

**Утверждена директором
государственного
предприятия «НЦЭУ»
06.06.2022**

С изменениями от 06.11.2024

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

Минск
2022

СОДЕРЖАНИЕ

1. Введение в политику применения сертификатов.....	4
1.1. Общие положения	4
1.2. Идентификация.....	5
1.3. Пользователи политики применения сертификатов.....	5
2. Требования к участникам инфраструктуры открытых ключей.....	5
2.1. Требования к республиканскому удостоверяющему центру	5
2.2. Требования к регистрационному центру	6
2.3. Требования к подписчикам	6
2.4. Требования к доверяющей стороне.....	6
3. Требования к республиканскому удостоверяющему центру.....	6
3.1. Требования по управлению ключами	6
3.1.1. Выработка личного ключа республиканского удостоверяющего центра	6
3.1.2. Хранение, резервное копирование и восстановление личного ключа республиканского удостоверяющего центра.....	7
3.1.3. Распространение открытого ключа республиканского удостоверяющего центра.....	7
3.1.4. Депонирование личного ключа республиканского удостоверяющего центра.....	7
3.1.5. Использование личного ключа республиканского удостоверяющего центра.....	7
3.1.6. Окончание срока действия личного ключа республиканского удостоверяющего центра.....	7
3.1.7. Управление средством электронной цифровой подписи, используемым для издания сертификатов.....	7
3.2. Требования по управлению сертификатами.....	8
3.2.1. Регистрация подписчика.....	8
3.2.2. Возобновление действия сертификата и обновление данных.....	8
3.2.3. Издание сертификатов	9
3.2.4. Распространение организационно-распорядительных документов	9
3.2.5. Распространение сертификатов	9
3.2.6. Отзыв сертификата.....	9
3.2.7. Предоставление информации о статусе сертификата	10
3.3. Управление деятельностью республиканского удостоверяющего центра	10
3.3.1. Управление безопасностью.....	11
3.3.2. Классификация и управление активами	11
3.3.3. Вопросы безопасности, связанные с персоналом	11

3.3.4. Физическая защита и защита от воздействий окружающей среды	11
3.3.5. Управление операционной деятельностью	11
3.3.6. Управление системным доступом	11
3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем.....	11
3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности	11
3.3.9. Прекращение функционирования республиканского удостоверяющего центра.....	11
3.3.10. Соответствие требованиям законодательства.....	12
3.3.11. Сохранение информации, касающейся сертификатов	12
3.4. Организационные положения	12
Приложение 1	13
Приложение 2	17
Приложение 3	21
Приложение 4.....	26

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 технологических сертификатов открытых ключей 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. № 113-3 «Об электронном документе и электронной цифровой подписи», СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата», 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 атрибутивных сертификатов», СТБ 34.101.69-2014 «Информационные технологии и безопасность. Криптология. Термины и определения», СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

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, 220140, г.Минск, ул.Притыцкого, 64.

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 (далее – РУЦ) 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) techn(2)} – (1.2.112.1.2.1.1.1.3.2.2).

Данные объектные идентификаторы включаются в соответствии с требованиями СТБ 34.101.19-2012 в расширение certificatePolicies сертификатов открытых ключей, издаваемых республиканским удостоверяющим центром.

1.3. Пользователи политики применения сертификатов

Настоящая политика применения сертификатов применяется для издаваемых республиканским удостоверяющим центром технологических сертификатов открытых ключей (сертификатов открытых ключей криптографических автоматов).

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

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

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

Подписчик с помощью средства электронной цифровой подписи, имеющего сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь вырабатывает личный ключ, соответствующий ему открытый ключ и формирует запрос на издание технологического сертификата открытого ключа (в виде файла). После этого оформляет заявку на издание технологического сертификата открытого ключа, которую с соответствующим файлом запроса отправляет оператору республиканского удостоверяющего центра посредством системы межведомственного электронного документооборота государственных органов Республики Беларусь, либо посредством автоматизированной системы технической поддержки пользователей услуг НЦЭУ (<https://support.nces.by/>). В заявке на издание технологического сертификата открытого ключа указывается адрес электронной почты подписчика для обратной связи.

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 осуществляет 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.

Личный ключ республиканского удостоверяющего центра используется не позднее чем за три года окончания срока действия сертификата открытого ключа республиканского удостоверяющего центра.

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 технологических сертификатов открытых ключей, осуществляется в соответствии с подпунктом 3.1.7. пункта 3.1. Регламента.

3.2. Требования по управлению сертификатами

3.2.1. Регистрация подписчика

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

Оказание услуг по изданию сертификатов открытых ключей осуществляется без обязательного личного присутствия подписчика.

Оператор осуществляет необходимые мероприятия для оказания подписчику услуг республиканского удостоверяющего центра в соответствии с Регламентом при наличии:

корректно оформленных документов, необходимых для оказания технологических услуг республиканского удостоверяющего центра;

представленной подписчиком полной и достоверной информации;

корректно сформированного файла запроса в соответствии с подпунктом 2.3 пункта 2 настоящей политики. Файл запроса, в зависимости от типа технологического сертификата открытого ключа должен соответствовать профилям форматов сертификатов, отраженным в приложениях к данной политике применения сертификатов.

В противном случае заявка на получение услуги аннулируется оператором с последующим уведомлением об этом подписчика на адрес электронной почты.

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

3.2.2. Возобновление действия сертификата и обновление данных

Возобновление действия технологического сертификата открытого ключа (сертификата открытого ключа криптографического автомата) 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 технологического сертификата открытого ключа (сертификата открытого ключа криптографического автомата) осуществляется путем отзыва действующего сертификата открытого ключа и издания нового сертификата открытого ключа в порядке, определенном в подпунктах 3.2.3, 3.2.6 пункта 3.2. настоящей политики применения сертификатов с внесением в издаваемый сертификат открытого ключа обновленной информации.

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

3.2.3. Издание сертификатов

Первичное издание подписчику технологического сертификата открытого ключа (сертификата открытого ключа криптографического автомата) осуществляется после проведения всех процедур регистрации подписчика в соответствии с подпунктом 3.2.1 пункта 3.2. настоящей политики применения сертификатов.

Порядок издания технологических сертификатов открытых ключей (сертификатов открытых ключей криптографических автоматов) определен в подпункте 3.2.3 пункта 3.2. Регламента.

Профили форматов технологических сертификатов открытых ключей определены в следующих приложениях:

- профиль формата технологического сертификата открытого ключа для комплекса программных средств прикладной системы (КПСИС) – приложение 1;
- профиль формата сертификата открытого ключа криптографического автомата – приложение 2;
- профиль технологического сертификата открытого ключа OCSP-сервера, службы штампа времени, службы заверения данных, доверенной третьей стороны, сервера идентификации, TLS – приложение 3;
- профиль формата технологического сертификата открытого ключа для программного комплекса создания объектов безопасности (ПК СОБ) – приложение 4.

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

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

Распространение подписчикам изданных им сертификатов открытых ключей осуществляется посредством электронной почты.

3.2.6. Отзыв сертификата

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) или изменения сведений, влияющих на содержание сертификата.

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.

Подписчик может подавать заявление как на бумажном носителе, так и в виде электронного документа.

Если 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

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

Безопасность, связанная с персоналом, осуществляется 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

Соответствие требованиям законодательства проводится 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

Организационные положения выполняются в соответствии с пунктом 3.4. Регламента.

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

Профиль формата технологического сертификата открытого ключа для комплекса программных средств прикладной системы (КПСИС)

Сертификат Сервиса 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 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 NULL**	постоянное	NULL**
issuer		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 Сервиса				
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				
commonName	2.5.4.3 id-at-commonName	DNS-имя, IP-адрес сервера, ID сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
countryName	2.5.4.6 id-at-countryName	Код страны нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
localityName	2.5.4.7 id-at-localityName	Населённый пункт нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
stateOrProvinceName	2.5.4.8 id-at-stateOrProvinceName	Область нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
streetAddress	2.5.4.9	Адрес нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
organizationName	2.5.4.10 id-at-organizationName	Наименование организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
organizationUnitName	2.5.4.11 id-at-organizationUnitName	Наименование подразделения организации- владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
description	2.5.4.13 id-at- description	Общее наименование сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
e-mailAddress	1.2.840.113549.1.9.1	Адрес электронной почты	<i>изменяемое*</i>	
subjectPublicKeyInfo				
algorithm		ИДЕНТИФИКАТОР алгоритма, с которым используется открытый ключ, в данном профиле <i>bign-pubkey</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.2.1</i>
parameters		Параметры открытого ключа, в данном профиле для <i>bign-curve256v1</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.3.1</i>
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>	
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа эмитента (издателя) (представляет хэш-значение SHA-1 20 байт согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	постоянное	
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 – политика применения сертификатов РУЦ ГосСУОК выпускающего СОК КА; 1.2.112.0.2.0.34.101.78.2.50 – СОК TLS-сервера; 1.2.112.0.2.0.34.101.78.2.70 – СОК КА;
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	<i>изменяемое*</i>	
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	<i>изменяемое*</i>	
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	<i>изменяемое*</i>	
KeyUsage	2.5.29.15	Назначение ключа (по согласованию с подписчиком может быть установлен одно или несколько назначений): digitalSignature, keyEncipherment, keyAgreement	Постоянное	10101
subjectAltName	2.5.29.17 id-ce-subjectAltName	Расширение сертификата, содержащее одно или несколько значений альтернативных имен субъекта (DNS-имя), используется только для TLS-сертификатов		

УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП), присвоенный МНС РБ	<i>изменяемое</i>	
ExtendedKeyUsage***	2.5.29.37	Расширенное назначение ключа		
ServerAuth	1.3.6.1.5.5.7.3.1	TLS-аутентификация интернет-сервера	<i>изменяемое*</i>	
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	<i>изменяемое</i>	

* – не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013

*** – по согласованию с заинтересованными организациями для целей использования в конкретной информационной системе поле может быть дополнено другими OID

Приложение 2
к Политике применения технологических сертификатов открытых ключей республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Профиль формата технологического сертификата открытого ключа криптографического автомата

Сертификат Сервиса 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 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 big-n-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**
issuer		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 Сервиса

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				
commonName	2.5.4.3 id-at-commonName	DNS-имя, IP-адрес сервера, ID сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
countryName	2.5.4.6 id-at-countryName	Код страны нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
localityName	2.5.4.7 id-at-localityName	Населённый пункт нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
stateOrProvinceName	2.5.4.8 id-at-stateOrProvinceName	Область нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
streetAddress	2.5.4.9	Адрес нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
organizationName	2.5.4.10 id-at-organizationName	Наименование организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
description	2.5.4.13 id-at-description	Общее наименование сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
e-mailAddress	1.2.840.113549.1.9.1	Адрес электронной почты	<i>изменяемое*</i>	
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)	изменяемое	
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа эмитента (издателя) (представляет хэш-значение SHA-1 20 байт согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	постоянное	
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 – политика применения сертификатов РУЦ ГосСУОК выпускающего СОК КА
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*	
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	изменяемое*	
KeyUsage	2.5.29.15	Назначение ключа (по согласованию с подписчиком может быть установлен одно или несколько назначений): digitalSignature, nonrepudiation, keyEncipherment, keyAgreement	Постоянное	11101
subjectAltName	2.5.29.17 id-ce-subjectAltName	Расширение сертификата, содержащее одно или несколько значений альтернативных имен субъекта (DNS-имя), используется только для TLS-сертификатов		
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*	
emailProtection	1.3.6.1.5.5.7.3.4	Защита электронной почты	постоянное	

	1.3.6.1.5.5.7.3.10	Сервис доверенной третьей стороны: dvcs_by	<i>изменяемое*</i>	
	1.3.6.1.5.5.7.3.8	Сервер меток точного времени: tsp_by	<i>изменяемое*</i>	
	1.3.6.1.5.5.7.3.9	OCSP	<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	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	<i>изменяемое</i>	

* – не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013

*** – по согласованию с заинтересованными организациями для целей использования в конкретной информационной системе поле может быть дополнено другими OID

Приложение 3
к Политике применения технологических сертификатов открытых ключей республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

**Профиль формата технологического сертификата открытого ключа
службы предоставления информации о действительности сертификатов и атрибутивных сертификатов (OCSP-сервер),
службы штампа времени, службы заверения данных, доверенной третьей стороны, сервера идентификации, TLS**

Сертификат Сервиса 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 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 big-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**
issuer		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 Сервиса

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				
commonName	2.5.4.3 id-at-commonName	DNS-имя, IP-адрес сервера, ID сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
countryName	2.5.4.6 id-at-countryName	Код страны нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое</i>	
localityName	2.5.4.7 id-at-localityName	Населённый пункт нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
stateOrProvinceName	2.5.4.8 id-at-stateOrProvinceName	Область нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
streetAddress	2.5.4.9	Адрес нахождения организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
organizationName	2.5.4.10 id-at-organizationName	Наименование организации – владельца сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	
description	2.5.4.13 id-at-description	Общее наименование сервера, устройства, процесса и т.п.	<i>изменяемое*</i>	

Идентификатор ГИС		<p>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: А – 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.</p>	<i>изменяемое*</i>	
e-mailAddress	1.2.840.113549.1.9.1	Адрес электронной почты	<i>изменяемое*</i>	
subjectPublicKeyInfo				
algorithm		ИДЕНТИФИКАТОР алгоритма, с которым используется открытый ключ, в данном профиле <i>bign-pubkey</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.2.1</i>
parameters		Параметры открытого ключа, в данном профиле для <i>bign-curve256v1</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.3.1</i>
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>	
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа эмитента (издателя) (представляет хэш-значение SHA-1 20 байт согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	постоянное	

certificatePolicies	2.5.29.32	Политика, в соответствии с которой был издан и может применяться сертификат	постоянное	1.2.112.0.2.0.34.101.78.2.30 — СОК OCSP сервера; 1.2.112.0.2.0.34.101.78.2.31 — СОК сервера штампа времени; 1.2.112.0.2.0.34.101.78.2.32 — СОК службы заверения данных; 1.2.112.0.2.0.34.101.78.2.33 — СОК сервера идентификации; 1.2.112.0.2.0.34.101.78.2.50 — СОК TLS-сервера
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*	
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	изменяемое*	
KeyUsage	2.5.29.15	Назначение ключа (по согласованию с подписчиком может быть установлен одно или несколько назначений): digitalSignature, nonRepudiation (только для DVCS, OCSP и КА), keyEncipherment, keyAgreement	постоянное	11101
subjectAltName	2.5.29.17 id-ce-subjectAltName	Расширение сертификата, содержащее одно или несколько значений альтернативных имен субъекта (DNS-имя), используется только для TLS-сертификатов		
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*	

emailProtection	1.3.6.1.5.5.7.3.4	Защита электронной почты	постоянное	
	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 big-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

*** – по согласованию с заинтересованными организациями для целей использования в конкретной информационной системе поле может быть дополнено другими OID

Приложение 4
к Политике применения технологических сертификатов открытых ключей республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Профиль формата технологического сертификата открытого ключа для программного комплекса создания объектов безопасности (ПК СОБ)

Сертификат ОРГ 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 x.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 sign-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
issuer		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	<i>изменяемое</i>	
countryName	2.5.4.6 id-at-contryName	Страна (код страны)	<i>изменяемое</i>	
subjectPublicKeyInfo				
algorithm		ИДЕНТИФИКАТОР алгоритма, с которым используется открытый ключ, в данном профиле <i>bign-pubkey</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.2.1</i>
parameters		Параметры открытого ключа, в данном профиле для <i>bign-curve256v1</i>	постоянное	<i>1.2.112.0.2.0.34.101.45.3.1</i>
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>	
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа эмитента (издателя) (представляет хэш-значение SHA-1 20 байт согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	постоянное	
KeyUsage	2.5.29.15	Назначение ключа: digitalSignature	постоянное	<i>1</i>
certificatePolicies	2.5.29.32	Политика, в соответствии с которой был издан и может применяться сертификат	постоянное	<i>1.2.112.0.2.0.34.101.78.2.71</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>	
УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП), присвоенный Министерством по налогам и сборам Республики Беларусь	<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	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	<i>изменяемое</i>	

*- не обязательно для заполнения