УТВЕРЖДАЮ
Директор республиканского унитарного предприятия «Национальный центр электронных услуг»

_____ А.А. Ильин

«20» _____12_____ 2016 г.

ПОЛИТИКА ПРИМЕНЕНИЯ АТРИБУТНЫХ СЕРТИФИКАТОВ,
изданных республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Минск
2016

СОДЕРЖАНИЕ

1. Введение в политику атрибутных сертификатов 3
1.2. Идентификация.....4
1.3. Пользователи ППАС.....5
1.4. Типы АС 5
2. Требования по управлению ключами ЦАС 6
2.1. Выработка личного ключа ЦАС.....6
2.1.2. Хранение, резервное копирование и восстановление личного ключа ЦАС 6
2.1.3. Распространение открытого ключа ЦАС 6
2.1.4. Депонирование личного ключа ЦАС 6
2.1.5. Использование личного ключа ЦАС 6
2.1.6. Окончание срока действия личного ключа ЦАС 6
2.1.7. Управление средствами ЭЦП, используемыми для издания АС 7
3. Требования по управлению АС 8
3.1. Порядок издания АС Подписчика 8
3.2. Распространение АС Подписчика 9
3.3. Управление статусом АС Подписчика (отзыв, приостановление действия, возобновление действия).....9
3.4. Предоставление информации о статусе АС Подписчика 11
Приложение 1 12

1. Введение в политику атрибутных сертификатов

1.1. Общие положения

Настоящая политика применения атрибутных сертификатов (далее – ППАС) является 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 атрибутных сертификатов (далее – АС), а также по управлению отзывом АС и предоставлению информации о статусе АС.

Для целей настоящей ППАС 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», СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов» и другими техническими нормативными правовыми актами, а также следующие термины и их определения:

регистрационный центр (далее – РЦ) - поставщик услуг достоверного подтверждения принадлежности открытого ключа определенным организации или физическому лицу;

удостоверяющий центр - поставщик услуг издания, распространения, хранения сертификатов открытых ключей (далее - СОК) и списков отозванных СОК;

атрибутный сертификат (далее АС) - структура данных с электронной цифровой подписью центра атрибутных сертификатов, связывающая определенные значения атрибутов с идентификационной информацией о держателе;

центр атрибутных сертификатов (далее – ЦАС) - центр (сервис), удостоверяющий полномочия или свойство стороны путем выпуска атрибутных сертификатов;

список отозванных АС (далее – СОАС) – список отозванных АС, которые были выпущены в ЦАС;

сертификат открытого ключа сервисов (далее – СОК СР) – СОК, предназначенный для обеспечения функционирования сервисов (приложения, серверы или устройства);

Субъект – конечный пользователь, определяемый сертификатом как владелец личного ключа, связанного с открытым ключом, указанным в сертификате;

Подписчик– участник, обращающийся в удостоверяющий центр от лица одного или более субъектов.

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 РУЦ (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 BY83AKBB30120893700845500000 филиал № 529 «Белсвязь» ОАО «АСБ Беларусбанк» БИК AKBBBY21529, 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

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);

Данные объектные идентификаторы разработаны в соответствии с требованиями СТБ 34.101.67-2012 «Информационные технологии

и безопасность. Инфраструктура атрибутных сертификатов» в расширение acceptablePrvilegePolicies АС, издаваемых центром атрибутных сертификатов.

1.3. Пользователи ППАС

На основании СОК Субъекта в РУЦ может издаваться АС, в котором определяются права владельца СОК в информационных системах (например, право подписи документов от имени юридического лица, право доступа к информации и т.д.).

АС изданные в РУЦ устанавливают права (привилегии) владельцев СОК в информационных системах, владельцы которых заключили соответствующее соглашение с Оператором.

АС являются элементом инфраструктуры управления правами (привилегиями) владельцев СОК. АС применяется в информационных системах совместно с СОК Субъекта, при этом СОК используется для идентификации и аутентификации, а АС для определения его прав.

Сервисы по изданию и управлению АС в РУЦ предоставляются ЦАС, являющейся частью инфраструктуры открытых ключей РУЦ.

1.4. Типы АС

ЦАС издает АС для Субъектов способом, обеспечивающим сохранение их подлинности и целостности.

АС издается только к существующему СОК Субъекта, изданного РУЦ.

Формат АС, издаваемых РУЦ соответствуют требованиям СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».

РУЦ гарантирует уникальность идентификационного номера АС Субъекта.

РУЦ обеспечивает конфиденциальность и целостность регистрационных данных предоставляемых Подписчиком.

РУЦ оказывает услуги по изданию и управлению в ГосСУОК АС (далее – АС ГосСУОК), устанавливающих (подтверждающих) связь ФЛ с юридическим лицом (далее – ЮЛ) с указанием идентификационных данных ЮЛ и должностью ФЛ (далее – АС ЮЛ, образец базового формата приведен в приложении 1 к настоящей ППАС).

Подписчик может заключить соглашение о выпуске других типов АС. Формат таких АС согласовывается с Оператором дополнительно. Форматы дополнительных АС размещаются на сайте Оператора.

2. Требования по управлению ключами ЦАС

2.1. Выработка личного ключа ЦАС

2.1.1. Выработка личного ключа и открытого ключа ЦАС осуществляется в соответствии с требованиями п. 3.1.1. Регламента РУЦ.

ЦАС является частью инфраструктуры открытых ключей РУЦ.

Порядок выработки личного ключа и открытого ключа ЦАС определен во внутреннем документе Оператора, утвержденного директором НЦЭУ.

Срок действия СОК СР ЦАС – 10 лет.

Оператор за два года до истечения срока действия СОК СР ЦАС вырабатывает новую пару ключей и принимает все необходимые меры для того, чтобы избежать нарушения деятельности любого участника ГосСУОК, использующего АС.

2.1.2. Хранение, резервное копирование и восстановление личного ключа ЦАС

Порядок хранения, резервного копирования и восстановления личного ключа ЦАС определен в п.3.1.2. Регламента РУЦ.

2.1.3. Распространение открытого ключа ЦАС

Порядок распространения открытых ключей РУЦ, включая открытый ключ ЦАС, определен в п.3.1.3. Регламента.

2.1.4. Депонирование личного ключа ЦАС

РУЦ не осуществляет депонирование личных ключей РУЦ, включая личный ключ ЦАС, несмотря на то, что он осуществляет их резервное копирование.

2.1.5. Использование личного ключа ЦАС

РУЦ использует свой личный ключ ЦАС только для целей издания АС, СОАС ЦАС и предоставления информации о статусе АС.

2.1.6. Окончание срока действия личного ключа ЦАС

Личный ключ ЦАС не используются по окончании срока его действия.

Оператор уничтожает без возможности восстановления все личные ключи РУЦ, включая личный ключ ЦАС, после окончания срока их действия в порядке, определенном Регламентом, в том числе и их резервную копию.

2.1.7. Управление средствами ЭЦП, используемыми для издания АС

РУЦ обеспечивает безопасность программных и программно-аппаратных средства ЭЦП в течение всего срока их применения для издания АС.

РУЦ гарантирует, что:

средства ЭЦП, используемые для издания АС и СОАС, не были повреждены во время поставки;

средства ЭЦП, используемые для издания АС и СОАС, не были скомпрометированы во время хранения;

установка, активация, резервное копирование и восстановление личных ключей ЦАС в программно-аппаратном средстве ЭЦП проводится под контролем, как минимум двух доверенных работников Оператора и владельцев порогового числа частичных секретов, участвующих в восстановлении под контролем комиссии;

средства ЭЦП, используемые для издания АС или СОАС, функционируют правильно;

личный ключ ЦАС, хранимый в программно-аппаратном средстве ЭЦП, уничтожается при изъятии данного средства из обращения.

3. Требования по управлению АС

3.1. Порядок издания АС ГосСУОК

Услуга издания АС ГосСУОК (далее – Услуга) осуществляется в соответствии с Порядком оказания электронных услуг республиканским удостоверяющим центром, аккредитованными регистрационными центрами ГосСУОК, утвержденным Оператором.

Для оказания Услуги не требуется обязательное личное присутствие (ФЛ, указанного в СОК Субъекта, в РУЦ, РЦ. Перечень документов можно направить Оператору РУЦ почтовым отправлением.

ФЛ обратившегося в РУЦ, РЦ, за оказанием Услуги, должен представить:

перечень сведений о Подписчике в двух экземплярах, заполненный разборчиво на русском языке, подписанный руководителем ЮЛ и заверенный печатью;

документ, подтверждающий полномочия руководителя 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 (далее – ЕГР) (во избежание выпуска СОК 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 (далее – Фонд);

копию документа, подтверждающего оплату Услуги.

При издании АС ГосСУОК регистратор РУЦ (РЦ) должен установить полноту и точность представленных данных.

Регистратор РУЦ (РЦ) регистрирует всю информацию, используемую для проверки организации, а также личности ФЛ, включая номер документа, удостоверяющего личность в соответствии с законодательством, дату выдачи данного документа, наименование органа, выдавшего его, и другие данные. После этого с Подписчиком заключается договор.

Договор может быть выполнен в бумажном или электронном виде в соответствии с Законом Республики Беларусь от 28 декабря 2009 года №113-З «Об электронном документе и электронной цифровой подписи».

С Подписчиком РУЦ может быть заключен публичный договор, который размещается на Интернет-сайте Оператора. Условия публичного договора являются общими для всех Подписчиков РУЦ. Оператор оставляет за собой право не рассматривать и не обсуждать предложения Подписчиков РУЦ по изменению и (или) дополнению условий публичного договора. Факт принятия (акцепта) Подписчиком РУЦ условий публичного договора выражается в оплате Подписчиком РУЦ услуги РУЦ. Публичный договор при условии соблюдения порядка его оплаты, считается заключенным в простой письменной форме. Публичный договор является действительным в той редакции и на тех условиях, которые существовали на момент оплаты услуг РУЦ.

После заключения Договора осуществляется процедура издания АС.

После издания АС Субъекту предоставляются:

АС, изданный ЦАС;

СОАС, изданный ЦАС;

СОК ЦАС, изданный РУЦ;

СОК и список отозванных сертификатов (далее – СОС) КУЦ и РУЦ (в виде «цепочки» сертификатов формата P7B).

3.2. Распространение АС

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

РУЦ обеспечивает доступность Подписчику информации о действительности и назначении АС. 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.

3.3. Управление статусом АС (отзыв, приостановление действия, возобновление действия)

Отзыв АС производится только при досрочном прекращении его действия по заявке Подписчика или в случае невозможности использования личного ключа Субъекта (в случаях компрометации личного ключа или прекращения деятельности Подписчиком).

Если о компрометации личного ключа Субъекта сообщила третья сторона, то РУЦ запрашивает подтверждение данной информации непосредственно у Подписчика (субъекта)– владельца личного ключа.

Приостановка действия АС Субъекта производится по запросу Подписчика в других обоснованных случаях.

Запрашивать отзыв (приостановку действия) АС может только Подписчик, для которого он выпущен.

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

РУЦ гарантирует, что АС отзывается (приостанавливается его действие) только на основании заявления Подписчика и в сроки, установленные Регламентом РУЦ.

АС считается приостановленным до тех пор, пока не будет подтвержден его отзыв. РУЦ гарантирует, что АС не будет считаться приостановленным дольше времени, необходимого для подтверждения его действительности.

РУЦ распространяет информацию о статусе АС посредством издания, соответствующего СОАС. СОАС издается РУЦ сразу же после обработки запроса на отзыв АС с соблюдением следующих правил:

каждый СОАС содержит информацию о времени издания следующего СОАС;

СОАС подписан личным ключом ЦАС.

Новый СОАС может быть издан перед установленным временем издания следующего СОАС.

Промежуток времени, в течение которого СОАС должен быть доведен до всех заинтересованных элементов ГосСУОК, определяется Регламентом.

Услуги РУЦ по управлению статусом АС (отзыв, приостановление действия, возобновление действия) доступны 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 АС доступна до истечения срока действия этого АС, установленного при его издании.

Возобновление действия АС осуществляется без изменения регистрационной информации, содержащейся в этом АС. Возобновление действия АС возможно только в течение срока, на который этот АС был выпущен.

Форма заявления на управление статусом АС приведена на Интернет-сайте Оператора. Заявление может подаваться как на бумажном носителе, так и в виде электронного документа.

3.4. Предоставление информации о статусе АС

ЦАС распространяет информацию о статусе АС посредством издания, соответствующего СОАС или путем предоставления информации об АС по онлайновому протоколу проверки статуса сертификата OCSP (далее – сервис OCSP).

Периодичность издания СОАС - ежемесячно. СОС издается РУЦ с соблюдением следующих правил:

каждый СОАС содержит информацию о времени издания следующего СОАС;

СОАС подписан личным ключом ЦАС.

Новый СОАС может быть издан перед установленным временем издания следующего СОАС. Например, внеочередной СОАС издается ЦАС сразу же после обработки запроса на управление статусом АС (отзыв, приостановление действия, возобновление действия).

С помощью сервиса OCSP можно получить своевременную и более полную информацию о статусе АС, чем с помощью СОАС. Реализация сервиса OSCP в ЦАС производится в соответствии с СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».

Порядок получения доступа к серверу OCSP ЦАС и использования сервиса OCSP для получения информации о статусе АС, определяется Оператором.

Приложение 1
к Политике применения атрибутных сертификатов, изданных республиканским удостоверяющим центром 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 {
attrCertifnfo AttributeCertificateInfo;
signatureAlgorithm AlgorithmIdentifier;
signatureValue BIT STRING}

1. Состав базового компонента **attrCertifnfo**

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
version		Версия формата сертификата по x.509. В текущей локализации используется Version3	постоянное	*1*
holder				
baseCertificateID		Содержит: issuerName (имя эмитента – ***BY NCES-CAFL***); serialNumber (серийный номер СОК ФЛ, для которого выпущен АС)	*изменяемое*	***Сервис для физических лиц РУЦ***
issure				
Набор полей и их значений совпадает с набором и значениями полей компонента **subject** в СОК ЦАС, издавшем данный атрибутный сертификат				
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***

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
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 СОК тип – GeneralizedTime	*изменяемое*	
afterBeforeTime		Дата окончания срока действия СОК тип – GeneralizedTime	*изменяемое*	
attributes				
organizationName	2.5.4.10 id-at-organizationName	Наименование организации	*изменяемое*	
organizationUnitName	2.5.4.11 id-at-organizationalUnitName	Наименование структурного подразделения	*изменяемое*	
title	2.5.4.12	Должность	*изменяемое*	
stateOrProvincename	2.5.4.8	Наименование области	*изменяемое*	
localityName	2.5.4.7	Название населенного пункта	*изменяемое*	
streetAddress	2.5.4.9	Информация о юридическом адресе организации	*изменяемое*	

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП), присвоенный юридическому лицу 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*	
Идентификатор ГИС		Принадлежность к ГИС: Идентификаторы государственных информационных систем, зарегистрированных в Государственном регистре информационных систем согласно Постановления Совета Министров Республики Беларусь от 26 мая 2009 года №673. Имеет вид 1.2.112.1.2.1.1.A.BBBB.CC.DDDD, где: A – признак типа ИС (1-базовая ИС,2-республиканская ИС, 3-региональная ИС; BBBB – четырехзначный порядковый номер государственной регистрации создания ИС данного типа; CC – двузначный порядковый номер государственной регистрации изменений ИС; DDDD – четырехзначное значение года регистрации ИС.	*Изменяе-мое**	
extensions				

Поле (компонент)	OID	Описание поля (компонента)	Тип поля	Постоянные значения
authorityKeyIdentifier	2.5.29.35	Уникальный идентификатор открытого ключа ЦАС (представляет хэш-значение **SHA-1** **20 байт** согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012)	*изменяемое*	
CRLDistributionPoints	2.5.29.31	Точка распространения СОС	*изменяемое*	
acceptablePrvilegePolicies	2.5.29.57	Политика применения АС. (п. 9.2.6 СТБ 34.101.67-2014)	*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**		
OCSP	1.3.6.1.5.5.7.48.1	Содержит указатель на OCSP сервис ЦАС	*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/aa-by.crt***

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 электронной цифровой подписи, вычисленное ЦАС ГосСУОК		

* – поле не обязательно для заполнения

** – соответствуют требованиям СТБ 34.101.45-2013