РТЛабс

«Обзор сомнительных практик удостоверяющих центров»

Терзи А.М.

Зачем мы это делаем?

- Оценка динамики, объемов выпускаемых и отзываемых сертификатов АУЦ при проектировании или доработке новых сервисов ИС ГУЦ
- Разбор обращений граждан и организаций при проблемах с проверкой сертификатов и подписи в ИЭП

Как производился анализ

- Сбор всех актуальных СОС от АУЦ, опубликованных на портале e-trust.gosuslugi.ru
- Анализ опубликованных crl
- Сравнение crl из ретроспективы ИС ГУЦ
- Анализ crl с точки зрения RFC
- Анализ регламентов АУЦ

1. Приостановка сертификата и возобновление его действия через удаление записи из CRL

Что делают АУЦ:

предусматривают возможность приостановки сертификата на уровне регламента с кодом причины отзыва (6 –действие сертификата приостановлено) соответственно

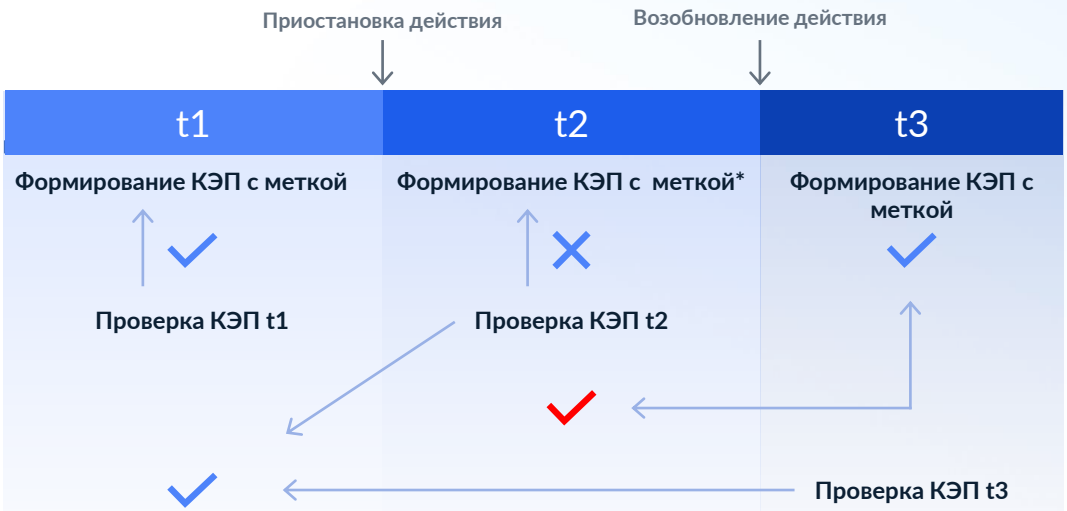
Проблема:

невозможность определения действительности сертификата на определенную дату

10 АУЦ предусматривающие приостановку,

~8000 приостановлено

1. Приостановка сертификата и возобновление его действия через удаление записи из CRL



2. Практика исключения из CRL записей о сертификатах, чей срок действия истек

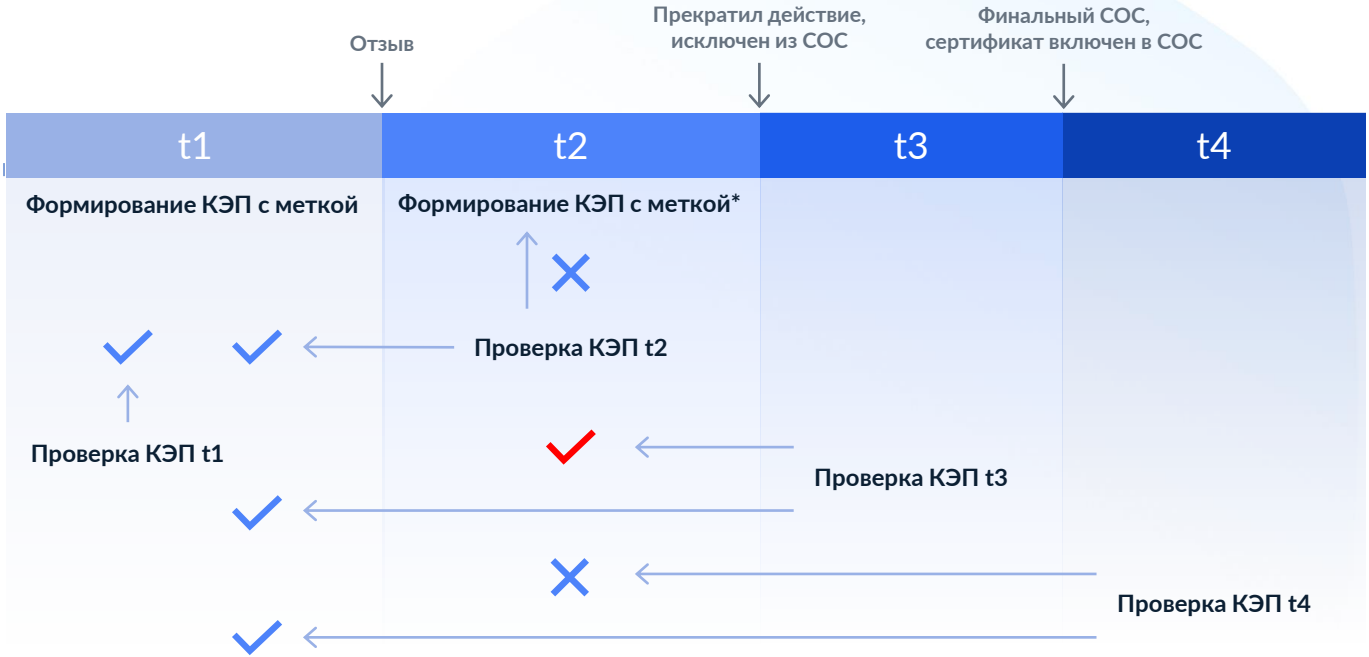
Что делают АУЦ:

исключают из crl отозванные сертификаты когда наступает срок окончания действия таких сертификатов

Проблема:

невозможность определения действительности сертификата на определенную дату, некорректность проверки в случае, если сертификат был отозван, а ЭП содержит метку времени

2. Практика исключения из CRL записей о сертификатах, чей срок действия истек



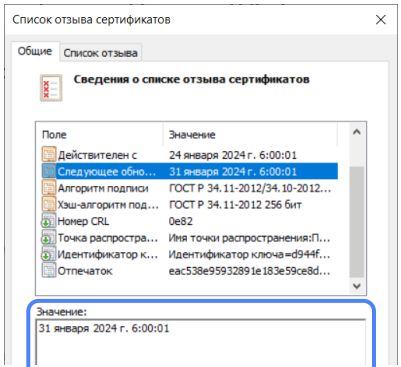
3. Практика «отложенного» отзыва сертификата с датой в будущем

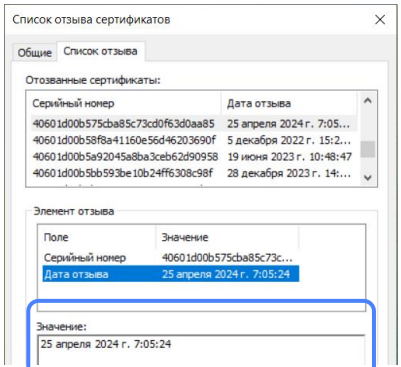
Что делают АУЦ:

при отзыве и добавлении сертификата в CRL устанавливается дата в будущем

Проблема:

при проверке сертификатов необходимо учитывать дату включения в CRL. Присутствие указанной функции в сертифицированных средствах УЦ. Не предусмотрено RFC





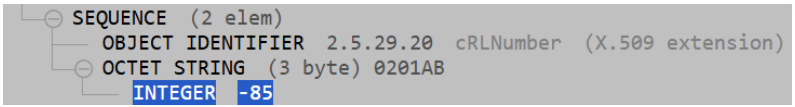
4. Некорректное формирование поля crlNumber некоторых средств УЦ АУЦ

Что делают АУЦ:

формируют некорректное значения поля crlNumber

Проблема:

в некоторых случаях может потенциально приводить к проблеме с проверкой ЭП



RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

CRLNumber ::= INTEGER (0..MAX)

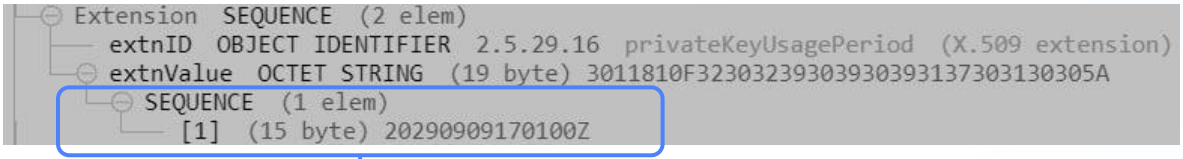
5. Некорректное формирование расширения Private key usage period

Что делают АУЦ:

не указывается только одно из обязательных полей PKUP с датой действия ключа подписи

Проблема:

не соответствие требованиям приказа ФСБ России 795



Содержится только поле со сроком окончания ключа

```
2.5.29.16: Флаги = 0, Длина = 13
Период использования закрытого ключа
    Действителен с момента начала действия сертификата
    Действителен по 9 сентября 2029 г. 20:01:00
```

Ваши вопросы и уточнения