УДК 004.056
DOI 10.51691/2541-8327_2022_12_35

ВНУТРЕННЯЯ СТРУКТУРА СЕРВИСА УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Микаева А.С.
к.э.н., доцент,
МИРЭА - Российский технологический университет,
Москва, Россия

Николаев Г.А.
студент,
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации,
Москва, Россия

Аннотация

Важнейший ресурс в современном мире – информация, поэтому защита информации является приоритетной задачей, стоящей перед обществом. Одним из решений данной задачи является криптография, основными средствами которой являются ключи шифрования, которые также требуют защиты. В связи с этим разработана система управления криптографическими ключами. Эта статья определяет ключевые моменты, на которые стоит обратить внимание при реализации собственной системы менеджмента ключей. Подробно рассмотрены задачи жизненного цикла криптографических ключей, их хранения, обеспечение безопасности, шифрования данных, а также ведения журналов аудита.

Ключевые слова: криптографические ключи, управление ключами, шифрование, криптография, аппаратный модуль безопасности

INTERNAL STRUCTURE FOR KEY MANAGEMENT SERVICE

Mikaeva A.S.
Candidate of Economics, Associate Professor,
MIREA - Russian Technological University,
Moscow, Russia

Nikolaev G.A.
student,
The Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia

Abstract

The most important resource in the modern world is information, so the protection of information is a priority task facing society. One of the solutions to this problem is cryptography, the main means of which are encryption keys. But keys are also information that needs to be protected. In this regard, they came up with a cryptographic key management system that provides the user with a convenient interface for data protection. This article identifies the key points to consider when implementing a key management system and will also help to better understand the topic of cryptography in general.

Keywords: cryptographic keys, key management service, encryption, cryptography, hardware security module.

Криптографические ключи играют важную роль в любой системе безопасности. Именно они управляют шифрованием данных, а также расшифровкой и аутентификацией пользователя. Если какой-либо из этих ключей будет скомпрометирован, это может разрушить всю инфраструктуру безопасности организации, что в итоге может позволить злоумышленнику получить доступ к конфиденциальным файлам, информации и данным компании. Кроме того, злоумышленник может аутентифицировать себя как уполномоченного специалиста, чтобы получить доступ к секретной информации. Но благодаря наличию сервисов управления ключами (KMS, Key Management Service) компаниям становится проще определять конкретные стандарты и политики конфиденциальности для защиты этих криптографических ключей при ограничении доступа к ним. Таким образом,

управление ключами формирует фундаментальную основу для защиты конфиденциальных данных и информации.

Основными функциями сервиса управления ключами криптографии являются: создание, хранение, обмен, использование, а также замена этих ключей по мере необходимости. Фактически, данный сервис реализует в себе управление жизненным циклом ключей шифрования с использованием стандартов PKI (Public Key Infrastructure) [1]. Для обеспечения максимальной безопасности криптосистемы KMS также включает в себя пользовательские процедуры, серверы ключей, схемы криптографических протоколов и т. д. Основные задачи KMS представлены на рисунке 1.

Рис. 1 – Задачи сервиса управления криптографическими ключам [4]

Для защиты и хранения ключей KMS использует аппаратные модули безопасности (HSM, Hardware Security Module). HSM — это физическое устройство, обеспечивающее дополнительную защиту ключей и использующееся для обработки критически важных криптографических операций, таких как шифрование и дешифрование, а также аутентификация [2].

С помощью KMS пользователь может создать ключ, который будет храниться в базе данных KMS в зашифрованном виде [3, 4]. При этом все криптографические операции над ним будут выполняться исключительно в HSM, включая создание, шифрование и последующую передачу зашифрованного ключа в хранилище KMS через основной сервис. Связи между

KMS, HSM, пользователем и хранилищем зашифрованных ключей пользователя представлены на рисунке 2.

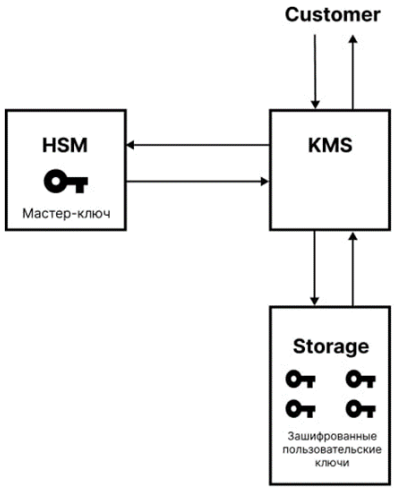

Рис. 2 - Связи между пользователем (Customer), KMS, HSM, хранилищем зашифрованных ключей пользователя (Storage) [2]

Шифрование пользовательского ключа происходит на мастер-ключе HSM [5]. Для выполнения криптографической операции KMS передает зашифрованный ключ пользователя в HSM, в ответ KMS получает результаты данной операции.

Основные этапы создания пользовательского ключа:

1. Пользователь отправляет запрос на создание ключа в KMS.
2. KMS передает запрос о создании ключа HSM.
3. HSM генерирует ключ и шифрует его с помощью мастер-ключа.
4. HSM передает зашифрованный ключ в KMS.
5. KMS кладет этот ключ в хранилище.
6. KMS возвращает пользователю некий результат работы.

Основные этапы прочих криптографических операций:

1. Пользователь отправляет запрос в KMS.

2. Из хранилища KMS извлекается зашифрованный пользовательский ключ.
3. Ключ и пользовательские данные отправляются в HSM.
4. В HSM происходит расшифровка ключа и выполняются криптографические операции.
5. KMS возвращает пользователю полученный от HSM результат работы.

Управление жизненным циклом ключей относится к созданию и изъятию криптографических ключей. Жизненный цикл криптографических ключей – это набор состояний, в которых находится ключ за период своего существования [6]. KMS является централизованной системой, обеспечивает автоматическое обновление и распространение ключей. С ее помощью можно управлять полным жизненным циклом криптографических ключей, основанных на симметричном или ассиметричном шифровании. Системы, реализующие жизненный цикл ключей как правило предоставляют схожий функционал:

- генерация ключей
- обновление ключей
- резервное копирование ключей
- восстановление ключей
- распределение ключей
- ведение журналов аудита
- шифрование данных с использованием мастер-ключа
- сертификация (к примеру X.509)

Жизненный цикл управления криптографическими ключами может быть разделить на четыре фазы:

1. Предоперационная фаза: Криптографический ключ еще недоступен для использования. Ключи еще не сгенерированы или находятся в состоянии предварительной активации.

2. Операционная фаза: криптографический ключ доступен для использования. Ключи находятся в активном или приостановленном состоянии

3. Постоперационная фаза: Криптографический ключ больше недоступен, но доступ к ключевому материалу может быть возможен. Ключи в деактивированном, скомпрометированном или архивном состоянии.

4. Фаза уничтожения: ключи находятся в уничтоженном состоянии и больше не имеется в наличии. Ключевые метаданные могут сохраняться, а могут и не сохраняться. Например, вновь сгенерированный ключ часто лежит в хранилище ключей вместе со старыми ключами, в случае если они не были скомпрометированы.

Определение и применение политик управления ключами шифрования влияет на каждый этап жизненного цикла управления ключами. Каждый ключ шифрования или группа ключей должны регулироваться отдельной политикой использования ключа, определяющей, какое устройство, группа устройств или типы приложений могут его запрашивать, а также какие операции может выполнять это устройство или приложение — например, шифровать, расшифровывать, или подписать. Кроме того, политика управления ключами шифрования может диктовать дополнительные требования к более высоким уровням авторизации в процессе управления ключами для выпуска ключа после того, как он был запрошен, или для восстановления ключа в случае потери.

Для KMS можно выделить два типа журналов аудита: журналы аудита действий администратора и журналы аудита доступа к данным. Журналы аудита действий администратора включает операции административной записи, которые записывают метаданные или информацию о конфигурации. Благодаря данному типу журнала можно вовремя выявить утечку и даже предотвратить возможную компрометацию пользовательских данных. Журналы аудита доступа к данным включает операции «административного чтения», которые считывают метаданные или информацию о конфигурации. Также включает операции

«чтение данных» и «запись данных», которые считывают или записывают предоставленные пользователем данные.

Подводя итог вышеописанному, отметим, что внутренняя структура сервиса управления ключами состоит из HSM, хранилища зашифрованных пользовательских ключей и сервиса-посредника, который взаимодействует с хранилищем и HSM, реализует в себе жизненный цикл криптографических ключей, ведет журнал аудита действий администратора и доступа к данным, а также предоставляет удобный пользовательский интерфейс для работы с KMS.

Библиографический список:

1. ISO/IEC 27099:2022 Information technology — Public key infrastructure — Practices and policy framework
2. ISO 13491-1:2016 Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements, and evaluation methods
3. ISO 8532:1995 Securities — Format for transmission of certificate numbers
4. ГОСТ Р 56938–2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».
5. ГОСТ ISO/IEC 17788–2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология» (ISO/IEC 17788:2014, IDT).
6. Плоткин А.С., Кесель С.А., Репин М.М., Федоров Н.В. Анализ уязвимостей систем управления ключами в распределенных реестрах на примере блокчейн IBM // Вопросы кибербезопасности. 2021. №2 (42). URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-sistem-upravleniya-klyuchami-v-raspredelennyh-reestrah-na-primere-blokcheyn-ibm (дата обращения: 23.12.2022).

Оригинальность 88%