
# Кросс-сертификация VS подчинённый УЦ

**Смирнов Павел**
**Зам. начальника отдела разработок, к.т.н.**
**ООО «КРИПТО-ПРО»**

# 63-ФЗ, ст.15, ч.2.1

«Аккредитованный удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган»

# Интерпретация «честного налогоплательщика»

Как можно использовать ЭП (информация в электронной форме…) для подписания сертификатов?

Что такое «ЭП, основанная на сертификате»?

# Интерпретация чиновника

Присылаемый запрос на сертификат д.б. запросом на сертификат «подчинённого УЦ», а не запросом на кросс-сертификат.

# Матчасть

X.509:

Кросс-сертификат – это сертификат, издателем и субъектом которого являются разные УЦ.

Сертификат подчинённого УЦ – … нет такого …

Т.е. «сертификат подчинённого УЦ» – один из видов кросс-сертификатов.

# Чиновник работает «тупо». Попытка №1.

Отправляем как раньше:

- Запрос на сертификат
- Самоподписанный сертификат УЦ

Ответ:

- Надо запрос на сертификат «подчинённого УЦ»

# Чиновник работает «тупо». Попытка №2.

Отправляем без самоподписанного сертификата:

- Запрос на сертификат

Ответ:

- Ваш запрос имеет расширение файла .req, а КриптоПро УЦ такое расширение даёт запросам на кросс-сертификат
- Надо запрос на сертификат «подчинённого УЦ»

# Чиновник работает «тупо». Попытка №3.

Отправляем файл с другим расширением:

- Тот же запрос с расширением .p10

Ответ:

- Ваш запрос не содержит атрибута «версия ОС», а КриптоПро УЦ при создании запроса «подчинённого УЦ» такой атрибут добавляет
- Надо запрос на сертификат «подчинённого УЦ»

Занавес…

# Доколе?

- На каком основании отказ?
- Всем 405 УЦ поднимать второй ПАК для «строгой иерархии»?
- Как проконтролировать отсутствие самоподписанного сертификата?