващ орган на Доставчика

1. Доставчикът генерира двойки криптографски (RSA) ключове на базовия и на оперативен УО като използва HSM с удостоверено 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 УО, съответно „B-Trust Root Qualified CA" и „B-Trust Operational Qualified CA" съгласно документирана вътрешна процедура, съгласувана и утвърдена от ръководството на Доставчика.
3. Процедурата се изпълнява в присъствие на представител на висшето ръководство на „БОРИКА“ АД и на нотариус.
4. Двойка ключове на УО 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 УО се съхраняват разделно върху отделни QSCD, 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 УО в отделните QSCD не позволява тези ключове да бъдат компрометирани и/или нерегламентирано репродуцирани извън Доставчика.

6.2.2 Генериране на криптографски ключове на Титуляря

1. Двойката ключове на Титуляр на КУКЕП се генерира с използване на специализиран софтуер, който е изцяло под контрола на Титуляра.

2. В случай, когато Доставчикът генерира Двойката ключове на Титуляр на КУКЕП, той използва специализиран лицензиран софтуер, проверен за успешна работа през интерфейсите на инфраструктурата на B-Trust.
3. Двойката ключове на Титуляр на КУКЕП се генерира в одобрен от Доставчика QSCD с проверено ниво на сигурност. Когато двойката ключове се генерира при Доставчика, винаги се използва B-Trust QSCD. Частният ключ на генерираната двойка ключове не може да бъде изведен от QSCD.
4. Контролът на частния ключ е чрез код за достъп, а дължината на RSA ключа е поне 2048 бита. Титулярът използва частния ключ за да създаде подписа, като въвежда кода за достъп до него.
5. Когато двойката ключове се генерира при Титуляр, Доставчикът препоръчва последният да използва одобрено в инфраструктурата на B-Trust решение или еквивалентно такова.
6. За целите на полагане на КЕП Доставчикът препоръчва Потребителят да използва B-Trust QSCD или друго QSCD, съвместимо в инфраструктурата на B-Trust.

6.2.3 Доставка на частния ключ

1. Когато двойката ключове се генерира при Доставчика, Титулярят или изрично упълномощено от него лице получава частния ключ и издаденото удостоверение от РО/МРС на Доставчика.
2. При издаване на КУКЕП частния ключ и издаденото удостоверение се предават върху B-Trust QSCD, където е генериран частния ключ. QSCD гарантира най-високо ниво на сигурност и защита на частния ключ и се предоставя заедно с начален код за достъп.
3. Титулярят е задължен да смени предоставения начален код за достъп и въведе свой личен.
4. Когато Титуляр генерира двойката ключове при себе си, той носи цялата отговорност за гарантиране на държането на частния ключ от него.
5. Когато Титуляр генерира двойката ключове за КУКЕП при себе си, той декларира пред Доставчика, че двойката ключове напълно отговаря на изискванията за полагане на КЕП в съответствие с Регламента.

6.2.4 Доставка на публичния ключ при Доставчика

1. Изпълнява се само от 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. Титулярят доставя чрез РО/МРС на Доставчика публичния ключ от генерираната двойка ключове.
3. Титулярят може да предостави електронната заявка на носител, лично в РО/МРС, заедно с другите документи съгласно Политиката на Доставчика, през Интернет-страницата на Доставчика или по друг подходящ начин.
4. РО/МРС на Доставчика задължително прави проверка на държането на частния ключ от 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 оперативен УО „B-Trust Operational Qualified CA" е 4096 бита.
3. Дължината на двойката RSA-ключове на оперативните органи „B-Trust Root Qualified OCSP Authority" и „B-Trust Qualified OCSP Authority" е не по-малка от 2048 бита.
4. Дължината на двойка ключове (RSA) за КЕП на Титуляр, генерирана чрез инфраструктурата на Доставчика е поне 2048 бита.

5. Дължината на двойка ключове (RSA) за КЕП на Титуляр, генерирана извън инфраструктурата на Доставчика е поне 2048 бита.
6. Независимо къде е генерирана двойката ключове за издаване на КУКЕП, ключът трябва да е с дължина най-малко от 1024 бита за алгоритми RSA.

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.

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 Qualified CA" и „B-Trust Operational Qualified CA" използват HSM с удостоверено ниво на сигурност FIPS 140-2 Level 3(съответно CC EAL 4+ или по-високо), която удовлетворява нормативните изисквания.
2. B-Trust QSCD, в което се генерира и съхранява частния ключ на Титуляр е с ниво на сигурност CC EAL 4+/FIPS 140-1 Level 2.
3. Всички QSCD извън инфраструктурата на B-Trust, които Потребителят може да ползва, за да генерира двойка ключове и да съхранява частния ключ за КЕП, 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 УО на Доставчика се използват само в 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 УО се изпълнява и процедурата по съхраняване на частния ключ в съответствие с утвърдена вътрешна процедура.
3. Частният ключ на КУКЕП на Титуляр се използва само в B-Trust QSCD или в QSCD с еквивалентно ниво на сигурност и е достъпен посредством личен код за достъп. В този случай едновременно с генериране на двойка ключове се изпълнява съхраняване на частния ключ в QSCD.

6.3.3 Съхранение и архивиране на частния ключ

1. Частните ключове на УО се съхраняват на части разделно върху отделни QSCD със защитен профил CC EAL 4+ или по-висок, като достъпът до всяко QSCD се контролира чрез код за достъп от съответното оторизирано лице от персонала на Доставчика.
2. Кодът за достъп до всяко QSCD е личен за всяко отделно оторизирано лице от персонала на Доставчика.
3. Разделното съхранение на частните ключове на УО върху няколко QSCD и личния контрол на достъп до тези QSCD не позволява ключовете да бъдат компрометирани или нерегламентирано репродуцирани извън Доставчика.
4. Репродуцирането на частни ключове на Доставчика върху резервен HSM след дефектиране на оперативната такава, се изпълнява само в присъствие на поне 2 оторизирани лица, всяко от които контролира достъпа до неговото QSCD.
5. Частният ключ на КУКЕП на Титуляр се съхранява само на QSCD и не може да се репродуцира на друго QSCD. При дефектиране на QSCD, Потребителят трябва да го подмени и да заяви издаване на ново удостоверение.
6. Доставчикът по никакъв начин не съхранява и не архивира частен ключ на Титуляр за създаване на КЕП, независимо къде се генерира двойката.

6.3.4 Трансфер на частен ключ в и от криптографски модул

1. Трансфер на частен ключ на УО на Доставчика от 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 УО.
2. Трансфер на частен ключ на Титуляр към и от Доставчика с цел съответно съхранение и възстановяване в друго QSCD не се поддържа.
3. Частният ключ на КУКЕП на Титуляр се съхранява само на QSCD, в което се генерира двойката ключове и не може да се трансферира/репродуцира на друго място.

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 HSM и се активира частния ключ.
3. Частен ключ на Титуляр се активира, чрез въвеждане на потребителския код за достъп до мястото, където защитено 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 УО се деактивира (прекратява се възможността за използване/достъп) посредством преустановяване на логическия достъп до съответния ключ в нея.
2. Частен ключ на Титуляр се деактивира (прекратява се възможността за използване/достъп) посредством преустановяване на логическия достъп до мястото, където защитено се съхранява ключа.

6.3.7 Унищожаване на частен ключ

1. Частен ключ на Доставчика в криптосистемата на УО се унищожава посредством изтриване на ключа или съответния слот. При необходимост се изтриват и съхраняваните в архива носители за възстановяване.
2. Частен ключ на КУКЕП на Титуляр се унищожава посредством изтриването му от мястото, където защитено се съхранява ключа.
3. Частен ключ на КУКЕП на Титуляр се унищожава посредством изтриването му от QSCD или цялостното изтриване/инициализация/унищожаване на QSCD.

6.4 Други аспекти на управление на двойка ключове

6.4.1 Архивиране на публичния ключ

1. Публичните ключове на УО 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 УО се архивират и съхраняват за период от 10 години след изтичане на периода на валидност или прекратяването на съответните удостоверения.
3. Публичните ключове на Титуляри се съдържат в издадените за тях удостоверения, които са публикувани в Публичен регистър и се съхраняват във вътрешен регистър.
4. Публичните ключове на 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. КУКЕП имат следните срокове на действие:
   - на базовия УО „B-Trust Root Qualified CA" - 20 (двадесет) години;
   - на оперативния УО „B-Trust Operational Qualified CA" - 15 (петнадесет) години;

- на Титуляр– съгласно договора между Доставчика и 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 УО, 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 УО се генерира и публичната й 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 генериране на двойка ключове за КУКЕП от Титуляря, последния сам създава и управлява данни за активация.
2. При генериране на двойка ключове за КУКЕП на Титуляря от Доставчика, последния предава заедно с частния ключ контрола на данни за активация на Титуляря.
3. При първоначално издаване на удостоверение върху B-Trust QSCD, преди генериране на двойка ключове, B-Trust QSCD се инициализира и се създават следните кодове за достъп/активация: Потребителски ("User") и Административен ("SO") и съответно, за персонален достъп до частния ключ в QSCD и за деблокиране на блокирано QSCD.
4. Началният Потребителски и Административен код за достъп и за деблокиране на B-Trust QSCD се предоставят на Титуляря или на упълномощеното от него лице в запечатен, непрозрачен хартиен плик.
5. Титулярят е задължен на смени първоначалния Потребителски код за достъп до B-Trust QSCD посредством софтуера, който се предоставя с него.
6. Доставчикът препоръчва Титулярят да сменя периодично своя Потребителски код за достъп до B-Trust QSCD.
7. Титулярят следва да използва предоставеният Административен код за достъп с цел деблокиране блокирано B-Trust QSCD.

6.5.2 Защита на данни за активация

1. Титулярят е задължен да съхранява и пази от компрометиране кодовете за достъп до мястото, където защитено се съхранява частния ключ.

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 Титуляря, B-Trust QSCD се блокира.
2. Титулярят трябва да използва предоставеният му Административен код за достъп, за да деблокира блокирано B-Trust QSCD.

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 Допълнителни тестове

1. Доставчикът предоставя възможност за извършване на тестове за работоспособност на издадените квалифицирани удостоверения за квалифициран електронен подпис на официалната си страница.

6.9 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.

6.10 Удостоверяване на време

1. Доставчикът публикува в отделен документ Политиката и практиката на Органа за издаване на квалифицирани електронни времеви печати.

7 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, НА CRL И НА OCSP

7.1 Профил на квалифицирани удостоверения

1. Пълното съдържание (профил) на КУКЕП се съдържа в настоящия документ, Част II: Политика на предоставяне на КУКЕП и КУУ.

7.1.1 Номер на версия

1. Доставчикът издава КУКЕП във формат X.509, v3.
2. Версията се вписва в издаваното КУКЕП.

7.1.2 Допустими 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 УО 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" - определя идентификатора на Политиката за КУКЕП.
6. Атрибут „Key Usage" - 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 УО на Доставчика.
9. Атрибут „Authority Information Access" - съдържа URL-адреса на OCSP сървъра на удостоверението.
10. Атрибут „Qualified Statements" - атрибутът съдържа указание, че удостоверението е квалифицирано и дали частния ключ е генериран и се съхранява върху QSCD.

7.1.3 Идентификатори на алгоритмите на електронен подпис

1. Атрибутът „Signature algorithm" идентифицира алгоритмите (криптографските механизми), които се използват.

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. КУКЕП се издават съгласно Политика на Доставчика, която се вписва в атрибута „Certificate Policy" на удостоверението.

7.1.7 Означение на квалифицираното удостоверение

1. Доставчикът използва в КУКЕП с профил по стандарта X.509 v.3 атрибута „Qualified Statements" с идентификатори: „id-etsi-qcs-QcCompliance“ (OID=0.4.0.1862.1.1), „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4) и „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6) със стойност „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1).
2. Доставчикът използва в КУКЕП с профил по стандарта X.509 v.3 атрибута "Certificate Policy", на който се присвоява идентификатора (OID) със значение, както следва:

Квалифицирано Удостоверение	Наименование	Идентификатор (OID)

		вписан в атрибута "Certificate Policy"
Персонално КУКЕП на физическо лице	B-Trust Personal qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2
Професионално КУКЕП на физическо лице	B-Trust Professional qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2

7.2 Профил на Списъка на прекратени удостоверения

7.2.1 Версия

1. Доставчикът, чрез своите УО 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 5280.
2. УО на Доставчика издават, публикуват и поддържат самостоятелни пълни CRL-и като в тях записват само прекратени удостоверения, които са издадени от съответния УО.
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 УО, издал и подписал Списъка;
   - „Effective Date"/"This update" - време на издаване на Списъка;
   - „Next Update"- времето на валидност на Списъка. След посоченото време, УО издава периодично нов Списък. През периода на валидност, в случай на прекратяване/спиране на удостоверение, УО 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 УО, който издава и подписва Списъка. Съдържа значението на „subjectKeyIdentifier" от удостоверението на УО, който подписва Списъка.

7.2.3 Формат на елемент в CRL

1. CRL на УО съдържа елементи за всички прекратени удостоверения от УО. Тези елементи са постоянни в Списъка.
2. CRL на УО съдържа елемент за всяко спряно удостоверение от УО. 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 Титуляр ;
   - "CACompromise" - компрометиран частен ключ на оперативен УО на Доставчика;

- "affiliationChange" - променен статус на Титуляр спрямо друго лице - 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. OCSP сървъра на Доставчика работи и предоставя услугата „онлайн проверка на статус на удостоверение в реално време" в съответствие с международно утвърдената препоръка IETF RFC 6960.
2. Информация за профила на заявка и на отговор при работа с OCSP сървъра 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“ 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 РО/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 РО/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 пряко или косвено свързани 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 документ с тяхната практическа реализация при изпълнение на дейността на Доставчика;
   - проверка на дейността на подизпълнители - външни РО/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 КУКЕП;
   - възнаграждение за подновяване на КУКЕП;
   - 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“ АД квалифицирани 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 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 КУКЕП 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 „Издаване на квалифицирани електронни времеви печати" 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. Титуляр може да възрази относно неточност или непълнота в съдържанието на издадено КУКЕП в 3-дневен срок след публикуването му в Публичния регистър.
2. Ако причина за невярното съдържание на удостоверението е в РО/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 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 КУКЕП 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 КУКЕП на 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 ДКУУ 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 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 Титуляр ;
   - компрометиране или загуба на частен ключ на Титуляр поради не полагане на дължимата грижа за опазване 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 Титуляр, 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 Титуляря с изключение на случаите, при които Доставчикът е задължен по силата на закон.
6. Никой освен Титуляря, включително и Доставчика, няма право да използва частния ключ за създаване на електронен подпис. Доставчикът препоръчва Титуляря да не излага потребителския код за достъп до частния ключ на КУКЕП, 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 Титулярят 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 Титуляри, станали му известни при изпълнение на дейността си като ДКУУ.
3. Съгласно утвърдената Политика на КУКЕП, елементи на информацията в тях могат да съдържат лични данни. 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 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 РО, 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 ДКУУ.
2. Доставчикът осъществява дейността на регистриран ДКУУ 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 КУКЕП 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 КУКЕП;
   - прекратява и спира действието на удостоверения при условията и по реда на съответната Политика;

- уведомява незабавно след спиране на удостоверение Титуляр;
- 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 КУКЕП да отмени валидността му;
- информира 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 КУКЕП, 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 КУКЕП 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 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 на Заявителя.

9.6.2 Отговорност и гаранции на РО/МРС

1. Доставчикът гарантира, че РО/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 РО/МРС в инфраструктурата на B-Trust.

9.6.3 Отговорност на Титуляря

1. Титулярят 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 „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА“ АД квалифицирани удостоверителни услуги“. 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 представената 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 частния ключ/ QSCD, 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 КУКЕП;
- приема условията за грижата и отговорността при доверяване на КУКЕП, в случай че действа като Доверяваща се страна.

2. Титулярят е отговорен ако е приел КУКЕП, издадено от Доставчика въз основа на предоставени от него неверни данни, съответно въз основа на премълчани или липсващи данни.
3. Доставчикът ще регресира спрямо 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 Титулярят 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 Титуляр 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 КУКЕП 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 КЕП 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 КЕП, 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 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 КУКЕП, 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 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 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 Титуляр, телекомуникационни и енергийни смущения и др.
8. Доставчикът не отговаря за вреди, причинени от използване на КУКЕП извън обхвата на вписаните в него ограничения и предназначения.

9.8 Ограничение на отговорност на Доставчика

1. За издавани КУКЕП, Доставчикът отговаря в рамките на Максимален лимит на отговорност 40 000 лв.
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 Титуляря, Доставчикът ще ангажира отговорността на 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 хранилището за документи на сайта на Доставчика.
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 РО/МРС както и електронни уведомления, които публикува на своята Интернет-страница.
2. Клиентите 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 15 115
факс: 02/ 981 45 18
имейл адрес: info@b-trust.org
Официална страница на доставчика: www.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 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.

ЧАСТ II:

ПОЛИТИКА

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

1. Политиката на предоставяне на КУКЕП и КУУ е документ, неделима част от „Политика за издаване на квалифицирани удостоверения за квалифициран електронен подпис и Практика при предоставяните от „БОРИКА“ АД квалифицирани удостоверителни услуги“, описващ политиката и процедурите, които Доставчикът следва при издаване на КУКЕП, видовете КУУ приложими за тези удостоверения, както и тяхното приложно поле.
2. Политиката определя начина и нивото на сигурност при идентификация на Титуляря, следваните процедури при издаване, поддръжка и управление на удостоверението, изискването за ниво на сигурност на QSCD за създаване на подписа, за 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 КУКЕП, които издава, поддържа и управлява „БОРИКА“ АД като регистриран ДКУУ:

Квалифицирано Удостоверение	Наименование на удостоверение	Политика
Персонално КУКЕП на физическо лице	B-Trust Personal qualified certificate QES	B-Trust Personal Qualified Certificate Policy (QCP-n-qscd) (Политика за предоставяне на КУКЕП на физическо лице)
Професионално КУКЕП на физическо лице	B-Trust Professional qualified certificate QES	B-Trust Professional Qualified Certificate Policy (QCP-n-qscd) (Политика за предоставяне на КУКЕП на физическо лице, асоциирано с юридическо лице)

4. Общите изисквания и отговорности на Доставчика, Титуляря и дължимата грижа на всяка Доверяваща се страна при използване на КУКЕП са посочени в Част I (ПРАКТИКА) на настоящия документ.
5. Общите процедури на спиране, възобновяване и прекратяване действието на издадено валидно КУКЕП се съдържат в Част I (ПРАКТИКА) на настоящия документ.
6. Цените на удостоверенията и на услугите по издаване и поддържане на КУКЕП се съдържат в Ценоразписа на Доставчика, достъпен на неговата Интернет-страница.

10 ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА ПЕРСОНАЛНИ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС (КУКЕП) НА ФИЗИЧЕСКИ ЛИЦА

B-Trust Personal Qualified Certificate Policy (QCP-n-qscd)
B-Trust O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 (ETSI EN 319 411-2 O.I.D. = 0.4.0.194112.1.2)

10.1 Обща характеристика на удостоверенията

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

10.2 Предназначение и приложимост на удостоверенията

1. Персонално КУКЕП на физическо лице може да се използва при създаване/полагане на КЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват най-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 Персонално КУКЕП на физическо лице 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 Персонално КУКЕП на физическо лице с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1, която съответства на политика „QCP-n-qscd“ (OID 0.4.0.194112.1.2) по ETSI EN 319 411.
2. Доставчикът допълнително вписва в Персонално КУКЕП на физическо лице политика „qcp-public-with-sscd“ (O.I.D. = 0.4.0.1456.1.1) по ETSI EN 101 456, с което обозначава, че частния

ключ е генериран, съхранява се и се използва върху QSCD.

3. Доставчикът вписва в Персонално КУКЕП на физическо лице атрибута „Qualified Statements" с идентификатор „ id-etsi-qcs-QcCompliance “ (OID=0.4.0.1862.1.1), с което обозначава, че удостоверението е квалифицирано.
4. Доставчикът вписва в Персонално КУКЕП на физическо лице атрибута „Qualified Statements" с идентификатор: „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4), с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
5. Доставчикът вписва в Персонално КУКЕП на физическо лице атрибута „Qualified Statements" с идентификатор: „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1), с което обозначава, че удостоверението се използва за полагане на квалифициран електронен подпис.

10.4 Профил на удостоверенията

1. Доставчикът издава Персонално КУКЕП на физическо лице (B-Trust Personal qualified certificate QES) с посочения по-долу профил:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN =	[Обичайно име: Избрано от физическото лице име. Ако не е избрано, се вписва пълното име на физическото лице]
	G =	[Собствено име на физическото лице според документ за самоличност]
	SN =	[Фамилно име на физическото лице според документ за самоличност]
	SERIALNUMBER =	[Идентификатор на физическото лице. • За български гражданин - един от следните: ○ PNOBG-XXXXXXXXXX за ЕГН ○ PASSBG-XXXXXXXX за номер на паспорт ○ IDCBG-XXXXXXXXX за номер на лична карта ○ TINBG-XXXXXXXXX за ДДС номер на физическо лице ○ PI:BG-XXXXXXXXXX за личен номер на чужденец ○ BT:BG-XXXXXXXXXX за номер на физическо лице, издаден от B-Trust УО • За чуждестранно лице – един от следните: ○ PNOYY- XXXXXXXXXX за национален личен номер ○ PASSYY- XXXXXXXX за номер на паспорт ○ IDCYY- XXXXXXXXX за национален номер на лична карта където YY е двубуквен код на държавата на физическото лице според ISO 3166]
	E =	[Имейл адрес]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[хеш на „Public key"]

Authority Key Identifier	KeyID =	[хеш на „Public key " на „Issuer“]	
Issuer Alternative Name	URL =	http://www.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2	
Enhanced Key Usage	-	Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

10.5 Оперативни процедури по издаване, подновяване и управление на удостоверението

1. Оперативните процедури по издаване, подновяване и управление на Персонално КУКЕП на физическо лице са описани в Глава 12 на документа.

11 ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА ПРОФЕСИОНАЛНИ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС (КУКЕП) НА ФИЗИЧЕСКИ ЛИЦА, АСОЦИИРАНИ С ЮРИДИЧЕСКИ ЛИЦА

B-Trust Professional Qualified Certificate Policy (QCP-n-qscd)
B-Trust O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 (ETSI EN 319 411-2 O.I.D. = 0.4.0.194112.1.2)

11.1 Обща характеристика на удостоверенията

1. Удостоверение за електронен подпис, издадено по тази политика, има характер на КУКЕП по смисъла на чл. 16, ал. 1 от ЗЕДЕП.
2. Професионално КУКЕП на физическо лице, асоциирано с юридическо лице се издава на Титуляр - физическо лице и удостоверява електронната идентичност и връзката на Титуляря с публичния му ключ.
3. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Доставчика на Титуляря или упълномощено от него лице при проверка на неговата самоличност.
4. Процедурата по идентификация включва представяне на доказателство за самоличността на Титуляря и тяхната проверка.
5. Проверката на искането за издаване на Професионално КУКЕП на физическо лице, асоциирано с юридическо лице се извършва по реда на предходните точки и осигурява най-високо ниво на сигурност по отношение на идентичността на Титуляря и връзката му с публичния ключ.
6. Титулярят може сам да генерира двойката ключове, като използва B-Trust QSCD и съответен софтуер за него или друго еквивалентно QSCD, което е съвместимо в инфраструктурата на Доставчика.
7. В искането за издаване на Професионално КУКЕП на физическо лице, асоциирано с юридическо лице се посочва и лицето, което Титуляря представлява. Проверява се и идентичността и на това лице.
8. Частният ключ за създаване на КЕП задължително се генерира в QSCD и не може да бъде изведен навън от него.
9. Издаденото Професионално КУКЕП на физическо лице, асоциирано с юридическо лице, удостоверяващо публичен ключ съответстващ на частния такъв, задължително се записва в QSCD, което се предоставя на Титуляря.
10. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Професионално КУКЕП на физическо лице, асоциирано с юридическо лице.

11.2 Предназначение и приложимост на удостоверенията

1. Професионално КУКЕП на физическо лице, асоциирано с юридическо лице може да се използва при създаване/полагане на КЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват най-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 Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице 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 КУКЕП на физическо лице, асоциирано с юридическо лице, с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2, която съответства на политика „QCP-n-qscd“ (OID 0.4.0.194112.1.2) по ETSI EN 319 411
2. Доставчикът допълнително вписва в Персонално КУКЕП на физическо лице политика „qcp-public-with-sscd“ (O.I.D. = 0.4.0.1456.1.1) по ETSI EN 101 456, с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
3. Доставчикът вписва в Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице атрибута „Qualified Statements" с идентификатор „ id-etsi-qcs-QcCompliance “ (OID=0.4.0.1862.1.1), с което обозначава, че удостоверението е квалифицирано.
4. Доставчикът вписва в Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице атрибута „Qualified Statements" с идентификатор: „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4), с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
5. Доставчикът вписва в Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице атрибута „Qualified Statements" с идентификатор: „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1), с което обозначава, че удостоверението се използва за полагане на квалифициран електронен подпис.

11.4 Профил на удостоверенията

1. Доставчикът издава Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице (B-Trust Professional qualified certificate QES) с посочения по-долу профил:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN =	[Обичайно име: Избрано от физическото лице име. Ако не е избрано, се вписва пълното име на физическото лице]
	G =	[Собствено име на физическото лице според документ за самоличност]
	SN =	[Фамилно име на физическото лице според документ за самоличност]
	SERIALNUMBER =	[Идентификатор на физическото лице. • За български гражданин - един от следните: ○ PNOBG-XXXXXXXXXX за ЕГН ○ PASSBG-XXXXXXXX за номер на паспорт ○ IDCBG-XXXXXXXXX за номер на лична карта ○ TINBG-XXXXXXXXX за ДДС номер на физическо лице ○ PI:BG-XXXXXXXXXX за личен номер на чужденец ○ BT:BG-XXXXXXXXXX за номер на физическо лице, издаден от B-Trust УО

		• За чуждестранно лице – един от следните: ○ PNOYY- XXXXXXXXXX за национален личен номер ○ PASSYY- XXXXXXXX за номер на паспорт ○ IDCYY- XXXXXXXXX за национален номер на лична карта където YY е двубуквен код на държавата на физическото лице според ISO 3166]
	O =	[Наименование на юридическото лице]
	2.5.4.97= (organizationIdentifier)	[Идентификатор на юридическо лице, с което физическото лице е асоциирано. Един от следните: • VATBG-XXXXXXXXX – за ДДС номер • NTRBG-XXXXXXXXX – за ЕИК (БУЛСТАТ)]
	E =	[Имейл адрес]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[хеш на „Public key "]
Authority Key Identifier	KeyID =	[хеш на „Public key " на „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.2 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2
Enhanced Key Usage	-	Client Authentication, Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2) / id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6) / id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) / PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

11.5 Оперативни процедури по издаване, подновяване и управление на удостоверението

1. Оперативните процедури по издаване, подновяване и управление на Професионалното КУКЕП на физическо лице, асоциирано с юридическо лице са описани в Глава 12 на документа.

12 ОПЕРАТИВНИ ПРОЦЕДУРИ ЗА ИЗДАВАНЕ, ПОДНОВЯВАНЕ И ПОДДРЪЖКА/УПРАВЛЕНИЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

1. Оперативните процедури на Доставчика за издаване, подновяване и поддръжка/управление на КУКЕП са общи за различните типове КУКЕП.

12.1 Регистрация на искане за издаване на квалифицирано удостоверение

1. Заявителят на КУКЕП прави искане пред РО/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 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 Титуляря.
3. Процесът на заявяване предоставя на Заявителя (Титуляр или упълномощено от него лице) или на оператора на РО/МРС да генерира двойката криптографски (RSA) ключове и да включи публичния ключ в информацията за издаване на удостоверението.
4. Двойката криптографски ключове за КУКЕП задължително се генерира в B-Trust QSCD или друго еквивалентно на него QSCD, 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 КУКЕП с информацията, която ще се включи в удостоверението е структура, подписана с частния ключ от генерираната двойка ключове.
6. Когато Заявителят не генерира при себе си криптографската двойка ключове, процесът на заявяване на удостоверение изисква само информацията, идентифицираща Титуляря, типа на удостоверението, както и друга допълнителна такава, без да включва генериране на криптографската двойка ключове за КУКЕП. Генерацията на двойката ключове като стъпка от искането за издаване на удостоверението се изпълнява от оператор в РО/МРС.
7. След успешна регистрация на искане за издаване на удостоверение, операторът в РО/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 КУКЕП, 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 РО/МРС изпълнява процедурата по идентификация и автентификация на Заявителя за издаване на удостоверение - Титуляр или упълномощено от него лице.
5. В съответствие с Част I (ПРАКТИКА) и утвърдени вътрешни процедури на Доставчика, на база постъпило и регистрирано искане за издаване на КУКЕП и представени документи, в личното присъствие на Заявителя - Титуляр или упълномощено от него лице, РО/МРС потвърждава пред Доставчика:
   - самоличността на Титуляря;
   - представителната власт на Титуляря, ако той е упълномощен от други лица;
   - 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 документ.

3. РО/МРС на Доставчика незабавно, в присъствието на Заявителя - 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.
4. Въз основа на утвърденото искане за издаване, УО на Доставчика издава заявения тип удостоверение.
5. 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. УО на Доставчика електронно идентифицира РО/МРС, който е утвърдил електронната заявка от искането за издаване на КУКЕП.
2. УО генерира заявеното КУКЕП, подписва го с електронния печат на Доставчика и го публикува в Публичния си регистър.
3. Службата за известяване на Доставчика изпраща до Титуляря известие по имейл с информация за издаденото КУКЕП, неговия сериен номер и периода му на валидност, освен в случаите, когато липсва имейл адрес.

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 УО.
2. Доставчикът, чрез оперативния УО публикува издаденото удостоверение в Публичния регистър на издадените удостоверения.
3. След публикуване на удостоверението 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 РО/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 КУКЕП, оператор в РО/МРС на Доставчика предоставя издаденото КУКЕП на Титуляря или упълномощеното от него лице. При необходимост преди предаването оператора записва удостоверението върху B-Trust QSCD.
2. Ако двойката ключове е генерирана при Титуляря, Доставчика го уведомява чрез електронния му пощенски адрес, съдържащ се в издаденото удостоверение, като посочва Интернет-страницата, от където може да бъде заредено издаденото удостоверение.
3. Срещу представяне на документ за самоличност, Титулярят или упълномощеното лице получава комплекта за КУКЕП, който може да включва и B-Trust QSCD, върху което е генериран частния ключ на удостоверението.

12.6 Подновяване на удостоверението

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

12.7 Спиране/възобновяване на удостоверението

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

12.8 Прекратяване на удостоверението

Прекратяване на КУКЕП се изпълнява от Доставчика в съответствие с общата оперативна процедура за Прекратяване на удостоверение, представена в Част I (ПРАКТИКА).