ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
(КАЗНАЧЕЙСТВО РОССИИ)

УТВЕРЖДАЮ
Заместитель руководителя
Федерального казначейства
_____С.Б. Гуральников

«25» апреля 2016 г.

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

Версия 3
Листов 60

СОГЛАСОВАНО
Начальник управления
режима секретности и
безопасности информации
_____ (В.С. Бражко)
«21» апреля 2016 г.

СОГЛАСОВАНО
Начальник управления
финансовых технологий
_____ (В.В. Ткаченко)
«20» апреля 2016 г.

Содержание

1.1. Назначение документа 3
1.2. Список сокращений 3
1.3. Термины и определения 4
1.4. Правила заполнения полей сертификата 5
1.5. Правила обработки полей сертификата 18
1.6. Правила проверки сертификата 21
1.7. Порядок внесения изменений 27
Приложение А (обязательное) 28
Приложение Б (обязательное) 30
Приложение В (обязательное) 60

1.1. Назначение документа

Настоящий документ содержит описание структуры и порядка использования полей сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром Федерального казначейства, с целью формализации атрибутов сертификата и порядка обработки информации, содержащейся в сертификате, в рамках информационных систем Федерального казначейства.

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 сертификата может включать значения, указанные в приложении «Б» к настоящим правилам.

1.2. Список сокращений

Сокращение	Описание
АРМ	Автоматизированное рабочее место
АС ФК	Автоматизированная система Федерального казначейства
ЕИС	Единая информационная система
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СПТО	Система поддержки технологического обеспечения
СЭД	Система электронного документооборота
ФК	Федеральное казначейство (Казначейство России)
ЦА ФК	Центральный аппарат Федерального казначейства
ГМУ	Официальный сайт Российской Федерации в сети «Интернет» для размещения информации об учреждениях
СПВБ	Санкт-Петербургская Валютная Биржа
СПЗ	Сводный перечень заказчиков

1.3. Термины и определения

Владелец сертификата ключа проверки электронной подписи	Лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – 63-ФЗ) порядке выдан сертификат ключа проверки электронной подписи
Ключ электронной подписи	Уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
Аннулированные сертификата ключа проверки электронной подписи	Процедура отзыва сертификата ключа проверки электронной подписи до истечения срока его действия
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
Квалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
CAC (Список аннулированных сертификатов)	Электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы

УЦ (Удостоверяющий центр)	Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные 63-ФЗ
ЭП (Электронная подпись)	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

1.4. Правила заполнения полей сертификата

Перечень основных полей приведен в
Таб. 1.

Таб. 1 Перечень основных полей

№ п\п	Поле	Описание
Основная информация		
1	Version	Версия формата сертификата X.509. Устанавливается УЦ при издании сертификата версия 3
2	Serial Number	Серийный номер сертификата ключа проверки электронной подписи. Устанавливается УЦ при издании сертификата. Комбинация полей Issuer, authorityKeyIdentifire и Serial Number является уникальным идентификатором сертификата ключа проверки электронной подписи
3	Signature	Идентификатор алгоритма электронной подписи, в соответствии с которым была осуществлена подпись настоящего

		сертификата УЦ
4	Issuer	Уникальное имя (Distinguished name, далее – DN) выпускающего УЦ. Устанавливается УЦ при издании сертификата
5	Validity	Срок действия сертификата ключа проверки электронной подписи[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 Таб. 2
7	Subject Public Key Info	Алгоритм и значение ключа проверки электронной подписи. Устанавливается УЦ при издании сертификата
8	Unique Identifiers	Не должен использоваться
9	Extensions	Расширения (детальное описание представлено в Таб. 3.)
Электронная подпись УЦ		
10	signatureAlgorithm	алгоритм ЭП
11	signatureValue	значение ЭП

Таб. 2 Перечень используемых относительных уникальных имен

Поле	Описание поля	Рекомендованная кодировка	Максимальная длина значения поля	Обязательность
SurName	Фамилия владельца сертификата с большой буквы в одно слово без пробелов	UTF8String	не более 2000 символов	Обязательно для всех систем, за исключением

1) Для КриптоПро CSP установлены следующие максимальные сроки действия ключей:

максимальный срок действия ключей электронной подписи для шифрования и ЭП - 1 год 3 месяца; максимальный срок действия ключей проверки электронной подписи (уровень защиты КС1) – 30 лет, (уровень защиты КС2) – 25 лет, (уровень защиты КС3) – 15 лет.

				сертификата юридического лица, в котором отсутствует ФИО
GivenName	ИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (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 одним словом, части которого соединены «подчеркиванием» без пробелов.	UTF8String	не более 2000 символов	Обязательно для всех систем, за исключением сертификата юридического лица, в котором отсутствует ФИО
Title	Должность владельца	UTF8String.	не более 2000	Обязатель

	сертификата		символов	но для всех систем, использующих сертификат юридического лица, за исключением сертификата юридического лица, в котором отсутствует ФИО
UnstructuredName	Наименование в свободной форме. Указывается код из справочника должностей (ведётся в ЦАФК)	PrintableString или UTF8String	в соответствии с PKCS#9 – 255 символов	Обязательно для АСФК, за 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 систем, за исключением сертифика

				та юридического лица, в котором отсутствует ФИО
OrganizationalUnit	Организационное подразделение владельца сертификата. Допускается многократное включение данного RDN для создания иерархии подразделений, при этом следует учитывать, что подразделение более высокой иерархии должно идти перед подразделением более низкой иерархии	UTF8String.	не более 2000 символов	Не обязательно
Organization	Наименование организации, от имени которой действует владелец сертификата, либо наименование организации-владельца сертификата (как в ЕГРЮЛ).	UTF8String	не более 2000 символов	Обязательно для всех систем
Locality	Наименование населенного пункта (город, село)	UTF8String	в соответствии с RFC5280 – 128 символов	Обязательно для всех систем
State	Наименование соответствующего субъекта Российской Федерации	UTF8String	в соответствии с RFC5280 – 128 символов	Обязательно для всех систем

Country	Двухбуквенный код страны в соответствие с ISO 3166. Для России указывается RU	PrintableString	в соответствии с RFC5280 – 2 символа	Обязательно для всех систем
EMail	Адрес электронной почты 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 № 795 длина поля составляет 12 символов	Обязательно для квалифицированного сертификата. Для сертификата

				заявителя указывается ИНН сотрудника Организации-заявителя. Для сертификата Организации-заявителя – ИНН юридического лица.

Таб. 3. Описание Extensions

Наименование поля	Описание поля	Обязательность
Authority Key Identifier	Идентификатор ключа проверки электронной подписи выпускающего УЦ в форме keyIdentifier. Требуется указание authorityCertIssuer (наименование издателя) и authorityCertSerialNumber (номер квалифицированного сертификата аккредитованного УЦ)	Обязательно для всех систем
Subject Key Identifier	Идентификатор ключа проверки электронной подписи сертификата. Устанавливается УЦ при издании сертификата	Обязательно для всех систем
Key Usage	Назначение использования ключей. Устанавливается в виде битовой маски. Перечень допустимых значений представлен в Таб.4. Для обеспечения корректного использования сертификата в системах ФК должны быть установлены следующие значения:	Обязательно для всех систем

	• digitalSignature; • nonRepudiation; • dataEncipherment; • keyEncipherment; • keyAgreement. Для разрабатываемых систем должны быть использованы значения в соответствие с RFC 4491 для сертификатов ключей проверки электронной подписи ГОСТ Р 34.10-2001	
Certificate Policies	Класс средств электронной подписи владельца квалифицированного сертификата. Устанавливается в виде списка идентификаторов. Перечень допустимых значений для использования в различных системах приведен в Приложении А. Для обеспечения корректного использования сертификата в системах Oracle (АСФК), СПТО, СЭД, Landocs, ЕИС, ГМУ должны быть установлены следующие значения: • id-cp-Subject-KC2.	Обязательно для всех систем
Subject Alternative Name	Дополнительные сведения о владельце сертификата ключа проверки электронной подписи. 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	Обязательно для конкретной системы

	(URI); • iPAddress – IP-адрес; • registeredID – идентификатор в виде OID. Для обеспечения корректного использования сертификата в системе Oracle (АСФК) должны быть заполнены следующие атрибуты: • 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 СПТО должны быть заполнены следующие атрибуты: • otherName должен содержать номер ключа при смене сертификата в качестве значения параметра OID=id-on-Keyid. 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 получается следующим образом: 1) если у пользователя нет сертификата для Landocs идентификатор формируется в виде GUID; 2) если у пользователя есть сертификат для Landocs идентификатор копируется из существующего сертификата. Для обеспечения корректного использования сертификата в системе ЕИС должны быть заполнены следующие атрибуты: otherName должен содержать учетный номер организации в СПЗ в качестве значения параметра OID=id-on-OrganizationId; (заполняется при необходимости) Для обеспечения корректного использования сертификата в системе ГМУ должны быть заполнены следующие атрибуты: • otherName должен содержать код ГМУ организации в качестве значения параметра OID=id-on-InstitutionId; (заполняется при необходимости)	
Issuer Alternative Name	Дополнительные сведения об УЦ, издавшем сертификат. Устанавливается УЦ при издании сертификата	Не обязательно
subjectSignTool (1.2.643.100.111)	Наименование используемого владельцем квалифицированного сертификата средства электронной подписи	Обязательно для всех систем
issuerSignTool (1.2.643.100.112)	Наименование средств электронной подписи и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизитов документов, подтверждающего соответствие указанных средств требованиям, установленным законодательством РФ.	Обязательно для всех систем

	Должны быть заполнены следующие атрибуты: • signTool – включает полное наименование средств ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного 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 квалифицированного сертификата, требованиям 63-ФЗ; • cAToolCert - включает реквизиты заключения ФСБ России о подтверждении соответствия средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП требованиям 63-ФЗ	
Basic Constraints	Тип сертификата ключа подписи. Допустимы два значения: • сертификат УЦ; • сертификат пользователя. Для сертификатов пользователей систем Oracle (АСФК), СПТО, СЭД, Landocs, ЕИС, ГМУ должно быть установлено значение «сертификат пользователя»	Обязательно для всех систем
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 Oracle (АСФК) должны быть установлены следующие значения:	Обязательно для всех систем

	• id-eku-GF01; • OID типа документа с правом подписи (один или несколько). Для обеспечения корректного использования сертификата в системе СПТО должны быть заполнены установлены следующие значения: • id-eku-GF07; • OID типа документа с правом подписи (один или несколько). Для обеспечения корректного использования сертификата в системе СЭД должны быть установлены следующие значения: • id-eku-GF03; Для обеспечения корректного использования сертификата в системе Landocs должны быть установлены следующие значения: • id-eku-GF02; Для обеспечения корректного использования сертификата в системе ЕИС должны быть установлены следующие значения: • Один или несколько идентификаторов группы id-eku-GF05 в соответствие с полномочиями организации владельца сертификата и самого владельца сертификата; • id-kp-clientAuth; Для обеспечения корректного использования сертификата в системе ГМУ должны быть установлены следующие значения: • Один или несколько идентификаторов группы id-eku-GF09 в соответствие с полномочиями владельца сертификата; Для обеспечения корректного использования сертификата в системе СМЭВ должны быть установлены следующие значения:	

	• Один идентификатор группы id-eku-GF10 в соответствие с полномочиями владельца сертификата или полномочиями организации • id-kp-clientAuth	
CRL Distribution Points	Множество точек распространения списков аннулированных сертификатов в виде URL	Обязательно для всех систем
Authority Information Access	Множество точек распространения информации о выпускающем УЦ. Устанавливается УЦ при издании сертификата и может содержать: • адрес публикации сертификата выпускающего УЦ • адрес доступа к службе оперативной проверки статусов сертификатов по протоколу OCSP. Для обеспечения корректного использования сертификата в системе Oracle (АСФК), СПТО, СЭД, Landocs, ЕИС, ГМУ должны быть установлены следующие значения: • адрес доступа к службе OCSP	Обязательно для всех систем
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	Обязательно для всех систем

Таб. 4 Перечень допустимых значений для расширения Key Usage

№ п\п	Название	Смещение битовой	Описание

		маски	
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 квалифицированных сертификатов
7	cRLSign	6	Проверка электронной подписи CAC
8	encipherOnly	7	Зашифрование
9	decipherOnly	8	Расшифрование

1.5. 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;
- для получения кода должности из справочника ЦАФК необходимо использовать RDN UnstructuredName поля Subject;
- в сертификате Заявителя в поле CommonName поля Subject указывается «Фамилия Имя Отчество», в сертификате Организации-заявителя – наименование Организации-заявителя;
- для получения наименования подразделения необходимо использовать RDN OrganizationalUnit поля Subject;
- для получения наименования организации, где работает владелец сертификата ключа проверки электронной подписи необходимо использовать RDN Organization поля Subject;
- для получения наименования населенного пункта, где расположено место работы владельца сертификата ключа проверки электронной подписи необходимо использовать RDN Locality поля Subject;

- для получения наименования субъекта Российской Федерации, где расположено место работы владельца сертификата ключа проверки электронной подписи необходимо использовать RDN State поля Subject;
- для получения кода страны необходимо использовать RDN Country поля Subject (для России устанавливается RU);
- для получения адреса электронной почты владельца сертификата необходимо использовать RDN EMail поля Subject;
- для получения адреса Организации - заявителя 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 организации пользователя необходимо использовать RDN OGRN поля Subject;
- для получения СНИЛС (физического лица) необходимо использовать RDN SNILS поля Subject;
- для получения учетной записи пользователя АСФК необходимо использовать значение параметра OID=pkcs9_at_friendlyName атрибута Other Name расширения Subject Alternative Name;
- для получения учетного номера организации в справочнике ОГС необходимо использовать значение параметра OID=id-on-InstitutionId атрибута Other Name расширения Subject Alternative Name;
- для получения полномочий организации и полномочий пользователя в ЕИС необходимо использовать значения идентификаторов расширения Extended Key Usage (полномочия организации являются составной частью идентификатора полномочий пользователя, перечень возможных полномочий организаций представлен в Таб.5.1);

- для получения полномочий пользователя на ГМУ необходимо использовать значения идентификаторов расширения Extended Key Usage (перечень возможных полномочий пользователей представлен в Таб.5.1);
- для получения прав пользователя на подпись документов необходимо использовать значения идентификаторов расширения Extended Key Usage (перечень прав подписи различных типов документов представлен в Таб.5.1).

Сертификат Организации-заявителя должен содержать как минимум следующие поля:

- «Наименование юридического лица», (поле CommonName);
- «Фамилия»*;
- «Имя, Отчество»*;
- «Страна»;
- «Субъект»;
- «Населенный пункт»;
- «Организация»;
- «Подразделение»;
- «Должность»*;
- «E-mail»;
- «ИНН организации»;
- «ОГРН»;
- «СНИЛС»*;
- «Адрес».

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

Сертификат Заявителя должен содержать как минимум следующие поля:

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

1.6 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 Certificate Policies требованиям к классу средств ЭП;
- проверка статуса сертификата ключа проверки электронной подписи;
- проверка корректности атрибутов владельца сертификата ключа проверки электронной подписи.

1.6.1. Проверка доверия к выпускающему УЦ

Проверка доверия к выпускающему УЦ должна включать построение цепочки сертификатов УЦ, начиная с выпускающего УЦ, издавшего 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 издание сертификатов с расширением Extended Key Usage и значением расширения Extended Key Usage, соответствующим требованиям раздела 1.6.4. настоящего документа;
- проверку наличия прав на издание сертификатов с расширением Certificate Policies и значением расширения Certificate Policies, соответствующим требованиям раздела 1.6.5 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).

1.6.2. Проверка ЭП УЦ в сертификате

Проверка ЭП УЦ в сертификате должна выполняться на основании ключа проверки электронной подписи в сертификате выпускающего УЦ и полей signatureAlgorithm и signatureValue в сертификате пользователя.

1.6.3. 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.

1.6.4. 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 Oracle (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 СПТО должна быть выполнена проверка наличия в списке идентификаторов OID, соответствующего типу электронного документа для которого выполняется проверка ЭП и идентификатора OID=id-eku-GF07;
- 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 идентификаторов OID= id-kp-clientAuth и идентификатора полномочий пользователя и организации пользователя, позволяющих создание ЭП данного типа;
- 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;
- для признания значений Extended Key Usage соответствующих использованию ключевой пары в системе межведомственного электронного взаимодействия (СМЭВ) должна быть выполнена проверка наличия в списке идентификаторов OID=id-eku-GF10.

1.6.5. Проверка соответствия значений Certificate Policies требованиям к классу средств ЭП

При проверке соответствия значений Certificate Policies подписи требованиям к классу средств ЭП необходимо выполнить проверку наличия идентификаторов определяющих класс средств ЭП.

1.6.6. Проверка статуса сертификата ключа проверки электронной подписи

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

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

Проверка на основании локального списка аннулированных сертификатов 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 CDP 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_UNKNOWN2 или CERT_TRUST_IS_OFFLINE_REVOCATION.

Проверка на основании локального списка аннулированных сертификатов и изменений к нему должна включать:

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

---

2) 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 CDP 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, издавшего проверяемый сертификат, и УЦ, издавшего 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 какCERT_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, выпустившему 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.

1.6.7. Проверка корректности атрибутов владельца сертификата ключа проверки электронной подписи

Проверка корректности атрибутов владельца сертификата ключа проверки электронной подписи должна выполняться на стадии утверждения издания сертификата обслуживающим персоналом УЦ.

1.6.8. Проверка доверия к головному УЦ

Проверка доверия к головному УЦ должна включать построение цепочки сертификатов УЦ, начиная с выпускающего УЦ, издавшего 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 издание сертификатов с расширением Extended Key Usage и значением расширения Extended Key Usage, соответствующим требованиям раздела 1.6.4. настоящего документа;
- проверку наличия прав на издание сертификатов с расширением Certificate Policies и значением расширения Certificate Policies, соответствующим требованиям раздела 1.6.5 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).

1.7. Порядок внесения изменений

При внесении изменений следует использовать следующие нотации:

- при добавлении идентификаторов Certificate Policies 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 Other 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 ключа проверки электронной подписи 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 программного обеспечения, для использования в котором вводятся новые идентификаторы, обязан внести в функционал программного обеспечения следующие возможности:

- регистрацию текстовых описаний для используемых идентификаторов (OID) в реестр ОС Microsoft Windows при установке программного обеспечения;

- регистрацию декодировщиков в реестр ОС Microsoft Windows для корректного отображения атрибута Other Name расширения SubjectAlternativeName при установке программного обеспечения.

Внесение изменений в формат сертификата осуществляется Федеральным казначейством. Федеральное казначейство оставляет за собой право согласовать формат с другими разработчиками эксплуатируемых систем и не принимать изменения до получения согласия всех разработчиков эксплуатируемых систем.

Приложение А (обязательное)

Перечень допустимых идентификаторов Certificate Policies

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

Таб. 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	В соответствие с приказом ФСБ России № 795
3	1.2.643.100.113.2	id-cp-Subject-КС2	Класс средства ЭП КС2	
4	1.2.643.100.113.3	id-cp-Subject-КС3	Класс средства ЭП КС3	
5	1.2.643.100.113.4	id-cp-Subject-КВ1	Класс средства ЭП КВ1	
6	1.2.643.100.113.5	id-cp-Subject-КВ2	Класс средства ЭП КВ2	
7	1.2.643.100.113.6	id-cp-Subject-КА1	Класс средства ЭП КА1	

Приложение Б (обязательное)

Перечень допустимых идентификаторов Extended Key Usage

В таблице (см. Таб. 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.

В сертификате для работы в ЕИС может быть использовано только одно полномочие Организации, за исключением полномочий, указанных в строках под номерами 102, 105.

Таб. 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.	1.2.643.3.251.3	id-eku-GF03	Электронный документооборот	для СЭД
19.	1.2.643.3.61.506160.1.4.1.2 (1.2.643.3.251.4)*	id-eku-GF08	ЭП документа СПТО	
20.	1.2.643.3.251.5	id-eku-GF05	Работа с ЕИС. Базовый OID	
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	id-eku-GF05-customer	Заказчик. Базовый OID	Полномочия организации «Заказчик»
23.	1.2.643.3.251.5.2.1	id-eku-GF05-customer-admin	Заказчик. Администратор организации	
24.	1.2.643.3.251.5.2.2	id-eku-GF05-	Заказчик.	

		customer-authorized	Уполномоченный специалист	
25.	1.2.643.3.251.5.2.3	id-eku-GF05-customer-sign	Заказчик. Должностное лицо с правом подписи контракта	
26.	1.2.643.3.251.5.2.4	id-eku-GF05-customer-template	Заказчик. Специалист с правом направления проекта контракта участнику закупки	
27.	1.2.643.3.251.5.2.5	id-eku-GF05-customer-submit	Заказчик. Специалист с правом согласования закупки	
28.	1.2.643.3.251.5.2.6	id-eku-GF05-customer-contract	Должностное лицо с правом удостоверения предварительной версии контракта	
29.	1.2.643.3.251.5.3	id-eku-GF05-authorizedOrgan	Уполномоченный орган. Базовый OID	Полномочия организации «уполномоченный орган»
30.	1.2.643.3.251.5.3.1	id-eku-GF05-authorizedOrgan-admin	Уполномоченный орган. Администратор организации	
31.	1.2.643.3.251.5.3.2	id-eku-GF05-authorizedOrgan-authorized	Уполномоченный орган. Уполномоченный специалист	
32.	1.2.643.3.251.5.3.3	id-eku-GF05-	Уполномоченный орган.	

		authorizedOrgan-template	Специалист с правом направления проекта контракта участнику закупки	
33.	1.2.643.3.251.5.3.4	id-eku-GF05-authorizedOrgan-copysign	Уполномоченный орган. Должностное лицо с правом подписи копии контракта	
34.	1.2.643.3.251.5.3.5	id-eku-GF05-authorizedOrgan-submit	Уполномоченный орган. Специалист с правом согласования закупки	
35.	1.2.643.3.251.5.3.6	id-eku-GF05-authorizedOrgan-sign	Уполномоченный орган. Должностное лицо с правом подписи контракта	
36.	1.2.643.3.251.5.3.7	id-eku-GF05-authorizedOrgan-preliminary	Уполномоченный орган. Должностное лицо с правом удостоверения предварительной версии контракта	
37.	1.2.643.3.251.5.4	id-eku-GF05-specializedOrg	Специализированная организация. Базовый OID	Полномочия организации «специализированная организация»
38.	1.2.643.3.251.5.4.1	id-eku-GF05-specializedOrg-admin	Специализированная организация. Администратор	

			организации	
39.	1.2.643.3.251.5.4.2	id-eku-GF05-specializedOrg-authorized	Специализированная организация. Уполномоченный специалист	
40.	1.2.643.3.251.5.5	id-eku-GF05-supervising	Контрольный орган в сфере закупок. Базовый OID	Полномочия организации «контрольный орган в сфере закупок»
41.	1.2.643.3.251.5.5.1	id-eku-GF05-supervising-admin	Контрольный орган в сфере закупок. Администратор организации	
42.	1.2.643.3.251.5.5.2	id-eku-GF05-supervising-authorized	Контрольный орган в сфере закупок. Уполномоченный специалист	
43.	1.2.643.3.251.5.6	id-eku-GF05-financial	Финансовый орган. Базовый OID	Полномочия организации «Финансовый орган»
44.	1.2.643.3.251.5.6.1	id-eku-GF05-financial-admin	Финансовый орган. Администратор организации	
45.	1.2.643.3.251.5.6.2	id-eku-GF05-financial-authorized	Финансовый орган. Уполномоченный специалист	
46.	1.2.643.3.251.5.7	id-eku-GF05-	Организация,	Полномочия организации

		siteOperator	оказывающая услуги по обслуживанию пользователей ЕИС. Базовый OID	«оператор общероссийского официального сайта»
47.	1.2.643.3.251.5.7.1	id-eku-GF05-siteOperator-admin	Организация, оказывающая услуги по обслуживанию пользователей ЕИС. Администратор организации	
48.	1.2.643.3.251.5.7.2	id-eku-GF05-siteOperator-authorized	Организация, оказывающая услуги по обслуживанию пользователей ЕИС. Уполномоченный специалист	
49.	1.2.643.3.251.5.8	id-eku-GF05-tradingOperator	Оператор электронной площадки. Базовый OID	Полномочия организации «оператор электронной площадки»
50.	1.2.643.3.251.5.8.1	id-eku-GF05-tradingOperator-admin	Оператор ЭП. Администратор организации	
51.	1.2.643.3.251.5.8.2	id-eku-GF05-tradingOperator-authorized	Оператор ЭП. Уполномоченный специалист	
52.	1.2.643.3.251.5.9	id-eku-GF05-	Орган, уполномоченный	Полномочия организации

		reestrOperator	на ведение реестра недобросовестных поставщиков Базовый OID	«Орган, уполномоченный на ведение реестра недобросовестных поставщиков»
53.	1.2.643.3.251.5.9.1	id-eku-GF05-reesrtOperator-admin	Орган, уполномоченный на ведение реестра недобросовестных поставщиков. Администратор организации	
54.	1.2.643.3.251.5.9.2	id-eku-GF05-reesrtOperator-authorized	Орган, уполномоченный на ведение реестра недобросовестных поставщиков. Уполномоченный специалист	
55.	1.2.643.3.251.5.10	id-eku-GF05-audit	Орган аудита в сфере закупок, Базовый OID	Организация, осуществляющая аудит в сфере закупок
56.	1.2.643.3.251.5.10.1	id-eku-GF05-audit-admin	Орган аудита в сфере закупок. Администратор организации	
57.	1.2.643.3.251.5.10.2	id-eku-GF05-audit-authorized	Орган аудита в сфере закупок. Уполномоченный специалист	

58.	1.2.643.3.251.5.11	id-eku-GF05-normalization	Орган, размещающий правила нормирования, Базовый OID	Полномочия организации «Орган, размещающий правила нормирования»
59.	1.2.643.3.251.5.11.1	id-eku-GF05-normalization-admin	Орган, размещающий правила нормирования. Администратор организации	
60.	1.2.643.3.251.5.11.2	id-eku-GF05-normalization-authorized	Орган, размещающий правила нормирования. Уполномоченный специалист	
61.	1.2.643.3.251.5.12	id-eku-GF05-requirement	Орган, устанавливающий требования к отдельным видам товаров, работ, услуг и (или) нормативные затраты. Базовый OID	Полномочия организации «Орган, устанавливающий требования к отдельным видам товаров, работ, услуг и (или) нормативные затраты»
62.	1.2.643.3.251.5.12.1	id-eku-GF05-requirement-admin	Орган, устанавливающий требования к отдельным видам товаров, работ, услуг и (или) нормативные затраты. Администратор организации	

63.	1.2.643.3.251.5.12.2	id-eku-GF05-requirement-authorized	Орган, устанавливающий требования к отдельным видам товаров, работ, услуг и (или) нормативные затраты. Уполномоченный специалист	
64.	1.2.643.3.251.5.13	id-eku-GF05-bank	Банк. Базовый OID	Полномочия организации «Банк»
65.	1.2.643.3.251.5.13.1	id-eku-GF05-bank-admin	Банк. Администратор организации	
66.	1.2.643.3.251.5.13.2	id-eku-GF05-bank-authorized	Банк. Уполномоченный специалист	
67.	1.2.643.3.251.5.14	id-eku-GF05-type	Орган, разрабатывающий типовые контракты и типовые условия контрактов. Базовый OID	Полномочия организации «Орган, разрабатывающий типовые контракты и типовые условия контрактов»
68.	1.2.643.3.251.5.14.1	id-eku-GF05-type-admin	Орган, разрабатывающий типовые контракты и типовые условия контрактов. Администратор	

			организации	
69.	1.2.643.3.251.5.14.2	id-eku-GF05-type-authorized	Орган, разрабатывающий типовые контракты и типовые условия контрактов. Уполномоченный специалист	
70.	1.2.643.3.251.5.15	id-eku-GF05-contract	Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ. Базовый OID	Полномочия организации «Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ»
71.	1.2.643.3.251.5.15.1	id-eku-GF05-contract-admin	Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ.	

			Администратор организации	
72.	1.2.643.3.251.5.15.2	id-eku-GF05-contract-authorized	Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ. Уполномоченный специалист	
73.	1.2.643.3.251.5.15.3	id-eku-GF05-contract-sign	Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ. Должностное лицо с правом подписи контракта	
74.	1.2.643.3.251.5.15.4	id-eku-GF05-contract-template	Организация, осуществляющая	

			полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ. Специалист с правом направления проекта контракта участнику закупки	
75.	1.2.643.3.251.5.15.5	id-eku-GF05-contract-copysign	Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Федерального закона № 44-ФЗ. Должностное лицо с правом подписи копии контракта	
76.	1.2.643.3.251.5.16	id-eku-GF05-federal	Орган по регулированию контрактной системы в сфере закупок. Базовый	Полномочия организации «Орган по регулированию контрактной системы в сфере закупок»

			OID	
77.	1.2.643.3.251.5.16.1	id-eku-GF05-federal-admin	Орган по регулированию контрактной системы в сфере закупок. Администратор организации	
78.	1.2.643.3.251.5.16.2	id-eku-GF05-federal-authorized	Орган по регулированию контрактной системы в сфере закупок. Уполномоченный специалист	
79.	1.2.643.3.251.5.17	id-eku-GF05-Instauthorized	Уполномоченное учреждение. Базовый OID	Полномочия организации «уполномоченное учреждение»
80.	1.2.643.3.251.5.17.1	id-eku-GF05-Instauthorized-admin	Уполномоченное учреждение. Администратор организации	
81.	1.2.643.3.251.5.17.2	id-eku-GF05-Instauthorized-authorized	Уполномоченное учреждение. Уполномоченный специалист	
82.	1.2.643.3.251.5.17.3	id-eku-GF05-Instauthorized-sign	Уполномоченное учреждение.	

			Должностное лицо с правом подписи контракта	
83.	1.2.643.3.251.5.17.4	id-eku-GF05-Instauthorized-template	Уполномоченное учреждение. Специалист с правом направления проекта контракта участнику закупки	
84.	1.2.643.3.251.5.17.5	id-eku-GF05-Instauthorized-copysign	Уполномоченное учреждение. Должностное лицо с правом подписи копии контракта	
85.	1.2.643.3.251.5.17.6	id-eku-GF05-Instauthorized-submit	Уполномоченное учреждение. Специалист с правом согласования закупки	
86.	1.2.643.3.251.5.17.7	id-eku-GF05-Instauthorized-preliminary	Уполномоченное учреждение. Должностное лицо с правом удостоверения предварительной версии контракта	
87.	1.2.643.3.251.5.18	id-eku-GF05-supervising-identcodes	Орган, уполномоченный на осуществление контроля в соответствии	Полномочия организации, осуществляющей контроль в соответствии с частью 5

			с частью 5 статьи 99 Федерального закона № 44-ФЗ. Базовый OID	статьи 99 Федерального закона № 44-ФЗ
88.	1.2.643.3.251.5.18.1	id-eku-GF05-supervising-identcodes-admin	Орган, уполномоченный на осуществление контроля в соответствии с частью 5 статьи 99 Федерального закона № 44-ФЗ. Администратор организации	
89.	1.2.643.3.251.5.18.2	id-eku-GF05-supervising-identcodes-authorized	Орган, уполномоченный на осуществление контроля в соответствии с частью 5 статьи 99 Федерального закона № 44-ФЗ. Уполномоченный специалист	
90.	1.2.643.3.251.5.19	id-eku-GF05-internalControl	Орган внутреннего контроля. Базовый OID	Полномочия организации «орган внутреннего контроля»
91.	1.2.643.3.251.5.19.1	id-eku-GF05-internalControl-admin	Орган внутреннего контроля. Администратор	

			организации	
92.	1.2.643.3.251.5.19.2	id-eku-GF05-internalControl-authorized	Орган внутреннего контроля. Уполномоченный специалист	
93.	1.2.643.3.251.5.20	id-eku-GF05-interacting	Оператор информационной системы, взаимодействующей с ЕИС. Базовый OID	Полномочие организации «Оператор информационной системы, взаимодействующей с ЕИС»
94.	1.2.643.3.251.5.20.1	id-eku-GF05-interacting-admin	Оператор информационной системы, взаимодействующей с ЕИС. Администратор организации	
95.	1.2.643.3.251.5.20.2	id-eku-GF05-interacting-authorized	Оператор информационной системы, взаимодействующей с ЕИС. Уполномоченный специалист	
96.	1.2.643.3.251.5.21	id-eku-GF05-library	Орган, уполномоченный на ведение библиотеки типовых контрактов, типовых условий	Полномочие организации «Орган, уполномоченный на ведение библиотеки типовых контрактов,

			контрактов. Базовый OID	типовых условий контрактов»
97.	1.2.643.3.251.5.21.1	id-eku-GF05-library-admin	Орган, уполномоченный на ведение библиотеки типовых контрактов, типовых условий контрактов. Администратор организации	
98.	1.2.643.3.251.5.21.2	id-eku-GF05-library-authorized	Орган, уполномоченный на ведение библиотеки типовых контрактов, типовых условий контрактов. Уполномоченный специалист	
99.	1.2.643.3.251.5.22	id-eku-GF05-monitoring	Орган, осуществляющий мониторинг закупок. Базовый OID	Полномочие организации «Орган, осуществляющий мониторинг закупок»
100.	1.2.643.3.251.5.22.1	id-eku-GF05-monitoring-admin	Орган, осуществляющий мониторинг закупок. Администратор организации	
101.	1.2.643.3.251.5.22.2	id-eku-GF05-monitoring-authorized	Орган, осуществляющий мониторинг закупок. Уполномоченный	

			специалист	
102.	1.2.643.3.251.5.23	id-eku-GF05-conformity	Организация, осуществляющая мониторинг соответствия в соответствии с Федеральным законом № 223-ФЗ. Базовый OID	Полномочие организации «Организация, осуществляющая мониторинг соответствия в соответствии с Федеральным законом № 223-ФЗ»
103.	1.2.643.3.251.5.23.1	id-eku-GF05-conformity-admin	Организация, осуществляющая мониторинг соответствия в соответствии с Федеральным законом № 223-ФЗ. Администратор организации	
104.	1.2.643.3.251.5.23.2	id-eku-GF05-conformity-authorized	Организация, осуществляющая мониторинг соответствия в соответствии с Федеральным законом № 223-ФЗ. Уполномоченный специалист	
105.	1.2.643.3.251.5.24	id-eku-GF05-assessment	Организация, осуществляющая оценку соответствия в	Полномочие организации «Организация, осуществляющая оценку

			соответствии с Федеральным законом № 223-ФЗ. Базовый OID	соответствия в соответствии с Федеральным законом № 223-ФЗ»
106.	1.2.643.3.251.5.24.1	id-eku-GF05-assessment-admin	Организация, осуществляющая оценку соответствия в соответствии с Федеральным законом № 223-ФЗ. Администратор организации	
107.	1.2.643.3.251.5.24.2	id-eku-GF05-assessment-authorized	Организация, осуществляющая оценку соответствия в соответствии с Федеральным законом № 223-ФЗ. Уполномоченный специалист	
108.	1.2.643.3.251.5.25	id-eku-GF05-customerNonPlacement	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в	Полномочие организации «Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения

			соответствии с положениями Федерального закона № 223–ФЗ. Базовый OID	о закупке в соответствии с положениями Федерального закона № 223–ФЗ»
109.	1.2.643.3.251.5.25.1	id-eku-GF05-customerNonPlacement-admin	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в соответствии с положениями Федерального закона № 223–ФЗ. Администратор организации	
110.	1.2.643.3.251.5.25.2	id-eku-GF05-customerNonPlacement-authorized	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в соответствии с положениями Федерального закона № 223–ФЗ.	

			Уполномоченный специалист	
111.	1.2.643.3.251.5.25.3	id-eku-GF05-customerNonPlacement-sign	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в соответствии с положениями Федерального закона № 223–ФЗ. Должностное лицо с правом подписи контракта	
112.	1.2.643.3.251.5.25.4	id-eku-GF05-customerNonPlacement-template	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в соответствии с положениями Федерального закона № 223–ФЗ. Специалист с правом	

			направления проекта контракта участнику закупки	
113.	1.2.643.3.251.5.25.5	id-eku-GF05-customerNonPlacement-submit	Заказчик, осуществляющий закупки в соответствии с Федеральным законом № 44–ФЗ, в связи с неразмещением положения о закупке в соответствии с положениями Федерального закона № 223–ФЗ. Специалист с правом согласования закупки	
114.	1.2.643.3.251.5.26	id-eku-GF05-customerAudit	Заказчик, осуществляющий закупку на проведение обязательного аудита. Базовый OID	Полномочие организации «Заказчик, осуществляющий закупку на проведение обязательного аудита»
115.	1.2.643.3.251.5.26.1	id-eku-GF05-customerAudit-admin	Заказчик, осуществляющий закупку на проведение обязательного аудита. Администратор организации	

116.	1.2.643.3.251.5.26.2	id-eku-GF05-customerAudit-authorized	Заказчик, осуществляющий закупку на проведение обязательного аудита. Уполномоченный специалист	
117.	1.2.643.3.251.5.26.3	id-eku-GF05-customerAudit-sign	Заказчик, осуществляющий закупку на проведение обязательного аудита. Должностное лицо с правом подписи контракта	
118.	1.2.643.3.251.5.26.4	id-eku-GF05-customerAudit-template	Заказчик, осуществляющий закупку на проведение обязательного аудита. Специалист с правом направления проекта контракта участнику закупки	
119.	1.2.643.3.251.5.26.5	id-eku-GF05-customerAudit-submit	Заказчик, осуществляющий закупку на проведение обязательного аудита. Специалист с правом согласования закупки	

120.	1.2.643.3.251.5.27	id-eku-GF06-customerInvestment	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Базовый OID	Полномочие организации «Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ»
121.	1.2.643.3.251.5.27.1	id-eku-GF06-customerInvestment-admin	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Администратор организации	
122.	1.2.643.3.251.5.27.2	id-eku-GF06-customerInvestment-authorized	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Уполномоченный специалист	
123.	1.2.643.3.251.5.27.3	id-eku-GF06-customerInvestment-sign	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Должностное	

			лицо с правом подписи контракта	
124.	1.2.643.3.251.5.27.4	id-eku-GF06-customerInvestment-template	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Специалист с правом направления проекта контракта участнику закупки	
125.	1.2.643.3.251.5.27.5	id-eku-GF06-customerInvestment- submit	Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Федерального закона № 44–ФЗ. Специалист с правом согласования закупки	
126.	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

127.	1.3.6.1.5.5.7.3.3	id-kp-codeSigning	ЭП программных компонентов	
128.	1.3.6.1.5.5.7.3.4	id-kp-emailProtection	Защита электронной почты	
129.	1.3.6.1.5.5.7.3.8	id-kp-timeStamping	Подпись меток доверенного времени	
130.	1.3.6.1.5.5.7.3.9	id-kp-OCSPSigning	Подпись ответов службы OCSP	
131.	1.2.643.3.251.7	id-eku-UNIFO	Работа с УНИФО. Базовый OID	
132.	1.2.643.3.251.7.1	id-eku-UNIFO-ftas	УНИФО. ЭП пользователя Федерального казначейства	
133.	1.2.643.3.251.7.2	id-eku-UNIFO-charges-administrator	УНИФО. ЭП пользователя Администратора начислений	
134.	1.2.643.3.251.7.3	id-eku-UNIFO-credit-institution	УНИФО. ЭП пользователя Кредитной организации	id-eku-UNIFO-credit-institution
135.	1.2.643.3.251.8	id-eku-GF09	Работа с ГМУ. Базовый OID	
136.	1.2.643.3.251.8.1	id-eku-GF09-admin	Работа с ГМУ. ЭП	

			администратора организации	
137.	1.2.643.3.251.8.2	id-eku-GF09-authorized	Работа с ГМУ. ЭП уполномоченного специалиста	
138.	1.2.643.100.2	id-eku-GF10	Работа с СМЭВ. Базовый OID	Для системы межведомственного электронного документооборота
139.	1.2.643.100.2.1	id-eku-GF10-authorized	СМЭВ. Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии	
140.	1.2.643.100.2.2	id-eku-GF10-legal-entity	СМЭВ. Для юридического лица для подписания электронных документов при межведомственном взаимодействии	
141.	1.3.6.1.4.1.5147.11.1.2	id-eku-GF11	Работа с биржами	Для ПО торгового терминала при проведении депозитного аукциона

142.	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
143.	1.2.643.6.22.255.1	id-eku-GF11-certificate	Сертификат	Сертификат выдан внешним аккредитованным УЦ (для ИС СПВБ)
144.	1.2.643.6.22.3	id-eku-GF11-system	Транспортные системы СПВБ	
145.	1.2.643.6.22.2.2.1	id-eku-GF12	СЭД СПВБ с Федеральным казначейством	
146.	1.3.6.1.4.1.311.20.2.2	id-eku-GF13	Вход в систему с помощью смарт-карты	
147.	1.2.643.3.251.9	id-eku-certrequest	Подпись запросов на издание сертификатов ключей проверки электронной подписи	Полномочие пользователя для подписания запросов на издание сертификатов ключей проверки электронной подписи
148.	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

149.	1.2.643.3.251.10.13	id-eku-use-restriction	Ограничения на использование квалифицированного сертификата (если имеется)	Используется при наличии ограничений

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 Таб. 7.2.

Таб. 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, СПТО
3.	1.2.643.3.61.5027 10.1.5	id-on-OrganizationId	учетный номер организации	DirectoryString	ЕИС
4.	1.2.840.113549.1.9.20	pkcs9_at_friendlyName	учетная запись пользователя АСФК	DirectoryString	АСФК
5.	1.2.643.3.61.5027 10.1.8	id-on-InstitutionId	учетный номер организации	DirectoryString	ГМУ

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 Таб. 7.2.

Таб. 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, СПТО
3.	1.2.643.3.61.5027 10.1.5	id-on-OrganizationId	учетный номер организации	DirectoryString	ЕИС
4.	1.2.840.113549.1.9.20	pkcs9_at_friendlyName	учетная запись пользователя АСФК	DirectoryString	АСФК
5.	1.2.643.3.61.5027 10.1.8	id-on-InstitutionId	учетный номер организации	DirectoryString	ГМУ