Утверждена директором
государственного
предприятия «НЦЭУ»
06.10.2021

ПОЛИТИКА ПРИМЕНЕНИЯ СЕРТИФИКАТОВ ФИЗИЧЕСКИХ ЛИЦ

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

Минск
2021

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, владельцами которых являются физические лица (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) 311 30 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 (далее – Регламент).

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, в том числе для владельцев биометрических документов, удостоверяющих личность (далее – ИД-карта).

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.

Оператор республиканского удостоверяющего центра несет ответственность в соответствии с законодательством за соответствие процедурам, установленным настоящей политикой применения сертификатов, даже в случае выполнения услуг республиканского удостоверяющего центра по распространению открытых ключей регистрационными центрами.

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 пунктом 2.2. Регламента.

2.3. Требования к подписчикам

В качестве подписчика выступает физическое лицо, являющееся гражданином Республики Беларусь, иностранным гражданином или лицом без гражданства, и обращающееся к поставщику услуг от собственного имени за услугой издания сертификата открытого ключа, либо физическое лицо, подавшее заявление о выдаче (обмене) ИД-карты в соответствии с подпунктами 11.1-1, 11.2-1, 11.10, 11,11, 11.14, 11.15, 11.15-1, 11.15-2 пункта 11 перечня административных процедур, осуществляемых государственными органами и иными организациями по заявлениям граждан, утвержденного Указом Президента Республики Беларусь от 26 апреля 2010 г. № 200 (далее — Перечень-200).

Подписчик может самостоятельно выработать личный ключ и соответствующий ему открытый ключ с помощью сертифицированного средства электронной цифровой подписи или эти ключи подписчику вырабатывает поставщик услуг в случаях, предусмотренных законодательством Республики Беларусь.

Требования к подписчикам предъявляются в соответствии с пунктом 2.3. Регламента.

2.4. Требования к доверяющей стороне

Требования предъявляются в соответствии с пунктом 2.4. Регламента.

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 подпунктом 3.1.1. пункта 3.1. Регламента.

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 подпунктом 3.1.2. пункта 3.1. Регламента.

3.1.3. Распространение открытого ключа республиканского удостоверяющего центра

Распространение открытого ключа осуществляется в соответствии с подпунктом 3.1.3. пункта 3.1. Регламента.

3.1.4. Депонирование личного ключа республиканского удостоверяющего центра

Республиканский удостоверяющий центр не осуществляет депонирование личного ключа республиканского удостоверяющего центра, несмотря на то, что он осуществляют его резервное копирование.

3.1.5. Использование личного ключа республиканского удостоверяющего центра

Республиканский удостоверяющий центр использует свой личный ключ в соответствии с подпунктом 3.1.5 пункта 3.1. Регламента.

3.1.6. Окончание срока действия личного ключа республиканского удостоверяющего центра

Личный ключ республиканского удостоверяющего центра не используется по окончании его срока действия.

Уничтожение личного ключа республиканского удостоверяющего центра, его резервных копий осуществляется в соответствии с подпунктом 3.1.6. пункта 3.1. Регламента.

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

Управление средством электронной цифровой подписи, используемым для издания сертификатов физических лиц, осуществляется в соответствии с подпунктом 3.1.7. пункта 3.1. Регламента.

3.2. Требования по управлению сертификатами

3.2.1. Регистрация подписчика

3.2.1.1. Регистрация подписчика, который самостоятельно обратился к поставщику услуг

Регистрация подписчика осуществляется в соответствии с подпунктом 3.2.1. пункта 3.2. Регламента.

Первичная регистрация подписчика осуществляется при его личном посещении регистрационного центра.

При регистрации подписчика, лично прибывшего в регистрационный центр для издания сертификата, регистрационный центр должен:

идентифицировать физическое лицо, на основании представленных им документов, удостоверяющих личность;

зарегистрировать всю информацию, используемую для проверки личности физического лица, а также другие данные.

Личность физического лица проверяется на основании документа, удостоверяющего личность (информация, которая при этом подтверждается, – это фамилия и имя, дата рождения, идентификационный номер).

В отношении подписчиков (физических лиц) – резидентов Республики Беларусь регистрируется вся информация, однозначно идентифицирующая физическое лицо, а также информация о документе, удостоверяющем личность в соответствии с законодательством Республики Беларусь (серия и номер документа, дата выдачи и наименование органа, выдавшего такой документ), содержащаяся в самом документе, удостоверяющем личность, или в государственной информационной системе (ресурсе).

В отношении подписчиков (физических лиц) – нерезидентов Республики Беларусь регистрируются данные, имеющиеся в представленном документе, удостоверяющем личность.

Перечень документов, представляемых подписчиками, а также уточненный перечень регистрируемых данных определяется в порядке оказания услуг республиканского удостоверяющего центра.

После проверки документов и регистрации данных подписчиков осуществляется процедура формирования запроса на издание сертификата.

Запрос на издание сертификата физического лица подписчику, самостоятельно выработавшему личный ключ и соответствующий ему открытый ключ с помощью сертифицированного средства электронной цифровой подписи, осуществляется в порядке, определенном подпунктом 1.1 пункта 1 приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 8 февраля 2019 г. № 45.

3.2.1.2. Регистрация подписчика, подавшего заявление о выдаче (обмене) ИД-карты

Регистрация подписчика, подавшего заявление о выдаче (обмене) ИД-карты осуществляется подразделениями по гражданству и миграции органов внутренних дел или дипломатическими представительствами или консульскими учреждениями Республики Беларусь в ходе осуществления административных процедур, предусмотренных подпунктами 11.1-1, 11.2-1, 11.10, 11,11, 11.14, 11.15, 11.15-1 и 11.15-2 пункта 11 Перечня-200.

В этом случае генерация личных ключей и соответствующих им открытых ключей, а также формирование запросов на издание сертификатов открытых ключей осуществляется в соответствии с подпунктом 3.2.1 пункта 3.2 Регламента в процессе производства ИД-карты в ходе осуществления вышеуказанных административных процедур.

3.2.2. Возобновление действия сертификата и обновление данных

3.2.2.1. Возобновление действия сертификата и обновление данных (кроме размещенных на ИД-карте)

Возобновление действия сертификата физического лица осуществляется путем издания нового сертификата, в порядке, определенном в подпункте 3.2.3 пункта 3.2. настоящей политики применения сертификатов, сохранив без изменения информацию, содержащуюся в сертификате (кроме открытого ключа, срока действия сертификата и адреса электронной почты), предварительно убедившись, что на момент обращения она является действительной.

Обновление данных сертификата физического лица осуществляется путем отзыва действующего сертификата физического лица и издания нового сертификата физического лица в порядке, определенном в подпунктах 3.2.6, 3.2.3 пункта 3.2. настоящей политики применения сертификатов с внесением в издаваемый сертификат физического лица обновленной информации.

Последовательность действий регистрационного центра, подписчика и перечень представляемых подписчиком документов указаны в порядке оказания услуг республиканского удостоверяющего оператора.

3.2.2.2. Возобновление действия сертификатов и обновление данных, размещенных на ИД-карте

Возобновление действия сертификатов и обновление данных размещенных на ИД-карте не осуществляется.

3.2.3. Издание сертификатов

3.2.3.1 Издание сертификата физического лица подписчику, который самостоятельно обратился к поставщику услуг

Первичное издание подписчику сертификата физического лица осуществляется после проведения всех процедур регистрации подписчика в соответствии с подпунктом 3.2.1.1 пункта 3.2. настоящей политики применения сертификатов при его личном посещении регистрационного центра.

Порядок издания сертификатов физических лиц определен в подпункте 3.2.3 пункта 3.2. Регламента.

Состав сертификата физического лица определен в профилях (приложения 1 и 2 к настоящей политике применения сертификатов).

При наличии у подписчика действующего сертификата физического лица республиканским удостоверяющим центром может быть издан новый сертификат физического лица, содержащий новое значение открытого ключа подписчика, сохранив без изменения другую информацию, содержащуюся в действующем сертификате этого подписчика, после установления факта ее неизменности и актуальности. Новый сертификат физического лица может быть издан при личном посещении подписчиком регистрационного центра, либо посредством личного кабинета на едином портале электронных услуг https://portal.gov.by.

При издании нового сертификата физического лица посредством регистрационного центра подписчик представляет данные, определенные в подпункте 3.2.1.1 пункта 3.2. настоящей политики применения сертификатов. Подлинность всей представленной подписчиком регистрационной информации проверяет регистрационный центр, в который обратился подписчик в соответствии с порядком, установленным для первичной регистрации.

Издание нового сертификата физического лица посредством личного кабинета на едином портале электронных услуг осуществляется в порядке, определенном в подпункте 3.2.3 Регламента и порядком оказания услуг. При этом новый сертификат открытого ключа может быть издан, если актуальность и неизменность всей информации, содержащейся в сертификате подписчика, будет подтверждена информацией из базовых государственных информационных ресурсов, интегрированных в общегосударственную автоматизированную информационную систему. После издания нового сертификата физического лица подписчик обязан осуществить вход в личный кабинет с использованием нового сертификата физического лица для подтверждения принадлежности ему это открытого ключа.

При установлении факта изменения фамилии, имени, отчества подписчика действующий сертификат открытого ключа с неактуальными данными подлежит отзыву.

3.2.3.2 Издание сертификатов физического лица подписчику, подавшему заявление о выдаче (обмене) ИД-карты

Издание сертификатов физического лица подписчику, подавшему заявление о выдаче (обмене) осуществляется в соответствии с подпунктом 3.2.3 пункта 3.2. Регламента в автоматическом режиме в процессе производства ИД-карты в ходе осуществления административных процедур, предусмотренных подпунктами 11.1-1, 11.2-1, 11.10, 11,11, 11.14, 11.15, 11.15-1 и 11.15-2 пункта 11 Перечня-200.

Для одного подписчика издается два сертификата физического лица для проверки подписи, выработанной в базовом и терминальном режиме.

3.2.4. Распространение организационно-распорядительных документов

Распространение организационно-распорядительных документов осуществляется в соответствии с подпунктом 3.2.4. пункта 3.2. Регламента.

3.2.5. Распространение сертификатов

3.2.5.1. Распространение сертификатов, кроме размещенных на ИД-карте

Распространение сертификатов осуществляется в соответствии с подпунктом 3.2.5. пункта 3.2. Регламента.

Распространение подписчикам изданных им сертификатов физических лиц осуществляется путем передачи подписчикам реквизитов (адрес в сети Интернет, уникальные логин и пароль) доступа к облачному хранилищу сертификатов, в котором располагаются необходимое программное обеспечение, изданные сертификаты и инструкции.

Логин и пароль для входа в облачное хранилище являются набором случайно сгенерированных символов, который подписчик получает после издания сертификата следующим образом, если иной порядок не предусмотрен в порядке оказания услуг республиканского удостоверяющего центра:

на бумажном носителе от работника регистрационного центра, если услуга оказывается в регистрационном центре;

отображается в личном кабинете единого портала электронных услуг, а также высылается на указанные подписчиком адрес электронной почты и номер мобильного телефона (SMS-сообщение), если услуга оказывается посредством личного кабинета на едином портале электронных услуг https://portal.gov.by.

Распространение сертификатов доверяющим сторонам осуществляется владельцем сертификата, либо оператором по письменному запросу.

Сведения о подлинности изданного сертификата любого подписчика могут быть предоставлены оператором по письменному запросу.

3.2.5.2. Распространение сертификатов, размещенных на ИД-карте

Распространение сертификатов осуществляется путем их записи на ИД-карту в ходе осуществления административных процедур, предусмотренных подпунктами 11.1-1, 11.2-1, 11.10, 11,11, 11.14, 11.15, 11.15-1, 11.15-2 Перечня-200.

На ИД-карту одного подписчика записываются два сертификата для проверки подписи, выработанной в базовом и терминальном режиме.

3.2.6. Отзыв сертификата

3.2.6.1. Отзыв сертификата, не принадлежащего владельцу ИД-карты

Отзыв сертификата осуществляется в соответствии с подпунктом 3.2.6. пункта 3.2. Регламента.

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 органов внутренних дел (в случае смерти владельца личного ключа). Запрашивать отзыв сертификата подписчика должен 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. Сразу же после обработки запроса на отзыв сертификата республиканским удостоверяющим центром издается список отозванных сертификатов.

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.

3.2.6.2. Отзыв сертификатов, принадлежащих владельцу ИД-карты

В случае признания ИД-карты недействительной в соответствии с пунктом 10 Положения о биометрических документах, удостоверяющих личность, утвержденного Указом Президента Республики Беларусь от 3 июня 2008 г. №294 (в редакции Указа Президента Республики Беларусь от 16 марта 2021 г. №107) до истечения срока ее действия Министерство внутренних дел представляет сведения о таком документе оператору РУЦ в целях осуществления им процедуры отзыва сертификата открытого ключа в соответствии с согласованным регламентом информационного взаимодействия в порядке, определенном законодательством.

3.2.7. Предоставление информации о статусе сертификата подписчика

Предоставление информации о статусе сертификата подписчика осуществляется в соответствии с подпунктом 3.2.7. пункта 3.2. Регламента.

3.3. Управление деятельностью республиканского удостоверяющего центра

3.3.1. Управление безопасностью

Управление безопасностью осуществляется в соответствии с подпунктом 3.3.1. пункта 3.3. Регламента.

3.3.2. Классификация и управление активами

Классификация и управление активами осуществляется в соответствии с подпунктом 3.3.2. пункта 3.3. Регламента.

3.3.3. Вопросы безопасности, связанные с персоналом

В соответствии с подпунктом 3.3.3. пункта 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 подпунктом 3.3.4. пункта 3.3. Регламента.

3.3.5. Управление операционной деятельностью

Управление операционной деятельностью осуществляется в соответствии с подпунктом 3.3.5. пункта 3.3. Регламента.

3.3.6. Управление системным доступом

Управление системным доступом осуществляется в соответствии с подпунктом 3.3.6. пункта 3.3. Регламента.

3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем

Внедрение и обслуживание безопасных доверенных информационных систем осуществляется в соответствии с подпунктом 3.3.7. пункта 3.3. Регламента.

3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности

Восстановление при сбоях и обеспечение непрерывности деятельности осуществляется в соответствии с подпунктом 3.3.8. пункта 3.3. Регламента.

3.3.9. Прекращение функционирования республиканского удостоверяющего центра

Прекращение функционирования республиканского удостоверяющего центра осуществляется в соответствии с подпунктом 3.3.9. пункта 3.3. Регламента.

3.3.10. Соответствие требованиям законодательства

В соответствии с подпунктом 3.3.10. пункта 3.3. Регламента.

3.3.11. Сохранение информации, касающейся сертификатов

Сохранение информации, касающейся сертификатов осуществляется в соответствии с подпунктом 3.3.11. пункта 3.3. Регламента.

3.4. Организационные положения

В соответствии с пунктом 3.4. Регламента.

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

Приложение 2
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 для ID-карты (базового и терминального)

Сертификат ФЛ 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 и Идентификационный (личный) номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т. д.)	*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*	
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)		
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		***1.2.112.1.2.1.1.1.4.2 (Фамилия физического лица на белорусском языке) 1.2.112.1.2.1.1.1.4.3 (Имя физического лица на белорусском языке) 1.2.112.1.2.1.1.1.4.4 (Отчество физического лица на белорусском языке)***

certificatePolicies	2.5.29.32	В поле *certificatePolicies* устанавливается три OID: Первый OID политики применения сертификатов, в соответствии с которой был издан сертификат открытого ключа - **1.2.112.1.2.1.1.1.3.2.1;** Второй OID типа носителя криптографического ключа – ID-карта; Третий OID роли в префиксе **bpki-role** согласно СТБ 34.101.78 в зависимости от вида персонализируемой ID-карты (смотри столбец «Постоянные значения»)		***1.2.112.0.2.0.34.101.78.2.60.1 — сертификаты открытого ключа на идентификационной карте гражданина Республики Беларусь;*** ***1.2.112.0.2.0.34.101.78.2.60.2 — сертификаты открытого ключа на биометрическом виде на жительство в Республике Беларусь иностранного гражданина;*** ***1.2.112.0.2.0.34.101.78.2.60.3 — сертификаты открытого ключа на биометрическом виде на жительство в Республике Беларусь лица без гражданства.***
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*	http://nces.by/wp-content/uploads/certificates/pki/ruc.crl
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**	
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	*изменяемое*	http://nces.by/wp-content/uploads/certificates/pki/ruc.cer
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	

ClientTM		Обозначение стороны, которая выступает в роли клиента при терминальном режиме в профиле **bpki-eku** согласно СТБ 34.101.78-2019	изменяемое*	***1.2.112.0.2.0.34.101.78.3.2***

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*	

* – не обязательно для заполнения.

** – в случае отсутствия отчества соответствующего элемента 2.5.4.42 и 1.2.112.1.2.1.1.1.4.4 исключается из структуры с фамилией, именем и отчеством.

*** – соответствуют требованиям СТБ 34.101.45-2013.