GS LABS
GS GROUP

Публичный - L0

ПАК «Криптокипер»

Руководство по установке ПО

Индекс	CryptoKeeper-IG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация

Документ предназначен для сотрудников отдела мониторинга и инсталляции, а также для других технических специалистов, в обязанности которых входит обновление программного обеспечения ПАК "Криптокипер". Перед применением настоящего Руководства настоятельно рекомендуется изучить документ "ПАК "Криптокипер". Руководство администратора".

2. Термины и сокращения

Термин	Определение
Активный набор IPkeys	Набор ipkeys, который используется на текущий момент в командах рабочего протокола.
Набор IPkeys	Набор промежуточных ключей, участвующих в шифровании данных с помощью Устройства. IPKeys используются для привязки к провайдерам (part type) чипа. IPkeys загружаются и хранятся на Устройстве в зашифрованном виде (с помощью корневых ключей из OTP чипа GS1.
Набор ключей по умолчанию	Файл (или несколько файлов) с наборами ключей (IPkeys), добавленные в прошивки в read-only подписанный/шифрованный раздел. Наборы по умолчанию являются нередактируемыми, и могут быть обновлены только вместе с прошивкой.
Оператор ТВ (TV Provider)	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
ECM	Сообщение CAS, содержащее служебную информацию и зашифрованные ключи (CW), дескремблирующие транспортный поток.
ECMG	Функциональный компонент CAS в архитектуре DVB-Simulcrypt, генерирующий ECM сообщения, добавляемые в транспортный поток.
EMM	Сообщение CAS, содержащее служебные данные, информацию о правах доступа и специальные команды (активация карты, изменение подписки, обновление операционного ключа и другие).
EMMG	Функциональный компонент CAS в архитектуре DVB-Simulcrypt, генерирующий EMM сообщения, добавляемые в транспортный поток.
OTM	Способ обновления ПО через подключаемый носитель информации. Способ обновления ПО через сеть, также используемый на Устройстве, является частным случаем обновления OTM, при этом используется аналогичный файл обновления, помещаемый на удаленной управляющей рабочей станции.
CryptoKeeper	(ПАК "Криптокипер"). Используется для хранения и обработки секретных данных и ключей шифрования в продуктах "Программный комплекс "Система условного доступа DREGUARD" и "Система управления цифровыми правами DREPLUS".

Сокращение	Расшифровка
API	Application Programming Interface
BL	Bootloader
CAS	Conditional Access System
DRM	Digital Right Management

MW	Middleware
OTP	One-Time Programmable
WDT	Watchdog Timer

3. Введение

ПАК "Криптокипер" (далее - устройство или CryptoKeeper) представляет собой программно-аппаратное решение на базе чипа GS1, используемое для хранения и обработки секретных данных и ключей шифрования в системах CAS/DRM. Первоначально, ПО устройства устанавливается в процессе производстве устройства при персонализации чипа (описание этого процесса относится к процессу персонализации чипов и выходит за рамки данного документа). В процессе эксплуатации устройства, на него может устанавливаться обновленная версия ПО. ПО устройства может обновляться администратором устройства. Способы и процедуры обновления описаны в следующих разделах.

3.1. Требования к квалификации администратора Cryptokeeper

Администратор устройства должен обладать навыками:

- Работа со скриптами Python.
- Настройка сетевых подключений.

3.2. Системные требования

Рабочая станция, с которой будет осуществляться удаленное управление Устройством, должна обладать следующими характеристиками:

- Наличие сетевого интерфейса Ethernet.
- Операционная система: *Microsoft Windows* или *Linux* (для управления с помощью скрипта).
- Установленный *Python 3.7* или выше.
- У становленная библиотека *requests* для *P ython* . Версия - не ниже 2.25.1.

> ⓘ Установить библиотеку можно, выполнив команду: pip install requests

4. Обновление ПО устройства

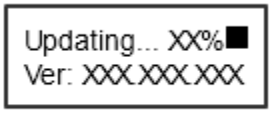
Обновление ПО Устройства возможно двумя способами:

1. Основной способ - через сетевой интерфейс.
2. Вспомогательный способ - через интерфейс USB, расположенный внутри корпуса Устройства.

⚠ В течение процесса обновления не рекомендуется без крайней необходимости посылать на Устройство запросы, связанные со считыванием данных (прочие запросы во время обновления запрещены, и будут возвращать ошибку), в частности, запрос информации о доступных наборах IP-ключей. Если в процессе обновления на Устройство был передан запрос доступных наборов IP-ключей (`--keysets`, см. документ "ПАК "Криптокипер". Руководство администратора"), выполнение запроса может через несколько секунд завершиться ошибкой, а индикатор хода обновления перестанет менять показания. Такая ситуация не является аварийной, процесс обновления будет продолжен, и через некоторое время (не более 1 мин.) ход обновления снова будет отображаться.

4.1. Обновление через сетевой интерфейс

1. Поместить файл с обновлением на рабочую станцию, с которой осуществляется управление Устройством (см. документ "ПАК "Криптокипер". Руководство администратора").
2. Под логином "configure" вызвать пользовательский скрипт с опцией --update, в качестве параметра указать путь к файлу с обновлением (если файл скрипта и файл с обновлением находятся в одной папке, указывается только имя файла).
3. В процессе обновления скрипт возвращает статус и процент обновления. Статус обновления также можно узнать с помощью команды `--update-status`
4. Процент обновления также отображается на дисплее Устройства в первой строке. Во второй строке показывается номер версии ПО, которая будет установлена на Устройстве. Пример отображения:



5. После успешного окончания обновления, скрипт вернет соответствующую информацию, Устройство автоматически перезагрузится.
6. В случае ошибки обновления, скрипт вернет сообщение об ошибке, на дисплее Устройства будет отображаться код ошибки, светодиодный индикатор на корпусе будет светиться желтым светом.

4.2. Обновление через USB-flash

1. Поместить файл с обновлением на чистый USB-накопитель (FAT32). Имя файла должно быть: ***ck3.upd*** .
2. Открыть корпус Устройства, сняв верхнюю крышку. Внешний вид платы Устройства со снятой верхней крышкой показан на рисунке:

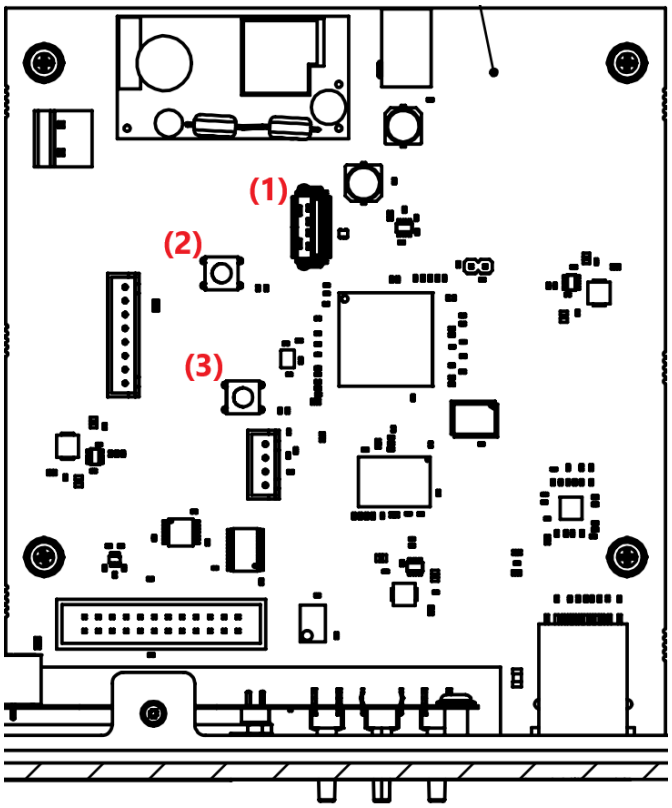
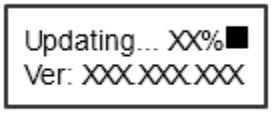


Рис. 4.3. Внешний вид основной платы Устройства со снятой верхней крышкой.

3. Включить Устройство, если оно было выключено.
4. Подсоединить USB-накопитель к USB-порту, расположенному на плате Устройства (поз. 1 на рис. 2.3).
5. Процесс обновления начнется автоматически, на дисплее Устройства в первой строке будет отображаться ход обновления, а во второй строке - номер версии ПО, которая будет установлена на Устройстве. Пример отображения:



6. После успешного окончания обновления, Устройство автоматически перезагрузится.
7. В случае ошибки обновления, на экране статуса будет отображаться код ошибки, светодиодный индикатор будет светиться желтым светом. Коды и описания ошибок обновления приведены в следующем разделе.

> ⚠ В процессе перезагрузки устройства после обновления (статус Rebooting на дисплее) следует отсоединить USB-накопитель. В противном случае, Устройство сделает попытку повторного обновления с подсоединенного накопителя. Т.к. повторное обновление той же версии ПО невозможно, будет отображен код ошибки (9), однако Устройство при этом продолжит нормально функционировать. Если данная ситуация произошла, для сброса ошибки следует отсоединить USB-накопитель, а затем перезагрузить Устройство.

4.3. Описание кодов статусов, возвращаемых при обновлении ПО устройства

Код ошибки	Возвращаемый текст	Описание ошибки
0	ok	Ошибок нет.
1	not initialized	Библиотека обновления не инициализирована.
2	already initialized	В текущем релизе данный код ошибки не используется.
3	invalid magic	В заголовке обновления не обнаружен magic "UPNH" (0x484E5055).
4	not supported	Обнаружена неподдерживаемая версия заголовка (поддерживаются только заголовки версии 2).
5	bad length	Неверная длина заголовка обновления.
6	bad compress	В заголовке указан неподдерживаемый тип сжатия обновления. В текущей версии принимается только несжатое обновление.
7	bad encryption	В заголовке обновления указан неподдерживаемый алгоритм шифрования. В текущей версии допустимы: AES128-CBC или AES256-CBC.
8	bad digest	В заголовке обновления указан неподдерживаемый алгоритм подписи. Поддерживаются: SHA1+RSA или SHA256+RSA
9	no suitable modules	Версия модуля в обновлении должна быть больше версии соответствующего раздела на Устройстве.
10	incorrect CRC	Не сходится CRC16 заголовка обновления.
11	not implemented	В текущем релизе данный код ошибки не используется.
12	digest error	Подпись обновления присутствует, но не сходится.
13	decryption error	В текущем релизе данный код ошибки не используется.
14	uncompress error	В текущем релизе данный код ошибки не используется.
15	erase mtd error	Ошибка при стирании раздела.
16	write mtd error	Ошибка при записи раздела.
17	check mtd error	Ошибка при проверке раздела.
18	finished	Обновление успешно завершено.
19	need more data	Неожиданное окончание данных в файле обновления.
20	not enough memory	Недостаточно оперативной памяти для обработки файла обновления.

21	module type not supported	Нет подходящих для обновления модулей. Поддерживаются типы модулей *linux* и *rootfs*. Ошибка выдается в случае, если испорчен заголовок модуля.
22	read only partition	Попытка обновления раздела, предназначенного только для чтения.
23	invalid partition number	Попытка обновления несуществующего раздела.
24	file too big for partition	Размер обновления превышает размер раздела.
25	corrupted file	Одно из двух событий: • Ошибка открытия или чтения файла с updater-ключами; • Неожиданное окончание данных в файле обновления при том, что файл обновления целиком обработан (ошибка подготовки файла).
26	no partition to erase	Нет модулей для обновления, но произведен запрос на стирание раздела.
27	max modules reached	Файл обновления содержит более 10 модулей.
28	stopped by user	Внешнее (по отношению к библиотеке обновления) прерывание процесса обновления.
29	clear mode forbidden	В заголовке обновления указано, что обновление не зашифровано или не подписано.
30	busy	Попытка запуска еще одного процесса обновления.
31	bad params	Ошибка внутренних данных библиотеки обновления (нулевые указатели).
32	no file	Не используется.
33	general error	Ошибка внутренних функций библиотеки обновления.
34	security version mismatch	Значение защитной версии ПО, указанное в заголовке обновления, меньше, чем в обновляемом устройстве, или больше 128.