ПОЛИТИКА И ПРАКТИКА

ЗА ПРЕДОСТАВЯНАТА ОТ „БОРИКА“ АД КВАЛИФИЦИРАНА УСЛУГА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ НА ОРГАНА ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ

B-Trust Qualified Time Stamp Authority

Версия 2.1

1 май 2023 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.2	Димитър Николов	13.01.2017	Утвърден	Изменения на документа, свързани с прилагане на Регламент 910/2014.
1.3	Димитър Николов	20.05.2018	Утвърден	Промяна на профил на Timestamp удостоверение. Актуализация на нормативна уредба.
2.0	Димитър Николов	01.03.2020	Утвърден	Технически корекции
2.1	Маргарита Бонева	01.05.2023	Утвърден	Промяна на профил на Timestamp удостоверение

СЪДЪРЖАНИЕ

1 Въведение 6
2 Обхват 6
3 Термини и определения 6
4 Концепция 7
4.1 Qualified Time Stamp Services (Qualified TSS) 7
4.2 B-Trust Qualified Time Stamp Authority (B-Trust QTSA) 7
4.3 Потребители 7
4.4 Политика и Практика 8
4.5 Управление на Практиката и Политиката на Доставчика 8
5 Политика на B-Trust Qualified Time Stamp Authority 8
5.1 Общ преглед 8
5.2 Идентификатор 10
5.3 Приложимост 10
5.4 Съответствие 11
6 Задължения на B-Trust QTSA 11
6.1 Общи задължения: 11
6.2 Задължения към потребители: 11
6.3 Задължения на потребители 11
6.4 Задължения на трета доверена страна 11
6.5 Отговорност на B-Trust QTSA 12
7 Практика и процедури на B-Trust QTSA 12
7.1 Управление на ключове 12
7.1.1 Генериране на двойка ключове 12
7.1.2 Защита на частен ключ 12
7.1.3 Разпространение на публичния ключ 12
7.1.4 Продължаване на срок и/или преиздаване на удостоверение 13
7.2 Удостоверяване на време 13
7.2.1 TST 13
7.2.2 Синхронизация на времето с UTC 14
7.3 Управление и опериране 14
7.3.1 Управление на сигурността 14
7.3.2 Оценка на риска 14

7.3.3 Сигурност на персонала 14
7.3.4 Контрол на достъпа 14
7.3.5 Сигурна среда 14
7.3.6 Прекратяване на TSA 15

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.;
- съдържа условията, съгласно които Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД (Доставчик) предоставя на Потребители квалифицирани електронни времеви печати, чрез организационно обособено звено - Орган за квалифицирани електронни времеви печати;
- има характер на общи условия по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД);
- включва подробно описание на политиката и практиката при предоставяне на квалифицирани електронни времеви печати от Доставчика и е публичен документ с цел установяване на съответствие на дейността на Доставчика с нормативната уредба;
- може да бъде променян от ДКУУ и всяка нова редакция на "Политика и практика за предоставяната от „БОРИКА“ АД квалифицирана услуга за издаване на квалифицирани електронни времеви печати" се публикува на интернет-страницата на Доставчика.

Настоящият документ е изготвен в съответствие с:

- Регламент 910/2014 на Европейския парламент и Съвет относно Удостоверителните услуги и се позовава на информация, съдържаща се в изготвените в съответствие с този Регламент и утвърдени международни препоръки, спецификации и стандарти;
- Закона за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ);
- Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги (НОПДДУУ);

Съдържанието и структурата на документа се позовава на информация, съдържаща се в следните утвърдени международни препоръки, спецификации и стандарти:

- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- EN 319 422: Time-stamping protocol and time-stamp token profiles.

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

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

1 Въведение

Доставчик на Квалифицирани Удостоверителни Услуги „БОРИКА” АД, наричан по-нататък за кратко „ДКУУ”, по силата на чл.19 на ЗЕДЕУУ издава Квалифицирани Електронни Времеви Печати (КЕВП).

Квалифицираният Електронен Времеви Печат предоставя калибрирано официално време, което удостоверява по сигурен и проследим начин съществуването на цифрови данни, включително съдържание на електронен документ преди определен момент. Приложено към КЕП, КЕВП утвърждава, че електронния подпис е създаден преди момента, указан в КЕВП.

Документът определя общите условия и правила, които ДКУУ следва при издаване на КЕВП при оперирането и поддръжката на тази услуга.

Органът, чрез който ДКУУ издава и поддържа КЕВП строго съблюдава Политиката и практиката съдържащи се в този документ. Тези Политика и Практика основно адресират посочения по-горе сценарий на приложимост на КЕВП към КЕП, но те са приложими и при други сценарии.

С оглед на това, че предоставяните от B-Trust Qualified Time Stamp Authority КЕВП са приложими при различни сценарии, ДКУУ „БОРИКА” АД публикува обща Политика и Практика, които съставляват този документ.

ДКУУ „БОРИКА” АД оперира B-Trust Qualified Time Stamp Authority и публично предоставя КЕВП на Интернет-адрес „http://tsa.b-trust.org”.

2 Обхват

Този документ определя изискванията към Политиката на ДКУУ относно издаваните КЕВП и дефинира Практиката при опериране и управление на B-Trust Qualified Time Stamp Authority, за да позволи на потребители и доверяващи се страни, които имат сключен Договор за използване на квалифицираните удостоверителни услуги на B-Trust или подписано Споразумение за ниво на обслужване към такъв договор, да получат описание и оценка на сигурността на предоставяната квалифицирана услуга за издаване на КЕВП.

B-Trust Qualified TSS ползва общата инфраструктура на B-Trust на „БОРИКА” АД като квалифициран доставчик на квалифицирани удостоверителни услуги съгласно ЗЕДЕУУ и Регламент 910/2014.

Изискванията и условията, съдържащи се в документа, са адресирани преди всичко към B-Trust Qualified TSS при употребата и поддръжката на КЕП. Те се базират на използването на PKI-криптография, удостоверения на публични ключове и източник на точно (официално) време, но биха могат да се използват и за други приложения.

Потребителите и доверяващите се страни трябва да ползват този документ, за да получат точно описание и оценка на сигурността на предоставените КЕВП.

3 Термини и определения

B-Trust QTSA (B-Trust Qualified Time Stamp Authority) – Удостоверяващ Орган в инфраструктурата на B-Trust, който предоставя КЕВП.

TST (Time Stamp Token) – електронно подписан КЕВП от B-Trust QTSA за съществуване на цифрово съдържание на електронен документ преди определен момент, посочен в удостоверението и за непроменимост на това съдържание след този момент. Приложено към електронен подпис, удостоверението създава неотменимост на подписа във времето.

Qualified *TSS (*Qualified *Time Stamp Services)* – квалифицирани удостоверителни услуги за генериране на сигурни КЕВП, поддържане на архив на издадени и доставени КЕВП, проверка и утвърждаване на валидност на КЕВП.

TSA-система – съвкупност от организирани ИТ продукти и компоненти, чрез които B-Trust QTSA предоставя КЕВП.

Coordinated Universal Time (UTC) – времеви мащаб, базиран на секунди, съгласно ITU-R Recommendation TF.460-5.

UTC(k) – времеви мащаб според лаборатория “k”, който се доближава до UTC, с цел постигане на точност плюс/минус 100ns (ITU-R Recommendation TF.536-1 [TF.536-1]).

Service Level Agreement (SLA) – Договорирано споразумение за ниво на обслужване при предоставяне на Qualified TSS.

GPS – *Global Positioning System* - Глобална система за спътниково определяне на местоположението

NTP – *Network Time Protocol* е протокол за синхронизиране на часовниците в компютърните системи

NTP Stratum – Ниво в NTP йерархичната подредба на източници на време, определящо отместването на сървъра спрямо референтен източника на време (Stratum 0).

Другите специфични термини, които се използват в документа следват определенията, дадени в документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS), който е публикуван и достъпен на Уеб сайта на ДКУУ „БОРИКА” АД (https://www.b-trust.bg/documents).

4 Концепция

4.1 Qualified Time Stamp Services (Qualified TSS)

Инфраструктурата в B-Trust, която предоставя, обслужва и поддържа Qualified TSS, включва:

- B-Trust Qualified Time Stamp Authority - оперира Qualified TSS, генерира КЕВП, поддържа журнал и архив на издадените КЕВП и управлява услугата;
- системна логистика - приемане на онлайн заявки и доставка на КЕВП, проверка и утвърждаване на издадени КЕВП.

Системната логистика включва достъп до източник на точно време (UTC(k)).

Това деление е условно за целите на документа и не налага ограничение в ползването на КЕВП.

4.2 B-Trust Qualified Time Stamp Authority (B-Trust QTSA)

„B-Trust Qualified Time Stamp Authority“ е удостоверяващия орган в инфраструктурата на B-Trust съгласно т. 4.1, който предоставя КЕВП в съответствие с Политиката и Практиката на ДКУУ, описани в този документ и изгражда доверието на потребителите на КЕВП.

4.3 Потребители

Потребители на КЕВП са лица или доверяващи се страни на B-Trust, съгласно „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ (B-Trust CPS-eIDAS), както и всяко друго физическо или юридическо лице, сключило отделен договор с „БОРИКА” АД за Qualified TSS и съответно споразумение за ниво на обслужване (SLA).

4.4 Политика и Практика

Този документ дефинира общите елементи на политиката и на практиката на ДКУУ да предоставя КЕВП в качеството му на общи условия.

Политиката определя условията и правилата, към които се придържа ДКУУ. Практиката описва как ДКУУ прилага описаната политика и процедурите, които той следва при предоставяне на КЕВП.

B-Trust QTSA издава КЕВП на всяка заинтересована страна, като съблюдава стандартно (негарантирано) ниво на обслужване. Правило в Политиката на B-Trust QTSA е да издава КЕВП, следвайки практиката и процедурите включени в настоящия документ.

Потребител, който се нуждае от гарантирано ниво на обслужване на КЕВП, сключва Договор за ползване на B-Trust Qualified TSS и SLA.

За услуга „Издаване на квалифицирани електронни времеви печати" при съгласувано ниво на обслужване (SLA, Service Level Agreement) се заплаща съгласно договорните условия за доставка и ползване на услугата.

Практиката на Доставчика при предоставяне на КЕВП се осъществява от удостоверяващия орган „B-Trust Qualified Time Stamp Authority“ и се означава с:

Удостоверяващ орган	Идентификатор (OID)
B-Trust Qualified Time Stamp Authority	O.I.D. = 1.3.6.1.4.1.15862.1.6.3

Политиката на Доставчика относно предоставяне на КЕВП се означава със следните идентификатори:

Квалифицираното Удостоверение	Наименование	Вписани Политики (OID)
Удостоверение на КЕВП	B-Trust Qualified Time Stamp Policy	O.I.D. = 1.3.6.1.4.1.15862.1.6.3 O.I.D. = 0.4.0.2023.1.1

4.5 Управление на Практиката и Политиката на Доставчика

1. Практиката и Политиката на Доставчика подлежат на административно управление и контрол от страна на Съвета на директорите на „БОРИКА“ АД.
2. Допускат се промени, редакции и допълнения, които не засягат правата и задължения, произтичащи от този документ и стандартния договор между Доставчика и Потребителите след съгласуване и утвърждаване от Съвета на директорите.
3. Всяка представена и одобрена нова версия или редакция на този документ незабавно се публикува на сайта на Доставчика.
4. Коментари, запитвания и разяснения по този документ могат да се отправят на:
   - електронен адрес на Удостоверяващ орган: info@b-trust.org;
   - електронен адрес на Доставчика: info@borica.bg;
   - тел.: (02) 9215 115 и факс: (02) 981 45 18

5 Политика на B-Trust Qualified Time Stamp Authority

5.1 Общ преглед

Политиката на B-Trust QTSA е наборът от правила, които означават приложимостта на КЕВП за конкретно приложение или клас от приложения с общи изисквания към нивото на сигурност.

B-Trust издава КЕВП в съответствие с “ ETSI EN 319 421 Policy and Security Requirements for

Trust Service Providers issuing Time-Stamps” и настоящата Политика.

Предоставяното точно калибрирано време спрямо UTC (Coordinated Universal Time) е с точност до 0.5 секунди. При добавяне или изваждане на секунда към точното време (leap second), B-Trust QTSA не издава КЕВП в рамките на тази секунда.

Системната логистика на B-Trust QTSA използва GPS източник на точно време с цел гарантиране на максимална точност.

Служебното удостоверение на B-Trust QTSA на Доставчика е удостоверение за публичния ключ, електронно подпечатано с базовия частен ключ на Доставчика. С частния ключ на B-Trust QTSA електронно се подпечатват КЕВП на представяне на съдържание на електронен документ от Потребител и/или Доверяваща се страна.

Това удостоверение на B-Trust QTSA, удостоверяващо принадлежността на публичния RSA ключ (2048 бита), с който се верифицира КЕПечата в издадения КЕВП, е с профил, съгласно документа „ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles“.

Електронните печати на Доставчика, които са придружени от служебното удостоверение на -Trust Qualified Time Stamp Authority са квалифицирани.

Профилът на удостоверението на B-Trust Qualified Time Stamp Authority е посочен по-долу.

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	4431e2c388ab5130
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2023-03-14 T12:14:21Z
Validity to	-	2028-03-13 T12:14:21Z
Subject	CN =	B-Trust Qualified Time Stamp Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 Bits)
Subject Key Identifier		c3 bb 28 36 0a 9f d9 b6 57 65 ca dc 8f bb 00 6c 6a d9 52 52
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Issuer Alternative Name	URL=	http://www.b-trust.org
Subject Alternative Name	URL=	http://tsa.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-

		TrustOperationalQCA.crl	
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)	
Enhanced Key Usage (critical)	-	Time Stamping (1.3.6.1.5.5.7.3.8)	
Thumbprint (Sha1)		2D:1E:10:B1:E7:1E:BC:05:80:50:F3:22:8F:80:10:36:8C:30:DB:F1	
Thumbprint (Sha256)		4A:D9:BA:68:27:5C:5B:73:0B:D8:78:6A:38:3A:54:9D:DA:74:7F:09:BD:D0:F1:B7:08:A9:BA:8D:C4:2C:38:4D	
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-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf language=en

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

Алгоритъм	Наименование
Хеш-алгоритми:	SHA256
Асиметрични алгоритми:	RSA

5.2 Идентификатор

B-Trust QTSA издава КЕВП за два типа данново съдържание:

- на КЕП;
- на произволен електронен документ/изявление.

Изискванията към горепосочените КЕВП са идентични и съответстват на тези с произволна употреба на КЕВП, съгласно „ETSI EN 319 421“ с политика „OID = 0.4.0.2023.1.1“.

В общия случай, B-Trust QTSA издава КЕВП, което съдържа идентификатор на Политика:

Политика на Доставчика	Идентификатор (OID)
B-Trust TST (КЕВП)	O.I.D. = 0.4.0.2023.1.1

При договорено SLA, B-Trust TSA издава КЕВП, който съдържа идентификатор описан в конкретното споразумение.

5.3 Приложимост

Политиката, съгласно този документ не ограничава приложимостта на доставяните КЕВП от B-

Trust Qualified Time Stamp Authority.

КЕВП могат да се използват при създаване на разширен формат на КЕП (XAdES, CAdES, PAdES), при създаване на архиви, регистри, електронни форми и др. по преценка на потребителите.

5.4 Съответствие

B-Trust QTSA може да използва при необходимост посочения в т. 5.2 идентификатор на Политика.

Издаваните КЕВП са електронно подписани от B-Trust QTSA като удостоверяващ орган, който се идентифицира със своето удостоверение.

Удостоверението на B-Trust QTSA се използва от потребители/доверяваща се страна за проверка и валидност на КЕП в доставяните КЕВП.

6 Задължения на B-Trust QTSA

6.1 Общи задължения:

- Да изпълнява всички посочени изисквания в т.7 на документа по прилагане на Политиката;
- Да гарантира съответствие с посочените тук изисквания в Политиката, дори когато функционалност на B-Trust Qualified QTSA или част от нея се предоставя по договор;
- Да гарантира съответствие на предоставяните КЕВП с документираните процедурите в Практиката.

6.2 Задължения към потребители:

- Да спазва общите задължения;
- Да гарантира постоянен достъп до КЕВП, без планираните технически прекъсвания и профилактики;
- Да имплементира и оперира надлежна и сигурна комуникационна инфраструктура;
- Да предоставя точно калибрирано време (UTC);
- Да указва в КЕВП удостовереното време с точност до 500 милисекунди;
- Да поддържа КЕВП в съответствие с общоприетите международни препоръки и спецификации;
- Да поддържа едновременно множество сесии на заявки на издаване на КЕВП;
- Възможност за мащабиране на производителността (КЕВП /сек.);
- Да използва техническо оборудване, отговарящо на общите изисквания за надеждност и сигурност на техническите средства на ДКУУ, съгласно нормативната база на ЗЕДЕУУ;
- Да не се нарушават лицензии, интелектуална собственост или други права в издаваните КЕВП;
- да не допуска модифициране на цифровите данни след издаване на КЕВП, без това да бъде установено.

6.3 Задължения на потребители

Потребители, които получават КЕВП следва да верифицират електронния подпис на B-Trust QTSA и да проверяват за валидност удостоверението на този орган.

B-Trust QTSA не изисква електронна автентификация и не налага други ограничения на потребителите на КЕВП.

6.4 Задължения на трета доверена страна

Общо задължение на всяка трета доверена страна е да верифицира квалифицирания

електронен печат в КЕВП. Тя следва да провери валидността на удостоверението на B-Trust QTSA. В случай, че периода на валидност на това удостоверение не е изтекъл, третата доверена страна следва:

- да провери дали това удостоверение не е в CRL-списъка;
- да провери степента/нивото на сигурност на използваната хеш функция за КЕВП;
- да провери степента/нивото на сигурност на използваните алгоритми, както и дължината на двойката ключове за КЕП в КЕВП.

6.5 Отговорност на B-Trust QTSA

B-Trust QTSA оперира TSS в пълно съответствие с Практиката на ДКУУ съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ и настоящия документ. B-Trust QTSA няма да публикува/представя допълнителна информация относно предоставяните КЕВП, освен ако потребител/трета доверена страна имат сключен Договор за ползване на КЕВП и SLA с ДКУУ.

B-Trust QTSA не отговаря за възникнали проблеми при предоставяне на КЕВП, които са породени от събития и причини извън компетенцията и обхвата на дейността на ДКУУ.

„БОРИКА” АД, като ДКУУ по ЗЕДЕП, е отговорен по този закон и неговата нормативна уредба. КЕВП е вид квалифицирана удостоверителна услуга с профил „неотменимост” и изисква ефикасен контрол върху всички елементи и събития в работата на B-Trust QTSA – процедури, КЕВП-транзакции, ключов материал, персонал, др.

7 Практика и процедури на B-Trust QTSA

Посочените тук процедури, механизми по контрол и технически характеристики на B-Trust QTSA са допълнение към тези, специфицирани в документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ (B-Trust CPS-eIDAS), по-конкретно в частите, регламентиращи дейността на „БОРИКА” АД като ДКУУ по предоставяне на квалифицирани удостоверителни услуги.

Настоящите условия и процедури са в основата на оперативната работа на B-Trust QTSA.

7.1 Управление на ключове

7.1.1 Генериране на двойка ключове

Двойката RSA ключове се генерира в крипто модул с удостоверено ниво на сигурност FIPS 140-2 Level 3 от персонал на ДКУУ, който има право да изпълнява тази роля. Генерираната двойка RSA ключове е с дължина 2048 бита.

Описанието и ролята на персонала на ДКУУ са посочени в документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“. Средата за генериране на двойка ключове на Удостоверяващ орган на ДКУУ е описана в същия документ.

7.1.2 Защита на частен ключ

Генерираният частен ключ на B-Trust QTSA се съхранява в крипто модул (HSM) с удостоверено ново на сигурност FIPS 140-2 Level 3.

В специален сейф, се съхраняват съответните копия на смарт карти с части от частния ключ на B-Trust QTSA.

7.1.3 Разпространение на публичния ключ

Публичният ключ на B-Trust QTSA е удостоверен в удостоверение за КЕП (квалифициран електронен печат), издадено от Базовия Удостоверяващ Орган (B-Trust Root Qualified CA) в

PKI-йерархията за издаване на квалифицирани удостоверения за квалифициран електронен подпис.

Това удостоверение с публичен ключ на B-Trust QTSA е заредено в Qualified TSS системата. Допълнително, удостоверението на B-Trust QTSA е публикувано в интернет страница на сайта на ДКУУ и може свободно да се достави в компютрите на потребители, които ползват КЕВП на B-Trust.

7.1.4 Продължаване на срок и/или преиздаване на удостоверение

Периодът на валидност на удостоверението на B-Trust QTSA е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 1 година. След този период се генерира нова двойка ключове, частният ключ от която се съхранява в крипто модула (HSM), а публичният ключ се удостоверява, чрез издаване на ново удостоверение на B-Trust QTSA. Двойката ключове с изтекъл период на валидност се съхранява, както следва:

- частен ключ – съхранява се за период от 10 години;
- публичен ключ – съхранява се за период от 10 години.

7.2 Удостоверяване на време

Сървърният софтуер на B-Trust Qualified Time Stamp Authority имплементира техническата спецификация на „ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles“. Комуникационният софтуер на B-Trust Qualified Time Stamp Authority системата поддържа комуникация с клиентите на Qualified TSS по протоколи: TCP/IP, HTTP/HTTPS.

7.2.1 TST

Профилът на заявките/отговорите на B-Trust QTSA системата е в съответствие с горепосочените технически спецификации и включва следните атрибути/параметри:

1. Заявката за издаване на КЕВП (TSQ) включва:

Име на атрибут	Стойност	Описание
Version	1	Версия
Message Imprint	Hash Algorithm: […]	използван хеш-алгоритъм (Sha256)
	Hash Value: […]	хеш-сума на електронен подпис на подписан електронен документ или други цифровите данни
Requested Policy	[опция]	идентификатор на политика, която да бъде удостоверена в КЕВП
Nonce	[опция]	допълнителни данни, които ще се съдържат в КЕВП
Certificate Request	[опция]	опция дали КЕВП да съдържа удостоверение на B-Trust QTSA
Extensions	[опция]	допълнителни разширения

2. КЕВП отговора (TSR) включва:

Име на атрибут	Стойност	Описание
Version	1	Версия
Policy	[Policy OID]	идентификатора на политиката за издаване на удостоверения за време
Message Imprint	Hash Algorithm: […]	използван хеш-алгоритъм (Sha256)
	Hash Value: […]	хеш-сума на представения на доставчика електронен подпис на подписан електронен документ или други цифрови данни
Serial Number	[…]	уникалния идентификационен номер
Generated Time	[…]	времето на представяне на електронния подпис (удостоверено време по UTC)
Accuracy	500	точност в милисекунди = 0.5 секунди
Ordering	True	
Nonce	[опция]	допълнителни данни, които се изискват в TSQ;
Tsa	CN = B-Trust Qualified Time Stamp Authority OU = B-Trust	

	O = BORICA AD OrganizationIdentifier(2.5.4.97) = NTRBG-201230426 C = BG	
Extensions	[опция]	допълнителни разширения
Digital Siganture	[…]	идентификаторите на алгоритмите, използвани за създаването на електронния подпис (Sha256RSA)
	Siganture Value: […]	електронен подпис на КЕВП
	[Удостоверението на B-Trust TSA]	удостоверението за квалифицирания електронен печат на доставчика на удостоверителни услуги

7.2.2 Синхронизация на времето с UTC

B-Trust QTSA използва хардуерен източник на точно калибрирано време с висока точност. Синхронизацията на UTC с източника на време е автоматична, на база NTP-протокол, след установяване на разлика между източника и времето в системата.

В случай на възникнал проблем в хардуерния източник на време и до подмяна на същия с резервен такъв, като източник на точно време се използват базирани в Интернет сървъри на време. Синхронизацията е на базата на поне два източника на време в Интернет чрез протокол NTP.

Точността на удостовереното време е с отклонение до 0.5 секунди спрямо UTC времето. B-Trust QTSA не издава удостоверения за време при по-големи отклонения, липса на синхронизация с UTC или при добавяне или изваждане на секунда към точното време (leap second).

7.3 Управление и опериране

7.3.1 Управление на сигурността

Всички аспекти на управлението на сигурността на B-Trust QTSA са в съответствие с документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ на ДКУУ „БОРИКА” АД.

При нарушаване на сигурността на услугата B-Trust QTSA или загуба на автентичност на данните, при първа възможност се уведомяват всички регистрирани потребители на услугата.

7.3.2 Оценка на риска

Всички аспекти на оценка на риска са в съответствие с документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ на ДКУУ „БОРИКА” АД.

7.3.3 Сигурност на персонала

Характеристиката на персонала на ДКУУ и назначените длъжности са в съответствие с документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ на ДКУУ „БОРИКА” АД.

7.3.4 Контрол на достъпа

Физическият контрол на достъпа до средата на ДКУУ и на B-Trust QTSA е в съответствие с документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“.

7.3.5 Сигурна среда

Крипто модулът (HSM) с удостоверено ниво на сигурност FIPS 140-2 Level 3 е оперативната среда за съхраняване на частния ключ и за електронно подписване на КЕВП, които се доставят на потребителите.

7.3.6 Прекратяване на TSA

В случай на прекратяване на B-Trust QTSA се изпълняват съответните процедури, съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги от „БОРИКА“ АД“ на ДКУУ „БОРИКА” АД.