Утверждена директором
государственного
предприятия «НЦЭУ»
22.04.2020

ПОЛИТИКА ПРИМЕНЕНИЯ СЕРТИФИКАТОВ ФИЗИЧЕСКИХ ЛИЦ

республиканского удостоверяющего центра
Государственной системы управления открытыми ключами
проверки электронной цифровой подписи Республики Беларусь

Минск
2020

СОДЕРЖАНИЕ

1. Введение в политику применения сертификатов

1.1. Общие положения

Настоящая политика применения сертификатов республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – политика применения сертификатов) является документом, устанавливающим политику безопасности в отношении издания и распространения информации о статусе сертификатов открытых ключей проверки электронной цифровой подписи (далее – сертификаты) физических лиц и разработана в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров».

Для целей настоящей политики термины и определения используются в значениях, определенных Законом Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи», СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей», СТБ 34.101.48-2012, СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов», СТБ 34.101.69-2014 «Информационные технологии и безопасность. Криптология. Термины и определения».

В соответствии с пунктом 5 Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» функции оператора республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – республиканский удостоверяющий центр) осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее – оператор).

Юридический адрес:

Республика Беларусь, 220004, г.Минск, ул.Раковская, 14.

УНП 191700161, ОКПО 380325925000.

Контактный телефон, факс, адрес электронной почты и интернет-сайт оператора:

телефон: 8 (017) 31130 00;

факс:8 (017)311 30 06;

e-mail: info@nces.by;

интернет-сайт: nces.by.

Основные функции республиканского удостоверяющего центра определены в Положении о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь,

утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118.

Требования настоящей политики применения сертификатов реализуются в соответствии с регламентом деятельности республиканского удостоверяющего центра.

1.2. Идентификация

Настоящая политика применения сертификатов имеет следующий объектный идентификатор (Object Identifier, OID):

{iso(1) member-body(2) by(112) registration-authority(1) oac(2) pki-gov(1) nces(1) ext(1) certificate-policy(3) ca-by(2) individuals(1)} – (1.2.112.1.2.1.1.1.3.2.1).

Данный объектный идентификатор включается в соответствии с требованиями СТБ 34.101.19-2012 в расширение certificatePolicies сертификатов, издаваемых республиканским удостоверяющим центром.

1.3. Пользователи политики применения сертификатов

Настоящая политика применения сертификатов применяется для издаваемых республиканским удостоверяющим центром сертификатов физических лиц.

Сертификаты, изданные в соответствии с настоящей политикой применения сертификатов, могут быть использованы для подтверждения целостности и подлинности электронных документов и проверки электронной цифровой подписи.

2. Требования к участникам инфраструктуры открытых ключей

2.1. Требования к республиканскому удостоверяющему центру

Республиканский удостоверяющий центр обязан выполнять все требования, установленные в настоящей политике применения сертификатов.

2.2. Требования к регистрационному центру

Регистрационный центр должен присоединиться к настоящей политике применения сертификатов и выполнять ее в части:

регистрации подписчиков республиканского удостоверяющего центра;

требований по управлению деятельностью регистрационного центра.

Требования к регистрационному центру предъявляются в соответствии с п. 2.2. регламента деятельности республиканского удостоверяющего центра.

2.3. Требования к подписчикам

В качестве подписчика выступает физическое лицо, являющееся в соответствии с законодательством владельцем личного ключа, на базе которого выработан открытый ключ, и обращающееся к поставщику услуг от собственного имени за услугой издания сертификата, включающего значение указанного открытого ключа.

Требования к подписчикам предъявляются в соответствии с п. 2.3. регламента деятельности республиканского удостоверяющего центра.

2.4. Требования к доверяющей стороне

Требования предъявляются в соответствии с п. 2.4. регламента деятельности республиканского удостоверяющего центра.

3. Требования к республиканскому удостоверяющему центру

3.1. Требования по управлению ключами

3.1.1. Выработка личного ключа республиканского удостоверяющего центра

Выработка личного ключа республиканского удостоверяющего центра осуществляется в соответствии с п. 3.1.1. регламента деятельности республиканского удостоверяющего центра.

3.1.2. Хранение, резервное копирование и восстановление личного ключа республиканского удостоверяющего центра

Хранение, резервное копирование и восстановление личного ключа республиканского удостоверяющего центра осуществляется в соответствии с п. 3.1.2. регламента деятельности республиканского удостоверяющего центра.

3.1.3. Распространение открытого ключа республиканского удостоверяющего центра

Распространение открытого ключа осуществляется в соответствии с п. 3.1.3. регламента деятельности республиканского удостоверяющего центра.

3.1.4. Депонирование личного ключа республиканского удостоверяющего центра

Депонирование личного ключа республиканского удостоверяющего центра осуществляется в соответствии с п. 3.1.4. регламента деятельности республиканского удостоверяющего центра.

3.1.5. Использование личного ключа республиканского удостоверяющего центра

Республиканский удостоверяющий центр использует свой личный ключ для целей, определенных настоящей политикой применения сертификатов.

3.1.6. Окончание срока действия личного ключа республиканского удостоверяющего центра

Окончание срока действия личного ключа республиканского удостоверяющего центра осуществляется в соответствии с п. 3.1.6. регламента деятельности республиканского удостоверяющего центра.

3.1.7. Управление средством электронной цифровой подписи, используемым для издания сертификатов

Управление средством электронной цифровой подписи, используемым для издания сертификатов, осуществляется в соответствии с п. 3.1.7. регламента деятельности республиканского удостоверяющего центра.

3.2. Требования по управлению сертификатами

3.2.1. Регистрация подписчика

Регистрация подписчика осуществляется в соответствии с п. 3.2.1. регламента деятельности республиканского удостоверяющего центра.

При регистрации подписчика для получения сертификата регистрационный центр должен:

очно установить и достоверно подтвердить личность физического лица, а также полноту и точность представленных идентификационных данных;

зарегистрировать всю информацию, используемую для проверки личности физического лица, включая номер документа, удостоверяющего личность в соответствии с законодательством, дату выдачи данного документа, наименование органа, выдавшего его, а также другие данные.

3.2.2. Возобновление действия сертификата и обновление данных

Возобновление действия сертификата физического лица осуществляется в соответствии с п. 3.2.2. регламента деятельности республиканского удостоверяющего центра.

3.2.3. Издание сертификатов

Издание сертификатов физических лиц осуществляется в соответствии с п. 3.2.3. регламента деятельности республиканского удостоверяющего центра.

Профиль формата сертификата физического лица приведен в приложении 1 к настоящей политики применения сертификатов.

Республиканский удостоверяющий центр может издать новый сертификат для нового значения открытого ключа подписчика, сохранив без изменения другую информацию, содержащуюся в сертификате этого подписчика, предварительно убедившись, что на момент обращения она является актуальной. Подлинность всей представленной подписчиком регистрационной информации проверяет регистрационный центр в соответствии с порядком, установленным для первичной регистрации.

В случае, если актуальность всей информации, содержащейся в сертификате подписчика, может подтвердиться информацией из базовых государственных информационных ресурсов, интегрированных в общегосударственную автоматизированную информационную систему, республиканский удостоверяющий центр может издать новый сертификат для нового значения открытого ключа подписчика, сохранив без изменения другую информацию, содержащуюся в сертификате этого подписчика, в автоматическом режиме при дистанционном обращении подписчика при условии использования действующего сертификата. Порядок оказания таких услуг определен организационно-распорядительными документами оператора.

3.2.4. Распространение организационно-распорядительных документов

Распространение нормативных и организационных документов осуществляется в соответствии с п. 3.2.4. регламента деятельности республиканского удостоверяющего центра.

Оператор предоставляет доступ подписчикам и доверяющим сторонам к следующим организационно-распорядительным документам (в дополнение к указанным в регламенте деятельности республиканского удостоверяющего центра):

форматы сертификатов открытых ключей и атрибутных сертификатов, издаваемых республиканского удостоверяющего центра;

перечень идентификаторов объектов информационных технологий, использующихся в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь;

перечни сведений о подписчике;

форма заявления об отзыве сертификата;

иные организационно-распорядительные документы.

Оператор размещает данную информацию на своем интернет-сайте.

3.2.5. Распространение сертификатов

Распространение сертификатов осуществляется в соответствии с п. 3.2.5. регламента деятельности республиканского удостоверяющего центра.

Сведения о подлинности изданного сертификата любого подписчика могут быть предоставлены в установленном оператором порядке.

Республиканский удостоверяющий центр обеспечивает доступность информации о действительности и назначении сертификата всем пользователям Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь путем размещения списка отозванных сертификатов. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от оператора, оператор принимает все необходимые меры, чтобы гарантировать, что данная услуга будет недоступна только в течение 1 часа.

3.2.6. Отзыв сертификата

Отзыв сертификата осуществляется в соответствии с п. 3.2.6. регламента деятельности республиканского удостоверяющего центра.

Отзыв сертификата производится только при досрочном прекращении его действия в случае невозможности использования личного ключа (в случаях компрометации личного ключа, либо смерти его владельца), либо изменения идентификационных данных его владельца (смена одного или нескольких основных персональных данных).

Если о невозможности использования личного ключа сообщила третья сторона, то республиканский удостоверяющий центр запрашивает подтверждение данной информации либо непосредственно у подписчика (в случае компрометации), либо у компетентных органов (в случае смерти владельца личного ключа). При этом сертификат считается приостановленным до тех пор, пока не будет подтвержден его отзыв.

Запрашивать отзыв сертификата подписчика может подписчик.

Запросы, связанные с отзывом сертификата, идентифицируются и проверяются республиканским удостоверяющим центром на предмет их получения из достоверных источников.

Республиканский удостоверяющий центр гарантирует, что сертификат отзывается только на основании заявления на отзыв в течении одного рабочего дня с момента получения оригинала заявления оператором.

Список отозванных сертификатов издается республиканским удостоверяющим центром сразу же после обработки запроса на отзыв сертификата.

Услуга республиканского удостоверяющего центра по управлению отзывом сертификата доступна в течение рабочего времени регистраторов регистрационных центров. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от оператора, предпринимаются все необходимые меры для того, чтобы данная услуга была недоступна только в течение 1 часа.

Информация об отзыве сертификата доступна до истечения срока действия этого сертификата, установленного при его издании.

Форма заявления на отзыв сертификата приведена на интернет-сайте оператора.

Заявление может подаваться как на бумажном носителе, так и в виде электронного документа.

Если не иное не предусмотрено в организационно-распорядительных документах оператора, отзыв может быть осуществлен в порядке, установленном оператором, на основании пароля для осуществления отзыва сертификата в срочном (время устанавливается организационно-распорядительных документах оператора) порядке.

3.2.7. Предоставление информации о статусе сертификата подписчика

Предоставление информации о статусе сертификата подписчика осуществляется в соответствии с п. 3.2.7. регламента деятельности республиканского удостоверяющего центра.

Новый список отозванных сертификатов может быть издан перед установленным временем издания следующего списка отозванных сертификатов. Например, внеочередной список отозванных сертификатов издается республиканским удостоверяющим центром сразу же после обработки запроса на отзыв сертификата подписчика.

Актуальный список отозванных сертификатов размещен на интернет-сайте оператора.

Услуги республиканского удостоверяющего центра по получению статуса сертификата доступны 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от оператора, оператор принимает все необходимые меры, чтобы гарантировать, что данные услуги будут недоступны только в течение 1 часа.

3.3. Управление деятельностью республиканского удостоверяющего центра

3.3.1. Управление безопасностью

Управление безопасностью осуществляется в соответствии с п. 3.3.1. регламента деятельности республиканского удостоверяющего центра.

3.3.2. Классификация и управление активами

Классификация и управление активами осуществляется в соответствии с п.3.3.2. регламента деятельности республиканского удостоверяющего центра.

3.3.3. Вопросы безопасности, связанные с персоналом

В соответствии с п. 3.3.3. регламента деятельности республиканского удостоверяющего центра.

3.3.4. Физическая защита и защита от воздействий окружающей среды

Физическая защита и защита от воздействий окружающей среды осуществляется в соответствии с п. 3.3.4. регламента деятельности республиканского удостоверяющего центра.

3.3.5. Управление операционной деятельностью

Управление операционной деятельностью осуществляется в соответствии с п.3.3.5. регламента деятельности республиканского удостоверяющего центра.

3.3.6. Управление системным доступом

Управление системным доступом осуществляется в соответствии с п. 3.3.6. регламента деятельности республиканского удостоверяющего центра.

3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем

Внедрение и обслуживание безопасных доверенных информационных систем осуществляется в соответствии с п. 3.3.7. регламента деятельности республиканского удостоверяющего центра.

3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности

Восстановление при сбоях и обеспечение непрерывности деятельности осуществляется в соответствии с п. 3.3.8. регламента деятельности республиканского удостоверяющего центра.

3.3.9. Прекращение функционирования республиканского удостоверяющего центра

Прекращение функционирования республиканского удостоверяющего центра осуществляется в соответствии с п. 3.3.9. регламента деятельности республиканского удостоверяющего центра.

3.3.10. Соответствие требованиям законодательства

В соответствии с п. 3.3.10. регламента деятельности республиканского удостоверяющего центра.

3.3.11. Сохранение информации, касающейся сертификатов

Сохранение информации, касающейся сертификатов осуществляется в соответствии с п. 3.3.11. регламента деятельности республиканского удостоверяющего центра.

3.4. Организационные положения

В соответствии с п. 3.4. регламента деятельности республиканского удостоверяющего центра.

Настоящая политика применения сертификатов вступает в силу с 23.04.2020.

Приложение 1
к Политике применения сертификатов открытых ключей физических лиц республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Профиль формата сертификата физического лица

Сертификат в соответствии с СТБ 34.101.19 состоит из трех базовых компонентов:

Certificate ::= SEQUENCE {
tbsCertificate TBSCertificate,
signatureAlgorithm AlgorithmIdentifier,
signatureValue BIT STRING }

Составбазовогокомпонента **tbsCertificate**

Поле (компонент)	OID	Описаниеполя (компонента)	Типполя	Постоянные значения
version		Версия сертификата по x.509. В текущей локализации используется Version3	постоянное	***2***
serialNumber		Уникальный серийный номер сертификата. Положительное целое число, не превышающее значение более 20 октетов	*изменяемое*	
signature				
algorithm		Идентификатор алгоритма, который УЦ использовал для выработки ЭЦП для данного сертификата, в данном профиле **bign-with-hbelt** согласно СТБ 34.101.45-2013	постоянное	***1.2.112.0.2.0.34.101.45.12***
parameters		Параметры алгоритма. Значение поля ***NULL*****	постоянное	***NULL*****
issure		Эмитент (издатель). Идентифицирует УЦ, который подписал и выдал сертификат		
Набор полей и их значений совпадает с набором и значениями полей компонента **subject** в сертификате УЦ, издавшем данный сертификат физического лица				
validity		Срок действия сертификата.		

notBefore		Дата начала срока действия сертификата (согласно п.6.1.2.5 СТБ 34.101.19-2012)	*изменяемое*	
afterBefore		Дата окончания срока действия сертификата (согласно п.6.1.2.5 СТБ 34.101.19-2012)	*изменяемое*	
subject				
commonName	2.5.4.3 id-at-commonName	Агрегированное значение фамилии и имени физического лица на латинице, идентификационный (личный) номер из паспорта.	*изменяемое*	
surName	2.5.4.4 id-at-surname	Фамилия физического лица на русском языке	*изменяемое*	
name	2.5.4.41 id-at-name	Имя физического лица на русском языке	*изменяемое*	
givenName	2.5.4.42 id-at-givenName	Отчество физического лица на русском языке	*изменяемое*	
serialNumber	2.5.4.5 id-at-serialNumber	Идентификационный (личный) номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т. д.) субъекта инфраструктуры открытых ключей ГосСУОК, являющегося физическим лицом	*изменяемое*	
countryName	2.5.4.6 id-at-contryName	Страна (код страны) — гражданство физического лица	*изменяемое*	
e-mailAddress	1.2.840.113549.1.9.1	Адрес электронной почты физического лица	*изменяемое**	
subjectPublicKeyInfo				
algorithm		ИДЕНТИФИКАТОР алгоритма, с которым используется открытый ключ, в данном профиле ***bign-pubkey***	постоянное	***1.2.112.0.2.0.34.101.45.2.1***
parameters		Параметры открытого ключа, в данном профиле для ***bign-curve256v1***	постоянное	***1.2.112.0.2.0.34.101.45.3.1***
subjectPublicKey		Значение открытого ключа	постоянное	
extensions		Расширения		

subjectAltName	2.5.29.17 id-ce-subjectAltName	Расширение сертификата, содержащее одно или несколько значений альтернативных имен субъекта, обеспечивающих дополнительную идентификацию субъекта - Фамилия, имя и отчество физического лица на белорусском языке. Задается компонентом **otherName**в кодировке UTF8String	*изменяемое**	
Прозвішча	1.2.112.1.2.1.1.1.4.2	Фамилия физического лица на белорусском языке	*изменяемое**	
Імя	1.2.112.1.2.1.1.1.4.3	Имя физического лица на белорусском языке	*изменяемое**	
Імя па бацьку	1.2.112.1.2.1.1.1.4.4	Отчество физического лица на белорусском языке	*изменяемое**	
subjectKeyIdentifier	2.5.29.14	Уникальный идентификатор открытого ключа субъекта (представляет хэш-значение **SHA-1 20 байт** согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	*изменяемое*	
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа субъекта (представляет хэш-значение **SHA-1 20 байт** согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)		
certificatePolicies	2.5.29.32	Политика, в соответствии с которой был издан и может применяться сертификат	постоянное	***1.2.112.1.2.1.1 .1.3.2.1***
BasicConstraints	2.5.29.19	Конечный субъект. Означает принадлежность к подписчикам РУЦ ГосСУОК. Формируется согласно раздела 6.2.1.9 СТБ 34.101.19-2012	постоянное	***True*** ***(или не установлен)***
CRLDistributionPoints	2.5.29.31	Точка распространения СОС. URL-адрес веб-ресурса РУЦ, на котором располагается актуальный СОС	*изменяемое*	
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Доступ к информации УЦ		
OCSP	1.3.6.1.5.5.7.48.1	Содержит указатель на OCSP сервис УЦ	*изменяемое**	***http://nces.by/pki/ocsp/ca-by***
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	*изменяемое*	***http://nces.by/pki/certs/ca-by.crt***
KeyUsage	2.5.29.15	Назначениеключа: digitalSignature, nonRepudiation, keyEncipherment	постоянное	***111***
ExtendedKeyUsage	**2.5.29.37**	Расширенное назначениеключа		
ClientAuth	1.3.6.1.5.5.7.3.2	Проверка подлинности абонента сервером во время установки защищённого TLS-соединения	постоянное	

emailProtection	1.3.6.1.5.5.7.3.4	Защитаэлектроннойпочты	постоянное	

Составбазовогокомпонента **signatureAlgorithm**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
signatureAlgorithm				
algorithm		Идентификатор алгоритма, который УЦ использовал для подписи сертификата, в данном профиле **bign-with-hbelt** согласно СТБ 34.101.45-2013	постоянное	***1.2.112.0.2.0.34.101.45.12***
parameters		Параметры алгоритма. Значение поля ***NULL*****	постоянное	***NULL*****

Состав базового компонента **signatureValue**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
signatureValue		Значение электронной цифровой подписи, вычисленное РУЦ	*изменяемое*	

* – не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013