Общодостъпен документ

ПОЛИТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ ОТ „БОРИКА” АД

(B-Trust QCP-eIDAS AES/AESeal/CAESeal)

Версия 5.0

В сила от:

1 Март 2026 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Димитър Николов	20.05.2018	Утвърден	Първо издание
2.0	Димитър Николов	01.04.2019	Утвърден	Технически корекции
3.0	Димитър Николов	01.03.2020	Утвърден	Технически корекции
4.0	Маргарита Бонева	10.03.2023	Утвърден	Корекции
5.0	Маргарита Бонева	01.03.2026	Утвърден	Корекции

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК 5
СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК 6
СЪОТВЕТСТВИЕ И УПОТРЕБА 8
ВЪВЕДЕНИЕ 10
Тази Политика: 10
1 ОБЩА ХАРАКТЕРИСТИКА НА УДОСТОВЕРЕНИЯТА 11
Тези удостоверения имат характер на квалифицирани удостоверения за усъвършенстван електронен подпис (УЕП) и за усъвършенстван електронен печат (УЕПечат) по смисъла на Регламент 910/2014. 11
1.1 Персонално КУУЕП 11
1.2 Професионално КУУЕП 11
1.3 КУУЕПечат 12
1.4 Идентификатори на Политиката 13
1.4.1 Персонално КУУЕП – обозначение на Политиката 13
1.4.2 Професионално КУУЕП – обозначение на Политиката 14
1.4.3 КУУЕПечат – обозначение на Политиката 14
1.5 Предназначение и приложимост на удостоверенията 14
1.5.1 Персонално КУУЕП 14
1.5.2 Професионално КУУЕП 15
1.5.3 КУУЕПечат 15
1.6 Ограничение на удостоверителното действие 16
1.7 Употреба на удостоверения извън приложното поле и ограниченията 16
1.8 Управление на Политиката на Доставчика 16
2 ПРОФИЛИ НА УДОСТОВЕРЕНИЯТА 16
2.1 Профил на Персонално КУУЕП 16
2.2 Профил на Професионално КУУЕП 18
2.3 Профил на КУУЕПечат 19
3 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР 21
3.1 Публичен Регистър 21
3.2 Публично хранилище на документи 21
3.3 Публикуване на информация за удостоверенията 21
3.4 Честота на публикуване 21
3.5 Достъп до Регистъра и до хранилището 21
4 ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ 21
4.1 Именуване 21
4.2 Първоначална идентификация и установяване на идентичност 21
4.3 Идентификация и установяване на идентичност при подновяване 21
4.4 Идентификация и автентификация при спиране 22
4.5 Идентификация и автентификация при прекратяване 22
4.6 Идентификация и автентификация при прекратяване 22
5 ОПЕРАТИВНИ ИЗИСКВАНИЯ И ПРОЦЕДУРИ 22
5.1 Искане за издаване на удостоверение 22
5.2 Процедура на издаване 22
5.3 Издаване на удостоверение 22
5.4 Приемане и публикуване на удостоверението 22
5.5 Употреба на двойката ключове и на удостоверението 22
5.6 Подновяване на удостоверение 23
5.7 Подмяна на двойка криптографски ключове в удостоверение 23
5.8 Промяна в удостоверение 23
5.9 Прекратяване и спиране на удостоверение 23
5.10 Статус на удостоверение 23
5.11 Прекратяване на договор за удостоверителни услуги 23
5.12 Възстановяване на ключове 23
6 СРЕДСТВА, УПРАВЛЕНИЕ И ОПЕРАТИВЕН КОНТРОЛ 23
6.1 Физически контрол 23
6.2 Процедурен контрол 23
6.3 Квалификация и обучение на персонал 23
6.4 Изготвяне и поддържане на журнали 24
6.5 Архив и поддържане на архива 24
6.6 Промяна на ключ 24
6.7 Компрометиране на ключове и възстановяване след аварии 24
6.8 Компрометиране на частен ключ 24
6.9 Прекратяване на дейността на Доставчика 24

7 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ 24
7.1 Генериране и инсталиране на двойка ключове 24
7.2 Процедура по генериране 24
7.3 Защита на частен ключ и контрол на криптографския модул 24
7.4 Други аспекти на управление на двойка ключове 24
7.5 Данни за активация 25
7.6 Сигурност на компютърните системи 25
7.7 Развой и експлоатация (жизнен цикъл) 25
7.8 Допълнителни тестове 25
7.9 Мрежова сигурност 25
7.10 Удостоверяване на време 25
8 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА 25
8.1 Периодична и обстоятелствена проверка 25
8.2 Квалификация на проверяващите лица 25
8.3 Отношения на проверяващите лица с Доставчика 25
8.4 Обхват на проверката 25
8.5 Обсъждане на резултатите и действия с оглед извършената проверка 26
9 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ 26
9.1 Цени и такси 26
9.2 Финансови отговорности 26
9.3 Конфиденциалност на бизнес информация 26
9.4 Поверителност на лични данни 26
9.5 Права върху интелектуална собственост 26
9.6 Отговорност и гаранции 26
9.7 Отказ от отговорност 26
9.8 Ограничение на отговорност на Доставчика 26
9.9 Компенсации за Доставчика 26
9.10 Срок и прекратяване 27
9.11 Уведомяване и комуникация между страните 27
9.12 Промени в Документа 27
9.13 Решаване на спорове и място (подсъдност) 27
9.14 Приложимо право 27
9.15 Съответствие с приложимото право 27

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
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
RQSCD	сървърна компонента в платформата за облачен КЕП на B-Trust за сигурно създаване на подпис от разстояние
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 01.03.2026 г.;**
- е с наименование „Политика при предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис/печат от „БОРИКА“ АД (**B-Trust CP-eIDAS AES/AESeal/CAESeal**)";
- 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. 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
- РЕГЛАМЕНТ (ЕС) 2024/1183 на Европейския парламент и на Съвета за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност;

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 TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects“;

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: https://www.b-trust.bg

ВЪВЕДЕНИЕ

Тази Политика:

- визира само квалифицираните удостоверения за усъвършенстван електронен подпис или 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 КУУЕП или КУУЕПечат, 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;
- определя приложимостта и степента на доверие в удостоверените факти в КУУЕП и КУУЕПечат.

Приема се, че Потребител, който ползва този документ, има познания и разбиране относно инфраструктурата на публични ключове, удостоверенията и концепцията за електронен подпис/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 следва да се ползва съвместно с Практиката на Доставчика.

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 усъвършенстван електронен подпис/печат, издавани на „БОРИКА“АД.

1 ОБЩА ХАРАКТЕРИСТИКА НА УДОСТОВЕРЕНИЯТА

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

- Персонално КУУЕП (B-Trust Personal qualified certificate AES);
- Професионално КУУЕП (B-Trust Professional qualified certificate AES);
- КУУЕПечат (B-Trust Legal qualified certificate AESeal);
- КУ за облачен УЕПечат (B-Trust Legal qualified certificate CAESeal).

Тези удостоверения имат характер на квалифицирани удостоверения за усъвършенстван електронен подпис (УЕП) и за усъвършенстван електронен печат (УЕПечат) по смисъла на Регламент 910/2014.

1.1 Персонално КУУЕП

1. Удостоверението за електронен подпис, издадено по тази политика, има характер на КУУЕП по смисъла Регламент 910/2014 и на чл. 16 от ЗЕДЕУУ.
2. Персонално КУУЕП се издава на физическо лице - Титуляр на УЕП 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 за проверка на самоличност. Удостоверяването на личността на Титуляря може да се извърши и чрез средство за електронна/отдалечена идентификация.
4. Процедурата по идентификация включва представяне на доказателства за самоличността на Титуляря и тяхната проверка.
5. Проверката на искането за издаване на Персонално КУУЕП 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 утвърден от Доставчика или друг лицензиран софтуер с еквивалентно ниво на сигурност, който е съвместим с инфраструктурата на Доставчика.
7. Частният ключ за създаване на Персонално КУУЕП на физическо лице се генерира с утвърдения или лицензиран софтуер, съхранява се в софтуерно в преносим криптографски файл и може да бъде пренесен в системи на Потребителя.
8. Издаденото Персонално КУУЕП на физическо лице, удостоверяващо публичен ключ съответстващ на частния такъв се записва в преносим софтуерен токън заедно със служебните удостоверения на Доставчика (PKCS#12 файл), когато двойката ключове се генерира при Доставчика (в МРС) и се предоставя на Титуляря.
9. Когато двойката ключове се генерира при Потребителя-Титуляр, отговорност за създаване на преносим софтуерен токън има Потребителя-Титуляр.
10. Допуска се Титулярят да използва хардуерен токън, съвместим с B-Trust инфраструктурата на Доставчика за генериране и съхраняване на двойката ключове за КУУЕП.
11. Персонално КУУЕП не се подновява, Потребителят-Титуляр може да заяви пред Доставчика да издаде ново КУУЕП с нова двойка ключове.
12. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Персонално КУУЕП на физическо лице.

1.2 Професионално КУУЕП

1. Удостоверението за електронен подпис, издадено по тази политика, има характер на КУУЕП по смисъла на Регламента и чл. 16 от ЗЕДЕУУ.
2. Професионално КУУЕП 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 за проверка на самоличност. Удостоверяването на личността на Титуляря може да се извърши и чрез средство за електронна/отдалечена идентификация.

4. Процедурата по идентификация включва представяне на доказателства за самоличността на Титуляря и за упълномощаването и тяхната проверка.
5. Проверката на искането за издаване на Професионално КУУЕП 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 асоциирането му с юридическото лице.
6. Титулярят може сам да генерира двойката ключове, като използва утвърден от Доставчика или друг лицензиран софтуер с еквивалентно ниво на сигурност, който е съвместим с инфраструктурата на Доставчика.
7. В искането за издаване на Професионално КУУЕП 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 УЕП на физическо лице, асоциирано с юридическо лице, се генерира с утвърдения или лицензиран софтуер, съхранява се софтуерно в преносим криптографски файл и може да бъде пренесен в системи на Потребителя.
9. Издаденото Персонално КУУЕП на физическо лице, асоциирано с юридическо лице се записва в преносим софтуерен токън заедно със служебните удостоверения на Доставчика (PKCS#12 файл), когато двойката ключове се генерира при Доставчика (в МРС) и се предоставя на Титуляря.
10. Когато двойката ключове се генерира при Потребителя-Титуляр, отговорност за създаване на преносим (и/или съхраним) софтуерен токън има Потребителя-Титуляр.
11. Допуска се Титулярят да използва хардуерен токън, съвместим с B-Trust инфраструктурата на Доставчика за генериране и съхраняване на двойката ключове за КУУЕП.
12. Професионално КУУЕП не се подновява, Потребителят-Титуляр може да заяви пред Доставчика да издаде ново професионално КУУЕП с нова двойка ключове.
13. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Професионално КУУЕП на физическо лице, асоциирано с юридическо лице.

1.3 КУУЕПечат

1. Удостоверението за електронен печат, издадено по тази политика, има характер на КУУЕПечат по смисъла на Регламент 910/2014 и на ЗЕДЕУУ.
2. КУУЕПечат 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 Създателя или упълномощено от него лице за проверка на самоличност. Удостоверяването на личността на Създателя може да се извърши и чрез средство за електронна/отдалечена идентификация.
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 КУУЕПечат 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 КУУЕПечат може да се посочва и физическото лице, което Създателя е упълномощил да го представлява. Проверява се самоличността и на физическото лице.
7. Създател може сам да генерира двойката ключове, като използва утвърден от Доставчика или друг лицензиран софтуер с еквивалентно ниво на сигурност, който е съвместим с инфраструктурата на Доставчика.
8. Частният ключ за създаване на КУУЕПечат се генерира се генерира с утвърдения или лицензиран софтуер, съхранява се софтуерно в преносим криптографски файл и може да

бъде пренесен в системи на Потребителя.

9. Издаденото КУУЕПечат на юридическо лице, удостоверяващо публичен ключ съответстващ на частния такъв се записва в преносим софтуерен токън заедно със служебните удостоверения на Доставчика (PKCS#12 файл), когато двойката ключове се генерира при Доставчика (в МРС) и се предоставя на Създателя.
10. Когато двойката ключове се генерира при Потребителя-Създател, отговорност за създаване на преносим софтуерен токън има Потребителя-Създател.
11. Допуска се Създателят да използва хардуерен токън, съвместим с B-Trust инфраструктурата на Доставчика за генериране и съхраняване на двойката ключове за КУУЕПечат.
12. КУУЕПечат не се подновява, Потребителят-Създател може да заяви пред Доставчика да издаде ново КУУЕПечат с нова двойка ключове.
13. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към КУУЕПечат на юридическо лице.

1.4 КУ за облачен УЕПечат

1. КУУЕПечат 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.
2. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Създателя или упълномощено от него лице за проверка на самоличност. Удостоверяването на личността на Създателя може да се извърши и чрез средство за електронна/отдалечена идентификация.
3. Процедурата по идентификация включва представяне на доказателства за самоличността на Създателя физическо лице, доказателство, че по време на искането за издаване юридическото лице съществува и, че Създателя физическо лице е получил разрешение да представлява юридическото лице, както и тяхната проверка.
4. Проверката на искането за издаване на Облачен УЕПечат 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.
5. В искането за издаване на Облачен УЕПечат може да се посочва и физическото лице, което Създателя е упълномощил да го представлява. Проверява се и самоличността и на физическото лице.
6. Частният ключ за създаване на КУ за облачен УЕПечат е сигурно защитен в платформата за облачен КЕП чрез утвърдени криптографски схеми с еквивалентно ниво на сигурност, съответстващо за B-Trust QSCD устройство.
7. Издаденото КУ за облачен УЕПечат не се предоставя на Създателя, а се публикува в Публичния регистър на Доставчика и е достъпно за проверка на валидност
8. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към Облачен УЕПечат на юридическо лице.

1.5 Идентификатори на Политиката

1.5.1 Персонално КУУЕП – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Персонално КУУЕП с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.7.1.1, която съответства на политика „QCP-n“ (OID 0.4.0.194112.1.0) по ETSI EN 319 411-2.
2. Доставчикът допълнително вписва в Персонално КУУЕП политика „qcp-public“ (O.I.D. = 0.4.0.1456.1.2) по ETSI EN 101 456, с което обозначава, че частния ключ не е генериран, не се съхранява и не се използва в QSCD.
3. Доставчикът вписва в Персонално КУУЕП 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 персоналното КУУЕП 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 усъвършенстван електронен подпис.
5. Доставчикът вписва в Персонално КУУЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS" (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса, на който е публикувана B-Trust „Публична Декларация" (Disclosure Statements) на Доставчика.

1.5.2 Професионално КУУЕП – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Професионалното КУУЕП на физическо лице, асоциирано с юридическо лице, с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.7.1.2, която съответства на политика „QCP-n" (OID 0.4.0.194112.1.0) по ETSI EN 319 411-2.
2. Доставчикът допълнително вписва в Професионално КУУЕП политика „qcp-public" (O.I.D. = 0.4.0.1456.1.2) по ETSI EN 101 456, с което обозначава, че частния ключ не е генериран, не се съхранява и не се използва в QSCD.
3. Доставчикът вписва в Професионалното КУУЕП 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 професионалното КУУЕП 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 усъвършенстван електронен подпис
5. Доставчикът вписва в Професионално КУУЕП в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS" (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса, на който е публикувана B-Trust „Публична Декларация" (Disclosure Statements) на Доставчика.

1.5.3 КУУЕПечат/ Облачен КУУЕПечат – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в КУУЕПечат на юридическо лице с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.7.1.3, която съответства на политика QCP-l (OID=0.4.0.194112.1.1) по ETSI EN 319 411-2.
2. Доставчикът допълнително вписва в КУКЕПечат политика „qcp-public" (O.I.D. = 0.4.0.1456.1.2) по ETSI EN 101 456, с което обозначава, че частния ключ не е генериран, не се съхранява и не се използва върху QSCD.
3. Доставчикът вписва в КУУЕПечат 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 КУУЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcType" (OID=0.4.0.1862.1.6), със стойност „id-etsi-qct-esign" (oid=0.4.0.1862.1.6.2), с което обозначава, че удостоверението се използва за полагане на усъвършенстван електронен печат.
5. Доставчикът вписва в КУУЕПечат в атрибута „Qualified Statements" идентификатор „id-etsi-qcs-QcPDS" (OID=0.4.0.1862.1.5) със стойност обозначаваща адреса, на който е публикувана B-Trust „Публична Декларация" (Disclosure Statements) на Доставчика.

1.6 Предназначение и приложимост на удостоверенията

1.6.1 Персонално КУУЕП

1. Персонално КУУЕП на физическо лице може да се използва при създаване на УЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват значително ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и

проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в Персонално КУУЕП 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. Персонално КУУЕП няма значението на саморъчен подпис спрямо всички по смисъла на Регламент 910/2014 г. и на чл.13 на ЗЕДЕУУ и идентифицира лицето като Титуляр на УЕП.
5. Персонално КУУЕП 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 значително ниво на сигурност.

1.6.2 Професионално КУУЕП

1. Професионално КУУЕП на физическо лице, асоциирано с юридическо лице може да се използва при създаване на УЕП от физическото лице посочено като Титуляр в удостоверението, към електронни документи и в приложения, които изискват значително ниво на информационна сигурност.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се създава и проверява подписа, когато се доверява на електронния подпис, придружен от това удостоверение.
3. Доверяващата се страна следва да провери в Професионалното КУУЕП 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. Професионално КУУЕП няма значението на саморъчен подпис спрямо всички по смисъла на Регламент 910/2014 г. и на чл.13 на ЗЕДЕУУ и идентифицира Потребителя като Титуляр на УЕП.
5. Професионално КУУЕП 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 значително ниво на сигурност.

1.6.3 КУУЕПечат

1. КУУЕПечат на юридическо лице се използва при създаване на УЕПечат от Създателя посочен в удостоверението към електронни документи и в електронни транзакции, които изискват значително ниво на информационна сигурност.
2. В съответствие с Регламент 910/2014 ЕС, КУУЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. КУУЕПечат служи само да автентифицира източника и интегритета на подпечатени електронни документи/изявления (от „електронен“ офис/организация). Когато за дадена транзакция се изисква електронен подпис на юридическо лице, квалифицираният или усъвършенстваният 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 КУУЕПечат 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 документи, 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.

1.7 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 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, КУ за КЕПечат не следва да се използва и прилага като електронен подпис на юридическо лице. КУ за КЕПечат служи само да автентифицира източника и интегритета на автоматично подпечатени електронни документи/изявления („електронен" офис/организация).

1.8 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.

1.9 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 КУУЕП

1. Доставчикът издава Персонално КУУЕП на физическо лице (B-Trust Personal qualified certificate AES) 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 Advanced 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 ○ PASBG-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 ○ PASYY- 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=1.3.6.1.4.1.15862.1.7.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.0
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-TrustOperationalACA.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-TrustOperationalACAOCSP.cer
Key Usage (critical)	-	Digital Signature, 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 (oid=0.4.0.1862.1.1)	
		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 КУУЕП

1. Доставчикът издава Професионално КУУЕП на физическо лице, асоциирано с юридическо лице (B-Trust Professional qualified certificate AES) 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 Advanced 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 ○ PASBG-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 ○ PASYY- 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]

	2.5.4.97= (organizationIdentifier	[Identifier of a legal entity with which the individual is associated. One of the following: • VATBG-XXXXXXXXX – for VAT number • NTRBG-XXXXXXXXX – for UIC (BULSTAT	
	O =	[Name of the legal person]	
	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=1.3.6.1.4.1.15862.1.7.1.2 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.0	
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-TrustOperationalACA.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-TrustOperationalACAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax- v2 (oid=1.3.6.1.5.5.7.11. 2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-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 КУУЕПечат/ Облачен КУУЕПечат

1. Доставчикът издава КУУЕПечат (B-Trust legal qualified certificate AESeal/CAESeal) 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 Advanced 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=1.3.6.1.4.1.15862.1.7.1.3 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3] Certificate Policy: Policy Identifier=0.4.0.194112.1.1	
Enhanced Key Usage	-	Client Authentication, Secure Email, Code Signing	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.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-TrustOperationalACAOCSP.cer	
Key Usage (critical)	-	Digital Signature, 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-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 тази Политика, Доставчикът не подновява квалифицирани удостоверения за усъвършенстван електронен подпис/печат. Виж 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;
   - спиране/възобновяване;
   - прекратяване;
   - статус на КУ.
2. Тези оперативни процедури на Доставчика са общи за КУУЕП и КУУЕПечат.
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 тази Политика, Доставчикът не подновява квалифицирани удостоверения за усъвършенстван електронен подпис/печат. Виж 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).