НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Обработка кросс-сертификатов и СОС аккредитованных УЦ

заместитель ген. директора по развитию

Сазонов Александр Валентинович

16 сентября 2015

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Когда и зачем это нужно?

ведомственные ИС

проверка КЭП документов, полученных через СМЭВ или от граждан

корпоративные ИС

проверка КЭП документов, полученных от внешних контрагентов

сервисы ДТС

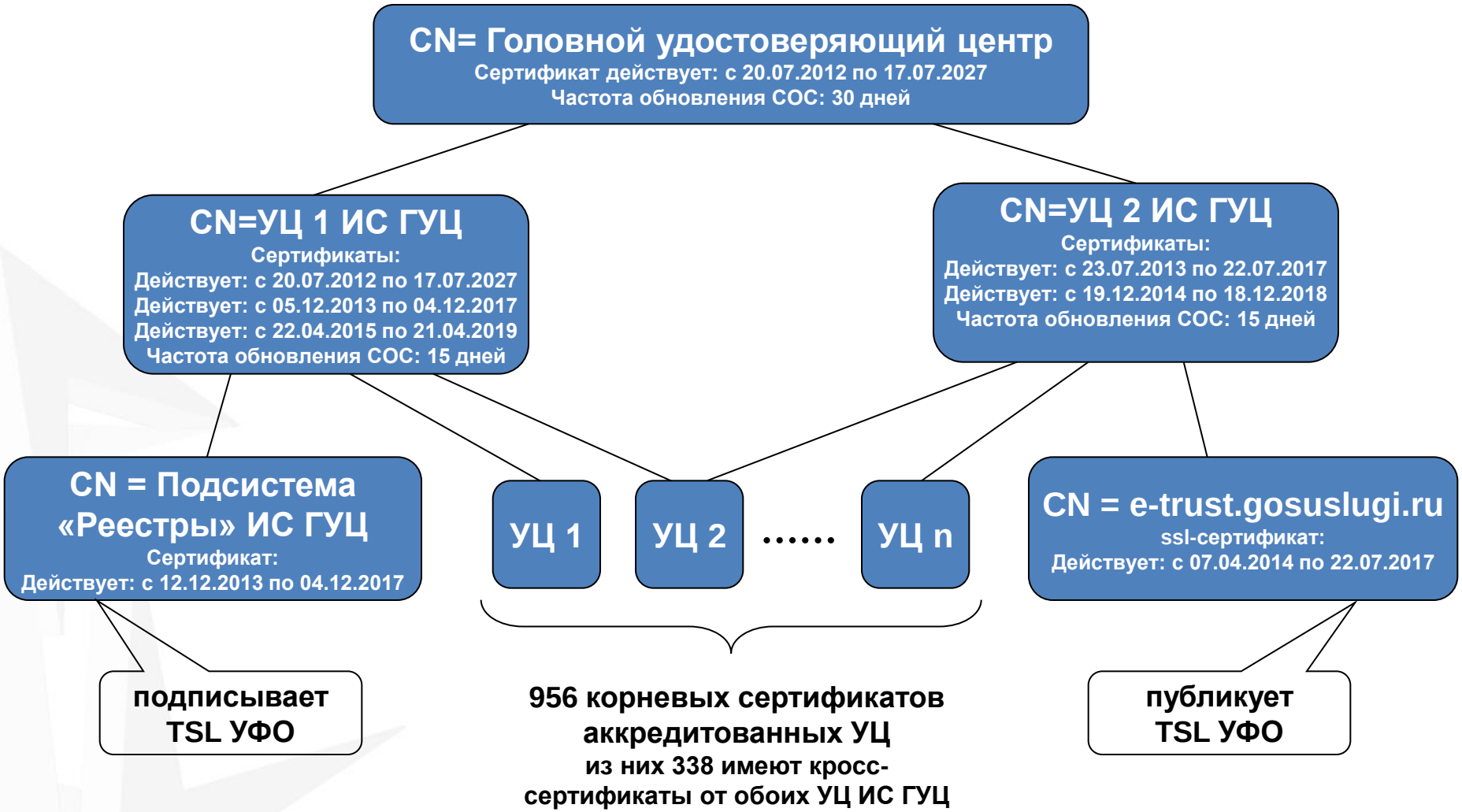
проверка и заверение КЭП документов по запросам

сервисы разбора конфликтных ситуаций

проверка КЭП документов на прошедший момент времени

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Архитектура УЦ УФО



НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Условия признания квалифицированной подписи

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"				Порядок проверки
Статья 11. Признание квалифицированной электронной подписи	**1)** квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, **аккредитация которого действительна <u>на день выдачи</u> указанного сертификата**;	Статья 14. Сертификат ключа проверки электронной подписи	6. **Сертификат** ключа проверки электронной подписи **прекращает свое действие**: ... 3) **в случае прекращения деятельности удостоверяющего центра** без перехода его функций другим лицам; ...	1. Обновить **TSL УФО**. 2. Проверить ЭП **Подсистемы «Реестры» ИС ГУЦ** на **TSL УФО**: 1. Осуществить математическую проверку ЭП **Подсистемы «Реестры» ИС ГУЦ**. 2. Проверить срок действия сертификата **Подсистемы «Реестры» ИС ГУЦ** на день проверки. 3. Проверить статус сертификата **Подсистемы «Реестры» ИС ГУЦ** по СОС **УЦ 1 ИС ГУЦ** на день проверки. 4. Проверить срок действия сертификата **УЦ 1 ИС ГУЦ** на день проверки. 5. Проверить статус сертификата **УЦ 1 ИС ГУЦ** по СОС **Головного удостоверяющего центра** на день проверки. 3. Проверить наличие кросс-сертификата **аккредитованного УЦ** в **TSL УФО**. 4. Проверить срок действия кросс-сертификата **аккредитованного УЦ** на день проверки. 5. Проверить статус кросс-сертификата **аккредитованного УЦ** по СОС **УЦ 1 ИС ГУЦ** (или **УЦ 2 ИС ГУЦ)** на день проверки. 6. Проверить срок действия сертификата **УЦ 1 ИС ГУЦ** (или **УЦ 2 ИС ГУЦ)** на день проверки. 7. Проверить статус сертификата **УЦ 1 ИС ГУЦ** (или **УЦ 2 ИС ГУЦ)** по СОС **Головного удостоверяющего центра** на день проверки.

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Условия признания квалифицированной подписи

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"				Порядок проверки
Статья 11. Признание квалифицированной электронной подписи	**2)** квалифицированный сертификат действителен **на момент подписания** электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или **на день проверки** действительности указанного сертификата, если момент подписания электронного документа не определен;	Статья 14. Сертификат ключа проверки электронной подписи	6. **Сертификат** ключа проверки электронной подписи **прекращает свое действие**: 1) в связи с **истечением установленного срока его действия**; ... 7. Информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов **в течение одного рабочего дня** со дня наступления обстоятельств, повлекших за собой прекращение действия сертификата ключа проверки электронной подписи. Действие сертификата ключа проверки электронной подписи прекращается **с момента внесения записи об этом в реестр сертификатов**.	8. Проверить срок действия сертификата **подписанта** на день проверки. 9. Проверить статус сертификата **подписанта** по СОС **аккредитованного УЦ** на день проверки. 10. Воспользоваться результатами проверки п.п. 4.-7.

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Условия признания квалифицированной подписи

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"				Порядок проверки
Статья 11. Признание квалифицированной электронной подписи	**3)** имеется положительный результат проверки **принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи**, с помощью которой подписан электронный документ, и подтверждено **отсутствие изменений**, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;			11. Осуществить математическую проверку ЭП **подписанта**.

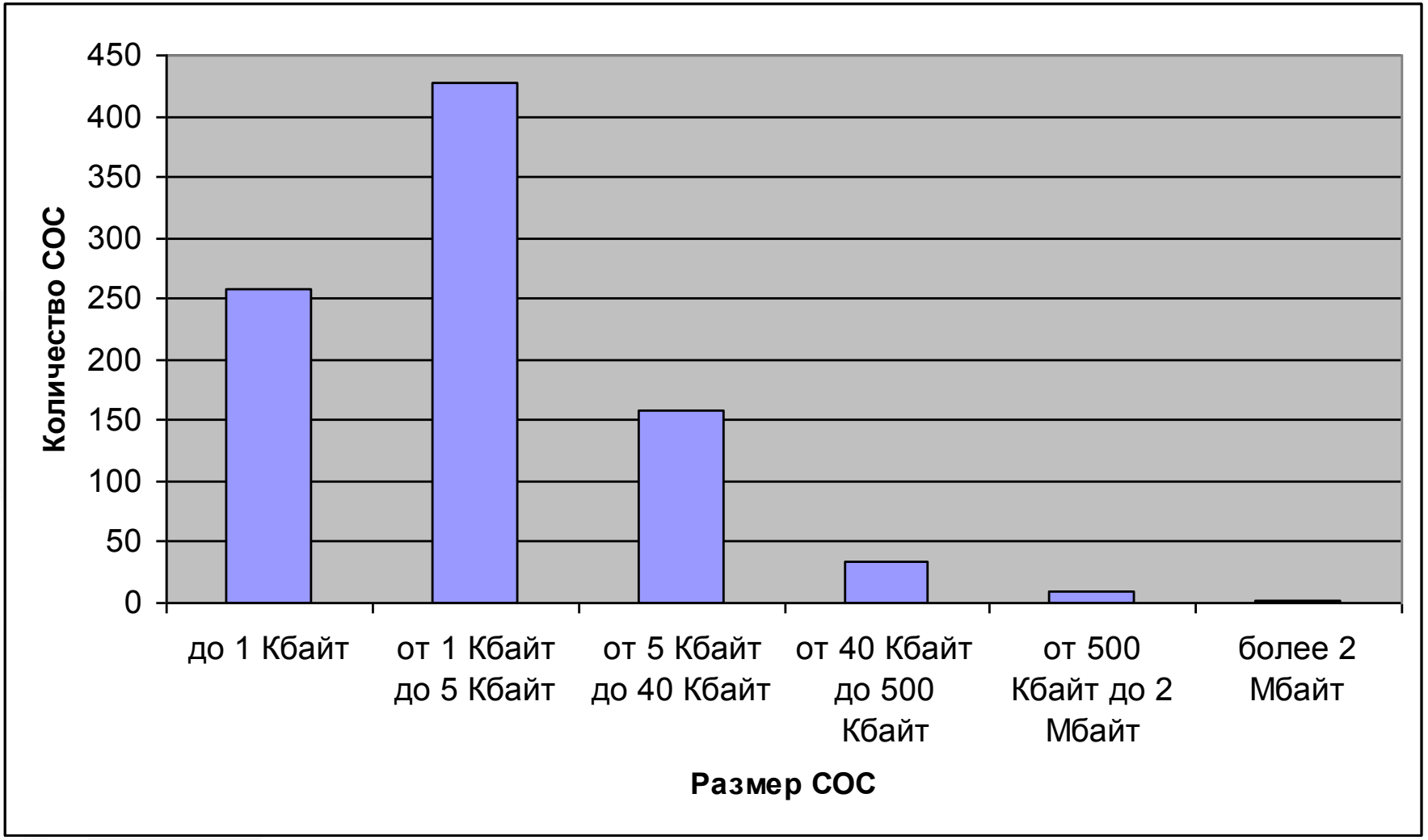
НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Условия признания квалифицированной подписи

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"				Порядок проверки
Статья 11. Признание квалифицированной электронной подписи	**4)** квалифицированная электронная подпись используется **с учетом ограничений, содержащихся в квалифицированном сертификате** лица, подписывающего электронный документ (если такие ограничения установлены).			12. По объектным идентификаторам (OID), указанным в сертификате **подписанта** восстановить **политики применения сертификатов**, в соответствии с которыми данный сертификат выпущен. Проверить ограничения на использование ЭП, указанные в данных политиках применения сертификатов.

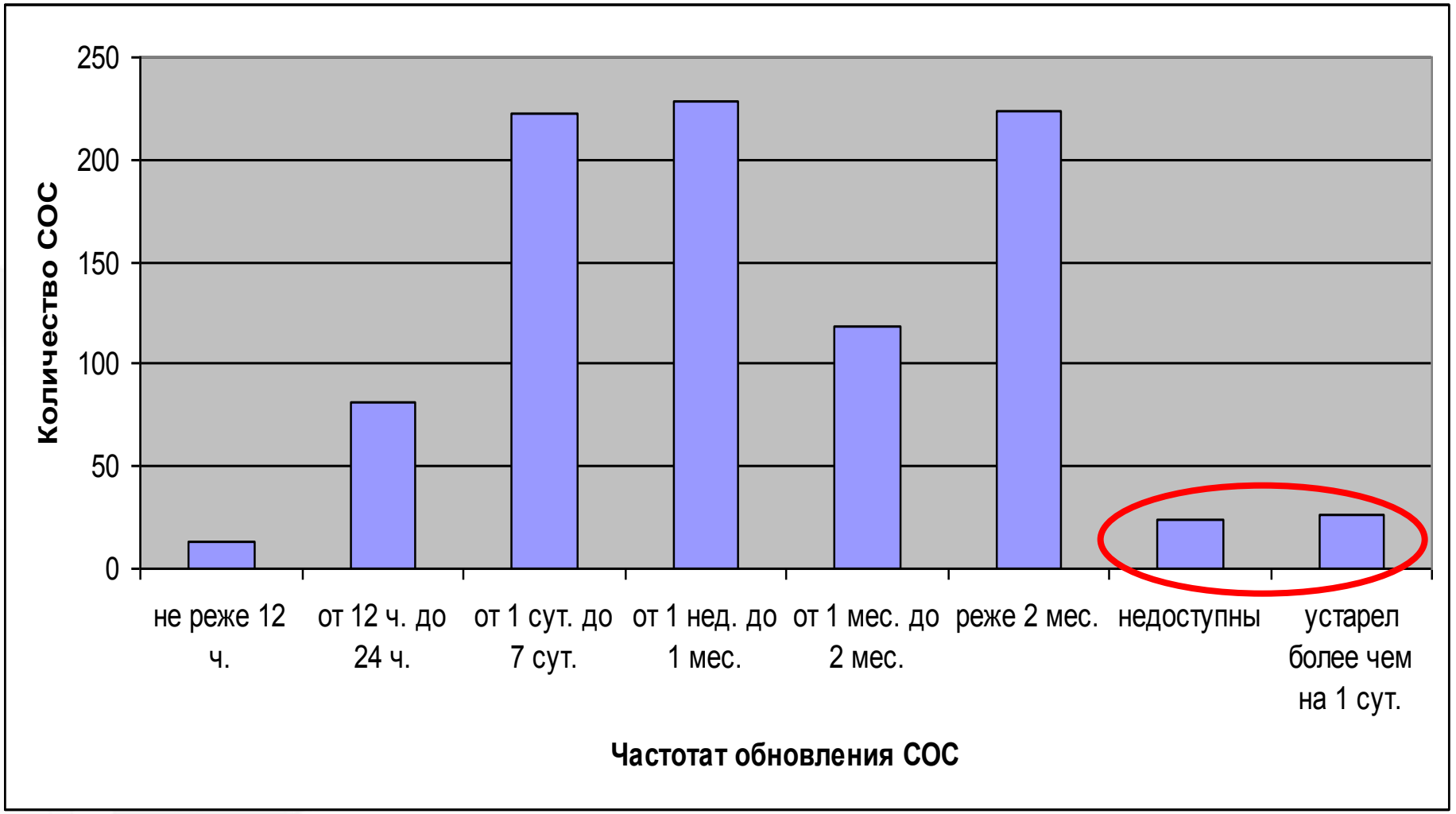
НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Размер СОС аккредитованных УЦ



НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Частота обновления СОС аккредитованных УЦ



НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Как часто нужно проверять обновление СОС?

Лучший вариант – проверять обновление СОС каждый раз при проверке ЭП.

В других случаях следует руководствоваться:

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"	**RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
Статья 11. Признание квалифицированной электронной подписи … 2) квалифицированный сертификат действителен **на момент подписания** электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или **на день проверки** действительности указанного сертификата, если момент подписания электронного документа не определен; …	**6.3. CRL Validation** This section describes the steps necessary to determine if a certificate is revoked when CRLs are the revocation mechanism used by the certificate issuer. Conforming implementations that support CRLs are not required to implement this algorithm, but they MUST be functionally equivalent to the external behavior resulting from this procedure when processing CRLs that are issued in conformance with this profile. Any algorithm may be used by a particular implementation so long as it derives the correct result. This algorithm assumes that all of the needed CRLs are available in a local cache. Further, **if the next update time of a CRL has passed, the algorithm assumes a mechanism to fetch a current CRL and place it in the local CRL cache**.

→ **следует обновлять СОС при достижении момента Next Update, но не реже 1 раза в сутки**

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Обработка TSL УФО

Модуль Актуализации Кросс-сертификатов и СОС

- **загружает TSL УФО** и проверяет ЭП на TSL УФО по цепочке до Головного удостоверяющего центра
- **загружает новые кросс-сертификаты** аккредитованных УЦ
- **проверяет срок действия локально установленных СОС** аккредитованных УЦ и **загружает новые СОС** при необходимости
- **загружает по расписанию СОС** с большим сроком действия
- **архивирует** все кросс-сертификаты и СОС аккредитованных УЦ
- **осуществляет выгрузку** кросс-сертификатов аккредитованных УЦ, сертификатов УЦ ИС ГУЦ и соответствующих СОС, актуальных **на запрашиваемый момент времени**

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Спасибо за внимание!

Сазонов Александр Валентинович

заместитель ген. директора по развитию

ЗАО «Национальный удостоверяющий центр»

www.nucrf.ru

sazonov@nucrf.ru