

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

	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.				
Не се разрешава неконтролирано копиране и размножаване! Всички права са запазени! © Copyright. All Rights reserved!				

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

СЪДЪРЖАНИЕ

Утвърдил	1
1. ВЪВЕДЕНИЕ	5
1.1. ПРЕГЛЕД	5
1.2. ИМЕ И ИДЕНТИФИКАЦИЯ	6
1.3. УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА СЕП БЪЛГАРИЯ	6
1.4. БАЗОВ ОРГАН (ESIGN SEP ROOT CA)	7
1.4.1. ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН (ESIGN SEP QES CA)	7
1.4.2. РЕГИСТРИРАЩ ОРГАН	7
1.4.3. ПОТРЕБИТЕЛИ	7
1.4.4. ДОВЕРЯВАЩИ СЕ СТРАНИ	7
1.4.5. ДРУГИ УЧАСТНИЦИ	8
1.5. УПОТРЕБА И ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	8
1.5.1. ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	8
1.5.2. ЗАБРАНА ЗА УПОТРЕБА НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	8
1.6. УПРАВЛЕНИЕ НА ПОЛИТИКАТА	8
1.6.1. ОРГАНИЗАЦИЯ, УПРАВЛЯВАЩА ПОЛИТИКАТА	8
1.6.2. ЛИЦЕ ЗА КОНТАКТ	8
1.6.3. ВРЪЗКА МЕЖДУ ПОЛИТИКАТА И ПРАКТИКАТА	8
1.6.4. ЛИЦЕ ЗА КОНТАКТ И ПРОЦЕДУРИ ЗА ОДОБРЕНИЕ НА ПРАКТИКАТА	9
1.7. ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ	9
1.7.1. ОПРЕДЕЛЕНИЯ	9
1.7.2. СЪКРАЩЕНИЯ	10
2. ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ	11
2.1. ХРАНИЛИЩЕ	11
2.2. ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ СЕП БЪЛГАРИЯ	11
2.3. ЧЕСТОТА НА ПУБЛИКУВАНЕ	11
2.4. ДОСТЪП ДО ПУБЛИКАЦИИ	12
3. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ	12
3.1. ИМЕНА	12
3.2. ПЪРВОНАЧАЛНА РЕГИСТРАЦИЯ	12
3.2.1. ПРОВЕРКА ЗА ПРИТЕЖАНИЕ НА ЧАСТЕН КЛЮЧ	13
3.2.2. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ	13
3.2.3. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ	13
3.2.4. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ	13
3.2.5. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПРАЖНЯВАЩО СВОБОДНА ПРОФЕСИЯ	13
3.2.6. ПРОВЕРКА ОТ УДОСТОВЕРЯВАЩИЯ ОРГАН	14
3.3. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	14
3.4. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	14
3.5. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	14
3.6. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	15
4. ОПЕРАТИВНИ ИЗИСКВАНИЯ	15
4.1. УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И ДВОЙКА КЛЮЧОВЕ	15
4.1.1. ОТ ПОТРЕБИТЕЛИ	15
4.1.2. ОТ ДОВЕРЯВАЩИ СЕ СТРАНИ	16
4.2. ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ (RENEWAL)	16
4.3. ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (RE-KEY)	16
4.4. ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	16
4.5. СПИРАНЕ И ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	16
4.5.1. ОБСТОЯТЕЛСТВА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	16
4.5.2. ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	17
4.5.2.1. ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КРАЕН ПОТРЕБИТЕЛ	17

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

4.5.3.	ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	17
4.5.4.	ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ	18
4.5.5.	ОБСТОЯТЕЛСТВА ЗА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	18
4.5.6.	ПРОЦЕДУРА ЗА СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	18
4.5.7.	ГРАТИСЕН ПЕРИОД НА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	18
4.5.8.	ВЪЗОБНОВЯВАНЕ ДЕЙСТВИЕТО НА СПРЯНО УДОСТОВЕРЕНИЕ	18
4.6.	ПРОВЕРКА НА АКТУАЛНОТО СЪСТОЯНИЕ (СТАТУС) НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	19
4.7.	ПРЕКРАТЯВАНЕ НА ДОГОВОР ЗА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ ПОТРЕБИТЕЛ	19
5.	КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ	19
5.1.	КОНТРОЛ НА ФИЗИЧЕСКАТА СИГУРНОСТ	19
5.1.1.	ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА	19
5.1.2.	ФИЗИЧЕСКИ ДОСТЪП	19
5.1.3.	СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ	20
5.1.4.	ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИ	20
5.2.	ОРГАНИЗАЦИОНЕН КОНТРОЛ	20
5.2.1.	ДОВЕРЕНИ РОЛИ	20
5.2.2.	ИЗИСКВАНИЯ ЗА РАЗДЕЛЯНЕ НА ОТГОВОРНОСТИТЕ	20
5.3.	КОНТРОЛ НА ПЕРСОНАЛА	20
5.3.1.	ИЗИСКВАНИЯ ЗА ОБУЧЕНИЕ НА ПЕРСОНАЛА НА СЕП БЪЛГАРИЯ	20
5.4.	ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ	21
5.4.1.	Уязвимост и оценка	21
5.5.	АРХИВИРАНЕ	21
5.6.	ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА	21
5.6.1.	ИЗИСКВАНИЯ, СВЪРЗАНИ С ПРЕХОДА ДО ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА	21
5.6.2.	ПРЕХВЪРЛЯНЕ НА ДЕЙНОСТ КЪМ ДРУГ РЕГИСТРИРАН ДОСТАВЧИК НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	22
5.7.	ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ДОСТАВЧИК ИЛИ НА КВАЛИФИЦИРАН СТАТУТ НА УДОСТОВЕРИТЕЛНА УСЛУГА ..	22
6.	УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ	23
6.1.	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА УДОСТОВЕРЯВАЩ ОРГАН	23
6.1.1.	ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ПОТРЕБИТЕЛ	23
6.1.1.1.	ИЗИСКВАНИЯ КЪМ УСТРОЙСТВОТА ЗА СЪЗДАВАНЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ (QSCD) 23	
6.1.2.	ДОСТАВКА НА ЧАСТЕН КЛЮЧ НА ПОТРЕБИТЕЛ	23
6.1.3.	ПРЕДОСТАВЯНЕ НА ПУБЛИЧЕН КЛЮЧ ОТ ПОТРЕБИТЕЛ НА ДОСТАВЧИК	24
6.1.4.	ДЪЛЖИНА НА КЛЮЧОВЕ	24
6.1.5.	ПАРАМЕТРИ НА ПУБЛИЧЕН КЛЮЧ	24
6.2.	ЗАЩИТА НА ЧАСТЕН КЛЮЧ И КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ	24
6.2.1.	КОНТРОЛ НА ИЗПОЛЗВАНЕ И СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ	24
6.2.2.	СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ	25
6.2.3.	МЕТОД ЗА АКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ	25
6.2.4.	МЕТОД ЗА ДЕАКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ	25
6.2.5.	МЕТОД ЗА УНИЩОЖАВАНЕ НА ЧАСТЕН КЛЮЧ	25
6.3.	ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕ НА ДВОЙКА КЛЮЧОВЕ	25
6.3.1.	АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ	25
6.3.2.	ПЕРИОД НА ВАЛИДНОСТ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И УПОТРЕБА НА КЛЮЧОВЕ	25
6.4.	ДАННИ ЗА АКТИВИРАНЕ	26
6.4.1.	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДАННИ ЗА АКТИВИРАНЕ	26
6.4.2.	ЗАЩИТА НА ДАННИ ЗА АКТИВИРАНЕ	26
6.5.	СИГУРНОСТ НА КОМПЮТЪРНИТЕ СИСТЕМИ	26
6.6.	СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА	26
6.7.	МРЕЖОВА СИГУРНОСТ	27
7.	ПРОФИЛИ НА УДОСТОВЕРЕНИЯ	27
7.1.	ПРОФИЛИ НА УДОСТОВЕРЕНИЯ НА ДОСТАВЧИКА	27
7.1.1.	ПРОФИЛ НА БАЗОВО УДОСТОВЕРЕНИЕ НА УДОСТОВЕРЯВАЩ ОРГАН (eSIGN SEP ROOT CA)	27
7.1.2.	ПРОФИЛ НА УДОСТОВЕРЕНИЕ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН (eSIGN SEP QES CA)	28
7.1.3.	ПРОФИЛ НА УДОСТОВЕРЕНИЕТО ЗА ОНЛАЙН ВАЛИДИРАНЕ (eSIGN OCSP)	28

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

7.1.4.	ПРОФИЛ НА СПИСЪКЪТ СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	29
7.2.	ПОТРЕБИТЕЛСКИ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	30
7.2.1.	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ (ESIGN QES NATURAL):	30
7.2.2.	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ, СВЪРЗАНО С ОРГАНИЗАЦИЯ, В КАЧЕСТВОТО МУ НА НЕИН ЗАКОНЕН ИЛИ ДОГОВОРЕН ПРЕДСТАВИТЕЛ (ESIGN QES DELEGATED):	31
7.2.3.	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ (ESIGN QESEAL):	33
8.	ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА	34
8.1.	ДЕЙСТВИЯ, ПРЕДПРИЕТИ В РЕЗУЛТАТ НА ИЗВЪРШЕН ОДИТ	34
9.	ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ	34
9.1.	ЦЕНИ И ТАКСИ	34
9.2.	ФИНАНСОВИ ОТГОВОРНОСТИ	34
9.3.	НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ	35
9.4.	ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ	35
9.4.1.	ПРАВО НА СОБСТВЕНОСТ НА ДВОЙКА КЛЮЧОВЕ	35
9.4.2.	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ДОСТАВЧИКА	35
9.4.3.	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН	36
9.4.4.	ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИ	37
9.5.	ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ	37
9.6.	ОТГОВОРНОСТ НА ПОТРЕБИТЕЛ	38

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1. ВЪВЕДЕНИЕ

Политиката за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати (Политиката/CP/Certificate Policy) съдържа общ преглед на правилата и нормите при предоставяне на квалифицирани удостоверителни услуги от „Система за електронни плащания България/СЕП България“ АД (СЕП България/Доставчика) в качеството му на регистриран квалифициран доставчик на удостоверителни услуги. Представена е общата концепция на СЕП България относно предоставяне на квалифицирани удостоверителни услуги. Документът дефинира страните участници в процеса по предоставяне на удостоверителни услуги, техните задължения, типовете удостоверения за квалифицирани електронни подписи/печати, процеса по идентификация и удостоверяване на автентичността на потребителите и областта на приложение на издадените удостоверения за квалифицирани електронни подписи/печати. Подробно описание на процесите и правилата, по които действа СЕП България, като квалифициран доставчик на удостоверителни услуги, са представени в документа Практика при предоставяне на удостоверителни услуги на СЕП България.

1.1. ПРЕГЛЕД

СЕП България в качеството си на регистриран квалифициран доставчик на удостоверителни услуги, осъществява следната дейност:

1. Издава удостоверения за квалифициран електронен подпис/печат, в съответствие с Регламент (ЕС) № 910/2014¹ и българското законодателство, и води регистър за тях;
2. Предоставя на всяко лице достъп до публикуваните удостоверения за квалифициран електронен подпис/печат;
3. Предоставя квалифицирани услуги по създаване на частен и публичен ключ за квалифициран електронен подпис/печат;
4. Предоставя и/или одобрява устройства за сигурно създаване на електронен подпис/печат;
5. Предоставя квалифицирани услуги по валидиране на квалифициран електронен подпис/печат.

СЕП България предоставя квалифицирани удостоверителни услуги посредством удостоверяващи и регистриращи органи. Тези органи извършват дейностите си от името и за сметка на СЕП България.

Настоящият документ е структуриран в съответствие с рамката, определена в препоръката IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

Политиката е относима със следните документи:

1. ETSI EN 319 411-2 v2.2.2 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates“;
2. ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“;
3. ETSI EN 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles“;
4. Part 5: QCStatements“;
5. ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates“.

Издаването на квалифицирани удостоверения за квалифицирани електронни подписи/печати се свързва с:

1. Издаване на квалифицирано удостоверение на физическо лице (Титуляр) - има характер на квалифицирано удостоверение за квалифициран електронен подпис;
2. Издаване на квалифицирано удостоверение на физическо лице (Титуляр), което се използва за потвърждаване на самоличността и професионална принадлежност на лице, извършващо услуги с личен труд или упражняващо свободна професия - има характер на квалифицирано удостоверение за квалифициран електронен подпис;
3. Издаване на квалифициран електронен печат на юридическо лице (Създател) - има характер на квалифицирано удостоверение за квалифициран електронен печат.

¹ 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/ЕО (Регламента)

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

4. Издаване на квалифицирано удостоверение на юридическо лице, но с Титуляр физическо лице, свързано с организация, в качеството му на неин законен или договорен представител - има характер на квалифицирано удостоверение за квалифициран електронен подпис.

Политика за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати на СЕП България е публичен документ. Този документ може да бъде променян по всяко време от Доставчика и всяка нова редакция се съобщава на заинтересованите лица, като се публикува на интернет страницата на СЕП България: <http://www.esign.bg/bg/полезно/документи/>.

1.2. ИМЕ И ИДЕНТИФИКАЦИЯ

Настоящият документ е с пълно наименование Политика за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати от „Система за електронни плащания България/СЕП България“ АД.

Удостоверенията включват идентификатор на политика, който може да се използва от доверяващите се страни при определяне на валидността и достоверността на дадено приложение, както е описано в препоръката IETF RFC 3647.

Идентификаторите за политиките на квалифицираните удостоверения, посочени в настоящия документ, са:

QCP-n-qscd:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-natural-qscd (2)

QCP-l-qscd:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-legal-qscd (3)

СЕП България поддържа и прилага Политика за квалифицирани удостоверения, която се основава на правила, определени в ETSI EN 319 411-1, с обектен идентификатор (OID – Object Identifier), както следва:

Certificate type	Object Identifier
eSign Sep Root CA	1.3.6.1.4.1.30299.3
eSign Sep QES CA	1.3.6.1.4.1.30299.3.1
eSign Sep OCSP	1.3.6.1.4.1.30299.3.1.1
eSign Sep TSA	1.3.6.1.4.1.30299.3.1.2
eSign QES Natural	1.3.6.1.4.1.30299.3.1.3
eSign QES Delegated	1.3.6.1.4.1.30299.3.1.4
eSign QESeal	1.3.6.1.4.1.30299.3.1.5

1.3. УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА СЕП БЪЛГАРИЯ

СЕП България като квалифициран доставчик на квалифицирани удостоверителни услуги предоставя услуги по генериране и управление (спиране, възобновяване и прекратяване) на квалифицирани удостоверения, чрез удостоверителен орган (УО) eSIGN SEP QES CA и услуги по идентификация и удостоверяване на автентичност на потребители, чрез регистриращ орган (РО). Други участници в инфраструктурата на Доставчика са потребители и доверяващи се страни.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1.4. БАЗОВ ОРГАН (ESIGN SEP ROOT CA)

eSign SEP Root CA издава базов електронен подпис на себе си и оперативни електронни подписи на другите удостоверяващи органи, принадлежащи към йерархията от удостоверяващи органи на СЕП България.

1.4.1. ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН (ESIGN SEP QES CA)

eSign SEP QES CA е удостоверяващ орган, който издава квалифицирани удостоверения за квалифицирани електронни подписи/печати, които се управляват от настоящата политика.

1.4.2. РЕГИСТРИРАЩ ОРГАН

Регистриращите органи (в случай, че има и външни) са част от инфраструктура на СЕП България, на които Доставчикът възлага осъществяване на услуги по регистрация, идентификация и удостоверяване на автентичност на потребителите.

Регистриращите органи предлагат следните услуги:

1. Приемат, проверяват, одобряват или отхвърлят искания за издаване на квалифицирани удостоверения за електронен подпис/печат;
2. Приемат, проверяват, одобряват или отхвърлят искания за управление на квалифицирани удостоверения за електронен подпис/печат;
3. Участват във всички етапи при идентифициране на заявителите, Титуляри и Създатели на квалифицирани удостоверителни услуги и проверка на самоличността, съответно на тяхната идентичност;
4. Сключват договори за предоставяне на квалифицирани удостоверения (по издаване, поддръжка и управление на удостоверения) с потребителите от името на СЕП България;
5. Извършват други дейности, свързани с предоставяне на квалифицирани удостоверителни услуги описани в политиките, практиките и процедурите на Доставчика.
6. Информация за контакт с регистриращите органи на СЕП България е на разположение на сайта на Доставчика в интернет: <http://www.esign.bg/bg/za> нас/.

1.4.3. ПОТРЕБИТЕЛИ

Всяко физическо или юридическо лице, което има сключен писмен договор със СЕП България е потребител на квалифицирана удостоверителна услуга, предоставена от СЕП България.

Потребителите биват:

1. Физическо лице (Титуляр), което създава квалифициран електронен подпис;
2. Физическо лице (Титуляр), което е упълномощен представител на юридическо лице и създава квалифициран електронен подпис;
3. Физическо лице (Титуляр), което упражнява свободна професия и създава квалифициран електронен подпис
4. Юридическо лице (Създател), което създава квалифициран електронен печат.

Когато това е практически осъществимо, предоставяните квалифицирани удостоверителни услуги и използваните при предоставянето на тези услуги продукти са достъпни и за хора с увреждания.

1.4.4. ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяваща се страна е физическо или юридическо лице, както и лице от държавния, обществен и политически сектор, което е адресат на електронни изявления. Доверяващата се страна разчита на електронната идентификация или удостоверителната услуга предоставена от СЕП България.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1.4.5. Други участници

Доставчикът запазва право при необходимост да сключва договори с външни фирми за предоставяне на определени удостоверителни услуги.

1.5. УПОТРЕБА И ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

1.5.1. ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

Потребителските квалифицирани удостоверения, издадени от СЕП България могат да се използват при създаване на квалифициран електронен подпис/печат в електронни документи и приложения, които изискват най-високо ниво на информационна сигурност.

1.5.2. ЗАБРАНА ЗА УПОТРЕБА НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

Квалифицирани удостоверения на СЕП България е забранено да се използват по начин, несъвместим с обявената за тях цел.

Квалифицирани удостоверения, издадени в съответствие с настоящата Политика не могат да бъдат използвани за незаконосъобразни цели.

1.6. УПРАВЛЕНИЕ НА ПОЛИТИКАТА

1.6.1. ОРГАНИЗАЦИЯ, УПРАВЛЯВАЩА ПОЛИТИКАТА

СЕП България отговаря за управлението на настоящата Политика.

Всяка версия на Политиката е в сила до момента на одобрение и публикуване на нова версия. Всяка нова версия се разработва от служители на СЕП България и след одобрение от ръководството на Доставчика се публикува.

Потребителите са длъжни да се съобразяват само с валидна версия на Политиката към момента на ползване на услугите на СЕП България.

1.6.2. ЛИЦЕ ЗА КОНТАКТ

Контактното лице за управление на документа Политика за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати от „Система за електронни плащания България/СЕП България“ АД е изпълнителния директор на Доставчика.

Допълнителна информация може да бъде получена на следния адрес:

„Система за електронни плащания България/СЕП България“ АД

София, 1164, р-н Лозенец, ж.к. „Лозенец“

ул. „Златовръх“ № 1

Телефон, 070018283

Email: eSign@sep.bg

1.6.3. ВРЪЗКА МЕЖДУ ПОЛИТИКАТА И ПРАКТИКАТА

Политиката и Практиката си партнират при предоставяне на квалифицирани удостоверения. Потребителите са длъжни да се съобразяват с двата документа при използване на квалифицираните услуги, предлагани от СЕП България.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1.6.4. ЛИЦЕ ЗА КОНТАКТ И ПРОЦЕДУРИ ЗА ОДОБРЕНИЕ НА ПРАКТИКАТА

Лицето, което взема решения относно изпълнение на Практика при предоставяне на квалифицирани удостоверителни услуги (CPS) и отговаря за нейното управление е изпълнителния директор на СЕП България. Практика при предоставяне на квалифицирани удостоверителни услуги (CPS) е разработена от екип на Доставчика и е одобрена от ръководството на СЕП България.

1.7. ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

1.7.1. ОПРЕДЕЛЕНИЯ

Акредитация – Доставчик на удостоверителни услуги може да получи статус „квалифициран“ за определен период в съответствие с Регламент (ЕС) № 910/2014;

Валидиране - Процеса на проверка и потвърждаване на валидността на електронен подпис или печат;

Данни за валидиране - Данни, които се използват за валидиране на електронен подпис или електронен печат;

Данни за идентификация на лица - Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице;

Данни за създаване на електронен подпис - Уникални данни, които се използват от Титуляря на електронния подпис за създаването на електронен подпис;

Данни за създаване на електронен печат - означава уникални данни, които се използват от създателя на електронния печат за създаването на електронен печат;

Доверяваща се страна (Relying Parties) - Физически или юридически лица, както и лица от държавния, обществен и политически сектор, които са адресати на електронни изявления. Доверяващата се страна разчита на електронна идентификация или удостоверителна услуга;

Доставчик на квалифицирани удостоверителни услуги – Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от Органа по надзор;

Електронен печат - Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произходът и целостта на последните. Електронният печат служи като доказателство, че даден електронен документ е издаден от юридическо лице и гарантира надеждния произход и целостта на документа;

Електронен подпис - Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, и които титулярят на електронния подпис използва, за да се подписва;

Електронен документ - означава всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис;

Квалифицирана удостоверителна услуга - Удостоверителна услуга, която отговаря на приложимите изисквания, определени в Регламент (ЕС) №910/2014;

Квалифицирано удостоверение за електронен подпис – Удостоверение за електронни подписи, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в Регламент (ЕС) № 910/2014;

Квалифицирано удостоверение за електронен печат - означава удостоверение за електронен печат, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в Регламент (ЕС) № 910/2014;

Квалифициран електронен подпис - Усъвършенствен електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи;

Квалифициран електронен печат - означава усъвършенствен електронен печат, който е създаден от устройство за създаване на квалифициран електронен печат и се основава на квалифицирано удостоверение за електронен печат;

Координирано универсално време (Coordinated Universal Time/UTC) – Часово време, спрямо което се изчислява времето в различните часови зони. При него за основа се използва международното атомно време (TAI);

Орган за одобрение на Политика (Policy Approval Authority/PAA) – Орган, упълномощен да одобри, наблюдава и поддържа удостоверителната Политика;

Орган за оценяване на съответствието - Орган, който е акредитиран в съответствие със Регламент (ЕО) № 765/2008 като компетентен да извършва оценяване на съответствието на доставчик на квалифицирани удостоверителни услуги и на предоставяните от този доставчик квалифицирани удостоверителни услуги;

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

Практика (CPS) - Практика при предоставяне на квалифицирани удостоверителни услуги е документ, съдържащ правила относно издаване, спиране, възобновяване и отмяна действието на удостоверенията, както и условията за предоставянето на достъп до удостоверенията;

Списък със спрени и прекратени удостоверения (CRL/Certificate Revocation List) – Списъкът съдържа удостоверения, които вече не може да се считат за валидни. CRL е цифрово подписан от издателя на удостоверенията - Удостоверяващия орган;

Създавател на печат - означава юридическо лице, което създава електронен печат;

Частен ключ – Низ от символи, който се използва в алгоритъм за преобразуване на информация от разбираем в шифриран вид (криптиран) или обратно – от шифриран в разбираем вид (декриптиране);

Публичен ключ – Единият от двойка ключове, използван в асиметрична криптосистема, който е достъпен и може да се използва за проверка на електронен подпис/печат;

Титуляр на електронен подпис - Физическо лице, което създава електронен подпис;

Удостоверителна услуга - Електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои във: създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или създаването, проверката и валидирането на удостоверения за автентичност на уебсайт; или съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги;

Удостоверение за електронен печат– означава електронен атестат, който свързва данните за валидиране на електронен печат с юридическо лице и потвърждава името на това лице;

Удостоверение за електронен подпис - Електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице и потвърждава най-малко името или псевдонима на това лице;

Устройство за създаване на квалифициран електронен печат - Устройство за създаване на квалифициран електронен печат, което отговаря на изискванията в Регламент (ЕС) № 910/2014;

Устройство за създаване на квалифициран електронен подпис - Устройство за създаване на квалифициран електронен подпис е устройство за създаване на електронен подпис, което отговаря на изискванията на Регламент (ЕС) № 910/2014;

Устройство за създаване на електронен подпис - Устройство за създаване на електронен подпис е конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис.

Устройство за създаване на електронен печат - означава конфигуриран софтуер или хардуер, който се използва за създаването на електронен печат.

1.7.2. СЪКРАЩЕНИЯ

QCP-I-qscd – Политика на квалифицирано удостоверение, издадено на юридическо лице, когато частния ключ и свързаното с него удостоверение са генерирани на QSCD;

QCP-n-qscd – Политика на квалифицирано удостоверение, издадено на физическо лице, когато частния ключ и свързаното с него удостоверение са генерирани на QSCD;

QSCD – Устройство за създаване на квалифициран електронен подпис/печат;

NCP+ - Засилена нормализирана удостоверителна политика, която включва допълнителни изисквания за квалифицирани удостоверения в съответствие с Регламент (ЕС) № 910/2014

CA Certification Authority- Удостоверяващ орган;

CN Common Name - Публично име;

CP Certificate Policy - Политика за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати;

CPS Certification Practice Statement - Практика при предоставяне на удостоверителни услуги;

CRL, Certificate Revocation List - Списък със спрени и прекратени удостоверения;

DN, Distinguished Name - Отличително име на субект, вписан удостоверението;

Enhanced key usage - Разширени цели за използването на ключа;

FIPS, Federal Information Processing Standard - Федерален стандарт за обработка на информация;

HSM, Hardware Security Module - Хардуерен криптографски модул;

Issuer – Издател;

LDAP, Lightweight Directory Access Protocol - Протокол за опростен достъп до регистър;

OID, Object Identifier - Идентификатор на обект;

PKCS, Public Key Cryptography Standards - Криптографски стандарт за пренос на публичен ключ;

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

PKI, Public Key Infrastructure - Инфраструктура на публичния ключ (съвкупност от хардуера, софтуера, персонала и документацията в СЕП България за създаване, използване, управление и проверка на издавани удостоверения за електронни подписи/печати);

RA, Registration Authority - Регистриращ орган;

RSA, Rivest-Shamir-Adelman - Вид асиметричен криптографски алгоритъм за създаване на електронен подпис;

SHA, Secure Hash Algorithm - Сигурен хеш-алгоритъм за извличане на хеш-идентификатор;

SSL, Secure Socket Layer - Сигурен канал за предаване на данни;

SMIME, Secure Multipurpose Internet Mail Extensions - Протокол за сигурно предаване на електронна поща през Интернет.

2. ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ

2.1. ХРАНИЛИЩЕ

Публичният регистър на СЕП България представлява хранилище, в което са разположени актуални и предишни версии на електронни документи, предназначени за потребителите, удостоверения на удостоверяващите органи, потребителски удостоверения, Списъци със спрени и прекратени удостоверения (CRL) и друга информация.

Хранилището се управлява и контролира от Доставчика.

Всички потребители и доверяващи се страни имат постоянен достъп до цялата информация в хранилището на адрес: <https://www.esign.bg/bg/услуги/публичен-регистър/>.

2.2. ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ СЕП БЪЛГАРИЯ

Информацията, публикувана от СЕП България се състои от следните документи:

1. Списък с оперативни удостоверения за електронни подписи/печати от своята йерархия;
2. Списък на издадените потребителски квалифицирани удостоверения за електронни подписи/печати;
3. Списък на спрени и прекратени удостоверения (CRL);
4. Предишни и актуални версии на документите, регламентиращи дейността на Доставчика;
5. Практика и Политики;
6. Инструкции, описващи начина на използване на електронен подпис/печат;
7. Ценова тарифа за удостоверителните услуги, предоставяни от СЕП България;
8. Друга информация, която може да се променя и модифицира в реално време;
9. Доклади от одити, извършени от упълномощена институция.

За online проверка на данни от регистъра е необходимо използването на подходящ софтуер (OCSP-клиент) или достъп през Интернет-страницата на доставчика.

Проверка на издадени квалифицирани удостоверения може да бъде направена и в Списъка със спрени и прекратени удостоверения (CRL), който се публикува на страницата на Доставчика в интернет и се осъвременява на всеки 3 (три) часа.

2.3. ЧЕСТОТА НА ПУБЛИКУВАНЕ

Документацията, включваща Политика и Практика при предоставяне на квалифицирани удостоверителни услуги, споразумения, образци, ръководства за работа с електронен подпис/печат, доклади от одити и др., издадена от СЕП България, се публикува на страницата на Доставчика в интернет при всяка актуализация.

Оперативните удостоверения на удостоверяващия орган се публикуват веднага след издаване на нови удостоверения.

Актуализация на публичния регистър с издадените потребителски квалифицирани удостоверения се осъществява автоматично след публикуване на новоиздадено валидно удостоверение.

Актуализация на текущия Списък със спрени и прекратени удостоверения (CRL) се осъществява автоматично на не повече от 3 (три) часа.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

2.4. Достъп до публикации

СЕРП България осигурява HTTP/HTTPS и OCSP базиран достъп до информацията в хранилището. Публикуваната информация, е достъпна постоянно (24/7/365), освен в случаите на събития, извън контрола на Доставчика.

3. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ

3.1. ИМЕНА

Имената в удостоверенията са в съответствие с препоръка ITU-T X.509 или IETF RFC 5280 и стандарт ETSI EN 319 412. Допуска се имената да бъдат в съответствие с Domain Name Service (DNS), описан в RFC 2247.

Полето „Subject“ в удостоверението съдържа наименованието на Титуляря/Създателя.

Името и другите индивидуализиращи белези на Титуляря/Създателя в съответните полета за всеки тип удостоверение са в съответствие с DN (Distinguished Name), формиращо се съобразно стандарта X.500 и X.520.

Доставчикът може да издава квалифицирано удостоверение като използва „псевдоним“ за да именува потребителя само след като регистриращия орган събере необходимата информация за самоличността му и успешно го идентифицира.

Имената, включени в Distinguished Name (DN) на потребителя имат своето значение в българския или в друг чужд език. Структурата DN е одобрена от регистриращия орган и зависи от вида на квалифицираното удостоверение и потребителя.

DN се състои от следните области, в съответствие с препоръка RFC 3280 и X.520:

1. C - BG,
2. ST – област,
3. L - град,
4. CU - име на физическото лице или на организацията,
5. O - име на институцията, която лицето представлява,
6. OU - името на организационната единица,
7. E - имейл адрес на абоната,

Титуляр/Създател с уникален DN в домейна на СЕРП България може да има повече от едно издадени действителни квалифицирани удостоверения.

Всяко издадено удостоверение има уникален сериен номер („SerialNumber“) в домейна на Доставчика. Комбинацията на полета „Issuer“ и „SerialNumber“ гарантират уникалността на издаденото удостоверение в публичния домейн.

3.2. ПЪРВОНАЧАЛНА РЕГИСТРАЦИЯ

При първоначално регистриране данните се обработват и записват в процеса на заявяване и приемане на искане за удостоверение. В същото време се прави идентификация и удостоверяване на автентичността на Титуляря/Създателя. Потвърждението на събираните данни изисква личен контакт с представител на регистриращия орган. Тази процедура може да се осъществи отдалечено при наличие на система за отдалечена идентификация.

Искането за регистрация включва следната информация:

1. Пълно наименование на Титуляря/Създателя или на упълномощен представител на юридическото лице;
2. Доказателства за представителна власт на Титуляря спрямо юридическото лице;
3. Идентификатори: ЕИК (персонален идентификационен номер) и др.;
4. Пощенски адрес на лицето (страна, област, пощенски код, град или село, номер на сграда, име на улица или квартал, телефон, номер на факс);
5. Имейл адрес;
6. Вид на исканото квалифицирано удостоверение, имайки предвид предназначението му;
7. Идентификатор на политиката за удостоверяване, въз основа на която се издава удостоверението;
8. Наличие на частен ключ, съответстващ на публичен ключ;
9. Публичен ключ;
10. Допълнителна информация, заявена за включване в удостоверението, както и допустима непотвърдена такава;
11. Подписване на договор за квалифицирани удостоверителни услуги и съгласие с условията на Политиката и Практиката при предоставяне на квалифицирани удостоверителни услуги от СЕРП България.

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

След проверка на предоставените данни и сключен договор за квалифицирана удостоверяваща услуга, лицето подало искане е включено като потребител на услугите на СЕП България.

3.2.1. ПРОВЕРКА ЗА ПРИТЕЖАНИЕ НА ЧАСТЕН КЛЮЧ

СЕП България може да предоставя на Титуляря/Създателя услугата локално или посредством отдалечено генериране на двойката ключове.

За издаване или продължаване на действието на квалифицирано удостоверение е необходимо СЕП България да получи електронно искане във формат PKCS#10. Спецификацията на този формат на искане за издаване на квалифицирано удостоверение изисква искането да бъде подписано от притежателя на частния ключ.

3.2.2. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ

Установяването на идентичността на юридическо лице (Създател), се осъществява от представител на регистрацията орган, чрез проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ.

Юридическите лица трябва да представят следните документи (списък с документи се публикува на сайта):

1. Съдебно решение или друг документ, удостоверяващи възникването на юридическото лице;
2. Документ, удостоверяващ актуалното състояние на лицето;
3. Уникален национален идентификатор.

3.2.3. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ

За издаване на квалифицирано удостоверение на физическо лице (Титуляр), което е упълномощен представител на юридическо лице, пред регистрацията орган се явява упълномощения представител. Физическото лице трябва да представи всички необходими документи за идентификация и удостоверяване на автентичност с цел да се докаже, че по време на разглеждане на заявката юридическото лице съществува и той като представително лице, което кандидатства за квалифицирано удостоверение е получил нотариално заверено разрешение (по образец на СЕП България) от юридическото лице да го представлява.

Удостоверяването на информацията, която се съдържа в представените документи става чрез:

1. Заверка „Вярно с оригинала“ и саморъчен подпис върху документите пред служител на регистрацията орган, в случай на лично предаване на документите;
2. Нотариална заверка на документите, които се изпращат по поща до регистрацията орган;
3. Подписване на приложените електронни формати на документите с валидно удостоверение за квалифициран електронен подпис/печат;

3.2.4. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ

Установяване и проверка на самоличността на физическо лице (Титуляр) се осъществява от представител на регистрацията орган. Идентификацията може да се извърши и автоматизирано, чрез отдалечена проверка.

Физическото лице потвърждава достоверността на данните, чрез (списък с документи се поддържа на сайта на СЕП България):

1. Саморъчно поставен подпис върху документите пред служител на регистрацията орган, в случай на лично предаване на документите;
2. Нотариална заверка на документите, които се изпращат по поща до регистрацията орган;
3. Подписване на приложените електронни документите с валидно удостоверение за квалифициран електронен подпис по смисъла на Регламент (ЕС) № 910/2014;

3.2.5. УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПРАЖНЯВАЩО СВОБОДНА ПРОФЕСИЯ

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

Установяване и проверка на самоличността на физическо лице (Титуляр) упражняващо свободна професия се осъществява от представител на регистриращия орган. Идентификацията може да се извърши и автоматизирано, чрез отдалечена проверка.

Физическото лице потвърждава достоверността на данните, чрез (списък с документи се поддържа на сайта на СЕП България):

1. Саморъчно поставен подпис върху документите пред служител на регистриращия орган, в случай на лично предаване на документите;
2. Нотариална заверка на документите, които се изпращат по поща до регистриращия орган;
3. Подписване на приложените електронни документите с валидно удостоверение за квалифициран електронен подпис по смисъла на Регламент (ЕС) № 910/2014;

3.2.6. ПРОВЕРКА ОТ УДОСТОВЕРЯВАЩИЯ ОРГАН

След успешна идентификация и проверка от регистриращия орган на условията за издаване или управление на квалифицирано удостоверение, представител на регистриращия орган потвърждава данните пред удостоверяващия орган. Удостоверяващият орган публикува незабавно издаденото квалифицирано удостоверение в публичния регистър/хранилището на издадените удостоверения.

3.3. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

СЕП България може да поднови валидно квалифицирано удостоверение, което не е прекратено в срока му на валидност, по два начина:

1. Като запази генерираната двойка ключове за текущото удостоверение (Renewal);
2. Като генерира нова двойка ключове (Re-key).

Удостоверение се подновява за същата двойка ключове (Renewal) на текущото удостоверение на Титуляря/Създателя, ако няма промяна в информацията на текущото удостоверение. Само периодът на валидност в подновеното удостоверение става различен от този в текущото.

СЕП България допуска многократно подновяване на квалифицираното удостоверение като запазва текущата двойка ключове (Renewal), но препоръчва тази практика да се ограничава с цел да се намали риска от компрометиране на частния ключ.

За идентификация и удостоверяване на автентичност на Титуляр/Създател на квалифицирано удостоверение, което се подновява, не се изисква тяхното лично присъствие в регистриращия орган на Доставчика.

При настъпили промени в информацията за Титуляря/Създателя на квалифицирано удостоверение, Доставчикът издава ново квалифицирано удостоверение, като следва първоначална идентификация и удостоверяване на автентичност и прекратява незабавно текущото квалифицирано удостоверение.

3.4. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спиране на валидността на квалифицирано удостоверение води до временна загуба на валидност на дадено удостоверение.

СЕП България спира действието на валидно удостоверение при постъпило искане за спиране, но за не повече от 24 часа. Доставчикът, възобновява автоматично действието на спряно удостоверение след изтичане на 24-часовия срок.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

3.5. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ ПРИ ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Когато СЕП България прекрати действието на квалифицирано удостоверение, той регистрира това в собствената си база данни с квалифицирани удостоверения и публикува отменения статут на удостоверението своевременно, но във всички случаи в срок до 24 часа след като бъде получено искането. Отмяната става валидна веднага след като бъде публикувана. СЕП България прекратява издадено от него удостоверение при:

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1. смърт или поставяне под запрещение на Титуляр/Създател;
2. прекратяване на представителната власт на Титуляря спрямо юридическото лице;
3. установяване на неверни данни при издаване на удостоверението;
4. станала впоследствие невярна удостоверена информация;
5. при промяна в удостоверена вече информация на Титуляр/Създател;
6. компрометиране на частен ключ;
7. забавяне в заплащането на дължимо възнаграждение;
8. искане за прекратяване от страна на Титуляр/Създател, след като Доставчикът се увери в самоличността им и в представителната власт на юридическото лице.

Искане за прекратяване на квалифицирано удостоверение се подава от Титуляр/Създател или упълномощен представител на юридическото лице на място при регистрацията орган или по електронен път.

Услугите по управление на прекратяване и спиране на действието на удостоверение са на разположение денонощно (7/24/365).

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

3.6. ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА АВТЕНТИЧНОСТ СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Политиката и практиката при предоставяне на квалифицирани удостоверителни услуги на СЕП България не допускат подновяване на квалифицирано удостоверение чрез Renewal или Re-key след прекратяването му.

След прекратяване на действието на удостоверение потребителя може да заяви издаване на ново удостоверение и тогава РО изпълнява първоначална идентификация и удостоверяване на автентичност на Титуляря/Създателя.

4. ОПЕРАТИВНИ ИЗИСКВАНИЯ

СЕП България, чрез регистрацията орган, в рамките на сключен договор за квалифицирани удостоверителни услуги, предоставя следните процедури за квалифицирани удостоверителни услуги, приложими към квалифицираните удостоверения за електронни подписи/печати:

1. Регистрация на искане за издаване на квалифицирано удостоверение;
2. Обработка на искане за издаване на квалифицирано удостоверение;
3. Издаване на квалифицирано удостоверение;
4. Предаване на потребител на издаденото квалифицирано удостоверение;
5. Подновяване на квалифицирано удостоверение чрез Renewal;
6. Подновяване на квалифицирано удостоверение чрез Re-key;
7. Спиране/възобновяване действие на квалифицирано удостоверение;
8. Прекратяване на квалифицирано удостоверение;

4.1. УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И ДВОЙКА КЛЮЧОВЕ

4.1.1. ОТ ПОТРЕБИТЕЛИ

Потребителите трябва да използват частните ключове и съответните им квалифицирани удостоверения:

1. В съответствие с тяхното предназначение;
2. Само в рамките на срока на тяхната валидност;
3. Когато удостоверението е спряно, потребителят не трябва да използва частния ключ, особено за създаване на електронен подпис/печат.

Отговорността за използването на частния ключ е на потребителя.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

4.1.2. ОТ ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяващите се страни, трябва да използват публичните ключове и съответните им удостоверения:

1. В съответствие с тяхното предназначение;
2. Само след проверка на техния статус и проверка на електронния подпис на удостоверяващия орган, издал удостоверението;
3. До отмяна валидността на даден ключ;

Когато удостоверението е спряно, доверяващата се страна не трябва да приема публичния ключ.

4.2. ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ (RENEWAL)

Подновяване на квалифицирано удостоверение с Renewal означава подмяна на валидно удостоверение с ново, без да се променя съществуващата информация в него, освен нов сериен номер и нов срок на валидност.

Подновяване се извършва само в рамките на срока на валидност на актуално удостоверение. То трябва да бъде предшествано от регистриране на искане за подновяване в подходяща форма, приета и одобрена от оператор в регистриращ орган, проверена идентичност и коректност на подаденото искане.

4.3. ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (RE-KEY)

СЕП България генерира нова двойка ключове, в случаите когато вече регистриран потребител поиска да му се генерира нова двойка ключове или нов потребител подаде искане за генериране на двойка ключове. Генерирането на нова двойка ключове се съпътства с издаване на ново квалифицирано удостоверение, потвърждаващо притежанието на новосъздадената ключова двойка.

СЕП България информира предварително потребителите си по имейл най-малко 14 дни преди изтичане срока на валидност на издадено удостоверение, когато това е възможно.

Искането за подновяване на квалифицирано удостоверение, чрез електронна заявка се удостоверява с електронен подпис/печат, съответстващ на валидно удостоверение на Титуляр/Създател или упълномощен представител на юридическото лице.

В случай, че удостоверението, което се подновява е с изтекъл срок на валидност, Титулярят/Създателят или упълномощеното от него лице трябва да посети лично регистриращия орган на Доставчика.

4.4. ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Промяна в квалифицирано удостоверение означава промяна в съдържанието на данните във вече издадено и публикувано квалифицирано удостоверение за електронен подпис/печат. При промяна в квалифицирано удостоверение се изисква задължително генериране на нова двойка ключове.

Промяната се третира по същия начин, както и издаването на ново квалифицирано удостоверение.

4.5. СПИРАНЕ И ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спирането води до временно спиране на действието на удостоверението. Прекратяването води до необратимо спиране на действието на удостоверението.

Спирането или прекратяването стават валидни веднага след като удостоверението бъде публикувано в CRL.

Услугите по управление на прекратяване и спиране на действието на квалифицирано удостоверение са на постоянно разположение (7/24/365).

4.5.1. ОБСТОЯТЕЛСТВА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

СЕП България прекратява издадено от него квалифицирано удостоверение, ако се появи следната ситуация:

1. Когато информацията, вписана в удостоверението се е променила;

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

2. Когато има подозрение, че частният ключ е компрометиран;
3. Потребителят реши да прекрати договора със СЕП България;
4. Смърт или поставяне под запрещение на Титуляря/Създателя;
5. Прекратяване на представителната власт на Титуляря спрямо юридическото лице;
6. Когато потребителят не отговаря на изискванията на Политиката за удостоверяване;
7. Ако удостоверяващия орган прекрати дейността си;
8. Ако потребителят дължи неизплатени такси за предоставяни квалифицирани удостоверителни услуги;
9. Когато надеждността и сигурността на частния ключ на удостоверяващия орган е нарушена;
10. Когато потребител, който е служител на една организация прекрати договора си за работа и не върне използваната криптографска карта, на която се съхранява удостоверението и съответния частен ключ.

4.5.2. ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.5.2.1. ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КРАЕН ПОТРЕБИТЕЛ

Прекратяване действието на квалифицирано удостоверение на краен потребител се предхожда от подаване на искане за прекратяване пред регистриращия орган на СЕП България. Искането за прекратяване на удостоверение може да се регистрира електронно, само когато Титуляря/Създателя има (друго) валидно и достъпно за ползване квалифицирано удостоверение за електронен подпис/печат. В противен случай се прави искане на място пред оторизиран оператор на регистриращия орган.

Всяко искане за прекратяване на удостоверение трябва да съдържа неоспорими доказателства за потвърждение на прекратяването. Всички мотиви за прекратяване трябва да са заверени (подписани по електронен път или подписани на ръка).

Процедурата за прекратяване на квалифицирано удостоверение се извършва, както следва:

1. Оторизираният оператор в регистриращия орган незабавно, без да идентифицира потребителя, спира действието на удостоверението за не повече от 24 часа;
2. Регистриращият орган строго следва изискванията за идентификация и установяване на автентичност на Титуляря/Създателя или упълномощен представител на юридическото лице и причините за прекратяване. Във всички случаи Титулярят/Създателят или упълномощеният представител на юридическото лице трябва да посети лично регистриращия орган на СЕП България за последваща проверка на идентичността, респективно самоличността на потребителя;
3. След успешно удостоверяване на автентичността на Титулярят/Създателят или на упълномощеният представител на юридическото лице регистриращия орган, чрез оторизирания оператор подава обработена заявка до оперативния удостоверяващ орган за прекратяване на удостоверението. След потвърждение удостоверяващия орган прекратява удостоверението;
4. При неуспешна идентификация и проверка на условията за прекратяване, регистриращият орган отхвърля искането за прекратяване на удостоверението и незабавно известява Титулярят/Създателят или упълномощеният представител на юридическото лице за причините за това;
5. Потребител с отхвърлено искане за прекратяване на квалифицирано удостоверение, може да подаде ново искане за прекратяване на удостоверението след като отстрани посочените причини за отказа;
6. След прекратяване на удостоверението, Доставчикът, чрез своя удостоверяващ орган, незабавно публикува прекратеното удостоверение в Списъка със спрени и прекратени удостоверения (CRL), като издава нов Списък;
7. След прекратяване на квалифицираното удостоверение, Доставчикът уведомява Титуляря/Създателя на прекратеното удостоверение.

Прекратено удостоверение на Титуляря/Създателя не подлежи на възобновяване или на подновяване.

4.5.3. ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Преди да прекрати действието на валидно квалифицирано удостоверение Доставчикът спира действието на удостоверението за максимум 24 часа гратисен период. В рамките на този период Доставчикът обработва искането за прекратяване на квалифицираното удостоверение.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

4.5.4. ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ

СЕП България осигурява квалифицирана услуга за проверка на състоянието на издадените удостоверения в реално време. Тази услуга се извършва въз основа на Протокол за онлайн проверка на статуса на удостоверение (OCSP), описан в RFC 2560.

OCSP услугата генерира отговор, основан на база данни. OCSP отговора е валиден в продължение на 7 дни. За да се поддържа правилното изпълнение на системата, отговорите на OCSP са кеширани за предварително определено време (обикновено не повече от няколко часа).

Проверка на статус на удостоверение в реално време може да се изпълни през интернет: <http://www.esign.bg/bg/услуги/валидация-на-удостоверения/>.

4.5.5. ОБСТОЯТЕЛСТВА ЗА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

СЕП България, чрез своя оперативен удостоверяващ орган (eSIGN SEP QES CA), спира действието на валидно удостоверение при определени условия и за срок до 24 часа.

Доставчикът предприема незабавни действия по искането за спиране на удостоверение.

За времето, през което удостоверението е спряно, то се счита за невалидно и всички електронни подписи/печати, проверявани с това удостоверение са недействителни.

4.5.6. ПРОЦЕДУРА ЗА СПИРАНЕ И ВЪЗБНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спиране действието на квалифицирано удостоверение се предхожда от регистриране на искане за спиране пред регистриращия орган.

1. Искането за спиране на удостоверение може да се регистрира по електронен път или да се подаде на хартия пред оторизиран оператор на регистриращия орган на СЕП България.
2. Искането за спиране на удостоверение, по електронен път се удостоверява с електронен подпис/печат, съответстващ на валидно удостоверение на Титуляря/Създателя.
3. Оторизираният оператор в регистриращия орган незабавно, без да идентифицира потребителя, спира действието на квалифицираното удостоверение.
4. Регистриращият орган не може да отхвърля искане за спиране.
5. След спиране на удостоверение, Доставчикът, чрез своя оперативен удостоверяващ орган незабавно публикува спряното удостоверение в Списъка на спрени и прекратени удостоверения (CRL), чрез издаване на нов Списък.
6. След спиране на удостоверение, Доставчикът незабавно уведомява Титуляря/Създателя на спряното квалифицирано удостоверение.

4.5.7. ГРАТИСЕН ПЕРИОД НА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

СЕП България спира действието на квалифицирано удостоверение за електронен подпис/печат за период до 24 часа.

4.5.8. ВЪЗБНОВЯВАНЕ ДЕЙСТВИЕТО НА СПРЯНО УДОСТОВЕРЕНИЕ

СЕП България възобновява действието на спряно удостоверение:

1. До 24 часа след неговото спиране;
2. След като изтече срока за спиране (24 часа) и не е постъпило искане за възобновяване;
3. След като отпадне основанието за спиране, преди да изтече периода на спиране;
4. По искане на потребителя, след изясняване на причините за поисканото спиране;

След възобновяване на удостоверение, последното се счита за действително.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

4.6. ПРОВЕРКА НА АКТУАЛНОТО СЪСТОЯНИЕ (СТАТУС) НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Информация за състоянието на удостоверения, издадени от СЕП България може да бъде получена в Списъка със спрени и прекратени удостоверения (CRL), публикуван на сайта на СЕП България в интернет и чрез Протокола за онлайн проверка на статуса на удостоверенията (OCSP).

Удостоверителните услуги за проверка на статуса на квалифицираните удостоверения са достъпни в режим 24/7/365 (непрекъснато действащи).

4.7. ПРЕКРАТЯВАНЕ НА ДОГОВОР ЗА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ ПОТРЕБИТЕЛ

Договорът за квалифицирани удостоверителни услуги между СЕП България и потребител се прекратява:

1. След изтичане на срока на валидност на последното издадено квалифицирано удостоверение и потребителят не е предприел действия, за да актуализира своето квалифицирано удостоверение;
2. Когато квалифицираното удостоверение е било прекратено и потребителя не е предприел действия по издаване на друго удостоверение.

5. КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ

5.1. КОНТРОЛ НА ФИЗИЧЕСКАТА СИГУРНОСТ

Мерките предприети по отношение на физическата защита на Доставчика са елемент от разработената и внедрена в СЕП България Система за информационна сигурност, съответстваща на изискванията на стандарта ISO/IEC 27001:2013 и ISO/IEC 19011:2011.

Мерките свързани с физическата защита на информационните данни, технологичните системи, помещенията и свързаните с тях поддържащи системи са насочени към предотвратяване на:

1. Неразрешен достъп, нанасяне на щети и намеса в условията на работа;
2. Загуба, вреди или компрометиране на ресурси;
3. Компрометиране или кражба на информация или средства за обработка на информацията.

Инфраструктурата на доставчика е физически и логически обособена и не се използва при други дейности, които СЕП България осъществява.

5.1.1. ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА

СЕП България разполага със специално конструирано и оборудвано помещение с най-висока степен на контрол на физически достъп, в което се помещават удостоверяващите органи на Доставчика и всичките основни компоненти на инфраструктурата.

5.1.2. ФИЗИЧЕСКИ ДОСТЪП

Физическата сигурност на системите за издаване и управление на удостоверения е съобразена с изискванията на международни стандарти и препоръки.

За оборудването в защитеното помещение на Доставчика е осигурена физическа неприкосновеност. Има двуфакторен контрол на достъпа и денонощна физическа охрана. Всеки достъп до помещенията с критична инфраструктура се документира в специални журналы.

Защитата на сградата на СЕП България е реализирана от невъоръжена 24-часова охрана. В помещенията на Доставчика има Система за алармена сигнализация, Система за видеонаблюдение, Сигнално-известителна система и Система за контрол на достъпа.

Офисът на регистриращия орган в сградата на СЕП България е обособен и отделен от останалите помещения. Съоръжен е с техника, позволяваща безопасно съхранение на данни и документи. Достъпът до него се следи и ограничава единствено до оторизирани лица, свързани с дейността на регистриращия орган.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

5.1.3. СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ

Всички носители съдържащи софтуер, архиви на данни или одитна информация се съхраняват в огнеупорна каса в специално архивно помещение с въведен контрол на достъп. В помещението с архива на Доставчика има изградена система на физическа и логическа защита.

5.1.4. ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИ

Хартиените и електронни носители, съдържащи евентуално значима информация за сигурността на СЕП България, след изтичане на определения съгласно вътрешните правила период на съхранение, се унищожават в специални устройства за нарязване.

Носителите на информация за криптографските ключове и ПИН/ПУК номера, използвани за тяхното съхранение, се раздробяват с подходящи устройства. Това се отнася за носителите, които не позволяват окончателно заличаване на съхранени данни и тяхното повторно използване.

В определени случаи, информацията от преносими носители се унищожават, чрез изтриване или форматиране на устройството без възможност за възстановяване.

5.2. ОРГАНИЗАЦИОНЕН КОНТРОЛ

Процедурите при издаване и управление на квалифицирани удостоверения се изпълняват от доверен персонал на СЕП България.

Доставчикът поддържа достатъчен брой квалифицирани служители, които във всеки момент от осъществяване на дейността му осигуряват съответствие с действащото законодателство и вътрешните процедури на дружеството.

5.2.1. ДОВЕРЕНИ РОЛИ

Подробно разпределение на функциите и отговорностите на персонала е разписано във вътрешните документи на СЕП България: длъжностни характеристики, щатно разписание и съответни вътрешни оперативни процедури.

Разпределянето на функциите се осъществява по такъв начин, че да бъде сведена до възможен минимум опасността от компрометиране, изтичане на конфиденциална информация или възникване на конфликт на интереси.

5.2.2. ИЗИСКВАНИЯ ЗА РАЗДЕЛЯНЕ НА ОТГОВОРНОСТИТЕ

Доверените дейности на персонала на Доставчика се изпълняват от различни лица.

5.3. КОНТРОЛ НА ПЕРСОНАЛА

Персоналът на СЕП България се състои от достатъчен брой високо квалифицирани служители. Лицата, извършващи доверени роли имат необходимата професионална подготовка и опит, което гарантира спазване на изискванията за сигурност и технически норми за оценка на сигурността. При избора на служители се взима предвид професионалния им опит в областта на информационните системи, криптографията и инфраструктурата на публичните ключове.

Служителите на СЕП България преминават периодично през курсове за последващо допълнително обучение, отговарящо на съвременните изисквания в областите на дейност на Доставчика.

5.3.1. ИЗИСКВАНИЯ ЗА ОБУЧЕНИЕ НА ПЕРСОНАЛА НА СЕП БЪЛГАРИЯ

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

Персоналът, който изпълнява функциите и задачите, произтичащи от неговата заетост в СЕП България или заетост в регистриращия орган (вкл. при наличие на външен регистриращ орган) трябва да премине през следните обучения:

1. Практика при предоставяне на квалифицирани удостоверителни услуги от „Система за електронни плащания България/СЕП България“ АД;
2. Политика за издаване на квалифицирани удостоверения за квалифицирани електронни подписи/печати от „Система за електронни плащания България/СЕП България“ АД;
3. Разпоредби, процедури и документация, свързана със заеманата роля;
4. Технологии за сигурност и процедури свързани със сигурността, използвани от удостоверяващия и регистриращ органи;
5. Системен софтуер на удостоверяващия орган и регистриращия орган;
6. Отговорности, произтичащи от роли и задачи, изпълнявани в системата;
7. Процедури, изпълнявани при отказ на системата или прекъсване на дейностите на удостоверяващия орган.

5.4. ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ

За ефективно управление и функциониране на СЕП България, всички събития, имащи съществено значение върху сигурността и надеждността на технологичната система, контрола върху персонала и потребителите, и въздействието върху сигурността на предоставяните квалифицирани удостоверителни услуги се записват.

Информацията за електронните журнали се генерира автоматично.

Журнали на записи на регистрирани събития се съхраняват във файлове на системния диск за най-малко 6 (шест) месеца. През това време те са достъпни онлайн или в процес на търсене от всеки оторизиран служител на СЕП България. След този период, записите се съхраняват в архивите.

Архивирани журнали се запазват в продължение на 10 (десет) години.

Архивът се подписва с електронен подпис. Информацията от записите в логовете периодично се записва на физически носители, които се съхраняват в специален сейф, намиращ се в помещение с висока степен на физическа защита и контрол на достъпа.

5.4.1. УЯЗВИМОСТ И ОЦЕНКА

СЕП България класифицира и поддържа регистри на всички активи в съответствие с изискванията на ISO/IEC 27001:20013. Съгласно „Политиката по сигурност“ на СЕП България се извършва анализ за оценката на уязвимост по всички вътрешни процедури, приложения и информационни системи. Изискванията за анализ могат, също така, да бъдат определени от външна институция, упълномощена да извършва одит на СЕП България.

Анализът на риска се извършва най-малко веднъж годишно.

5.5. АРХИВИРАНЕ

Данните се архивират на различни нива според следния времеви график:

1. База данни с потребителските удостоверения и данните на Титуляра/Създателя се съхраняват на сървърите на СЕП България до 10 (десет) години от момента на издаване на удостоверението или последното действие по неговото управление, след което се архивира на оптичен носител без възможност за добавяне или изтриване на записи;
2. Носителите с данните се предават в документален архив за съхранение.

Информацията за значимите събития се архивира в електронен вид периодично.

5.6. ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

5.6.1. ИЗИСКВАНИЯ, СВЪРЗАНИ С ПРЕХОДА ДО ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

Преди Доставчика да прекрати дейността си, той е длъжен да:

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

1. Уведоми надзорния орган за своето намерение да прекрати услугите си, в случай на иск за обявяване на дружеството в несъстоятелност, обявяване на дружеството за недействително или за друго искане за прекратяване, или за започване на процедура по ликвидация. Уведомлението следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;
2. Уведоми (най-малко 4 месеца преди това) своите потребители за решението да прекрати предоставяните от него услуги;
3. Промени статуса на оперативните удостоверения;
4. Прекрати всички удостоверения на потребителите в рамките на обявения период за прекратяване на дейността;
5. Уведоми всички свои потребители за преустановяване на услугите;
6. Прави търговски разумни усилия, за да сведе до минимум нарушаването на интересите на потребителите;
7. Изплаща компенсация на потребителите (компенсациите трябва да бъдат пропорционални на оставащия период на валидност на удостоверенията);
8. Извършва необходимите действия, за да може надзорния орган да поддържа Списъка със спрени и прекратени удостоверения (CRL).

Ако решението за прекратяване на удостоверителните услуги се отнася само до регистриращия орган, той е длъжен да:

1. Уведоми СЕП България за своето намерение да прекрати дейността по регистрация. Уведомлението следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;
2. Предава на Доставчика цялостната документация, свързана с потребителите, включително архива и данните за одит.

5.6.2. ПРЕХВЪРЛЯНЕ НА ДЕЙНОСТ КЪМ ДРУГ РЕГИСТРИРАН ДОСТАВЧИК НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

При прехвърляне на дейност на квалифициран доставчик към друг квалифициран доставчик първия трябва да подпише споразумение, в което да положи всички усилия за да осигури непрекъснатост на издаване на квалифицирани удостоверителни услуги за потребителите. В този случай, Доставчикът трябва да:

1. Уведоми надзорния орган за намерението си, не по-късно от 4 месеца преди датата на прекратяване и прехвърляне на дейността;
2. Полага всички усилия и грижи, за да продължи действието на издадените потребителски удостоверения;
3. Уведоми писмено надзорния орган и потребителите, че дейността му се поема от друг регистриран доставчик, както и относно името му. Уведомлението се публикува в интернет страницата на Доставчика;
4. Уведоми потребителите относно условията по поддръжка на прехвърлените удостоверения към приемащия Доставчик;
5. Промени статуса на оперативните удостоверения и надлежно предаде цялата документация, свързана с дейността си на приемащия Доставчик, заедно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени);
6. Извърши необходимите действия за прехвърляне на задълженията по поддръжка на информацията към приемащия Доставчик;
7. Прехвърли управлението на вече издадените удостоверения за крайни потребители към приемащия Доставчик;

Приемащият Доставчик поема правата и задълженията на Доставчика с прекратена дейност и продължава да управлява активните квалифицирани удостоверения до края на тяхното действие.

Архивът на Доставчика с прекратен статус трябва да бъде предаден на Доставчика приел дейността.

5.7. ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ДОСТАВЧИК ИЛИ НА КВАЛИФИЦИРАН СТАТУТ НА УДОСТОВЕРИТЕЛНА УСЛУГА

При отмяна на квалифицирания статут на Доставчика или на някоя от предоставяните от него удостоверителни услуги, Доставчикът извършва следното:

1. Уведомява потребителите си за променения статут на своите услуги;
2. Промени статуса на своите удостоверения;
3. Прекратява всички квалифицирани удостоверения на потребителите си в момента от влизане в сила на променения статут;
4. Прави търговски разумни усилия, за да се сведе до минимум нарушаването на интересите на потребителите;

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

5. Изплаща компенсации на потребителите, пропорционални на оставащия период на валидност на удостоверенията;

6. УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

6.1. ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА УДОСТОВЕРЯВАЩ ОРГАН

Доставчикът генерира двойки криптографски (RSA) ключове на базовия и на оперативния удостоверяващи органи като използва хардуерна криптосистема (HSM/Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо.

Доставчикът използва своите частни ключове само за целите на дейността си, както следва:

- Да подписва издаваните оперативни удостоверения на удостоверяващите органи в своята инфраструктура;
- Да подписва издаваните и публикувани Списъци със спрени и прекратени удостоверения (CRL);
- Да подписва всички издадени и публикувани квалифицирани удостоверения за електронен подпис/печат на потребителите.

6.1.1. ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ПОТРЕБИТЕЛ

Двойката ключове на Титуляр/Създател на квалифицирано удостоверение за електронен подпис/печат се генерира само в одобрено от Доставчика устройство за създаване на квалифициран електронен подпис/печат (QSCD), проверено за ниво на сигурност и за успешна работа през интерфейсите на инфраструктурата на СЕП България.

Титулярят/Създателят се задължава да използва лицензиран софтуер за работа с устройство за създаване на квалифициран електронен подпис/печат (QSCD).

6.1.1.1. ИЗИСКВАНИЯ КЪМ УСТРОЙСТВОТА ЗА СЪЗДАВАНЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ (QSCD)

Устройствата за създаване на квалифициран електронен подпис/печат гарантират, чрез подходящи технически и процедурни средства, най-малко че:

1. Поверителността на данните за създаване на електронен подпис/печат, използвани за създаването на електронния подпис/печат, е разумно гарантирана;
2. Данните за създаване на електронен подпис/печат на практика се срещат само веднъж;
3. Данните за създаване на електронен подпис/печат са обезпечени в достатъчна степен и не могат да бъдат извлечени, а електронният подпис/печат е надеждно защитен срещу подправяне, чрез използване на наличната към момента технология;
4. Данните за създаване на електронен подпис могат да бъдат надеждно защитени от законния Титуляр/Създател на електронния подпис/печат срещу използване от други лица.

Устройствата за създаване на квалифициран електронен подпис/печат не изменят данните, които ще бъдат подписвани, и не пречат за представянето им на Титуляря/Създателя на електронния подпис/печат преди подписване.

Генерирането или управлението на данни за създаване на електронен подпис/печат от името на Титуляря на електронния подпис/печат може да се извърши единствено от Доставчика.

6.1.2. ДОСТАВКА НА ЧАСТЕН КЛЮЧ НА ПОТРЕБИТЕЛ

След генериране на двойката ключове потребителя получава частния ключ и издаденото квалифицирано удостоверение върху устройство за създаване на квалифициран електронен подпис/печат (QSCD) в регистриращия орган на Доставчика. Началният потребителски и административен код за достъп и за деблокиране на устройството се предоставят на Титуляря/Създателя или на упълномощения представител на юридическото лице в запечатан, непрозрачен хартиен плик.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

6.1.3. ПРЕДОСТАВЯНЕ НА ПУБЛИЧЕН КЛЮЧ ОТ ПОТРЕБИТЕЛ НА ДОСТАВЧИК

Публичния ключ от двойката се предоставя за удостоверяване от удостоверяващия орган. Това става като се спазва изискванията посочени в PKCS#10 Certification Request Syntax.

Регистриращият орган на Доставчика задължително прави проверка на държането на частния ключ от потребителя и потвърждава искането за квалифицирано удостоверение.

6.1.4. ДЪЛЖИНА НА КЛЮЧОВЕ

Дължината на използваните ключове е както следва:

eSign Sep Root CA	4096 bits
eSign Sep QES CA	4096 bits
eSign Sep OCSP	2048 bits
eSign Sep TSA	2048 bits
eSign QES Natural	2048 bits
eSign QES Delegated	2048 bits
eSign QES Seal	2048 bits

6.1.5. ПАРАМЕТРИ НА ПУБЛИЧЕН КЛЮЧ

Параметрите на публичния ключ са посочени в удостоверението, което Доставчикът издава за този публичен ключ, съответстващ на частния ключ, който е генериран и записан в устройство за създаване на електронен подпис/печат.

Използваната среда за генериране и съхраняване на частните ключове на основните компоненти в инфраструктурата на СЕП България е криптомодул (HSM) с удостоверено ниво на сигурност FIPS 140-2 Level 3 и CC EAL 4+.

Устройствата за създаване на квалифициран електронен подпис/печат и осигурената среда за генериране и съхраняване на ключовете на потребителя са с ниво на сигурност CC EAL 4+ и FIPS 140-2 Level 3.

6.2. ЗАЩИТА НА ЧАСТЕН КЛЮЧ И КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ

Частните ключове на удостоверяващия орган на СЕП България се съхраняват в сигурни криптографски модули, удовлетворяващи нормативните изисквания на Регламент (ЕС) № 910/2014.

6.2.1. КОНТРОЛ НА ИЗПОЛЗВАНЕ И СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на Доставчика и потребителите се генерират, съхраняват и използват посредством устройства за сигурно създаване на електронен подпис/печат (SSCD). Хардуерните криптографски модули, които използва СЕП България са в съответствие с изискванията на Регламент (ЕС) № 910/2014, като създаването, съхраняването и използването на частния ключ на Доставчика се извършват в система със защитен профил, определен в съответствие с общите изисквания (CC), ниво на сигурност EAL 4 или по-високо съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността.

СЕП България издава удостоверения и удостоверява предоставени от потребителя публични ключове, ако ключовата двойка е генерирана чрез SSCD с ниво на сигурност EAL 3 или по-високо.

Доставчикът по никакъв начин не съхранява и не архивира частен ключ на потребител.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

6.2.2. СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ

Доставчикът не създава копия на частните ключове на потребителите. Частният ключ на Титуляря/Създателя или на упълномощения представител на юридическото лице се съхранява само на устройство за създаване на квалифициран електронен подпис/печат (QSCD) и не може да се възпроизведе на друго устройство. При дефектиране на устройството за създаване на квалифициран електронен подпис/печат (QSCD), потребителят трябва да го подмени и да поиска издаване на ново квалифицирано удостоверение.

6.2.3. МЕТОД ЗА АКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на СЕП България се активират след трансфер на всички поделени секретни части в криптомодула и въвеждане на ПИН или код за активиране от всеки държател на поделена част. Активирането се извършва най-малко от двама надлежно овластени служители на доверени позиции.

Частният ключ на потребител се активира, чрез въвеждане на потребителския код за достъп до мястото, където защитено се съхранява ключа.

6.2.4. МЕТОД ЗА ДЕАКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на СЕП България се деактивират като се стартира процедура по инициализация на криптомодула. Деактивирането се извършва най-малко от двама надлежно овластени служители на доверени позиции.

Частен ключ на потребител се деактивира посредством преустановяване на логическия достъп до устройството за създаване на квалифициран електронен подпис/печат (QSCD) или чрез физическо му унищожаване.

6.2.5. МЕТОД ЗА УНИЩОЖАВАНЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на СЕП България в криптомодула се унищожават, като се стартира процедура по инициализация на криптомодула и последваща процедура за унищожаване на всички поделени части. Процедурата се извършва най-малко от двама надлежно овластени служители на доверени позиции.

Частният ключ на потребител се унищожаване посредством изтриването му от устройството за създаване на квалифициран електронен подпис/печат (QSCD) или чрез физическото унищожаване на устройството.

6.3. ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕ НА ДВОЙКА КЛЮЧОВЕ

6.3.1. АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ

СЕП България не поддържа архив на частни ключове след изтичане на жизнения им цикъл. Всички частни ключове в края на своя жизнен цикъл се унищожават по такъв начин, че да се предотврати тяхното използване

6.3.2. ПЕРИОД НА ВАЛИДНОСТ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И УПОТРЕБА НА КЛЮЧОВЕ

Периода на употреба на публични ключове се определя от стойността на полето в удостоверението му, описващо валидността на публичния ключ. Валидността на удостоверенията и съответните им частни ключове могат да бъдат съкратени, в случай на прекратяване на удостоверенията.

Максимален период на валидност на удостоверенията:

Удостоверение	Период на валидност
eSign Sep Root CA	20 години

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

eSign Sep QES CA	10 години
eSign Sep OCSP	10 години
eSign Sep TSA	3 години
eSign QES Natural	3 години
eSign QES Delegated	3 години
eSign QESeal	3 години

6.4. ДАННИ ЗА АКТИВИРАНЕ

Данните за активиране на ключови двойки на удостоверяващите органи, ПИН и/или пароли и кодове на СЕП България са разделени на защитени части и се държат от различни служители на доверени позиции. СЕП България следва специална процедура по събирането и използването на данните за активиране, която гарантира защита от неправомерно и неоторизирано ползване на ключовите двойки. Всяка поделена част е защитена с отделен ПИН и/или парола или код. Данните за активиране се генерират по защитен и сигурен начин.

Данните за активиране на достъпа до частния ключ на потребителите на Доставчика се генерират по време на процедурата по издаване на квалифицирано удостоверение, когато услугата по издаване е свързана с предоставяне на SSCD на потребителя.

Данните за достъп до потребителското устройство (PIN/PUK кодове) се предава в запечатан плик или по друг сигурен и надежден начин, осигуряващ невъзможност за тяхното компрометиране.

6.4.1. ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДАННИ ЗА АКТИВИРАНЕ

Данни за активиране се използват при първоначално издаване на удостоверение, върху устройство за създаване на квалифициран електронен подпис/печат (QSCD), преди генериране на двойка ключове. В този случай устройството се инициализира и се създават кодове за достъп: потребителски („User“) и административен („SO“). Тези кодове позволяват персонален достъп до частния ключ в устройството и при необходимост за деблокиране на същото.

Кодовете за достъп и за деблокиране на устройството за създаване на квалифициран електронен подпис/печат (QSCD) се предоставят на потребителя в запечатан, непрозрачен хартиен плик.

6.4.2. ЗАЩИТА НА ДАННИ ЗА АКТИВИРАНЕ

Потребителят е задължен да съхранява и пази от компрометиране кодовете за достъп до устройството за създаване на квалифициран електронен подпис/печат (QSCD).

6.5. СИГУРНОСТ НА КОМПЮТЪРНИТЕ СИСТЕМИ

СЕП България използва единствено надежден и сигурен хардуер и софтуер, които са част от компютърната система на Доставчика.

Компютърните системи, на които работят всички критични компоненти от инфраструктурата на СЕП България, са оборудвани и конфигурирани със средства за локална защита на достъпа до софтуера и информационните данни.

Доставчикът използва процедури за управление на информационната сигурност на цялата инфраструктура на СЕП България в съответствие с общоприети в международната практика стандарти.

6.6. СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА

Всички хардуерни промени се наблюдават и регистрират от оторизирани служители на Доставчика. При закупуване на ново техническо оборудване, то се доставя с необходимите процедури за експлоатация и инструкции за ползване.

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

Управлението на контролите на функционалността на технологичната система гарантира, че тя функционира правилно и в съответствие с доставената производствена конфигурация.

6.7. МРЕЖОВА СИГУРНОСТ

В инфраструктурата на СЕП България се използват съвременни технически средства за обмен и защита на информация, за да се гарантира мрежовата сигурност на системите срещу външни интервенции и заплахи.

7. ПРОФИЛИ НА УДОСТОВЕРЕНИЯ

Профилите на удостоверенията за електронен подпис/печат и Списъка със спрени и прекратени удостоверения са дефинирани в съответствие с RFC 3280 и ITU-T X.509 v.3. Профилът за OCSP е в съответствие с RFC 2560.

7.1. ПРОФИЛИ НА УДОСТОВЕРЕНИЯ НА ДОСТАВЧИКА

7.1.1. ПРОФИЛ НА БАЗОВО УДОСТОВЕРЕНИЕ НА УДОСТОВЕРЯВАЩ ОРГАН (eSIGN SEP ROOT CA)

eSign Sep Root CA		
Version	V3	
Signature algorithm	sha256RSA	
Signature hash algorithm	sha256	
Issuer	CN	eSign Sep Root CA
	OU	SEP Bulgaria JSC Qualified Root Authority
	2.5.4.97 (organizationIdentifier)	NTRBG-131107204
	O	SEP Bulgaria JSC
	C	BG
Validity	20 years	
Subject	CN	eSign Sep Root CA
	OU	SEP Bulgaria JSC Qualified Root Authority
	2.5.4.97 (organizationIdentifier)	NTRBG-131107204
	O	Sep Bulgaria JSC
	C	BG
Public key	RSA 4096 bits	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/	
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=No	
Key Usage(Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Friendly name	eSign Sep Root CA	

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

7.1.2. ПРОФИЛ НА УДОСТОВЕРЕНИЕ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН (eSIGN SEP QES CA)

eSign Sep QES CA		
Version	V3	
Signature algorithm	sha256RSA	
Signature hash algorithm	sha256	
Issuer	CN	eSign Sep Root CA
	OU	SEP Bulgaria JSC Qualified Root Authority
	2.5.4.97 (organizationIdentifier)	NTRBG-131107204
	O	SEP Bulgaria JSC
	C	BG
Validity	20 years	
Subject	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
Public key	RSA 4096 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=https://www.esign.bg/bg/services/public-register/eSign_Sep_Root_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 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/	
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSignSepRootCA.crl	
Basic Constraints (Critical)	Subject Type=CA Path Length Constraint=None	
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Friendly name	eSign Sep QES CA	

7.1.3. ПРОФИЛ НА УДОСТОВЕРЕНИЕТО ЗА ОНЛАЙН ВАЛИДИРАНЕ (eSIGN OCSP)

eSign Sep OCSP		
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

 <p>electronic signature</p>	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

	O	SEP Bulgaria JSC
	C	BG
Validity	5 years	
Subject	CN	Common Name
	O	Organization
	L	Locality
	C	Country
Public key	RSA 2048 bits	
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3.1.1 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)	OCSP Signing (1.3.6.1.5.5.7.3.9)	

7.1.4.ПРОФИЛ НА СПИСЪКЪТ СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)

поле	Стойност, подполе	
version	Version 2	
issuer (Distinguished Name)	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	{eSign Sep Root CA, eSign Sep QES CA}
	Street	1 Zlatovrah Str.
	E	eSign@sep.bg
thisUpdate	Дата на издаване на Списъка на прекратените удостоверения	
nextUpdate	Дата на издаване на следващ Списък на прекратените удостоверения	
signature	Електронен подпис на издателя на Списъка на прекратените удостоверения	
CRLNumber	Число от монотонно нарастваща редица	
AuthorityKeyIdentifier		
revokedCertificates	userCertificate	Serial number

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

	revocationDate	Дата на поставяне в Списъка на прекратените удостоверения
	crlEntryExtensions	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

7.2. ПОТРЕБИТЕЛСКИ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

7.2.1. ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ (eSIGN QES NATURAL):

eSign QES Natural		
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	3 years	
Subject	Pseudonym (2.5.4.65)	Pseudonym
	*E	Email
	*CN	Common Name
	*SERIALNUMBER	Уникален идентификатор за физическото лице: За български гражданин: PNOBG-xxxxxxxx /ЕГН/ PASBG-xxxxxxxx /номер на паспорт/ TINBG-xxxxxxxx /ДДС номер/ За чуждестранно лице: PNOYY-xxxxxxxx /ЕГН/ PASYY-xxxxxxxx /номер на паспорт/ IDCYY-xxxxxxxx /национална карта/ YY- код на държава
	*G	Given
	*SN	SurName
	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=https://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:	

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

	URL=http://ocsp.esign.bg/ocsp
Qualified Certificate Statements (Non Critical)	id-etsi-qcs-semanticId-Natural(oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.esign.bg/pds/pds_en.pdf language=en
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3.1.3 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/ [3]Certificate Policy: Policy Identifier=0.4.0.1456.1.1
CRL Distribution Points (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSignSepQESCA.crl
Enhanced Key Usage (Non Critical)	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Basic Constraints (Critical)	Subject Type=End Entity Path Length Constraint=None
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment (e0)

7.2.2.Профил на квалифицирано удостоверение на квалифициран електронен подпис на физическо лице, свързано с организация, в качеството му на неин законен или договорен представител (ESIGN QES DELEGATED):

eSign QES Delegated	
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	3 years
Subject	Pseudonym (2.5.4.65) Pseudonym
	*E Email
	*CN Common Name
	*SERIALNUMBER Уникален идентификатор за физическото лице: За български гражданин:

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

		PNOBG-xxxxxxxx /ЕГН/ PASBG-xxxxxxxx /номер на паспорт/ TINBG-xxxxxxxx/ДДС номер/ За чуждестранно лице: PNOYY-xxxxxxxx /ЕГН/ PASY-xxxxxxxx /номер на паспорт/ IDCY-xxxxxxxx /национална карта/ YY- код на държава
	*G	Given
	*SN	SurName
r)	*2.5.4.97 (organizationIdentifie	Идентификатор за юридическо лице NTRY-xxxxxxxx /национален идентификационен код/ VATYY-xxxxxxxx /Данъчен номер/ YY – код на държава
	O	Organization (Име на юридическо лице)
	L	Locality
	*C	Country
Public key	RSA 2048 bits	
Access	Authority Information	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://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
Statements	Qualified Certificate (Non Critical)	id-etsi-qcs-semanticId-Natural(oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.esign.bg/pds/pds_en.pdf language=en
Certificate Policies	(Non Critical)	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3.1.4 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/ [3]Certificate Policy: Policy Identifier=0.4.0.1456.1.1
CRL Distribution Points	(Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSignSepQESCA.crl
Enhanced Key Usage	(Non Critical)	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Basic Constraints	(Critical)	Subject Type=End Entity Path Length Constraint=None

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment (e0)
----------------------	---

7.2.3. ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ (ESIGN QESEAL):

eSign QESeal		
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	3 years	
Subject	*E	Email
	*2.5.4.97 (organizationIdentifier)	Идентификатор за юридическо лице NTRY-xxxxxxx /национален идентификационен код/ VATYY-xxxxxxx /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 (1.3.6.1.5.7.48.2) 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 (1.3.6.1.5.7.48.1) Alternative Name: URL=http://ocsp.esign.bg/ocsp	
Qualified Certificate Statements (Non Critical)	id-etsi-qcs-semanticId-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-qct-eseal (oid=0.4.0.1862.1.6.2) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.esign.bg/pds/pds_en.pdf language=en	
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.3.1.5 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esign.bg/bg/useful/documents/ [3]Certificate Policy:	

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

	Policy Identifier=0.4.0.1456.1.1
CRL Distribution Points (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSignSepQESCA.crl
Enhanced Key Usage (Non Critical)	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)
Basic Constraints (Critical)	Subject Type=End Entity Path Length Constraint=None
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment (e0)

8. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

Проверките (одитите), извършвани в СЕП България се отнасят до обработката на информационните данни и управление на ключовите процедури.

СЕП България ежегодно извършва най-малко един вътрешен одит.

СЕП България е обект на одит най-малко веднъж на 24 месеца от Орган за оценяване на съответствието. Целта на одита е да се потвърди, че Доставчика на квалифицирани удостоверителни услуги и предоставяните от него квалифицирани удостоверителни услуги отговарят на изискванията, посочени в Регламент ЕС) № 910/2014.

8.1. ДЕЙСТВИЯ, ПРЕДПРИЕТИ В РЕЗУЛТАТ НА ИЗВЪРШЕН ОДИТ

Докладът от Органа за оценяване на съответствието се предава на надзорен орган в рамките на 3 (три) дни след връчването му на ръководството на СЕП България.

Въз основа на направените оценки от доклада, ръководството на Доставчика набелязва мерки и срокове за отстраняване на констатираните пропуски и несъответствия.

9. ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ

9.1. ЦЕНИ И ТАКСИ

СЕП България поддържа документ ценова тарифа за предоставяни квалифицирани удостоверителни услуги на страницата си в интернет: <http://www.esign.bg/bg/цени/>.

9.1.1. Връщане на удостоверение и възстановяване на плащане

Потребител може да възрази относно неточност или непълнота в съдържанието на издадено квалифицирано удостоверение в 3-дневен срок след публикуването му в публичния регистър.

Ако причината за възражението е в регистриращ орган, Доставчикът прекратява удостоверението и издава ново за своя сметка или възстановява направеното плащане.

9.2. ФИНАНСОВИ ОТГОВОРНОСТИ

Финансовата отговорност на всяко лице, участник в дейността по предоставяне и ползване на квалифицирана удостоверителна услуга се посочва, чрез взаимни споразумения.

Ако СЕП България потвърди и приеме, че са настъпили вреди по негова вина, той се ангажира да плати щетите. Максималната граница на плащане не надвишава размера на щетите.

9.2.1. Застраховка на дейността

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

СЕП България сключва задължителна застраховка на дейността си като регистриран Доставчик на квалифицирани удостоверителни услуги.

9.3. НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ

СЕП България е регистриран като администратор на лични данни по реда на Закона за защита на лични данни. В качеството си на администратор на лични данни, Доставчикът строго съблюдава изискванията за поверителност и неразпространение на лични данни.

9.4. ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

Данни, включени в издаваните от Доставчика квалифицирани удостоверения или данни публикувани в публичния регистър са обект на права върху интелектуалната собственост.

9.4.1. ПРАВО НА СОБСТВЕНОСТ НА ДВОЙКА КЛЮЧОВЕ

Двойката ключове на потребителите и свързаното с публичния ключ квалифицирано удостоверение издадено от СЕП България, както и съответния секретен материал е собственост на Доставчика, независимо от собствеността на физическата среда, в която ключовете се съхраняват и защитават.

9.4.2. ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ДОСТАВЧИКА

СЕП България гарантира, че осъществява дейността си като:

1. Спазва точно условията в настоящия документ, изискванията на Регламент (ЕС) № 910/2014 и националното законодателство при осъществяване на дейността си на Доставчик на квалифицирани удостоверителни услуги;
2. Предоставените услуги не нарушават авторските права и лицензирани права на трети страни;
3. Използва техническо оборудване и технологии, които осигуряват надеждност на системите и техническата и криптографска сигурност при осъществяване на процесите, в това число и сигурен и защитен механизъм/устройство за генериране на ключове и за създаване на квалифициран електронен подпис/печат в своята инфраструктура;
4. Издава квалифицирани удостоверения за електронни подписи/печати след като провери с допустими от закона средства представената информация;
5. Сигурно съхранява и поддържа информация, свързана с издаваните удостоверения и оперативната работа на системите;
6. Спазва установените процедури за работа и правила за технически и физически контрол, в съответствие с условията в настоящата Политика и Практика при предоставяне на квалифицирани удостоверителни услуги;
7. Създава възможност за незабавно спиране и прекратяване на действието на квалифицирано удостоверение;
8. Прекратява и спира действието на удостоверения при условията и по реда на съответната Политика;
9. Уведомява незабавно заинтересованите лица след спиране на квалифицирано удостоверение;
10. Осигурява условия за точно определяне на времето на издаване, спиране, възобновяване и прекратяване на действието на квалифицирани удостоверения;
11. Изпълнява процедури по идентификация и установяване на автентичност на Титуляря/Създателя или на упълномощения представител на юридическо лице;
12. Осигурява мерки срещу подправяне на квалифицирани удостоверенията и поверителност на данните, до които има достъп в процеса на създаването на квалифицирания електронен подпис/печат;
13. Използва надеждни системи за съхраняване и управление на удостоверения;
14. Само надлежно овластени служители имат достъп за внасяне на промени в данните, установяване на автентичността и валидността на удостоверенията;
15. Взима незабавни мерки при възникване на технически проблеми във връзка със сигурността;
16. С изтичане на срока на валидност на квалифицирано удостоверение отменя валидността му;

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

17. Информира потребителите, както и доверяващите се страни за техните задължения и дължима грижа на поведение при използването и доверяването на предоставяните от Доставчика квалифицирани удостоверителни услуги, така също относно правилното и сигурно използване на издадените квалифицирани удостоверения и предоставените удостоверителни услуги, свързани с тях;
18. Използва и съхранява събраната лична и друга информация само за целите на своята дейност по предоставяне на квалифицирани удостоверителни услуги в съответствие с националното законодателство;
19. Не съхранява и не копира данни за създаване на потребителски частни ключове;
20. Поддържа разполагаеми средства, които осигуряват възможност за извършване на дейността му;
21. Сключва застраховка за времето на своята дейност;
22. Поддържа доверен персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността;
23. Поддържа публичен регистър/хранилище, в който публикува издадените квалифицирани удостоверения, актуален Списък със спрени и прекратени удостоверения (CRL), други обстоятелства и електронни документи, съгласно тази Политика и националното законодателство;
24. Осигурява постоянен достъп до публичния регистър по електронен път (24/7/365);
25. Осигурява защита срещу внасяне на промени в поддържания публичен регистър от нерегламентиран и неправомерен достъп или поради случайно събитие;
26. Публикува незабавно в публичния регистър издадените и подписани удостоверения;
27. Създава условия на всяка доверяваща се страна да провери статуса на издадено и публикувано квалифицирано удостоверение в публичния регистър на удостоверения;
28. Извършва периодични вътрешни одити на дейността на удостоверяващия орган и регистрацията орган;
29. Извършва външни одити от независими одитори и публикува на сайта си резултатите от проверката;
30. Използва в дейността си сертифициран софтуер и хардуер, както и сигурни и надеждни технологични системи;
31. Поддържа на сайта на Доставчика списък с регистриращи органи, списък с препоръчителен софтуер и хардуер за използване от потребителите, бланки, формуляри, типов договор и др. документи в полза на потребителите;

Доставчикът носи отговорност пред потребители и доверяващи се страни за причинени вреди от груба небрежност или умисъл от:

1. Неизпълнение на изискванията от Регламент (ЕС) № 910/2014 при осъществяване на дейността си по предоставяне на квалифицирани удостоверителни услуги;
2. Неверни или липсващи данни в квалифицираното удостоверение към момента на издаването му;
3. Вреди, които са причинени в случай, че по време на издаването на квалифицираното удостоверение лицето, посочено като Титуляр/Създател или упълномощен представител на юридическо лице, не е разполагало с частния ключ, съответстващ на публичния ключ;
4. Алгоритмичното несъответствие между частния ключ и публичния ключ, вписван в квалифицираното удостоверение;
5. Неспазване на задълженията си по издаване и управление на квалифицирани удостоверения;
6. Пропуски в установяване на идентичността на Титуляря/Създателя или на упълномощения представител на юридическо лице.

9.4.3. задължения, Отговорност и гаранции на Регистрацията орган

Доставчикът гарантира, че регистрацията орган изпълнява своите функции и задължения в пълно съответствие с условията в този документ, с изискванията и процедурите в Политиката и издадените вътрешни оперативни инструкции.

Доставчикът отговаря за действията на регистрацията орган в инфраструктурата на СЕП България.

СЕП България гарантира, че регистрацията орган:

1. Изпълнява своята дейност, като използва надеждни и сигурни устройства и софтуер;
2. Предоставя услуги, които са в съответствие със националното законодателство и не нарушава авторските права и лицензирани права на потребителите;
3. Полага нужните усилия, за да извършва правилна идентификация на потребителите, въвежда правилно и точно данните в базата данни на Доставчика и актуализира тази информация в момента на потвърждаване на данните;
4. Не прави умислени грешки или не внася неточности в информацията, съдържаща се в квалифицираните удостоверения;
5. Неговите услуги са в съответствие с общоприетите стандарти: X.509, PKCS # 10, PKCS # 7, PKCS # 12.

	ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ	eIDAS-CP-QES For public use
Regulation 910 / 2014 eIDAS	CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA	Version – 2.5 11.05.2021

9.4.4. ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИ

Потребителят има следните задължения:

1. Да се запознае и да спазва условията на договора, Политиките и Практиките при предоставяне на квалифицирани удостоверителни услуги от СЕП България, както и изискванията в останалите документи, публикувани в публичния регистър на СЕП България;
2. При подаване на искания за издаване и управление на квалифицирани удостоверения да предостави вярна, точна и пълна информация, която СЕП България изисква съгласно договора, нормативните изисквания, приложимите Политики и Практики;
3. Да генерира криптографски ключове, използвайки сигурен метод и алгоритъм, съобразно изискванията на Регламент (ЕС) № 910/2014 и да използва одобрени от Доставчика устройства за създаване на квалифициран електронен подпис/печат (QSCD);
4. Да провери пълнотата и верността на съдържанието на предоставената от него информация за удостоверяване в поле DN (Distinguished Name) на издаваните квалифицирани удостоверения. В случай на несъответствие между представената информация и удостовереното съдържание, потребителят трябва да уведоми незабавно СЕП България;
5. Да преустанови използването на квалифицирано удостоверение в случай на съмнение за загуба или компрометиране на частния ключ и да подаде до СЕП България заявка за неговото спиране;
6. Да преустанови използването на квалифицирано удостоверение при наличие в него на остаряла, променена, неточна и/или невярна информация и да подаде искане за спиране на действието на удостоверението;
7. Преди да използва ново квалифицирано удостоверение, да промени досегашния ПИН за достъп до устройството за създаване на електронен подпис/печат (QSCD), където се съхранява частният ключ;
8. Да приложи необходимата дължима грижа и да предприеме необходимите мерки за предотвратяване на частния ключ от компрометиране, загуба, разкриване, модификация или друго неразрешено действие;
9. Да използва издаденото от СЕП България квалифицирано удостоверение само за законни цели и в съответствие с указаната в него политика и практика;
10. Да одобрява условията, посочени в договора между него и СЕП България (това одобрение трябва да се състои в поставяне на саморъчен подпис върху договора);
11. Да одобри издаденото му квалифицирано удостоверение;
12. Да не разкрива паролата за достъп до устройството за създаване на квалифициран електронен подпис/печат на неупълномощени лица;
13. Да не прави достъпен своя частен ключ за други лица.

9.5. ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ

1. СЕП България не носи отговорност в случаи на вреди причинени от:
2. Използване на квалифицирано удостоверение извън пределите на вписаните в него предназначения и ограничения на неговото действие;
3. Незаконни действия от страна на потребители и доверяващи се страни;
4. Предоставяне на начина на идентифициране на устройството за създаване на квалифициран електронен подпис/печат и достъп до частния ключ от страна на потребители на трети лица;
5. Случайни събития, имащи характера на непреодолима сила, включително злоумишлени действия на трети лица (хакерски атаки, отнемане на устройството за създаване на квалифициран електронен подпис/печат (QSCD), достъп до частния ключ, узнаване без знанието на Титуляря/Създателя на начина на идентифициране и др.)
6. Използване на квалифицирано удостоверение, което не е издадено или използвано в съответствие с изискванията и процедурите на Практиката и Политиката на СЕП България;
7. Използване на невалидно удостоверение (удостоверение, което е спряно или прекратено);
8. Не своевременно действие по прекратяване или спиране на удостоверение (следствие от забавено от страна на Титуляря/Създателя искане или поради причини извън контрола на СЕП България);
9. Компрометиран частен ключ, кореспондиращ на публичния ключ в квалифицираното удостоверение по вина на Титуляря/Създателя;
10. Лошо качество и функционалност на софтуерните продукти и хардуерни устройства използвани от Титуляря/Създателя и доверяващи се страни.

	<p style="text-align: center;">ПОЛИТИКА ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ</p>	<p style="text-align: center;">eIDAS-CP-QES For public use</p>
<p style="text-align: center;">Regulation 910 / 2014 eIDAS</p>	<p style="text-align: center;">CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE/SEA</p>	<p style="text-align: center;">Version – 2.5 11.05.2021</p>

9.6. ОТГОВОРНОСТ НА ПОТРЕБИТЕЛ

Отговорността на потребител е в резултат от изпълнение на неговите задължения. Условието на отговорност се уреждат с договор със СЕП България.

Потребителят отговаря спрямо доверяващите се лица ако:

1. При създаването на двойката частен-публичен ключ е използвал алгоритъм и устройства за създаване на квалифициран електронен подпис/печат (QSCD), които не отговарят на изискванията на Регламент (ЕС) № 910/2014;
2. Не изпълнява точно изискванията за сигурност, определени от СЕП България;
3. Не поиска от Доставчика спиране на действието на квалифицирано удостоверение, след като е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерното му използване;
4. Ако е извършил неверни изявления, направени пред СЕП България и имащи отношение към съдържанието или към издаването на квалифицираното удостоверение;
5. Когато квалифицираното удостоверение е издадено с вписано юридическо лице и овластено от него лице (Титуляр), отговаря за неизпълнението от страна на овластените на задълженията му.