БОРИКА
БАНКОВИ УСЛУГИ

# ПОЛИТИКА

# ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРЕНИЯ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ОТ „БОРИКА” АД

# (B-Trust QCP-eIDAS Web SSL)

Версия 1.0

В сила от:

1 Юли 2018 г.

| Хронология на измененията на документа | | | | |
|---|---|---|---|---|
| **Версия** | **Автор (и)** | **Дата** | **Състояние** | **Коментар** |
| 1.0 | Димитър Николов | 25.05.2018 | Утвърден | Първо издание |
| | | | | |

# СЪДЪРЖАНИЕ

## СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК

| | |
|---|---|
| АД | Акционерно дружество |
| ДВ | Държавен вестник |
| ДКУУ | Доставчик на квалифицирани удостоверителни услуги |
| ЕГН | Единен граждански номер |
| ЕП | Електронен подпис |
| ЗД | Закон за далекосъобщенията |
| 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 |
| НДДУУ | Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията при предоставяне на удостоверителни услуги |
| НИАКЕП | Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис |
| 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 |
| 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 |
| CD | Compact Disk – Компакт диск |
| CEN | European Committee for Standardization - Европейски стандартизационен комитет |
| CENELEC | European Committee for Electrotechnical Standardization - Европейски комитет за електротехническа стандартизация |
| CP | Certificate Policy – Политика за предоставяне на удостоверителни услуги |
| CPS | Certification Practice Statement – Практика при предоставяне на удостоверителни услуги |
| CRL | Certificate Revocation List – Списък с прекратени и спрени удостоверения |
| 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 он-лайн проверка на статуса на удостоверения |
| PKCS | Public Key Cryptography Standards – Криптографски стандарт за публичен ключ |
| PKI | Public Key Infrastructure – Инфраструктура на публичния ключQC 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 подписQSCD Qualified Signature Creation Device – Квалифицирано устройство за сигурно създаване на подписа |
| SAD | Signature Activation Data – Данни за активация на подписа |
| SAP | Signature Activation Protocol – Прокол 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 |
| Website | A collection of related web pages, including multimedia content, typically identified with a common domain name (DN), and published on at least one web server. |

## 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 удостоверения за автентичност на уебсайт от „БОРИКА“ АД (B-Trust CP-eIDAS Web SSL)”;
- 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 на основание чл. 33, ал. 2 Наредбата за Дейността на Доставчиците на Удостоверителни Услуги (НДДУУ) и по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД). Тези условия са част от писмен Договор за удостоверителни услуги, който се сключва между Доставчика и Потребителите на основание чл.23 от 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.org/bg/elektronni-podpisi/dokumenti;
- 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 дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и изискванията при предоставяне на удостоверителни услуги (НДДУУ);
- Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис (НИАКЕП);
- Регламент (ЕС) № 910/2014 на европейския парламент и на съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

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

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1,2,3 и 5: Certificate Profiles;
- CA/Browser Forum: "Baseline Requirements for the Issuance and Management of
- Publicly-Trusted Certificates".

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

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

## ВЪВЕДЕНИЕ

Тази Политика:

- визира удостоверенията за автентичност на уебсайт (Удостоверения SSL/TLS), 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 Удостоверения SSL/TLS, 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 Удостоверения SSL/TLS.

Приема се, че Потребител, който ползва този документ, има познания и разбиране относно инфраструктурата на публични ключове, удостоверенията и концепцията за уебсайт, автентификация на уебсай и протокол SSL/TLS. 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.

Инфраструктурата за публични ключове (PKI) B-Trust® на „БОРИКА” АД е изградена и функционира в съответствие с правната рамка на Регламент 910/2014 и ЗЕДЕП 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 Удостоверения в този документ.

Акредитацията на „БОРИКА“ АД като ДКУУ в съответствие с Регламента и ЗЕДЕУУ цели най-високо ниво на сигурност на предоставяните Удостоверения 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 Удостоверения SSL/TLS, издадвани на „БОРИКА“АД.

# 1 ОБЩА ХАРАКТЕРИСТИКА НА УДОСТОВЕРЕНИЯТА

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

- Удостоверения за автентичност на уебсайт (домейн) - (B-Trust Domain Validation SSL certificate/B-Trust DVC SSL);
- Удостоверения за автентичност на уебсайт (организация) - (B-Trust Organization Validation SSL certificate/B-Trust OVC SSL).

## 1.1 Удостоверения за автентичност на уебсайт (домейн) (DVC SSL) – Обща характеристика

1. Удостоверението B-Trust DVC SSL за автентичност на уебсайт (домейн), издадено по тази политика, има характер на Удостоверение по смисъла на Регкамента и чл. 16 от ЗЕДЕУУ само ако се използва за валидация на домейна.
2. Това удостоверение се издава на Потребител – юридическо лице или физическо лице и удостоверява електронната идентичност на притежателя на домейна, хостващ уебсайт с високо ниво на сигурност за браузърния клиент.
3. Допуска се wild card” (*) в името на хоста (например, *.b-trust.bg).
4. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Потребителя или упълномощено от него лице за изпълнение на процедурата по идентификация от страна на Доставчика.
5. Процедурата по идентификация включва представяне на доказателства за притежание на домейна, хостващ уебсайт и за идентичността на Потребителя и на упълномощеното лице и тяхната проверка.
6. Проверката на искането за издаване на удостоверението за автентичност на уебсайт (домейн) се извършва по реда на предходните точки и осигурява високо ниво на сигурност по отношение на притежаването на домейна от Потребителя (юридическото лице), посочен в удостоверението.
7. Относно използването на TLS/SSL протокола, политиката за това удостоверение допуска достатъчно ниво на осигуреност спрямо браузърния клиент, достъпващ уебсайт в домейна – генерирането и съхранението на частния ключ, съответстващ на публичния ключ в удостоверенето използва утвърден или лицензиран софтуери и криптографски софтуерен токън.
8. Потребителят 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.
9. В искането за издаване на удостоверението за автентичност на уебсайт (домейн) се посочва и лицето, което представлява Потребителя. Проверява се и идентичността и на това лице.
10. Частният ключ за създаване на удостоверението за автентичност на уебсайт (домейн) се генерира с утвърдения или лицензиран софтуер, съхранява се софтуерно в преносим криптографски файл и може да бъде пренесен в системи на Потребителя.
11. Издаденото удостоверение 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 Потребителя.
12. Когато двойката ключове се генерира при Потребителя, отговорността за създаване на преносим (софтуерен токън е на Потребителя.
13. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към удостоверението за автентичност на уебсайт (домейн).

## 1.2 Удостоверения за автентичност на уебсайт (организация) (OVC SSL) – Обща характеристика

1. Удостоверението B-Trust OVC SSL за автентичност на уебсайт (организация), издадено по

тази политика, има характер на Удостоверение по смисъла Регламент 910/2014 и на чл. 16 от ЗЕДЕУУ ако само се използва за валидация.
2. Това удостоверение се издава на Потребител-юридическо лице (организация) или физическо лице и удостоверява електронната идентичност и акредитацията на Потребителя с високо ниво на сигурност за браузърния клиент, че уебсайтът който достъпва е собственост на организацията идентифицирана в удостоверението.
3. Допуска се „wild card" (*) в името на хоста (например, *.b-trust.bg).
4. За издаването на това удостоверение се изисква лично присъствие пред РО/МРС на Потребителя или на упълномощено лице от него за изпълнение на процедурата по идентификация от страна на Доставчика.
5. Процедурата по идентификация включва представяне на доказателства за притежание на домейна, хостващ уебсайта на Потребителя, както и доказателства за идентичността на Потребителя и упълномощеното лице и тяхната проверка.
6. Проверката на искането за издаване на Удостоверения за уебсайта (организация) се извършва по реда на предходните точки и осигурява високо ниво на сигурност по отношение на собствеността на уебсайта и домейна на Потребителя, посочен в удостоверението.
7. Относно използването на TLS/SSL протокола, политиката за това удостоверение допуска достатъчно ниво на осигуреност спрямо браузърния клиент, достъпващ уебсайта – използва се утвърден или лицензирн софтуер и криптографски софтуерен токън за генериране и съхранение на частния ключ, съответстващ на публичния в удостоверението.
8. Потребителят 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.
9. Когато двойката ключове на удостоверението за автентичност на уебсайт (организация) се генерира софтуерно, частният ключ се съхранява в преносим криптографски файл (PKCS#12) и може да бъде пренесен в системи на Потребителя.
10. Когато двойката ключове се генерира софтуерно при Доставчика (в МРС), издаденото удостоверение заедно със служебните удостоверения на Доставчика се записва в преносим софтуерен токън (PKCS#12 файл) и се предоставя на Потребителя.
11. Когато двойката ключове се генерира софтуерно при Потребителя, отговорността за създаване на преносим (и/или съхраняем) софтуерен токън е на Потребителя.
12. Доставчикът запазва право при необходимост да добавя допълнителни атрибути към удостоверението за автентичност на уебсайт (организация).

## 1.3 Идентификатори на Политиката

### 1.3.1 Удостоверения за автентичност на уебсайт (домейн) – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Удостоверения за автентичност на уебсайт (домейн), с идентификатор на текущата политикаOID = 1.3.6.1.4.1.15862.1.7.1.5, която съответства на политика DVC (OID = 0.4.0.2042.1.6) по ETSI TS 102 042.
2. Доставчикът вписва вписва в атрибута „Certificate policy" на удостоверението политика с OID = 2.23.140.1.2.1, съответстваща на CA/B Forum SSL DV ако удостоверението изпълнява само валидация на домейн (Compliant with Baseline Requirements – No entity identity asserted).

### 1.3.2 Удостоверения за автентичност на уебсайт (организация) – обозначение на Политиката

1. Доставчикът поддържа и прилага обща политика, обозначена в Удостоверения за автентичност на уебсайт с идентификатор на текущата политика O.I.D. = 1.3.6.1.4.1.15862.1.7.1.6, която съответства на политика "OVC" (OID = 0.4.0.2042.1.7) по ETSI TS 102 042.
2. Доставчикът вписва в атрибута „Ceficate policy" на удостоверението политика с OID =

2.23.140.1.2.2, съответстваща на CA/B Forum SSL OV ако Потребителят на удостоверението е юридическо лице (организация/институция) (Compliant with Baseline Requirements – Organization identity asserted).

## 1.4 Предназначение и приложимост на удостоверенията

### 1.4.1 Удостоверение за автентичност на уебсайт (домейн) – B-Trust DVC SSL

1. Удостоверение за автентичност на уебсайт (домейн) се използва да идентифицира притежателя на домейн и акредитацията на лицето (Потребителя) с достатъчно ниво на сигурност за браузърния клиент, че достъпвания от него уебсайт е собственост на лицето, което е идентифицирано в удостоверението.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се използва удостоверението.
3. Доверяващата се страна следва да провери 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 това удостоверение.
4. Валидността на удостоверението за автентичност на уебсайт (домейн) е 1 (една) или 2 (две) години. Удостоверението не подлежи на подновяване. Доставчикът издава ново удостоверение за автентичност на уебсайт (домейн).

### 1.4.2 Удостоверение за автентичност на уебсайт (организация) – B-Trust OVC SSL

1. Удостоверение за автентичност на уебсайт (организация) основно се използва да установи обмен на данни чрез TLS/SSL протоколи за услуги и приложения, и конкретно:
   - да идентифицира организацията, която притежава домейна (DNS), предоставяйки допустимо ниво на сигурност за браузърния клиент, че уебсайтът който достъпва е на организация, идентифицирана в удостоверението чрез име и адрес;
   - криптиране на комуникации между клиент и уебсайт като улеснява обмена на криптоключове за защита на данните през Интернет.
2. Дължима грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението и софтуерните приложения, с които се използва удостоверението.
3. Доверяващата се страна следва да провери 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 удостоверението.
4. Валидността на удостоверението за автентичност на уебсайт (организация) е 1 (една) или 2 (две) години. Удостоверението не подлежи на подновяване. Доставчикът издава ново удостоверение за автентичност на уебсайт (организация).

## 1.5 Ограничение на удостоверителното действие

1. Удостоверителното действие при употреба на удостоверенията за автентичност на уебсайт е регламентирано само в обхвата на тяхното приложно поле съгласно т. 1.5 на тази Политика. Всяка друга употреба на удостоверенията е нерегламентирана и девалидира удостоверителното им действие.
2. Удостоверенията за автентичност на уебсайт не следва да се прилагат за дейности, попадащи под ограничения и забрана съгласно законодателството на Р. България, както и приложимите регламенти и директиви на ЕС.
3. Ако Удостоверение се издава с ограничение на удостоверителното действие, Практиката на Доставчика допуска да се вписва в удостоверението ограничение по отношение на цели и/или стойност на сделки между Потребители и Доверяващи се страни при използване на удостоверение за автентичност на уебсайт.
4. Ограничителното действие на Удостоверение за автентичност на уебсайт по отношение на

стойности на сделки при онлайн електронни транзакции между Потребители и Доверяващи се страни и е извън обхвата на настоящия документ.

### 1.6 Употреба на удостоверения извън приложното поле и ограниченията

1. Когато Потребител или Доверяваща се страна използват и се доверяват на Удостоверения за автентичност на уебсайт 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.

### 1.7 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 Удостоверения за автентичност на уебсайт (домейн) – B-Trust DVC SSL

1. Доставчикът издава Удостоверения за автентичност на уебсайт (домейн) 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 = | [Име на домейна (DNS name), притежаван/собственост на Потребителя] |
| | OU = | [DV SSL] |
| | E = | [Имейл адрес на Потребителя] |
| | L = | [Населено място на Потребителя] |
| | C = | BG или YY<br>където YY е двубуквен код на държавата според ISO 3166, където е регистриран Потребителя |
| Public key | - | RSA(2048 bits) |
| SubjectAlternativeName | - | [DNS име] |
| 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 =<br>Path length Constraint = | End Entity<br>None | |
| Certificate Policy | - | [1] Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.7.1.5<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier ID=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2] Certificate Policy:<br>Policy Identifier=2.23.140.1.2.1<br>[3] Certificate Policy:<br>Policy Identifier=0.4.0.2042.1.6 | |
| Enhanced Key Usage | - | Server Authentication, Client Authentication, Secure Email | |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl | |
| Authority Information Access | - | [1] Authority Info Access<br>Access Method=On-line Certificate Status Protocol<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2] Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>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-QcType (oid=0.4.0.1862.1.6) | id-etsi-qct-web (oid=0.4.0.1862.1.6.3) |
| | | id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf<br>language=en |

## 2.2 Профил на Удостоверения за автентичност на уебсайт (организация) – B-Trust OVC SSL

1. Доставчикът издава Удостоверения за автентичност на уебсайт (организация) 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 = | [Име на домейна (DNS name), притежаван/собственост на Потребителя] | |
| | OU = | [OV SSL] | |
| | E = | [Имейл адрес на Потребителя] | |
| | O = | [Наименование на Потребителя (Организация или компания/фирма)] | |
| | 2.5.4.97= (organizationIdentifier) | [Идентификатор на юридическо лице, с което физическото лице е асоциирано. Един от следните:<br>• VATBG-XXXXXXXXX – за ДДС номер<br>• NTRBG-XXXXXXXXX – за ЕИК (БУЛСТАТ)<br>] | |
| | L = | [Населено място на Потребителя] | |
| | C = | BG или YY<br>където YY е двубуквен код на държавата според ISO 3166, където е регистриран Потребителя | |
| Public key | - | RSA(2048 bits) | |
| SubjectAlternativeName | - | [DNS име] | |
| 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 =<br>Path length Constraint = | End Entity<br>None | |
| Certificate Policy | - | [1] Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier ID=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2] Certificate Policy:<br>Policy Identifier=2.23.140.1.2.2<br>[3] Certificate Policy:<br>Policy Identifier=0.4.0.2042.1.7 | |
| Enhanced Key Usage | - | Server Authentication, Client Authentication, Secure Email | |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl | |
| Authority Information Access | - | [1] Authority Info Access<br>Access Method=On-line Certificate Status Protocol<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2] Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>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-QcType (oid=0.4.0.1862.1.6) | id-etsi-qct-web (oid=0.4.0.1862.1.6.3) |
| | | id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf<br>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).

Съгласно тази политика, Доставчикът ще идентифицира Потребителя, под чието име е регистриран домейна (DNS). Идентифицира се още упълномощеното лице, представляващо Потребителя пред Доставчика и ако е приложимо, администратора на домейна на Потребителя.

Правният инструмент в процедурата по идентификация преди издаване на удостоверение за автентичност на уебсайт и за двете страни - Доставчик и Потребител включва установяване на съответствие съгласно изискванията по ETSI и CA/B Forum.

Доставчикът, чрез МРС ще изпълни всички подходящи и позволени средства за да провери информацията, която ще се удостовери чрез издаването на удостоверение за автентичност на уебсайт (сървър, домейн или организация), включително чрез използване на национални публични регистри – Търговски регистър, регистър БУЛСТАТ, други публични регистри на организации/сдружения с нестопанска/идеална цел, както и съществуването на домейна и неговата принадлежност за Потребителя.

Доставчикът може да заяви пред и изиска от Потребителя допълнителна информация и документи с цел сигурна идентификация/автентификация и установяване на съответствие.

### 4.3 Идентификация и установяване на идентичност при подновяване

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 Удостоверения 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 Удостоверения за автентичност на уебсайт.
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).

Освен проверката за съществуването на Потребителя, РО/МРС проверява съществуването на домейна и неговата принадлежност за Потребителя. Проверката се извършва в някои от следните саитове:

- за домейни .bg – www.nic.bg
- за домейни .eu – www.euric.eu
- за домейни .eus – whois.nic.eus
- за останалите домейни – whois.icann.org

За удостоверения B-Trust DVC SSL и B-Trust OVC SSL не се допуска „wildcard” (*) в корена на DNS името (т.е., за TLD/Top Level Domains).

### 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.8.1 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.8.2 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.8.3 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.8.4 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.8.5 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).