

Приложение № 13

Формат сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 либо ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома). 8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) OGRN (ОГРН). 12) INN (ИНН).
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	1) commonName (общее имя). 2) surname (фамилия). 3) givenName (приобретенное имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома). 8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) E = электронная почта 12) UnstructuredName (UN) 13) OGRN (ОГРН). 14) SNILS (СНИЛС). 15) INN (ИНН).
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 либо ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 либо ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Могут быть внесены дополнительные области использования
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП
IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280