1. Инфраструктура открытых ключей

*Управление открытыми ключами. Организация и компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509.*

*Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа.*

В основе большинства средств защиты, применяемых в информационных системах, лежат криптографические алгоритмы и протоколы или механизмы защиты, которые так или иначе используют их. При конструировании алгоритмов и протоколов предполагается, что секретные и открытые ключи, необходимые для выполнения криптографических операций, уже имеются у субъектов системы. Им остается только грамотно использовать средства защиты, в которых реализованы соответствующие криптографические алгоритмы и протоколы. Однако на практике применение криптографических средств защиты информации сталкивается с необходимостью грамотно распоряжаться криптографическими ключами всех участников системы. Задачи генерации, распространения, хранения, уничтожения криптографических ключей принято относить к одному из разделов прикладной криптографии, получившему название управление ключами.

Управление ключами (key management) - это совокупность технологий и процедур, посредством которых устанавливаются и поддерживаются состояние, в котором взаимодействующие стороны разделяют общие данные – ключи шифрования, между участниками криптографического протокола.

Стойкость любой криптосистемы определяется только степенью безопасности используемых в ней ключей, так как все долговременные элементы криптосистемы (множество правил шифрования, его механизм и пр.) рано или поздно станут известными злоумышленнику. Этот принцип был сформулирован еще в конце XIX в. и получил название правила Керкхоффса (Kerck- hoffs’ desiderata).

Для обеспечения безопасности криптографических ключей хороши любые доступные методы:

* технические средства охраны (изолированные помещения, сигнализация и т. п.);
* защищенная от взлома аппаратура (очень важно обеспечить надежную аутентификацию пользователя при работе с нею!);
* концентрация ключевого материала в небольшом количестве легко наблюдаемых и внушающих доверие компонентов системы.

Основными угрозами ключевому материалу являются следующие:

* утрата конфиденциальности (секретности) секретных криптографических ключей;
* утрата аутентичности секретных или открытых ключей: требование аутентичности означает возможность проверки идентичности лица, обладающего ключевым материалом, действительному владельцу ключа
* несанкционированное использование секретных или открытых ключей, например использование недействительного ключа, нецелевое использование ключа.

Компрометация ключа - событие, в результате которого произошла или могла произойти утрата одного из свойств криптографического ключа, обеспечивающего безопасность криптосистемы.

Таким образом, можно заключить, что основными задачами управления ключами являются:

* обеспечение секретности, подлинности и целостности для секретных криптографических ключей;
* обеспечение подлинности и целостности для открытых криптографических ключей.

Здесь под секретными криптографическими ключами понимаются как общие секретные ключи симметричных криптосистем, так и секретные ключи асимметричных криптосистем (которые в отличие от первых не являются общими для двух или более участников системы, а известны исключительно своим владельцам).

На практике дополнительной целью управления ключами является согласие с действующей политикой безопасности системы.

Жизненный цикл криптографического ключа - это последовательность состояний, в которых пребывает ключевой материал за время своего существования в криптосистеме. На предоперационной стадии ключ еще не доступен для штатного использования в криптосистеме. Находясь в операционной стадии жизненного цикла, ключ доступен пользователям криптосистемы и применяется ими в штатном режиме. На постоперационной стадии ключ более не используется в штатном режиме, но доступ к нему возможен в особом режиме для специальных целей. На стадии выхода из эксплуатации ключ более недоступен, а все записи, содержащие значение ключа, удалены из криптосистемы.

Внутри перечисленных общих стадий жизненного цикла можно более точно выделить различные состояния, или фазы, жизненного цикла, в которых пребывает ключ, а также условия переходов между ними (рис. 4.1).

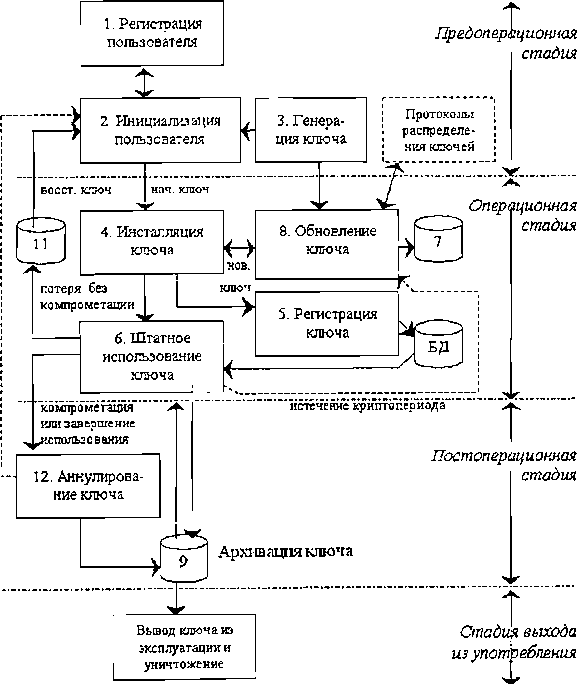
1. Регистрация пользователя: субъект становится авторизованным пользователем криптосистемы, приобретает или создает безопасным одноразовым способом начальный ключевой материал (пароли, персональные коды и др.).
2. Инициализация пользователя: субъект криптосистемы инициализирует свои криптографические приложения, например, производит инсталляцию программного и аппаратного обеспечения, включая инсталляцию на него начального ключевого материала, полученного во время регистрации.
3. Генерация ключа: производится таким образом, чтобы гарантировать необходимые свойства для приложения или алгоритма и случайность (в смысле возможности предсказания его противником с пренебрежимо малой вероятностью). Субъект может генерировать свои собственные ключи или приобретать ключи от доверенного компонента криптосистемы.
4. Инсталляция ключа: ключевой материал инсталлируется для функционального использования в программном или аппаратном обеспечении субъекта, включая ручной ввод пароля или персонального кода, запись на магнитный диск, в постоянную память, микроэлектронную схему или на другие носители. Начальный ключевой материал может служить для установления сеанса с доверенным компонентом криптосистемы, во время которого в реальном масштабе времени согласуются рабочие ключи. Во время последовательных обновлений новый ключевой материал заменяет используемый.

Рис. 4.1. Жизненный цикл криптографических ключей

1. Регистрация ключа: одновременно с инсталляцией ключа ключевой материал может быть публично записан как ассоциированный с уникальным именем субъекта системы. Для открытых ключей регистрация может выполняться специально выделенной третьей стороной, при посредстве которой они становятся доступными для остальных субъектов через открытые директории или другие средства.
2. Штатное использование ключа: при нормальных обстоятельствах это состояние продолжается, пока не истечет период, предусмотренный регламентом системы (так называемый криптопериод ключа), но он может быть разделен, например, для пар секретного и открытого ключей шифрования (когда открытый ключ более не является действительным для шифрования, а секретный ключ остается в нормальном использовании для расшифрования). Цель жизненного цикла - содействовать операционной доступности ключевого материала для стандартных криптографических целей. Иными словами, эта фаза жизненного цикла является самой основной, центральной, ради которой реализуются все остальные фазы, да и сама инфраструктура криптосистемы.
3. Резервирование ключа: копирование ключевого материала на независимом, безопасном носителе обеспечивает источник данных для восстановления ключа. Резервирование подразумевает кратковременное хранение ключа во время операционного использования.
4. Обновление ключа: по истечении периода, предусмотренного регламентом, операционный ключевой материал заменяется на новый. Это может включать процедуры генерации ключа, наследования ключа, выполнение протоколов распределения ключей. Для открытых ключей обновление и регистрация новых ключей обычно включает безопасные коммуникационные протоколы с доверенной третьей стороной.
5. Архивация ключа: ключевой материал, более не используемый в штатном режиме, может быть заархивирован, чтобы обеспечить источник восстановления ключа при специальных обстоятельствах (например, в случае возникновения конфликтов о принадлежности цифровой подписи).
6. Вывод из эксплуатации и уничтожение: когда более нет необходимости поддерживать ассоциацию ключа с субъектом, ключ выводится из эксплуатации, т. е. удаляется из всех публичных записей и все копии ключа уничтожаются. В случае секретных ключей должны быть безопасно стерты все «следы» ключа. Это действие является обратным к регистрации ключа (фаза № 5).
7. Восстановление ключа: если ключевой материал потерян, но при этом не случилось компрометации (сбой оборудования, забыт пароль), должно быть возможно восстановить ключевой материал с безопасной резервной копии.
8. Аннулирование ключа: может быть необходимо удалить ключи из операционного использования до истечения предполагаемого срока по различным причинам, включая компрометацию ключей или выбытие владельца ключа из системы.

Изображенный на рис. 4.1 жизненный цикл ключа более соответствует асимметричным криптосистемам. В симметричных он, как правило, проще (например, сеансовые ключи не регистрируются, не резервируются, не восстанавливаются, не архивируются). Самой сложной для реализации и самой потенциально опасной является фаза распространения ключей, включающая транспортировку ключей между участниками криптосистемы.

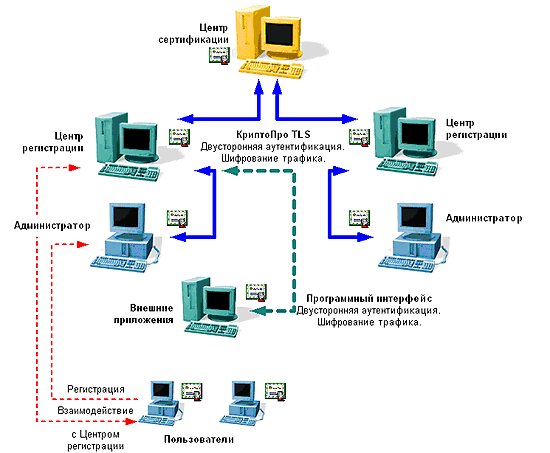
В сложной криптосистеме участники - абоненты криптосистемы- могут не иметь изначально криптографических ключей для связи друг с другом. Более того, в системе с большим числом абонентов они могут даже не знать друг друга, или число участников системы вообще может быть неопределенным или меняющимся. В связи с этим необходимо предусмотреть способы координации действий участников по управлению своими криптографическими ключами, т. е. ввести управление ключами в масштабах всей системы в целом. Для организованного управления ключами должна поддерживаться какая-либо модель управления ключами. В криптосистеме может быть реализована одна из двух моделей управления ключами: децентрализованное либо централизованное (трехстороннее) управление ключами.

Централизованное (трехстороннее) управление ключами предполагает наличие в системе, помимо «рядовых» абонентов, специально выделенного участника - «третьей стороны». Т. Она выполняет функции центра распределения ключей (key distribution center - KDC) либо центра трансляции ключей (key translation center -КТС).

Mетод сертификации открытых ключей применяется в криптосистемах, включающих большое число участников (рис. 4.2). Среди участников криптосистемы выделяется один, специальный, которому доверяют все остальные. Он получает название удостоверяющий центр, или центр сертификации ключей, или агентство сертификации (Certification Authority - СА). Его функции может выполнять, например, администратор системы, оснащенный соответствующим аппаратным и программным обеспечением (сервер регистрации и сертификации ключей). Все остальные участники являются обычными, «рядовыми» абонентами криптосистемы.

При введении в систему каждого из этих участников он должен пройти процедуру регистрации в криптосистеме (что соответствует первой фазе жизненного цикла его криптографического ключа). Для этого он контактирует с удостоверяющим центром, чтобы зарегистрировать свой открытый ключ и получить от него так называемый *сертификат* своего открытого ключа. Удостоверяющий центр должен проверить представленные ему учетные данные, а также (что очень важно!) знание секретного ключа, соответствующего представленному для регистрации открытому ключу. Решить эту задачу можно различными способами: в самом простом случае удостоверяющий центр может попросить пользователя А зашифровать на своем секретном ключе текст заданного формата и проверить правильность его расшифрования при помощи представленного открытого ключа, а можно воспользоваться протоколом доказательства знания с нулевым разглашением знания.

Сертификат открытого ключа - специальная структура данных, состоящая из полей данных и поля подписи. Поле данных содержит как минимум какие-либо признаки абонента (идентификатор, атрибуты) и его открытый ключ. Поле подписи - это цифровая подпись удостоверяющего центра под полем данных, логически связывающая признаки абонента с его открытым ключом.

Рис. 4.2. Процессы получения и использования сертификатов участниками криптосистемы

Все абоненты, заинтересованные в связи с абонентом A, получают впоследствии его сертификат либо путем обмена с абонентом A, либо извлекая его из открытого общедоступного справочника, который заводится в криптосистеме. Сертификат, таким образом, является средством для хранения, распространения и передачи через небезопасные каналы связи открытых ключей без опасения их не обнаружимого изменения.

В идентификационном сертификате обязательно присутствует идентификатор субъекта - владельца ключа, по которому можно однозначно установить его личность. Основным стандартом по идентификационным сертификатам является стандарт Международного телекоммуникационного союза ПU Х.509. В соответствии со стандартом Х.509 сертификат имеет следующий формат (рис. 2.3).

Сертификат состоит из двух полей: поля данных и поля подписи. Поле данных имеет формат, описанный в стандарте. Поле подписи содержит цифровую подпись удостоверяющего центра под полем данных.

Удостоверяющий центр (центр сертификации открытых ключей) - это специально выделенный участник криптосистемы, которому доверяют все остальные участники («центр доверия»).

Рис. 4.3. Формат сертификата открытого ключа по стандарту ITU Х.509

Подпись центра сертификации открытых ключей служит гарантией подлинности ключей и он выполняет следующие функции:

1. сбор сведений об участниках системы, необходимых для сертификации: имя, почтовый адрес, права доступа, должность, номер кредитной карты и т. п. (зависит от конкретного приложения);
2. генерация и рассылка (либо помещение в общедоступное хранилище) сертификатов открытых ключей;
3. уничтожение сертификатов с истекшим сроком годности;
4. обновление сертификатов;
5. аннулирование сертификатов.