ПРИЛОЖЕНИЕ №11. ФОРМАТ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Обозначение	**Название**	**Длина поля**	**Примечание**
Version	Версия	-	Должна быть не ниже 3
serial number	Серийный номер	-	Уникальный номер квалифицированного сертификата
Signature	Алгоритм подписи	-	В поле algorithm должен содержаться идентификатор алгоритма подписи ГОСТ Р 34.11-94/34.10-2001 (OID.1.2.643.2.2.3, в соответствии с RFC4491)
Имя издателя СКП ЭП (issuer). Данный атрибут включает следующее поля:			
1. CN	Общее имя	64	OID 2.5.4.3 Псевдоним удостоверяющего центра
2. C	Страна	2	OID 2.5.4.6 Двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997)
3. S	Регион	128	OID 2.5.4.8 Наименование субъекта РФ местонахождения ПАК РУЦ АО
4. L	Населенный пункт	128	OID 2.5.4.7 Наименование населенного пункта местонахождения ПАК РУЦ АО
5. O	Организация	64	OID 2.5.4.10 Полное или сокращенное наименование организации
6. OU	Подразделение	64	OID 2.5.4.11 В случае выпуска СКП ЭП на должностное лицо – соответствующее подразделение организации
7. OGRN	ОГРН	13	OID 1.2.643.100.1 ОГРН организации
8. INN	ИНН	12	OID 1.2.643.3.131.1.1 ИНН организации
notBefore	Дата и время начала действия СКПЭП	-	-
notAfter	Дата и время окончания действия СКПЭП	-	-
Имя владельца СКЭП (subject). Данный атрибут включает следующее поля:			
1. CN	Общее имя	64	OID 2.5.4.3 **ЮЛ:** В зависимости от типа

Обозначение	Название	Длина поля	Примечание
			конечного владельца СКПЭП: - наименование организации; - ФИО должностного лица; - название автоматизированной системы; - другое отображаемое имя по требованиям информационной системы. **ФЛ:** ФИО
2. C	Страна	2	OID 2.5.4.6 Двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997)
3. surname	Фамилия	128	OID 2.5.4.4 В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую фамилию физического лица.
4. givenName	Приобретенное имя	128	OID 2.5.4.42 В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя и отчество (если имеется) физического лица
5. S	Регион	128	OID 2.5.4.8 Наименование субъекта РФ: **ЮЛ:** По адресу местонахождения **ФЛ:** По адресу регистрации
6. L	Населенный пункт	128	OID 2.5.4.7 Наименование населенного пункта: **ЮЛ:** По адресу местонахождения **ФЛ:** По адресу регистрации
7. streetAddress	Название улицы, номер дома	128	OID 2.5.4.9 В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую часть адреса места нахождения соответствующего лица, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется).
8. O	Организация	64	OID 2.5.4.10 Полное или сокращенное наименование организации (только для ЮЛ)
9. OU	Подразделение	64	OID 2.5.4.11

Обозначение	Название	Длина поля	Примечание
			ЮЛ: В случае выпуска СКПЭП на должностное лицо – соответствующее подразделение организации (если имеется)
10. T	Должность	64	OID 2.5.4.12 **ЮЛ:** В случае выпуска СКПЭП на должностное лицо – его должность
11. OGRN	ОГРН	13	OID 1.2.643.100.1 ОГРН организации (только для ЮЛ)
12. SNILS	СНИЛС	11	OID 1.2.643.100.3 **ФЛ:** СНИЛС **ЮЛ:** Не обязательно, но в случае выпуска СКПЭП на должностное лицо – данное поле рекомендуется включать для упрощения идентификации должностных лиц.
13. INN	ИНН	12	OID 1.2.643.3.131.1.1 **ЮЛ/ИП:** ИНН **ФЛ:** Не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС.
14. E	E-mail	128	OID 1.2.840.1135.49.1.9.1 **ЮЛ/ИП/ФЛ** Адрес электронной почты.
subjectPublicKeyInfo	Открытый ключ	-	-
Дополнения (расширения) сертификата (Extensions)			
1. Authority Key Identifier	Идентификатор ключа РУЦ АО	-	OID.2.5.29.35
2. Key Usage	Область использования ключа	-	OID.2.5.29.15
3. Certificate Policies	Политики сертификата	-	OID.2.5.29.32 Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующие идентификаторы: для класса средств ЭП КС2: 1.2.643.100.113.1, 1.2.643.100.113.2 Помимо идентификаторов политик, описывающих класс ЭП владельца квалифицированного сертификата, в дополнении

Обозначение	Название	Длина поля	Примечание
			«Политики сертификата» могут содержаться другие описатели политик.
4. Subject Sign Tool	Средство ЭП владельца сертификата	-	OID.1.2.643.100.111 наименование используемого средства ЭП и (или) стандарты, требованиям которых соответствует ключ ЭП и ключ проверки ЭП
5. Issuer Sign Tool	средство ЭП РУЦ АО	-	OID.1.2.643.100.112 наименования средств ЭП и средств аккредитованного РУЦ АО, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом
6. ExtendedKeyUsage расширенное использования ключа. Состав дополнения зависит от информационной системы, в которой используется СКПЭП OID.2.5.29.37, может содержать следующие поля:			
6.1. Доступ к СМЭВ	ЭП-СП	-	OID 1.2.643.100.2.1 Доступ к СМЭВ (ЭП-СП)
	ЭП-ОВ	-	1.2.643.100.2.2 Доступ к СМЭВ (ЭП-ОВ)
6.2.При необходимости запросов из ЕГРП	Руководитель ОГВ субъекта РФ или иное уполномоченное лицо данного органа в соответствии с ФЗ	-	OID 1.2.643.5.1.24.2.6
	Руководитель ОМСУ или иное уполномоченное лицо данного органа в соответствии с ФЗ	-	OID 1.2.643.5.1.24.2.19
7. CDP	Точки распространения списков отзыва	-	OID.2.5.29.31