УТВЕРЖДАЮ
Директор республиканского унитарного предприятия «Национальный центр электронных услуг»

_____ А.А. Ильин

«30» ____12_____ 2016 г.

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

Минск
2016

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 – ППС) является долговременным документом, содержащим описание услуг, которые оказывает республиканский удостоверяющий центр (далее – РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) по изданию, распространению, хранению сертификатов открытых ключей (далее – сертификат) и списков отозванных сертификатов (далее – СОС), а также по управлению статусом сертификатов. РУЦ является подчиненным удостоверяющим центром корневого удостоверяющего центра ГосСУОК.

ППС разработана в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров» и устанавливает принципы деятельности РУЦ на основе систематизированного изложения процессов и процедур оказания услуг, но не содержит их детального описания.

Для целей настоящего ППС термины и их определения используются в значениях, установленных Законом Республики Беларусь от 28 декабря 2009 года «Об электронном документе и электронной цифровой подписи» (Национальный реестр правовых актов Республики Беларусь, 2010 г., № 15, 2/1665), Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10.12.2015 № 118 (Национальный правовой Интернет-портал Республики Беларусь, 10.12.2015, № 7/3335, далее – положение о ГосСУОК), государственным стандартом Республики Беларусь СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров» и другими техническими нормативными правовыми актами.

В соответствии с Положением о ГосСУОК основными функциями РУЦ являются:

генерация личных и открытых ключей РУЦ;

издание, распространение, предоставление информации о статусе, отзыв и хранение сертификатов регистраторов РУЦ и регистрационных

центров (далее – регистратор), центра атрибутных сертификатов, физических лиц (далее – ФЛ), сервисов (приложения, серверы или устройства) (далее – СР);

удостоверение формы внешнего представления электронных документов на бумажном носителе;

функции регистрационного центра (далее – РЦ).

РУЦ осуществляет согласование регламентов работы и инструктаж персонала РЦ, присоединившихся к ППС.

В соответствии с Указом Президента Республики Беларусь от 23 января 2014 г. № 46 (Национальный правовой Интернет-портал Республики Беларусь, 27.01.2014, № 1/14787) функции Оператора (далее - Оператор) осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее – НЦЭУ).

Юридический адрес:

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

Банковские реквизиты:

Расчетный счет 3012089370084 филиал № 529 «Белсвязь» ОАО «АСБ Беларусбанк» МФО 153001720, 220005 г. Минск, пр. Независимости, 56.

УНП 191700161.

Адрес местонахождения:

Республика Беларусь, 220002, г. Минск, пр. Машерова, 25-200.

Контактные телефоны, факс, адрес электронной почты и Интернет-сайта Оператора:

телефон:	(017) 229 30 00;
факс:	(017) 229 30 06;
e-mail:	pkigov@nces.by
адрес Интернет-сайта:	http://nces.by

Требования ППС реализуется Оператором в соответствии с регламентом деятельности по применению сертификатов открытых ключей (далее – Регламент).

1.2. Идентификация

ППС имеет следующие объектные идентификаторы (Object Identifier, OID):

для сертификатов ФЛ –

{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);

для сертификатов сервисов (приложения, серверы или устройства) –

{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) services(2)} – (1.2.112.1.2.1.1.1.3.2.2)

Данный OID включается в расширения сертификатов `certificatePolicies`, издаваемых РУЦ, в соответствии с СТБ 34.101.19-2012 «Информационные технологии и безопасность. Формат сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

1.3. Пользователи политики применения сертификатов

Сертификаты ФЛ, изданные в соответствии с данной ППС, могут быть использованы для подтверждения целостности и подлинности электронных документов и проверки электронной цифровой подписи (далее – ЭЦП), которая в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» является равнозначной собственноручной подписи в документе на бумажном носителе.

Сертификаты СР, изданные в соответствии с данной ППС, могут быть использованы для обеспечения работы сервисов (приложения, серверы или устройства).

Настоящая ППС не ограничивает использование данных сертификатов никакими программными приложениями.

2. Требования к участникам инфраструктуры открытых ключей

2.1. Требования к РУЦ

Оператор должен выполнять все требования, установленные в разделе 3 настоящей ППС.

Оператор несет ответственность за соответствие процедурам, установленным настоящей ППС, в соответствии с законодательством Республики Беларусь.

Положения Регламента не должны противоречить ППС.

2.2. Требования к РЦ

РЦ должен быть аккредитован в ГосСУОК в соответствии с требованиями Инструкции о порядке проведения аккредитации поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и осуществления контроля за соблюдением условий аккредитации, утвержденной приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.11.2013 № 89 (Национальный правовой Интернет-портал Республики Беларусь, 2.12.2013, № 7/2650).

РЦ должен осуществлять свою деятельность в соответствии с настоящей ППС, Регламентом РУЦ, регламентом работы, согласованным с РУЦ.

РЦ должен осуществлять проверку информации, вносимой в сертификат, формирование заявок на издание и отзыв сертификата, передачу конечным пользователям изданных сертификатов и карточек открытых ключей, обеспечение их взаимодействия с РУЦ.

РЦ должен нести ответственность за проверку идентификационных данных подписчиков и подтверждение запросов на издание сертификатов.

При формировании заявки на издание или отзыв сертификата РЦ должен установить и достоверно подтвердить личность физического лица (данные о государственной регистрации юридического лица), а также полноту и точность представленных идентификационных данных согласно настоящей ППС и регламенту РЦ.

2.3. Требования к подписчикам

Подписчиком может являться ФЛ или юридическое лицо (далее - ЮЛ).

Подписчик должен:

гарантировать, что вся информация, предоставляемая для издания и использования его открытого ключа и сертификата, является полной и точной;

использовать личный и открытый ключи только для выработки и проверки ЭЦП соответственно, а также в соответствии с любыми другими ограничениями, о которых уведомляется подписчик;

осуществлять выработку личного ключа и открытого ключа с использованием средства ЭЦП, имеющего сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь;

хранить в тайне личный ключ;

обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);

отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена.

не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия такого открытого ключа истек.

В случае, если подписчик и субъект являются разными лицами, подписчик должен информировать субъекта о данных требованиях.

2.4. Требования к доверяющей стороне

Перед установлением доверия к электронному документу, в частности сертификату, доверяющая сторона должна:

убедиться в действительности сертификата, включая его проверку на отзыв и истечение срока действия;

удостовериться, что назначение сертификата соответствует предполагаемой области применения и любым другим ограничениям, связанным с его использованием, которые указаны в нем или в настоящей ППС.

3. Требования к РУЦ

3.1. Требования по управлению ключами

3.1.1. Выработка личного ключа РУЦ

Выработка личного ключа РУЦ осуществляется в соответствии с п.3.1.1. Регламента.

Срок действия сертификата открытого ключа РУЦ – 15 лет.

3.1.2. Хранение, резервное копирование и восстановление личного ключа РУЦ

Хранение, резервное копирование и восстановление личного ключа РУЦ осуществляется в соответствии с п.3.1.2. Регламента.

3.1.3. Распространение открытого ключа РУЦ

Распространение открытого ключа осуществляется в соответствии с п.3.1.3. Регламента.

3.1.4. Депонирование личного ключа РУЦ

Депонирование личного ключа РУЦ осуществляется в соответствии с п.3.1.4. Регламента.

3.1.5. Использование личного ключа

РУЦ использует свой личный ключ только для целей, определенных настоящей ППС.

3.1.6. Окончание срока действия личного ключа РУЦ

Окончание срока действия личного ключа РУЦ осуществляется в соответствии с п.3.1.6. Регламента.

3.1.7. Управление средством ЭЦП, используемым для издания сертификатов

Управление средством ЭЦП, используемым для издания сертификатов осуществляется в соответствии с п.3.1.7. Регламента.

3.2. Требования по управлению сертификатами

3.2.1. Регистрация владельца сертификата, издаваемого РУЦ

Регистрация владельца сертификата, издаваемого РУЦ осуществляется в соответствии с п.3.2.1. Регламента.

Подписчик осуществляет выработку личного ключа и открытого ключа на базе личного ключа подписи. Личный ключ подписи помещается

на носитель ключевой информации (далее – НКИ). Средства ЭЦП, используемые для выработки ключей, а также НКИ должны соответствовать требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) и в зависимости от выбранной услуги могут предоставляться РУЦ или РЦ. Запрос на издание сертификата соответствует требованиям СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

Перечень НКИ, которые можно использовать в ГосСУОК размещен на Интернет-сайте Оператора.

3.2.1.1. Регистрация подписчика для получения сертификата ФЛ

ФЛ, обратившееся в РУЦ либо в РЦ за оказанием услуги регистрации и издания сертификата ФЛ, должно представить:

документ, удостоверяющий личность, в соответствии с законодательством Республики Беларусь. Для иностранных граждан, имеющих документ, удостоверяющий личность без русскоязычного представления персональных данных, необходимо представить его перевод на русском языке, заверенный в соответствии с законодательством Республики Беларусь;

перечень сведений о подписчике (форма размещена на Интернет-сайте Оператора), заполненный разборчиво на русском (либо на русском и белорусском) языке;

копию документа, подтверждающего оплату услуги РУЦ.

3.2.1.2. Регистрация подписчика для получения сертификата СР

Руководитель (представитель) ЮЛ, обратившегося в РУЦ, либо в РЦ, за оказанием услуги регистрации и издания сертификата СР, должен представить:

документ, удостоверяющий личность представителя ЮЛ, в соответствии с законодательством Республики Беларусь. Для иностранных граждан, имеющих документ, удостоверяющий личность без русскоязычного представления персональных данных, необходимо представить его заверенный в соответствии с законодательством Республики Беларусь перевод на русском языке;

перечень сведений о подписчике, подписанный руководителем ЮЛ и заверенный печатью (форма размещена на Интернет-сайте Оператора);

документ, подтверждающий полномочия руководителя на момент оказания услуги (типы документов указаны на Интернет-сайте Оператора) или доверенность (рекомендуемая форма приведена на Интернет-сайте Оператора), в случае наделения представителя полномочиями на выполнение действий от имени ЮЛ;

заверенную в соответствии с законодательством Республики Беларусь копию свидетельства о государственной регистрации или выписку из Единого государственного регистра ЮЛ и индивидуальных предпринимателей (во избежание выпуска сертификата на основании недостоверных (ошибочных) сведений о подписчике и последующей перерегистрации за счет подписчика, рекомендуется наряду с указанными выше документами представлять данный документ);

заверенную в соответствии с законодательством Республики Беларусь копию извещения о постановке на учет, подтверждающую учетный номер плательщика в органе Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь;

копию документа, подтверждающего оплату услуги РУЦ.

3.2.2. Возобновление действия сертификата и обновление данных

Возобновление действия сертификата осуществляется в соответствии с п.3.2.2. Регламента.

Последовательность действий подписчика и перечень представляемых им документов соответствует первичной регистрации (см. п.3.2.1. настоящей ППС).

Обновление данных сертификата не осуществляется.

3.2.3. Издание сертификатов ФЛ и СР.

Издание сертификатов ФЛ и СР осуществляется в соответствии с п.3.2.3. Регламента.

Образцы форматов сертификатов ФЛ и СР приведен в приложениях 1 и 2 к настоящей ППС.

3.2.4. Распространение нормативных и организационных документов

Распространение нормативных и организационных документов осуществляется в соответствии с п.3.2.4. Регламента.

РУЦ предоставляет доступ подписчикам и доверяющим сторонам к следующим нормативным и организационным документам РУЦ (в дополнение к указанным в Регламенте):

форматы сертификатов открытых ключей и атрибутных сертификатов, издаваемых РУЦ;

перечень идентификаторов объектов информационных технологий, использующихся в ГосСУОК;

рекомендуемая форма доверенности, типы иных документов, подтверждающих полномочия руководителя на момент оказания услуги;

перечни сведений о подписчике;

форма заявления об отзыве сертификата.

Оператор размещает данную информацию на своем Интернет-сайте.

3.2.5. Распространение сертификатов

Распространение сертификатов осуществляется в соответствии с п.3.2.5. Регламента.

Сведения о подлинности изданного сертификата любого подписчика могут быть предоставлены письменному запросу в установленном Оператором порядке.

РУЦ обеспечивает доступность информации о действительности и назначении сертификата всем пользователям ГосСУОК путем размещения СОС. 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.

Отзыв сертификата подписчика производится только при досрочном прекращении его действия в случае невозможности использования личного ключа подписчика (в случаях компрометации личного ключа или прекращения деятельности подписчиком).

Если о компрометации личного ключа подписчика сообщила третья сторона, то РУЦ запрашивает подтверждение данной информации непосредственно у подписчика – владельца личного ключа.

Запрашивать отзыв сертификата подписчика может только подписчик, для которого он выпущен.

Запросы, связанные с отзывом сертификата подписчика, идентифицируются и проверяются РУЦ на предмет их получения из достоверных источников.

РУЦ гарантирует, что сертификат подписчика отзывается только на основании заявления на отзыв подписчика в течении одного рабочего дня с момента получения оригинала заявления Оператором.

СОС издается РУЦ сразу же после обработки запроса на отзыв сертификата подписчика.

Услуги РУЦ по управлению отзывом сертификата подписчика доступна в течение рабочего времени регистраторов РУЦ (РЦ). В случае отказа системы, сервисов или при наличии других факторов, не зависящих от Оператора, предпринимаются все необходимые меры для того, чтобы данная информационная услуга была недоступна только в течение времени, оговоренного в Регламенте.

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

РУЦ 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.

РУЦ (РЦ) проверяет подлинность всей представленной подписчиком регистрационной информации в соответствии с порядком, установленным для первичной регистрации.

Форма заявления на отзыв сертификата подписчика приведена на Интернет-сайте Оператора.

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

3.2.7. Предоставление информации о статусе сертификата подписчика

Предоставление информации о статусе сертификата подписчика осуществляется в соответствии с п.3.2.7. Регламента.

Новый СОС может быть издан перед установленным временем издания следующего СОС. Например, внеочередной СОС издается РУЦ сразу же после обработки запроса на отзыв сертификата подписчика.

Актуальный СОС размещен на Интернет-сайте Оператора по адресу: http://nces.by/pki/certs/ .

3.3. Управление деятельностью РУЦ

3.3.1. Управление безопасностью

Управление безопасностью осуществляется в соответствии с п.3.3.1. Регламента.

3.3.2. Классификация и управление активами

Классификация и управление активами осуществляется в соответствии с п.3.3.2. Регламента.

3.3.3. Вопросы безопасности, связанные с персоналом

В соответствии с п.3.3.3. Регламента.

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

3.3.5. Управление операционной деятельностью

Управление операционной деятельностью осуществляется в соответствии с п.3.3.5. Регламента.

3.3.6. Управление системным доступом

Управление системным доступом осуществляется в соответствии с п.3.3.6. Регламента.

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.

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.

3.3.9. Прекращение функционирования РУЦ

Прекращение функционирования РУЦ осуществляется в соответствии с п.3.3.9. Регламента.

3.3.10. Соответствие требованиям законодательства

В соответствии с п.3.3.10. Регламента.

3.3.11. Сохранение информации, касающейся сертификатов

Сохранение информации, касающейся сертификатов осуществляется в соответствии с п.3.3.11. Регламента.

3.4. Организационные положения

В соответствии с п.3.4. Регламента.

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

Профиль формата сертификата физического лица

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

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

Состав базового компонента **tbsCertificate**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	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 абонентам 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***
calssuers	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	Назначение ключа: digitalSignature, nonRepudiation, keyEncipherment	постоянное	***111***
ExtendedKeyUsage	**2.5.29.37**	**Расширенное назначение ключа**		

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	Защита электронной почты	постоянное	

Состав базового компонента **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*	

* – поле не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013

Приложение 2

к Политике применения сертификатов открытых, изданных республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Профиль формата сертификата сервисов (сертификат СР)

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

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

Состав базового компонента **tbsCertificate**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	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 СР				
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	DNS-имя, IP-адрес сервера, ID сервера, устройства, процесса и т.п.	*Изменяемое*	
description	2.5.4.13 id-at- description	Общее наименование сервера, устройства, процесса и т.п.	*Изменяемое*	
organizationName	2.5.4.10 id-at-organizationName	Наименование организации –владельца сервера, устройства, процесса и т.п.	*Изменяемое*	
countryName	2.5.4.6 id-at-countryName	Код страны нахождения организации – владельца сервера, устройства, процесса и т.п.	*Изменяемое*	
stateOrProvinceName	2.5.4.8 id-at-stateOrProvinceName	Область нахождения организации – владельца сервера, устройства, процесса и т.п.	*Изменяемое* *	
localityName	2.5.4.7 id-at-localityName	Населённый пункт нахождения организации –владельца сервера, устройства, процесса и т.п.	*Изменяемое*	
streetAddress	2.5.4.9	Адрес нахождения организации – владельца сервера, устройства, процесса и т.п.	*Изменяемое*	

Идентификатор ГИС		Принадлежность к ГИС: Идентификаторы государственных информационных систем, зарегистрированных в Государственном регистре информационных систем согласно Постановления Совета Министров Республики Беларусь от 26 мая 2009 года №673 (http://infores.mpt.gov.by/it/database_is/). Имеет вид 1.2.112.1.2.1.1.A.BBBB.CC.DDDD, где: A – признак типа ИС (1-базовая ИС,2-республиканская ИС, 3-региональная ИС; BBBB – четырехзначный порядковый номер государственной регистрации создания ИС данного типа; CC – двузначный порядковый номер государственной регистрации изменений ИС; DDDD – четырехзначное значение года регистрации ИС.	*Изменяемое* *	
e-mailAddress	1.2.840.113549.1.9.1	Адрес электронной почты	*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**		
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 .1.3.2.2***
BasicConstraints	2.5.29.19	Конечный субъект. Означает принадлежность к абонентам 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	Назначение ключа: digitalSignature, nonRepudiation (только для DVCS и OCSP), dataEnchipherment, keyEncipherment, keyAgreement	Постоянное	***111***
ExtendedKeyUsage	**2.5.29.37**	**Расширенное назначение ключа**		
ClientAuth	1.3.6.1.5.5.7.3.2	TLS-аутентификация интернет-клиента	*Изменяемое* *	
ServerAuth	1.3.6.1.5.5.7.3.1	TLS-аутентификация интернет-сервера	*Изменяемое* *	
	1.3.6.1.5.5.7.3.10	Сервис доверенной третьей стороны: dvcs_by	*Изменяемое* *	
	1.3.6.1.5.5.7.3.8	Сервер меток точного времени: tsp_by	*Изменяемое* *	
	1.3.6.1.5.5.7.3.9	OCSP	*Изменяемое* *	

Состав базового компонента **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*	

* – поле не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013