ПОЛИТИКА И ПРАКТИКА

НА

ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

B-Trust Time Stamp Authority

Версия 1.1

1 Септември 2015 г.

1 Въведение

Доставчик на Удостоверителни Услуги „БОРИКА – БАНКСЕРВИЗ" АД, наричан по-нататък за кратко „ДУУ", по силата на чл.19 на ЗЕДЕП издава и поддържа удостоверения за Квалифициран електронен подпис (КЕП) и Удостоверения за време (УВ).

Удостоверението за време предоставя калибровано официално време, което удостоверява по сигурен и проследим начин съществуването на цифрови данни, включително съдържание на електронен документ преди определен момент. Приложено към КЕП в съответствие с чл. 40 на ЗЕДЕП, УВ утвърждава, че електронния подпис е създаден преди момента, указан в УВ.

Документът определя общите условия и правила, които ДУУ следва при издаване на удостоверенията за време в съответствие с чл.40 на ЗЕДЕП и при оперирането и поддръжката на тази услуга.

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

С оглед на това, че предоставяните от B-Trust TSA удостоверения за време са приложими при различни сценарии, ДУУ „БОРИКА – БАНКСЕРВИЗ" АД публикува обща Политика и Практика, които съставляват този документ.

ДУУ „БОРИКА – БАНКСЕРВИЗ" АД оперира B-Trust TSA и публично предоставя TSS-услуги на Интернет-адрес „http://tss.b-trust.org".

2 Обхват

Този документ определя изискванията към Политиката на ДУУ относно издаваните TST и дефинира Практиката при опериране и управление на B-Trust TSA, за да позволи на потребители и доверяващи се страни, които имат сключен Договор за използване на удостоверителните услуги на B-Trust или подписано Споразумение за ниво на обслужване към такъв договор, да получат описание и оценка на сигурността на предоставените B-Trust TSS.

B-Trust TSS ползва общата инфраструктура на B-Trust на „БОРИКА – БАНКСЕРВИЗ" АД като регулиран доставчик на удостоверителни услуги съгласно ЗЕДЕП.

Структурата и съдържанието на документа следват и са в съответствие с документа ETSI TS 102 023 v.1.2.1 (2003-01) Policy Requirements for time-stamping authorities.

Изискванията и условията, съдържащи се в документа, са адресирани преди всичко към B-Trust 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 TSS услуги.

3 Термини и определения

B-Trust TSA (Time Stamp Authority) – Удостоверяващ Орган в инфраструктурата на B-Trust, който предоставя TSS-услуги.

TST (Time Stamp Token) – електронно подписано удостоверение от B-Trust TSA 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.

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

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

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 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 B-Trust "Наръчник на Потребителя", който е публикуван и достъпен на Уеб сайта на ДУУ „БОРИКА – БАНКСЕРВИЗ" АД (http://www.b-trust.org).

4 Концепция

4.1 Time Stamp Service (TSS)

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

- B-Trust TSA - оперира TSS, генерира TST, поддържа журнал и архив на издадените TST и управлява услугата;
- системна логистика - приемане на онлайн заявки и доставка на TST, проверка и утвърждаване на издадени TST.

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 TSS.

4.2 B-Trust TSA

„B-Trust TSA" е удостоверяващия орган в инфраструктурата на B-Trust съгласно т. 4.1, който предоставя TSS в съответствие с Политиката и Практиката на ДУУ, описани в този документ и изгражда доверието на потребителите на TST.

4.3 Потребители

Потребители на TSS са абонати или доверяващи се страни на B-Trust удостоверителните услуги, съгласно B-Trust „Наръчник на Потребителя", както и всяко друго физическо или юридическо лице, сключило отделен договор с „БОРИКА – БАНКСЕРВИЗ" АД за 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 ДУУ да предоставя TSS в качеството му на общи условия.

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

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

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

5 Политика на B-Trust TSA

5.1 Общ преглед

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

B-Trust издава TST в съответствие с "ETSI TS 102 023 Policy Requirements for time-stamping authorities" и настоящата Политика. Съдържанието на "ETSI TS 102 023" е технически еквивалентно на "IETF RFC 3628: Requirements for Time-Stamping Authorities".

Предоставяното точно калибровано време спрямо UTC (Coordinated Universal Time) е с точност до 0.5 секунди.

Системната логистика на B-Trust TSA използва GPS източник на точно време, както и алтернативни източници на време с цел гарантиране на максимална точност.

Удостоверението на B-Trust TSA, удостоверяващо принадлежността на публичния RSA ключ (2048 бита), с който се верифицира КЕП в издадения TST, е с профил, съгласно документа „IETF RFC 3161, Internet x.509 PKI Time Stamp Protocol (TSP)“.

Профилът на удостоверението на B-Trust TSA е посочен по-долу.

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	0b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 април 2015 09:34:16 UTC
Validity to	-	15 април 2020 09:34:16 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5tss@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117.
	CN =	B-Trust Time Stamp Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2d 79 0e 96 e8 dc 9d c2 40 fd 08 71 da ae 06 67 4e 49 e6 2e
Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d
		Certificate Issuer: Directory Address: CN=B-Trust Root CA OU=B-Trust O=BORICA - BANKSERVICE AD L=Sofia C=BG Certificate SerialNumber=01
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://tss.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
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)		17 8e 35 12 63 06 b2 eb 74 a9 e5 c7 72 e6 9d 7a ee a8 0a 8c

Thumbprint (Sha256)		4f a4 8f 10 1b a9 69 db 32 b3 1f d9 00 3b 74 4a fa 97 91 c2 20 5a 37 10 a4 94 5b 94 a7 7b e7 0d

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

Алгоритъм	Наименование
Хеш-алгоритми:	SHA1,SHA256
Асиметрични алгоритми:	RSA

5.2 Идентификатор

B-Trust TSA издава TST за два типа съдържание:

- Квалифициран TST за КЕП;
- Квалифициран TST за цифрово съдържание на произволен електронен документ/изявление.

Изискванията към горепосочените TST са идентични и съответстват на тези с произволна употреба на TST, съгласно „ETSI TS 102 023“ с политика „OID = 0.4.0.2023.1.1“.

В общия случай, B-Trust TSA издава TST, който съдържа идентификатор на Политика:

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

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

5.3 Приложимост

Политиката, съгласно този документ не ограничава приложимостта на доставяните TST от B-Trust TSA.

TST 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 TSA може да използва при необходимост посочения в т. 5.2 идентификатор на Политика.

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

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

6 Задължения на B-Trust TSA

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 TSA или част от нея се предоставя по договор;
- Да гарантира съответствие на предоставяните TSS с документираните процедурите в Практиката.

6.2 Задължения към потребители:

- Да спазва общите задължения;
- Да гарантира постоянен достъп до TSS, без планираните технически прекъсвания и профилактики;
- Да имплементира и оперира надлежна и сигурна комуникационна инфраструктура;
- Да предоставя точно калибровано време (UTC);
- Да указва в TST удостовереното време с точност до 500 милисекунди;

- Да поддържа TSS в съответствие с общоприетите международни препоръки и спецификации;
- Да поддържа едновременно множество сесии на заявки на издаване на TST;
- Възможност за мащабиране на производителността (TST/сек.);
- Да използва техническо оборудване, отговарящо на общите изисквания за надеждност и сигурност на техническите средства на ДУУ, съгласно нормативната база на ЗЕДЕП;
- Да не се нарушават лицензии, интелектуална собственост или други права в издаваните TST;
- да не допуска модифициране на цифровите данни след издаване на TST, без това да бъде установено.

6.3 Задължения на потребители

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

B-Trust TSA не изисква електронна автентификация и не налага други ограничения на потребителите на TSS.

6.4 Задължения на трета доверена страна

Общо задължение на всяка трета доверена страна е да верифицира КЕП в TST. Тя следва да провери валидността на удостоверението на B-Trust TSA. В случай, че периода на валидност на това удостоверение не е изтекъл, третата доверена страна следва:

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

6.5 Отговорност на B-Trust TSA

B-Trust TSA оперира TSS в пълно съответствие с Политиката и Практиката на ДУУ съгласно документа „B-Trust - Наръчник на потребителя" и настоящите Политика и Практика. B-Trust TSA няма да публикува/представя допълнителна информация относно предоставяните TSS, освен ако потребител/трета доверена страна имат сключен Договор за ползване на B-Trust TSS и SLA с ДУУ.

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

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

7 Практика и процедури на B-Trust TSA

Посочените тук процедури, механизми по контрол и технически характеристики на B-Trust TSA са допълнение към тези, специфицирани в документа "B-Trust Наръчник на Потребителя" , по-конкретно в частите, регламентиращи дейността на „БОРИКА – БАНКСЕРВИЗ" АД като ДУУ по предоставяне на удостоверителни услуги.

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

7.1 Управление на ключове

7.1.1 Генериране на двойка ключове

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

Описанието и ролята на персонала на ДУУ са посочени в документа "B-Trust Наръчник на Потребителя". Средата за генериране на двойка ключове на Удостоверяващ орган на ДУУ е описана в същия документ.

7.1.2 Защита на частен ключ

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

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

7.1.3 Разпространение на публичния ключ

Публичният ключ на B-Trust TSA е удостоверен в удостоверение за КЕП, издадено от Базовия Удостоверяващ Орган (B-Trust Root CA) в PKI-йерархията за издаване на удостоверения за квалифициран електронен подпис.

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

7.1.4 Продължаване на срок и/или преиздаване на удостоверение

Периодът на валидност на удостоверението на B-Trust TSA е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 3 години. След този период се генерира нова двойка ключове, частният ключ от която се съхранява в криптомодула (HSM), а публичният ключ се удостоверява, чрез издаване на ново удостоверение на B-Trust TSA. 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 TSA имплементира техническата спецификация на „ETSI TS 101 861 v.1.3.1 (2006-01) Time Stamp Profile“. Тази спецификация е еквивалентна на международната препоръка на IETF RFC 3161 (Time Stamp Protocol).

Комуникационният софтуерен на TSA системата поддържа комуникация с клиентите на TSS по протоколи: TCP/IP, HTTP/HTTPS.

7.2.1 TST

Профилът на заявките/отговорите на TSA системата е в съответствие с горепосочените технически спецификации и включва следните атрибути/параметри:

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

Име на атрибут	Стойност	Описание
Version	1	версия
Message Imprint	Hash Algorithm: […]	използван хеш-алгоритъм (Sha1/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 TST
Nonce	[опция]	допълнителни данни, които ще се съдържат в TST
Certificate Request	[опция]	опция дали TST да съдържа удостоверение на B-Trust TSA
Extensions	[опция]	допълнителни разширения

2. TST отговора на заявката (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 (Sha1/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	Phone = +359 2 9 215 100 E = ca5tss@b-trust.org PostalCode = 1784 STREET = bul. Tsarigradsko shose No 117 CN = B-Trust Time Stamp Authority OU = B-Trust O = BORICA - BANKSERVICE AD, EIK 201230426 L = Sofia C = BG	
Extensions	[опция]	допълнителни разширения
Digital Siganture	[…]	идентификаторите на алгоритмите, използвани за създаването на електронния подпис (Sha1RSA/Sha256RSA)
	Siganture Value: […]	електронен подпис на TST
	[Удостоверението на B-Trust TSA]	удостоверението за квалифицирания електронен подпис на доставчика на удостоверителни услуги

7.2.2 Синхронизация на времето с UTC

B-Trust TSA използва хардуерен източник на точно калибровано 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.

7.3 Управление и опериране

7.3.1 Управление на сигурността

Всички аспекти на управлението на сигурността на B-Trust TSA са в съответствие с документа „B-Trust - Наръчник на потребителя” на ДУУ „БОРИКА – БАНКСЕРВИЗ” АД.

7.3.2 Оценка на риска

Всички аспекти на оценка на риска са в съответствие с документа „B-Trust - Наръчник на потребителя” на ДУУ „БОРИКА – БАНКСЕРВИЗ” АД.

7.3.3 Сигурност на персонала

Характеристиката на персонала на ДУУ и назначените длъжности са в съответствие с документа „B-Trust - Наръчник на потребителя“ на ДУУ „БОРИКА – БАНКСЕРВИЗ” АД .

7.3.4 Контрол на достъпа

Физическият контрол на достъпа до средата на ДУУ и на B-Trust TSA е в съответствие с документа „B-Trust - Наръчник на потребителя” „БОРИКА – БАНКСЕРВИЗ” АД .

7.3.5 Сигурна среда

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

7.3.6 Прекратяване на TSA

В случай на прекратяване на B-Trust TSA се изпълняват съответните процедури, съгласно „B-Trust - Наръчник на

потребителя” на ДУУ „БОРИКА – БАНКСЕРВИЗ” АД .