PKI-FORUM
РОССИЯ

НЦЭУ

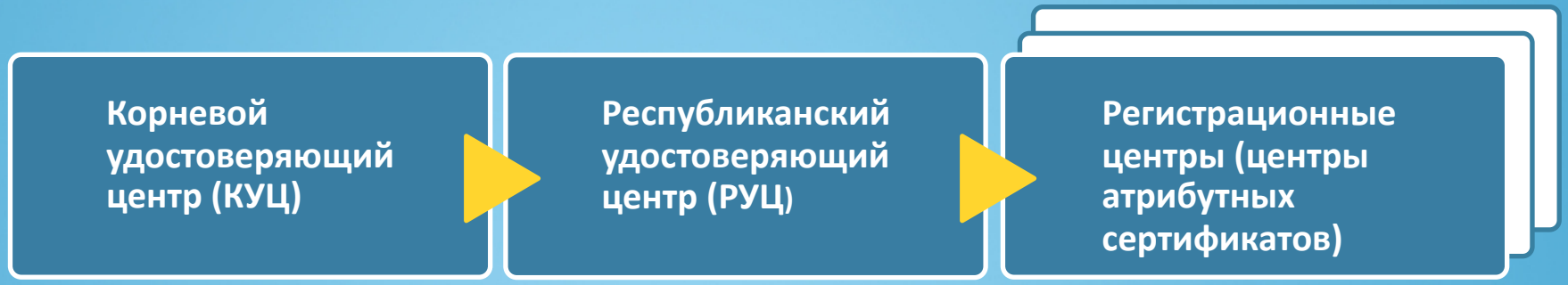
НАЦИОНАЛЬНЫЙ ЦЕНТР ЭЛЕКТРОННЫХ УСЛУГ

ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ ПРОЕКРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ РЕСПУБЛИКИ БЕЛАРУСЬ (ГОССУОК).

ПРАКТИЧЕСКИЙ ОПЫТ УПРАВЛЕНИЯ ПОЛНОМОЧИЯМИ НА ОСНОВЕ АТРИБУТНЫХ СЕРТИФИКАТОВ.

НАЗНАЧЕНИЕ ГОССУОК

ГосСУОК предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах проверки электронной цифровой подписи и их владельцах в Республике Беларусь и представляет собой систему взаимосвязанных и аккредитованных в ней удостоверяющих и регистрационных центров



Сертификаты открытых ключей, изданные в ГосСУОК, обязательны к применению при обращении электронных документов во всех государственных информационных системах, а также в иных информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено (ст.29 Закона об ЭД и ЭЦП)

РАСПРЕДЕЛЕНИЕ РОЛЕЙ В ГОССУОК

ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

определяет:
порядок функционирования ГосСУОК;
условия аккредитации поставщиков услуг в ГосСУОК;
порядок проведения аккредитации поставщиков услуг в ГосСУОК;
порядок взаимодействия с поставщиками услуг иностранных государств
утверждает:
политику применения сертификатов открытых ключей (СОК) и регламент корневого удостоверяющего центра
осуществляет:
согласование политики применения СОК и регламента республиканского удостоверяющего центра
аккредитацию поставщиков услуг в ГосСУОК;
контроль за соблюдением условий аккредитации поставщиков в ГосСУОК

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ «НЦЭУ»

осуществляет:
функции оператора корневого удостоверяющего центра (КУЦ);
функции оператора республиканского удостоверяющего центра (РУЦ);
функции национально оператора доверенной третьей стороны по признанию подлинности электронных документов при межгосударственном электронном взаимодействии

РЕГИСТРАЦИОННЫЕ ЦЕНТРЫ (ЦЕНТРЫ АТРИБУТНЫХ СЕРТИФИКАТОВ)

осуществляют:
проверку информации, вносимой в сертификаты и атрибутные сертификаты;
формирование заявок на издание и отзыв сертификатов и атрибутных сертификатов;
передачу конечным пользователям изданных сертификатов и атрибутных сертификатов;
Обеспечение взаимодействия пользователей с РУЦ

НЦЭУ

PKI-FORUM РОССИЯ

В соответствии с частью четвертой статьи 29 Закона Республики Беларусь от 28.12.2009 «Об электронном документе и электронной цифровой подписи» порядок функционирования ГосСУОК определяется Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – Положение о ГосСУОК), утверждаемым ОАЦ.

Приказом ОАЦ от 10.12.2015 № 118 (в редакции приказа ОАЦ от 08.02.2019 №45) утверждено Положение о ГосСУОК.

Положением о ГосСУОК определены типы сертификатов открытых ключей, которые могут издаваться в ГосСУОК:

СОК для организаций;

СОК для физических лиц (содержащие сведения только о физическом лице (далее – ФЛ): Ф.И.О., личный номер и e-mail);

атрибутные сертификаты (далее – АС), которые издаются на основании СОК ФЛ и в которых определяются полномочия владельца сертификата.

П.2. Центр атрибутных сертификатов (ЦАС) - поставщик услуг издания, распространения, хранения атрибутных сертификатов и списков отозванных атрибутных сертификатов, предоставления информации о действительности атрибутных сертификатов, их отзыва.

П.4. Конечными пользователями ГосСУОК выступают физические лица и организации, которые являются владельцами сертификатов, атрибутных сертификатов и (или) доверяющими сторонами.

П.18. На основании сертификатов физических лиц, работающих в государственных органах и других государственных организациях, а также иных физических лиц центр атрибутных сертификатов издает атрибутные сертификаты в соответствии с политикой применения атрибутных сертификатов. В атрибутных сертификатах содержится информация о полномочиях таких физических лиц.

Политика применения атрибутных сертификатов разрабатывается и утверждается НЦЭУ по согласованию с ОАЦ.

П.21. Для отзыва сертификата и (или) атрибутного сертификата его владелец взаимодействует с регистрационным центром или с республиканским удостоверяющим центром либо с центром атрибутных сертификатов в соответствии с регламентом республиканского удостоверяющего центра. После рассмотрения заявки на отзыв сертификата и (или) атрибутного сертификата регистрационный центр направляет запрос на его отзыв в республиканский удостоверяющий центр или центр атрибутных сертификатов.

Приказ оперативно-аналитического центра при Президенте Республики Беларусь от 10.12.2015 № 118 (в редакции приказа ОАЦ от 08.02.2019 №45) «Об утверждении Положения о ГосСУОК»

НЦЭУ

PKI-FORUM РОССИЯ

Статья 1. атрибутный сертификат – электронный документ, изданный поставщиком услуг и содержащий информацию о полномочиях физического лица, в том числе индивидуального предпринимателя (далее, если не предусмотрено иное, – физическое лицо), являющегося владельцем личного ключа электронной цифровой подписи (далее – личный ключ), на подписание определенных видов электронных документов, а также иные полномочия, предоставленных ему от имени организации или другого физического лица (далее, если не предусмотрено иное, - полномочия);

Статья 22. Если в соответствии с законодательством Республики Беларусь и (или) соглашением сторон документ должен быть подписан собственноручно и заверен печатью, электронный документ, подписанный электронной цифровой подписью, владельцем личного ключа которой является физическое лицо, информация о полномочиях которого на подписание документа содержится в атрибутном сертификате, приравнивается к документу на бумажном носителе, подписанному собственноручно и заверенному печатью, и имеет одинаковую с ним юридическую силу.

Электронный документ, подписанный электронной цифровой подписью, владельцем личного ключа которой является физическое лицо, может быть дополнительно подписан электронной цифровой подписью, владельцем которой является организация. В этом случае предоставление атрибутного сертификата, содержащего информацию о полномочиях физического лица на подписание электронного документа от имени этой организации, не требуется.

Закон РБ от 28 декабря 2009 № 113-З «Об электронном документе и электронной цифровой подписи» (с изменениями, внесенными Законом РБ от 08.11.2018 № 143-З).

Формат атрибутного сертификата (АС)

Формат и механизм использования АС определен в государственном стандарте РБ – СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов», разработанного на основе международного стандарта ITU-T X.509 (2008)|ISO/IEC 9594-8:2008 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (Информационные технологии. Взаимосвязь открытых систем. Директория. Структура сертификата открытого ключа и атрибутного сертификата).

В СТБ определен механизм связывания привилегий с их держателем через атрибутные сертификаты. Для этих целей УЦ может наделяться полномочиями центра атрибутных сертификатов (далее – ЦАС), а период действия привилегий совпадает с периодом действия СОК. Стандарт допускает, что ЦАС может не являться одновременно УЦ и различные привилегии могут удостоверяться различными ЦАС. К одному СОК может издаваться несколько АС.

Формат АС базируется на абстрактно-синтаксической нотации версии 1 (АСН.1).

НЦЭУ

PKI-FORUM РОССИЯ

В РУЦ разработана и утверждена Политика применения атрибутных сертификатов, изданных республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (ППАС).

ППАС присвоен объектный идентификатор (Object Identifier, OID):(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.

Профиль формата базового атрибутного сертификата ГосСУОК определен Приложением 1 к ППАС.

АС распространяется владельцем открытого ключа или поставщиком услуг. АС может также распространяться организацией или физическим лицом, от имени которых другому физическому лицу предоставляются полномочия, информация о которых содержится в этом АС.

Владелец АС имеет право отзыва АС.

Отзыв СОК влечет за собой отзыв всех АС, связанных с этим СОК.

Профиль формата базового атрибутного сертификата 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
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	
УНП	1.2.112.1.2.1.1.1.1.2	Учетный номер плательщика (УНП),	изменяемое	
УНПФ	1.2.112.1.2.1.1.1.4.1	Учетный номер плательщика в органах Фонда социальной защиты населения (УНПФ)	изменяемое	
Идентификатор ГИС		Принадлежность к государственным информационным системам,	изменяемое*	
extensions				
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
calssuers	1.3.6.1.5.5.7.48.2	Содержит URL-адрес сертификата УЦ	изменяемое	http://nces.by/pki/certs/aa-by.crt

Профиль формата базового атрибутного сертификата ГосСУОК

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

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.67 – 2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»

государственный стандарт является частью группы стандартов, представляющих инфраструктуру управления привилегиями, и определяет форматы атрибутных сертификатов инфраструктуры управления привилегиями, а также процедуры проверки их подлинности.

3.1. атрибутный сертификат (attribute certificate; AC): Структура данных с цифровой подписью центра ат-рибутных сертификатов, связывающая определенные значения атрибутов с идентификационной ин-формацией о держателе.

3.6 инфраструктура управления привилегиями (privilege management infrastructure; PMI): Инфраструктура, которая позволяет управлять привилегиями при поддержке сервиса надежной авторизации и во взаимодействии с инфраструктурой открытых ключей.

НЦЭУ

PKI-FORUM РОССИЯ

СТБ 34.101.80 – 2018 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи»

Стандарт устанавливает форматы расширенной электронной цифровой подписи, которая, дополнительно к базовой, включает (и при необходимости контролирует) атрибуты подписанного документа и подписавшей его стороны.

Стандарт применяется при создании и обработке электронных документов форматов АСН.1, XML и PDF.

Стандартом определено, что АС может включаться в базовые атрибуты расширенной ЭЦП (подписанный атрибут SignerAttributes). При этом вышеуказанный атрибут содержит АС – атрибуты подписанта, подписанные (удостоверенные) ЦАС.

В неподписанном атрибуте AttributeCertificateReferences (атрибуты расширенной ЭЦП для указания проверочных данных) могут содержаться ссылки на сертификаты, используемые для проверки атрибутных сертификатов.

В неподписанном атрибуте AttributeRevocationReferences (атрибуты расширенной ЭЦП для указания проверочных данных) могут содержаться ссылки на аттестаты отзыва сертификатов (в том числе АС).

НЦЭУ

PKI-FORUM РОССИЯ

Универсальная система доступа

С января 2018 года РУП «НЦЭУ» оказывает услуги по идентификации и аутентификации юридических и физических лиц в различных прикладных информационных системах с использованием СОК, изданных в ГосСУОК, включая СОК мобильной ЭЦП и АС, посредством информационной системы «Универсальная система доступа» (далее – ИС УСД).

Основной функцией ИС УСД является обработка персональных данных с целью идентификации и аутентификации пользователей (физических или юридических лиц) и выработки ЭЦП в интересах поставщиков услуг (владельцев прикладных информационных систем):

- получение и хранение персональных данных физических (юридических) лиц из действующих СОК, включая данные из АС;
- передача данных физических (юридических) лиц (включая соответствующие им СОК) поставщикам услуг (владельцам прикладных информационных систем);
- выработка ЭЦП при наличии у физического (юридического) лица средства ЭЦП.

После доработки ИС УСД с декабря 2018 года отработан механизм авторизации/аутентификации юридических и физических лиц в различных прикладных информационных системах с использованием мобильной ЭЦП в связке с АС.

Признание иностранного сертификата открытого ключа в Республике Беларусь

Статья 30. Иностранный сертификат открытого ключа, соответствующий требованиям законодательства иностранного государства, в котором этот сертификат издан, признается на территории Республики Беларусь в случаях и порядке, определенных международным договором Республики Беларусь, предусматривающим взаимное признание сертификатов открытых ключей, или путем установления доверия к нему доверенной третьей стороной. Доверенной третьей стороной является определенная Президентом Республики Беларусь организация, осуществляющая функции по признанию подлинности электронных документов при межгосударственном электронном взаимодействии.

Сертификат открытого ключа, изданный поставщиком услуг иностранного государства, аккредитованным в Государственной системе управления открытыми ключами, признается на территории Республики Беларусь.

Закон РБ от 28 декабря 2009 № 113-З «Об электронном документе и электронной цифровой подписи» (с изменениями, внесенными Законом РБ от 08.11.2018 № 143-З).

PKI-FORUM
РОССИЯ

НЦЭУ

- г. Минск, ул. Раковская, 14

+375 17 311 30 00

nces.by

Контактные данные:
МОСКАЛЕВ Дмитрий Владимирович,
Республиканский удостоверяющий центр
Государственного предприятия «НЦЭУ»
Телефон: (017) 311-30-00, доб.330
E-mail: mdv@nces.by