О построении систем управления ключами на основе облачных решений, существующей PKI и методических документов ТК 26

Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации

PKI-Форум Россия 2016

Спецификация KMIP

Основная цель

Возможность создания совместимых систем работы с ключами, позволяющих решать вопросы выбора той или иной стратегии управления ключами отдельно от прикладных продуктов, в которых предполагается криптографическая защита.

- 2010: OASIS KMIP 1.0 — принципы работы с ключами, хранимыми на сервере.
- 2016: OASIS KMIP 1.4 — уточнение механизмов импорта/экспорта ключей, поддержка транспортных контейнеров.

2015, RSA Conference

- 14 компаний демонстрируют совместимость со спецификацией.
- Ведущие производители (включая Thales, SafeNet) рассказывают о широких перспективах рынка решений по управлению ключами в соответствии с KMIP.
- Интеграция с Dropbox, Google Cloud, Amazon Web Services.

Key Management Interoperability Protocol (KMIP): Addressing the Need for Standardization in Enterprise Key Management

„Most important is the risk that the data, once encrypted, cannot be decrypted because the key for that encrypted data has been lost. For this reason, applications, devices and other systems using symmetric key encryption need to be supported by robust key management systems that ensure that keys cannot be lost or misused.“

Отчет Thales e-Security

“53% утечек связаны с ошибками сотрудников — ключи должны храниться под корпоративным контролем.“

DELL

„Критично для защиты данных на долговременном хранении.“

HP

„Важность надежной единой точки управления ключами.“

IDQ

„Предотвращение проблем из-за слабых ДСЧ.“

Intel

„Критичность хранения ключей под контролем организации.“

NetApp

„Обеспечивает безопасное резервное копирование в облаке.“

Amazon Web Services

- Централизованное хранение и аудит ключей.
- Строгое разграничение доступа к ключам.
- Работа в точности как с локальным провайдером/ключевым носителем.
- Неизвлекаемость долговременных ключей из HSM.
- Доверенные ДСЧ.
- Работа с PFS-сюитами в качестве TLS-сервера.

IBM

- Строгое журналирование.
- Централизованное управление работой с серверами TSP и OCSP.
- Мгновенная блокировка доступа уволенного сотрудника к ключам.
- Защита от проблемы утери данных из-за потери сотрудником ключевых носителей.

Преимущества работы с ключами в облаке

- Безопасные процедуры создания и уничтожения ключевой информации.
- Централизованное управление процедурами защиты информации: форматами подписи, доступом к TSP и OCSP.
- Управление доступом пользователей к ключам.
- Аудит использования ключей.
- Контролируемое кратковременное использование сессионных ключей.
- Решение критичных для отказоустойчивости систем вопросов резервирования ключевой информации

Возможность развития аналогичных технологий в РФ

Создание консорциума/ТК/ПК в ТК 26 с нуля?

Избыточно тяжелая система мероприятий.

Интеграция в работы OASIS для поддержки российских алгоритмов?

Различия в криптографических и инженерных требованиях к системам работы с ключами, так и из-за вероятного отсутствия заинтересованности зарубежной стороны в данном процессе.

- Отсутствие самостоятельной криптосистемы с открытым ключом.
- Требования по нагрузке на ключ (пример: TLS и Sweet32).
- Строгие требования по стойкости алгоритмов: на уровне не менее 2^{128} (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, 256), которому соответствует (см. NIST 800-57) RSA-3072, а де-факто массово с AES-128 и AES-256 используется RSA-2048.

Существующий задел в рамках существующего Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)

Процедуры перехода от ключевых пар к симметричным ключам

В документах ТК 26: большой объем наработок в области ключевых систем, имеющих своим фундаментом долговременные пользовательские ключевые пары ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012, хранимые на носителях или в памяти программно-аппаратных криптографических модулей (ПАКМ).

Существующий задел

Функционал, аналогичный построенному на основе ключей RSA (при отсутствии стандарта на КС с ОК): широкий спектр протокольных решений, использующих ключи ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012 для построения на их основе систем ключей шифрования, аутентификации и имитозащиты.

- RFC 4357, RFC 4490, RFC 7836.
- Рекомендации ТК 26 „Использование криптографических алгоритмов, сопутствующих применению ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012“: VKO, KDF_TREE.
- Проекты ТК 26: ACPKM, процедуры экспорта ключа.
- Документы ТК 26 по использованию российских криптографических стандартов в CMS, TLS, IKE.
- Нестандартизованные, но происследованные решения: российские криптоалгоритмы в XMLenc, EFS, IKEv2.

Существующий задел

Основное: переход между ключевыми парами и сессионными ключами в отсутствии криптосистемы с открытым ключом.

- Выработка ключа KEK по VKO на основе открытого ключа адресата и эфемерного ключа.
- Шифрование ключа защиты данных на KEK.

Пример

Защита PIN при передаче от терминала на карту в документах РГ ТК 26 по криптоалгоритмам в НСПК.

Осталось в рамках тех же процедур переместить долговременные ключи с токена на „виртуальный токен“ — в облачное хранилище.

Предлагаемый путь:

- Работу с долговременными ключами производить не на пользовательском рабочем месте, а на защищенном ключевом сервере на основе сертифицированного ПАКМ.
- С помощью существующих исследованных (в т.ч., в ТК 26) механизмов вырабатывать одноразовые сессионные ключи.
- Решения перекрывают существенную часть вопросов, рассматриваемых в KMIP.
- Бесшовность перехода существующих решений на поддержку корпоративных систем управления ключами: всего лишь выбрать в качестве криптопровайдера тот, что для работы с долговременными ключами обращается (прозрачным для пользователя образом) к ключевому серверу.
- Аутентификация пользователей производится на основе существующей PKI.
- Механизмы управления ключами — на базе существующих криптографических протоколов.

Преимущества

- Централизованная система хранения, управления и использования ключевой информации.
- Требует минимальных модификаций существующего ПО для работы с личными ключами.
- Благодаря использованию существующих интерфейсов и протоколов не требует отдельной стандартизации для обеспечения совместимости.
- Одноразовые симметричные ключи — решение вопросов с ограничением нагрузки.

Защищенность серверной части

Существенная часть вопросов, связанных с переносом ключей на сервер, сопряжена с безопасностью самого хранилища ключей и должна быть рассмотрена в рамках тематических исследований ПАКМ, обеспечивающего работу ключевого сервера.

- Thales (семейство KeyAuthority), SafeNet (семейство KeySecure): требования к хранению ключей, криптографической и инженерной защите по FIPS 140-2.
- В России: действующая система требований ФСБ России.

Обеспечение защищенного доступа

Критически важно обеспечить защиту канала связи от пользовательского рабочего места до ключевого сервера.

Иначе: возможность проведения атак с подменой подписываемых сообщений противоречит принципу персональной ответственности пользователя за подписываемые данные.

- Аутентификация по сертификатам.
- Аутентификация на основе мобильных устройств.
- Аутентификация на основе пароля без снижения стойкости (пример — HP, протокол PKEX).

Обеспечение защищенного доступа

Решения на основе рекомендаций по стандартизации ТК 26

- Доступ с использованием сертификатов: „Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)“.
- Доступ с использованием мобильного устройства на основе HMAC_GOSTR3411_2012_256 и KDF_TREE (RFC 7836): решения для аутентификации операций пользователей, в т.ч. на основе SIM-карт (см. доклад Positive Technologies „Актуальные проблемы и методы решения двухфакторной аутентификации в финансовых сервисах для физических лиц“ на РусКрипто’2016).
- Доступ с использованием пароля с уровнем защищенности не меньше, чем в случае высокоэнтропийного секрета: протокол SESPAKE, „Протокол выработки общего ключа с аутентификацией на основе пароля“.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии: svs@cryptopro.ru.