**Утверждена директором
государственного
предприятия «НЦЭУ»
12.04.2024**

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

Минск
2024

СОДЕРЖАНИЕ

1. Введение в политику применения атрибутных сертификатов

1.1. Общие положения

Настоящая политика применения атрибутных сертификатов республиканского удостоверяющего центра (далее – РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) (далее – ППАС) является документом, содержащим описание услуг, которые оказывает центр атрибутных сертификатов (далее – ЦАС) по изданию, распространению, отзыву, хранению атрибутных сертификатов (далее – АС), и списков отозванных АС (далее – СОАС), а также по управлению статусом АС.

Функции ЦАС осуществляет РУЦ.

ППАС разработана в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров» (далее – СТБ 34.101.48-2012), Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10.12.2015 № 118 (далее – Положение о ГосСУОК), и устанавливает принципы деятельности РУЦ на основе систематизированного изложения процессов и процедур оказания услуг, но не содержит их подробного описания.

Для целей ППАС термины и их определения используются в значениях, установленных Законом Республики Беларусь от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой подписи», Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16.04.2013 № 196, Положением о ГосСУОК, государственным стандартом Республики Беларусь СТБ 34.101.48-2012 и другими техническими нормативными правовыми актами.

Основными функциями РУЦ являются:

генерация личных и открытых ключей РУЦ;

управление сертификатами открытых ключей (далее – СОК) физических лиц, включая индивидуальных предпринимателей (далее – ФЛ), и организаций, в том числе государственных органов и других государственных организаций (далее – организации), регистрационных центров (далее – РЦ), ЦАС, службы предоставления информации о действительности СОК и АС (OCSP-сервер), службы штампа времени, службы заверения данных, доверенной третьей стороны, сервера идентификации, TLS;

удостоверение формы внешнего представления электронных документов на бумажном носителе.

Также РУЦ осуществляет функции ЦАС, может осуществлять функции РЦ, осуществляет согласование регламентов работы РЦ, присоединившихся

к политике (политикам) применения его сертификатов, и инструктаж персонала РЦ.

В соответствии с Указом Президента Республики Беларусь от 08.11.2011 № 515 «О некоторых вопросах развития информационного общества» функции корневого удостоверяющего центра, РУЦ осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее – Оператор).

Место нахождения Оператора:

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

УНП 191700161, ОКПО 380325925000.

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

телефон: (017) 311 30 00;

факс: (017) 311 30 06;

e-mail: info@nces.by;

адрес Интернет-сайта: http://nces.by.

1.2. Идентификация

ППАС 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) sub-ca(2) sub-ca(3)} (1.2.112.1.2.1.1.1.3.2.3).

Данный объектный идентификатор разработан в соответствии с требованиями СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов» и включается в расширение acceptablePrivilegePolicies АС, издаваемых ЦАС.

1.3. Пользователи ППАС

Пользователями ППАС являются подписчики в соответствии с регламентом деятельности республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – Регламент).

АС применяется в информационных системах совместно с СОК, при этом СОК используется для идентификации и аутентификации подписчика, а АС – для определения его полномочий. Один и то же подписчик может являться владельцем нескольких АС.

2. Требования к участникам инфраструктуры управления привилегиями

2.1. Требования к ЦАС

ЦАС должен выполнять все требования, установленные в разделе 3 ППАС и п. 2.5 Регламента.

Оператор несет ответственность за соответствие процедурам, установленным ППАС, в соответствии с законодательством.

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 29.11.2013 № 89.

РЦ несет ответственность за проверку идентификационных данных подписчиков.

2.3. Требования к владельцам АС, подписчикам

Требования предъявляются в соответствии с п. 2.3 Регламента.

Выработка личного и открытого ключей подписи осуществляется с использованием сертифицированных средств электронной цифровой подписи (далее – ЭЦП).

2.4. Требования к доверяющей стороне

Требования предъявляются в соответствии с п. 2.4 Регламента.

3. Требования к ЦАС

3.1. Требования по управлению ключами

3.1.1. Выработка личного ключа ЦАС

Выработка личного и открытого ключа ЦАС осуществляется в соответствии с подп. 3.1.1 п. 3.1 Регламента.

Срок действия СОК ЦАС – 10 лет.

3.1.2. Хранение, резервное копирование и восстановление личного ключа ЦАС

Хранение, резервное копирование и восстановление личного ключа ЦАС осуществляется в соответствии с подп. 3.1.2 п. 3.1 Регламента.

3.1.3. Распространение открытого ключа ЦАС

Распространение открытого ключа осуществляется в соответствии с подп. 3.1.3 п. 3.1 Регламента.

3.1.4. Депонирование личного ключа ЦАС

Депонирование личного ключа ЦАС осуществляется в соответствии с подп. 3.1.4 п. 3.1 Регламента.

3.1.5. Использование личного ключа ЦАС

ЦАС использует свой личный ключ только для целей, определенных подп. 3.1.5 п. 3.1 Регламента.

3.1.6. Окончание срока действия личного ключа ЦАС

Окончание срока действия личного ключа ЦАС осуществляется в соответствии с подп. 3.1.6 п. 3.1 Регламента.

3.1.7. Управление средством ЭЦП, используемым для издания АС

Управление средством ЭЦП, используемым для издания АС осуществляется в соответствии с подп. 3.1.7 п. 3.1 Регламента.

3.2. Требования по управлению АС

3.2.1. Регистрация подписчика

Регистрация подписчика осуществляется в соответствии с подп. 3.2.1 п. 3.2 Регламента.

При обращении в РЦ за изданием АС подписчик представляет информацию о:

СОК, с которым будет связан АС;

ФЛ, являющемся владельцем данного СОК и которому предоставлены полномочия на подписание определенных видов электронных документов, а также иные полномочия от имени организации или другого ФЛ (далее – полномочия);

организации или другом ФЛ, предоставившие полномочия ФЛ;

полномочиях, предоставленных ФЛ.

Документы, подтверждающие вышеуказанную информацию, могут быть представлены в виде электронных документов и (или) электронных копий документов на бумажном носителе.

Перечень документов и порядок их предоставления определяется Порядком оказания услуг республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь аккредитованными регистрационными центрами (далее – Порядок оказания услуг РУЦ) и иными документами Оператора.

3.2.2. Возобновление действия и обновление данных АС

Возобновление действия АС не осуществляется.

Обновление данных АС осуществляется путем отзыва действующего АС и издания нового АС.

Последовательность действий подписчика и перечень представляемых им документов соответствует регистрации согласно подп. 3.2.1 п. 3.2 ППАС, если иное не предусмотрено в организационно-распорядительных документах Оператора.

3.2.3. Издание АС

Издание АС осуществляется с учетом подп. 3.2.3 п. 3.2 Регламента в соответствии с Порядком оказания услуг РУЦ.

Для издания АС РЦ обязан:

в соответствии с Порядком оказания услуг РУЦ проверить связь ФЛ, которому предоставляются полномочия, с организацией или другим ФЛ, а также эти полномочия;

установить принадлежность сертификата ФЛ, которому предоставляются полномочия, а также убедиться в действительности этого СОК на момент оказания услуги;

при положительных результатах всех проверок обеспечить издание АС;

сохранить все исходные данные, представленные подписчиком для издания АС.

Профиль формата АС приведен в приложении 1 к ППАС.

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

После издания АС подписчику предоставляются АС, СОК корневого удостоверяющего центра, СОК РУЦ и СОК ЦАС, а также списки отозванных

сертификатов (далее – СОС) КУЦ, РУЦ и СОАС ЦАС (в виде «цепочки» сертификатов формата P7B).

3.2.4. Распространение нормативных и организационно-распорядительные документов для ознакомления

Распространение нормативных и организационно-распорядительных документов осуществляется в соответствии с подп. 3.2.4 п. 3.2 Регламента.

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

форматы АС, издаваемых ЦАС;

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

форма заявления об отзыве АС.

Оператор размещает данную информацию на своем Интернет-сайте.

3.2.5. Распространение АС

Распространение АС осуществляется в соответствии с подп. 3.2.5 п. 3.2 Регламента.

После издания АС он размещается в хранилище РУЦ и становится действительным для ГосСУОК.

Оператор обеспечивает доступность подписчику информации о действительности и назначении АС. В случае отказа информационной системы, сервисов, Оператор обеспечивает восстановление работоспособности данной информационной услуги:

в срок не более 24 часов с момента недоступности информационной услуги, если выход из строя или недоступность наступили по причине, зависящей от Оператора;

в иные сроки, о которых Оператор информирует подписчиков путем размещения соответствующей информации на Интернет-сайте Оператора, если выход из строя произошел по причинам, не зависящим от Оператора.

3.2.6. Отзыв и приостановка действия АС

Отзыв СОК влечет за собой отзыв АС, связанного с указанным СОК.

Инициировать отзыв АС может владелец АС (организация или другое ФЛ, от имени которых ФЛ предоставлены полномочия) путем направления Оператору соответствующего запроса в соответствии с Порядком оказания услуг РУЦ.

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

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

СОАС издается РУЦ сразу же после обработки запроса на отзыв АС.

Услуги РУЦ по управлению отзывом АС доступны в течение рабочего времени РЦ. В случае отказа информационной системы, сервисов, Оператор обеспечивает восстановление работоспособности данной информационной услуги:

в срок не более 24 часов с момента недоступности информационной услуги, если выход из строя или недоступность наступили по причине, зависящей от Оператора;

в иные сроки, о которых Оператор информирует подписчиков путем размещения соответствующей информации на Интернет-сайте Оператора, если выход из строя произошел по причинам, не зависящим от Оператора.

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

Форма заявления на отзыв АС приведена на Интернет-сайте Оператора.

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

Если иное не предусмотрено нормативными правовыми актами и (или) организационно-распорядительной документацией Оператора, отзыв может быть осуществлен в порядке, установленном Оператором, на основании заявления подписчика (владельца АС) для осуществления отзыва АС в срочном (время устанавливается в организационно-распорядительной документации Оператора) порядке.

Приостановка действия АС не осуществляется.

3.2.7. Предоставление информации о статусе АС

Предоставление информации о статусе АС осуществляется в соответствии с подп. 3.2.7 п. 3.2 Регламента.

Новый СОАС может быть издан перед установленным временем издания следующего СОАС. В частности, внеочередной СОАС издается ЦАС сразу же после положительного результата обработки запроса на отзыв АС.

Актуальный СОАС размещен на Интернет-сайте Оператора.

Услуги РУЦ по получению статуса АС доступны 24 часа в сутки 365 дней в году. В случае отказа информационной системы, сервисов или при наличии других факторов, не зависящих от Оператора, Оператор принимает все необходимые меры, чтобы гарантировать, что данные услуги будут недоступны только в течение 1 часа.

3.3. Управление деятельностью РУЦ

3.3.1. Управление безопасностью

Управление безопасностью осуществляется в соответствии с подп. 3.3.1 п. 3.3 Регламента.

3.3.2. Классификация и управление активами

Классификация и управление активами осуществляется в соответствии с подп. 3.3.2 п. 3.3 Регламента.

3.3.3. Вопросы безопасности, связанные с персоналом

В соответствии с подп. 3.3.3 п. 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 подп. 3.3.4 п. 3.3 Регламента.

3.3.5. Управление операционной деятельностью

Управление операционной деятельностью осуществляется в соответствии с подп. 3.3.5 п. 3.3 Регламента.

3.3.6. Управление системным доступом

Управление системным доступом осуществляется в соответствии с подп. 3.3.6 п. 3.3 Регламента.

В системе защиты информации применяются сертифицированные средства защиты информации (средства криптографической защиты информации и средства технической защиты информации).

3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем

Внедрение и обслуживание безопасных доверенных информационных систем осуществляется в соответствии с подп. 3.3.7 п. 3.3 Регламента.

3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности

Восстановление при сбоях и обеспечение непрерывности деятельности осуществляется в соответствии с подп. 3.3.8 п. 3.3 Регламента.

3.3.9. Прекращение функционирования РУЦ

Прекращение функционирования РУЦ осуществляется в соответствии с подп. 3.3.9 п. 3.3 Регламента.

3.3.10. Соответствие требованиям законодательства

В соответствии с подп. 3.3.10 п. 3.3 Регламента.

3.3.11. Сохранение информации, касающейся АС

Сохранение информации, касающейся АС осуществляется в соответствии с подп. 3.3.11 п. 3.3 Регламента.

3.4. Организационные положения

В соответствии с п. 3.4 Регламента.

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

Профиль формата базового атрибутного сертификата ГосСУОК (АС ГосСУОК)

Атрибутный сертификат в соответствии с СТБ 34.101.67-2014 состоит из трех базовых компонентов:

AttributeCertificate ::= SEQUENCE {
attrCertInfo AttributeCertificateInfo;
signatureAlgorithm AlgorithmIdentifier;
signatureValue BIT STRING}

1. Состав базового компонента **attrCertInfo**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
version		Версия формата сертификата по x.509. В текущей локализации используется Version 2	*постоянное*	***1***
holder				
baseCertificateID		Содержит: serialNumber (серийный номер СОК ФЛ, для которого выпущен АС); issuerName (имя эмитента – республиканского удостоверяющего центра)	*изменяемое*	
issuer				
Набор полей и их значений совпадает с набором и значениями полей компонента **subject** в СОК ЦАС				
signature				

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
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*****
serialNumber	2.5.4.5 id-at-serialNumber	Серийный номер, который однозначно определяет АС среди всех сертификатов, выпущенных ЦАС, присваивается ЦАС, является уникальным	*изменяемое*	
attrCertValidityPeriod				
notBeforeTime		Дата начала срока действия АС тип – GeneralizedTime	*изменяемое*	
notAfterTime		Дата окончания срока действия АС тип – GeneralizedTime	*изменяемое*	
attributes				
countryName	2.5.4.6 id-at-contryName	Страна (код страны)	*постоянное*	***BY***
localityName	2.5.4.7	Название населенного пункта	*изменяемое*	
stateOrProvinceName	2.5.4.8	Наименование области	*изменяемое**	
streetAddress	2.5.4.9	Информация о юридическом адресе организации	*изменяемое**	
organizationName	2.5.4.10 id-at-organizationName	Наименование организации	*изменяемое*	

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
organizationUnitName	2.5.4.11 id-at-organizationalUnitName	Наименование структурного подразделения	*изменяемое**	
title	2.5.4.12	Должность	*изменяемое*	
УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП), присвоенный МНС РБ для которого устанавливается связь с физическим лицом	*изменяемое*	
УНПФ	1.2.112.1.2.1.1.1.4.1	Учетный номер плательщика в органах Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь (УНПФ)	*изменяемое**	
extensions				
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа ЦАС (представляет хэш-значение **SHA-1 20 байт** согласно п. 6.2.1.2 СТБ 34.101.19-2012)	*изменяемое*	
CRLDistributionPoints	2.5.29.31	Содержит URI-адрес точки распространения СОС	*изменяемое**	
acceptablePrvilegePolicies	2.5.29.57	Политика применения привилегий (п. 9.2.6 СТБ 34.101.67-2014)	*изменяемое**	
certificatePolicies	2.5.29.32	Политика применения сертификатов	*изменяемое**	*1.2.112.1.2.1.1.1.3.2.3*
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Доступ к информации ЦАС	*изменяемое**	
OCSP	1.3.6.1.5.5.7.48.1	Содержит URI-адрес OCSP-сервера	*изменяемое**	
caIssuers	1.3.6.1.5.5.7.48.2	Содержит URI-адрес сертификата ЦАС	*изменяемое**	

2. Состав базового компонента **signatureAlgorithm**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
signatureAlgorithm				

algorithm		Идентификатор алгоритма, который ЦАС 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*****

3. Состав базового компонента **signatureValue**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
signatureValue		Значение ЭЦП, вычисленное ЦАС		

* – поле не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013