Практические выводы по результатам тестирования решения TLS ГОСТ в рамках выполнения поручения президента Пр-1380

Бадмаева Римма

Предыстория

TLS ГОСТ: почему и зачем?

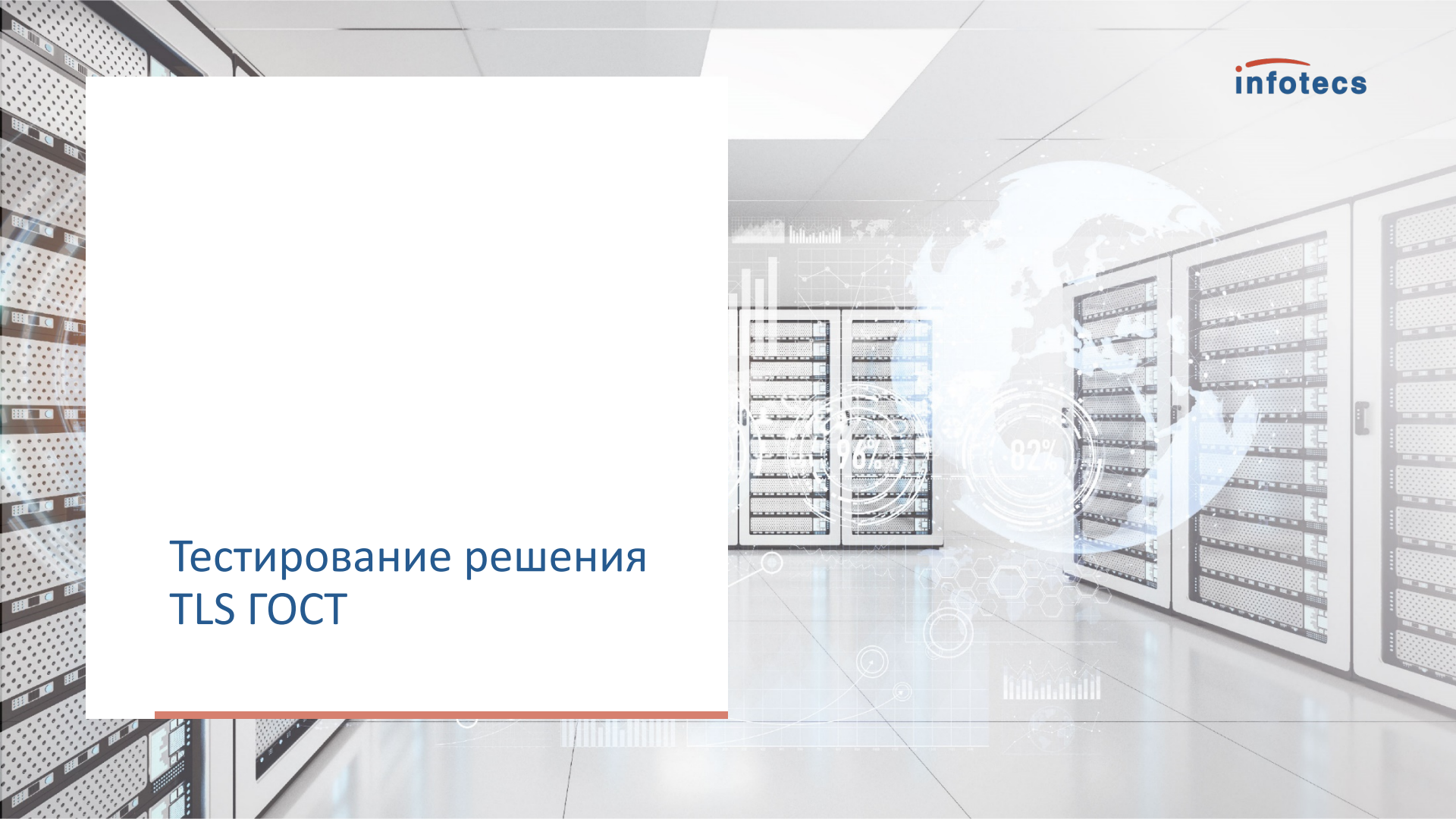
infotecs

Уже прозвучал доклад:

Пьянченко Андрей Андреевич, *руководитель департамента, НИИ «Восход»*

Мероприятия по переходу на использование российских криптографических алгоритмов между государством и обществом

Не будем повторяться!



Тестирование решения TLS ГОСТ

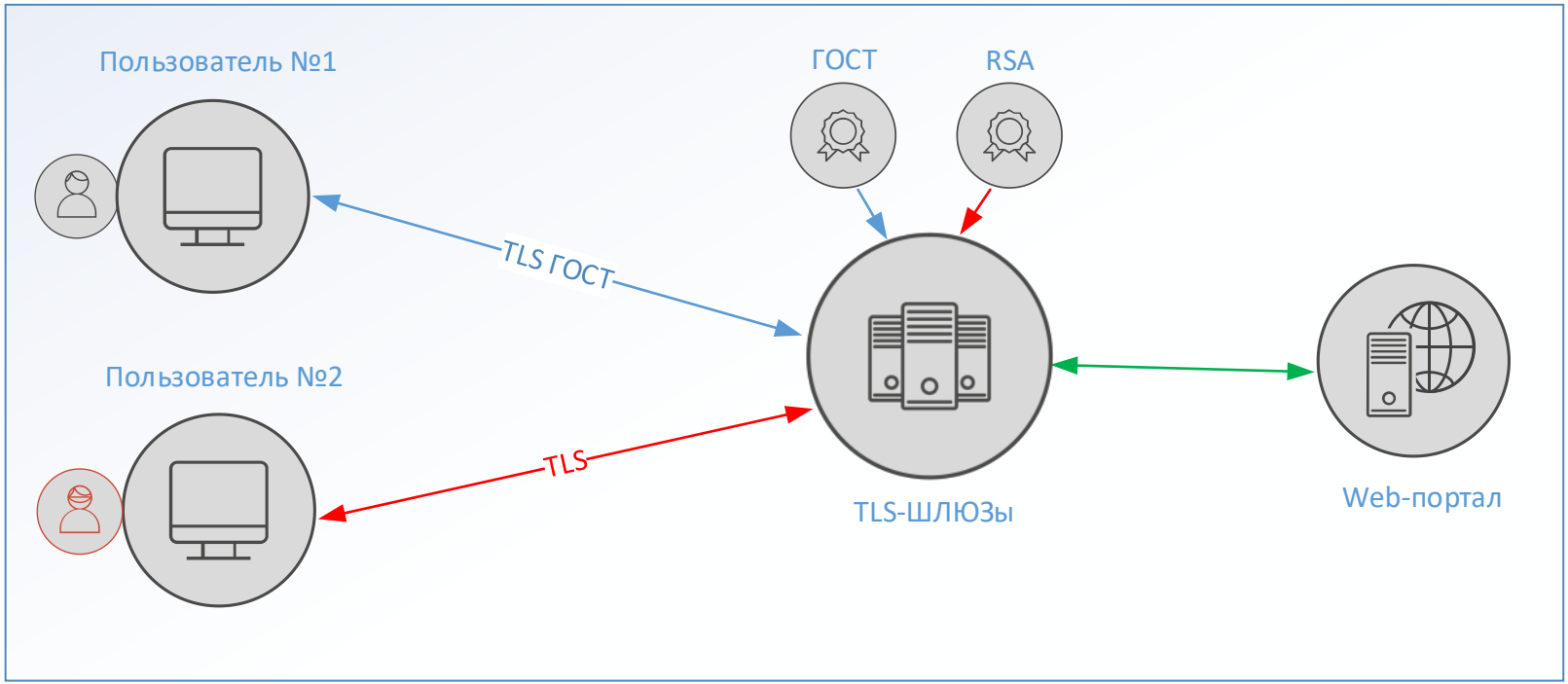
Тестирование решения TLS ГОСТ: как это было

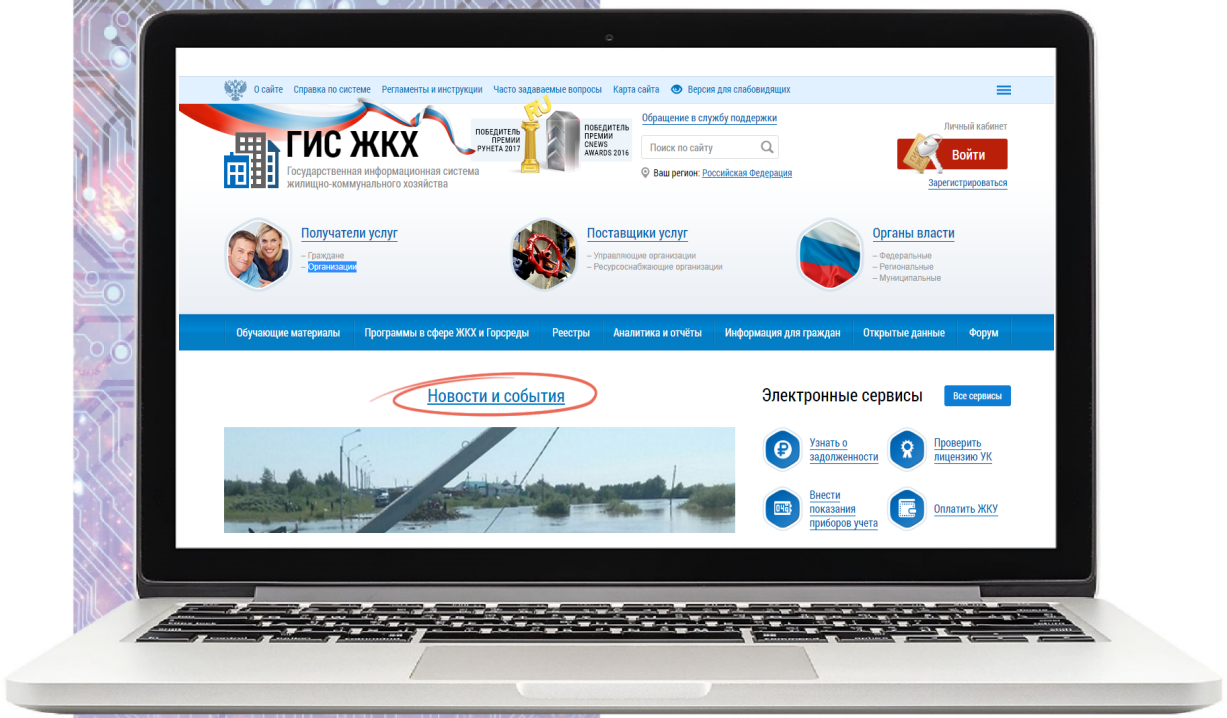
Дано:

1. TLS-шлюзы нескольких вендоров.
2. Общедоступный государственный портал - ГИС ЖКХ.
3. Площадка для тестирования – НИИ «Восход».

Задача: защита канала связи между ПК пользователя (ОС Windows) и порталом в прозрачном для самого пользователя режиме.

Тестирование решения TLS ГОСТ: как это было





Тестирование решения TLS ГОСТ: результаты

Теорема существования доказана!

Есть техническая возможность перехода на использование российских криптоалгоритмов!

infotecs

Анализ результатов тестирования

Вопросы, которые необходимо решить для полномасштабного перехода на TLS ГОСТ

1. Обеспечение доверия к сертификату серверной стороны

Обеспечение доверия к сертификату серверной стороны

infotecs

Ждем Национальный удостоверяющий центр…

Вопросы, которые необходимо решить для полномасштабного перехода на TLS ГОСТ

2. Возможность использовать любой браузер для доступа к информационным ресурсам, защищённым на алгоритмах ГОСТ. В ряде случаев требуется встраивание криптобиблиотек в конечные приложения

Вопросы, которые необходимо решить для полномасштабного перехода на TLS ГОСТ

При встраивании криптографических SDK возникает целый ряд трудностей и ограничений. Разработчику мобильного приложения требуется:

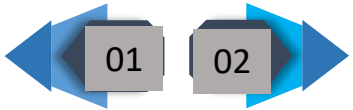
- иметь соответствующий набор лицензий: распространение СКЗИ так же является лицензируемым видом деятельности.
- выполнять предписанные требованиями меры по учёту и контролю целостности СКЗИ.

Для обеспечения массового распространения СКЗИ, реализующих TLS ГОСТ, необходимо внесение изменений в нормативную базу, упрощающих порядок разработки и оборота подобных средств.

TLS ГОСТ : технические решения ИнфоТеКС

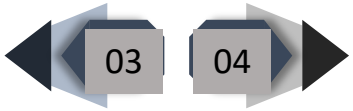
Для серверной стороны: ViPNet TLS Gateway

Шлюз безопасности, обеспечивающий защиту каналов по протоколу TLS с использованием алгоритмов ГОСТ и не ГОСТ



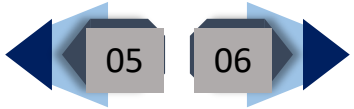
ГОСТ Р 34.10-2001/2012,
ГОСТ Р 34.11-94/2012,
ГОСТ 28147-89

Поддержка сертификатов, изданных разными УЦ, в т.ч. аккредитованными



Разные схемы аутентификации для защищаемых ресурсов

Поддержка политик разграничения доступа



Исполнения ПАК и ПК

Для серверной стороны: ViPNet TLS Gateway

Название исполнения	TLS VA	TLS 500	TLS 1000	TLS 5000
Предельная пропускная способность в режиме обратного HTTPS-прокси (Мбит/с)	зависит от характеристик аппаратного обеспечения	до 300	до 750	до 3000
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси и TCP-туннеля	зависит от характеристик аппаратного обеспечения	до 4700	до 8900	до 43500

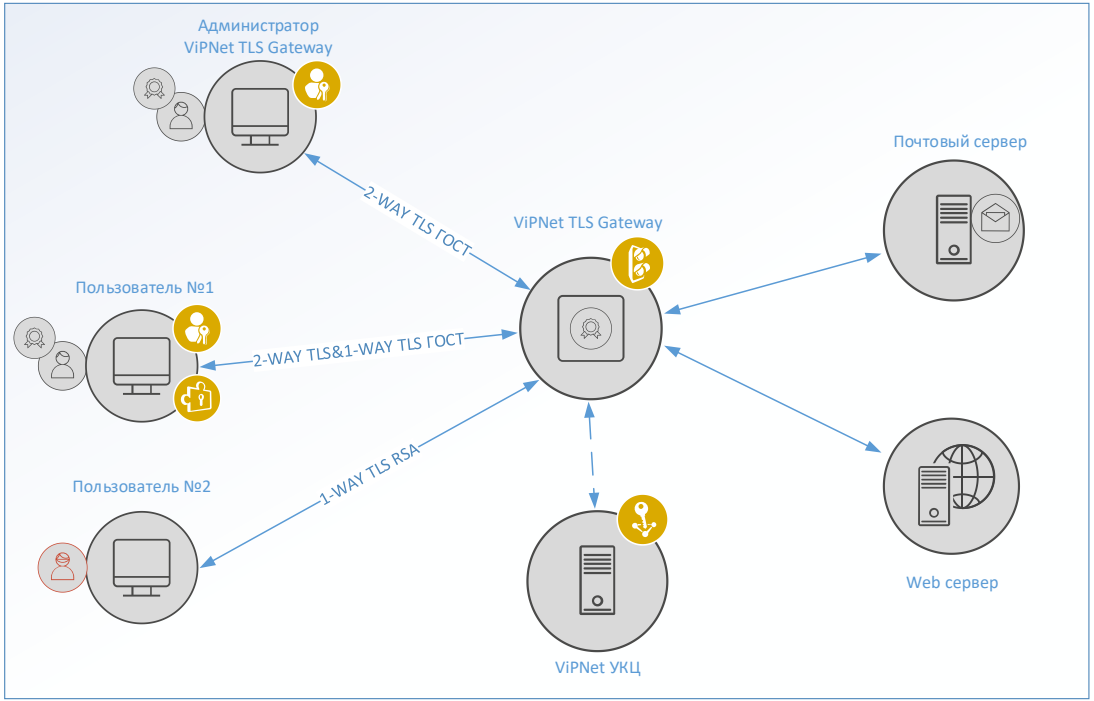
Для клиентской стороны: ViPNet PKI Client

1. Универсальный клиент для работы в инфраструктуре открытых ключей
2. Простой и удобный
3. TLS ГОСТ в любом браузере (Win&Lin)

Хотите TLS ГОСТ? Смотрите как!

Разные режимы работы:

1. Портальный режим.
2. Прозрачный режим.
3. Дуальный режим.



Хотите TLS ГОСТ? Спросите как!

infotecs

Выбирайте профессионалов при проектировании!

Обращайтесь к вендору!

infotecs

Спасибо
за внимание!