

Генерация и хранение ключей терминалов

Содержание

ВВЕДЕНИЕ	1
ГЛАВА 1. ОСНОВНЫЕ ПРИНЦИПЫ УПРАВЛЕНИЯ КЛЮЧАМИ	2
Формирование ключей	2
Передача ключей	3
Хранение ключей	3
Аннулирование ключей	3
Удаление ключей	4
ГЛАВА 2. УПРАВЛЕНИЕ ТЕРМИНАЛЬНЫМИ КЛЮЧАМИ	5
Типы используемых ключей терминалов	5
Хранение ключей терминалов	5
Хранение ключей POS-терминалов	5
Хранение ключей банкоматов	7
Формирование ключей	9
Опция "Generate Key & Component Print"	10
Опция "Generate Key & Split Print"	10
Опция "Generate Key (No Printing)"	11
Опция "Generate Device Key under KLK or TMK&LMK"	11
Опция "Generate XOR Component"	11
Опция "Verify KCV"	12
Параметры пайпа "DES Key Management"	12
Шаблоны для печати ключей	13
Переменные шаблонов для печати ключей	14
Печать контрольной суммы ключа (KCV) на PIN-конверте с последней компонентой	15
Распределение ключей	16
Аннулирование ключей	16
Удаление ключей	16



Введение

Данный документ описывает процедуры управления криптографическими ключами в системе WAY4™. Документ предназначен для администраторов системы, обслуживающих банкоматы и POS-терминалы.

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации OpenWay:

- "Модуль эквайринга. Руководство пользователя";
- "Контроллер банкоматов".

В документе используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- названия кнопок экранных форм приводятся в квадратных скобках, например [Approve];
- последовательность выбора пункта в меню пользователя отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: "Database => Change password";
- комбинации клавиш, используемые при работе с DB Manager, приводятся в угловых скобках, например <Ctrl>+<F3>;
- различные переменные значения, например, имена каталогов и файлов, а также, пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS_HOME>;
- предостережения в связи с возможностью совершения неправильных действий отмечены знаком ;
- сообщения, помеченные знаком , содержат информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

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 аппаратный модуль безопасности (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 безопасности. Они обязаны убедиться в том, что раскрытие незашифрованных компонент ключа во время передачи его из аппаратного модуля безопасности (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 безопасности, имеющий доступ к одному из компонентов ключа или к его носителю, не должен иметь доступа к любому другому компоненту данного ключа.

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 устройства HSM. Отдельные 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 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.

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.

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.

Глава 2. Управление терминальными ключами

В данной главе представлено описание основных положений управления терминальными ключами, т.е. работы с ключами, используемыми POS-терминалами и банкоматами для шифрования PIN-кода и расчета MAC-подписи. Все ключи хранятся в базе данных в зашифрованном виде. Ключи шифруются во время генерации в аппаратном модуле безопасности (HSM).

Типы используемых ключей терминалов

В системе WAY4 используются четыре типа терминальных ключей:

- ТМК – Terminal Master Key. Под этим ключом шифруются ключи ТРК и ТАК, записываемые в терминал или передаваемые ему в режиме онлайн.
- ТРК – Terminal PIN Key. Под этим ключом шифруется PIN-блок, который терминал передает системе.
- ТАК – Terminal Authentication Key. Под этим ключом выполняется электронная подпись сообщений (MAC), которые передаются между терминалом и системой.
- Power-Up ТРК – Power-Up Terminal PIN Key. Power-Up ТРК – это значение ключей ТРК и ТАК, которое банкомат активизирует после включения питания. Для системы служит справочной величиной и в процессе проведения транзакций не используется.

Ниже используются следующие обозначения:

- LMK – Local Master Key, локальный мастер-ключ HSM;
- LMK xx-yy – пара локальных мастер-ключей HSM с номерами xx-yy.

Хранение ключей терминалов

Хранение ключей POS-терминалов

Схема хранения ключей POS-терминалов представлена на Рис. 1.

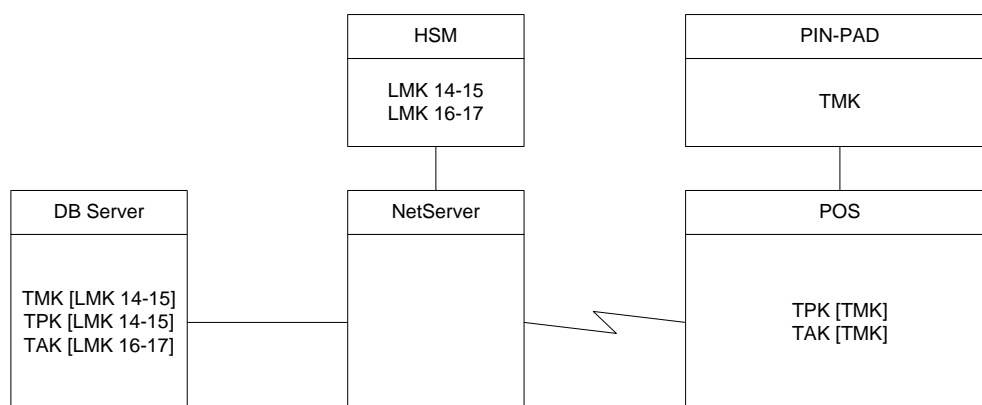


Рис. 1. Типовая схема хранения ключей POS-терминалов

В системе обычно используется следующий механизм хранения и генерации ключей терминалов. Для POS-терминалов следует сгенерировать три ключа: TMK, TPK и TAK. Все три ключа, зашифрованные под соответствующими парами LMK, заносятся в базу данных. В PIN-клавиатуру (PIN-PAD) POS-терминала заносится TMK в чистом виде, а в сам POS-терминал заносятся TPK и TAK, зашифрованные под TMK. Механизм хранения и генерации ключей терминалов может отличаться от стандартного и зависеть от типа POS-терминала. В этом случае следует обратиться к документации используемого POS-терминала.

В ходе проведения транзакции PIN-клавиатура шифрует PIN-блок ключом TPK и подписывает сообщения ключом TAK. Подпись принимаемых сообщений системы PIN-клавиатура проверяет при помощи того же ключа TAK. Ключи TPK и TAK, зашифрованные под TMK, передаются POS-терминалом в PIN-клавиатуру, их расшифровка происходит внутри PIN-клавиатуры и чистые (нешифрованные) ключи POS-терминалу не передаются.

i В случае использования динамической смены ключей POS-терминалов, необходимые настройки системы см. в документе "Настройка динамической смены ключей на POS-терминалах в системе WAY4".

Система обрабатывает PIN-блок, полученный от POS-терминала, при помощи ключа TPK, который хранится в базе данных. При этом PIN-блок и зашифрованный TPK передаются в HSM, который и осуществляет обработку. Вся обработка PIN-блока происходит внутри HSM и чистые (нешифрованные) значения TPK и PIN-блока системе не передаются.

Все зашифрованные под LMK ключи, используемые POS-терминалами, хранятся в таблице PM_KEYS базы данных. Управление ключами осуществляется в форме "Keys For <наименование POS-терминала>" (см. Рис. 2).

The screenshot shows the 'POS Management' window. The top section contains configuration fields for a terminal: Terminal ID (12343652), Service Class (Unique), Business Hours from (09:09) to (05:05), POS Type (Olivetti), Default Curr (EUR), Cut-Off Time (10:10), POS Location (LOCATION2), MAC Status (None), Time Offset (4), Serial Number (SerialNumber2), PBT Status (None), and Device Status (OK). Below these are tabs: Ins, Del, Query, Setup, Operations, Parns, Enh Parns, and Keys. The 'Keys' tab is active, showing a table titled 'Keys for POS Hotels'.

Key Algorithm	Key Type	Key Name	DES Key	Key Check	Used as MK	Storage MK	Serial Number	Is Active
3DES ABA	Terminal Master Key	TMK1	U8787AD83781FF89012345FF7AC7	Yes				Active
3DES ABA	Terminal Authentication Key	TAK1	U8787AD83781FF67890123FF7AC7					Active
3DES ABA	Terminal PIN Key	TPK1	U8787AD83781FF12345678FF7AC7					Active

Below the table are tabs: Ins, Del, Query, Manage, and Key Options.

Рис. 2. Форма для ввода криптографических ключей POS-терминала

Хранение ключей банкоматов

Схема хранения ключей банкоматов представлена на Рис. 3.

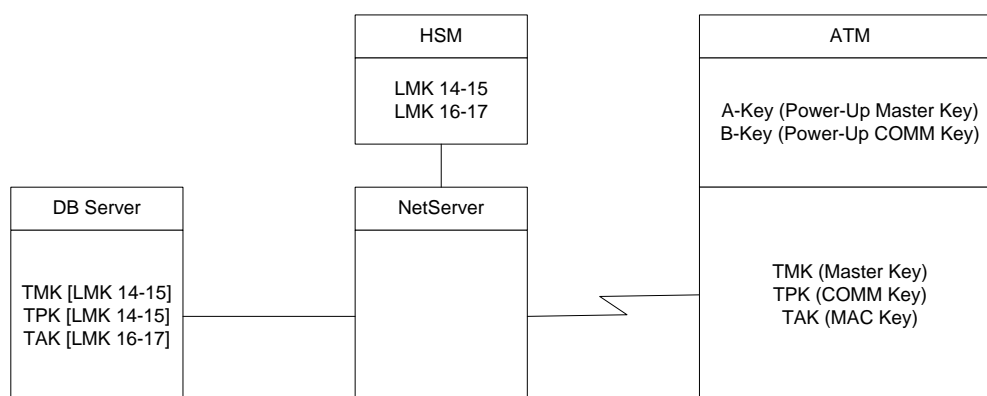


Рис. 3. Типовая схема хранения ключей банкоматов

Для банкоматов необходимо сгенерировать вручную и занести в базу данных лишь один ключ – ТМК. Этот ключ заносится в ячейку банкомата "А-Key". Ключ заносится сотрудниками службы безопасности в чистом (нешифрованном) виде непосредственно с технологической консоли банкомата. При включении банкомата конфигурация банкомата переносит этот ключ в Master Key банкомата, который при работе используется как ТМК.

Каждый сотрудник службы безопасности должен заносить в ячейку банкомата свою компоненту ключа. В зависимости от модели банкомата, количество компонент может быть две или более.

Сотрудник службы безопасности вводит свою полноразмерную компоненту ключа. Так, в случае использования ключа одинарной длины каждый сотрудник службы безопасности введет свою компоненту, состоящую из 16 шестнадцатеричных цифр.

При включении банкомата он присылает системе сообщение "Power-Up Message". При получении этого сообщения система передает банкомату значения ключей ТРК и ТАК, зашифрованные под ТМК. Система также сохраняет переданные ключи ТРК и ТАК в базе данных, зашифровав их в HSM под соответствующими парами LMK. Чистые (нешифрованные) значения ТРК и ТАК при этом системе не передаются.

В ходе проведения транзакции банкомат шифрует PIN-блок ключом ТРК, который хранится в ячейке "COMM-Key", и подписывает сообщения ключом ТАК, который хранится в ячейке "MAC-Key". Подпись принимаемых сообщений системы банкомат проверяет при помощи того же ключа ТАК.

Система обрабатывает полученный от банкомата PIN-блок при помощи ключа ТРК, который хранится в базе данных. При этом PIN-блок и зашифрованный ТРК передаются в HSM, который и осуществляет обработку. Вся обработка PIN-блока происходит внутри HSM и чистые (нешифрованные) значения ТРК и PIN-блока системе не передаются.

Если в ходе взаимодействия банкомата и системы возникает ошибка криптографии (Response Code 88), то система должна передать банкомату новые значения ключей ТРК и ТАК. Ошибка криптографии возникает в том случае, если по какой-то причине произошла рассинхронизация значений ключей ТРК и ТАК в банкомате и системе.

В системе возможно также генерирование для банкомата ключей ТРК и ТАК "по умолчанию". В этом случае значение этих ключей должно совпадать. Чистое (нешифрованное) значение ключа ТРК/ТАК заносится в ячейку банкомата "B-Key". Ключ заносится сотрудниками службы безопасности в чистом (нешифрованном) виде непосредственно с технологической консоли банкомата. При этом значение ключа ТРК/ТАК, зашифрованное под соответствующими парами LMK, следует сохранить в базе данных в полях *ТРК*, *ТАК* и *Power-Up ТРК*. При включении банкомата конфигурация банкомата переносит значение ячейки "B-Key" в ячейки "COMM-Key" и "MAC-Key", которые в дальнейшем используются как ТРК и MAC соответственно.

Ячейка банкомата "VISA-Key" в процессе проведения транзакций не используется.

Все зашифрованные под LMK ключи, используемые банкоматами, хранятся в таблице PM_KEYS базы данных. Управление ключами осуществляется в форме "Keys For <наименование банкомата>" (см. Рис. 4).

- "Generate Device Key under KLK or TMK&LMK" – формирование ключа устройства, зашифрованного под LMK или TMK (см. "Опция "Generate Device Key under KLK or TMK&LMK");
- "Generate XOR Component" – формирование компонент той же длины, что и данный ключ (см. "Опция "Generate XOR Component");
- "Verify KCV" – проверка контрольной суммы ключа (Key Check Value, KCV); см "Опция "Verify KCV".

Перед началом формирования ключа в форму "Keys For <...>" необходимо ввести следующую обязательную информацию:

- тип ключа;
- алгоритм шифрования ключа.



Категорически запрещается использования одного и того же ключа для нескольких терминалов.


Опция "Generate Key & Component Print"

Режим "Generate Key & Component Print" предназначен для формирования компонент той же длины, что и данный ключ. Компоненты ключа будут сформированы внутри HSM в открытой форме и напечатаны на принтере, подключенном к HSM, после чего ключ заданной длины может быть собран из данных компонент посредством выполнения операции "побитовое исключающее ИЛИ" между ними. Для этого HSM собирает открытый ключ из зашифрованных компонентов и шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных. Количество формируемых компонент задается с помощью параметра пайпа "KEY_COMPONENTS" (см. "Параметры пайпа "DES Key Management") или с помощью дополнительного параметра типа ключа "Num of XOR Components" (см. "Шаблоны для печати ключей").

Печать компонент ключа в PIN-конвертах будет осуществляться в соответствии с настроенными шаблонами (см. "Шаблоны для печати ключей"). Ключ в данном режиме печатается покомпонентно: сначала первая компонента ключа, затем вторая компонента ключа и т. д. Все конверты с компонентами ключа должны храниться у сотрудников службы безопасности и быть безопасно уничтожены непосредственно после использования.

Опция "Generate Key & Split Print"

Режим "Generate and Split Print" предназначен для формирования компонент одинарной длины данного ключа. Компоненты ключа будут сформированы в открытой форме, после чего ключ заданной длины может быть собран из данных компонент посредством их конкатенации. Печать компонент будет осуществляться в соответствии с настроенными шаблонами (см. "Шаблоны для печати ключей"). В данном режиме отсутствует возможность задавать параметр "LAST_PRN_TEMPL_FILE" (см. "Параметры пайпа "DES Key Management"), т.е. для всех компонент ключа шаблон печати одинаковый.


 Следует иметь в виду, что использование данного метода разрешено только для устаревших терминалов, которые не поддерживают метод сбора ключей XOR. В режиме "Generate Key & Split Print" часть ключа распечатывается в качестве компонента ключа, что не соответствует базовому принципу управления ключами: принципу безопасной генерации ключей.

Опция "Generate Key (No Printing)"

Режим "Generate Key & Component Print" предназначен для формирования ключа без печати его на принтере, подключенном к HSM. Для этого HSM генерирует случайный ключ определенного типа, после чего шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных.


Опция "Generate Device Key under KLK or TMK&LMK"

Режим "Generate Device Key under KLK or TMK&LMK" служит для формирования ключа устройства, а также шифрования его с помощью ключей LMK и TMK. При этом в форме "Keys for <...>" (см. Рис. 2 или Рис. 4) будут созданы две записи для данного ключа, каждая из которых будет содержать данный ключ, зашифрованный под соответствующим мастер-ключом. Данный режим не предполагает печати компонент ключа.

 Для шифрования ключа под ключом TMK необходимо, чтобы ключ TMK был предварительно сформирован. Для ключа TMK необходимо указать, что он является мастер-ключом, т. е. в поле *Used as MK* формы "Keys for <...>" (см. Рис. 2 или Рис. 4) необходимо выбрать значение "Yes". Кроме того, для шифрования ключа под ключом TMK в данной форме необходимо указать сформированный мастер-ключ, выбрав его в поле *Storage MK*.

Опция "Generate XOR Component"

Режим "Generate XOR Component" предназначен для формирования компонент той же длины, что и данный ключ. Компоненты ключа будут сформированы в открытой форме и напечатаны на принтере, подключенном к HSM, после чего ключ заданной длины может быть собран из данных компонент посредством выполнения операции "побитовое исключающее ИЛИ" между ними. Для этого HSM собирает открытый ключ из зашифрованных компонентов и шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных. Количество формируемых компонент задается с помощью параметра "KEY_COMPONENTS" (см. "Параметры пайпа "DES Key Management") или с помощью дополнительного параметра типа ключа "Num of XOR Components" (см. "Шаблоны для печати ключей"). Сформированный ключ, а также контрольная сумма ключа (KCV) будут занесены соответственно в поля *DES Key* и *DES Key Check* формы "Keys for <...>" (см. Рис. 2 или Рис. 4) после того, как будет сформирована последняя компонента ключа (см. "Шаблоны для печати ключей").

 Следует иметь в виду, что при каждом вызове процедуры происходит формирование только одной компоненты ключа. Сборка компонент ключа будет осуществляться после формирования и печати последней компоненты ключа, количество которых определено параметром "KEY_COMPONENTS".

Печать компонент осуществляется в соответствии с настроенными шаблонами (см. "Шаблоны для печати ключей"). Ключ в данном режиме печатается покомпонентно: сначала первая компонента ключа, затем вторая компонента ключа и т. д. Все конверты с компонентами ключа должны храниться у сотрудников службы безопасности и быть безопасно уничтожены непосредственно после использования.

Опция "Verify KCV"

Режим "Verify KCV" предназначен для проверки контрольной суммы сформированного ключа (Key Check Value, KCV).

В случае если значение KCV, содержащееся в поле *Key Check* формы "Keys for <...>" (см. Рис. 2 или Рис. 4), отличается от рассчитанного с помощью HSM, на экране будет представлено окно с сообщением об ошибке "Invalid Key Check Value <значение> for Key <значение ключа>".

Параметры пайпа "DES Key Management"

Для пайпа "DES Key Management" можно указать следующие параметры:

- "COMM_PARAMS" – предназначен для указания параметров сетевого соединения с аппаратным модулем безопасности (HSM) по протоколу TCP/IP;
- "PRN_TEMPL_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта компоненты ключа (см. "Шаблоны для печати ключей");
- "LAST_PRN_TEMPL_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта последней компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component");
- "KCV_TEMPL_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта контрольной суммы ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component" после того, как будет сформирована последняя компонента). Если параметр принимает значение "NONE", то контрольная сумма ключа не печатается;
- "KEY_COMPONENTS" – с помощью данного параметра указывается количество компонент ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component"). Возможные значения – "2" или "3" (значение по умолчанию – "3").

Шаблоны для печати ключей

Для печати компонент ключей на PIN-конвертах необходимо настроить соответствующие шаблоны. Настройка шаблонов для печати ключей осуществляется одним из следующих способов:

- В форме "PM Key Type Options" (Full → Configuration Setup → Merchant Device Setup → Device Key Type Options) следует выбрать тип ключа, нажать на кнопку [Options] и в открывшейся форме "Options for <...>" (см. Рис. 6) определить шаблоны для печати.

Name	Code	Owner Type
Terminal Encryption Key	TEK	Device
Terminal Master Key	TMK	Device
Terminal Offline PIN Key	TOPK	Device

Key Type	Key Algorithm	Option Code	Option Value
Terminal Master Key	3DES ABA	Num of XOR Components	3
Terminal Master Key	3DES ABA	KCV Print Template	Check Value : {{KCV}}-
Terminal Master Key	3DES ABA	XOR Component Final Print Template	-Clear DES Key Component {{COMPONENT_NUM}}, Key {{KEY_NAME}},
Terminal Master Key	3DES ABA	XOR Component Print Template	-Clear DES Key Component {{COMPONENT_NUM}}, Key {{KEY_NAME}},
Terminal Master Key	3DES ABA	Split Component Print Template	-Key part 1, Key {{KEY_NAME}}, Type {{KEY_TYPE}} Key Serial# {{KEY_SER

Рис. 6. Задание шаблонов для печати ключей

В данной форме необходимо выбрать алгоритм шифрования ключа данного типа (поле *Key Algorithm*), дополнительный параметр типа ключа (поле *Option Code*), а также значение дополнительного параметра (поле *Option Value*). При этом для шаблонов печати ключей используются следующие дополнительные параметры:

- "Num of XOR Components" – количество компонент ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component"). Возможные значения – "2" или "3".
- "XOR Component Print Template" – шаблон для печати PIN-конверта компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component").
- "XOR Component Final Print Template" – шаблон для печати PIN-конверта последней компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component").
- "KCV Print Template" – шаблон для печати PIN-конверта контрольной суммы ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component" после того, как будет сформирована последняя компонента).

- "Split Component Print Template" – шаблон для печати компонент ключа одинарной длины (используется только для режима "Generate and Split Print").
- Шаблон для печати необходимо сохранить в файле с расширением "*.txt".

Переменные шаблонов для печати ключей и примеры шаблонов представлены в разделе "Переменные шаблонов для печати ключей".

В процессе формирования ключей поиск шаблона для печати осуществляется следующим образом:

- Сначала осуществляется поиск шаблона, настроенного в форме "Options for <...>" (см. Рис. 6).
- Если в форме "Options for <...>" не задан шаблон печати ключей, проверяется наличие параметров "PRN_TEMPL_FILE", "LAST_PRN_TEMPL_FILE", "KCV_TEMPL_FILE" и "KEY_COMPONENTS" пайпа "DES Key Management".
- Если в форме "Options for <...>" не задан шаблон и не заданы параметры пайпа, на экране будет представлено окно "Choose print template file", в котором следует выбрать созданный вручную файл шаблона для печати ключей.

Переменные шаблонов для печати ключей

В шаблонах используются следующие переменные:

- "COMPONENT_NUM" – количество печатаемых компонент ключа;
- "KEY_NAME" – наименование ключа;
- "KEY_SERIAL" – серийный номер ключа (по умолчанию не используется для ключей устройств); поле может использоваться для хранения дополнительной идентификационной информации о ключе;
- "KEY_TYPE" – тип ключа;
- "KCV" – контрольная сумма ключа;
- "KEY_OWNER_TYPE" – тип владельца ключа;
- "KEY_OWNER_ID" – идентификационный номер владельца ключа;
- "DEVICE_BANK" – наименование банка, которому принадлежит терминал;
- "DEVICE_LOCATION" – адрес терминала;
- "DEVICE_CITY" – город, в котором расположен терминал.

Кроме того, в шаблонах могут использоваться стандартные поля HSM (см. документацию HSM).

Пример шаблона:

```
-  
Clear 3-DES Key Component [{COMPONENT_NUM}], Key [{KEY_NAME}], Type  
[{KEY_TYPE}]
```



```
Key Serial# [{KEY_SERIAL}]

Key Owner [{KEY_OWNER_TYPE}] , ID [{KEY_OWNER_ID}]

Bank [{DEVICE_BANK}] Device City [{DEVICE_CITY}] Device Location
[{DEVICE_LOCATION}]

Component : [{^P}]
-
```

Печать контрольной суммы ключа (KCV) на PIN-конверте с последней компонентой

Для печати контрольной суммы ключа (KCV) на PIN-конверте с последней компонентой ключа следует отредактировать соответствующие шаблоны. При этом необходимо, чтобы содержимое двух шаблонов могло быть напечатано на одном PIN-конверте.

Для этого в шаблоне для печати PIN-конверта последней компоненты ключа нужно оставить все переменные до "KCV" (не включая переменную "KCV"), а в шаблон для печати контрольной суммы ключа поместить переменную "KCV" и финальные отступы.

Таким образом, шаблон для печати последней компоненты ключа не должен содержать в конце указания перевода формы (FORM FEED) или группы переводов строк:

```
-
Clear DES Key Component [{COMPONENT_NUM}], Key [{KEY_NAME}], Type
[{KEY_TYPE}]

Key Serial# [{KEY_SERIAL}]

Key Owner [{KEY_OWNER_TYPE}] , ID [{KEY_OWNER_ID}]

Bank [{DEVICE_BANK}] Device City [{DEVICE_CITY}] Device Location
[{DEVICE_LOCATION}]

Component : [{^P}]
```

Шаблон для печати контрольной суммы ключа будет иметь следующий вид:

```
Check Value : [{KCV}]
-
```

Таким образом, после выполненных изменений в шаблонах контрольная сумма ключа (KCV) будет напечатана на PIN-конверте вместе с последней компонентой ключа.

Распределение ключей

Распределение ключей производится следующим образом:

- Открытые компоненты ключей – в запечатанных конвертах. Каждый конверт должен иметь как минимум следующие атрибуты:
 - Идентификационный номер терминала;
 - Тип ключа;
- Зашифрованные ключи в конфигурации терминала – посредством стороннего программного обеспечения для управления терминалами;
- Зашифрованные ключи – с использованием процедуры динамической смены ключей, поставляемой вместе с системой WAY4.

Аннулирование ключей

Аннулирование ключей требуется выполнять в следующих случаях:

- Ключ скомпрометирован или подозревается в том, что он скомпрометирован (чрезвычайная ситуация);
- Истек срок действия ключа (нормальная ситуация);
- Счетчик количества использований ключа превышает максимально разрешенное количество использований (нормальная ситуация).

В любой из данных ситуаций ключ должен быть немедленно аннулирован. Если ключ, аннулируемый в чрезвычайной ситуации, является мастер-ключом, все ключи, зашифрованные с использованием данного мастер-ключа, также должны быть в срочном порядке аннулированы. Процедура аннулирования состоит из следующих действий:

- Сгенерировать новый ключ того же типа;
- Распределить ключ, используя стандартный для данного терминала метод;
- Удалить аннулируемый ключ.

В случае опции динамической смены ключей аннулирование ключей производится автоматически. Для аннулирования ключа в чрезвычайной ситуации следует непосредственно в форме установить его срок действия равным текущей дате или установить счетчик использования ключа в максимальное разрешенное значение.

Удаление ключей

Все неиспользуемые данные, относящиеся к ключам, должны быть уничтожены. Открытые компоненты ключей должны быть безопасным образом уничтожены; зашифрованные ключи должны быть удалены из базы данных через форму "Keys For <...>".