НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Тестирование совместимости создаваемых СКЗИ различных производителей, использующих криптографические алгоритмы, утверждённые в качестве национальных стандартов

Минаков С.С., НТЦ ЦК, 2025 г.

НТЦ ЦК

Цели проекта

РусКрипто XXVII научно-практическая конференция

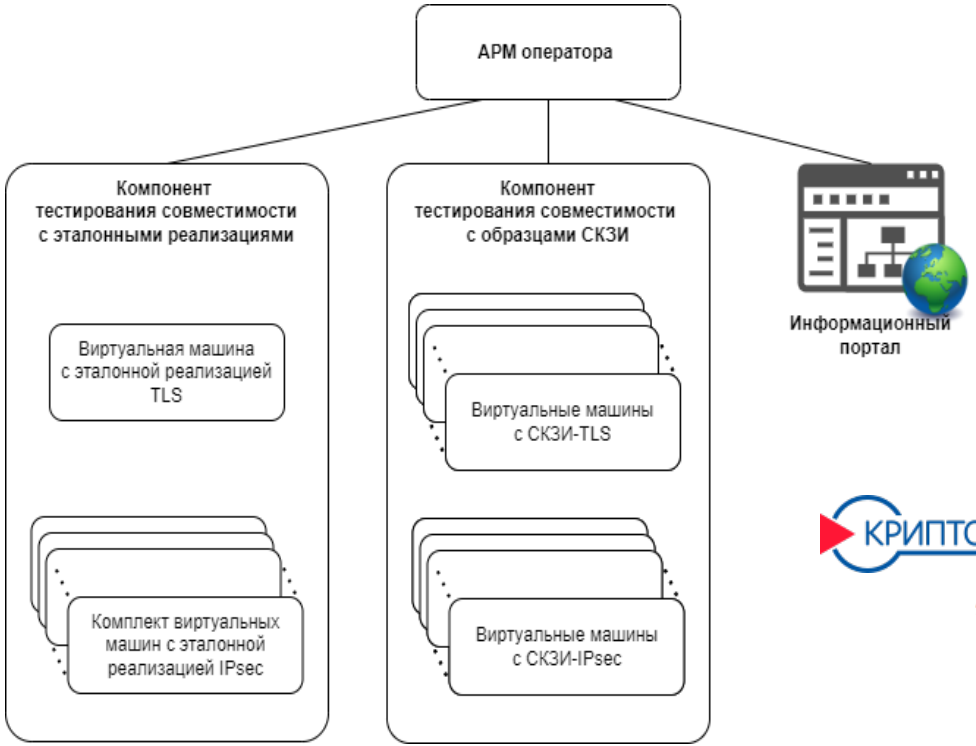
Цели проекта:

- **устранение несовместимости продуктов** от разных производителей,
- **снижение финансовых и иных затрат** потребителей отечественных продуктов в области информационной безопасности,
- **повышение уровня доверия потребителей** к отечественным СКЗИ и сервисам, работающим на их основе,
- **содействие разработчикам** решений в сфере защиты информации, основанных на российских криптографических стандартах,
- **ускорение темпов внедрения** и продвижения отечественных СКЗИ в информационные системы.

Способ достижения цели - создание и использование платформы тестирования алгоритмической совместимости с СКЗИ

НТЦ ЦК

Схема платформы тестирования



Компоненты:

- эталонные реализации
- коммерческие образцы
- узел управления
- информационный портал

КРИПТОПРО infotecs элвис-плюс криптоком КОД безопасности

РусКрипто XXVII научно-практическая конференция

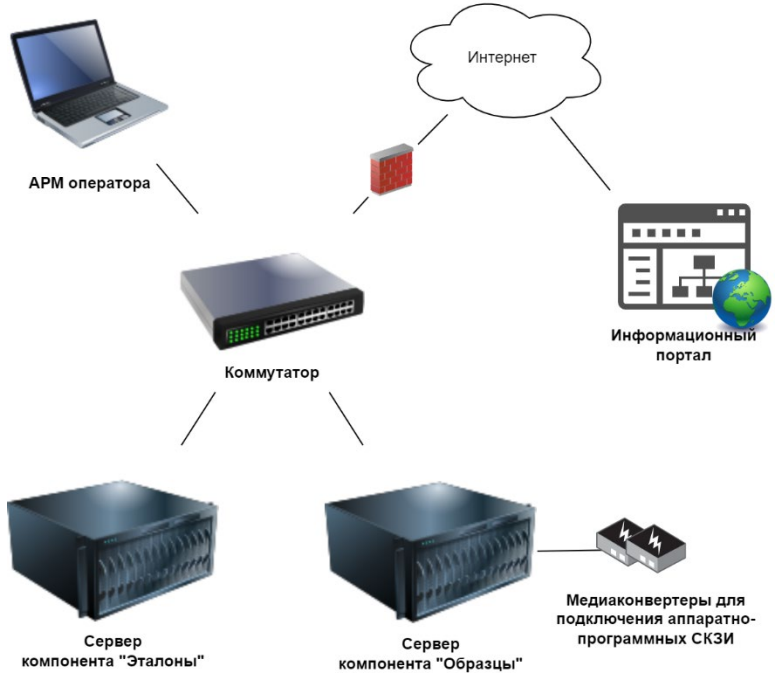
НТЦ ЦК

Из чего построена платформа

РусКрипто XXVII научно-практическая конференция

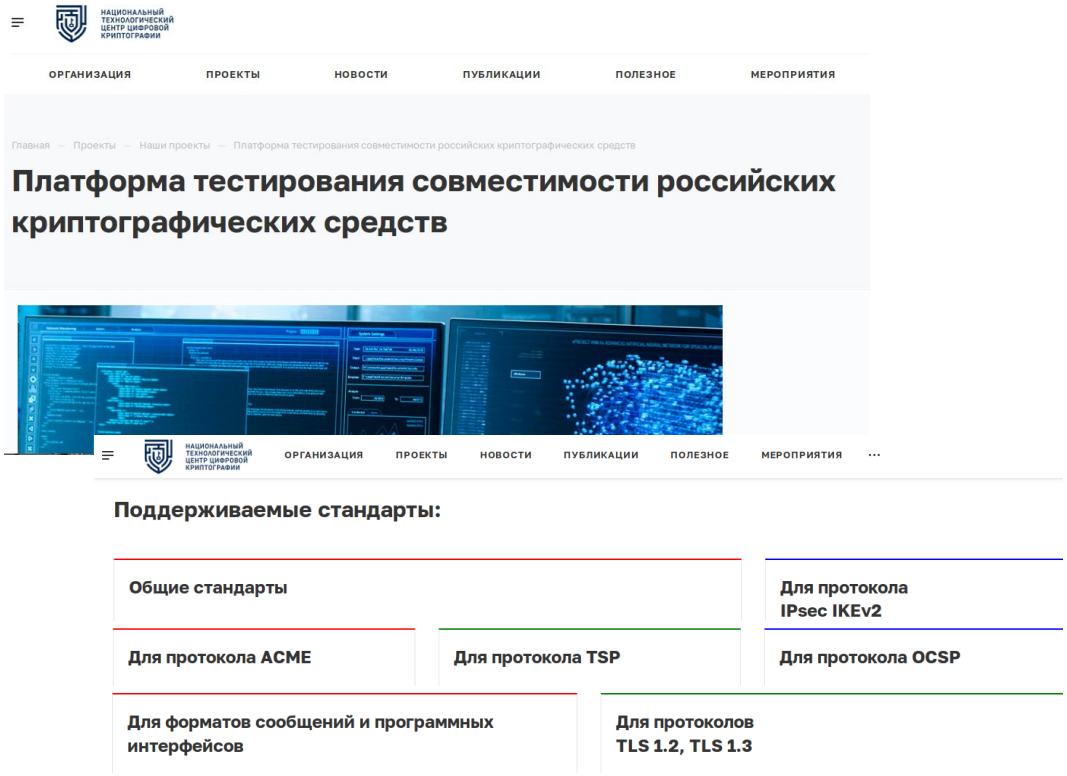
Серверное и телекоммуникационное оборудование:

- высокопроизводительные сервера YADRO X2-105
- ноутбук ASUS VivoBook
- коммутатор, медиаконвертеры, структурированная кабельная сеть
- Операционная система: Astra Linux Special Edition



НТЦ ЦК

Разработан портал платформы



Возможности портала:

- предоставляет информацию о поддерживаемых стандартах, протоколах, форматах сообщений
- обеспечивает приём заявок на проведение испытаний
- описывает последовательность работ

РусКрипто XXVII

НТЦ ЦК

Методология проведения тестирования

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Регламентирующие документы:

- Методика проведения тестовых испытаний совместимости
- Сценарии тестирования совместимости СКЗИ, реализующих протоколы безопасности TLS 1.2, TLS 1.3 и набор протоколов IPsec IKEv2/ESP с отечественными криптографическими алгоритмами:
    - TLS 1.2 – 6 сценариев
    - TLS 1.3 – 5 сценариев
    - IPsec IKEv2/ESP – 15 сценариев

НТЦ ЦК

Возможности Платформы в 2024 году

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Функционал Платформы в части:

тестирования протоколов:

- получения статуса сертификата (OCSP),
- штампов времени (TSP);

форматов сообщений и криптоконтейнеров:

- сообщения, защищённые криптографическими методами (CMS),
- запрос подписания сертификата (PKCS#10),
- транспортный ключевой контейнер (PKCS#12),
- список аннулированных сертификатов (CRL);

программных интерфейсов:

- PKCS#11.

НТЦ ЦК

Сценарии проведения тестирования

РусКрипто XXVII

Примеры сценариев тестирования для протокола TLS 1.2

Возможности		Сценарий					
		1	2	3	4	5	6
Схема обмена сообщениями в протоколе Handshake	Полная						
	Упрощённая с механизмом Session ID						
	Упрощённая с механизмом Session Ticket						
Тип аутентификации	Односторонняя						
	Двусторонняя						
Сертификат сервера ГОСТ Р 34.10-2012	EC512a						
	EC256b						
	EC256a						
	EC512c						
Сертификат клиента ГОСТ Р 34.10-2012	EC256b						
	EC512c						
Криптонабор	TLS_GOSTR341112_256_WITH_ KUZNYECHIK_CTR_OMAC (0xC1 0x00)						
	TLS_GOSTR341112_256_WITH_ MAGMA_CTR_OMAC (0xC1 0x01)						
	TLS_GOSTR341112_256_WITH_ 28147_CNT_IMIT (0xC1 0x02)						
	TLS_GOSTR341112_256_WITH_ 28147_CNT_IMIT (0xFF 0x85)						
Расширение renegotiation_info[1]	Пустое						
	verify_data						
Расширение extended_master_secret*	Есть						
	Нет						
Смены ключей защиты записей**							

Пример выполнения (сценарий №2):

1. Соединение Full Handshake:
   - аутентификация двусторонняя с использованием сертификатов. Алгоритм подписи ГОСТ Р 34.10-2012 256 бит, EC256b
   - криптонабор TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC (IANA 0xC1 0x01)
2. Обмен данными:
   - скачать файл размером 1040 байт
3. Проверка корректности передачи данных:
   - вычислить значения хэш-функции по ГОСТ Р 34.11-2012

НТЦ ЦК

Этапы проведения тестирования на Платформе

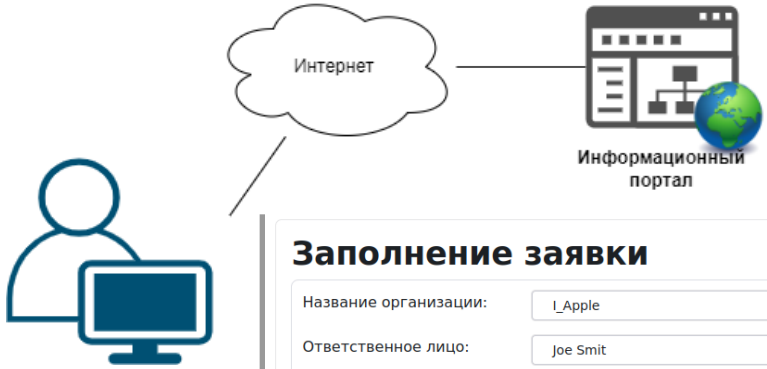
1. Подача заявки через информационный портал Платформы
2. Подготовка индивидуального стенда для тестируемого в виде набора виртуальных машин в зависимости от перечня тестируемых протоколов
3. Проведение тестирования совместимости в соответствии с методикой и сценариями (удаленно или с прямым подключением к Платформе)
4. Документирование результатов тестирования

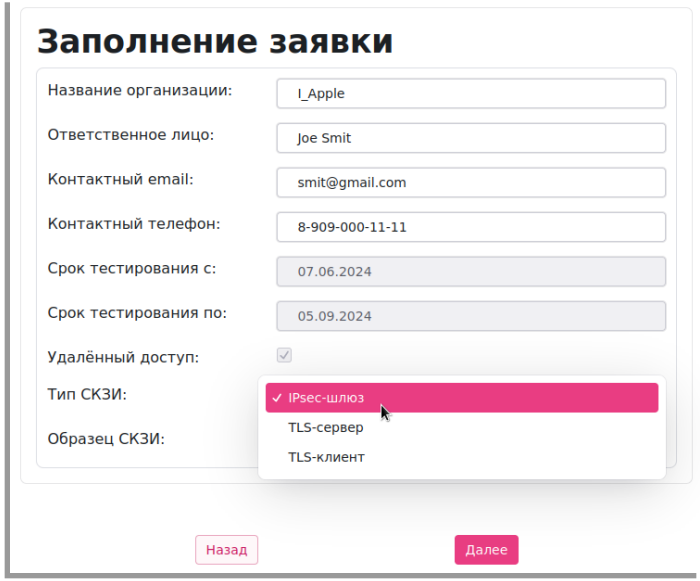
РусКрипто XXVII научно-практическая конференция

НТЦ ЦК

Автоматизация подачи заявки

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ





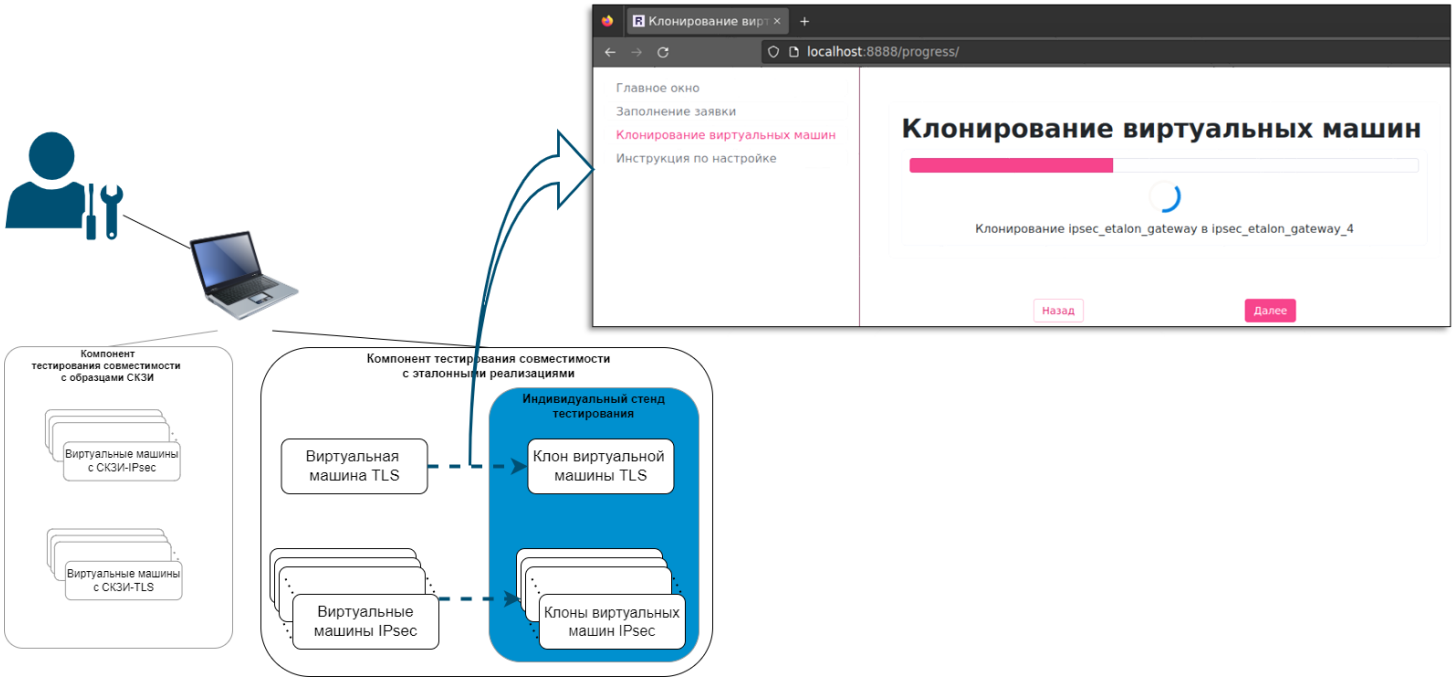
Способы подачи заявки:

- заполнение формы на портале
- e-mail

НТЦ ЦК

Подготовка индивидуального стенда для тестируемого в виде набора виртуальных машин в зависимости от перечня тестируемых протоколов

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ



НТЦ ЦК

Этап тестирования совместимости в соответствии с методикой и сценариями (с прямым подключением к стенду Платформы)

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

СПАСИБО:

МОИ КОЛЛЕГАМ ИЗ НТЦ ЦК
И КРИПТОНИТ - ЗА РАЗРАБОТКУ

СЛУШАТЕЛЯМ - ЗА ВНИМАНИЕ