

УТВЕРЖДАЮ

Директор республиканского
унитарного предприятия
«Национальный центр
электронных услуг»



А.А. Ильин

2016 г.

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

Минск
2016

СОДЕРЖАНИЕ

1. Введение в политику применения сертификатов.....	4
1.1. Общие положения	4
1.2. Идентификация	5
1.3. Пользователи политики применения сертификатов.....	6
2. Требования к участникам инфраструктуры открытых ключей	7
2.1. Требования к РУЦ	7
2.2. Требования к РЦ	7
2.3. Требования к подписчикам	7
2.4. Требования к доверяющей стороне	8
3. Требования к РУЦ.....	9
3.1. Требования по управлению ключами.....	9
3.1.1. Выработка личного ключа РУЦ.....	9
3.1.2. Хранение, резервное копирование и восстановление личного ключа РУЦ.....	9
3.1.3. Распространение открытого ключа РУЦ	9
3.1.4. Депонирование личного ключа РУЦ.....	9
3.1.5. Использование личного ключа	9
3.1.6. Окончание срока действия личного ключа РУЦ.....	9
3.1.7. Управление средством ЭЦП, используемым для издания сертификатов.....	9
Управление средством ЭЦП, используемым для издания сертификатов осуществляется в соответствии с п.3.1.7. Регламента	9
3.2. Требования по управлению сертификатами.....	9
3.2.1. Регистрация владельца сертификата ЮЛ, издаваемого РУЦ.....	9
3.2.1.1. Регистрация подписчика для получения сертификата ЮЛ	10
3.2.2. Возобновление действия сертификата и обновление данных	11
3.2.3. Издание сертификата ЮЛ.....	11
3.2.4. Распространение нормативных и организационных документов	11
3.2.5. Распространение сертификатов ЮЛ	11
3.2.6. Отзыв и приостановка действия сертификата ЮЛ.....	11
3.2.7. Предоставление информации о статусе сертификата ЮЛ.....	12
3.3. Управление деятельностью РУЦ	13
3.3.1. Управление безопасностью	13
3.3.2. Классификация и управление активами	13
3.3.3. Вопросы безопасности, связанные с персоналом	13
3.3.4. Физическая защита и защита от воздействий окружающей среды	13
3.3.5. Управление операционной деятельностью.....	13
3.3.6. Управление системным доступом	13
3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем	13

3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности.....	13
3.3.9. Прекращение функционирования РУЦ.....	13
3.3.10. Соответствие требованиям законодательства.....	14
3.3.11. Сохранение информации, касающейся сертификатов	14
3.4. Организационные положения	14
Приложение 1	17

1. Введение в политику применения сертификатов

1.1. Общие положения

Настоящая политика применения сертификатов юридических лиц (далее - ЮЛ) республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ППС ЮЛ) 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 юридических лиц (далее – сертификат) и списков отозванных сертификатов (далее – СОС), а также по управлению статусом сертификатов. РУЦ является подчиненным удостоверяющим центром корневого удостоверяющего центра ГосСУОК.

ППС ЮЛ 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 настоящей ППС ЮЛ 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 атрибутивных сертификатов, физических лиц, сервисов (приложения, серверы или устройства);

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 Политикам применения сертификатов РУЦ.

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 РУЦ ГосСУОК (далее – Регламент).

1.2. Идентификация

ППС ЮЛ имеет следующий объектный идентификатор (Object Identifier, OID): {1.2.112.1.2.1.1.1.3.2}

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 ЮЛ, изданные в соответствии с данной ППС ЮЛ, 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.

Настоящая ППС ЮЛ 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 ЮЛ.

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

Положения Регламента не должны противоречить ППС ЮЛ.

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 ЮЛ, Регламентом РУЦ, регламентом работы, согласованным с РУЦ.

РЦ должен осуществлять проверку информации, вносимой в ЮЛ, формирование заявок на издание и отзыв сертификата ЮЛ, передачу конечным пользователям изданных сертификатов ЮЛ 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 ЮЛ 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 ЮЛ и регламенту РЦ.

2.3. Требования к подписчикам

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 ЮЛ, доверяющая сторона должна:

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

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

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 ЮЛ, 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/ВУ) 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 ЮЛ

ЮЛ, обратившееся в РУЦ либо в РЦ за оказанием услуги регистрации и издания сертификата ЮЛ, 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, подписанный руководителем ЮЛ и заверенный печатью (форма размещена на Интернет-сайте Оператора), заполненный разборчиво на русском языке;

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 и обновление данных 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 ЮЛ).

3.2.3. Издание сертификата ЮЛ.

Издание сертификата ЮЛ осуществляется в соответствии с п.3.2.3. Регламента.

Образец формата сертификата ЮЛ приведен в приложении 1 к настоящей ППС ЮЛ.

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):

- 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 ЮЛ

Распространение сертификатов ЮЛ 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 и приостановка действия сертификата ЮЛ

Отзыв и приостановка действия сертификата ЮЛ осуществляется в соответствии с п.3.2.6. Регламента.

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

Если о компрометации личного ключа субъекта (подписчика) сообщила третья сторона, то РУЦ приостанавливает действие сертификата ЮЛ и запрашивает подтверждение данной информации непосредственно у подписчика.

Запросы, связанные с отзывом сертификата ЮЛ, идентифицируются и проверяются РУЦ на предмет их получения из достоверных источников. Сертификат ЮЛ считается приостановленным до тех пор, пока не будет подтвержден его отзыв.

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

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

Услуга РУЦ по управлению отзывом сертификата ЮЛ 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 ЮЛ доступна до истечения срока действия этого сертификата, установленного при его издании.

Форма заявления на отзыв сертификата ЮЛ 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 ЮЛ

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

Профиль формата сертификата юридического лица

Сертификат юридического лица в соответствии с СТБ 34.101.19 состоит из трех базовых компонентов:
tbsCertificate;
signatureAlgorithm;
signatureValue

Состав базового компонента **tbsCertificate**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
version		Версия формата сертификата по х.509. В текущей локализации используется Version3	постоянное	2
serialNumber		Уникальный серийный номер сертификата. Положительное целое число, не превышающее значение более 20 октетов	<i>изменяемое</i>	
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 <i>NULL</i>	постоянное	<i>NULL</i>
issure		Эмитент (издатель, субъект). Идентифицирует субъект, который подписал и выдал сертификат		
Набор полей и их значений совпадает с набором и значениями полей компонента subject в сертификате УЦ, издавшем данный сертификат				
validity		Срок действия сертификата.		
notBefore		Дата начала срока действия сертификата (согласно п.6.1.2.5 СТБ 34.101.19-2012)	<i>изменяемое</i>	
afterBefore		Дата окончания срока действия сертификата (согласно п.6.1.2.5 СТБ 34.101.19-2012)	<i>изменяемое</i>	
subject				

organizationName	2.5.4.10 id-at-organizationName	Наименование организации	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 и 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	
Подразделение	1.2.112.1.2.1.1.5.2	Наименование структурного подразделения	изменяемое	
title	2.5.4.12 id-at-title	Должность	изменяемое	
countryName	2.5.4.6 id-at-contryName	Страна (код страны) — гражданство физического лица	изменяемое	
localityName	2.5.4.7 id-at-localityName	Наименование населенного пункта	изменяемое	
stateOrProvinceName	2.5.4.8 id-at-stateOrProvinceName	Наименование области	изменяемое	
streetAddress	2.5.4.9 id-at- streetAddress	Юридический адрес организации	изменяемое	
УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП), присвоенный юридическому лицу МЧС РБ для которого устанавливается связь с физическим лицом	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 <i>bign-pubkey</i>	постоянное	1.2.112.0.2.0.34.101.45.2.1
parameters		Параметры открытого ключа, в данном профиле для <i>bign-curve256v1</i>	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)	<i>изменяемое</i>	
KeyUsage	2.5.29.15	Назначение ключа: digitalSignature, nonRepudiation, keyEncipherment	постоянное	<i>III</i>
certificatePolicies	2.5.29.32	Политика, в соответствии с которой был издан и может применяться сертификат	постоянное	<i>1.2.112.1.2.1.1 .1.3.2.1</i>
CRLDistributionPoints	2.5.29.31	Точка распространения СОС. URL-адрес веб-ресурса РУЦ, на котором располагается актуальный СОС	<i>изменяемое</i>	
AuthorityInfoAccess OCSP	1.3.6.1.5.5.7.48.1	Содержит указатель на OCSP сервис УЦ	<i>Изменяемое*</i>	
AuthorityInfoAccess caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	<i>Изменяемое</i>	

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 big-with-hbelt согласно СТБ 34.101.45-2013	постоянное	<i>1.2.112.0.2.0.34.101.45.12</i>
parameters		Параметры алгоритма. Значение поля <i>NULL</i>	постоянное	<i>NULL</i>

Состав базового компонента **signatureValue**

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

*- поле не обязательно для заполнения