УТВЕРЖДАЮ
Директор республиканского
унитарного предприятия
«Национальный центр электронных
услуг»

_____ А.А. Ильин

«12» декабря 2014 г.

Форматы сертификатов открытых ключей и атрибутных сертификатов, издаваемых Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Республиканский удостоверяющий центр Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – РУЦ ГосСУОК) обеспечивает поддержку следующих типов сертификатов абонента:

сертификат открытого ключа физического лица;

атрибутные сертификаты, устанавливающие права (привилегии) владельцев сертификатов открытых ключей в информационных системах, владельцы которых заключили соответствующие соглашения с НЦЭУ.

Атрибутные сертификаты (далее – АС) являются элементом инфраструктуры управления правами (привилегиями) владельцев сертификатов открытых ключей. АС пользователя применяется в информационных системах совместно с сертификатом открытого ключа (далее – СОК) пользователя, при этом СОК используется для идентификации и аутентификации пользователя, а АС для определения прав пользователя

Форматы СОК и списков отозванных сертификатов (далее – СОС), издаваемых РУЦ ГосСУОК, соответствуют требованиям СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

Форматы запросов на выдачу СОК абонентов, обрабатываемых РУЦ ГосСУОК, соответствуют требованиям СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

Форматы атрибутных сертификатов, издаваемых РУЦ ГосСУОК соответствуют требованиям СТБ 34.101.67-2014 «Информационные

технологии и безопасность. Инфраструктура атрибутных сертификатов».

Алгоритм ЭЦП, используемый РУЦ ГосСУОК при выдаче СОК, удовлетворяет требованиям СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых», при этом используется алгоритм хэширования, удовлетворяющий требованиям СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности».

Сервисы по изданию и управлению АС в РУЦ ГосСУОК предоставляются центром атрибутных сертификатов РУЦ ГосСУОК (далее – ЦАС РУЦ ГосСУОК), являющимся частью инфраструктуры открытых ключей РУЦ ГосСУОК.

РУЦ ГосСУОК оказывает услуги по изданию и управлению **следующими типами АС**, устанавливающими (подтверждающими):

связь физического лица с юридическим лицом с указанием идентификационных данных юридического лица и должности физического лица;

связь физического лица с его классом и должностью государственного служащего в государственном органе (ведомстве).

Владельцы информационных систем могут заключить соглашения с НЦЭУ о выпуске других типов АС

Заявителями на издание АС могут выступать как физические, так и юридические лица. **АС издается только к существующему СОК физического лица.**

Владельцам АС **на договорной основе** предоставляются:

комплект программного обеспечения абонента (далее – комплект ПО абонента) предназначенный для выполнения криптографических функций в среде ОС MS Windows;

АС пользователя, изданный ЦАС РУЦ ГосСУОК;

список отозванных АС (далее – СОАС), изданный ЦАС РУЦ ГосСУОК;

СОК ЦАС РУЦ ГосСУОК, изданный РУЦ ГосСУОК;

СОК и СОС КУЦ и РУЦ ГосСУОК (в виде «цепочки» сертификатов формата P7B);

заверенная карточка открытых ключей ЦАС РУЦ ГосСУОК;

заверенные карточки открытых ключей КУЦ и РУЦ ГосСУОК.

Ниже приведены описания основных полей сертификатов, издаваемых РУЦ ГосСУОК, с указанием идентификаторов объектов (далее – OID) относящихся к основным приведенным компонентам СОК.

Образец формата СОК корневого удостоверяющего центра ГосСУОК

Наименование поля (OID поля, при наличии)	Описание (значение) поля (OID значения поля, при наличии)	Примечание
Версия сертификата	V3	Согласно x.509
Серийный номер сертификата		Формируется КУЦ ГосСУОК, является уникальным
Идентификатор алгоритма подписи	СТБ 34.101.45/СТБ 34.101.31 (1.2.112.0.2.0.34.101.45.12)	Идентификатор алгоритма ЭЦП, который использовался КУЦ ГосСУОК для подписи сертификата (bign-with-hbelt согласно СТБ 34.101.45).
Имя издателя (Issuer)		Содержит имя субъекта КУЦ ГосСУОК, используемое в СОК: в случае корневого самоподписанного сертификата значение поля «Имя издателя» совпадает со значением поля «Имя субъекта».
Срок действия (attrCertValidityPeriod)		Содержит даты начала и окончания периода действия СОК
Имя субъекта (Subject):		
Данные об организации, ответственной за использование личного ключа КУЦ ГосСУОК	Наименование организации (organizationName - 2.5.4.10)	Наименование организации владельца личного ключа КУЦ ГосСУОК (Приложение А СТБ 34.101.19-2012)
	Общие данные (commonName - 2.5.4.3)	Полное наименование КУЦ ГосСУОК
	Код страны (countryName - 2.5.4.6)	Двухбуквенный код страны по ISO 3166
Информация об открытом ключе субъекта		Значение открытого ключа и параметры используемого алгоритма ЭЦП
Дополнения:		
Назначение ключа (KeyUsage – 2.5.29.15):	Подписывание СОК	Возможность подписывать СОК своим личным ключом
	Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)	Возможность подписывать СОС своим личным ключом
Идентификатор ключа субъекта (subjectKeyIdentifier - 2.5.29.14)	Уникальный идентификатор открытого ключа субъекта	Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1). В случае корневого самоподписанного сертификата значение поля «Идентификатор ключа субъекта» совпадает со значением поля «Идентификатор ключа центра сертификации».
Идентификатор ключа удостоверяющего центра (authorityKeyIdentifier - 2.5.29.35)	Уникальный идентификатор открытого ключа УЦ	Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1).
Политика сертификата	Политика применения сертификата -	Политика, в соответствии с которой был выдан и может применяться

(certificatePolicies - 2.5.29.32)	КУЦ (1.2.112.1.2.1.1.1.3.1)
Основные ограничения (basicConstraints – 2.5.29.19)	Основные ограничения применения открытого ключа
Бланк карточки открытого ключа (1.2.112.1.2.1.1.1.2.1)	1.2.112.1.2.1.1.1.2.1.1
Электронная цифровая подпись (signatureValue)	

сертификат
Формируется согласно раздела 6.2.1.9 СТБ 34.101.19-2012. Тип субъекта – Центр сертификации, ограничение на длину пути цепочки отсутствует
Бланк карточки открытого ключа корневого удостоверяющего центра инфраструктуры открытых ключей ГосСУОК
Содержит значение электронной цифровой подписи, вычисленное КУЦ ГосСУОК

Образец формата СОК республиканского удостоверяющего центра ГосСУОК

Наименование поля (OID поля, при наличии)	**Описание (значение) поля (OID значения поля, при наличии)**	**Примечание**
Версия сертификата	V3	Согласно x.509
Серийный номер сертификата		Формируется КУЦ ГосСУОК, является уникальным
Идентификатор алгоритма подписи	СТБ 34.101.45/СТБ 34.101.31 (1.2.112.0.2.0.34.101.45.12)	Идентификатор алгоритма ЭЦП, который использовался КУЦ ГосСУОК для подписи сертификата (bign-with-hbelt согласно СТБ 34.101.45).
Имя издателя (Issuer)		Содержит наименование КУЦ ГосСУОК, используемое в СОК
Срок действия (attrCertValidityPeriod)		Содержит даты начала и окончания периода действия СОК
Имя субъекта (Subject):		
Данные об организации, ответственной за использование личного ключа РУЦ ГосСУОК	Наименование организации (organizationName - 2.5.4.10)	Наименование организации владельца личного ключа РУЦ ГосСУОК (Приложение А СТБ 34.101.19-2012)
	Общие данные (commonName - 2.5.4.3)	Полное наименование РУЦ ГосСУОК
	Код страны (countryName - 2.5.4.6)	Двухбуквенный код страны по ISO 3166
	Область (stateOrProvincename - 2.5.4.8)	Информация о юридическом адресе организации. (Приложение А СТБ 34.101.19-2012)
	Населённый пункт (localityName - 2.5.4.7)	
	Адрес (streetAddress - 2.5.4.9)	
	Электронная почта (email - 1.2.840.113549.1.9.1)	Электронная почта РУЦ ГосСУОК
Информация об открытом ключе субъекта		Значение открытого ключа и параметры используемого алгоритма ЭЦП
Дополнения:		
Назначение ключа (KeyUsage – 2.5.29.15)	Подписывание сертификатов	Возможность подписывать СОК своим личным ключом
	Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)	Возможность подписывать СОС своим личным ключом
Идентификатор ключа субъекта (subjectKeyIdentifier - 2.5.29.14)	Уникальный идентификатор открытого ключа субъекта	Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1)
Идентификатор ключа удостоверяющего центра	Уникальный идентификатор открытого ключа УЦ	Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1)

(authorityKeyIdentifier - 2.5.29.35)		
Точка распространения СОС CRLDistributionPoints (2.5.29.31)	URL-адрес	URL-адрес веб-ресурса РУЦ ГосСУОК, на котором располагается актуальный СОС: - http://pki.gov.by/certs/rep_ca.crl - http://www.nces.by/certs/rep_ca.crl (СОС РУЦ)
Доступ к информации удостоверяющего центра (authorityInfoAccess - 1.3.6.1.5.5.7.1.1)	Информация об УЦ, выпустившим сертификат (AuthorityInfoAccesscaIssuers - 1.3.6.1.5.5.7.48.2)	Содержит URL-адрес сертификата УЦ и может содержать указатель на OCSP сервис УЦ: - http://pki.gov.by/certs/root_ca.cer (СОК КУЦ) - http://pki.gov.by/ocsp/root/responder (OCSP КУЦ)
Политика сертификата (certificatePolicies - 2.5.29.32)	Политика применения сертификата - ПУЦ (1.2.112.1.2.1.1.1.3.2)	Политика, в соответствии с которой был выдан и может применяться сертификат
Основные ограничения (basicConstraints - 2.5.29.19)	Основные ограничения применения открытого ключа	Формируется согласно раздела 6.2.1.9 СТБ 34.101.19-2012. Тип субъекта – Центр сертификации, ограничение на длину пути цепочки отсутствует
Бланк карточки открытого ключа (1.2.112.1.2.1.1.1.2.1)	1.2.112.1.2.1.1.1.2.1.2	Бланк карточки открытого ключа подчинённого удостоверяющего центра инфраструктуры открытых ключей ГосСУОК
Электронная цифровая подпись (signatureValue)		Содержит значение электронной цифровой подписи, вычисленное КУЦ ГосСУОК

Образец формата СОК физического лица, издаваемых РУЦ ГосСУОК

Наименование поля (OID поля, при наличии)	Описание (значение) поля (OID значения поля, при наличии)	Примечание
Версия сертификата	V3	Согласно x.509
Серийный номер сертификата		Формируется РУЦ ГосСУОК, является уникальным
Идентификатор алгоритма подписи	СТБ 34.101.45/СТБ 34.101.31 (1.2.112.0.2.0.34.101.45.12)	Идентификатор алгоритма ЭЦП, который использовался РУЦ ГосСУОК для подписи сертификата (bign-with-hbelt согласно СТБ 34.101.45).
Имя издателя (Issuer)		Содержит наименование РУЦ ГосСУОК, используемое в СОК
Срок действия (attrCertValidityPeriod)		Содержит даты начала и окончания периода действия СОК
Имя субъекта (Subject):		
Данные о лице, ответственном за использование личного ключа, позволяют уникально идентифицировать субъект	Фамилия (surname - 2.5.4.4)	Фамилия Имя и Отчество лица, ответственного за использование личного ключа
	Имя и отчество (name - 2.5.4.41)	
	Идентификационный (личный) номер (serialNumber - 2.5.4.5)	Поле, определяющее идентификационный (личный) номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т. д.) субъекта инфраструктуры открытых ключей ГосСУОК, являющегося физическим лицом
	Общие данные (commonName - 2.5.4.3)	Содержит общие данные абонента РУЦ ГосСУОК, то есть владельца личного ключа, соответствующего открытому ключу данного СОК и состоит из набора полей (2.5.4.4), (2.5.4.41).
	Код страны (countryName - 2.5.4.6)	Двухбуквенный код страны по ISO 3166
Информация об открытом ключе субъекта		Значение открытого ключа и параметры используемого алгоритма ЭЦП
Дополнения:		
Информационные дополнения	Идентификатор ключа субъекта (subjectKeyIdentifier - 2.5.29.14)	Уникальный идентификатор открытого ключа субъекта. Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1)
	Идентификатор ключа удостоверяющего центра (authorityKeyIdentifier - 2.5.29.35)	Уникальный идентификатор открытого ключа УЦ. Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1)

	Точка распространения СОС CRLDistributionPoints (2.5.29.31)	URL-адрес веб-ресурса РУЦ ГосСУОК, на котором располагается актуальный СОС: - http://pki.gov.by/certs/ca.crl - http://www.nces.by/certs/ca.crl (СОС ПУЦ физических лиц)
Основные ограничения (BasicConstraints - 2.5.29.19)	Конечный субъект	Принадлежность к абонентам РУЦ ГосСУОК. Формируется согласно раздела 6.2.1.9 СТБ 34.101.19-2012.
Назначение ключа (KeyUsage - 2.5.29.15)	Цифровая подпись (digitalSignature)	Проверка ЭЦП для целей аутентификации, проверки целостности
	Невозможность отказа от авторства (nonRepudiation)	Проверка ЭЦП для обеспечения юридической значимости электронных документов
	Шифрование ключей (keyEncipherment)	Использование в алгоритме транспорта ключа
	Согласование ключей (keyAgreement)	Выработка общего ключа в протоколах формирования общего ключа
Расширенное назначение ключа (ExtendedKeyUsage - 2.5.29.37)	Проверка подлинности клиента (ClientAuth – 1.3.6.1.5.5.7.3.2)	Проверка подлинности абонента сервером во время установки защищённого TLS-соединения
Политика сертификата (certificatePolicies - 2.5.29.32)	Идентификатор политики (1.2.112.1.2.1.1.1.3.2.1)	Политика, в соответствии с которой был выдан и может применяться сертификат
Доступ к информации удостоверяющего центра (authorityInfoAccess - 1.3.6.1.5.5.7.1.1)	Информация об УЦ, выпустившим сертификат (AuthorityInfoAccess OCSP – 1.3.6.1.5.5.7.48.1) (AuthorityInfoAccesscaIssuers - 1.3.6.1.5.5.7.48.2)	Содержит URL-адрес сертификата УЦ и может содержать указатель на OCSP сервис УЦ: - http://pki.gov.by/certs/ca.cer (СОК ПУЦ физических лиц) - http://pki.gov.by/ocsp/ca/ (OCSP ПУЦ физических лиц)
Бланк карточки открытого ключа (1.2.112.1.2.1.1.1.2.1)	1.2.112.1.2.1.1.1.2.1.5	Расширение сертификата X.509, определяющее бланк карточки открытого ключа физического лица – пользователя инфраструктуры открытых ключей ГосСУОК
Электронная цифровая подпись (signatureValue)		Содержит значение электронной цифровой подписи, вычисленное РУЦ ГосСУОК

Образец формата АС, издаваемых ЦАС РУЦ ГосСУОК

Наименование поля (OID поля, при наличии)	Описание (значение) поля (OID значения поля, при наличии)	Примечание
Версия	V2	Согласно x.509
Серийный номер сертификата		Присваивается центром атрибутных сертификатов РУЦ ГосСУОК, является уникальным
Идентификатор алгоритма подписи	СТБ 34.101.45/СТБ 34.101.31 (1.2.112.0.2.0.34.101.45.12)	Идентификатор алгоритма ЭЦП, который использовался центром атрибутных сертификатов РУЦ ГосСУОК для подписи сертификата (bign-with-hbelt согласно СТБ 34.101.45).
Имя издателя (Issuer)		Содержит отличительное имя центра атрибутных сертификатов РУЦ ГосСУОК (п. 6.1. СТБ 34.101.67-2014)
Срок действия (attrCertValidityPeriod)		Содержит даты начала и окончания периода действия атрибутного сертификата. (п. 6.1. СТБ 34.101.67-2014)
Информация о держателе привилегий (holder)		Содержит указатель на СОК физического лица, для которого выпускается АС или одно, или несколько имен владельца АС. (п. 6.1. СТБ 34.101.67-2014)
Дополнения:		
Идентификатор ключа субъекта (subjectKeyIdentifier - 2.5.29.14)	Идентификатор ключа субъекта	Формируется согласно разделов 10.4.1 СТБ 34.101.67-2014 / 6.2.1.2 СТБ 34.101.19-2012 (пункт 1).
Идентификатор ключа удостоверяющего центра (authorityKeyIdentifier - 2.5.29.35)	Уникальный идентификатор открытого ключа центра атрибутных сертификатов РУЦ ГосСУОК.	Формируется согласно разделов 10.4.1 СТБ 34.101.67-2014 / 6.2.1.2 СТБ 34.101.19-2012 (пункт 1).
Точка распространения СОС CRLDistributionPoints (2.5.29.31)	URL-адрес (например, http://pki.gov.by/certs/...)	URL-адрес веб-ресурса ЦАС РУЦ ГосСУОК, на котором располагается актуальный СОС (п. 9.3.3 СТБ 34.101.67-2014 / п. 6.2.1.13 СТБ 34.101.19-2012): - http://pki.gov.by/certs/aca.crl - http://www.nces.by/certs/aca.crl (СОС ЦАС)
Политика применения атрибутного сертификата (acceptablePrvilegePolicies)	Идентификатор политики (1.2.112.1.2.1.1.1.3.2.3)	Политика применения атрибутных сертификатов центра атрибутных сертификатов ГосСУОК. (п. 9.2.6 СТБ 34.101.67-2014)

Доступ к информации ЦАС (authorityInfoAccess - 1.3.6.1.5.5.7.1.1)	Информация об ЦАС, выпустившим атрибутный сертификат (AuthorityInfoAccess OCSP - 1.3.6.1.5.5.7.48.1) (AuthorityInfoAccess caIssuers - 1.3.6.1.5.5.7.48.2)	Содержит URL-адрес сертификата ЦАС и может содержать указатель на OCSP сервис ЦАС (п. 10.4.1 СТБ 34.101.67-2014 /пункт 6.2.2.1 СТБ 34.101.19-2012): - http://pki.gov.by/certs/aca.cer (СОК ЦАС) - http://pki.gov.by/ocsp/aca/ (OCSP ЦАС)
Атрибуты:		
Данные о атрибутах юридического лица, характеризующих физическое лицо. Содержит отличительное имя юридического лица, для которого устанавливается связь с физическим лицом и состоит из набора полей:	Код страны (countryName - 2.5.4.6)	Информация о юридическом адресе организации (Приложение А СТБ 34.101.19-2012)
	Область (stateOrProvincename - 2.5.4.8)	
	Населённый пункт (localityName - 2.5.4.7)	
	Адрес (streetAddress - 2.5.4.9)	
	Наименование организации (organizationName - 2.5.4.10)	Наименование организации и должность физического лица для которого устанавливается связь с юридическим лицом. (Приложение А СТБ 34.101.19-2012)
	Должность (title - 2.5.4.12)	
	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
	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) (постановление Совета Министров Республики Беларусь от 10.07.2009 № 917
Электронная цифровая подпись (signatureValue)		Содержит значение ЭЦП, вычисленное центром атрибутных сертификатов РУЦ ГосСУОК (п. 6.1 СТБ 34.101.67-2014)

Форматы технологических сертификатов открытых ключей, издаваемых Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Республиканский удостоверяющий центр Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – РУЦ ГосСУОК) в соответствии с Концепцией развития Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, обеспечивает поддержку технологических сертификатов открытых ключей (ТСОК) для субъектов, в роли которых выступают приложения, серверы (сервисы) и устройства (например, VPN-сертификаты (IPsec), сертификаты сетевых и телекоммуникационных устройств (маршрутизаторы), SSL-сертификаты) и т.п.

Форматы ТСОК и списков отозванных сертификатов (далее – СОС), издаваемых РУЦ ГосСУОК, соответствуют требованиям СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

Форматы запросов на выдачу СОК абонентов, обрабатываемых РУЦ ГосСУОК, соответствуют требованиям СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

Алгоритм ЭЦП, используемый РУЦ ГосСУОК при выдаче ТСОК, удовлетворяет требованиям СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых», при этом используется алгоритм хэширования, удовлетворяющий требованиям СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности».

Сервисы по изданию и управлению ТСОК в РУЦ ГосСУОК предоставляются отдельным подчиненным УЦ (подчиненным РУЦ ГосСУОК), являющимся частью инфраструктуры открытых ключей РУЦ ГосСУОК.

Ниже приведены описания основных полей ТСОК, издаваемых РУЦ ГосСУОК, с указанием идентификаторов объектов (далее – OID) относящихся к основным приведенным компонентам СОК.

Образец формата технологического СОК, издаваемых РУЦ ГосСУОК

Наименование поля (OID поля, при наличии)	Описание (значение) поля (OID значения поля, при наличии)	Примечание
Версия сертификата	V3	Согласно x.509
Серийный номер сертификата		Формируется РУЦ ГосСУОК, является уникальным
Идентификатор алгоритма подписи	СТБ 34.101.45/СТБ 34.101.31 (1.2.112.0.2.0.34.101.45.12)	Идентификатор алгоритма ЭЦП, который использовался РУЦ ГосСУОК для подписи сертификата (bign-with-hbelt согласно СТБ 34.101.45).
Имя издателя (Issuer)		Содержит отличительное имя РУЦ ГосСУОК
Срок действия (attrCertValidityPeriod)		Содержит даты начала и окончания периода действия сертификата.
Данные о субъекте и юридическом лице, владельце открытого ключа субъекта (сервера, сервиса, устройства)	Название субъекта (commonName - 2.5.4.3)	DNS-имя, IP-адрес сервера, ID устройства или процесса.
	Описание субъекта (description - 2.5.4.13)	Общее наименование сервера, устройства, процесса и т.п.
	Серийный номер субъекта (serialNumber - 2.5.4.5)	Серийный номер сервера, сервиса, устройства
	Наименование организации (organization - Name2.5.4.10)	Содержит отличительное имя юридического лица - абонента РУЦ ГосСУОК, то есть владельца личного ключа, соответствующего открытому ключу данного СОК и состоит из набора полей
	Код страны (countryName - 2.5.4.6)	
	Область (stateOrProvinceName - 2.5.4.8)	
	Населённый пункт (localityName - 2.5.4.7)	
	Адрес (streetAddress - 2.5.4.9)	
Информация об открытом ключе субъекта		Значение открытого ключа и параметры используемого алгоритма ЭЦП
Информационные дополнения	Адрес электронной почты (emailProtection – 1.3.6.1.5.5.7.3.4)	Необязательный атрибут. Используется при необходимости
	Идентификатор ключа субъекта (subjectKeyIdentifier - 2.5.29.14)	Уникальный идентификатор открытого ключа субъекта. Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1).

	Идентификатор ключа удостоверяющего центра (authorityKeyIdentifier - 2.5.29.35)	Уникальный идентификатор открытого ключа УЦ. Значение формируется согласно раздела 6.2.1.2 СТБ 34.101.19-2012 (пункт 1).
	Точка распространения СОС CRLDistributionPoints (2.5.29.31)	URL-адрес веб-ресурса РУЦ ГосСУОК, на котором располагается актуальный СОС: - http://pki.gov.by/certs/tca.crl - http://www.nces.by/certs/tca.crl (СОС ПУЦ технологические)
	Идентификатор ГИС (1.2.112.1.2.1.1.5.6=1.2.112.1.2.1.1.ABBBBCCDDDD)	Идентификатор государственной информационной системы, в которой используется субъект (сервер, процесс и т.п.), для которого издан данный технологический сертификат открытого ключа
Основные ограничения (Basic Constraints – 2.5.29.19)	Конечный субъект	Принадлежность к абонентам РУЦ ГосСУОК
Назначение ключа (Key Usage - 2.5.29.15)	Цифровая подпись (digitalSignature)	Проверка ЭЦП для целей аутентификации, проверки целостности
	Шифрование ключей (keyEncipherment)	Использование в алгоритме транспорта ключа
	Согласование ключей (keyAgreement)	Выработка общего ключа в протоколах формирования общего ключа
Расширенное применение ключа (ExtKeyUsage - 2.5.29.37)	ServerAuth (1.3.6.1.5.5.7.3.1)	Проверка подлинности сервера (только для сертификатов серверов)
	ClientAuth (1.3.6.1.5.5.7.3.2)	Проверка подлинности клиента (только для сертификатов клиентов)
	Подписывание OCSP-ответов (1.3.6.1.5.5.7.3.9)	Личный ключ может быть использован для выработки ЭЦП под OCSP-ответами сервера (только для OCSP-серверов)
Политика сертификата (certificatePolicies - 2.5.29.32)	Идентификатор политики (1.2.112.1.2.1.1.1.3.2.2)	Политика идентифицирует организационные процедуры, соблюденные при выпуске сертификата
Доступ к информации удостоверяющего центра (authorityInfoAccess - 1.3.6.1.5.5.7.1.1)	Информация о РУЦ ГосСУОК, выпустившим сертификат	Содержит URL-адрес сертификата РУЦ ГосСУОК и может содержать указатель на OCSP сервис УЦ: - http://pki.gov.by/certs/tca.cer (СОК ПУЦ технологические) - http://pki.gov.by/ocsp/tca/ (OCSP ПУЦ технологические)
Электронная цифровая подпись (signatureValue)		Содержит значение электронной цифровой подписи, вычисленное издателем сертификата.

ПРИМЕЧАНИЕ: Перечень полей может дополняться и изменяться НЦЭУ по согласованию с ОАЦ.