Общодостъпен документ

ПРАКТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ „БОРИКА“ АД

(B-Trust CPS-eIDAS)

Версия 7.0

В сила от:

1 Януари 2021 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.
4.0	Димитър Николов	01.06.2017	Утвърден	Разделяне на документа на обща практика при предоставяне на квалифицирани удостоверителни услуги и съответни политики. Добавяне на обща практика при предоставяне на Квалифицирани удостоверения за квалифициран електронен печат. Добавяне на обща практика при предоставяне на Квалифицирани удостоверения за облачен квалифициран електронен подпис. Добавяне на обща практика за квалифицирана услуга за валидиране на квалифицирани електронни подписи/печати.
5.0	Димитър Николов	01.04.2019	Утвърден	Добавени „Квалифицирана услуга за валидиране на квалифицирани електронни подписи и печати“ и „Услуга за квалифицирано съхраняване на квалифицирани електронни подписи и печати
6.0	Димитър Николов	01.03.2020	Утвърден	Технически корекции
6.1	Димитър Николов	01.10.2020	Утвърден	Допълнени изисквания за установяване на самоличност
7.0	Димитър Николов	01.01.2021	Утвърден	Добавен процес по отдалечено установяване на самоличност

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК

АД	Акционерно дружество
ДВ	Държавен вестник
ДКУУ	Доставчик на квалифицирани удостоверителни услуги
ЕГН	Единен граждански номер
ЕП	Електронен подпис
ЗЕДЕУУ	Закон за електронния документ и електронните удостоверителни услуги
КЕП	Квалифициран Електронен Подпис
КУ	Квалифицирано удостоверение
КУУ	Квалифицирани удостоверителни услуги
КУКЕП	Квалифицирано удостоверение за Квалифициран Електронен Подпис
КУУЕП	Квалифицирано удостоверение за Усъвършенстван Електронен Подпис
КУКЕПечат	Квалифицирано удостоверение за Квалифициран Електронен Печат
КУУЕПечат	Квалифицирано удостоверение за Усъвършенстван Електронен Печат
КРС	Комисия за регулиране на съобщенията
МТС	Министерство на транспорта и съобщенията
МРС	Местна регистрираща служба
НОПДДУУ	Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги
НИАКЕП	Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис
ОКЕП	Облачен КЕПЕ-ОКЕП Еднократен ОКЕП
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на КУ и 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/ЕОРО
РО	Регистриращ орган
УЕП	Усъвършенстван Електронен Подпис
УЕПечат	Усъвършенстван Електронен Печат
УО	Удостоверяващ орган

СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК

AES	Advanced Electronic Signature – Усъвършенстван електронен подпис
AESeal	Advanced Electronic Seal – Усъвършенстван електронен печат
BG	Bulgaria – България
B-Trust QHSM	Квалифициран HSM в платформата за облачен КЕП, със защитен профил, отговарящ на изискванията за ниво на сигурност EAL 4+ или по-високо, съгласно CC или друга спецификация, определяща еквивалентни нива на сигурността
CA	Certification Authority – Удостоверяващ орган (УО)
CC	Common Criteria for Information Technology Security Evaluation - Международен стандарт (ISO/IEC 15408) за информационна сигурност
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
CQES	Cloud Qualified Electronic Signature – Квалифициран Облачен КЕП/ОКЕП
CQES_OT	One Time CQES – Еднократен Е-ОКЕП
DSA	Digital Signature Algorithm – Вид криптографски алгоритъм за създаване на подпис
DN	Distinguished Name – Уникално име
eIDAS	ЕС Регламент 910/2014
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
GDPR	Регламент (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни
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 онлайн проверка на статуса на удостоверения
PKCS	Public Key Cryptography Standards – Криптографски стандарт за публичен

	ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
QC	Qualified Certificate – Квалифицирано удостоверение
QES	Qualified Electronic Signature – Квалифициран електронен подпис
QESeal	Qualified Electronic Seal – Квалифициран електронен печат
RA	Registration Authority – Регистриращ орган
RSA	Rivest – Shamir - Adelman – Криптографски алгоритъм за създаване на подпис
QSCD	Qualified Signature Creation Device – (локално) устройство за сигурно създаване на квалифициран подпис съгласно ЕС Регламент 910/2014
QHSM	HSM с ниво на сигурност на QSCD
RQSCD	Remote QSCD – сървърна компонента с QHSM за сигурно създаване на подпис от разстояние
SAD	Signature Activation Data – Данни за активация на подписа
SAP	Signature Activation Protocol – Протокол за активация на подписа
SAM	Signature Activation Module - Модул активиращ генериране на подпис
SCT	Signature Creation Token – софтуерен токън (PKCS#12 крипто-файл)
B-Trust SCT	PKCS#12 – преносим стандартен крипто-файл (софтуерен токън)
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
QCP-l-qscd	Certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
QCP-w	Certificate policy for EU qualified website authentication certificates

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 01.01.2021 г. ;
- съдържа условията, съгласно които Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД (Доставчик) предоставя на Потребители срещу възнаграждение квалифицирани удостоверения (КУ) и удостоверителни услуги (КУУ) за електронен подпис (ЕП), за облачен електронен подпис, за електронен печат (ЕПечат) и за автентичност на уебсайт (WEB), 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 Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ);
- има характер на общи условия 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 ЗЕДЕЕУУ. Договорът може да съдържа специални условия, които се ползват с предимство пред общите условия в настоящия документ;
- включва подробно описание на практиката на Доставчика при предоставяне на КУ и КУУ за тях и е публичен документ с цел установяване на съответствие на дейността на Доставчика със ЗЕДЕУУ и нормативната уредба;
- е общодостъпен по всяко време на интернет-страницата на Доставчика на адрес: https://www.b-trust.bg/documents;
- може да бъде променян от ДКУУ и всяка нова редакция на се публикува на интернет-страницата на Доставчика;

Настоящият документ е изготвен в съответствие с:

- Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ);
- Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги (НОПДДУУ);
- 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 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1/5: Certificate Profiles;
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles;
- ETSI EN 419 241, part 2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- ETSI EN 419 241, part 3 – Trustworthy Systems Supporting Server Signing – Part 3: Protection profile for Signature Activation Data management and Signature Activation Protocol(PP-SAD+SAP);
- ETSI EN 419 221-5 - Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- ETSI TS 119 312 – ESI Cryptographic Suites;
- ETSI TS 119 495 – ESI Sector Spesific Requirements: Qualifed Certificates Profiles and TSP Policy Requirements under the PSD2;
- ETSI TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

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

бул. „Цар Борис III" № 41
София 1612
„БОРИКА“ АД
телефон: 0700 199 10
имейл адрес: info@b-trust.org
Официална страница на доставчика: www.b-trust.org

ВЪВЕДЕНИЕ

Практиката при предоставяне на КУ и КУУ за тях от „БОРИКА“ АД съдържа описание на участниците в инфраструктурата на публични ключове B-Trust® и на нейните компоненти, чрез които Доставчика издава, поддържа, публикува и управлява КУ за КЕП/УЕП, облачен КЕП, КЕПечат/УЕПечат и автентичност на уебсайт. Описани са общите оперативни процедури при заявяване на КУ, идентифициране на Заявители, издаване и публикуване, доставяне и приемане на КУ, 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 КУ и КУУ за тях чрез инфраструктурата на B-Trust® в съответствие със ЗЕДЕУУ 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 ЗЕДЕУУ.

1 ОСНОВНИ ПОЛОЖЕНИЯ

1.1 Доставчик на квалифицирани удостоверителни услуги

1. „БОРИКА“ АД е юридическо лице - търговец, осъществяващо дейност на ДКУУ съгласно ЗЕДЕУУ и нормативната уредба.
2. PKI на „БОРИКА” АД е изградена и се управлява съгласно правната рамка на Регламент 910/2014 и ЗЕДЕУУ и в съответствие с международните спецификации и стандарти ETSI EN 319 411-1/5 и ETSI EN 319 412.
3. Доставчикът използва идентификатори на обекти (OID) в B-Trust PKI- инфраструктурата, формирани на база код 15862, присвоен на „БОРИКА“ АД от IANA в клона iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA –Registered Private Enterprise) и в съответствие със стандартите ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).
4. В качеството си на регистриран ДКУУ, „БОРИКА“ АД осъществява следните правно-регламентирани дейности по:
   - издаване на КУ:
     - приемане на искане за първоначално издаване;
     - установяване на идентичност и валидни данни за Потребителя;
     - предоставяне на услуги по създаване на двойки криптографски ключове - частен и публичен ключ
     - подписване на КУ с усъвършенстван електронен подпис/печат на ДКУУ;
     - запис на издадено КУ.
   - поддръжка и управление на КУ:
     - подновяване на издадено валидно КУ;
     - промяна в статуса на валидно КУ- спиране, възобновяване и прекратяване;
     - проверка на статуса на КУ;
     - проверка на статуса на КУ в реално време (OCSP статус).
   - водене на регистри:
     - водене на публичен регистър на всички издадени КУ;
     - публикуване на издадено КУ в публичния регистър;
     - водене на списък на всички прекратени КУ;
     - незабавно публикуване на прекратено КУ в списъка с прекратени удостоверения;
     - осигурява постоянен достъп на трети лица до публичния регистър и до списъка

на прекратени удостоверения.
- проверка (валидация) на електронни подписи.
- предоставяне на QSCD за (локално) генериране и съхранение на криптографски ключове и за създаване на КЕП – смарт карта/и.
- Предоставяне на RQSCD за генериране и съхранение на криптографски ключове при ДКУУ и за създаване на КЕП от разстояние (Облачен КЕП/ОКЕП).
- издаване на квалифицирани електронни времеви печати:
    - на представено съдържание на електронно подписан/подпечатан документ (време на подписване/подпечатване);
    - на цифрово съдържание в даден момент и непроменимост на съдържанието след този момент
    - доказателствена проверка на издадените квалифицирани електронни времеви печати.

5. Доставчикът предоставя посочените КУУ в съответствие с настоящата Практика на Удостоверяващия орган и посочената в удостоверението Политика.
6. 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.
7. Доставчикът може да публикува отделно общи условия за тези КУУ.

1.2 Регулация и контрол

1. Пълното наименование на този документ е „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS)“
2. „БОРИКА“ АД е уведомило КРС за започване на дейност като ДКУУ по реда на ЗЕДЕУУ и действащата нормативна уредба.
3. Акредитацията на „БОРИКА“ АД като ДКУУ по ЗЕДЕУУ 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.
4. Доставчикът уведомява Потребителите за своята акредитация при предоставяне на посочените КУУ в този документ.
5. В отношенията с Потребителите и трети лица е валидна само версията, която е актуална към момента на ползването на услугите на „БОРИКА“АД.
6. Този документ е публично достъпен на адрес: https://www.b-trust.bg/documents.
7. Практиката при предоставяне на КУУ е приложима за следните Политики на Доставчика:
    - Политика при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис/облачен електронен подпис/печат (B-Trust CP-eIDAS QES/CQES/QESeal);
    - Политика при предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис/печат (B-Trust CP-eIDAS AES/AESeal);
    - Политика при предоставяне на квалифицирани удостоверения за автентичност на уебсайт (B-Trust QCP-eIDAS QWAC);
    - Политика при предоставяне на квалифицирани удостоверения за електронен печат и за автентичност на уебсайт на Доставчици на платежни услуги (B-Trust QCP-PDS2 QSealC и QWebC).

    Тези политики изпълняват специфичните изисквания на удостоверителните политики, посочени в стандарта ETSI EN 319 411-2: QCP-n; QCP-n-qscd, QCP-l, QCP-l-qscd и QCP-w, които са базирани на общите изисквания в съответните политики NCP и NCP+ посочени в стандарта ETSI EN 319 411-1.

    Политиките на Доставчика за конкретните типове квалифицирани удостоверения са публикувани в отделни документи и са публично достъпни на адрес: https://www.b-trust.bg/documents.

1.3 Идентификатори в документа

1. Обектите в B-Trust инфраструктурата на „БОРИКА“ АД за издаване и поддръжка на квалифицираните удостоверенията се обозначават с идентификатори (OID - Object Identifier).
2. Квалифицираните удостоверения за подпис, печат и автентичност на уебсайт като обекти на инфраструктурата се идентифициран чрез идентификаторите на политики за тях, които могат да бъдат проверени в атрибута CertificatePolicies на тези удостоверения.
3. Идентификаторите на обекти в B-Trust са посочени в следната Таблица:

Обект	Идентификатор (OID)
BORICA AD	1.3.6.1.4.1.15862
B-Trust	1.3.6.1.4.1.15862.1
B-Trust Root Qualified CA	**1.3.6.1.4.1.15862.1.6**
B-Trust Operational Qualified CA	**1.3.6.1.4.1.15862.1.6.1**
B-Trust Personal qualified certificate QES	1.3.6.1.4.1.15862.1.6.1.1
B-Trust Professional qualified certificate QES	1.3.6.1.4.1.15862.1.6.1.2
B-Trust Organization qualified certificate QESeal	1.3.6.1.4.1.15862.1.6.1.3
B-Trust PDS	1.3.6.1.4.1.15862.1.6.2
B-Trust Qualified Time Stamp Authority	1.3.6.1.4.1.15862.1.6.3
B-Trust Qualified Time Stamp Authority PDS	1.3.6.1.4.1.15862.1.6.4
B-Trust Root Qualified OCSP Authority	1.3.6.1.4.1.15862.1.6.5
B-Trust Qualified OCSP Authority	1.3.6.1.4.1.15862.1.6.5.1
B-Trust Qualified Validation Service	1.3.6.1.4.1.15862.1.6.6
B-Trust Qualified Long-Terms Preservation Service	1.3.6.1.4.1.15862.1.6.7
B-Trust Remote QSCD (RQSCD)/Server Signing Service Component	1.3.6.1.4.1.15862.1.6.8
B-Trust Remote Signature Creation Service Component	1.3.6.1.4.1.15862.1.6.9
B-Trust Remote Video Identification Service Component	1.3.6.1.4.1.15862.1.6.10
B-Trust Root Advanced CA	**1.3.6.1.4.1.15862.1.7**
B-Trust Operational Advanced CA	**1.3.6.1.4.1.15862.1.7.1**
B-Trust Personal qualified certificate AES	1.3.6.1.4.1.15862.1.7.1.1
B-Trust Professional qualified certificate AES	1.3.6.1.4.1.15862.1.7.1.2
B-Trust Organization qualified certificate AESeal	1.3.6.1.4.1.15862.1.7.1.3
B-Trust Application qualified certificate	1.3.6.1.4.1.15862.1.7.1.4
B-Trust Domain Validation SSL qualified certificate (B-Trust DVC SSL)	1.3.6.1.4.1.15862.1.7.1.5
B-Trust Organization Validation SSL qualified certificate (B-Trust OVC SSL)	1.3.6.1.4.1.15862.1.7.1.6
B-Trust Organization qualified certificate AESeal PSD2	1.3.6.1.4.1.15862.1.7.1.7
B-Trust Organization Validation SSL qualified certificate PSD2	1.3.6.1.4.1.15862.1.7.1.8
B-Trust PSD2 PDS	1.3.6.1.4.1.15862.1.7.1.9
B-Trust Root Advanced OCSP Authority	1.3.6.1.4.1.15862.1.7.2
B-Trust Advanced OCSP Authority	1.3.6.1.4.1.15862.1.7.2.1

4. Практиката на Доставчика при издаване и поддържане на КУ се осъществява посредством следните оперативни УО:

Оперативен УО	**Идентификатор (OID)**
B-Trust Operational Qualified CA	1.3.6.1.4.1.15862.1.6.1
B-Trust Operational Advanced CA	1.3.6.1.4.1.15862.1.7.1

5. Политиките на Доставчика относно видовете КУ и предоставяните за тях КУУ се означават в издаваните КУ със следните идентификатори:

Квалифицирано удостоверение	Политика	Идентификатор на политика (OID)
B-Trust Personal qualified certificate QES (**Персонално КУКЕП** на физическо лице) B-Trust Personal Qualified certificate CQES (**Персонално КУ за облачен КЕП** на физическо лице)	B-Trust Personal qualified certificates Policy (QCP-n-qscd) (Политика на предоставяне на КУКЕП и КУ за облачен КЕП на физическо лице)	1.3.6.1.4.1.15862.1.6.1.1 (0.4.0.1456.1.1) (0.4.0.194112.1.2)
B-Trust Professional qualified certificate QES (**Професионално КУКЕП** на физическо лице, асоциирано с юридическо лице) B-Trust Professional qualified certificate CQES (**Професионално КУ за облачен КЕП** на физическо лице, асоциирано с юридическо лице)	B-Trust Professional qualified certificates Policy (QCP-n-qscd) (Политика на предоставяне на КУКЕП и КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице)	1.3.6.1.4.1.15862.1.6.1.2 (0.4.0.1456.1.1) (0.4.0.194112.1.2)
B-Trust Organization qualified certificate QESeal (**КУКЕПечат** на юридическо лице)	B-Trust Organization qualified certificates Policy (QCP-l-qscd) (Политика на предоставяне на КУКЕПечат на юридическо лице на B-Trust QSCD)	1.3.6.1.4.1.15862.1.6.1.3 (0.4.0.194112.1.3)
B-Trust Personal qualified certificate AES (**Персонално КУУЕП** на физическо лице)	B-Trust Personal qualified certificates Policy (QCP-n) (Политика на предоставяне на КУУЕП на физическо лице)	1.3.6.1.4.1.15862.1.7.1.1 (0.4.0.1456.1.2) (0.4.0.194112.1.0)
B-Trust Professional qualified certificate AES (**Професионално КУУЕП** на физическо лице асоциирано с юридическо лице)	B-Trust Professional qualified certificates Policy (QCP-n) (Политика на предоставяне на КУУЕП на физическо лице, асоциирано с юридическо лице)	1.3.6.1.4.1.15862.1.7.1.2 (0.4.0.1456.1.2) (0.4.0.194112.1.0)
B-Trust Organization qualified certificate AESeal (**КУУЕПечат** на юридическо лице)	B-Trust Organization qualified certificates Policy (QCP-l) (Политика на предоставяне на КУУЕПечат на юридическо лице)	1.3.6.1.4.1.15862.1.7.1.3 (0.4.0.1456.1.2) (0.4.0.194112.1.1)
B-Trust Domain Validation SSL qualified certificate (B-Trust DVC SSL) (**КУ за автентичност на уебсайт - домейн**)	B-Trust certificate for Domain Validation Certificate Policy (DVCP) (Политика на предоставяне на удостоверения за автентичност на уебсайт - домейн)	1.3.6.1.4.1.15862.1.7.1.5 (0.4.0.2042.1.6)
B-Trust SSL Organization Validation qualified certificate (B-Trust OVC SSL) (**КУ за автентичност на уебсайт - организация**)	B-Trust certificate for Organization Validation Certificate Policy (OVCP) (Политика на предоставяне на удостоверения за автентичност на уебсайт - организация)	1.3.6.1.4.1.15862.1.7.1.6 (0.4.0.2042.1.7)
B-Trust Organization qualified certificate AESeal PSD2 (B-Trust QSeal PSD2) (**КУПечат** на юридическо лице – платежна институция по PSD2)	B-Trust PSD2 Organization qualified certificates Policy (QCP-l) (Политика на предоставяне на КУУЕПечат на юридическо лице – платежна институция по PSD2)	1.3.6.1.4.1.15862.1.7.1.7 (0.4.0.1456.1.2) (0.4.0.194112.1.1)
B-Trust SSL Organization Validation qualified certificate PSD2 (B-Trust QWebC PSD2) (**КУ за автентичност на уебсайт –** организация–платежна институция по PSD2/КУУеб PSD2))	B-Trust certificate for PSD2 Organization Validation Certificate Policy (OVCP) (Политика на предоставяне на удостоверения за автентичност на уебсайт – организация – платежна институция по PSD2)	1.3.6.1.4.1.15862.1.7.1.8 (0.4.0.2042.1.7)

1.4 Участници в инфраструктурата на B-Trust®

1.4.1 Удостоверяващи органи

1. „Удостоверяващия орган“ на B-Trust® на ДКУУ „БОРИКА“ АД е организационно обособено звено, което осъществява дейност по издаване, по предоставяне и по поддържане на КУ и 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 и КУКЕПечат, 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 и КУКЕПечат, съгласно Политиката за предоставяне на тези КУ;
3. Инфраструктурата на B-Trust® има двустепенна йерархия на УО за издаване и поддръжка на КУУЕП, КУУЕПечат и КУ за автентичност на уебсайт, както следва:
   - Базов УО „B-Trust Root Advanced CA" - издава удостоверения на подчинените в йерархично отношение оперативни УО на Доставчика и такива на други Доставчици;
   - Оперативен УО „B-Trust Operational Advanced CA" - издава КУУЕП и КУУЕПечат, съгласно Политиките за предоставяне на тези КУ.
4. 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 КУ;
   - регистрира подадени искания до УО за издаване и внася промени в статуса на КУ;
   - 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;
   - уведомява УО да издаде КУ след успешна идентификация и заплатена услуга;
   - предава на Потребителя или на упълномощено от него лице издаденото КУ, съответстващо на генерирана двойка ключове;
   - приема или отхвърля регистрирани искания за поддръжка и управление на КУ;
   - сключва договори за предоставяне на удостоверителни и други криптографски, информационни и консултантски услуги с Потребителите от името на Доставчика.
2. Регистриращият орган осъществява гореизброените дейности:
   - в офис на органа като изисква физическо присъствие на заявител на КУ (присъствена идентификация, регистрация и издаване на КУ);
   - чрез отдалечена онлайн видео идентифкация на заявител (неприсъствена идентификация, регистрация и издаване на КУ за Облачен КЕП).
3. Политиката и Практиката на РО, който изпълнява дейностите по т.1 в офис на органа, са неделима част от настоящия документ.
4. Политиката и Практиката на РО, който изпълнява дейностите по т.1 чрез отдалечена онлайн видео идентификация са в отделен документ – „Политика и Практика при предоставяне на отдалечена видео идентификация за издаване на квалифицирани удостоверения за облачен КЕП от „БОРИКА“ АД“.
5. Регистриращият орган на Доставчика може да предоставя удостоверителни услуги на

Потребители в офис (присъствено) чрез Местни Регистриращи Служби (МРС).

6. 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.
7. Регистриращият орган (РО) на Доставчика може да предоставя удостоверителни услуги на Потребители чрез Местни Регистриращи Служби (МРС).
8. 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 Потребители. Правомощието се удостоверява пред Заявителите и всички трети лица с писмено или електронно удостоверение за РО/МРС.
9. В случаите, когато РО е самостоятелно юридическо лице, МРС към този орган се разкриват само след изрично одобрение от страна на Доставчика.
10. Отношенията между Доставчика и РО/МРСсе уреждат с договор.
11. 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 Потребители 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 КУ) доказване спрямо приемащата страна на факта на подписване/подпечатване на изявление или на електронен документ.
2. „B-Trust Qualified Time Stamp Authority " е УО за издаване на квалифицирани електронни времеви печати на Доставчика.
3. Електронният подпис на Доставчика на квалифицирания електронен времеви печат е със статус на квалифициран електронен печат.
4. Квалифицирани електронни времеви печати могат да се интегрират в процеса на създаване или приемане на подписи/печати към електронни документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и други.
5. Доставчикът разработва и публикува отделна Политика на УО за издаване на квалифицирани електронни времеви печати.

1.4.4 Квалифицирана услуга за валидиране на квалифицирани електронни подписи/печати

1. Квалифицираната услуга за валидиране на квалифицирани електронни подписи/печати (B-Trust QSVS) е обособено и неделимо звено към Доставчика, което осъществява следните дейности:
   - приема подписани/подпечатани файлове/е-документи с определени формати и профили на подпис/печат за валидиране;
   - валидира подписаните/подпечатани файлове/е-документи в съответствие с Регламент 910/2014 (чл. 32, 33 и 40);
   - изготвя и предоставя подпечатани от Доставчика статус(и) и отчет от валидиране на е-подпис(и)/печат(и) в приетите файлове/е-документи;
   - осигурява възможност за разпечатване (PDF формат) на хартия на авторизирания отчет от валидиране на подпис(ите)/печат(ите).
2. Услугата авторизира статуса и отчета от валидиране с квалифициран електронен печат

издаден от Доставчика.
3. Статусите на валидиране на квалифицирани е-подписи/печати могат да се интегрират в процеси на приемане на подписи/печати към електронни документи и електронни транзакции, при съхранение на подпис/печати, както и архивиране на електронни документи, в електронни нотариати и др.
4. Доставчикът разработва и публикува отделна Политика и Практика на услугата за квалифицирано валидиране на КЕП/КЕПечати.

1.4.5 Услуга за квалифицирано съхраняване на квалифицирани електронни подписи/печати

1. Услугата за квалифицирано съхраняване на квалифицирани е-подписи/печати (B-Trust QSPS) е обособено и неделимо звено към Доставчика, което осъществява следните дейности:
   - приема е-подписи/печати (подписани/подпечатани файлове/е-документи) с определени формати и профили на подпис/печат за съхранение;
   - сигурно съхранява подписаните/подпечатани файлове/е-документи в съответствие с Регламент 910/2014 (чл. 34 и 40);
   - изготвя и съхранява подпечатани от Доставчика доказателствени записи от съхраняване на е-подпис(и)/печат(и) в приетите файлове/е-документи;
   - изготвя по заявка уведомления след успешно съхраняване на файлове/е-документи с подпис(и)/печат(и);
   - осигурява възможност за авторизиран достъп, четене, модифициране и изтриване на съхранявани файлове/е-документи с подпис(и)/печат(и).
2. Услугата авторизира (доказателствени) записи и уведомления за съхраняване чрез квалифициран електронен печат издаден от Доставчика.
3. Доставчикът разработва и публикува отделна Политика и Практика на услугата за съхраняване на КЕП/КЕПечати.

1.4.6 Платформа за облачен КЕП

1. Платформата за облачен КЕП включва две части:
   - Отдалечена сървърна компонента RQSCD (софтуер и HSM) при Доставчика;
   - Мобилно приложение (B-Trust Mobile) в смартфона на Потребител.
2. RQSCD е обособена и неделима компонента в B-Trust инфраструктурата на Доставчика, която изпълнява следните дейности:
   - генерира двойка ключове за облачен КЕП в HSM при Доставчика по заявка на удостоверен от него Потребитетел
   - съхранява сигурно генерираната двойка ключове при Доставчика
   - активира от разстояние генериране на цифров подпис (PKCS#1)
   - генерира цифров подпис на Титуляр в HSM-а при Доставчика (Облачен КЕП)
   - предоставя на Титуляря генерирания подпис и съответстващото удостоверение за проверка на подписа
3. RQSCD получава заявките за издаване на облачен КЕП чрез РО/МРС на Доставчика след успешно удостоверен Заявител и регистрирано мобилно устройство (смартфон) на Заявителя на подпис.
4. RQSCD използва УО B-Trust Operational CA на Доставчика за да издава квалифицирано удостоверение, съответстващо на генерирания подпис от разстояние.
5. Мобилното приложение B-Trust Mobile в смартфона на Потребителя служи да активира генерирането на цифров подпис за Облачен КЕП в HSM-а на RQSCD само след удостоверен персонален контрол на частния ключ на подписа чрез строга автентификация на Титуляря и въведен от него ПИН (код за активиране) чрез мобилното устройство

(смартфона).

6. Предоставените от Платформата цифров подпис и съответстващо квалифицирано удостоверение на Облачния КЕП могат да се интегрират в контейнера на подписани документи с Облачен КЕП от услуга за подписване, оперирана от Доставчика или от външна такава (при Потребител/Доверяваща се страна).

   Платформата за Облачен КЕП „премества“/виртуализира физическата смарт карта (локално QSCD) за КЕП на Титуляря в HSM на RQSCD при ДКУУ. В RQSCD се алокира ‚виртуален слот‘ като отдалечен ресурс на Титуляря с еквивалентни криптографски параметри и характеристики на смарт картата (локално QSCD.

1.4.7 OCSP сървър

1. „OCSP сървър" е обособено и неделимо звено на УО, което осъществява дейности на Доставчика както следва:
   - приема заявки от Потребители 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", съответно „B-Trust Root Advanced OCSP Authority" и „B-Trust Advanced OCSP Authority".
3. Всяка доверяващата се страна, когато приема КУ, може да заяви проверка на статуса на удостоверенията в реално време.
4. Проверката на статуса на КУ в реално време не е задължителна за Доверяващите се страни, но Доставчикът препоръчва да се използва тази услуга и нейното интегриране при създаване или приемане на електронно подписани/подпечатани документи и при проверка на автентичността на уебсайт в електронни транзакции.

1.4.8 Потребител

1. Потребителите са физически или юридически лица, които са подали искане и след успешно завършване на процедурата им се издава квалифицирано удостоверение. Преди да бъде извършена проверка и да бъде издадено квалифицирано удостоверение, Потребителят е само Заявител за квалифицирани услуги на B-Trust.
2. Отношенията между „БОРИКА“ АД като ДКУУ и Потребител се уреждат с писмен договор.

1.4.8.1 Титуляр

1. „Титуляр" е Потребител-физическо лице на КУКЕП/КУУЕП или на КУ за облачен КЕП, 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/КУУЕП и КУ за облачен КЕП може да се посочи и лицето, което Титулярят представлява.
4. Единствено Титулярят на КУКЕП/КУУЕП и КУ за облачен КЕП, има право на достъп до частния ключ за подписване на електронни изявления.

1.4.8.2 Създател

1. „Създател“ е Потребител-юридическо лице, което създава електронен печат, данните на което са удостоверени в КУ, използвано за проверка на електронния печат. Създателят може да бъде само юридическо лице.

2. „Юридически лица“ по смисъла на Договора за функционирането на Европейския съюз (ДФЕС) означава всички образувания, учредени или регламентирани съгласно правото на държава членка, независимо от тяхната правна форма.
3. Електронният Печат не е подпис на юридическото лице и служи само да удостовери източника и целостта на подпечатан електронен документ или изявление.
4. Когато юридическо лице използва електронен печат, препоръчва се да бъде установен вътрешен контролен механизъм при юридическото лице, позволяващ само на физическо лице, упълномощено от това юридическо лице („Създател“) да създава печата (например, да „натисне“ бутон за (автоматично) създаване на електронни печати).
5. В КУ за електронен печат може да се посочи физическото лице, което представлява „Създателя“.
6. Единствено, това физическо лице има право на достъп до частния ключ за генериране на печата.
7. Когато за дадена трансакция се изисква квалифициран електронен печат от юридическо лице, квалифицираният електронен подпис на упълномощения представител на юридическото лице се приема равностойно.

1.4.9 Доверяващи се страни

1. „Доверяващи се страни" са адресатите на подписани/подпечатани електронни изявления и документи от Потребители, които притежават издадени от Доставчика КУ или крайни клиенти, които адресират уебсайтове, за които са издадени удостоверения от Доставчика.
2. Доверяващите се страни следва да имат познания и умения относно използването на КУ и се доверяват на удостоверените обстоятелства в тях само с оглед на приложимата Политика, особено по отношение на нивото на сигурност при проверка на Потребителите на тези КУ.
3. Доверяващите се страни имат постоянен достъп до регистрите на Доставчика за проверка на валидността на КУ, за установяване на съответните Потребители 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 Потребителя и публичния му ключ в КУ, съответстващ на частния ключ на този Потребител и служи за проверка на подписа/печата в електронни документи и обекти или за проверка на автентичността на уебсайт.
2. КУ могат да се използват за дейности, които изискват подписване на електронни документи, автентификация на Потребител или уебсайт, както и за криптиране на данни при електронни транзакции, изискващи най-високо или значително ниво на сигурност.
3. Само удостоверенията с означените в този документ политики, които издава Доставчикът, имат характер на КУ.

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 ЗЕДЕУУ 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 както следва:

B-Trust Root Qualified CA

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

B-Trust Root Advanced CA

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	01
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust

	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-24T18:55:40Z
Validity to	-	2037-04-24T18:55:40Z
Subject	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
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-TrustRootACA.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)	-	ba 11 d6 ad 94 b2 4f c9 16 11 3a f6 82 cd 76 2a b3 bf d7 75
Thumbprint (Sha256)	-	fb 2c 73 6f 3c f1 ad 7c 89 ec 36 e8 60 c9 0c d6 be 87 f7 0d 66 09 8e 0a cc d5 4a 49 ea fa 2c a9

3. На основание Регламент 910/2014 електронните печати на Доставчика, които са придружени от базовите му удостоверения са квалифицирани.
4. Доставчикът може да инсталира и поддържа други базови удостоверения в инфраструктурата на B-Trust.

Оперативни удостоверения на Доставчика

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

B-Trust Operational Qualified CA

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	69 0e 4f b7 9a ed 13 94
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	-	2018-06-01T16:44:50Z
Validity to	-	2033-05-31T16:44:50Z
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=1.3.6.1.4.1.15862.1.6.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.2 [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3
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)	-	ad 4c 92 43 9a 5b 83 28 13 1e b8 45 65 d1 46 2b f0 3d 3d 55
Thumbprint (Sha256)	-	49 9a 9c a8 b4 7e e8 44 37 f9 0b 96 fb 40 41 3e a2 93 f9 b3 94 2a 16 08 37 a0 c6 7b 0e c5 ba 0c

B-Trust Operational Advanced CA

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	55 6c c1 9f 35 f1 95 ca
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	O =	BORICA AD
	C =	BG
Validity from	-	2018-06-01T16:29:34Z
Validity to	-	2033-05-31T16:29:34Z
Subject	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
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=1.3.6.1.4.1.15862.1.7.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.1 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.2 [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.3 [5]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.4 [6]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.5 [7]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6 [8]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.7 [9]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.8
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustRootACA.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)	-	2d 11 f1 fb 79 b9 46 0a d5 e7 04 bf 36 18 8d a6 b6 e8 d8 c4
Thumbprint (Sha256)	-	e7 42 69 82 c0 26 4b 78 6b 94 25 ce 45 f3 63 58 7f 34 83 4f a3 4a 6a 7f fd d5 05 67 41 76 ad 0d

3. На основание Регламент 910/2014 електронните печати на Доставчика, които са придружени от тези оперативни удостоверения са квалифицирани.
4. Доставчикът може да инсталира и поддържа други оперативни удостоверения в инфраструктурата на B-Trust.

Удостоверения на OCSP сървъри на Доставчика

B-Trust Root Qualified OCSP Authority

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

B-Trust Qualified OCSP Authority

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

B-Trust Root Advanced OCSP Authority

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	03
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:31:30Z
Validity to	-	2022-04-26T14:31:30Z
Subject	CN =	B-Trust Root Advanced 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	-	0a fe c2 5d 35 50 0a e1 00 2a c9 a7 09 2a 0a 4c f0 c5 cf 41
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
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-TrustRootACA.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-TrustRootACAOCSP.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)		34 0a 07 e7 9a 27 88 3f 55 a6 0a 84 85 02 a7 62 98 96 c2 6a
Thumbprint (Sha256)		01 86 c1 46 66 50 68 b5 17 81 62 c5 c8 55 9b ab 67 06 6c c0 17 ca 12 5f 00 1e f4 38 f6 90 0b f3

B-Trust Advanced OCSP Authority

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	29 B9 27 00
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:36:08Z
Validity to	-	2022-04-26T14:36:08Z
Subject	CN =	B-Trust Advanced 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	-	30 9c f5 49 43 6c af 46 3d 6f eb 5e ad 2e 55 06 de f6 30 de
Authority Key Identifier	KeyID =	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef
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-TrustRootACA.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-TrustOperationalACAOCSP.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)		0c 88 77 18 0e 60 d2 a9 37 f5 45 28 35 b2 cf 2f 30 d1 99 01
Thumbprint (Sha256)		0d 0b 59 a0 6b 13 8d ca b2 bc 11 d7 b9 e4 09 1e 95 52 01 26 6e c8 33 a4 7e 0e b0 c7 9a f9 e2 4f

1. Удостоверението на OCSP сървъра на Доставчика „B-Trust Root Qualified OCSP Authority" е КУ за неговия публичен ключ, 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 от проверката в реално време на статуса на представени КУ, издадени от УО „B-Trust Root Qualified CA".
2. Удостоверението на OCSP сървъра на Доставчика „B-Trust Qualified OCSP Authority" е КУ

на неговия публичен ключ, 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 от проверката в реално време на статуса на представени КУ, издадени от УО “B-Trust Operational Qualified CA".

3. Удостоверението на OCSP сървъра на Доставчика „B-Trust Root Advanced OCSP Authority" е КУ за неговия публичен ключ, подпечатано с базовия частен ключ на УО „B-Trust Root Advanced CA“ на Доставчика. С частния ключ на двойката ключове на OCSP сървъра „B-Trust Root Advanced OCSP Authority" Доставчикът подпечатва резултата от проверката в реално време на статуса на представени КУ, издадени от УО „B-Trust Root Advanced CA”
4. Удостоверението на OCSP сървъра на Доставчика „B-Trust Advanced OCSP Authority" е КУ на неговия публичен ключ, подпечатано с частния ключ на оперативния УО “B-Trust Operational Advanced CA" на Доставчика. С частния ключ на двойката ключове на OCSP сървъра „B-Trust Advanced OCSP Authority" Доставчикът подпечатва резултата от проверката в реално време на статуса на представени КУ, издадени от УО “B-Trust Operational Advanced CA".
5. Електронните печати на Доставчика, които са придружени от служебните удостоверения на OCSP сървърите на Доставчика са КЕПечати.

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 ЗЕДЕУУ, 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 ЗЕДЕУУ .
2. Издаването на тези удостоверения се осъществява на базата на конкретна договореност със съответните доставчици.
3. Удостоверението на УО „B-Trust Qualified Time Stamp Authority“ е представено в отделен документ „Политика и Практика за предоставяната от „БОРИКА“ АД квалифицирана услуга за издаване на квалифицирани електронни времеви печати“ на този орган.

1.5.4 Квалифицирани удостоверения за Потребители и приложимост

1.5.4.1 Квалифицирани удостоверения за квалифициран електронен подпис

1. Доставчикът издава КУКЕП и КУ за облачен КЕП в зависимост от Потребителите, приложното поле и предназначение на електронния подпис, както следва:
   - Персонално КУКЕП „B-Trust Personal Qualified Certificate QES";
   - Персонално КУ за облачен КЕП „B-Trust Personal Qualified Certificate CQES”;
   - Професионално КУКЕП „B-Trust Professional Qualified Certificate QES";
   - Професионално КУ за облачен КЕП „B-Trust Professional Qualified Certificate CQES”.
2. Практиката и Политиката на Доставчика за тези КУ определят процедурите, формата и изискванията за сигурност, приложими при издаване и използване на КУКЕП и КУ за облачен КЕП. Съответните Политики и профилите на КУ за КЕП и за облачен КЕП са еднакви.
3. Доставчикът издава КУКЕП и КУ за облачен КЕП само на Потребители - физически лица.
4. Персонално КУКЕП „B-Trust Personal Qualified Certificate QES" и КУ за облачен КЕП „B-Trust Personal Qualified Certificate CQES" се издава персонално на физическо лице (Титуляр).
5. Професионално КУКЕП „B-Trust Professional Qualified Certificate QES" и КУ за облачен КЕП „B-Trust Personal Qualified Certificate CQES" се издава на физическо лице (Титуляр), представляващо 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 Потребителя изисква лично присъствие или изрично упълномощаване от страна на Потребителя-Титуляр. Проверява се и идентичността на представляваното лице, респективно на упълномощеното физическо лице (ако има такова). Идентификационната процедура и процедурите при генериране на двойката ключове, при издаване и предоставяне на КУКЕП и КУ за облачен КЕП на Потребителя гарантират най-високо ниво на сигурност на удостоверените данни 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 генерират, съхраняват и предоставят на Потребителя-Титуляр задължително на B-Trust QSCD.
8. КУ за облачен КЕП „B-Trust Personal Qualified Certificate CQES" и „B-Trust Professional Qualified Certificate CQES" и съответстващите им частни ключове се генерират, съхраняват и ползват от Потребителя-Титуляр задължително на HSM в RQSCD на платформата за облачен КЕП на Доставчика
9. Срокът на валидност на КУКЕП и КУ за Облачен КЕП е 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за КУУ.

1.5.4.2 Квалифицирани удостоверения за усъвършенстван електронен подпис

1. Доставчикът издава два вида КУУЕП в зависимост от Потребителите, приложното поле и предназначение на електронния подпис, както следва:
   - персонално КУУЕП „B-Trust Personal Qualified Certificate AES";
   - професионално КУУЕП „B-Trust Professional Qualified Certificate AES".
2. Практиката и Политиката на Доставчика за тези КУ определят процедурите, формата и изискванията за сигурност, приложими при издаване и използване на КУУЕП.
3. Доставчикът издава КУУЕП само на Потребители - физически лица.
4. Персонално КУУЕП „B-Trust Personal Qualified Certificate AES" се издава персонално на физическо лице (Титуляр).
5. Професионално КУУЕП „B-Trust Professional Qualified Certificate AES" се издава на физическо лице (Титуляр), представляващо юридическо лице по силата на закона или упълномощаване.
6. Искането за регистрация и издаване на тези КУУЕП се прави отдалечено (по електронен способ) или локално (на място) в РО/МРС, като процедурата по идентификация чрез установяване на самоличността на Потребителя изисква лично присъствие или изрично упълномощаване от страна на Потребителя-Титуляр. Проверява се и идентичността на представляваното лице, респективно на упълномощеното физическо лице (ако има такова). Идентификационната процедура и процедурите при генериране на двойката ключове при издаване и предоставяне на КУУЕП на Потребителя гарантират значително ниво на сигурност на удостоверените данни в удостоверението и връзката им с публичния ключ.
7. КУУЕП „B-Trust Personal Qualified Certificate AES" и „B-Trust Professional Qualified Certificate AES" и съответстващите им частни ключове се генерират чрез специализиран, утвърден от Доставчика софтуер и се съхраняват и предоставят на Потребителя-Титуляр на софтуерен токън B-Trust SCT (PKCS#12 криптофайл).
8. Срокът на валидност на КУУЕП е 1(една) година, считано от датата на издаване.

1.5.4.3 Квалифицирано удостоверение за електронен печат

1. Доставчикът издава два вида КУЕПечат в зависимост от приложното поле и предназначение на електронния печат, както следва:
   - Квалифицирано удостоверение за квалифициран ЕПечат “B-Trust Organization Qualified

Certificate QESeal” (КУКЕПечат);
- Квалифицирано удостоверение за усъвършенстван Печат „B-Trust Organization Qualified Certificate AESeal” (КУУЕПечат);

2. Практиката и Политиката на Доставчика за тези КУ определят процедурите, формата и изискванията за сигурност, приложими при издаване и използване на КУЕПечат.
3. Доставчикът издава КУЕПечат само на Потребител–юридическо лице (Създател).
4. Искането за регистрация и издаване на тези КУЕПечат се прави отдалечено (по електронен способ) или локално (на място) в РО/МРС, като процедурата по идентификация чрез установяване на самоличността на Потребителя изисква лично присъствие или изрично упълномощаване от страна на Потребителя-Създател. Проверява се и идентичността на юридическото лице, респективно на упълномощеното физическо лице (ако има такова). Идентификационната процедура и при издаване и предоставяне на КУЕПеат на Потребителя гарантират най-високо ниво на сигурност на удостоверените данни в удостоверението и връзката им с публичния ключ.
5. Процедурата при генериране на двойката ключове за КУКЕПечат използва B-Trust QSCD и гарантира най-високо ниво на сигурност. Частният ключ се съхранява и предоставят на Създателя задължително на B-Trust QSCD.
6. Процедурата при генериране на двойката ключове за КУУЕПечат използва специализиран софтуер, утвърден от Доставчика и гарантира значително ниво на сигурност. Частният ключ се съхранява и предоставя на Създателя на B-Trust SCT (PKCS#12 криптофайл).
7. КУЕПечат няма значението на електронен подпис и се използва само да автентифицира източника и интегритета на електронния документ или изявление.
8. КУЕПечат могат да се използват още при защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и онлайн транзакции изискващи най-високо или значително ниво на сигурност.
9. Срокът на валидност на КУКЕПечат е 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за КУУ.
10. Срокът на валидност на КУУЕПечат е 1(една) година, считано от датата на издаване и се определя в договора за КУУ.
11. В съответствие с Регламент 910/2014 ЕС, КУЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. Когато за дадена трансакция се изисква квалифициран електронен печат от юридическо лице, квалифицираният електронен подпис на упълномощения представител на юридическото лице се приема равностойно.

1.5.4.4 Квалифицирано удостоверение за автентичност на уебсайт

1. Доставчикът издава квалифицирани удостоверения за автентичност на уебсайт, както следва:
   - Квалифицирано удостоверение за автентичност на уебсайт (домейн) „B-Trust Domain Validation SSL Certificate” (B-Trust DVC SSL);
   - Квалифицирано удостоверение за автентичност на уебсайт (организация) „B-Trust Organization Validation SSL Certificate” (B-Trust OVC SSL).
2. Политиката на Доставчика за тези удостоверения определя процедурата, формата и изискванията за сигурност, приложими при издаване и използване на удостоверенията за автентичност.
3. Доставчикът издава удостоверения за автентичност на уебсайт на Потребител–физическо или юридическо лице.
4. Искането за регистрация и издаване на тези удостоверения се прави отдалечено (по електронен способ) или локално (на място) в РО/МРС, като процедурата по идентификация чрез установяване на самоличността на физическото и/или на юридическото лице изисква лично присъствие или изрично упълномощаване от страна на Потребителя. Проверява се и идентичността на юридическото лице, респективно на упълномощеното физическо лице

(ако има такова) и се изпълнява проверка на представените данни за наименование на домейн, изискуеми елементи за адреса и регистрационен номер (в публичните регистри). Идентификационната процедура при издаване и предоставяне на удостоверение за автентичност на уебсайт гарантират високо или значително ниво на сигурност на удостоверените данни в удостоверението и връзката им с публичния ключ.

7. Процедурата при генериране на двойката ключове за КУ B-Trust DVC SSL и B-Trust OVC SSL използва специализиран софтуер, утвърден от Доставчика и гарантира значително ниво на сигурност. Частният ключ се съхранява и предоставя на Потребителя на преносим софтуерен токън (PKCS#12 криптофайл).
8. Срокът на валидност на КУ B-Trust DVC SSL и B-Trust OVC SSL е 1(една) или 825 дни, считано от датата на издаване и се определя в договора за удостоверенията.
9. Удостоверение B-Trust DVC SSL служи да идентифицира притежателя на домейна, който хоства уебсайта, като гарантира значително ниво на сигурност за клиента с браузъра. Това удостоверение може да съдържа „Wildcard” (*) за името на хоста (например, *.b-trust.bg). Издава се в съответствие с политика DVCP в ETSI EN 319 411-1.
10. Удостоверение B-Trust OVC SSL служи да идентифицира притежателя на домейна и акредитацията на организацията, като гарантира значително ниво на сигурност за клиента с браузъра, че сайта който достъпва принадлежи на организацията, идентифицирана в удостоверението. Това удостоверение може да съдържа „Wildcard” (*) за името на хоста (например, *.b-trust.bg). Издава се в съответствие с политиката OVCP в ETSI EN 319 411-1.

1.5.4.5 Квалифицирани удостоверения за Доставчици на платежни услуги

1. Доставчикът издава квалифицирани удостоверения на Доставчици на платежни услуги по PSD2, както следва:
   - КУПечат PSD2 (QSealC PSD2) - Квалифицирано удостоверение за Електронен Печат (на платежна институция) за PSD2;
   - КУУеб PSD2 (QWebC PSD2) Квалифицирано удостоверение за автентичност на уебсайт (на платежна институция) за PSD2.

Тези удостоверения имат характер на квалифицирани удостоверения по смисъла на Регламент 910/2014.

2. Политиката на Доставчика за тези удостоверения определя процедурата, формата и изискванията за сигурност, приложими при издаване и използване на удостоверенията от Доставчиците на платежни услуги.
3. Доставчикът издава тези квалиифицирани удостоверения само на Потребители-юридически лица, които са Доставчици на платежни услуги по PSD2.
4. За издаване на тези удостоверения се изисква лично присъствие пред РО/МРС в B-Trust на „БОРИКА“ АД на упълномощено от Доставчика на платежната услуга физическо лице за проверка на идентичността на юридическото лице и на самоличността на упълномощеното от него лице.
5. Процедурата по идентификация в РО/МРС включва представяне на доказателства за идентичността и авторизацията на Доставчика на платежните услуги и на идентичността на упълномощеното лице и тяхната проверка.
6. Доставчик на платежна услуга може сам да генерира двойката ключове за съответното удостоверение като използва утвърден от „БОРИКА“ АД или друг лицензиран софтуер с еквивалентно ниво на сигурност, който е съвместим с инфраструктурата на B-Trust.
7. Когато двойката ключове се генерира в „БОРИКА“ АД, издадените удостоверения на Доставчика на платежна услуга, удостоверяващи публичните ключове съответстващи на частните такива, се записват в преносими криптографски софтуерени токъни (PKCS#12) заедно със служебните удостоверения на ДККУ и се предоставят на Доставчика на платежната услуга.
8. Срокът на валидност на квалифицираните удостоверения на Доставчици на платежни

услуги по PSD2 съответства на срока на валидност на съответните стандартни квалифицирани удостоверения за печат и автентичност на уебсайт (организация).

1.5.5 Предназначение на квалифицираните удостоверения за Потребители

1. Издадените от Доставчика КУ на Потребители се използват по предназначение съобразно съответните Политики за тези удостоверения. Доставчикът има обща (еднаква) Политика за КУКЕП и за КУ за облачен КЕП.
2. Всяко КУ 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/подпечатване на електронно изявление или на съдържание и неговата проверка;
   - да автентифицира Потребителя като Титуляр на подписа или да автентифицира източника (Създателя) и интегритета на подпечатаните данни и на изявлението;
   - неотменимост (nonRepudiation) - да осигури възможност за последващо доказване спрямо Потребителя на факта на подписване/подпечатване на електронно изявление или на съдържание и на невъзможност за отказ от положения електронен подпис/печат;
   - криптиране на ключове (keyEncipherment) - да криптира и/или декриптира ключове, използвани при шифроване на данни;
   - криптиране на данни (dataEncipherment) - да криптира и/или декриптира данни.
3. Чрез реквизит „Extended Key Usage" в съответствие с RFC 5280, който също може да се съдържа в издаваните от Доставчика КУ, се детайлизира приложимостта на удостоверението с оглед предназначението му.
4. Издаваните квалифицирани удостоверения на Доставчици на платежни услуги съдържат атрибути със специфични данни, които се изискват от PSD2 (използват се атрибути „QCStatement“ и „organizationIdentifier“).

5. КУКЕП и КУ за облачен КЕП има значението на саморъчен подпис спрямо всички по смисъла на чл.13, ал.3 на ЗЕДЕУУ и идентифицира Потребителя като Титуляр на КЕП. КУКЕП и КУ за облачен КЕП може да се използва още при защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и онлайн транзакции изискващи най-високо ниво на сигурност
6. КУУЕП няма значението на саморъчен подпис спрямо всички по смисъла на чл.13, ал.3 на ЗЕДЕУУ, но идентифицира Потребителя като Титуляр на УЕП.
7. КУУЕП могат да се използват още при защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и онлайн транзакции изискващи значително ниво на сигурност.
8. В съответствие с Регламент 910/2014 ЕС, КУЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. КУЕПечат служи само да автентифицира източника (Създателя) и интегритета на подпечатани електронни документи или изявления.
9. Освен при удостоверяването на автентичността на документ, издаден от юридическо лице, електронните печати могат да се използват за удостоверяване на автентичността на цифровите активи на юридическо лице, като софтуерен код или сървъри.
10. Квалифицираното удостоверение за автентичност на уебсайт дава възможност да се установи автентичността на уебсайт, като го свързва с физическото или юридическото лице, на което ДКУУ е издал удостоверението в съответствие с изискванията на Регламент (ЕС) № 910/2014.
11. Квалифицираните удостоверения на Доставчиците на платежни услуги са с приложно поле, съответстващо на приложното поле на съответните квалифицирани удостоверения с общо предназначение.

12. Приложното поле на издаваните от Доставчика типове КУ е както следва:

Квалифицирано удостоверение	Приложно поле
Персонално КУКЕП на физическо лице „B-Trust Personal Qualified Certificate QES" Персонално КУ за облачен КЕП на физическо лице „B-Trust Personal Qualified Certificate CQES"	Персонална идентичност на Потребителя като Титуляр на КЕП/облачен КЕП 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 ЗЕДЕУУ.
Професионално КУКЕП на физическо лице „B-Trust Professional Qualified Certificate QES" Професионално КУ за облачен КЕП на физическо лице „B-Trust Professional Qualified Certificate CQES"	Професионална идентичност на Потребителя като Титуляр на КЕП/облачен КЕП 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 ЗЕДЕУУ.
Персонално КУУЕП на физическо лице „B-Trust Personal Qualified Certificate AES“	Персонална идентичност на Потребителя като Титуляр на УЕП в приложения, изискващи значително 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 ЗЕДЕУУ.
Професионално КУУЕП на физическо Лице „B-Trust Professional Qualified Certificate AES"	Професионална идентичност на Потребителя като Титуляр на УЕП в приложения, изискващи (достатъчно) 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 ЗЕДЕУУ.
КУКЕПечат на юридическо лице „B-Trust Organization Qualified Certificate QESeal”	Електронна автентификация на източника и на интегритета на електронни документи и изявления в публични и бизнес електронни транзакции (в смисъл на „електронен офис“ на юридически лица), изискваща най-високо ниво на сигурност. Освен при удостоверяването на автентичността на документ, издаден от юридическо лице, електронните печати могат да се използват за удостоверяване на автентичността на цифровите активи на юридическо лице, като софтуерен код или сървъри. Когато за дадена транзакция се изисква квалифициран електронен подпис на юридическо лице, квалифицираният електронен подпис на упълномощения представител на юридическото лице се приема равностойно.
КУУЕПечат на юридическо лице „B-Trust Organization Qualified Certificate AESeal”	Електронна автентификация на източника и на интегритета на електронни документи и изявления в публични и бизнес електронни транзакции (в смисъл на „електронен офис“) на юридически лица, изискваща значително ниво на сигурност. Освен при удостоверяването на автентичността на документ, издаден от юридическо лице, електронните печати могат да се използват за удостоверяване на автентичността на цифровите активи на юридическо лице, като софтуерен код или сървъри. Когато за дадена транзакция се изисква квалифициран електронен подпис на юридическо лице, квалифицираният електронен подпис на упълномощения представител на юридическото лице се приема равностойно.
КУ за автентичност на уебсайт (домейн) “B-Trust Domain Validation qualified certificate”	Идентифицира притежателя на домейна, който хоства уебсайта, като гарантира значително ниво на сигурност за клиента с браузъра.
КУ за автентичност на уебсайт (организация) “B-Trust Organization Validation qualified certificate”	Идентифицира притежателя на домейна и акредитацията на организацията, като гарантира със значително ниво на сигурност за клиента с браузъра, че сайта който достъпва принадлежи на организацията, идентифицирана в удостоверението. Криптиране на комуникацията между клиента и уебсайта (TSL/SSL протокол).

1.5.5.1 Ограничение на удостоверителното действие

1. Ако КУ се издава с ограничение на удостоверителното действие, Практиката на Доставчика допуска да се вписва в удостоверението ограничение по отношение на цели и/или стойност на сделки между Потребители и Доверяващи се страни при използване на електронен подпис.
2. Доставчикът задължително използва реквизит "Qualified Statements" в КУ.
3. Ограничителното действие на издадени КУ по отношение на стойността на сделките, които Потребителите сключват посредством използване на електронен подпис, се съгласува между тях и всяка Доверяваща се страна и е извън обхвата на настоящия документ.
4. В съответствие с Регламент 910/2014 ЕС, КУЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. КУЕПечат служи само да автентифицира източника и интегритета на подпечатани електронни документи или изявления (в смисъла на „електронен” офис/организация).

1.5.5.2 Употреба на удостоверения извън приложното поле и ограниченията

1. Когато Потребител или Доверяваща се страна използват и се доверяват на КУ 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 на Доставчика

1. Практиката на Доставчика подлежи 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. 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.: 0700 199 10

2 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР

2.1 Публичен регистър

1. Доставчикът води електронен Публичен регистър, в който публикува всички издадени КУ на Потребители и актуален Списък на прекратените КУ (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. Потребител на КУ, издадено от Доставчика, 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 КУ. 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 КУ до момента на публикуването му в регистъра. Спряно удостоверение се поддържа в CRL за период от време, регламентиран от ЗЕДЕУУ 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:
   - Публични Декларации на Доставчика (PDS);
   - Практика при предоставяне на КУ и КУУ;
   - Политики при предоставяне на КУ и КУУ за тях;
   - Договор за КУУ;
   - Тарифа на предоставяните КУУ;
   - Правила за издаване на КУ;
   - Условия и ред за използване на КУ, включително изискванията за съхраняване на частния ключ;
   - Документи, изискуеми при първоначално издаване на КУ, при подновяване и спиране/прекратяване на КУ;
   - Други документи, изискуеми по ЗЕДЕУУ 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.
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 Политиките и Практиката, както и на други съпътстващи документи по ЗЕДЕУУ, се осъществява незабавно.

2.5 Достъп до Регистъра и до хранилището

1. Доставчикът води Публичен регистър на издадените удостоверения, който е онлайн 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 Политиките 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 КУ;
   - осъществява проверка за установяване на самоличността на Потребителя 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 Потребителя.
3. Автентификацията/идентификацията на Потребителя след регистрация и преди да бъде издадено КУ, 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 КУ 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 и/или юридическото лице.

3.1 Именуване

3.1.1 Използване на имена

1. КУ са с формат, съответстващ на стандарта X.509. РО/МРС, работещ от името на Доставчика утвърждава, че имената в заявките за удостоверения съблюдават стандарта X.509.
2. Полето „Subject" в удостоверението електронно идентифицира Потребителя, свързан с публичния ключ в КУ.
3. Името и други индивидуализиращи белези на Потребителя 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 полета "Subject" и "Issuer" атрибут DN формиращ неговото уникалното име.
5. Детайлна спецификация на издаваните КУ се съдържа в съответните документи за Политики на Доставчика за тези удостоверения.

3.1.2 Използване на псевдоним

1. Доставчикът може да издава КУ като използва „псевдоним", за да именува Потребителя само след като РО/МРС събере необходимата информация за самоличността му и успешно го идентифицира.
2. Не се допуска използване на „псевдоним” в КУ за електронен печат, за да се именува Създателя на печата.

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. КУ съдържат имена, съвпадащи с автентифицираните идентификационни имена на Потребителите, субекти на тези удостоверения.
3. За по-удобна електронна комуникация с Потребител, Доставчикът изисква и удостоверява в КУ негов имейл адрес. 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 КУ информация за електронна идентификация на Потребители, която е успешно проверена и потвърдена от РО/МРС, въз основа на представените документи за самоличност.
2. Във всички удостоверения, в които се вписва Потребителя, полето за обичайно име (Common Name, CN) съдържа име на физическото или юридическо лице, с което то е обичайно обозначавано в дейността си.
3. В професионалното удостоверение, атрибутът за уникално име (DN) съдържа информация и за идентичността на лицето, което Потребителя представлява.
4. В удостоверението за юридическо лице, атрибутът за уникално име (DN) съдържа информация и за идентичността на упълномощения представител на юридическото лице.

3.1.5 Уникалност на имената

1. Електронната идентификация на Потребителя на издадено от Доставчика КУ е на базата на DN.
2. Полето "Subject" в удостоверението се формира от информацията за Потребителя, която се предоставя онлайн 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 Потребителя в домейна B-Trust чрез добавяне на реквизит, който гарантира такава уникалност.
4. Потребител с уникален DN в домейна B-Trust може да има повече от едно издадени действителни КУ.
5. Всяко издадено удостоверение има уникален сериен номер ("SerialNumber") в обхвата на съответния УО на Доставчика. 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. Потребителят 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 Потребителя на КУ, Доставчикът изисква регистрирано искане за първоначално издаване на удостоверението.
2. Заявител/потребител на КУ за облачен КЕП трябва да има мобилно устройство със заредено мобилно приложение B-Trust Mobile за Android или за iOS.
3. Искането за първоначално издаване на КУ пред РО/МРС на Доставчика е процедура, чрез която Доставчикът изисква, събира и получава необходима информация за идентификация на Потребителя в удостоверението както и идентификационни данни за мобилното устройство/мобилното приложение.
4. Процедурата по регистрация включва:
   - попълване на регистрационна форма за издаване на КУ;
   - 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 КУ;
- възможност за заявяване на други услуги, свързани с издаваното удостоверение.

5. Установяването на самоличността на Потребителя след регистрация и преди издаване на заявеното КУ изисква лично присъствие на Потребителя или на упълномощен негов представител в РО/МРС. С цел предотвратяване на неоторизирано използване на услугите, и с оглед осигуряване на възможност за проверка на автентичността на данните, предоставени от Потребителя, както и предвид разпоредбата на чл. 24, пар. 1, т. „в“, съгласно който проверка на самоличността на лицето, на което се издава квалифицирано удостоверение, може да бъде проверена чрез удостоверение за квалифициран електронен подпис, в интерес както на Потребителя, така и на Доставчика е постигане на максимално високо ниво на сигурност чрез снемането на копие от документа за самоличност на Потребителя и съхраняването му в хартиен или електронен вид. Уговорка за снемане и съхраняване на копие от документа за самоличност на Потребителя може да бъде включена в сключения между страните Договор за удостоверителни услуги. В случай, че съгласие за снемане и съхранение на копие от документ за самоличност не бъде постигнато, Доставчикът може да откаже предоставянето на квалифицирана удостоверителна услуга предвид невъзможността да гарантира безпрепятственото и за пълния обем от услуги приемане на квалифицираното удостоверение от доверяващи се страни, за които постигането на максимално високо ниво на сигурност е приоритет, в това число доставчици на платежни услуги, които, съгласно приложимото законодателство за мерките срещу изпирането на пари, са задължени да събират и съхраняват копие на документа за самоличност на клиента като част от процеса по неговата идентификация.
6. Първоначалната идентификация и потвърждаване на самоличността включва:
   - държането на частния ключ от Потребителя или от изрично упълномощено от него лице, съответстващ на публичния ключ, представен на Доставчика за издаване на удостоверението;
   - принадлежност на мобилното устройство/мобилното приложение от заявителя/Потребител или от изрично упълномощено от него лице
   - проверка и потвърждаване на самоличността на Потребителя на издаваното удостоверение.
7. След успешна проверка на самоличността на Потребителя, 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 B-Trust QSCD (за КЕП/КЕПечат) и да го предаде на Потребителя или на упълномощеното лице;
   - може да запише издаденото удостоверение (за УЕП/УЕПечат) на B-Trust STC (PKCS#12 криптофайл) като използва утвърден от Доставчика софтуер (CSP/Crypto Service Provider).
8. Издадено КУ за облачен КЕП не се предава на Потребителя-Титуляр. Доставчикът го публикува в B-Trust Публичния регистър на удостоверенията и го съхранява в RQSCD на платформата за облачен КЕП като го асоциира в потребителския акаунт на Титуляря снеговото мобилно устройство/мобилно приложение (смартфона) и с генерираната двойка ключове в HSM за този облачен КЕП.

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 Потребителя.
2. Електронната заявка с публичния ключ, която се генерира за издаване на КУ 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. Онлайн 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. Автентификация на държателя на частния ключ за КУ на облачен КЕП допълнително включва TOTP-схема, базирана на мобилното приложение в мобилно устройство и асоциираният потребителски акаунт, за който се генерира двойката ключове.
6. Двойката ключове за КЕП и КЕПечат, съответстваща на издаваното от Доставчика КУ, задължително се генерира в QSCD () или в утвърден от Доставчика софтуер (Crypto Service Provider/CSP) за УЕП/УЕПечат.
7. Двойката ключове, съответстваща на издавано от Доставчика КУ за облачен КЕП, задължително се генерира в HSM (CC EAL 4+) на RQSCD на платформата за облачен КЕП и се съхранява при Доставчика на база утвърдени вътрешни крипто-схеми за персонален контрол в съответствие с SAD/SAP/SAM (Signature Activation Data/Signature Activation Protocol/Signature Activation Module) на ETSI EN 419 241 (part 2/3) и защитен профил (PP) съгласно EN 419 221-5.
8. Достъпът както и отдалеченият достъп до частния ключ се държи само от Титуляря на КЕП или на Облачен КЕП (sole control).

3.2.2 Установяване на идентичност на юридическо лице или едноличен търговец

1. Удостоверяване на идентичността и автентичността на юридическо лице има две цели:
   - да се докаже, че по време на разглеждане на заявката юридическото лице съществува;
   - да се докаже, че представителното лице, което кандидатства за удостоверение е получило разрешение от юридическото лице да го представлява
2. 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.
3. Установяването на идентичността на юридическо лице или едноличен търговец, данните за което се вписва в КУ, изисква в РО/МРС да се яви упълномощен представител на лицето и да представи изискуемите документи, доказващи правния му статус.
4. Установяването на идентичността на българско юридическо лице се осъществява от РО/МРС на Доставчика, чрез проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ по реда на ЗЕУ. Служител на РО/МРС може да провери регистрацията посредством всички достъпни публични услуги съгласно българското законодателство.
5. За българските юридически лица, които не са търговци, както и за чуждестранните юридически лица, за които не може да се извърши онлайн (или автоматизирана) проверка се представят:
   - Съдебно решение или друг документ, удостоверяващи възникването на юридическото лице;
   - Документ, удостоверяващ актуалното състояние на лицето;
   - Уникален национален идентификатор.
6. Списък с изискуеми документи е публикуван на B-Trust сайта на ДКУУ. След копиране на всички изискуеми документи, със съгласието на лицето подало искане, копията остават в архива на Доставчика.
7. Когато вместо юридическо лице се явява негов упълномощен представител, удостоверяването на информацията, която се съдържа в представените документи става чрез:

- Заверка „Вярно с оригинал” и саморъчен подпис върху документите пред служител на РО/МРС;
- Нотариално заверени документи;
- Подписване на приложените електронни формати на документите с валидно удостоверение за квалифициран електронен подпис.

3.2.3 Установяване самоличността на физическо лице

1. Установяване и проверка на самоличността на физическото лице като Потребител на КУ или като 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 изисква физическото лице като Потребител или като упълномощен представител на друго физическо лице или на юридическо лице да представи в РО/МРС следните документи:

Наименование на КУ	Необходими документи
Персонално КУКЕП „B-Trust Personal Qualified Certificate QES" **Персонално КУ за облачен КЕП** „B-Trust Personal Qualified Certificate CQES"	Документи, доказващи самоличността на Потребителя - при лично явяване. Документи, доказващи самоличността на упълномощеното лице и пълномощно – при явяване на упълномощено лице. Утвърдено от Доставчика мобилно приложение в мобилно устройство (за облачен КЕП).
Професионално КУКЕП „B-Trust Professional Qualified Certificate QES" **Професионално КУ за облачен КЕП** „B-Trust Professional Qualified Certificate CQES"	Документи, доказващи самоличността на Потребителя, идентичността на юридическото лице и представителната власт на Потребителя спрямо юридическото лице. Утвърдено от Доставчика мобилно приложение в мобилно устройство (за облачен КЕП).
Персонално КУУЕП „B-Trust Personal Advanced Certificate AES"	Документи, доказващи самоличността на Потребителя - при лично явяване. Документи, доказващи самоличността на упълномощеното лице и пълномощно – при явяване на упълномощено лице
Професионално КУУЕП „B-Trust Professional Advanced Certificate AES"	Документи, доказващи самоличността на Потребителя, идентичността на юридическото лице и представителната власт на Потребителя спрямо юридическото лице.
КУКЕПечат КУКЕПечат на юридическо лице „B-Trust Organization Qualified Certificate QESeal”	Документи, доказващи самоличността на Потребителя, идентичността на юридическото лице и представителната власт на Потребителя спрямо юридическото лице.
КУУЕПечат КУУЕПечат на юридическо лице „B-Trust Organization Qualified Certificate AESeal”	Документи, доказващи самоличността на Потребителя, идентичността на юридическото лице и представителната власт на Потребителя спрямо юридическото лице.
КУ за автентичност на уебсайт „B-Trust Web authentication Qualified Certificate”	Документи, доказващи самоличността на Потребителя - при лично явяване. Документи, доказващи самоличността на упълномощеното лице и пълномощно – при явяване на упълномощено лице. Документи, доказващи принадлежност на уебсайта (домейна) на Потребителя.

3.2.4 Особени атрибути

1. Доставчикът може да включва в издаваното удостоверение особени атрибути, свързани с Потребителя, 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, КУ за облачен КЕП или КУКЕПечат, 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. Подновяване на КУУЕП и КУУЕПечат не се допуска. По искане на Потребителя, Доставчикът издава ново КУУЕП или КУУЕПечат като изпълнява първоначална идентификация и установяване на самоличността му.
3. Удостоверение се подновява за същата двойка асиметрични ключове (Renew) на текущото КУ, 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.
4. Доставчикът допуска многократно подновяване на КУ, като запазва текущата двойка ключове (Renew), но препоръчва тази практика да се ограничава с цел да се намали риска от компрометиране на частния ключ.
5. Доставчикът ще поднови текущо КУ с нова двойка ключове (Re-key), само ако Потребителя 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.
6. След подновяване текущото удостоверение не се прекратява и остава валидно в срока му на валидност.
7. За идентификация, установяване на идентичност и самоличност на Потребителя на удостоверение, което се подновява, не се изисква тяхното лично присъствие в РО/МРС на Доставчика.
8. При настъпили промени в информацията за Потребителя на КУ, текущото удостоверение не се подновява. Доставчикът издава ново КУ, като следва първоначална идентификация и установяване на самоличността му и прекратява незабавно текущото удостоверение.
9. 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.
10. Доставчикът съблюдава следните времеви ограничения и изисквания за идентификация при подновяване на КУ:

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	Не се подновява	

валидност на удостоверение		

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 ЗЕДЕУУ.

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 ЗЕДЕУУ.
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. Потребител на прекратено удостоверение може да заяви издаване на ново удостоверение.
3. Доставчикът, чрез РО/МРС изпълнява първоначална идентификация, установяване на идентичност на Потребителя, 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 КУ:
   - регистрация на искане за издаване;
   - обработка на искане за издаване;
   - издаване;
   - предаване на издадено;
   - употреба на двойката ключове и КУ;
   - подновяване чрез “Renew”;
   - подновяване чрез “Re-key”;
   - спиране/възобновяване;
   - прекратяване;
   - статус на КУ.
2. Доставчикът, чрез РО/МРС, допуска Потребител 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 Потребител или упълномощено лице.
3. Искането за заявяване на КУ за облачен КЕП се предхожда от инсталиране и инициализиране/активиране на мобилното приложение за облачен КЕП в мобилното устройство на Заявителя/Потребителя.
4. Заявителят регистрира искане за издаване на удостоверение в онлайн режим или чрез оператор в РО/МРС на Доставчика.
5. 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 Потребителя.

4.1.1 Процес на заявяване

1. Искането за издаване включва цялата изискуема информация по ЗЕДЕУУ за Потребителя 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 Потребител да генерира двойката криптографски ключове и да включи публичния ключ в информацията за издаване на удостоверението.
3. Двойката криптографски ключове за издаване на КУКЕП и КУКЕПечат задължително се генерира в B-Trust QSCD, отговарящо на изискванията за ниво на сигурност за създаване подписа/печата.
4. Двойката криптографски ключове за издаване на КУ за облачен КЕП задължително се генерира при Доставчика в HSM-а в RQSCD на платформата за облачен КЕП.
5. Двойката криптографски ключове за издаване на КУУЕП и КУУЕПечат се генерира софтуерно чрез утвърден от Доставчика софтуер (Crypto Service Provider/CSP), отговарящ на изискванията за допустимото ниво на сигурност/осигуреност за създаване усъвършенстван подпис/печат.
6. 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.
7. В случаите, когато е необходимо, РО/МРС предоставя на Потребителя или на

упълномощено от него лице в защитен вид информация/код за достъп до частния ключ.

8. Ако Заявителят не притежава QSCD, когато представя искане за издаване на КУ на РО/МРС на Доставчика, той само въвежда информацията за идентифициране на Потребителя, както и друга допълнителна такава, без да генерира криптографска двойка ключове за исканото удостоверение. Криптографската двойка ключове се генерира при РО/МРС на Доставчика.
9. Комуникациите между Потребителите и защитени Интернет страници на сайта на Доставчика се базират на HTTPS протокол.
10. Одобрените заявки за издаване и управление на КУ 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 - Потребител 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 Потребителя или упълномощеното лице;
   - представителната власт на физическото спрямо юридическото лице и на упълномощеното лице;
   - проверява упълномощаването;
   - държането на частния ключ, съответстващ на публичния ключ (когато двойката ключове е генерирана ппри Потребител);
   - (за облачен КЕП) успешно инициализиране/активиране на мобилното приложение в мобилното устройство и регистриране (т.е., асоциирането му с потребителския акаунт, чрез сканиране на изпратен QR-код) от Доставчика ;
   - (за облачен КЕП) принадлежност/притежание на мобилното устройство с мобилното приложение за облачен КЕП от Заявителя/Потребител чрез TOTP-механизъм/схема;
   - 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 Потребителя, РО/МРС следва да провери предоставената електронна заявка и изискванията за нивото на сигурност на двойката ключове.

4.2.2 Идентификация и автентикация с асистент

1. Когато Заявителят/Потребителят е грамотен, но е ням, глух или глухоням, глухият трябва сам да прочете гласно документите, които подписва, и да обяви дали е съгласен със съдържанието им, а немият или глухонемият трябва след прочитане на документа да напише собственоръчно в него, че го е прочел и че е съгласен със съдържанието му.
2. Когато Заявителят/Потребителят е неграмотен, същият следва да осигури грамотно лице (тълковник), което да му предаде съдържанието на подлежащите на подписване документи. Подписването на документи от неграмотно лице се извършва чрез полагане на пръстов отпечатък от десния му палец. В случай, че полагане на пръстов отпечатък от десния палец е невъзможно, в документа се отбелязва причината за това, както и с кой друг пръст е сложен отпечатъкът.
3. Когато Заявителят/Потребителят е сляп, същият следва да осигури двама грамотни свидетели, които да го запознаят със съдържанието на документите, които подписва, и да приподпишат същите.
4. РО/МРС установява самоличността на тълковника и свидетелите по реда на т. 3.2.3. от настоящия документ. Данните за самоличността на тълковника и свидетелите се записват

в документите, в подписването на които същите участват.

4.2.3 Потвърждаване или отхвърляне на искане за издаване

1. След успешно направените проверки и заплащане от страна на Заявителя/Потребител, оторизиран оператор на РО/МРС утвърждава пред Доставчика искането за издаване на удостоверение.
2. РО/МРС отхвърля искането за издаване на удостоверение, ако уттвърждаването е неуспешно или не е изпълнено заплащане в 5-дневен срок от заявеното искане за издаване на КУ за облачен КЕП.
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. Потребител на КУ има задължението незабавно да информира Доставчика за настъпили промени в удостоверената информация след издаването му.

4.2.4 Срок за обработка на искане за издаване на удостоверение

1. РО/МРС на Доставчика незабавно, в присъствието на Заявителя/Потребител или упълномощено от него лице, изпълнява всички функции по проверка, след като той е представил необходимите за това документи и утвърждава представената информация чрез направеното искане за издаване на удостоверение.
2. Допуска се 5-дневен срок за обработка на искане за издаване на КУ за облачен КЕП, през който Потребителят може да заплати онлайн заявеното удостоверение. След този срок, мобилното приложение блокира използването на облачния КЕП. Ако този срок не е изтекъл или заявката е потвърдена (след заплащане) от РО/МРС, мобилното приложение изисква Потребителят да въведе ПИН-код за облачния КЕП.
3. 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 КУ.
2. УО генерира заявеното КУ съгласно избрания профил, подписва го с електронния подпис на Доставчика и го публикува незабавно в Публичния си регистър.

4.3.2 Известяване на Потребителя на удостоверение от Доставчика

1. Доставчикът, чрез Службата за известяване на Потребители на КУУ, незабавно известява Потребителя на издаденото и публикувано удостоверение.
2. Службата за известяване изпраща до Потребителя електронно известие по имейл или push-нотификация до мобилното приложение с информация за издаденото КУ, неговия сериен номер и периода му на валидност, освен в случаите, когато липсва имейл адрес.
3. Доставчикът доставя издаденото удостоверение на Потребителя, респективно на упълномощеното от него лице, чрез РО/МРС.
4. Оторизиран оператор на РО/МРС записва КУ на B-Trust QSCD или на B-Trust SCT (PKCS#12 криптофайл), в зависимост от това къде е била генерирана двойката криптографски ключове за това удостоверение, когато това е възможно.
5. Доставчикът, чрез РО/МРС доставя издаденото удостоверение на Потребителя, респективно на упълномощеното от него лице.
6. В случая, когато Потребител е генерирал двойката ключове и частния ключ е на негов

компютър, той следва да достави/зареди издаденото КУ на този компютър от посочения адрес (URL) в имейла.
7. Генерирането на защитен преносим софтуерен токън (PKCS#12 файл) е задължение на Потребителя или на упълномощено лице след като достави издаденото КУ и удостоверенията на Доставчика.

4.4 Приемане и публикуване на удостоверението

1. Доставчикът, чрез оперативния УО публикува незабавно издаденото удостоверение в Публичния регистър на издадените удостоверения.
2. Потребителят 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 Потребителя 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 Потребителя

1. Частният ключ, съответстващ на удостоверения публичен ключ е под контрола само на Потребителя. Отговорността за използването на частния ключ е на Потребителя.
2. Потребител употребява удостоверението и съответстващата двойка ключове на удостоверението, както следва:
   - в съответствие с означената в удостоверението Политика "Certificate Policy" и съгласно атрибутите „keyUsage" и „extendedKeyUsage";
   - за полагане на електронен подпис или електронен печат в рамките на срока на валидност на удостоверението;
   - проверка на положен електронен подпис или електронен печат;
   - до момента на прекратяване на удостоверението;
   - когато удостоверението е спряно, не използва частния ключ за създаване на електронен подпис или на електронен печат;
   - съгласно Договора за удостоверителни услуги между него и Доставчика.

4.5.2 От доверяваща се страна

1. Публичният ключ в КУ, съответстващ на държания от Потребителя частен ключ, е публично достъпен за всички.
2. Всяка доверяваща се страна, включително оператор в РО/МРС следва да използва КУ и публичния ключ на Потребител, 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 КУ запазва информацията от текущото удостоверение, като в подновеното удостоверение се променя периода на валидност.
2. КУУЕП, КУУЕПечат и КУ за облачен КЕП не се подновява. Потребителят може да заяви издаване на ново КУ за подпис, за печат или за облачен КЕП.
3. Подновяването на КУ се предхожда от регистриране на искане за подновяване пред РО/МРС.
4. Подновяване на КУ, 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).

5. Искането за подновяване на удостоверение се регистрира онлайн, когато Потребителят има валидно КУКЕП, което трябва да поднови.
6. Когато удостоверението е с изтекъл срок на валидност и искането за подновяване е съгласно посочените времеви ограничения и изисквания за идентификация при подновяване, Потребителят или упълномощено от него лице трябва лично да посети РО/МРС на Доставчика.
7. Потребител или упълномощено от него лице може да поднови многократно свое КУ при съблюдаване на посочените по-долу условия за подновяване.
8. Доставчикът не допуска използване на двойка ключове за период, по-голям от 3 (три) години.
9. Доставчикът не препоръчва многократното подновяване на КУ чрез „Renew" с цел да се намали риска от компрометиране на частния ключ.
10. Доставчикът препоръчва на Потребителя да поднови свое удостоверение чрез „Re-key”.

4.6.1 Условия за подновяване на удостоверение

1. РО/МРС ще поднови едно КУ чрез „Renew" при съблюдаване на следните условия:
   - удостоверението не е прекратено в периода му на валидност;
   - Потребител или упълномощено 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 КУ чрез „Re-key" при съблюдаване на следните условия:
   - удостоверението не е прекратено в срока му на валидност;
   - Потребител 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 Потребителя на текущото удостоверение, последното не подлежи на подновяване, а Доставчикът издава ново удостоверение.

4.6.2 Кой може да заяви подновяване на удостоверение

1. Потребител 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 КУ 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, Потребителят 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 КУ.

4.6.4 Известяване на Потребител след подновяване на удостоверение

1. Доставчикът, чрез Службата за известяване на Потребители на удостоверителни услуги, незабавно известява Потребителя на подновеното и публикувано удостоверение.
2. Службата за известяване изпраща до Потребителя електронно известие по имейл или push-нотификация на мобилното приложение с информация за издаденото КУ, 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, Потребител получава подновеното удостоверение от оторизирания оператор, който при необходимост го записва на B-Trust QSCD, в което е генерирана двойката криптографски ключове за удостоверението.
4. Подновено КУ за облачен КЕП не се доставя на Потребителя, само се записва в потребителския акаунт, съответстващ на асоцииранoто с него мобилно приложение/мобилно устройство.

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 КУ само при спазване на изискванията и на условията за издаване на ново удостоверение.
2. Доставчикът не допуска промяна в профила на КУ, специфициран в Политиката за това удостоверение.
3. Доставчикът не предлага услугата "Модификация на удостоверение" (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 КУ, 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 (например, изгубено/откраднато QSCD устройство или мобилно устройство с мобилно приложение) е необходимо това да се заяви на телефон: 0700 199 10.
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 КУ при:
   - смърт или поставяне под запрещение на Потребител с прекратяване на юридическо лице на Потребителя;
   - прекратяване на представителната власт на Потребителя 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 Потребителя;
   - компрометиране на частния ключ;
   - загуба на B-Trust QSCD или мобилно устройство с инициализирано/активирано мобилно приложение или заличаване (delete) на мобилното приложение в мобилното устройство;
   - забава в заплащането на дължимо възнаграждение;
   - искане за прекратяване, след като се увери в самоличността и в представителната власт на Потребителя.
2. Доставчикът предприема незабавно прекратяване на действието на издаденото КУпри 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 Потребителя 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 Потребителя.
4. Оторизираният оператор в РО/МРС незабавно, без да идентифицира Потребителя, спира действието на удостоверението за не повече от 24 часа.
5. Във всички случаи, Потребителят или упълномощено от него лице трябва да посети лично РО/МРС на Доставчика за последваща проверка на идентичността, респективно самоличността му.
6. РО/МРС строго следва изискванията за идентификация и установяване на идентичност, респективно самоличност на Потребителя 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 Потребителя за причините за това.
9. Потребител, 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 Потребителя чрез е-мейл или push-нотификация на мобилното устройство/мобилното приложение на прекратеното удостоверение.
12. Прекратено удостоверение на Потребител 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 КУ, 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 Потребителя 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 Потребителя 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 КУ 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 КУ, 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 КУ 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 КУ в реално време (по OCSP протокол) може да се изпълни и през Интернет страницата на Доставчика.

4.9.10 Съгласуване на информацията в Списък на прекратени удостоверения и OCSP

1. Тъй като Доставчикът поддържа два метода за проверка на статус на удостоверение (OCSP и CRL) съществуват процедури за поддържане на еднаквост на информацията за статус.
2. Информация за статуса на удостоверение се актуализира най-напред по OCSP, след което се синхронизира и съответния Списък на прекратени удостоверения. Разликата в информацията за статуса на удостоверение има период на уеднаквяване в зависимост от Удостоверяващия орган, издаващ съответния Списък на прекратени удостоверения, както следва:
   - За B-Trust Root Qualified CA и B-Trust Root Advanced CA – период до 2 часа;
   - За B-Trust Operational Qualified CA и B-Trust Operational Advanced CA – период до 2 минути.

4.9.11 Условия за спиране на удостоверение

1. Доставчикът, чрез своя оперативен УО, спира действието на валидно КУ 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).

4.9.12 Кой може да заяви искане за спиране на удостоверение

1. Доставчикът спира издадено от него валидно удостоверение ако:
   - постъпи искане на Потребител 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 ЗЕДЕУУ.

4.9.13 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 (или УЕП) или облачен КЕП.
4. Оторизираният оператор в РО/МРС незабавно, без да идентифицира Потребителя, спира действието на удостоверението. Спирането на удостоверението се извършва чрез временното му вписване в списъка на прекратените удостоверения, съгласно чл. 26, ал. 5 от ЗЕДЕУУ.
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 Потребителя чрез е-мейл или push-нотификация на мобилното

устройство на спряното удостоверение.

4.9.14 Ограничение на периода на спиране на удостоверение

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

4.9.15 Възобновяване действието на спряно удостоверение

1. Доставчикът възобновява действието на спряно КУ:
   - 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 Потребителя, 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.

4.9.16 Процедура за възобновяване на действието на удостоверение

1. РО/МРС възобновява спряно КУ след като получи искане за възобновяване от Потребителя 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 КУ, 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 Reason" 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";
   - Базов УО „B-Trust Root Advanced CA";
   - Оперативен УО „B-Trust Operational Qualified CA";
   - Оперативен УО „B-Trust Operational Advanced CA"
   - Регистриращ орган;
   - Публичен регистър;
   - Орган за издаване на квалифицирани електронни времеви печати „B-Trust Qualified Time Stamp Authority";
   - RQSCD в платформа за Облачеен КЕП;
   - OCSP сървър „B-Trust Root Qualified OCSP Authority";
   - OCSP сървър „B-Trust Qualified OCSP Authority";
   - OCSP сървър „B-Trust Root Advanced OCSP Authority";
   - OCSP сървър „B-Trust Advanced 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", „B-Trust Root Advanced CA“, „B-Trust Operational Advanced 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, 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 КУ, включително създаване на двойка ключове - частен и публичен за КУ;
   - 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“;
   - управление на HSM на „B-Trust Root Advanced CA” и „B-Trust Operational Advanced 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 7 (седем) години.

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 КУ, само като издаде ново удостоверение или поднови текущото с „Re-Key”.
2. Промяна на ключа, съответстващ на КУУЕП, облачен КЕП и КУУЕПечат се изпълнява само като се издаде ново удостоверение.

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 Потребителите, 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 Потребител

1. При компрометиране на частен ключ на Потребител, 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 НОПДДУУ.
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 КУ на Потребителите.
3. Криптографските (RSA) двойки ключове на издаваните КУКЕП в инфраструктурата на Доставчика се генерират, както следва:
   - от Потребителя - с хардуер и софтуер или само с утвърден от Доставчика софтуер (Crypto Service Provider/CSP), който е под негов контрол;
   - от РО/МРС на Доставчика - с хардуер и софтуер или само с утвърден от Доставчика софтуер (Crypto Service Provider/CSP), който е под контрол на оператор на Доставчика.
4. Криптографските (RSA) двойки ключове на издавани КУ за облачен КЕП се генерират на HSMa в RQSCD на платформата за облачен КЕП при Доставчика с изискуемото ниво на сигурност (CC EAL 4+ и по-високо).
5. Доставчикът може на базата на договорни отношения да предостави на Потребителите одобрени от него технически средства, които отговарят на изискванията за ниво на сигурност.
6. Само електронни подписи и печати, създадени с частен ключ на двойка ключове генерирани в QSCD и RQSCD на платформата за облачен КЕП имат характера на КЕП, КЕПечат и облачен КЕП.
7. Потребителят се задължава да използва утвърден от Доставчика софтуер или лицензиран такъв за работа с КУ и с асоцииран (съответен) с тях токън (QSCD или SCT/PKCS#12 файл).

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 Базовите и на Оперативните УО, съответно „B-Trust Root Qualified CA", „B-Trust Operational Qualified CA" и „B-Trust Root Advanced CA", „B-Trust Operational Advanced 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 Потребител

1. Двойката ключове на Потребител се генерира с използване на утвърден специализиран софтуер, който е изцяло под негов контрол.
2. В случай, когато Доставчикът генерира Двойката ключове на Потребителя, той използва специализиран и утвърден софтуер, проверен за успешна работа през интерфейсите на инфраструктурата на B-Trust.
3. Двойката ключове на Потребител се генерира в одобрен от Доставчика QSCD с проверено ниво на сигурност или чрез утвърден от него софтуер (Crypto Service Provider/CSP). Когато двойката ключове за КЕП/КЕПечат се генерира при Доставчика, винаги се използва B-Trust QSCD. Частният ключ на генерираната двойка ключове не може да бъде изведен от QSCD.
4. Двойката ключове на Потребител на облачен КЕП винаги се генерира в HSM на RQSCD в платформата за облачен КЕП на Доставчика, съхранява се при него чрез утвърдена крипто-схема и се достъпва от разстояние (отдалечено) като се гарантира персонален контрол на частния ключ в съответствие с защитен профил на SAD/SAP/SAM съгласно ETSI EN 419 241-2/3.
5. Контролът на частния ключ е чрез код за достъп, а дължината на RSA ключа е поне 2048 бита. Потребителят използва частния ключ за да създаде подписа, като въвежда кода за достъп до него.
6. Когато двойката ключове се генерира при Потребител, Доставчикът препоръчва последният да използва одобрено в инфраструктурата на B-Trust решение или еквивалентно такова.
7. За целите на полагане на КЕП/КЕПечат Доставчикът препоръчва Потребителят да използва B-Trust QSCD или друго QSCD, съвместимо в инфраструктурата на B-Trust.
8. За целите на полагане на облачен КЕП Доставчикът доставя утвърдено от него мобилно приложение за смартфон, което Потребителят следва да инсталира, инициализира/регистрира и използва при активиране на подписа.
9. За целите на полагане на УЕП/УЕПечат Доставчикът препоръчва Потребителят да използва B-Trust SCT (PKCS#12 файл) или друго SCD, съвместимо в инфраструктурата на B-Trust.

6.2.3 Доставка на частния ключ

1. Когато двойката ключове за КЕП/КЕПечат се генерира при Доставчика, Потребителят или изрично упълномощено от него лице получава от РО/МРС на Доставчика частния ключ и издаденото удостоверение върху QSCD.
2. Когато двойката ключове за УЕП/УЕПечат се генерира при Доставчика, Потребителят или изрично упълномощено от него лице получава от РО/МРС на Доставчика частния ключ и издаденото удостоверение чрез B-Trust STC (PKCS#12 криптофайл).
3. При издаване на КУКЕП/КУКЕПечат 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.
4. При издаване на КУ за облачен КЕП частният ключ, съответстващ на удостоверен публичен ключ в удостоверението, се съхранява в HSM-а на RQSCD в платформата за облачен КЕП при Доставчика чрез утвърдена крипто-схема, гарантираща персонален контрол на частния ключ; достъпът до ключа е в съответствие с защитен профил на SAD/SAP съгласно ETSI EN 419 241-2/3.
5. Потребителят е задължен да смени предоставения начален код за достъп и въведе свой личен.

6. Когато Потребител генерира двойката ключове при себе си, той носи цялата отговорност за гарантиране на държането на частния ключ от него.
7. Когато Потребител генерира двойката ключове при себе си, той декларира пред Доставчика, че двойката ключове напълно отговаря на изискванията за полагане на електронен подпис/печат в съответствие с Регламента.

6.2.4 Доставка на публичния ключ при Доставчика

1. Изпълнява се само от Потребител, 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. Потребителят доставя чрез РО/МРС на Доставчика публичния ключ от генерираната двойка ключове.
3. Потребителят може да предостави електронната заявка на носител, лично в РО/МРС, заедно с другите документи съгласно Политиките на Доставчика за издаване на КУ, през Интернет-страницата на Доставчика или по друг подходящ начин.
4. РО/МРС на Доставчика задължително прави проверка на държането на частния ключ от Потребителя.

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 базовите RSA-ключове на Доставчика е 4096 бита.
2. Дължината на двойката RSA-ключове на оперативните УО „B-Trust Operational Qualified CA" и “B-Trust Operational Advanced CA" е 4096 бита.
3. Дължината на двойката RSA-ключове на оперативните органи „B-Trust Root Qualified OCSP Authority", „B-Trust Qualified OCSP Authority" и “B-Trust Root Advanced OCSP Authority", „B-Trust Advanced OCSP Authority" е не по-малка от 2048 бита.
4. Дължината на двойка ключове (RSA) за КЕП/КЕПечат, облачен КЕП и УЕП/УЕПечат на Потребител, генерирана чрез инфраструктурата на Доставчика е поне 2048 бита.
5. Дължината на двойка ключове (RSA) за КЕП/КЕПечат и УЕП/УЕПечат на Потребител, генерирана извън инфраструктурата на Доставчика е поне 2048 бита.
6. Независимо къде е генерирана двойката ключове за издаване на КУ, 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. Ключовите компоненти в инфраструктурата на B-Trust „B-Trust Root Qualified CA", „B-Trust Operational Qualified CA", „B-Trust Root Advanced CA", „B-Trust Operational Advanced CA", RQSCD в платформата за облачен КЕП и OCSP сървърите 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, респективно HSM-а в RQSCD на платформата където се генерира и съхранява частния ключ на Потребителя е с ниво на сигурност CC EAL 4+/FIPS 140-1 Level 2, респективно Level 3.
3. Софтуерът за генериране на двойка ключове (Crypto Service Provider/CSP) е утвърден от Доставчика и проверен за работа в инфраструктурата на B-Trust.
4. Всички QSCD извън инфраструктурата на B-Trust, които Потребителят може да ползва, за да генерира двойка ключове и да съхранява частния ключ за КЕП/КЕПечат, трябва да са сертифицирани за еквивалентно ниво на сигурност CC EAL 4 и по-високо.

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 КЕП/КЕПечат на Потребител 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.
4. Частният ключ на облачен КЕП на Потребител се използва само в HSM-а на RQSCD в платформата за облачен КЕП и е достъпен посредством SAD/SAP/SAM схема и личен код за достъп в съответствие с ETSI EN 419 241-2/3. В този случай едновременно с генериране на двойка ключове се изпълнява съхраняване на частния ключ на база утвърдена криптосхема от Доставчика, осигуряваща защита и персонален контрол на ключа.
5. Частният ключ на УЕП/УЕПечат на Потребител се използва само с лицензиран софтуер чрез B-Trust SCT (PKCS#12 криптофайл) и е достъпен посредством личен код за достъп.

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 КЕП/КЕПечат на Потребител 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. Частният ключ на облачен КЕП на Потребител се съхранява само в HSM-а на RQSCD в платформата за облачен КЕП и не може да се репродуцира на друга такава платформа. B-Trust платформата за облачен КЕП е резервирана относно критичните компоненти в нея, включително и HSM модула.
7. Частният ключ на П/КУУЕПечат на Потребител се съхранява софтуерно и може да се репродуцира на друга система само под контрол Потребителя. При дефектиране на частния ключ, Потребителят трябва да като заяви издаване на ново удостоверение.
8. Доставчикът по никакъв начин не съхранява и не архивира частен ключ за КУКЕП/КУКЕПечат на Потребител, независимо къде и как се генерира двойката ключове.
9. Доставчикът съхранява частен ключ на облачен КЕП само на база утвърдени криптограми

за защита и гарантиран персонален контрол върху ключа от страна на Потребителя.

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 Потребител към и от Доставчика с цел съответно съхранение и възстановяване в друго QSCD/HSM или в софтуер се поддържа.
3. Частният ключ на КЕП/КЕПечат на Потребител се съхранява само на QSCD, в което се генерира двойката ключове и не може да се трансферира/репродуцира на друго място.
4. Частният ключ на УЕП/УЕПечат на Потребител се съхранява софтуерно и може да се репродуцира на друга система само под контрол Потребителя.

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 Потребител се активира, чрез въвеждане на потребителския код за достъп до мястото, където защитено се съхранява ключа или се използва друг способ на идентификация.
4. Частен ключ на облачен КЕП на Потребител в RQSCD на платформата се активира чрез изпълнение на схема за TOTP-автентификация за принадлежност на смартфона и въвеждане на потребителския код за достъп (ПИН) за облачен КЕП в съответствие със SAD/SAP/SAM на ETSI EN 419 241-2/3. Частният ключ за облачен КЕП се активира само ако съществуват подписани искане за издаване на Облачен КЕП и Договор за удостоверителни услуги от Потребителя. Подписването на тези документи може да стане след издаване на удостоверение за Облачен КЕП.

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) посредством преустановяване на логическия достъп до съответния ключ в нея.
2. Частен ключ на Потребител се деактивира (прекратява се възможността за използване) 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 КЕП/КЕПечат на Потребител се унищожава посредством изтриването му от QSCD или цялостното изтриване на QSCD.
3. Частен ключ на облачен КЕП на Потребител се унищожава посредством изтриването му (на криптограмата за него) от потребителския акаунт за облачен КЕП.
4. Частен ключ на УЕП/УЕПечат на Потребител се унищожава посредством изтриването му от мястото, където защитено се съхранява ключа.

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 Потребители се съдържат в издадените за тях удостоверения, които са публикувани в Публичен регистър и се съхраняват във вътрешен регистър.
4. Публичните ключове на Потребители се съхраняват и архивират чрез периодично архивиране на вътрешния регистър.

6.4.2 Период на валидност на удостоверение и употреба на двойка ключове

1. КУ имат следните срокове на действие:
   - на базовия УО „B-Trust Root Qualified CA" и „B-Trust Root Advanced CA" - 20 (двадесет) години;
   - на оперативните УО „B-Trust Operational Qualified CA" и „B-Trust Operational Advanced CA" - 15 (петнадесет) години;
   - на OCSP сървъри – 5 (пет) години;
   - на Потребител – съгласно договора между Доставчика и Потребителя, но не повече от 3 (три) години.
2. Когато се използва ключа за подписване/подпечатване след изтекъл период на валидност на удостоверението, подписът/печатът е невалиден и съответния подписан/подпечатан обект или изявление следва да се считат недействителни.
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 от Потребител, последния сам създава и управлява данни за активация.
2. При генериране на двойка ключове на Потребителя от Доставчика, последния предава на Потребителя контрола на данни за активация заедно с частния ключ.
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: 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 Потребителя или на упълномощеното от него лице в запечатен, непрозрачен хартиен плик.
5. Потребителят е задължен на смени първоначалния Потребителски код за достъп до B-Trust QSCD посредством софтуера, който се предоставя с него.
6. Доставчикът препоръчва Потребителят да сменя периодично своя Потребителски код за достъп до B-Trust QSCD.
7. Потребителят следва да използва предоставеният Административен код за достъп с цел деблокиране блокирано B-Trust QSCD.

6.5.2 Генериране и инсталиране на данни за активация на облачен КЕП

1. Двойката ключове за облачен КЕП се генерира в HSM-а на RQSCD вплатформата за облачен КЕП като частният ключ защитено се съхранява при Доставчика.
2. При първоначално издаване на КУ за облачен КЕП, преди генериране на двойка ключове, Потребителят следва да зареди и инициализира/активира мобилното приложение за

облачен КЕП в смартфона.

3. Инициализацията/активацията на мобилното приложение се изпълнява автономно в смартфона, а регистрацията на мобилното приложения се изпълнява съвместно с латформата за облачен КЕП на Доставчика като включват:
   - Създаване на парола;
   - Регистрация (асоцииране) на приложението/мобилното устройство в платформата за облачен КЕП (въздаване на потребителски акаунт, обмен на общ (shared) ключ за TOTP-схема на автентификация, ключ за защита на ПИН-а);
   - Сигурно съхраняване на двата ключа в мобилното устройство /приложението – единият се използва за TOTP-автентификация (притежание на мобилното устройство от Потребителя, другият – за защита на ПИН-а за достъп до частния ключ);
   - Генериране на двойка ключове след въвеждане на ПИН чрез мобилното приложение от Потребителя; частния ключ се защитава чрез утвърдена криптосхема, гарантираща персонален контрол до частния ключ и се съхранява;
4. Данните за активация на облачния КЕП (общ ключ за TOTP-автентификация, ключ за защита на ПИН) са под контрола на Потребителя.
5. TOTP-автентификационния механизъм и криптосхемата за защита на частния ключ на облачен КЕП въвеждат и гарантиран персонален контрол на Потребителя до защитения частен ключ на облачния КЕП.

6.5.3 Защита на данни за активация

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

6.5.4 Други аспекти на данните за активация

1. След определен брой неуспешни опити за въвеждане на коректен код за достъп до частния ключ на Потребителя, B-Trust QSCD се блокира.
2. След определен брой неуспешни опити за въвеждане на коректен код за достъп до частния ключ на облачен КЕП на Потребителя, криптограмата с частния ключ в потребителския акаунт се блокира.
3. Потребителят трябва да използва предоставеният му Административен код за достъп, за да деблокира блокирано B-Trust QSCD.
4. Потребителят на облачен КЕП трябва да използва предоставен му допълнителен (административен) код, за да деблокира криптограмата съдържаща частния ключ.

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 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 ОЦЕНКА НА РИСКА

1. Отчитайки установени бизнес и технически проблеми при доставка, опериране и поддръжка на удостоверителните услуги, Доставчикът извършва оценка на риска за да идентифицира, анализира и оцени свързаните с това рискове.
2. Избират се подходящи мерки за избягване на идентифицирани рискове като се отчитат резултатите от оценката на риска. Приеманите мерки гарантират ниво на сигурност, съизмеримо със степента на идентифицираните рискове.
3. Доставчикът документира чрез Практиката и съответните Политики на предоставяните удостоверителни услуги изискванията към сигурността и оперативните процедури, необходими за избягване на идентифицирани рискове.
4. Периодично се изпълнява преглед и оценка на риска с цел преодоляване на идентифицирани рискови фактори.
5. Мениджмънтът на Доставчика одобрява резултатите от оценката на риска, предписаните мерки за преодоляване на идентифицирани рискови фактори и приема установените остатъчни рискове.

8 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, НА CRL И НА OCSP

8.1 ПРОФИЛ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

1. Пълното съдържание (профил) на КУ се съдържа в публикуваните документите за съответните Политики на Доставчика.

8.1.1 Номер на версия

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

8.1.2 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 КУ.
6. Атрибут „Key Usage" - атрибут, който определя употребата и 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 за валидация на удостоверението.
10. Атрибут „Qualified Statements" - атрибутът съдържа указание, че удостоверението е квалифицирано и дали частния ключ е генериран и се съхранява върху QSCD.

8.1.3 Идентификатори на алгоритмите на електронен подпис

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

8.1.4 Форми на именуване

Виж секция „Именуване" от този документ.

8.1.5 Ограничения на имената

Виж секция „Именуване" от този документ.

8.1.6 Идентификатор на Политика

1. КУ се издават съгласно Политика на Доставчика, идентификаторът (OID) на която се вписва в атрибута „Certificate Policy" на удостоверението. Тази Политика на Доставчика е в съответствие с международно установените политики, съгласно ETSI/ITU-T в документи EN 319 411-1/2. Виж Таблица в т.1.3 на документа.

8.1.7 Означение на квалифицираното удостоверение

1. Доставчикът използва в КУ 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) и „id-etsi-qct-eseal“ (oid=0.4.0.1862.1.6.2) и „id-etsi-qcs-QcPDS“

(oid=0.4.0.1862.1.6.5).

8.2 Профил на Списъка на прекратени удостоверения

8.2.1 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.

8.2.2 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.

8.2.3 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 Потребителя;
   - "CACompromise" - компрометиран частен ключ на оперативен УО на Доставчика;
   - "affiliationChange" - променен статус на Потребител 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.

8.3 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.

9 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

9.1 Периодична и обстоятелствена проверка

1. Контрол на правно-регламентираната дейност на Доставчика, свързана с удостоверенията за електронен подпис и нейната съобразност с изискванията на ЗЕДЕУУ 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 Политики относно дейността на Доставчика.
5. Доставчикът изпълнява постоянен контрол върху дейността на РО/МРС.

9.2 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 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.

9.3 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.

9.4 Обхват на проверката

1. Проверката от страна на Органи за оценяване на съответствието с Регламент 910/2014 обхваща нормативно регламентираните изисквания към дейността на Доставчика съгласно ЗЕДЕУУ .
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.

9.5 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.

10 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

10.1 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 Потребителите посредством публикуване на промените на Интернет страницата.
3. Промяната има действие спрямо Потребител от деня, следващ деня на публикацията.
4. В 5 (пет) дневен срок от датата на промяната и доколкото е налице увеличение на цените, Потребителят 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 Потребителят е съгласен с промяната.
6. Промяната на възнагражденията не може да засегне вече заплатени възнаграждения.

10.1.1 Възнаграждения

1. Стойността на договора включва едно или няколко от следните възнаграждения:
   - възнаграждение за издаване и поддържане на КУ;
   - възнаграждение за подновяване на КУ;
   - възнаграждение за извършени по искане на Потребителя 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 Потребителят 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 Потребителя услуги от тях за целите на предоставяните услуги от Доставчика. Те се дължат изцяло от Потребителя 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 Потребителя.

10.1.2 Възнаграждения за удостоверителни, криптографски, информационни и консултантски услуги

1. За услугите по предоставяне и използване на КУ 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 Потребителя се уреждат съгласно общите правила на договора за продажба, респ. договора за наем.
5. При забавяне на плащанията след договорения срок Потребителят 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.

10.1.3 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.

10.1.4 Връщане на удостоверение и възстановяване на плащане

1. Потребител може да възрази относно неточност или непълнота в съдържанието на издадено КУ 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 Потребителя, 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 КУ с вярно съдържание, което Доставчикът ще прекрати незабавно без да възстанови направеното плащане за прекратеното удостоверение.

10.1.5 Безплатни услуги

1. Доставчикът предоставя безплатно регистърни и информационни услуги, свързани с ползване на Публичния регистър, както следва:
   - проверка на публикувано в регистъра КУ на Потребител;
   - 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.

10.2 Финансови отговорности

10.2.1 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 ЗЕДЕУУ и НОПДДУУ.
4. Доставчикът има задължителна застраховка в размер на застрахователни суми посочени в НОПДДУУ.
5. Задължителната застраховка покрива отговорността на Доставчика към Потребители, съответно Доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в ЗЕДЕУУ и НОПДДУУ.
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.

10.2.2 Застрахователно покритие

1. Застрахователното покритие за нанесени неимуществени и/или имуществени вреди на Потребител не надхвърля размера установен от НОПДДУУ.
2. Застраховката не покрива случаите по отказ на отговорност, в частност за вреди причинени от:
   - неспазване на задълженията на Потребител;
   - компрометиране или загуба на частен ключ на Потребител 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.

10.3 Конфиденциалност на бизнес информация

10.3.1 Обхват на конфиденциалната информация

1. Информация за Потребител, 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, в това число при:
   - Проверки на Комисията за защита на лични данни;
   - Проверки на външни и вътрешни одитори за доказване съответствие към стандарти, закони, наредби, правилници и други регулаторни изисквания, изрично необходими за реализирането на бизнес процесите на Доставчика;
   - Предоставяне на държавни институции, когато това е законосъобразно и изрично се изисква.
4. 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 Потребителя с изключение на случаите, при които Доставчикът е задължен по силата на закон.
5. Никой освен Потребител, включително и Доставчика, няма право да използва частния ключ за създаване на електронен подпис. Доставчикът препоръчва Потребителя да не излага потребителския код за достъп до частния ключ на КУ, дори ако той е шифрован.
6. Всички частни ключове на лица от персонала и звена в инфраструктурата на Доставчика са надеждно защитени срещу компрометиране и разпространение.
7. Записи в журналите и логовете от системите на Доставчика се разглеждат като конфиденциална информация и са защитени от неправомерен достъп и въздействие.

10.3.2 Неконфиденциална информация

1. Общодостъпна е всяка информация, съдържаща се в Публичния регистър по отношение на издадените удостоверения, (освен ако Потребителят е посочил опция „забрана на достъпа“) както и в публикувания актуален CRL и в архивните копия на този списък.

10.3.3 Защита на конфиденциалната информация

1. Доставчикът и Потребителят 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.

10.4 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 Потребители, станали му известни при изпълнение на дейността си като ДКУУ.
3. Личните данни, които Доставчикът събира, съгласно т.10.3.1, се съхраняват и обработват единствено и само за целите на предоставяните от Доставчика удостоверителни услуги в съответствие с изискванията на ЗЕДЕУУ, действащата нормативна уредба и GDPR
4. Съгласно утвърдените Политики на КУ, 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".
5. Потребителят, в качеството си на субект на лични данни има правото:
   - Да изисква от Доставчика да коригира, или ограничи обработването на неговите лични данни или да направи възражение срещу тяхното обработване;
   - Да изисква от Доставчика да изтрие без ненужно забавяне неговите лични данни, което ще се извърши от Доставчика, ако са приложими условията на чл.17 от GDPR;
   - Да получи своите лични данни при поискване по съответния ред, описан в т.10.11.
   - На преносимост за лични данни, при условията нас Чл.20 от GDPR и нормативна а уредба в страната.
   - Да бъде уведомен за извършените корекции, направено изтриване и ограничаване в обработката на неговите лични данни, ако изрично поиска това.
   - Да подава жалба до надзорния орган – Комисията за защита на личните данни, по отношение на неговите лични данни, които са предоставени на Доставчика

10.5 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 Потребители, се запазват от собствениците 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.

10.6 Отговорност и гаранции

10.6.1 Отговорност и гаранции на Доставчика

1. Доставчикът отговоря и гарантира, че спазва точно условията в настоящия документ, изискванията на ЗЕДЕУУ 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 КУ 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 КУ;
   - прекратява и спира действието на удостоверения при условията и по реда на съответната Политика;
   - уведомява незабавно след спиране на удостоверение Потребител;
   - 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 КУ да отмени валидността му;
   - информира Потребителите 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 ЗЕДЕУУ 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 ЗЕДЕУУ, в съответствие със Застрахователната политика;
   - поддържа персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността;
   - публикува и осигурява достъп до утвърдено мобилно приложение за облачен КЕП;
   - поддържа Регистър, в който публикува издадените КУ, актуален CRL, други обстоятелства и електронни документи, съгласно този документ и ЗЕДЕУУ;

- 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 КУ 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;
- при извършване на обичайната дейност на БОРИКА по предоставяне на всички удостоверителни услуги от портфолиото на Борика АД, доставчикът не дискриминира по никакъв начин своите клиенти и служители.

3. Доставчикът отговаря пред Потребител 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.

10.6.2 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 Политиките и издадените вътрешни оперативни инструкции.
2. Доставчикът отговаря за действията на РО/МРС в инфраструктурата на B-Trust.

10.6.3 Отговорност на Потребителя

1. Потребителят 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 съответната Политика. Всяко използване на частния ключ се приема като извършено от Потребителя 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 в 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 КУ;
- приема условията за грижата и отговорността при доверяване на КУ, в случай че действа като Доверяваща се страна.

2. Потребителят е отговорен ако е приел КУ, издадено от Доставчика въз основа на предоставени от него неверни данни, съответно въз основа на премълчани или липсващи данни.
3. Доставчикът ще регресира спрямо Потребителя 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 Потребителят 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 Потребител не е бил овластен да поиска издаването на удостоверението.

10.6.4 Грижа и отговорност на Доверяваща се страна

1. Лицата, които се доверяват на КУ трябва да притежават основни познания относно принципите на използване и приложимост на електронния подпис/печат и на услугите, свързани с употреба на удостоверението.
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 подписа/печата, както и валидността на електронния подпис/печат 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 сигурна (квалифицирана) проверка (валидация), която гарантира, че:
   - публичният ключ, който се използва за проверка на подписа/печата съответства на този, който се представя в удостоверението;
   - 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/подпечатан електронен документ/изявление;
   - автентичността и валидността на удостоверението към момента на подписването/подпечатване надеждно се проверяват;
   - резултатите от проверката и електронната идентичност на Потребителя на КУ 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.

10.7 Отказ от отговорност

1. С изключение на случаите на претърпени вреди от използване и доверяване на КУ, 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 Потребителя 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 Потребителя.
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 Потребители 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 Потребител, телекомуникационни и енергийни смущения и др.
8. Доставчикът не отговаря за вреди, причинени от използване на КУ извън обхвата на вписаните в него ограничения и предназначения.

10.8 Ограничение на отговорност на Доставчика

1. За издавани КУКЕП/КУКЕПечат, Доставчикът отговаря в рамките на максимален лимит на отговорност 40000 лв.
2. Посочените лимити на отговорност се считат за ограничения на отговорността на Доставчика.

10.9 Компенсации за Доставчика

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

10.10 Срок и прекратяване

1. Разпоредбите в настоящия документ, както и асоциираните с него Политики на предоставяне на КУ и 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 Политиките ассоциирани с 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 на този документ и асоциираните с него Политики.

10.11 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: 0700 199 10
   имейл адрес: info@b-trust.org
   Официална страница на доставчика: https://www.b-trust.bg

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

10.12 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.

10.13 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.

10.14 Приложимо право

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

българското законодателство.

10.15 Съответствие с приложимото право

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