БОРИКА
БАНКОВИ УСЛУГИ

ПОЛИТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, ОБЛАЧЕН КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС И КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ ОТ „БОРИКА” АД

(B-Trust QCP-eIDAS QES/CQES/QESeal)

Версия 5.0

В сила от:

1 Април 2019 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
4.0	Димитър Николов	20.05.2018	Утвърден	Отделяне на документа от общата Политика и Практика. Добавяне на Политики при предоставяне на Квалифицирани удостоверения за квалифициран електронен печат и Квалифицирани удостоверения за облачен квалифициран електронен подпис.
5.0	Димитър Николов	01.04.2019	Утвърден	Технически корекции.

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 Квалифициран Електронен Подпис
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на КУ и квалифицирани удостоверителни услуги
Политика	Политика за предоставяне на КУ и квалифицирани удостоверителни услуги
О_КЕП	Облачен КЕП
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
DSA	Digital Signature Algorithm – Вид криптографски алгоритъм за създаване на подпис
DN	Distinguished Name – Уникално име
ETSI	European Telecommunications Standards Institute - Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз
FIPS	Federal Information Processing Standard – Федерален стандарт за обработка на информация
HSM	Hardware Security Module – специализирана хардуерна криптосистема за съхранение и работа с криптографски ключове
IEC	International Electrotechnical Commission - Международна електротехническа комисия
ISO	International Standardization Organization - Международна организация за стандартизация
IP	Internet Protocol – Интернет протокол
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за 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 – Квалифицирано устройство за сигурно създаване на подписа
SAD	Signature Activation Data – Данни за активация на подписа
SAP	Signature Activation Protocol – Протокол за активация на подписа
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;
- влиза в сила на 01.07.2018г.;
- е с наименование „Политика при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис, квалифициран облачен електронен подпис и квалифициран електронен печат от „БОРИКА“ АД (B-Trust CP-eIDAS QES/CQES/QESeal)”;
- се асоциира с публикуваната актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS)“, която съдържа общите условия и изисквания към процедурите при идентификация, при издаване и поддържане на КУ, както и изискванията за ниво на сигурност при генерация и съхраняване на частния ключ за тези удостоверения;
- е разработен в съответствие с формалните изисквания за съдържание, структура и обхват, посочени в международната препоръка RFC 3647, включвайки секциите, които са специфични и приложими за включените в документа квалифицирани удостоверения;
- 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 ЗЕДЕУУ. Договорът може да съдържа специални условия, които се ползват с предимство пред общите условия в настоящия документ;
- е публичен документ с цел установяване на съответствие на дейността на Доставчика „БОРИКА“ АД 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 документа 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 319 412-1,2,3 и 5: Certificate 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.

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.bg

ВЪВЕДЕНИЕ

Тази Политика:

- визира само квалифицираните удостоверения за квалифициран електронен подпис, облачен квалифициран електронен подпис и квалифициран електронен печат, издавани от „БОРИКА“ АД в съответствие с Регламент (ЕС) № 910/2014 и приложимото законодателство в Република България;
- описва конкретните условия и изисквания, които Доставчикът изпълнява при издаване и поддръжка на КУКЕП, КУ за облачен КЕП и КУКЕПечат, както и тяхната приложимост с оглед на нивото на сигурност и ограниченията при използването им;
- определя техническите профили и съдържание на квалифицираните удостоверения;
- се изпълнява чрез общите технически процедури и отговаря на техническите изисквания за ниво на сигурност при генериране и съхраняване на частния ключ, съответстващ на публичен ключ в удостоверенията, посочени в Практиката на Доставчика (документ B-Trust CPS-eIDAS);
- определя приложимостта и степента на доверие в удостоверените факти в КУКЕП, КУ за облачен КЕП и КУКЕПечат.

Приема се, че Потребител, който ползва този документ, има познания и разбиране относно инфраструктурата на публични ключове, удостоверенията и концепцията за електронен подпис и печат. В противен случай, препоръчва се той да се запознае с тези концепции както и с документа „Практиката при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги на „БОРИКА“ АД (B-Trust CPS-eIDAS)“, преди да ползва настоящия документ. При всички случаи, настоящия документ (Политика) следва да се ползва съвместно с Практиката на Доставчика (B-Trust CPS-eIDAS).

Инфраструктурата за публични ключове (PKI) B-Trust® на „БОРИКА” АД е изградена и функционира в съответствие с правната рамка на Регламент 910/2014 и ЗЕДЕУУ и с международните спецификации и стандарти ETSI EN 319 411-1/5 и ETSI EN 319 412. Доставчикът използва идентификатори на обектите (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 с 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).

„БОРИКА“ АД е уведомило КРС за започване на дейност като ДКУУ по реда на ЗЕДЕУУ и действащата нормативна уредба. Доставчикът уведомява Потребителите за своята акредитация при предоставяне на посочените КУ в този документ.

Акредитацията на „БОРИКА“ АД като ДКУУ в съответствие с Регламента и ЗЕДЕУУ цели най-високо ниво на сигурност на предоставяните КУ съгласно тази Политика и по-добро хармонизиране на тази дейност със съответната такава в страните-членки на Европейския съюз.

В отношенията с Потребителите и трети лица е валидна само версията на Политиката, която е актуална към момента на ползване на КУ за квалифициран електронен подпис, облачен квалифициран електронен подпис и квалифициран електронен печат, издавани на „БОРИКА“АД.

1 ОБЩА ХАРАКТЕРИСТИКА НА УДОСТОВЕРЕНИЯТА

Съгласно тази Политика, ДКУУ „БОРИКА“ АД издава и поддържа следните типове квалифицирани удостоверения:

- 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 QES);
- КУКЕПечат (B-Trust Organization qualified certificate QESeal).

Тези удостоверения имат характер на квалифицирани удостоверения за квалифициран електронен подпис (КЕП), за облачен КЕП и за квалифициран електронен печат (КЕПечат) по смисъла на Регламент 910/2014.

1.1 Персонално КУКЕП - Обща характеристика

1. Удостоверението за електронен подпис, издадено по тази политика, има характер на КУКЕП по смисъла Регламент 910/2014 и на чл. 16 от ЗЕДЕУУ.
2. Персонално КУКЕП се издава на физическо лице – Титуляр на КЕП и удостоверява електронната идентичност на Титуляря на подписа и връзката на Титуляря с публичния му ключ в удостоверението.
3. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Титуляря или упълномощено от него лице при проверка на неговата самоличност от Доставчика.
4. Процедурата по идентификация включва представяне на доказателства за самоличността на Титуляря и тяхната проверка.
5. Проверката на искането за издаване на Персонално КУКЕП се извършва по реда на предходните точки и осигурява най-високо ниво на сигурност по отношение на идентичността на Титуляря и връзката му с публичния ключ.
6. Титулярят може сам да генерира двойката ключове, като използва B-Trust QSCD и съответен софтуер за него или друго еквивалентно QSCD, което е съвместимо в инфраструктурата на Доставчика.
7. Частният ключ за създаване на Персонално КУКЕП на физическо лице задължително се генерира в QSCD и не може да бъде изведен навън от него.
8. Издаденото Персонално КУКЕП на физическо лице, удостоверяващо публичен ключ съответстващ на частния такъв, задължително се записва в QSCD, което се предоставя на Потребителя.
9. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Персонално КУКЕП на физическо лице.

1.2 Персонално КУ за облачен КЕП

1. Удостоверението за облачен електронен подпис, издадено по тази политика, има характер на КУ по смисъла на Регламент 910/2014.
2. Персонално КУ за облачен КЕП се издава на физическо лице - Титуляр на облачния КЕП и удостоверява електронната идентичност на Титуляря на подписа и връзката на Титуляря с публичния му ключ в удостоверението.
3. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Титуляря или упълномощено от него лице при проверка на неговата самоличност от Доставчика.
4. Процедурата по идентификация включва представяне на доказателства за самоличността на Титуляря, принадлежността на смартфона с мобилното приложение за облачен КЕП, което се регистрира в потребителския акаунт на Титуляря и тяхната проверка.
5. Проверката на искането за издаване на Персонално КУ за облачен КЕП се извършва по реда на предходните точки и осигурява най-високо ниво на сигурност по отношение на идентичността на Титуляря, връзката му с публичния ключ и неговия персонален контрол

върху достъпа до частния ключ и данните за активиране на подписа.
6. Титулярят генерира двойката ключове при Доставчика, като използва B-Trust QHSM модул в платформата за облачен КЕП и съответен софтуер, поддържащ SAD/SAP схема за сигурен персонален контрол върху частния ключ на облачния КЕП.
7. Частният ключ за създаване на Персонално КУ за облачен КЕП е сигурно защитен в платформата за облачен КЕП чрез утвърдени криптографски схеми с еквивалентно ниво на сигурност, съответстващо за B-Trust QSCD устройство.
8. Издаденото Персонално КУ за облачен КЕП на физическо лице, удостоверяващо публичен ключ съответстващ на частния такъв не се предоставя на Титуляря, но се публикува в Публичния регистър на Доставчика и е достъпно за проверка на валидност.
9. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Персонално КУ за облачен КЕП на физическо лице.

1.3 Професионално КУКЕП – Обща характеристика

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

1.4 Професионално КУ за облачен КЕП

1. Удостоверението за облачен електронен подпис, издадено по тази политика, има характер на КУ по смисъла на Регламента и чл. 16 от ЗЕДЕУУ.
2. Професионално КУ за облачен КЕП се издава на Потребител-титуляр - физическо лице, което е асоциирано с юридическо лице и удостоверява електронната идентичност на Титуляря на подписа и връзката на Титуляря с публичния му ключ в удостоверението.
3. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Потребителя или упълномощено от него лице при проверка на неговата самоличност от Доставчика.
4. Процедурата по идентификация включва представяне на доказателства за самоличността на Потребителя-титуляр, принадлежността на смартфона с мобилното приложение за облачен КЕП, което се регистрира в потребителския акаунт на Потребителя и тяхната

проверка.

5. Проверката на искането за издаване на Професионално КУ за облачен КЕП се извършва по реда на предходните точки и осигурява най-високо ниво на сигурност по отношение на идентичността на Потребителя-титуляр, връзката му с публичния ключ и неговия персонален контрол върху достъпа до частния ключ и данните за активиране на подписа.
6. Потребителят генерира двойката ключове при Доставчика, като използва B-Trust QHSM модул в платформата за облачен КЕП и съответен софтуер, поддържащ SAD/SAP схема за сигурен персонален контрол върху частния ключ на облачния КЕП.
7. В искането за издаване на Професионално КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице се посочва и лицето, което Потребителя-титуляр представлява. Проверява се и идентичността и на това лице.
8. Частният ключ за създаване на Професионално КУ за облачен КЕП е сигурно защитен в платформата за облачен КЕП чрез утвърдени криптографски схеми с еквивалентно ниво на сигурност, съответстващо за B-Trust QSCD устройство за създаване на КЕП.
9. Издаденото Професионално КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице, удостоверяващо публичен ключ съответстващ на частния такъв, не се предоставя на Потребителя, но се публикува в Публичния регистър на Доставчика и е достъпно за проверка на валидност.
10. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Професионално КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице.

1.5 КУКЕПечат – Обща характеристика

1. Удостоверението за електронен печат, издадено по тази политика, има характер на КУКЕПечат по смисъла на Регламент 910/2014 и на ЗЕДЕУУ.
2. КУКЕПечат се издава само на юридическо лице - Създател на печат и служи да автентифицира източника и интегритета на данните или електронните изявления и връзката на Създателя с публичния му ключ.
3. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на упълномощено от Създателя физическо лице за проверка на идентичността на юридическото лице и самоличност на упълномощеното лице от Доставчика.
4. Процедурата по идентификация включва представяне на доказателства за идентичността на Създателя и на упълномощеното лице и тяхната проверка.
5. Проверката на искането за издаване на КУКЕПечат се извършва по реда на предходните точки и осигурява най-високо ниво на сигурност по отношение на идентичността на Създателя и връзката му с публичния ключ.
6. В искането за издаване на КУКЕПечат може да се посочва и физическото лице, което Създателя е упълномощил да го представлява. Проверява се и самоличността и на физическото лице.
7. Създател може сам да генерира двойката ключове, като използва B-Trust QSCD и съответен софтуер за него или друго еквивалентно QSCD, което е съвместимо в инфраструктурата на Доставчика.
8. Частният ключ за създаване на КУКЕПечат задължително се генерира в QSCD и не може да бъде изведен навън от него.
9. Издаденото КУКЕПечат на юридическо лице, удостоверяващо публичен ключ съответстващ на частния такъв, задължително се записва в QSCD, което се предоставя на Създателя.
10. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към КУЕПечат на юридическо лице.

1.6 Идентификатори на Политиката

1.6.1 Персонално КУКЕП и Персонално КУ за облачен КЕП – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Персонални КУКЕП и КУ за облачен КЕП на физическо лице с идентификатор на текущата политика O.I.D. =

1.3.6.1.4.1.15862.1.6.1.1, която съответства на политика „QCP-n-qscd“ (OID 0.4.0.194112.1.2) по ETSI EN 319 411-2.
2. Доставчикът допълнително вписва в Персонални КУКЕП и КУ за облачен КЕП политика „qcp-public-with-sscd“ (O.I.D. = 0.4.0.1456.1.1) по ETSI EN 101 456, с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
3. Доставчикът вписва в Персонални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcCompliance “ (OID=0.4.0.1862.1.1), с което обозначава, че удостоверението е квалифицирано.
4. Доставчикът вписва в Персонални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор: „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4), с което обозначава, че частния ключ е генериран, съхранява се и се използва с QSCD.
5. Доставчикът вписва в Персонални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор: „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1), с което обозначава, че удостоверението се използва за полагане на квалифициран електронен подпис.
6. Доставчикът вписва в Персонални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS” (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса (URL-линк), на който е публикувана B-Trust „Публична Декларация” (Disclosure Statements) на Доставчика.

1.6.2 Професионално КУКЕП и Професионално КУ за облачен КЕП – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Професионалните КУКЕП и КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице, с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2, която съответства на политика „QCP-n-qscd“ (OID 0.4.0.194112.1.2) по ETSI EN 319 411-2.
2. Доставчикът допълнително вписва в Професионални КУКЕП и КУ за облачен КЕП политика „qcp-public-with-sscd“ (O.I.D. = 0.4.0.1456.1.1) по ETSI EN 101 456, с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
3. Доставчикът вписва в Професионални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcCompliance “ (OID=0.4.0.1862.1.1), с което обозначава, че удостоверението е квалифицирано.
4. Доставчикът вписва в Професионални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор: „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4), с което обозначава, че частния ключ е генериран, съхранява се и се използва върху QSCD.
5. Доставчикът вписва в Професионални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор: „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1), с което обозначава, че удостоверението се използва за полагане на квалифициран електронен подпис.
6. Доставчикът вписва в Професионални КУКЕП и КУ за облачен КЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS” (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса (URL-линк), на който е публикувана B-Trust „Публична Декларация” (Disclosure Statements) на Доставчика.

1.6.3 КУКЕПечат – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в КУКЕПечат на юридическо лице с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.6.1.3, която съответства на политика „QCP-l“ (OID 0.4.0.194112.1.1) по ETSI EN 319 411-2.
2. Доставчикът вписва в КУКЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcCompliance” (OID=0.4.0.1862.1.1), с което обозначава, че удостоверението е квалифицирано.
3. Доставчикът вписва в КУКЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcSSCD” (OID=0.4.0.1862.1.4), с което обозначава, че частния ключ е генериран, се

съхранява и се използва върху QSCD.

4. Доставчикът вписва в КУКЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcType" (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-eseal" (oid=0.4.0.1862.1.6.2), с което обозначава, че удостоверението се използва за полагане на усъвършенстван електронен печат.
5. Доставчикът вписва в КУКЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS" (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса (URL-линк), на който е публикувана B-Trust „Публична Декларация" (Disclosure Statements) на Доставчика.

1.7 Предназначение и приложимост на удостоверенията

1.7.1 Персонално КУКЕП и Персонално КУ за облачен КЕП

1. Персонални КУКЕП и КУ за облачен КЕП на физическо лице могат да се използва при създаване на КЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват най-високо ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в Персонални КУКЕП и КУ за облачен КЕП обозначената политиката, приложима към това удостоверение (атрибут "Certificate Policy") и предназначението и ограниченията на действието на удостоверението, описани в атрибутите "Key Usage" и "Extended Key Usage", преди да се довери на положения електронен подпис.
4. Персоналните КУКЕП и КУ за облачен КЕП имат значението на саморъчен подпис спрямо всички по смисъла на Регламент 910/2014 г. и на чл.13, ал.3 на ЗЕДЕУУ и идентифицира Потребителя като Титуляр на КЕП.
5. Персонални КУКЕП и КУ за облачен КЕП могат 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.

1.7.2 Професионално КУКЕП и Професионално КУ за облачен КЕП

1. Професионални КУКЕП и КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице могат да се използва при създаване на КЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват най-високо ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в Професионалните КУКЕП и КУ за облачен КЕП обозначената политиката, приложима към това удостоверение (атрибут "Certificate Policy") и предназначението и ограниченията на действието на удостоверението, описани в атрибутите "Key Usage" и "Extended Key Usage", преди да се довери на положения електронен подпис.
4. Професионални КУКЕП и КУ за облачен КЕП има значението на саморъчен подпис спрямо всички по смисъла на Регламент 910/2014 г. и на чл.13, ал.3 на ЗЕДЕУУ и идентифицира Потребителя като Титуляр на КЕП.
5. Професионалните КУКЕП и КУ за облачен КЕП могат 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.

1.7.3 КУКЕПечат

1. КУКЕПечат на юридическо лице се използва при създаване на КЕПечат от Създателя посочен в удостоверението към електронни документи и в електронни транзакции/приложения, които изискват най-високо ниво на информационна сигурност.
2. В съответствие с Регламент 910/2014 ЕС, КУКЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. КУКЕПечат служи само да автентифицира източника и интегритета на подпечатени електронни документи/изявления (от „електронен“ офис/организация). Когато за дадена транзакция се изисква квалифициран електронен подпис на юридическо лице, квалифицираният електронен подпис на упълномощения представител на юридическото лице се приема равностойно.
3. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява печата, когато се доверява на квалифициран електронен печат, придружен от това удостоверение.
4. Доверяващата се страна следва да провери в КУКЕПечат обозначената политиката, приложима към това удостоверение (атрибут "Certificate Policy") и предназначението и ограниченията на действието на удостоверението, описани в атрибутите "Key Usage", "Extended Key Usage", и „Qualified Statements" преди да се довери на положения електронен печат.
5. 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.

1.8 Ограничение на удостоверителното действие

1. Ако КУ се издава с ограничение на удостоверителното Практиката на Доставчика допуска да се вписва в удостоверението ограничение по отношение на цели или стойност на сделки между Потребители и Доверяващи се страни при използване на квалифициран електронен подпис/печат.
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 автоматично подпечатени електронни документи/изявления („електронен” офис/организация).

1.9 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.

1.10 Управление на Политиката на Доставчика

1. Политиката на Доставчика (този документ) 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.
4. Коментари, запитвания и разяснения по този документ могат да се отправят на:
   - електронен адрес на Удостоверяващ орган: info@b-trust.org;

- електронен адрес на Доставчика: info@borica.bg;
- тел.: 0700 199 10.

2 ПРОФИЛИ НА УДОСТОВЕРЕНИЯТА

2.1 Профил на Персонално КУКЕП и Персонално КУ за облачен КЕП

1. Персоналните КУКЕП и КУ за облачен КЕП имат един и същ профил.
2. Доставчикът издава Персонално КУКЕП (B-Trust Personal qualified certificate QES) и Персонално КУ за облачен КЕП (B-Trust Personal qualified certificate CQES) с посочения по-долу профил:

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

Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2	
Enhanced Key Usage	-	Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.0)
		id-etsi-qcs-QcCompliance (QcSSCD) (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

2.2 Профил на Професионално КУКЕП и на Професионално КУ за облачен КЕП

1. Професионалните КУКЕП и КУ за облачен КЕП имат един и същ профил.
2. Доставчикът издава Професионално КУКЕП на физическо лице, асоциирано с юридическо лице (B-Trust Professional qualified certificate QES) и Професионално КУ за облачен КЕП на физическо лице, асоциирано с юридическо лице (B-Trust Professional qualified certificate CQES) с посочения по-долу профил:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG

Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN =	[Обичайно име: Избрано от физическото лице име. Ако не е избрано, се вписва пълното име на физическото лице]
	G =	[Собствено име на физическото лице според документ за самоличност]
	SN =	[Фамилно име на физическото лице според документ за самоличност]
	SERIALNUMBER =	[Идентификатор на физическото лице. • За български гражданин - един от следните: ○ PNOBG-XXXXXXXXXX за ЕГН ○ PASSBG-XXXXXXXX за номер на паспорт ○ IDCBG-XXXXXXXXX за номер на лична карта ○ TINBG-XXXXXXXXX за ДДС номер на физическо лице ○ PI:BG-XXXXXXXXXX за личен номер на чужденец ○ BT:BG-XXXXXXXXXX за номер на физическо лице, издаден от B-Trust УО • За чуждестранно лице – един от следните: ○ PNOYY- XXXXXXXXXX за национален личен номер ○ PASSYY- XXXXXXXX за номер на паспорт ○ IDCYY- XXXXXXXXX за национален номер на лична карта където YY е двубуквен код на държавата на физическото лице според ISO 3166]
	O =	[Наименование на юридическото лице]
	2.5.4.97= (organizationIdentifier)	[Идентификатор на юридическо лице, с което физическото лице е асоциирано. Един от следните: • VATBG-XXXXXXXXX – за ДДС номер • NTRBG-XXXXXXXXX – за ЕИК (БУЛСТАТ)]
	E =	[Имейл адрес]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[хеш на „Public key "]
Authority Key Identifier	KeyID =	[хеш на „Public key " на „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.2 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2
Enhanced Key Usage	-	Client Authentication, Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name:

		URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

2.3 Профил на КУКЕПечат

1. Доставчикът издава КУКЕПечат (B-Trust Organization qualified certificate QES) с посочения по-долу профил:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Начало на периода на валидност]
Validity to	-	[Край на периода на валидност]
Subject	CN=	[Наименование на Създателя (Обичайно име)]
	O =	[Наименование на Създателя (Организация или юридическо лице)]
	2.5.4.97= (organizationIdentifier)	[Идентификатор на Създателя. Един от следните: • VATBG-XXXXXXXXX – за ДДС номер • NTRBG-XXXXXXXXX – за ЕИК (БУЛСТАТ)]
	E =	[Имейл адрес]
	C =	BG или YY където YY е двубуквен код на държавата според ISO 3166, където е регистриран Създателя
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[хеш на „Public key "]
Authority Key Identifier	KeyID =	[хеш на „Public key " на „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3

		[1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.1	
Enhanced Key Usage	-	Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Key Encipherment, Code Signing	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

3 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР

3.1 Публичен Регистър

Съгласно т.2.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

3.2 Публично хранилище на документи

Съгласно т.2.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

3.3 Публикуване на информация за удостоверенията

Съгласно т.2.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

3.4 Честота на публикуване

Съгласно т.2.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

3.5 Достъп до Регистъра и до хранилището

Съгласно т.2.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4 ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ

4.1 Именуване

Съгласно т.3.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4.2 Първоначална идентификация и установяване на идентичност

Съгласно т.3.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4.3 Идентификация и установяване на идентичност при подновяване

Съгласно т.3.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4.4 Идентификация и автентификация при спиране

Съгласно т.3.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4.5 Идентификация и автентификация при прекратяване

Съгласно т.3.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

4.6 Идентификация и автентификация при прекратяване

Съгласно т.3.6 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5 ОПЕРАТИВНИ ИЗИСКВАНИЯ И ПРОЦЕДУРИ

1. Доставчикът, чрез РО/МРС, в рамките на сключен Договор за КУУ, изпълнява следните оперативни процедури за КУУ, приложими към КУ от тази Политика:
   - 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. Тези оперативни процедури на Доставчика са общи за КУКЕП и КУКЕПечат.
3. Доставчикът, чрез РО/МРС, допуска Потребител (Титуляр/Създател) да прекрати договора за удостоверителни услуги между тях.

5.1 Искане за издаване на удостоверение

Съгласно т.4.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.2 Процедура на издаване

Съгласно т. 4.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.3 Издаване на удостоверение

Съгласно т.4.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.4 Приемане и публикуване на удостоверението

Съгласно т.4.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.5 Употреба на двойката ключове и на удостоверението

Съгласно т.4.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.6 Подновяване на удостоверение

Съгласно т.4.6 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.7 Подмяна на двойка криптографски ключове в удостоверение

Съгласно т.4.7 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.8 Промяна в удостоверение

Съгласно т.4.8 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.9 Прекратяване и спиране на удостоверение

Съгласно т.4.9 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.10 Статус на удостоверение

Съгласно т.4.10 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.11 Прекратяване на договор за удостоверителни услуги

Съгласно т.4.11 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

5.12 Възстановяване на ключове

Съгласно т.4.12 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6 СРЕДСТВА, УПРАВЛЕНИЕ И ОПЕРАТИВЕН КОНТРОЛ

6.1 Физически контрол

Съгласно т.5.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.2 Процедурен контрол

Съгласно т.5.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.3 Квалификация и обучение на персонал

Съгласно т.5.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.4 Изготвяне и поддържане на журнали

Съгласно т.5.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.5 Архив и поддържане на архива

Съгласно т.5.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.6 Промяна на ключ

Съгласно т.5.6 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.7 Компрометиране на ключове и възстановяване след аварии

Съгласно т.5.7 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.8 Компрометиране на частен ключ

Съгласно т.5.8 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

6.9 Прекратяване на дейността на Доставчика

Съгласно т.5.9 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

7.1 Генериране и инсталиране на двойка ключове

Съгласно т.6.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.2 Процедура по генериране

Съгласно т.6.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.3 Защита на частен ключ и контрол на криптографския модул

Съгласно т.6.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.4 Други аспекти на управление на двойка ключове

Съгласно т.6.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.5 Данни за активация

Съгласно т.6.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.6 Сигурност на компютърните системи

Съгласно т.6.6 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.7 Развой и експлоатация (жизнен цикъл)

Съгласно т.6.7 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.8 Допълнителни тестове

Съгласно т.6.8 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.9 Мрежова сигурност

Съгласно т.6.9 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

7.10 Удостоверяване на време

Съгласно т.6.10 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

8 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

8.1 Периодична и обстоятелствена проверка

Съгласно т.9.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

8.2 Квалификация на проверяващите лица

Съгласно т.9.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

8.3 Отношения на проверяващите лица с Доставчика

Съгласно т.9.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

8.4 Обхват на проверката

Съгласно т.9.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

8.5 Обсъждане на резултатите и действия с оглед извършената проверка

Съгласно т.9.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

9.1 Цени и такси

Съгласно т.10.1 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от БОРИКА“ АД (B-Trust CPS-eIDAS).

9.2 Финансови отговорности

Съгласно т.10.2 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.3 Конфиденциалност на бизнес информация

Съгласно т.10.3 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.4 Поверителност на лични данни

Съгласно т.10.4 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.5 Права върху интелектуална собственост

Съгласно т.10.5 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.6 Отговорност и гаранции

Съгласно т.10.6 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.7 Отказ от отговорност

Съгласно т.10.7 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.8 Ограничение на отговорност на Доставчика

Съгласно т.10.8 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.9 Компенсации за Доставчика

Съгласно т.10.9 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.10 Срок и прекратяване

Съгласно т.10.10 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.11 Уведомяване и комуникация между страните

Съгласно т.10.11 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.12 Промени в Документа

Съгласно т.10.12 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.13 Решаване на спорове и място (подсъдност)

Съгласно т.10.13 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.14 Приложимо право

Съгласно т 10.14 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9.15 Съответствие с приложимото право

Съгласно т.10.15 от актуална версия на документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS).