КриптоПро NGate – уникальный шлюз и VPN

Что внутри, и когда оно случится

ТЗ на КриптоПро NGate

ТЗ, согласованное с ФСБ России 30 января 2017 года:

- Исполнения 1-10: на основе TLS (SSL) с ГОСТ: КС1, КС2, КС3
- Исполнения 11-20: на основе IPsec с ГОСТ: КС1, КС2, КС3

Для всех классов и обоих протоколов:

- Серверные исполнения
- Клиентские исполнения
- Система управления

Исполнения с TLS (SSL): тематические исследования завершены, отчет с положительными выводами на экспертизе в ФСБ России.

Основа NGate: КриптоПро CSP

18 лет развития продукта.

- Рекордные скорости реализации российской криптографии: скорости шифрования в 420 МБ/с на поток, оптимальность алгоритмов вычисления кратких точек, низкоуровневые реализации всех криптографических механизмов с учетом специфики архитектур…
- Меры ИК-защиты и защиты от атак по побочным каналам на всех уровнях кода криптопровайдера.
- Полностью самостоятельные реализации как российской, так и международной криптографии.

Основа NGate: КриптоПро CSP

КриптоПро CSP – основа многочисленных партнерских VPN-решений как на IPsec, так и на TLS (SSL).

- Многочисленные совместные сертификации совместных решений, стремление КриптоПро подавляющую часть требований ФСБ выполнять на уровне криптоядра.
- Ключевая система криптопротоколов непосредственно в ядре CSP.
- Система непрерывного нагрузочного тестирования и тестирования производительности криптоядра, ориентированная на скорость работы VPN-решений.
- Реализации с учетом различий в использовании криптоядра на серверной и клиентской стороне.
- 19 вариантов режимов пакетной и мультипакетной обработки данных, заточенных под конкретные протоколы и их применение в VPN-решениях.
- Более 15 лет работы над «TLS с ГОСТ» в российских и международных организациях по стандартизации с учетом потребностей VPN-решений.

Прошлое: первый TLS (SSL) с ГОСТ

«GOST 28147-89 Cipher Suites for Transport Layer Security (TLS)»

- Работа в рамках IETF велась специалистами КриптоПро.
- Документ не был принят в качестве RFC, работа продолжилась в ТК 26 (Технический комитет по стандартизации «Криптографическая защита информации»).

«Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms»

- Работа в рамках IETF велась специалистами КриптоПро.
- Документ был принят в качестве RFC 4357, исходный основной RFC по криптографии представителей РФ.

Настоящее: TLS на текущей базе криптографических стандартов

«Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)»

- Методические рекомендации утверждены ТК 26 24.04.2014.
- Разработка – в Рабочей группе ТК 26.
- Основной протокол криптографической защиты с использованием ГОСТ в сети Интернет.
- Криптографический стержень текущей версии КриптоПро NGate.

Ближайшее будущее: TLS с «Кузнечиком» и «Магмой»

КРИПТОПРО

«Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»

- В Плане национальной стандартизации Росстандарта на 2018 год от ТК 26; ответственные – КриптоПро.
- Разработка документа – в Рабочей группе ТК 26.
- Прошел экспертизу по криптографической стойкости, 29 марта 2018 года на заседании Рабочей группы вынесен на утверждение в ТК 26 (на заседание 11 апреля 2018 года).
- В 2018 году должен быть утвержден в Росстандарте и введен в действие.
- Разработка стандарта велась с полным учетом потребностей VPN-решений, в том числе будущих версий КриптоПро NGate.

Будущее: TLS 1.3 с ГОСТ

«Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)»

- В Лондоне на IETF 101 в марте 2018 принят TLS 1.3: безопаснее, быстрее, удобнее и надежнее.
- В Плане национальной стандартизации Росстандарта на 2019 год от ТК 26.
- Разработка документа – в Рабочей группе ТК 26.
- Цикл научных семинаров в МГУ имени М.В. Ломоносова под руководством специалистов МГУ и КриптоПро.
- Работы в ТК 26 и IETF по разработке механизмов, необходимых для работы TLS 1.3.
- Будущее КриптоПро NGate.

От фундамента до продукта – примеры

КРИПТОПРО

Синтез ключевой системы в рамках работ в ТК 26

Глубокое понимание архитектуры протокольных решений

Максимальное использование ресурса параллелизма в реализациях

Исключительные параметры производительности NGate

От фундамента до продукта – примеры

КРИПТОПРО

Синтез эллиптических кривых для PKI России (RFC 4357, RFC 7836, P 50.1.114–2016)

Доскональное изучение быстрых алгоритмов работы на эллиптических кривых

Оптимальные по времени реализации процедур согласования ключей

Большое количество соединений в секунду в NGate

От фундамента до продукта – примеры

Разработка понятийного аппарата функциональной законченности СКЗИ

Инкапсуляция безопасной работы с ключами ниже реализации протоколов

- Повышение защищенности по Требованиям ФСБ России
- Сокращение времени тематических исследований

Фундамент продукта

Работа над решениями на основе TLS и IPsec от теоретических основ и синтеза криптографических механизмов до законченных продуктов и сертификатов ФСБ России.

- Руководство рабочими группами ТК 26, членство в экспертном совете IETF по криптографии, конференции под эгидой ФСБ России.
- Десятки стандартов и спецификаций по протоколам и используемым в них криптографическим механизмам, разработанных под руководством или при участии экспертов КриптоПро.

- Многолетнее развитие криптоядра с поддержкой TLS и IPsec, десятки сертифицированных решений на TLS и IPsec.
- Сотни инженерно-технических решений, направленных на повышение производительности TLS и IPsec.

Фундамент продукта

Работа над решениями на основе TLS и IPsec от теоретических основ и синтеза криптографических механизмов до законченных продуктов и сертификатов ФСБ России.

- Руководство рабочими группами ТК 26, членство в экспертном совете IETF по криптографии, конференции под эгидой ФСБ России.
- Десятки стандартов и спецификаций по протоколам и используемым в них криптографическим механизмам, разработанных под руководством или при участии экспертов КриптоПро.

- Многолетнее развитие криптоядра с поддержкой TLS и IPsec, десятки сертифицированных решений на TLS и IPsec.
- Сотни инженерно-технических решений, направленных на повышение производительности TLS и IPsec.

Максимальное использование всех наработок в КриптоПро NGate – ради быстродействия, надежности и соответствия требованиям ФСБ России.

Планы по срокам

КРИПТОПРО

Исполнения 1-10: TLS с ГОСТ

- ТЗ согласовано ФСБ России 30 января 2017 года.
- Тематические исследования проводились с середины 2017 года.
- Завершены с положительными результатами в феврале 2018 года.
- Отчет с положительными выводами направлен на экспертизу в ФСБ России 27 февраля 2018 года.
- Ожидаемый срок получения заключения – 3 квартал 2018 года.

Спасибо за внимание!