Управление криптографическими ключами в системе WAY4™

Содержание

Введение

В документе описаны процедуры управления криптографическими ключами в системе WAY4™.

Глава 1. Основные принципы управления ключами

Процедуры управления ключами, такие как формирование, передача, хранение, аннулирование и удаление, должны выполняться в соответствии с нижеуказанными требованиями.

Формирование ключей

Секретные ключи должны создаваться с помощью процедур или процессов, которые полностью гарантируют невозможность прогнозирования значений генерируемых секретных ключей, а также определения того, что формирование некоего ключа более вероятно, чем формирование других ключей. Поэтому в процессе генерации секретных ключей используется Hardware Security Module (HSM), который формирует секретные ключи или их компоненты случайным образом.

Допускается только генерация криптоустойчивых ключей. Секретные ключи для симметричных криптографических алгоритмов, например, 3DES, AES и т.д., должны состоять как минимум из 112 непредсказуемых битов.

Формирование секретных ключей необходимо выполнять в присутствии как минимум двух уполномоченных сотрудников службы информационной безопасности. Они обязаны убедиться в том, что раскрытие незашифрованных компонентов ключа во время передачи его из устройства генерации ключей (HSM) в устройство-получатель секретного ключа или его компонента (принтер), является невозможным.

Компоненты ключей должны быть распечатаны внутри PIN-конверта либо запечатаны немедленно после печати таким образом, чтобы доступ к каждому компоненту имело только уполномоченное лицо и чтобы любые манипуляции с конвертом могли быть легко обнаружены.

Сотрудник службы информационной безопасности, имеющий доступ к одному из компонентов ключа или к его носителю, не должен иметь доступа к любому другому компоненту данного ключа. Сотрудник службы безопасности должен полностью осознавать ответственность за неразглашение информации о компоненте ключа, а также должен подписать форму, содержащую информацию об этой ответственности. Данная форма может, например, содержать следующую информацию:

- Фамилия имя и отчество сотрудника службы информационной безопасности.
- Идентификационный номер и тип ключа.
- Дата формирования ключа (ММ. ДД. ГГ).
- Дата окончания срока действия ключа (ММ. ДД. ГГ).
- Незашифрованная компонента ключа.
- Контрольная величина (сумма) ключа (при наличии).

- Следующий текст: "Я полностью понимаю и беру на себя всю ответственность за хранение информации о компонентах ключа, включая (но не ограничиваясь) принятие всех необходимых мер, препятствующих раскрытию информации о компонентах ключа неуполномоченным лицам, а также незамедлительно сообщая о фактах раскрытия информации о ключе или о любых подозрениях".
- Личная подпись сотрудника службы информационной безопасности.

Любые материалы, полученные в процессе печати или записи, которые могут раскрыть компонент ключа, должны быть уничтожены, прежде чем к ним может получить доступ неуполномоченное лицо.

Компонентами секретного ключа для алгоритма 3DES должны быть как минимум два значения двойной длины. Процесс сбора ключа из компонентов должен исключать возможность определения любого "активного" бита ключа при отсутствии хотя бы одного из его компонентов.

Криптографический ключ создается автоматическим сбором всех введенных компонентов ключа внутри криптографического устройства HSM. Например, для алгоритма 3DES компоненты, состоящие из 32 (или 48) шестнадцатеричных символов, должны собираться с помощью побитовой операции "исключающее ИЛИ" (XOR) для создания уникального ключа. Следует иметь в виду, что конкатенированные значения не удовлетворяют этому критерию.

Каждый состоящий из 32 (48) шестнадцатеричных символов компонент, а также собранный ключ должен иметь контрольную величину, рассчитанную в соответствии с процедурами, определенными для данного алгоритма шифрования. Например, для алгоритма 3DES контрольная величина рассчитывается с использованием всех 128 (192) битов с помощью операции Encrypt, Decrypt, Encrypt на блоке нулевого бита, где пять младших байтов полученного значения отбрасываются, а три старших байта являются контрольной величиной.

Передача ключей

Допускаются только следующие методы передачи секретных ключей:

- Путем физической передачи отдельных компонентов полной длины (в виде распечатки, на магнитных носителях или в электронном устройстве) посредством безопасных каналов связи. Этот метод используется для передачи мастер-ключей, т.е. ключей, используемых для шифрования других ключей.
- Путем передачи ключей в зашифрованном виде.

Хранение ключей

Хранение ключей в открытом виде разрешено только в аппаратном модуле безопасности. При необходимости хранения компонентов ключа следует обеспечить их безопасное хранение в минимально возможном

количестве хранилищ. Рекомендуется уничтожать открытые компоненты ключей непосредственно после использования.

Необходимо ограничить доступ к ключам и ключевым компонентам, доступ должен быть предоставлен как можно наименьшему числу хранителей.

Аннулирование ключей

Скомпрометированные или подозреваемые в этом ключи должны быть немедленно аннулированы и заменены. Если скомпрометированный ключ является мастер-ключом, все зашифрованные под этим мастер-ключом ключи следует считать скомпрометированными.

У каждого ключа должны быть следующие ограничения по использованию:

- Временные рамки, т.е. ключ должен быть аннулирован и заменен после окончания его срока действия;
- Количество использований, т.е. ключ должен быть аннулирован и заменен, когда текущий счетчик использований равняется или превышает предельное значение.

Для определения временных рамок использования ключа, а также максимального количества использований ключа необходимо выполнить рекомендации, описанные, например в документе "NIST Special Publication 800-57".

Удаление ключей

Все аннулированные или неиспользуемые ключи должны быть удалены безопасным образом для того, чтобы данные ключи или компоненты ключей не могли быть использованы после удаления.

Журнал управления ключами

В случае отсутствия автоматизированных систем ведения журнала управления ключами, каждая операция (формирование, передача, аннулирование или удаление) должна быть вручную зарегистрирована в журнале сотрудника службы информационной безопасности. Необходимо регистрировать следующую информацию:

- Фамилия имя и отчество сотрудника службы информационной безопасности.
- Идентификационный номер и тип безопасного хранилища.
- Дата формирования ключа (ММ. ДД. ГГ).
- Дата окончания срока действия ключа (ММ. ДД. ГГ).
- Действие, совершенное с ключом (формирование, передача, аннулирование или удаление).

- Личная подпись сотрудника службы информационной безопасности.

Глава 2. Управление ключами в безопасном хранилище

Безопасное хранилище используется для защиты данных, таких как interchange-файлы или стоп-листы, посылаемые из системы WAY4 в другие системы. Безопасное хранилище – это программное обеспечение сторонних производителей, например TrueCrypt или PGP Disc, или аппаратное обеспечение, производящее шифровку файловой системы.

Формирование ключей

Формирование ключей необходимо производить согласно документации на соответствующий тип безопасного хранилища в соответствии с основными принципами, изложенными в разделе "Основные принципы управления ключами". Лучший метод формирования ключей – это генерация ключей случайным образом без вывода.

Передача ключей

Для передачи ключей другим сторонам не требуется специальной процедуры. Если используемое безопасное хранилище поддерживает данную опцию, передача ключей должна производиться согласно основным принципам, изложенными в разделе "Основные принципы управления ключами".

Хранение ключей

При наличии действительной необходимости, ключи следует хранить в соответствии с основными принципами, изложенными в разделе "Основные принципы управления ключами".

Аннулирование ключей

Аннулирование и смену ключей следует производить как минимум один раз в год. Для определения времени, когда необходимо аннулирование ключей, используется журнал сотрудника службы информационной безопасности. После аннулирования ключа в журнале сотрудника службы информационной безопасности необходимо сделать соответствующую запись. Самый простой способ аннулирования и замены ключей состоит в повторной инициализации безопасного хранилища после удаления из него всех данных.

После аннулирования ключа необходимо сделать соответствующую запись в журнале сотрудника службы информационной безопасности.

Удаление ключей

При необходимости удаления ключей из используемого безопасного хранилища удаление следует производить согласно основным принципам, изложенным в разделе "Основные принципы управления ключами".

Журнал управления ключами

Данные о ключах обязательно должны записываться и храниться в журнале управления ключами (см. "Журнал управления ключами").

Глава 3. Управление ключами при использовании Oracle Transparent Data Encryption

Механизм Oracle Transparent Data Encryption предназначен для хранения уязвимых данных в зашифрованном виде. Дополнительную информацию см. в документации Oracle.

Формирование ключей

Формирование ключей необходимо производить согласно документации Oracle (см. "Oracle Database Advanced Security Administrator's Guide 10g Release 2 (10.2)", Chapter 3 "Transparent Data Encryption") в соответствии с основными принципами, изложенными в разделе "Основные принципы управления ключами".

Передача ключей

Данная процедура обычно не используется, так как отсутствует необходимость передавать ключи другим сторонам.

Аннулирование ключей

Аннулирование и смену ключей следует производить как минимум один раз в год. Для определения времени, когда необходимо аннулирование ключей, используется журнал сотрудника службы информационной безопасности. После аннулирования ключа в журнале сотрудника службы информационной безопасности необходимо сделать соответствующую запись.

Более подробную информацию см. в документации Oracle.

Удаление ключей

Удаление ключей необходимо выполнять в соответствии с основными принципами, изложенными в разделе "Основные принципы управления ключами".

Журнал управления ключами

Данные о ключах обязательно должны записываться и храниться в журнале управления ключами (см. "Журнал управления ключами").

Глава 4. Управление терминальными ключами

Процедуры управления криптографическими ключами POS-терминалов и банкоматов описаны в документе "Генерация и хранение ключей терминалов".