

Безопасный интернет в современных реалиях

Национальный удостоверяющий центр
сертификаты безопасности
обеспечение доверия

Пьянченко А.А.
заместитель директора ФГАУ НИИ «Восход»



Многие российские организации в этом году столкнулись с отзывом либо отказом в продлении TLS-сертификатов на российские домены

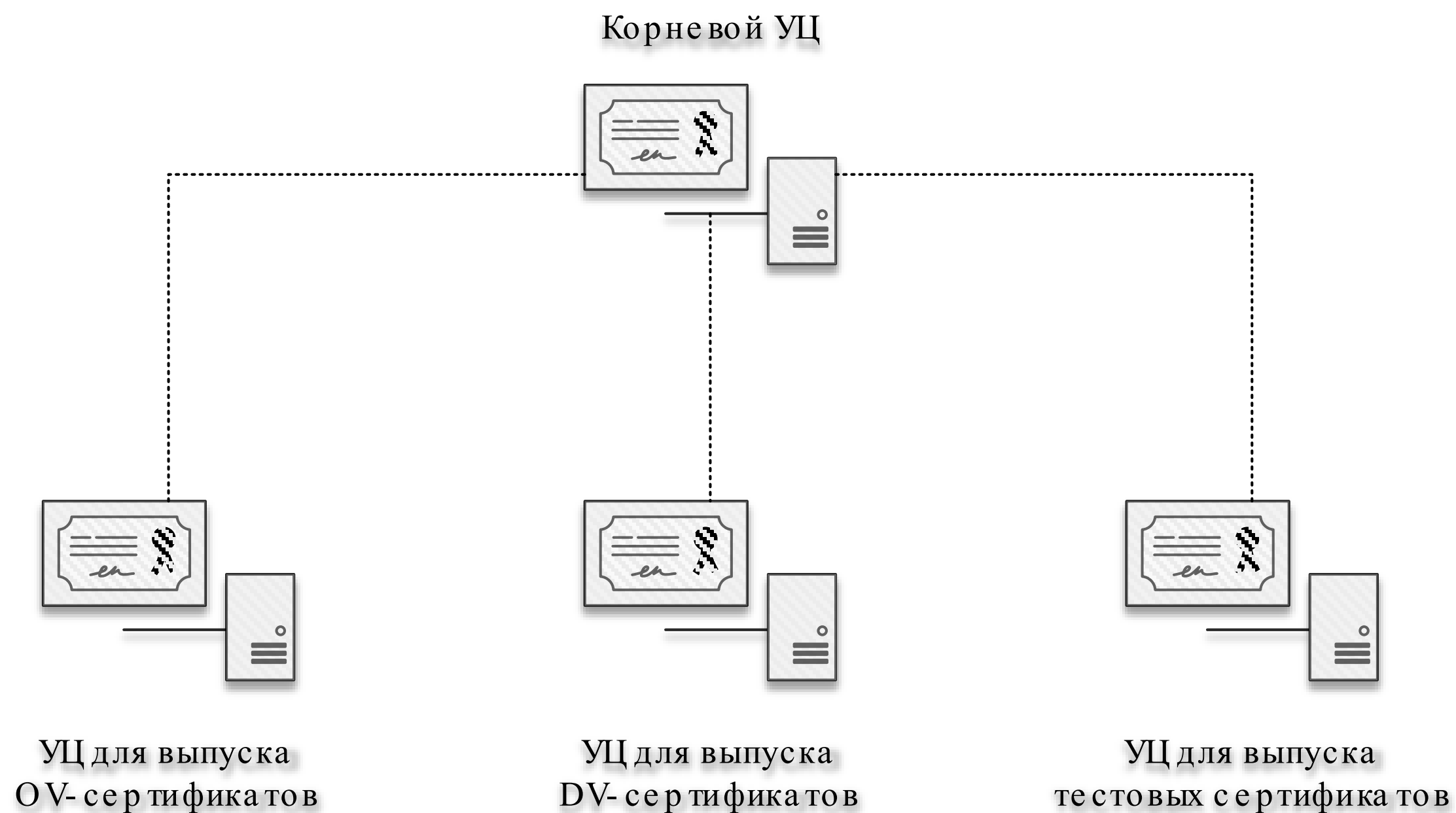
Как быстро и эффективно ответить на санкционную политику зарубежных УЦ?

В целевой модели конечно переходом на массовое использование протокола TLS с поддержкой алгоритмов шифрования ГОСТ.

А до тех пор – обеспечить выдачу TLS-сертификатов на зарубежных алгоритмах и сделать процесс их применения прозрачным и безопасным.



На чем выпускаются сертификаты?



Сервера на базе процессоров отечественного производства (Эльбрус)



Сертифицированная ФСТЭК России операционная система (сертификат №3866 от 10.08.2018)




Основан на решении, корректность реализации функций которого подтверждена ФСБ России (выписка из заключения № 149/3/2/2/-326 от 14.02.2020)


Какие есть типы сертификатов?


1

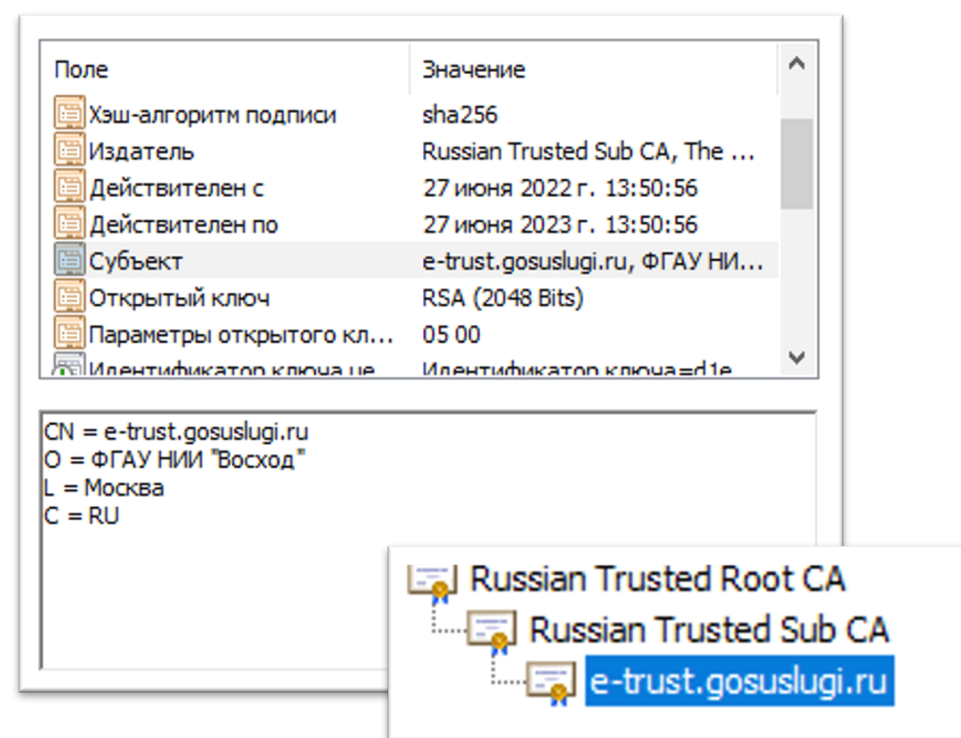
OV-сертификаты

Проверка владения доменом и проверка организации

 до 99 доменных имен

 юридические лица


 12 месяцев



2

DV-сертификаты

Проверка владения доменом

 1 доменное имя

 юридические лица, ИП и физические лица

 3 месяца



А зачем Certificate Transparency?

Что насчет MITM? Откуда мне знать, что на мой домен не выпустят сертификат без моего ведома?

Для этого мы применяем технологию Certificate Transparency

1

Независимость – журналы СТ ведутся независимо разными организациями

2

Публичность – журналы СТ доступны для мониторинга и аудита

3

Обязательность – УЦ не может выпустить сертификат без записи в журналы СТ

4

Контроль – российские браузеры проверяют запись сертификата в журналы СТ

Как работает эта технология?

1

Запрос

Владелец домена формирует запрос на выпуск сертификата и направляет его через портал госуслуг

2

Обработка

НУЦ обрабатывает поступивший запрос, формирует пресертификат и направляет его в журналы СТ

3

Запись

Информация о сертификате вносится в журналы СТ

4

SCT-метки

Журналы СТ отправляют обратно в НУЦ SCT-метки (Signed Certificate Timestamp)

5

Выпуск

НУЦ выпускает сертификат, в котором записаны SCT-метки от всех журналов СТ

6

Установка

Владелец домена устанавливает полученный сертификат

7

Проверка

Браузеры при обращении к сайту с установленным сертификатом проверяют наличие этого сертификата в журналах СТ



Подробнее о технологии Certificate Transparency можно почитать в RFC 6962

И где это посмотреть?

https://23.ctlog.digital.gov.ru/

```
{"tree_size":1345,"timestamp":1662711903781,"sha256_root_hash":"Iu3qaIMCr+atwAQ9sHyWiTm+iZW1iYnFz7GFvT2TNCU=","tree_head_signature":"BAMARzBFAiEA5X6Ss4I9nz+s54PtGR/rSMUHI+/i704pwW32MR9kK4CIFgpoSOcZF6eQMKo+7u00VLBH1Wse4o9GX85kegTzBkR"}
```

Subject 23.ctlog.digital.gov.ru
SAN 23.ctlog.digital.gov.ru
Valid from Fri, 22 Apr 2022 09:52:52 GMT
Valid until Sat, 22 Apr 2023 09:52:52 GMT
Issuer Russian Trusted Sub CA

Open full certificate details

Certificate Transparency

- SCT Yandex Agate-2023 log (Embedded in certificate, Verified)
- SCT VK 'NCA2023' Log (Embedded in certificate, Verified)
- SCT The Ministry of Digital Development and Communications '2023' Log (Embedded in certificate, Verified)

Сертификат

Общие Состав Путь сертификации

Путь сертификации

- Russian Trusted Root CA
 - Russian Trusted Sub CA
 - 23.ctlog.digital.gov.ru

Просмотр сертификата

Состояние сертификата:

Этот сертификат действителен.

OK

Сертификат

Общие Состав Путь сертификации

Показать: <Все>

Поле	Значение
Идентификатор ключа...	Идентификатор ключа=d1e1710d0...
Использование ключа	Цифровая подпись, Шифрование ...
Дополнительное имя...	DNS-имя=23.ctlog.digital.gov.ru
Улучшенный ключ	Проверка подлинности сервера (1...
Основные ограничения	Тип субъекта=Конечный субъект, ...
Доступ к информации...	[1]Доступ к сведениям центра сер...
Точки распространения...	[1]Точка распределения списка от...
Список SCT	v1, dead694a0af3d42b868241d45ee...
Отпечаток	b18d4f191f907e9375ecec6ff627364a...

v1
dead694a0af3d42b868241d45eef0563fbcf6a5143e2dc621a845fe89f509bdd
22 апреля 2022 г. 12:50:58
SHA256
ECDSA
3045022100d4f1906815714ab0e51a8a99f931974e967f2f7de1f69960d4e251c6c34e7e600220202a17fbfa5881d478edfa871796cb606e7e188dd727ac160bc637513b2617f9

Свойства... Копировать в файл...

OK

Вебмастер

Выбрать сайт +

Уведомления Проверка наличия сертификата НУЦ

Проверка наличия сертификата национального удостоверяющего центра

Сертификат Национального центра сертификации можно получить на портале [Госуслуги](#), если был отозван сертификат безопасности международного центра. При выдаче документа обязательно будет проверена связь получателя с сайтом, а само название ресурса будет опубликовано в публичном логе <https://www.gosuslugi.ru/tls>. Подробно см. [о поддержке сайтов с национальными сертификатами в Яндекс Браузере](#).

23.ctlog.digital.gov.ru

Домены	Тема	Выдан	Действительность	Сертификат
23.ctlog.digital.gov.ru	CN=23.ctlog.digital.gov.ru, O=The Ministry of Digital Development and Communications, L=Moscow, ST=Moscow, C=RU	CN=Russian Trusted Sub CA, O=The Ministry of Digital Development and Communications, C=RU	22 апреля 2022 г. - 22 апреля 2023 г.	<input type="button" value="Показать сведения"/> (CT Precertificate)

Какие планы на будущее?



**Благодарим
за внимание!**

