ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
(КАЗНАЧЕЙСТВО РОССИИ)

УТВЕРЖДАЮ
Заместитель руководителя
Федерального казначейства
_____ А.С. Албычев
«26» сентября 2019 г.

Описание структуры и порядка использования полей квалифицированного сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром Федерального казначейства

Версия 6
Листов 36

СОГЛАСОВАНО

Начальник Управления режима
секретности и безопасности информации
Федерального казначейства
_____ / В.С. Бражко
«25» сентября 2019 г.

Содержание

1.1. Назначение документа

Настоящий документ содержит описание структуры и порядка использования полей (атрибутов) квалифицированного сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром Федерального казначейства, при его использовании в рамках информационных систем, оператором которых является Федеральное казначейство.

Структура полей квалифицированного сертификата ключа проверки электронной подписи, утверждена приказом Федеральной службы безопасности Российской Федерации от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Описание состава поля Extended Key Usage квалифицированного сертификата ключа проверки электронной подписи может включать значения, указанные в приложении «Б» к настоящему документу.

1.2. Список сокращений

Сокращение	Описание
АС ФК	Автоматизированная система Федерального казначейства
ЕИС	Единая информационная система в сфере закупок
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СЭД ФК	Система электронного документооборота Федерального казначейства
ФК	Федеральное казначейство (Казначейство России)
ЦА ФК	Центральный аппарат Федерального казначейства
СПВБ	Санкт-Петербургская Валютная Биржа
ГМУ	Официальный сайт Российской Федерации в информационно-телекоммуникационной сети Интернет для размещения информации о государственных (муниципальных) учреждениях
ИП	Индивидуальный предприниматель
САС	Список аннулированных сертификатов
УЦ	Удостоверяющий центр Федерального казначейства
ЭП	Электронная подпись
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
ЕГРЮЛ	Единый государственный реестр юридических лиц
ОГРН	Основной государственный регистрационный номер
ОГРНИП	Основной государственный регистрационный номер индивидуального предпринимателя
ИНН	Идентификационный номер налогоплательщика
СНИЛС	Страховой номер индивидуального лицевого счета
ЗЧ	Закрытая часть

1.3. Правила заполнения полей сертификата

Перечень основных полей приведен в
Табл. 1.

Табл. 1 Перечень основных полей

№ п\п	Поле	Описание
Основная информация		
1	version	Версия формата сертификата X.509. Устанавливается УЦ при создании сертификата версия 3
2	serialNumber	Серийный номер сертификата. Устанавливается УЦ при создании сертификата. Комбинация полей issuer, authorityKeyIdentifire и serialNumber является уникальным идентификатором сертификата
3	signature	Идентификатор алгоритма ЭП, в соответствии с которым была осуществлена подпись настоящего сертификата УЦ
4	issuer	Уникальное имя (Distinguished name, далее – DN) выпускающего УЦ. Устанавливается УЦ при создании сертификата
5	validity	Срок действия сертификата[1]. Включает дату и время начала срока действия и дату и время окончания срока действия (время указывается в часовом поясе GMT+0).
6	subject	DN владельца сертификата. Перечень используемых относительных уникальных имен (relative distinguished name, далее – RDN) приведен в Табл. 2

1) Для «КриптоПро CSP» версии 4.0 установлены следующие максимальные сроки действия ключей:

- максимальный срок действия ключа ЭП - 1 год 3 месяца;

- максимальный срок действия ключа проверки ЭП - 15 лет;

- максимальный срок действия закрытых и открытых ключей обмена – 1 год 3 месяца.

7	subjectPublicKeyInfo	Алгоритм и значение ключа проверки ЭП. Устанавливается УЦ при создании сертификата
8	UniqueIdentifier	Не должен использоваться
9	extensions	Расширения (детальное описание представлено в Табл. 3.)
Электронная подпись УЦ		
10	signatureAlgorithm	алгоритм ЭП
11	signatureValue	значение ЭП

Табл. 2 Перечень используемых относительных уникальных имен

Атрибут	Описание атрибута	Рекомендованная кодировка	Максимальная длина значения поля	Обязательность
surname	Фамилия владельца сертификата с большой буквы в одно слово без пробелов. Если в написании фамилии присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов.	UTF8String	не более 2000 символов	Обязательно для всех сертификатов, за исключением сертификата юридического лица, в котором отсутствует ФИО
givenName	ИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца	UTF8String	не более 2000 символов	Обязательно для всех сертификатов, за исключением сертификата юридического лица, в котором отсутствует ФИО

	(например, паспорт). Формат: a. первое слово – Имя; b. 1 пробел; c. второе слово – Отчество (если имеется); d. 1 пробел (если есть еще текст после отчества); • Если в имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов. Если, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится с пробелами			
title	Должность владельца сертификата	UTF8String	не более 2000 символов	Обязательно для всех систем, использующих сертификат юридического лица, за исключением сертификата юридического лица, в котором отсутствует ФИО
UnstructuredName	Наименование в свободной форме.	PrintableString или	в соответствии	Обязательно для АСФК, за

	Указывается код из справочника должностей	UTF8String	с PKCS#9 – 255 символов	исключением сертификата юридического лица
streetAddress	Наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется) юридического лица	UTF8String	не более 2000 символов	Обязательно для сертификата юридического лица
commonName	Фамилия, имя, отчество владельца сертификата, либо наименование организации – юридического лица (как в ЕГРЮЛ)	UTF8String	не более 2000 символов	Обязательно для всех сертификатов.
organizationUnitName	Наименование подразделения юридического лица	UTF8String	не более 2000 символов	Не обязательно
organizationName	Наименование организации, от имени которой действует владелец сертификата, либо наименование организации-владельца сертификата (как в ЕГРЮЛ).	UTF8String	не более 2000 символов	Обязательно для всех сертификатов
localityName	Наименование населенного пункта	UTF8String	в соответствии с RFC5280 – 128 символов	Обязательно для сертификата юридического лица

stateOrProvinceName	Наименование соответствующего субъекта Российской Федерации	UTF8String	в соответствии с RFC5280 – 128 символов	Обязательно для сертификата юридического лица
countryName	Двухсимвольный код страны в соответствие с ISO 3166. Для России указывается RU	PrintableString	в соответствии с RFC5280 – 2 символа	Обязательно для всех сертификатов
EMail	Адрес электронной почты в сети Интернет владельца сертификата	IA5String (или UTF8String при использовании кирилличесих доменов)	в соответствии с PKCS#9 – 255 символов	Обязательно для всех сертификатов
OGRN	ОГРН	Numeric String	В соответствии с приказом ФСБ России от 27.12.2011 № 795 длина поля составляет 13 символов	Обязательно для квалифицированного сертификата юридического лица
SNILS	СНИЛС	Numeric String	В соответствии с приказом ФСБ России 27.12.2011 № 795 длина поля составляет 11 символов	Обязательно для квалифицированного сертификата в случае наличия в его составе ФИО
INN	ИНН	Numeric String	В соответствии с приказом ФСБ России 27.12.2011	Обязательно для сертификата. Для сертификата должностного лица указывается ИНН

			№ 795 длина поля составляет 12 символов	получателя сертификата. Для сертификата юридического лица – ИНН юридического лица, при этом две первые цифры строки устанавливаются равными нулю. Для сертификата индивидуального предпринимателя – ИНН индивидуального предпринимателя
OGRNIP	ОГРНИП	Numeric String	Длина поля составляет 15 символов	Обязательно для сертификата индивидуального предпринимателя

Табл. 3. Описание Extensions

Наименование дополнений	Описание	Обязательность
Authority Key Identifier	Идентификатор ключа проверки ЭП выпускающего УЦ в форме keyIdentifier. Требуется указание authorityCertIssuer (наименование издателя) и authorityCertserialNumber (номер сертификата аккредитованного УЦ)	Обязательно для всех сертификатов
Subject Key Identifier	Идентификатор ключа проверки ЭП сертификата. Устанавливается УЦ при создании сертификата	Обязательно для всех сертификатов
Key Usage	Назначение использования ключей. Устанавливается в виде битовой маски. Перечень допустимых значений представлен в Табл.4. Для обеспечения корректного использования сертификата в системах	Обязательно для всех сертификатов

	ФК должны быть установлены следующие значения: • digitalSignature; • nonRepudiation; • dataEncipherment; • keyEncipherment; • keyAgreement. Для разрабатываемых систем должны быть использованы значения в соответствии с RFC 4491 для сертификатов ГОСТ Р 34.10-2012.	
Certificate Policies	Класс средств электронной подписи владельца сертификата. Устанавливается в виде списка идентификаторов. Перечень допустимых значений для использования в различных системах приведен в Приложении А[2].	Обязательно для всех сертификатов
Subject Alternative Name	Дополнительные сведения о владельце сертификата. Допускается использование следующих атрибутов: • otherName – последовательность пар «OID»-«данные», перечень допустимых значений представлен в Приложении В; • rfc822Name – адрес электронной почты в соответствии с RFC822; • dNSName – DNS-имя; • x400Address – адрес в соответствии со стандартом X.400; • directoryName – данные в формате X.501 Name; • ediPartyName – последовательность пар «имя»-«имя»; • uniformResourceIdentifier – универсальный идентификатор ресурса (URI); • iPAddress – IP-адрес; • registeredID – идентификатор в виде	Обязательность использования в зависимости от требований системы

[2] Для ГИС ЖКХ сертификат должен содержать обозначение класса средств ЭП не ниже КС2.

	OID. Для обеспечения корректного использования сертификата в системе АСФК должен быть заполнен следующий атрибут: • otherName должен содержать номер ключа при смене сертификата в качестве значения параметра OID=id-on-Keyid, при этом при каждой последующей смене ключей номер должен увеличиваться на единицу. Для обеспечения корректного использования сертификата в системе СЭД должны быть заполнены следующие атрибуты: • otherName должен содержать номер ключа при смене сертификата в качестве значения параметра OID=id-on-Keyid; • uniformResourceIdentifier должен содержать привилегии владельца сертификата. Для обеспечения корректного использования сертификата в системе Landocs должны быть заполнены следующие атрибуты: otherName должен содержать идентификатор безопасности в качестве значения параметра OID=id-on-Landocsid, значение идентификатора должно быть уникально в рамках системы Landocs. Значение идентификатора заполняется значением СНИЛС владельца сертификата. Для обеспечения корректного использования сертификата в системе	

	ГМУ должны быть заполнены следующие атрибуты[3]: • otherName должен содержать код ГМУ организации в качестве значения параметра OID=id-on-InstitutionId; (заполняется при необходимости)	
subjectSignTool (1.2.643.100.111)	Наименование используемого владельцем сертификата средства ЭП	Обязательно для всех сертификатов
issuerSignTool (1.2.643.100.112)	Наименование средств электронной подписи и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, а также реквизитов документов, подтверждающих соответствие указанных средств требованиям, установленным законодательством РФ. Должны быть заполнены следующие атрибуты: • signTool – включает полное наименование средств ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и сертификата; • cATool – включает полное наименование средства аккредитованного УЦ, которое было использовано для создания ключа ЭП, • ключа проверки ЭП и квалифицированного сертификата; • signToolCert – включает реквизиты заключения ФСБ России о подтверждении соответствия средства УЦ, которое было использовано для создания сертификата, соответствующего требованиям 63-ФЗ; • cAToolCert - включает реквизиты заключения ФСБ России о подтверждении соответствия средства ЭП, которое было использовано для	Обязательно для всех сертификатов

[3] Данный атрибут в составе сертификата необходимо использовать до завершения работ по интеграции ГМУ с Подсистемой обеспечения информационной безопасности Системы обеспечения безопасности информации

	создания ключа ЭП, ключа проверки ЭП соответствующим требованиям 63-ФЗ.	
Basic Constraints	Тип сертификата ключа подписи. Допустимы два значения: • сертификат УЦ; • сертификат пользователя.	Обязательно для всех сертификатов
Extended Key Usage	Назначение использования ключей. Устанавливается в виде перечня идентификаторов. Перечень допустимых значений представлен в Приложении Б. Для обеспечения корректного использования сертификата в системе АСФК должны быть установлены следующие значения: • id-eku-GF01; • OID типа документа с правом подписи (один или несколько). Для обеспечения корректного использования сертификата в системе СЭД должно быть установлено следующее значение: • id-eku-GF03; Для обеспечения корректного использования сертификата в системе Landocs должно быть установлено следующее значение: • id-eku-GF02; Для обеспечения корректного использования сертификата в системе ЕИС должно быть установлено следующее значение: • id-kp-clientAuth; Для обеспечения корректного использования сертификата в системе ГМУ должны быть установлены следующие значения[4]:	Обязательно для всех сертификатов

[4] Данные атрибуты в составе сертификата необходимо использовать до завершения работ по интеграции ГМУ с Подсистемой обеспечения информационной безопасности Системы обеспечения безопасности информации

	• Один или несколько идентификаторов группы id-eku-GF09 в соответствие с полномочиями владельца сертификата.	
CRL Distribution Points	Множество точек распространения CAC в виде URL	Обязательно для всех сертификатов
Authority Information Access	Множество точек распространения информации о выпускающем УЦ. Устанавливается УЦ при создании сертификата и может содержать: • адрес публикации сертификата выпускающего УЦ; • адрес доступа к службе оперативной проверки статусов сертификатов по протоколу OCSP.	Обязательно для всех сертификатов
Subject Alternative Name	Для обеспечения корректного использования сертификата при аутентификации в службе каталога Active Directory (Microsoft) по смарт-карте должны быть заполнены следующие атрибуты: • в otherName должно быть задано UPN (User Principal Name) пользователя в формате user@fsfk.local, где User – имя учетной записи.	Не является обязательным

Табл. 4 Перечень допустимых значений для расширения Key Usage

№ п\п	Название	Смещение битовой маски	Описание
1	digitalSignature	0	Электронная подпись
2	nonRepudiation / contentCommitment	1	Неотрекаемость от авторства
3	keyEncipherment	2	Шифрование ключей
4	dataEncipherment	3	Шифрование данных
5	keyAgreement	4	Согласование ключей
6	keyCertSign	5	Проверка подписей сертификатов
7	cRLSign	6	Проверка электронной подписи САС
8	encipherOnly	7	Зашифрование
9	decipherOnly	8	Расшифрование

1.4. Правила обработки полей сертификата

При обработке атрибутов сертификата необходимо:

- для получения фамилии владельца сертификата необходимо использовать RDN surname поля subject;
- для получения имени и отчества необходимо использовать RDN givenName поля subject;
- для получения наименования должности необходимо использовать RDN title поля subject;
- в сертификате должностного лица в поле commonName поля subject указывается «Фамилия Имя Отчество», в сертификате юридического лица, индивидуального предпринимателя – наименование Заявителя;
- для получения наименования подразделения необходимо использовать RDN organizationUnitName поля subject;

- для получения наименования организации, где работает владелец сертификата необходимо использовать RDN organizationName поля subject;
- для получения наименования населенного пункта, где находится юридическое лицо, необходимо использовать RDN localityName поля subject;
- для получения наименования субъекта Российской Федерации, где находится юридическое лицо, необходимо использовать RDN StateOrProvinceName поля subject;
- для получения кода страны необходимо использовать RDN countryName поля subject (для России устанавливается RU);
- для получения адреса электронной почты владельца сертификата необходимо использовать RDN EMail поля subject;
- для получения адреса юридического лица необходимо использовать RDN streetAddress поля subject;
- для получения идентификатора безопасности необходимо использовать значение параметра OID=id-on-Landocsid атрибута Other Name расширения Subject Alternative Name;
- для получения номера ключа при смене сертификата необходимо использовать значение параметра OID=id-on-Keyid атрибута Other Name расширения Subject Alternative Name;
- для получения учетного номера организации необходимо использовать значение параметра OID=id-on-organizationId атрибута Other Name расширения Subject Alternative Name;
- для получения ИНН необходимо использовать RDN INN поля subject;
- для получения ОГРН необходимо использовать RDN OGRN поля subject;
- для получения ОГРНИП необходимо использовать RDN OGRNIP поля subject;
- для получения СНИЛС необходимо использовать RDN SNILS поля subject;
- для получения прав пользователя на подпись документов необходимо использовать значения идентификаторов расширения Extended Key Usage (перечень прав подписи различных типов документов представлен в Табл.5.1).

Сертификат юридического лица должен содержать минимальный набор следующих атрибутов имени:

- «Наименование юридического лица», (поле commonName);
- «Фамилия»*;
- «Имя, Отчество»*;
- «Страна»;
- «Субъект»;
- «Населенный пункт»;
- «Организация»;
- «Подразделение»*;
- «Должность»*;
- «E-mail»;
- «ИНН организации»;
- «ОГРН»;
- «СНИЛС»*;
- «Адрес».
- Неструктурированное имя=<имя системы/подсистемы на латинице> или Дополнительное имя субъекта (DNS-имя), SAN**

*- не указывается в сертификате, который используется при автоматическом подписании информации.

** - указывается в сертификате, который используется при автоматическом подписании информации.

Сертификат должностного лица должен содержать минимальный набор следующих атрибутов имени:

- «Фамилия Имя Отчество», (поле commonName);
- «Фамилия»;
- «Имя, Отчество»;
- «Страна»;
- «Организация»;
- «Подразделение»;
- «E-mail»;
- «ИНН»;
- «СНИЛС»
- «Субъект»***;
- «Населенный пункт»***.

*** - не обязательны к заполнению.

Сертификат ИП должен содержать минимальный набор следующих атрибутов имени:

- «Фамилия Имя Отчество», (поле commonName);

- «Фамилия»;
- «Имя, Отчество»;
- «Страна»;
- «Субъект»;
- «Населенный пункт»;
- «E-mail»;
- «ИНН»;
- «СНИЛС»;
- «ОГРНИП».

1.5 Правила проверки сертификата

При проверке сертификата должны быть выполнены следующие действия:

- проверка доверия к выпускающему УЦ;
- проверка ЭП УЦ в сертификате;
- проверка срока действия сертификата;
- проверка соответствия значений KeyUsage использованию ключевой пары сертификата;
- проверка соответствия значений Extended Key Usage использованию ключевой пары сертификата;
- проверка соответствия значений CertificatePolicies требованиям к классу средств ЭП;
- проверка статуса сертификата ключа проверки ЭП;
- проверка корректности атрибутов владельца сертификата.

1.5.1. Проверка доверия к выпускающему УЦ

Проверка доверия к выпускающему УЦ должна включать построение цепочки сертификатов УЦ, начиная с выпускающего УЦ, создавшего проверяемый сертификат и заканчивая доверенным сертификатом УЦ. При построении цепочки должны быть выполнены операции по проверке сертификатов цепочки в соответствие с требованиями раздела 6.1 RFC5280, включая, но не ограничиваясь, следующими операциями:

- проверку ЭП сертификата цепочки;

- проверку срока действия сертификата цепочки на требуемый момент времени;
- проверку наличия прав на создание сертификатов с расширением Extended Key Usage и значением расширения Extended Key Usage, соответствующим требованиям раздела 1.6.4. настоящего документа;
- проверку наличия прав на создание сертификатов с расширением CertificatePolicies и значением расширения CertificatePolicies, соответствующим требованиям раздела 1.5.5 настоящего документа;
- проверку одновременного присутствия следующих битовых масок KeyUsage: digitalSignature, nonRepudiation, keyCertSign (в случае отсутствия данного расширения проверка считается выполненной успешно);
- проверку наличия расширения Basic Constrains со значением IsCA=TRUE;
- другие проверки в соответствие с RFC5280.

Проверка доверия к первому сертификату цепочки должна выполняться на основании нахождения сертификата в хранилище сертификатов доверенных УЦ. В качестве доверенного хранилища могут использоваться:

- хранилище «Доверенные корневые центры сертификации» контекста LocalMachine операционной системы Microsoft Windows;
- хранилище «Корневые сторонние центры сертификации» контекста LocalMachine операционной системы Microsoft Windows;
- специализированное хранилище доверенных сертификатов ППО (при условии обеспечения защиты от изменения хранилища доверенных сертификатов пользователем ПО, не входящим в группу администраторов данного ПО).

1.5.2. Проверка ЭП УЦ в сертификате

Проверка ЭП УЦ в сертификате должна выполняться с использованием ключа проверки ЭП в сертификате выпускающего УЦ и полей signatureAlgorithm и signatureValue в сертификате пользователя.

1.5.3. Проверка срока действия сертификата

При проверке срока действия сертификата должна быть выполнена проверка выполнения одновременно двух условий:

- момент времени, на который осуществляется проверка, должен быть не раньше даты и времени, указанных в поле notBefore;
- момент времени, на который осуществляется проверка, должен быть не позже даты и времени, указанных в поле notAfter.

1.5.4. Проверка соответствия значений Extended Key Usage использованию ключевой пары сертификата

При проверке соответствия значений Extended Key Usage использованию ключевой пары сертификата необходимо выполнить:

- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе АСФК должна быть выполнена проверка наличия в списке идентификаторов OID, соответствующего типу электронного документа для которого выполняется проверка ЭП и идентификатора OID=id-eku-GF01;
- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе СЭД должна быть выполнена проверка наличия в списке идентификаторов OID, соответствующего типу электронного документа для которого выполняется проверка ЭП и идентификатора OID=id-eku-GF03;
- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе Landocs должна быть выполнена проверка наличия в списке идентификаторов OID=id-eku-GF02;
- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе ЕИС должна быть выполнена проверка наличия в списке идентификатора OID=id-kp-clientAuth;
- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе ГМУ должна быть выполнена проверка наличия в списке идентификаторов OID= id-kp-clientAuth и идентификатора полномочий пользователя, позволяющих создание ЭП данного типа (OID=id-eku-GF09).

1.5.5. Проверка соответствия значений CertificatePolicies требованиям к классу средств ЭП

При проверке соответствия значений дополнения CertificatePolicies сертификата выполняется проверка наличия идентификаторов определяющих класс средств ЭП.

1.5.6. Проверка статуса сертификата

Способ проверок статуса устанавливается отдельно для каждой из систем и может включать:

- проверка на основании локального CAC;
- проверка на основании локального CAC и изменений к нему;
- проверка на основании ответа службы оперативной проверки статусов сертификата (OCSP).

Проверка на основании локального CAC должна включать:

- проверку ЭП локального CAC, в том числе соответствие выпускающего УЦ, издавшего проверяемый сертификат, и УЦ, издавшего CAC;
- проверку срока действия CAC на момент времени проверки, в случае, если момент времени, на который осуществляется проверка, лежит за границами срока действия CAC, должна быть выполнена попытка или получить актуальный CAC (возможно использование для этого адреса точки распространения CAC в проверяемом сертификате), или уведомить пользователя о необходимости получить CAC, действительный на необходимую дату, или установить битовую маску для статуса проверки как CERT_TRUST_REVOCATION_STATUS_UNKNOWN5 или CERT_TRUST_IS_OFFLINE_REVOCATION.

Проверка на основании локального CAC и изменений к нему должна включать:

- проверку ЭП локального CAC, в том числе соответствие выпускающему УЦ, создавшего проверяемый сертификат, и УЦ, создавшего CAC;

5) При использовании Microsoft CryptoAPI

- проверку срока действия САС на момент времени проверки, в случае, если момент времени, на который осуществляется проверка, лежит за границами срока действия САС, должна быть выполнена попытка или получить актуальный САС (возможно использование для этого адреса точки распространения САС в проверяемом сертификате), или уведомить пользователя о необходимости получить САС, действительный на необходимую дату, или установить битовую маску для статуса проверки как CERT_TRUST_REVOCATION_STATUS_UNKNOWN или CERT_TRUST_IS_OFFLINE_REVOCATION;
- проверку ЭП дополнения к локальному САС, в том числе соответствие выпускающему УЦ, создавшего проверяемый сертификат, и УЦ, создавшего дополнение к САС;
- проверку срока действия дополнения к САС на момент времени проверки, в случае, если момент времени, на который осуществляется проверка, лежит за границами срока действия дополнения к САС, должна быть выполнена попытка или получить актуальный САС (возможно использование для этого адреса Freshest CRL в проверяемом сертификате), или уведомить пользователя о необходимости получить САС, действительный на необходимую дату, или установить битовую маску для статуса проверки как CERT_TRUST_REVOCATION_STATUS_UNKNOWN или CERT_TRUST_IS_OFFLINE_REVOCATION.

Проверка на основании ответа службы оперативной проверки статусов сертификата (OCSP) должна включать:

- обращение к службе OCSP в соответствие со спецификацией протокола;
- получение ответа службы OCSP;
- проверку соответствия идентификатора сертификата, отправленного службе OCSP, – полученному;
- проверку ЭП ответа службы OCSP, включая:
  - проверку отсутствия изменений в полученном ответе;
  - проверку ЭП УЦ в сертификате службы OCSP;
  - проверку наличия доверия к УЦ, создавшему сертификат службы OCSP;
  - проверку срока действия сертификата службы OCSP на текущий момент времени;

- проверку наличия идентификатора id-kp-OCSPSigning в расширении Extended Key Usage сертификата службы OCSP.

1.5.7. Проверка корректности атрибутов владельца сертификата

Проверка корректности атрибутов владельца сертификата должна выполняться при создании сертификата в установленном УЦ порядке.

1.5.8. Проверка доверия к головному УЦ

Проверка доверия к головному УЦ должна включать построение цепочки сертификатов УЦ, начиная с выпускающего УЦ, создавшего проверяемый сертификат, сертификатами информационных систем головного УЦ и заканчивая сертификатом головного УЦ. При построении цепочки должны быть выполнены операции по проверке сертификатов цепочки в соответствие с требованиями раздела 6.1 RFC5280, включая, но не ограничиваясь, следующими операциями:

- проверку ЭП сертификата цепочки;
- проверку срока действия сертификата цепочки на требуемый момент времени;
- проверку наличия прав на создание сертификатов с расширением Extended Key Usage и значением расширения Extended Key Usage, соответствующим требованиям раздела 1.6.4. настоящего документа;
- проверку наличия прав на создание сертификатов с расширением CertificatePolicies и значением расширения CertificatePolicies, соответствующим требованиям раздела 1.5.5 настоящего документа;
- проверку одновременного присутствия следующих битовых масок KeyUsage: digitalSignature, nonRepudiation, keyCertSign (в случае отсутствия данного расширения проверка считается выполненной успешно);
- проверку наличия расширения Basic Constrains со значением IsCA=TRUE;
- другие проверки в соответствие с RFC5280.

Проверка доверия к первому сертификату цепочки должна выполняться на основании нахождения сертификата в хранилище сертификатов доверенных УЦ. В качестве доверенного хранилища могут использоваться:

- хранилище «Доверенные корневые центры сертификации» контекста LocalMachine операционной системы Microsoft Windows;
- хранилище «Корневые сторонние центры сертификации» контекста LocalMachine операционной системы Microsoft Windows;
- специализированное хранилище доверенных сертификатов прикладного программного обеспечения (при условии обеспечения защиты от изменения хранилища доверенных сертификатов пользователем программного обеспечения, не входящим в группу администраторов данного программного обеспечения).

1.6. Порядок внесения изменений

При внесении изменений следует использовать следующие нотации:

- при добавлении идентификаторов CertificatePolicies должен использоваться принцип именования OID id-cp-<относительный ID>, не допускается повторное использование ранее зарегистрированных OID для целей, отличных от заявленных изначально. Любое изменение принципов обработки OID должно выполняться путем введения нового OID;
- при добавлении идентификаторов Extended Key Usage должен использоваться принцип именования OID id-eku-<относительный ID>, не допускается повторное использование ранее зарегистрированных OID для целей, отличных от заявленных изначально. Любое изменение принципов обработки OID должно выполняться путем введения нового OID;
- при добавлении идентификаторов Name расширения SubjectAlternativeName должен использоваться принцип именования OID id-on-<относительный ID>, не допускается повторное использование ранее зарегистрированных OID для целей, отличных от заявленных изначально. Любое изменение принципов обработки OID должно выполняться путем введения нового OID;
- при внесении изменений в содержание Subject сертификата недопустимо использование RDN для целей, отличных от описанных в X.500, X.501, X.509. В случае необходимости добавления атрибутов владельца сертификата в сертификат необходимо задействовать атрибут Other Name расширения SubjectAlternativeName.

Разработчик ПО, для использования в котором вводятся новые идентификаторы, обязан внести в функционал ПО следующие возможности:

- регистрацию текстовых описаний для используемых идентификаторов (OID) в реестр ОС Microsoft Windows при установке ПО;
- регистрацию декодировщиков в реестр ОС Microsoft Windows для корректного отображения атрибута Other Name расширения SubjectAlternativeName при установке ПО.

Приложение А (обязательное)

Перечень допустимых идентификаторов CertificatePolicies

В таблице (см. Табл. 5.1) представлен актуальный на момент составления документа перечень идентификаторов для использования в расширении CertificatePolicies сертификата. Данный перечень может дополняться в соответствие с разделом 4 настоящего документа.

Табл. 5.1. Перечень зарегистрированных идентификаторов

№ п\п	OID	Наименование	Назначение (для 1-9 – группы функций)	Примечание
1	1.2.643.100.113	id-cp-Subject	Класс средств ЭП. Базовый OID	
2	1.2.643.100.113.1	id-cp-Subject-КС1	Класс средства ЭП КС1	
3	1.2.643.100.113.2	id-cp-Subject-КС2	Класс средства ЭП КС2	

Приложение Б (обязательное)

Перечень допустимых идентификаторов

Extended Key Usage

В таблице (см. Табл. 5.1) представлен актуальный на момент составления документа перечень идентификаторов для использования в расширении Extended Key Usage сертификата. Данный перечень может дополняться в соответствие с разделом 4 настоящего документа.

Табл. 6.1. Перечень зарегистрированных идентификаторов Extended Key Usage

№	OID в новом порядке ЭП	Наименование	Назначение	Примечание
1.	1.2.643.3.61.1.1.6.502710.3.4.1.1 (1.2.643.3.251.1)*	id-eku-GF01	АСФК	для АСФК
2.	1.2.643.2.1.6.8.5 (1.2.643.3.251.1.1)*	id-eku-documentSigning	ЭП файла документа	
3.	1.2.643.3.61.1.1.6.502710.3.4.1.2 (1.2.643.3.251.1.2)*	id-eku-ftas2	ЭП документа ППО АС ФК	
4.	1.2.643.3.61.1.1.6.502710.3.4.1.3 (1.2.643.3.251.1.3)*	id-eku-ftas3	Подпись первичных документов, содержащих бюджетные данные	

* обозначены идентификаторы, которые будут использоваться после доработки соответствующего ППО.

5.	1.2.643.3.61.1.1.6.502710.3.4.1.4 (1.2.643.3.251.1.4)*	id-eku-ftas4	Подпись первичных документов ЗКР	
6.	1.2.643.3.61.1.1.6.502710.3.4.1.5 (1.2.643.3.251.1.5)*	id-eku-ftas5	Подпись первичных документов по обработке поступлений	
7.	1.2.643.3.61.1.1.6.502710.3.4.1.6 (1.2.643.3.251.1.6)*	id-eku-ftas6	Подпись электронных платежных документов	
8.	1.2.643.3.61.1.1.6.502710.3.4.1.7 (1.2.643.3.251.1.7)*	id-eku-ftas7	Подпись первичных документов по бухгалтерскому учету	
9.	1.2.643.3.61.1.1.6.502710.3.4.1.8 (1.2.643.3.251.1.8)*	id-eku-ftas8	Подпись отчетов	
10.	1.2.643.3.61.1.1.6.502710.3.4.1.9 (1.2.643.3.251.1.9)*	id-eku-ftas9	Подпись первичных документов по внесению изменений в НСИ	
11.	1.2.643.3.61.1.1.6.502710.3.4.1.10 (1.2.643.3.251.1.10)*	id-eku-ftas10	Подпись протоколов и квитанций	
12.	1.2.643.3.61.1.1.6.502710.3.4.1.11 (1.2.643.3.251.1.11)*	id-eku-ftas11	Имитозащита данных	
13.	1.2.643.3.61.1.1.6.502710.3.4.1.12 (1.2.643.3.251.1.12)*	id-eku-ftas12	Подпись файлов АСФК	

14.	1.2.643.3.61.1.1.6.502710.3.4.1.13 (1.2.643.3.251.1.13)*	id-eku-ftas13	Тестирование	
15.	1.2.643.3.61.1.1.6.502710.3.4.1.14 (1.2.643.3.251.1.14)*	id-eku-ftas14	Замещение права подписи	
16.	1.3.6.1.5.5.7.3.1	id-kp-serverAuth	Аутентификация сервера	Используется при установлении защищенного соединения по протоколу TLS для подтверждения подлинности сервера
17.	1.2.643.3.61.502710.1.6.3.3 (1.2.643.3.251.2)*	id-eku-GF02	Делопроизводство	для Landocs
18.	1.2.643.3.61.502710.1.6.3.2 (1.2.643.3.251.3)*	id-eku-GF03	Электронный документооборот	для СЭД
19.	1.2.643.3.61.506160.1.4.1.2 (1.2.643.3.251.4)*			Резерв ФК
20.	1.2.643.3.251.5			Резерв ФК
21.	1.2.643.3.251.5.1	id-eku-technological	Подпись пакетов информационного обмена между системами	
22.	1.2.643.3.251.5.2		Заказчик	Резерв ФК (только

				для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
23.	1.2.643.3.251.5.2.1		Заказчик. Администратор	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
24.	1.2.643.3.251.5.2.2		Заказчик. Уполномоченный специалист	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
25.	1.2.643.3.251.5.2.3		Заказчик. Должностное лицо с правом подписи контракта	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
26.	1.2.643.3.251.5.2.4		Заказчик. Специалист с правом направления проекта контракта участнику закупки	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших

				перерегистрацию в ЕИС)
27.	1.2.643.3.251.5.2.5		Заказчик. Специалист с правом согласования закупки	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
28.	1.2.643.3.251.5.2.6		Заказчик. Должностное лицо с правом удостоверения предварительной версии контракта	Резерв ФК (только для организаций ЗЧ ЕИС или не прошедших перерегистрацию в ЕИС)
29.	1.2.643.3.251.6	id-eku-GF06	ЭП в системе внутреннего документооборота	Для внутреннего ведомственного документооборота сторонних участников. Один идентификатор для внутреннего документооборота любого ведомства
30.	1.3.6.1.5.5.7.3.3	id-kp-codeSigning	ЭП программных компонентов	
31.	1.3.6.1.5.5.7.3.4	id-kp-emailProtection	Защита электронной	

			почты	
32.	1.3.6.1.5.5.7.3.8	id-kp-timeStamping	Подпись меток доверенного времени	
33.	1.3.6.1.5.5.7.3.9	id-kp-OCSPSigning	Подпись ответов службы OCSP	
34.	1.2.643.3.251.7			Резерв ФК
35.	1.2.643.3.251.8	id-eku-GF09	Работа с ГМУ. Базовый OID	
36.	1.2.643.3.251.8.1	id-eku-GF09-admin	Работа с ГМУ. ЭП администратора организации	
37.	1.2.643.3.251.8.2	id-eku-GF09-authorized	Работа с ГМУ. ЭП уполномоченного специалиста	
38.	1.2.643.100.2			Резерв ФК
39.	1.3.6.1.4.1.5147.11.1.2	id-eku-GF11	Работа с биржами	Для ПО торгового терминала при проведении депозитного аукциона
40.	1.3.6.1.4.1.5147.11.1.22	id-eku-GF11-deposit-auction	ПО «ЛУЧ»	Используется для заключения электронных договоров по

				итогам депозитного аукциона
41.	1.2.643.6.22.255.1	id-eku-GF11-certificate	Сертификат	Сертификат выдан внешним аккредитованным УЦ (для ИС СПВБ)
42.	1.2.643.6.22.3	id-eku-GF11-system	Транспортные системы СПВБ	
43.	1.2.643.6.22.2.2.1	id-eku-GF12	СЭД СПВБ с Федеральным казначейством	
44.	1.3.6.1.4.1.311.20.2.2	id-eku-GF13	Вход в систему с помощью смарт-карты	
45.	1.2.643.3.251.9	id-eku-certrequest	Подпись запросов на издание сертификатов ключей проверки электронной подписи	Полномочие пользователя для подписания запросов на создание сертификатов
46.	1.3.6.1.5.5.7.3.2	id-kp-clientAuth	Аутентификация клиента	Используется при установлении защищенного соединения по протоколу TLS для подтверждения

				подлинности клиента
47.	1.2.643.3.251.10.13	id-eku-use-restriction	Ограничения на использование квалифицированного сертификата (если имеется)	Используется при наличии ограничений
48.	1.2.643.5.1.24.2.43		Для Росреестра	Для работы сотрудников ТОФК, осуществляющих полномочия в контрольно-ревизионной сфере, а также обеспечения административно-хозяйственной деятельности ТОФК на сайте Федеральной службы государственной регистрации, кадастра и картографии

Приложение В (обязательное)

Перечень допустимых значений SubjectAlternativeName.OtherName

Согласно RFC5280 атрибут OtherName расширения SubjectAlternativeName должен кодироваться как объект класса TYPE-IDENTIFIER (см. X.681).

```
TYPE-IDENTIFIER ::= CLASS {
    &id OBJECT IDENTIFIER UNIQUE,
    &Type
  }
  WITH SYNTAX { &Type IDENTIFIED BY &id }
```

При этом id указывается в колонке «OID», а Type – в колонке «Тип кодирования данных» таблицы Табл. 7.2.

Табл. 7.2. Перечень допустимых значений SubjectAlternativeName.OtherName

№ п\п	OID	Наименование	Данные	ASN.1 тип данных	Область применения
1.	1.2.643.1.12345.1	id-on-Landocsid	идентификатор безопасности	DirectoryString	Landocs
2.	1.2.643.3.61.5027 10.1.9	id-on-Keyid	идентификатор ключей пользователя при смене сертификата	DirectoryString	СЭД, АСФК
3.	1.2.643.3.61.5027 10.1.8	id-on-InstitutionId	учетный номер организации	DirectoryString	ГМУ