

«Обзор сомнительных практик удостоверяющих центров»

Терзи А.М.

Зачем мы это делаем?

- Оценка динамики, объемов выпускаемых и отзывааемых 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:

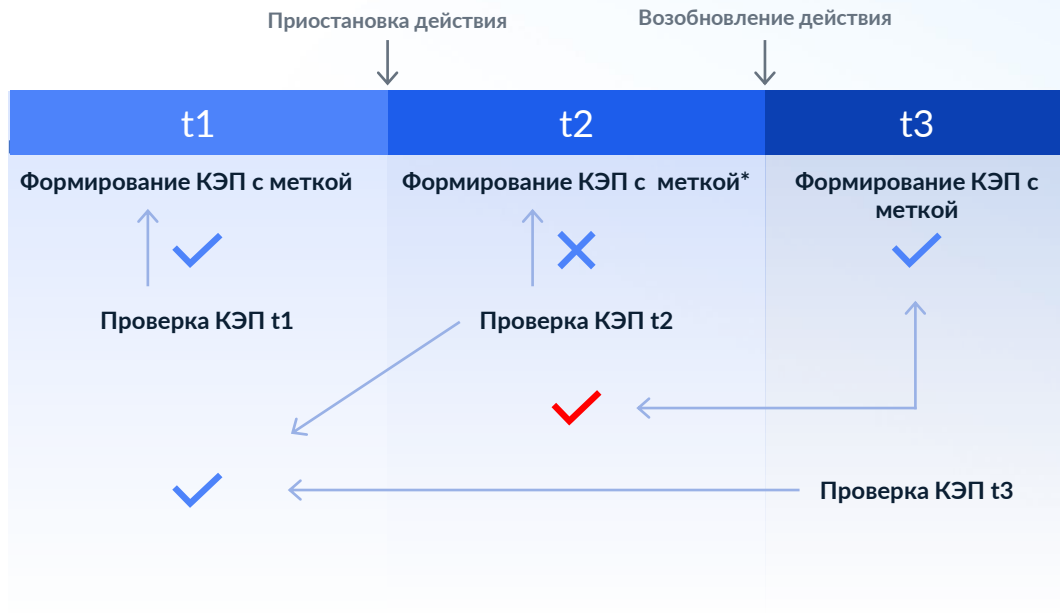
предусматривают возможность приостановки сертификата на уровне регламента с кодом причины отзыва (6 – действие сертификата приостановлено) соответственно

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

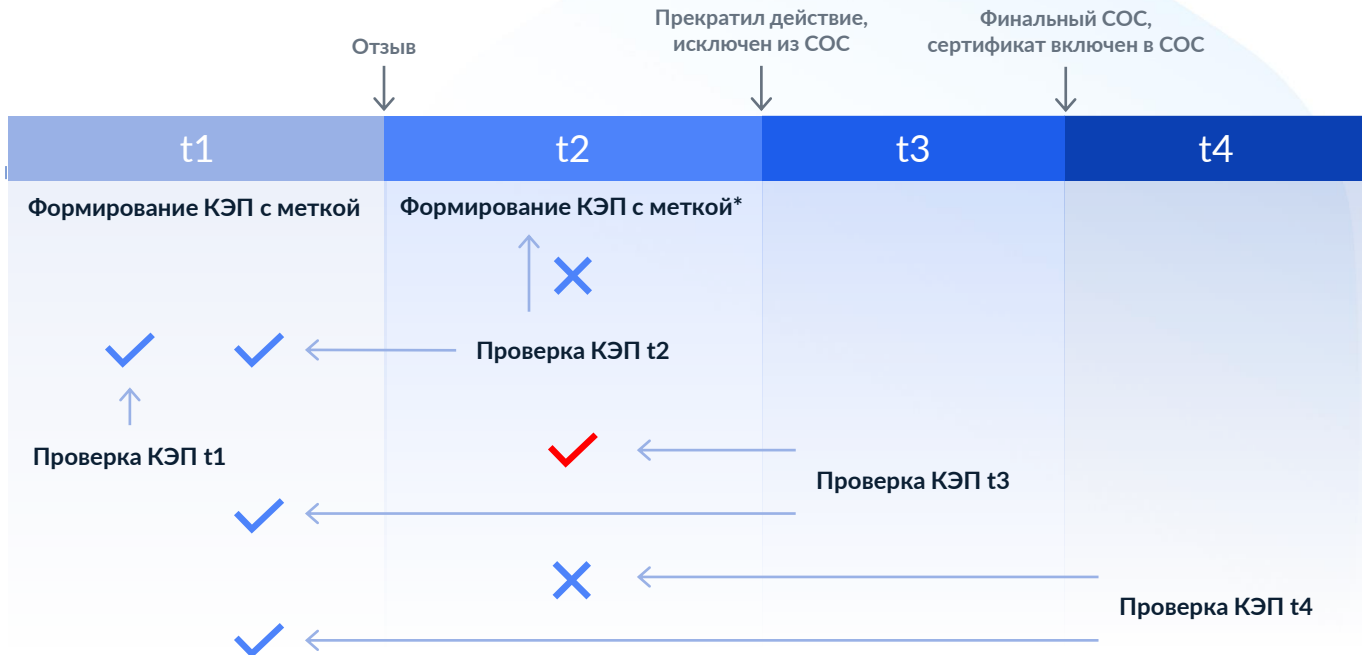
Что делают АУЦ:

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

Сведения о списке отзыва сертификатов

Поле	Значение
Действителен с	24 января 2024 г. 6:00:01
Следующее обновление	31 января 2024 г. 6:00:01
Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012...
Хэш-алгоритм под...	ГОСТ Р 34.11-2012 256 бит
Номер CRL	0e82
Точка распростра...	Имя точки распространения:П...
Идентификатор к...	Идентификатор ключа=d944f...
Отпечаток	ea538e95932891e183e59ce8d...

Значение:
31 января 2024 г. 6:00:01

Срок следующего обновления crl

Отозванные сертификаты:

Серийный номер	Дата отзыва
40601d00b575cba85c73cd0f63d0aa85	25 апреля 2024 г. 7:05:24
40601d00b58f8a+1160e56d46203690f	5 декабря 2022 г. 15:2...
40601d00b5a92045a8ba3ceb62d90958	19 июня 2023 г. 10:48:47
40601d00b5bb593be10b24ff6308c98f	28 декабря 2023 г. 14:...

Элемент отзыва

Поле	Значение
Серийный номер	40601d00b575cba85c73c...
Дата отзыва	25 апреля 2024 г. 7:05:24

Значение:
25 апреля 2024 г. 7:05:24

Дата отзыва из этого же crl

4. Некорректное формирование поля cRLNumber некоторых средств УЦ АУЦ

Что делают АУЦ:

формируют некорректные значения поля cRLNumber

Проблема:

в некоторых случаях может потенциально приводить к проблеме с проверкой ЭП

```
SEQUENCE (2 elem)
├── OBJECT IDENTIFIER 2.5.29.20 cRLNumber (X.509 extension)
└── OCTET STRING (3 byte) 0201AB
    └── INTEGER -85
```

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

```
Extension SEQUENCE (2 elem)
├── extnID OBJECT IDENTIFIER 2.5.29.16 privateKeyUsagePeriod (X.509 extension)
└── extnValue OCTET STRING (19 byte) 3011810F32303239303930393137303130305A
    └── SEQUENCE (1 elem)
        └── [1] (15 byte) 20290909170100Z
```

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**

