	Длъжност	**Име, фамилия**	**Дата**	**Подпис**
Утвърдил	Изпълнителен директор	Димитър Бранков	*11.05.2021*	
Съгласувал	Представител на ръководството по СУСИ	Емил Даутов	*11.05.2021*	
Разработил	Администратор по сигурността	Емил Даутов	*11.05.2021*	

Дата на регистрация на документа:	*01.07.2017*
Дата на последна корекция на документа:	11.05.2021
Оригиналът се съхранява:	*при Представител на ръководството по СУСИ*

Вид на екземпляра и пореден №

Оригинал		**Контролирано копие**	X	**Информационен**	

Разпространение на документа:	**Абонат:**
Вътрешно:	
Външно:	

Този документ е част от Система за управление на сигурността на информацията на "СИСТЕМА ЗА ЕЛЕКТРОННИ ПЛАЩАНИЯ БЪЛГАРИЯ/СЕП БЪЛГАРИЯ" АД
Всички потребители на този документ трябва да изпълняват изискванията на СУСИ за работа с чувствителна информация.

This document is part of the Information Security Management System of "SYSTEM FOR ELECTRONIC PAYMENTS BULGARIA/SEP BULGARIA" JSC
Everyone who uses this document shall carry out the ISMS requirements for work with sensitive information.

CONTENTS

1. ВЪВЕДЕНИЕ

Политика и практика за предоставяне квалифицирани услуги за Time-Stamp Certification (“***Time-Stamp Certification Policy”***) е документ, съдържащ общи правила и регламенти, прилагани за квалифицирани удостоверителни услуги от „Система за Електронни Плащания/СЕП България. Този документ определя политиката и сигурността изискванията, свързани с функционирането и управлението на практиките, използвани от Time-Stamp Certification Authority ("eSign Sep TSA") за издаване на квалифициран електронен време печати.

В „Политика на органа за удостоверяване на време“ са определени участниците в процеса на издаване и поддържане на потребителски квалификация електронни време печати, както и техните отговорности, права и задължения. Приложимия диапазон на ефекта на електронното време печати също е посочено. Подробно описание на тези правила е предоставена в документа, CPS на СЕП България.

Структурата и съдържанието на настоящата политика, се подготвят в съответствие с техническата спецификация ETSI TS 102 023. СЕП България изпълнява " Политика на органа за удостоверяване на време " при предоставяне на електронни време печати и публично осигурява квалифицирани удостоверителни услуги за предоставянето на квалифицирани електронни време печати.

Тя е достъпна на:

http://www.eSign.bg.

Квалифициран електронен времето печат се използва по подразбиране за точност на датата и часа, определени от нея за целостта на данните, с които са свързани на дата и час. Квалифициран време-печат, издаден от СЕП България е признат във всички държави-членки на Европейския съюз и отговаря на следните изисквания:

1. той се свързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязано данни промяна;
2. се основава на източник на точно време, свързани с координираното универсално време;
3. е подписан с разработени или квалифициран електронен подпис или е подпечатан с разработени или квалифициран електронен печат на СЕП България в качеството си като квалифицирано доставчик на квалифицирани удостоверителни услуги.

2. ОБХВАТ

“ПОЛИТИКА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ” (***Политиката***) могат да бъдат използвани от разчитащите страни и потребителите на квалифицирани удостоверителни услуги.

SEP България гарантира надеждността на предоставените квалифицирани TSS чрез своя сертификационен орган за удостоверяване на време (eSign Sep TSA).

Предоставянето на квалифицирани електронни времеви печат се основава на инфраструктурата с публичен ключ, защитени източници на време и сертификат X.509.

3. ПРЕПРАТКИ

В настоящия документ се съдържат препратки към стандарти и стандартизационни документи, процедури, директиви, национално законодателство и Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (Регламент (ЕС) No 910/2014), в това число:

1. Recommendation ITU-R TF.460-6: „Standard-frequency and time-signal emissions";
2. ISO/IEC 19790:2012: „Information technology - Security techniques - Security requirements for cryptographic modules";
3. ISO/IEC 15408 (parts 1 to 3): „Information technology - Security techniques - Evaluation criteria for IT security";
4. ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
5. ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps";
6. ETSI EN 319 422: „Electronic Signatures and Infrastructures (ESI); Time-Stamping protocol and Time-Stamp token profiles";
7. FIPS PUB 140-2: „Security Requirements for Cryptographic Modules";
8. IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)";
9. IETF RFC 5816: „ESSCertIDV2 update to RFC 3161";
10. Практика при предоставяне на квалифицирани удостоверителни услуги (Certification Practice Statement/CPS) на СЕП България.

4. ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

4.1. ОПРЕДЕЛЕНИЯ

1. Network Time Protocol (NTP) - мрежов протокол, който се използва от програми за синхронизация на времето на една или мрежа от много информационни системи;
2. Electronic time-stamp (Time-Stamp tamp) - данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент;
3. Qualified Electronic Time-stamp - електронен времеви печат, който отговаря на изискванията на Регламент (ЕС) № 910/2014;
4. Time-Stamp Certification Authority ("eSign Sep TSA") - вътрешна инфраструктурна единица в рамките на eSign SEP QES CA която издава квалифицирани електронни времеви печати;
5. Qualified Time-Stamping Service (TSS) (Квалифицираната услуга за удостоверяване на време) - услуга за удостоверяване на датата и часа на предоставяне на електронен документ;
6. Time-Stamp tamp token profiles (TST) - Информационен обект определен в препоръка IETF RFC 3161 (профил на електронно подписано удостоверение от „ eSign Sep 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);

7. Relying party: физическо или юридическо лице, което приема електронен времеви печат и се доверява на удостоверените в него факти;

8. User: физическо или юридическо лице (Титуляр/Създател), на което е предоставена услугата за издаване на квалифициран електронен времеви печат
9. Time-stamp policy: набор от правила, който указва приложимостта на знак за времева маркировка към определена общност и / или клас на приложение с общи изисквания за сигурност;
10. Time-stamp token: Информационен обект определен в препоръка IETF RFC 3161. Удостоверява съществуването 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;
11. Time-Stamping Authority (TSA): орган за удостоверяване на време
12. time-stamping unit(TSU): конфигуриран хардуер и софтуер, който се управлява като единна система и има активен секретен/частен ключ за подписване по време на предоставяне на квалифицираната удостоверителна услуга за време

4.2. СЪКРАЩЕНИЯ

1. TSA - Time-Stamping Authority;
2. TSS - Time-Stamping Service;
3. TSU - Time-Stamping Unit;
4. TST - Time-stamp Token;
5. UTC - Coordinated Universal Time;
6. PKI - Public Key Infrastructure.

5. ОБЩИ ПОНЯТИЯ

5.1. QUALIFIED TIME-STAMPING CERTIFICATION SERVICES (TSS / TIME-STAMPING SERVICES)

Обменът на данни в инфраструктурата на СЕП България, която се използва за издаване и управление на квалифицирани електронни времеви печати се състои от два основни компонента:

1. Технологична система, която издава квалифицирани електронни времеви печати, поддържа регистър и архив на генерираните токъни за електронен времеви печати;
2. Управление на системата, чрез която се наблюдават и контролират операциите по приемане на онлайн заявки, издаване, проверка и утвърждаване на издадените токъни за електронни времеви печати .

Управлението на системата гарантира директен достъп до сигурен източник на координирано универсално време (UTC) и надеждно управление на компонентите на технологичната система. TSS се изпълнявана от вътрешно звено на eSign -

Орган за удостоверяване на време ("eSign Sep TSA"). Органът за удостоверяване на време издава квалифицирани електронни времеви печати (Qualified Timestamp), чрез които потребителите на Доставчика могат да удостоверят времето за представяне на електронни документи, електронни подписи, електронни транзакции и др. Квалифицираният електронен времеви печат е доказателство, че обектът от данни е съществувал към момента на поставяне на времевия печат..

За тази цел е необходимо “eSign Sep TSA” да:

a) Потвърди съществуването на данните;

b) осигури доказателство, че електронния подпис/печат е положен при валидна двойка криптографски ключове, използвани за подписване/подпечатване на електронния документ или електронното съобщение;

c) издаде квалифициран електронен времеви печат в съответствие със стандарт ETSI EN 319 422;

d) издаде квалифициран електронен времеви печат, който не съдържа грешки или неточна информация;

e) не е страна по сделките, посочени и обозначени с удостоверението за време.

5.2. ОРГАН ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ, ESIGN SEP TSA

„eSign Sep TSA“ е Удостоверяващ орган в структурата на СЕП България, който предоставя квалифицирани услуги за удостоверяване на време, съгласно условията посочени в този документ.

СЕП България потвърждава че, “eSign Sep TSA” подлежи на одит, най-малко веднъж на 24 месеца от Орган за оценяване на съответствието. В рамките на нормативното време, докладът за оценяване на съответствието се предава на Органа по надзор – Комисия за регулиране на съобщенията.

5.3. ПОТРЕБИТЕЛИ

Потребители са лицата, описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги" на СЕП България.

Когато потребителят е организация състояща се от няколко крайни потребителя или индивидуален краен потребител, някои от задълженията отнасящи се за организацията, ще бъдат прилагани и към крайните потребители. Следователно, организацията следва да информира своите крайни потребители относно отговорността и задълженията им. При всички положения организацията носи отговорност, ако задълженията на крайните потребители не са коректно изпълнени.

Когато потребителят е краен клиент, той носи отговорност в случай, че не изпълнява задълженията си коректно, съгласно условията, произтичащи от този документ.

5.4. ОБЩИ РАЗПОРЕДБИ

Настоящата политика определя набор от правила, които СЕП България спазва при издаването на електронни времеви печати. Този документ допълва „Практиката при предоставяне на квалифицирани удостоверителни услуги" на СЕП България.

Доставчикът издава квалифицирани електронни времеви печати на всяка заинтересована страна, без никакви технически лимити. Издаването на квалифицирани електронни времеви печати може да бъде възмездно или безвъзмездно. Информация за такси, събирани от СЕП България мажете да намерите на интернет страницата: http://www.eSign.bg

1. Предназначение

   Политиката се публикува на уебсайта на Доставчика и е достъпна за всички заинтересовани страни.

   Управлението на персонала, физическата и оперативната сигурност на дейностите на Доставчика при предоставяне на квалифицирани удостоверени услуги са описани в CPS на СЕП България.

2. Специфика

   Политиката определя само общите правила за издаване и управление на квалифицирани електронни времеви печати. Подробно описание на технологичния процес се съдържа в допълнителни документи, които не са публични. Непубликуваните документи, заедно със записите, са резултат от външни и вътрешни одити и са достъпни само за упълномощени лица.

3. Подход

   Тази документ е разработен в общ план и не описва всеки технически детайл. Той определя условията и правилата, към които се придържа СЕП България, в качеството си на квалифициран доставчик на удостоверителни услуги и е неделима част от Общите условия на договора с Потребителите, при предоставяне на квалифицирани електронни времеви печати.

6. ПОЛИТИКА

6.1. ОБЩИ ПОЛОЖЕНИЯ

Политиката определя набор от правила, които СЕП България спазва при издаване на квалифицирани времеви печати, за да осигури точно време спрямо Coordinated Universal Time (UTC) с точност до 0.5 секунди.

СЕП България гарантира:

1. публичен достъп за получаване и проверка на издадените квалифицирани удостоверения за време;
2. че са спазени съответните мерки за сигурност в съответствие с общоприетите международни практики;
3. че са спазени съответните мерки за сигурност в съответствие с общоприетата международна практика;
4. дейността на доставчика е организирана по такъв начин, че издаването на квалифицирани електронни времеви печати е отделено от другите дейности на СЕП България;
5. профилът на токън за електронни времеви печат е в съответствие със стандарт ETSI EN 319 422;
6. Токънът за електронен времеви печат (TST) издаден от „eSign Sep TSA" съдържа информация за печата (TST-info structure) разположен в Signed-Data структура (RFC 2630), подписан от eSign Sep TSA и вградени в Content-Info

структура (RFC 2630). Издаваните времеви печати са съвместими с препоръките на RFC 3161. Квалифицираната услуга за удостоверяване на време издава RSA 2048 битови криптирани квалифицирани електронни времеви печати, като се използва алгоритъм SHA256.

Профилът на удостоверението на „eSign Sep TSA“, с което се верифицира електронния времеви печат в издадения токън за електронен времеви печат (TST) е:

eSign Sep TSA		
Version	V3	
Signature algorithm	sha256RSA	
Signature hash algorithm	sha256	
Issuer	CN	eSign Sep QES CA
	OU	SEP Bulgaria JSC Qualified QES Authority
	2.5.4.97 (organizationIdentifier)	NTRBG-131107204
	O	Sep Bulgaria JSC
	C	BG
Validity	5 years	
Subject	CN	Common Name
	*2.5.4.97 (organizationIdentifier)	Идентификатор за юридическо лице NTRYY-xxxxxxxxx /национален идентификационен код/ VATYY-xxxxxxxxx /Данъчен номер/ YY – код на държава
	O	Organization
	L	Locality
	C	Country
Public key	RSA 2048 bits	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.esign.bg/bg/services/public-register/eSign_Sep_QES_CA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.esign.bg/ocsp	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/	
CRL Distribution Points (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSignSepQESCA.crl	
Basic Constraints (Critical)	Subject Type=End Entity Path Length Constraint=None	
Key Usage (Critical)	Digital Signature (80)	
Enhanced Key Usage (Critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	

6.2.ИДАНТИФИКАТОР НА ПОЛИТИКАТА (OID)

Чрез включването на този обектен идентификатор в издадените токъни за електронен времеви печат, СЕП България потвърждава съответствие с настоящата политика.

Идентификаторът (OID) на eSign SEP TSA е: 1.3.6.1.4.30299.3.1.2

Горепосоченият обектен идентификатор е в съответствие с ETSI BTSP (Best Practices Policy for Timestamps) 0ID=0.4.0.2023.1.1, съгласно стандарта ETSI EN 319 422

6.3.ПРИЛОЖИМОСТ НА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ

Квалифицираната услуга за удостоверяване на време (TSS), позволява за всеки подписан с електронен подпис/печат документ, да се удостовери датата и часа на представяне на електронния подпис/печат.

Този документ не определя никакви ограничения в приложимостта на токъна за електронен времеви печат (TST), издаден в съответствие с тази политика.

Политиката е насочена към изпълнение на изискванията за квалифицирани електронни времеви печати с дълъг период на валидност (ETSI EN 319 122 [6]), но е приложима към всяка друга употреба на времеви печати с еквивалентни изисквания.

6.4.СЪОТВЕТСТВИЕ

Издаденият токън за електронен времеви печат (TST) включва идентификатора на Политиката, описан т. 6.2.

„eSign SEP TSA“ изпълнява само заявки за електронни времеви печати, издавани в съответствие на настоящата политика.

„eSign SEP TSA“ осъществява дейността си в съответствие с приложимото законодателство и стандарти:

1. Регламент (ЕС) № 910/2014;
2. ETSI TS 119 421;
3. IETF RFC 3161;
4. IETF RFC 5816.

7. ЗАДЪЛЖЕНИЯ

7.1. ОБЩИ ЗАДЪЛЖЕНИЯ НА ESIGN SEP TSA

СЕП България гарантира съответствие на процедурите в настоящата политика с изискванията на Регламент (ЕС) № 910/2014 и относимите към него нормативни актове, както и националното законодателство. Процедурите подлежат на контрол от Орган за оценяване на съответствието и Орган по надзор.

СЕП България гарантира постоянен достъп до Квалифицираната услуга за удостоверяване на време (Qualified TSS) (24/7/365), с изключение на времето за редовните технически профилактики на технологичната система. Услугата за издаване на квалифицирани електронни времеви печати е с точност до 0,5 (половин) секунда и гарантира на потребителите точност, дори при множество едновременни връзки (например над 100 потребители).

СЕП България гарантира:

1. предоставяните удостоверителни услуги са съобразени с общоприети международни стандарти и документи, описани в „Практика за предоставяне на квалифицирани удостоверителни услуги";
2. използва надеждно и сигурно технологично оборудване (хардуер и софтуер), за предоставяне на квалифицираната удостоверителна услуга;
3. осъществява дейността си, в съответствие със законодателството;
4. издадения електронен TST не съдържа никакви неверни данни или грешки;
5. не се нарушават лицензни, интелектуална собственост или други права в издаваните токъни за електронни времеви печати (TST);
6. не допуска модифицирането на цифровите данни след издаване на токъна на времевия печат TST, без това да бъде установено.

7.2.ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИ

Потребителите са задължени да проверят валидността на електронния подпис на eSign Sep TSA и/или Списъка със спрени и прекратени удостоверения (CRL) при извличане на токъна за електронен времеви печат (TST). Актуализираните списъци (CRL) са публикувани на уеб страницата на СЕП България на:

http://www.eSign.bg.

Проверка на удостоверението на eSign Sep TSA може да се направи и с използване на услугата за Онлайн проверка на статуса на удостоверение (OCSP): http://www.eSign.bg..

Допълнителни задължения на потребителите са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги „ на СЕП България.

7.3.ЗАДЪЛЖЕНИЯ НА ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяващата се страна трябва да има необходимия минимум от технически познания за използване на квалифицираната услуга за удостоверяване на време и да полага дължимата грижа. Основното задължение на Доверяващата се страна е да провери подписа върху токъна за електронния времеви печат (TST). Доверяващата се страна трябва да провери валидността на удостоверението на Органа за удостоверяване на време eSign Sep TSA, както

и срока на валидност на това удостоверение. В случай на проверка на времеви печати, след изтичане на срока на валидност на удостоверението на eSign Sep TSA, доверяващите се страни трябва:

1. да направят проверка в CRL за удостоверението на eSign Sep TSA;
2. да направят проверка за приложимостта на използвания хеш алгоритъм;
3. да се уверят в сигурността на използвания електронен подпис, като проверят приложимата комбинация на асиметрични и хеш алгоритми.

Използването на времеви печати трябва да отговаря на изискванията на настоящата политика и на CPS на СЕП България.

8. ОТГОВОРНОСТ

Отговорността на всяко лице, участник в дейността по предоставяне и ползване на квалифицирана удостоверителна услуга е уредена в закона или се уговаря в договора между СЕП България и потребителя.

СЕП България отговаря пред потребителите на удостоверителни услуги, които разчитат на неговата дейност за вреди, причинени от умисъл и груба небрежност. Отговорност на Доставчика се отнася само, ако вредите са пряка и непосредствена последица от виновно поведение на СЕП България или на лицата, на които е възложил осъществяване на функции във връзка с предоставяните удостоверителни услуги по удостоверяване на време.

Ако Доставчика потвърди и приеме, че са настъпили вреди, той се ангажира да възмезди увреденото лице. СЕП България отговаря до размера на реалните вреди.

Задължителната застраховка покрива отговорността на СЕП към Потребители, съответно Доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в националното законодателство и тази практика.

9. REQUIREMENTS TO ESIGN SEP TSA

СЕП България гарантира, че осъществява надеждно, сигурно и законосъобразно управление на дейността си. като контролира всички страни, свързани по някакъв начин с процедурите на отчитане на времето, записва информацията и управлява по подходящ начин персонала, за да извършва коректно задълженията си. Всички документи, свързани с регистрираната информация и събития се записват в журнали и се архивират. Съхранението на записите се осъществява по сигурен начин. Достъп до тези данни имат единствено оторизирани служители на Доставчика.

eSign Sep TSA осъществява контрол на дейността си, което позволява предоставянето на квалифицирана удостоверителна услуга в съответствие с разпоредбите на настоящата Политика. За да се контролира ефективното функциониране на технологичната система за отчитане на времето, профилите на потребителите и дейността на персонала, всички събития в системата се регистрират..

10. ПРАКТИКА НА ESING SEP TSA

10.1. ПРАКТИКА

Управление на сигурността и поддръжка на инфраструктурата, процедури, механизми за контрол на Доставчика са подробно описани в документа CPS на СЕП България.

Задълженията и отговорността на eSign Sep TSA са описани в т. 7.1 на настоящата политика и са в основата на функциониране на Удостоверяващия орган.

Контролите позволяват непрекъсната проверка на целостта на технологичната система, своевременна актуализация и отстраняване на неизправности. Осъществяваният надзор на функционалността на технологичната система гарантира, че тя работи правилно и в съответствие с доставената производствена конфигурация.

10.2. ДОСТЪПНОСТ НА УСЛУГАТА

СЕП България прилага следните мерки, за да осигури достъп до услугата:

1. резервираност на компютърните системи;
2. резервираност на интернет свързаността;
3. употреба на непрекъсваеми електрозахранвания.

Настоящата политика е публична достъпна на интернет страницата на Доставчика:

http://www.eSign.bg

11. ПРОЦЕДУРИ НА ESIGN SEP TSA

11.1. УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКАЛ НА ДВОЙКАТА КЛЮЧОВЕ

11.1.1 ГЕНЕРИРАНЕ НА ДВОЙКАТА КЛЮЧОВЕ НА ESIGN SEP TSA

Изискванията за използваните алгоритми и дължината на подписващия частен ключ на eSign Sep TSA са в съответствие с техническата спецификация ETSI TS 119 312.

Генерирането на подписващия ключ се извършва в криптографски модул (HSM) с ниво на сигурност FIPS 140-2, ниво 3.

Генерираната двойка RSA ключове е с дължина 2048 бита.

Генерирането на ключ за подписване на eSign Sep TSA се извършва в физически защитена среда от хора с доверени роли. Достъпът е двустепенен от поне две упълномощени лица..

11.1.2 РАЗПРОСТРАНЕНИЕ НА ПУБЛИЧНИЯ КЛЮЧ НА ESIGN SEP TSA

Удостоверението на eSign Sep TSA заедно със съответния публичен ключ се публикува на интернет страницата на Доставчика: https://www.eSign.bg

11.1.3 ПРЕИЗДАВАНЕ НА ЧАСНИЯ КЛЮЧ НА ESIGN SEP TSA

Жизненият цикъл на частния ключ на eSign Sep TSA не може да бъде по-дълъг от периода на време, през който избраният алгоритъм или дължина на ключа удовлетворяват целта, за която са приети за използване. Периодът на валидност на удостоверението на eSign Sep TSA е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 5 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 eSign Sep TSA. Двойката ключове с изтекъл период на валидност се съхранява, както следва:

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

Всички използвани алгоритми се проверяват веднъж годишно или когато настъпят промени. В случай, че алгоритъмът бъде компрометиран или стане неподходящ, за целта се пристъпва към прегенерирането на всички засегнати ключове.

11.1.4 УНИЩОЖАВАНЕ НА ЧАСТНИЯ КЛЮЧ НА ESIGN SEP TSA

След изтичането на срока на валидност на частния ключ на eSign Sep TSA, същият се унищожава по начин, по който не може да бъде възстановен.

11.1.5 ЗАЩИТА НА ЧАСНИЯ КЛЮЧ НА ESIGN SEP TSA

Частният ключ на eSign Sep TSA се генерира и съхранява в криптографски модул (HSM) съответстващ на стандарт FIPS 140-2, ниво 3.

Архивираните копия на частния ключ на eSign Sep TSA се съхраняват в специален сейф.

Съхраняването на копие на ключа се прави, за да бъде извлечено в случай на природно бедствие или катастрофа на системата. Съхраняването на ключа се проверява периодично от одитора на СЕП България. Методът на съхранение е описан в процедурите от вътрешната документация на СЕП България.

11.2. УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ПОДПИСВАЩОТО КРИПТОГРАФСКО ОБОРУДВАНЕ

По време на транспортиране и съхранение използваният криптографски модул се проверява от доверен персонал с двоен контрол. Модулът се проверява за повреди:

1. на стикерите за сигурност;
2. по кутията на модула (драскотини, вдлъбнатини);
3. по опаковката.

Прилагат се следните мерки:

1. инсталацията, активацията и създаването на резервно копие на подписващия частен ключ на eSign Sep TSA в HSM се извършва само от доверен персонал с двуфакторен контрол във физически защитена среда;
2. в случай на бракуване на криптографския модул, съдържащите се на него частни ключове ще бъдат изтрити и унищожени в съответствие с препоръките на производителя.

11.3. УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIME-STAMPING)

Сървърният софтуер на eSign Sep TSA i имплементира техническата спецификация ETSI TS 101 861 v.1.3.1 и международната препоръка IETF RFC 3161.

Системният софтуер на eSign Sep TSA поддържа комуникация с клиентите на услугата по удостоверяване на време по протоколи: TCP/IP, HTTP/HTTPS.

11.4. ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TST)

Всеки токън за електронен времеви печат (TST), издаден от СЕП България, включва уникален идентификатор на политиката на. eSign Sep TSA

Профилът на заявките/отговорите на eSign Sep TSA е в съответствие с горепосочените технически спецификации и включва следните атрибути/параметри.

1. Заявката за издаване на TSQ съдържа:

Поле	Значение/Стойност
Version	1
Message Imprint Hash Algorithm	OID на хеша SHA-1, SHA-256
Message Imprint Hash Value	Хеш стойност на данните
Requested Policy	(null)
Nonce	Само ако присъства в заявката
Request certificates	Ако е TRUE се включва калифицираното удостоверение eSign Sep TSA

2. Отговора на заявката (TSR) съдържа:

Поле	Значение/Стойност
Status	0/ Operation Okay
Policy	1.3.6.1.4.1.30299.3.1.2
Message Imprint hash algorithm	OID на хеша SHA-1, SHA-256
Message Imprint hash value	Хеш стойност на данните
Serial Number	Сериен номер на удостоверението
Generated Time	Времето на представяне на електронния подпис/печат (удостоверено време по UTC)
Accuracy	500ms
Nonce	Само ако присъства в заявката
TSA	CN=eSign Sep TSA

11.5. СИНХРОНИЗАЦИЯ НА ЧАСОВНИКА С КООРДИНИРАНО УНИВЕРСАЛНО ВРЕМЕ

СЕП България гарантира, че осигурява физическа и информационна сигурност на технологичната система за предотвратяване на неразрешени операции, насочена към липса на калибриране на часовника или физическо увреждане.
eSign Sep TSA използва хардуер и източник на точно калибрирано време с висока степен на точност. Синхронизирането на UTC с източника на време е автоматично, базирано на протокол NTP, след установяване на разликата 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, чрез протокол NTP.
СЕП България има одити, които позволяват откриването на всяка разлика между часовника и времето, включена в електронния TST.

11.6. УПРАВЛЕНИЕ И СИГУРНОСТ

11.6.1 ОЦЕНКА НА РИСКА

СЕП България редовно извършва оценка на риска, за да осигури качество и надеждност на предлаганите услуги. Проверките на сигурността, дефинирани в концепцията за сигурност на Доставчика се контролират на всеки три месеца с цел осигуряване ефективност на контрола.

Описание на процедурите и плановете за постигане на непрекъснатост и сигурност на дейността на Доставчика са описани в документа CPS на СЕП България.

Всички системи, включени в издаването на квалифициран електронен времеви печат предлагат висока степен на надеждност.

Технопогичната система се намира във физически защитена среда, което минимизира риска от природни бедствия.

В случай, че частният ключ на eSign Sep TSA бъде компрометиран, засегнатият криптомодул (HSM) бива незабавно изолиран от мрежата, след което се вземат коригиращи мерки:

1. уведомяване на администратора по сигурността, с цел предприемане на бъдещи действия;
2. започване на одит по сигурността на останалите криптомодупи (HSM-и) - проверка на интегритет и анализ на журнала;
3. уведомяване на доверяващите се страни, които са засегнати от компрометирането;
4. започване на процедура по подмяна.

11.6.2 УПРАВЛЕНИЕ НА СИГУРНОСТТА

В СЕП България е въведена политика по информационна сигурност. Политиката по информационна сигурност се разглежда редовно и в случай на настъпили промени.

Всички въпроси, свързани с управлението на сигурността, са описани в документа CPS на СЕП България.

11.6.3 ОПЕРАТИВНА СИГУРНОСТ

Характеристиката на персонала и доверените роли на Доставчика са в съответствие с документа CPS на СЕП България.

СЕП България поддържа квалифицирани служители на длъжности, които осигуряват изпълнения на задълженията си във всеки момент при осъществяването на дейността по издаване на квалифицирани електронни времеви печати, в съответствие с нормативната уредба.

11.6.4 ФИЗИЧЕСКА СИГУРНОСТ

Сигурното и надеждно извършване на операции от eSign Sep се осъществява посредством различни нива на сигурност на физическия и логически достъп до технологичната система.

СЕП България осигурява:

1. наблюдение на мрежата и услугите;
2. разделяне на задълженията;
3. разделяне на мрежови сегменти;
4. защитена физическа среда;
5. подсигуряване на компютърните системи.

В случай, че служител, който отговаря за дейности за удостоверяване на време, смени своята роля или напусне дружеството, всички принадлежащи му носители, свързани със сигурността се връщат или инвалидират.

Физическият контрол и достъпа са в съответствие с документа CPS на СЕП България.

11.6.5 МРЕЖОВА СИГУРНОСТ

Въз основа на оценката на риска, мрежовата инфраструктура е разделена на зони, като се има в предвид функционалната, логическа и физическа връзка между надеждните системи и услуги. СЕП България ограничава достъпа и комуникациите до такова ниво, което е необходимо за нормалната работа на сертифицираните услуги. Връзките и услугите, които не се отнасят към удостоверителните услуги са деактивирани. Установеното правило за достъп се разглежда на определен период.

Всички елементи на критичната инфраструктура се пазят в защитена зона.

Изградена е административна мрежа, която е отделена от мрежата за оперативни цели. Системите използвани за администрация не могат да бъдат използвани за неадминистративни дейности.

Тестовата и експлоатационната платформа са отделени от други среди нямащи отношение към работни операции.

Комуникацията между отдалечени доверени системи се извършва само през сигурни канали, които са логически отделени от останалите комуникационни канали и предоставят идентификация на своите крайни точки. Осигурена е защита на данните по канала срещу разкриване или модификация.

Свързаността към интернет е резервирана.

Редовно се сканират за уязвимости публичните и частните IP адреси за достъп, след което се изготвя доклад.

Тест за проникване в системите се извършва в следните случаи: след първоначална настройка на системите и след инфраструктурни или надграждания на приложения и промени. След приключване на теста се изготвя доклад.

11.6.6 УПРАВЛЕНИЕ НА ДЕЙНОСТТА

СЕП България е защитила всички системи в съответствие с политиката за сигурност.

СЕП България прилага политики, осигуряващи своевременно прилагане на корекции за сигурност (patch/software corrections).

При всяка ново разработена система се прави анализ на изискванията по отношение на сигурността още по време на етапа на дизайн и планиране на функционалността.

При пускането на нови версии се прилагат процедури за контрол на промените, включително при спешни промени в софтуера.

Интегритетът на системите и информацията на eSign Sep TSA е защитен от вируси, злонамерен код и неразрешен софтуер.

Боравенето с външни носители в СЕП България се осъществява по сигурен начин с цел защитата им от повреда, кражба или остаряване.

Въведени са процедури за всички доверени и административни роли, които имат отношение към предоставяне на удостоверителни услуги.

Изискванията към капацитета на компютърните системи се следят, с цел осигуряване на достатъчно количество изчислителна мощност и дисково пространство.

11.6.7 УПРАВЛЕНИЕ НА ДОСТЪПА ДО СИСТЕМА

СЕП България осигурява наблюдение върху достъпа до компютърните системи и потребителски заявки, относно:

1. необичайни системни дейности, които показват потенциално нарушение на сигурността, включително проникване в мрежата на СЕП България и докладване, чрез система за алармиране;
2. стартиране и изключване на логващите функции;
3. наличност и използване на услуги в мрежата на СЕП България.

При всяко нарушение на сигурността или загуба на интегритет, които имат значително влияние върху предлаганата доверена услуга, както и върху управляваните лични данни, СЕП България съобщава на Органа по надзор. След откриването на критичен пробив в сигурността Органа по надзор се уведомява в срок от 24 ч.

11.6.8 СИГУРНА СРЕДА

Оперативната среда за съхранение на частния ключ на eSign Sep TSA и за електронно подписване на електронни TST, предоставена на потребителите, е HSM със сертификат за ниво на сигурност FIPS 140-2 Level 3.

Документите, свързани със сигурността на средата са предимно вътрешна документация на СЕП България и се преглеждат периодично от одитора.

11.7. КОМПРОМЕТИРАНЕ НА ЧАСНИЯ КЛЮЧ НА ESIGN SEP TSA

СЕП България полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на частния ключ на eSign Sep TSA вследствие на човешка грешка, природни бедствия или аварии.

В случай на компрометиране или съмнение за компрометиране на частен ключ на eSign Sep TSA, се предприемат следните действия:

1. прекратява се незабавно удостоверението на eSign Sep TSA;
2. eSign Sep QES CA генерира нова двойка ключове и ново удостоверение;
3. всички потребители и доверяващи се страни се информират за случилото се незабавно, с информация на страницата на СЕП България;
4. удостоверението, съответстващо на компрометирания ключ се поставя в Списъка със спрени и прекратени удостоверения (CRL), заедно с подходяща причина за прекратяване;
5. извършва се незабавен анализ и се изготвя доклад за причината за компрометирането.

Тези операции се извършват в съответствие с плана, разработен от СЕП България за инциденти със сигурността.

11.8. ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ESIGN SEP TSA

СЕП България изпълнява процедурите от CPS в случай на прекратяване на eSign Sep TSA.

11.9. СЪОТВЕТСТВИЯ С ПРАВНИ ИЗИСКВАНИЯ

За всички въпроси, неуредени в CPS на СЕП България се прилагат разпоредбите на Регламент 910/ЕС и приложимото законодателство.

Всички изисквания за предоставяне на квалифицирани електронни времеви печати, произтичащи от настоящия документ, са в съответствие с изискванията на стандартите и стандартизационни документи на ETSI, произтичащи от разпоредбите на Регламент (ЕС) № 910/2014..

11.10. ЗАПИС НА СЪБИТИЯ

СЕП България регистрира и поддържа достъпна цялата информация, свързана с издадените или получените данни, за съответния период от време. Тези записи се съхраняват дори след прекратяване на услугата. Всяко доказателство за състоянието на технологичната система и информационните данни се записва по сигурен и надежден начин..

СЕП България осигурява:

1. записи, отнасящи се до дейността на услугата, могат да бъдат предоставени на компетентните органи за целите на съдопроизводството, в случай че е нужно доказателство за правилната й работа;
2. водят се записи на всички събития, отнасящи се до жизнения цикъл на ключовете и удостоверенията на eSign Sep TSA ;
3. водят се записи на всички събития свързани със синхронизацията на часовника на eSign Sep TSA с координираното универсално време (UTC). Това включва информация отнасяща се до нормалното прекалибриране или синхронизиране на часовниците, използвани при предоставянето на квалифицирани електронни времеви печати ;
4. записи за всички събития при установяването на загуба на синхронизация;
5. всички събития са записват по начин, който ги прави трудни за изтриване.
6. журналите на събития се пазят най-малко 3 месеца;
7. журналът за издадените квалифицирани електронни времеви печати се пази най-малко 10 години;
8. поддържане на конфиденциалност и интегритет на текущите и архивирани записи, отнасящи се до дейността на услугата съобразно добрите практики.

11.11. ОРГАНИЗАЦИОННА СХЕМА

СЕП България поддържа вътрешни документи за правилната работа на eSign Sep TSA, описвайки оперативния контрол, свързан с: :

1. сигурност на персонала;

2. контрол на достъп;

3. оценка на риска;

4. т.н..

Тези вътрешни документи се анализират от независим Орган за оценяване на съответствието съгласно изискванията на техническа спецификация ETSI TS 119421.

„СИСТЕМА ЗА ЕЛЕКТРОННИ ПЛАЩАНИЯ/СЕП БЪЛГАРИЯ“ АД (СЕП България / Доставчик) е юридическо лице, вписано в Търговския регистър на Агенцията по вписванията под ЕИК 131107204, със седалище и адрес на управление:
Гр. София, 1164, кв. Лозенец, ул. „Златоврът“ 1
Телефон за контакти: 070018283. Интернет адрес: http://www.eSign.bg/

Регистър на измененията																				
Страница																				
Валидно изменение																				