

## Структура сертификата ключа проверки электронной подписи Субъекта информационного обмена Удостоверяющего центра АО «Россельхозбанк»

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Hash Signature Algorithm	Алгоритм хэширования подписи	ГОСТ Р 34.11-2012 256 бит
Issuer	Издатель сертификата	CN = Russian Agricultural Bank CA GOST 2012 O = Russian Agricultural Bank C = RU
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм Мск Действителен по: дд.мм.гггг чч:мм Мск
Subject	Владелец сертификата	CN = Общее имя = Фамилия, Имя, Отчество OU = Подразделение = наименование подразделения O = Организация = наименование организации L = Город S = Область C = Страна/Регион = RU E = Адрес E-Mail Компоненты имени CN, O, C, ... обязательны для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата.
Public Key	Ключ проверки электронной подписи	Ключ проверки электронной подписи ГОСТ Р 34.10-2012 256 бит
Расширения сертификата		
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре АО «Россельхозбанк»
Certificate template information	Сведения о шаблоне	Сведения о примененном шаблоне сертификата
Authority Information Access	Доступ к сведениям центра сертификации	Доступ к сертификату Уполномоченного лица АО «Россельхозбанк»
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL)	Набор адресов точек распространения CRL
Authority Key Identifier	Идентификатор ключа центра сертификатов	Идентификатор ключа электронной подписи Уполномоченного лица АО «Россельхозбанк», на котором подписан данный сертификат
Subject Key Identifier	Идентификатор ключа субъекта	Идентификатор ключа электронной подписи владельца сертификата
Key Usage (critical)	Использование ключа	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей
Stamp Algorithm	Алгоритм отпечатка	sha1
Stamp	Отпечаток	Уникальное значение