GS LABS
GS GROUP

Публичный - L0

ПАК «Криптокипер»

Общее описание

Индекс	CryptoKeeper-GD
Конфиденциальность	Публичный - L0
Ревизия	1.2
Статус	Согласован

Содержание

1. Аннотация

Данный документ содержит общее описание ПАК "Криптокипер", являющегося программно-аппаратным решением (устройством) на базе чипа GS1, используемым для хранения и обработки секретных данных и ключей шифрования в продуктах "Программный комплекс "Система условного доступа DREGUARD" и "Система управления цифровыми правами DREPLUS". Основной акцент сделан на описании назначения устройства, основных возможностей, без технических подробностей. Документ предназначен для широкого круга специалистов, которым необходимо составить общее представление о продукте.

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.
CAS DREGUARD	Программный комплекс "Система условного доступа DREGUARD"
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.

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. Общие сведения. Назначение

ПАК "Криптокипер" (далее - устройство) представляет собой программно-аппаратное решение на базе чипа GS1, используемое для хранения и обработки секретных данных и ключей шифрования в системах CAS/DRM. Под устройством понимается комплекс, включающий:

- чип GS1 с собственным ОЗУ и флеш-памятью (ПЗУ) для хранения ПО (прошивки) и временных данных;
- порты ввода/вывода для обмена данными с внешними системами (CAS/DRM и т.п.), конфигурирования устройства и обновления ПО;
- органы управления и индикации на корпусе.

Использование секретных ключей из хранилища OTP и обработка данных в устройстве основываются на ядре SRISC чипа GS1 и на реализованных в нем мерах защиты от анализа и перехвата данных и ключей. Таким образом, использование устройства в системах CAS/DRM позволяет исключить появление корневых ключей и промежуточных (сессионных) ключей шифрования и подписи для управляющих команд в открытом виде. Шифрование контента и генерация ключа контента в устройстве не выполняется, т.к. для сервисов CAS/DRM используются различные сторонние схемы защиты и скремблеры.

3.1. Внешнее исполнение

В текущей реализации корпус устройства имеет стандартный серверный размер 1U. В одном корпусе размещены 2 полностью независимых устройства.

Далее следует описание для одного устройства, при этом подразумевается, что в каждом корпусе присутствует 2 комплекта соответствующих органов коммутации, индикации и управления.

На задней панели расположен разъем для подключения кабеля питания устройства (220В).

На передней панели расположены:

- Выключатель питания.
- Светодиодный индикатор включения и статуса.
- Двухстрочный текстовый дисплей для отображения основных параметров работы устройства.
- Кнопки для навигации по меню параметров и перезагрузки устройства.
- Разъем RJ-45 - служит для подсоединения устройства к LAN. Через сетевой интерфейс происходит связь устройства с клиентами, а также удаленное управление устройством.

3.2. Основные возможности

Ниже перечислены основные возможности устройства.

- Шифрование данных по алгоритму *M* с ключом *N*. Алгоритм и ключ указываются клиентом.
- Вычисление подписи для данных с использованием алгоритма *M* и ключа *N*. Алгоритм и ключ указываются клиентом.
- Возможность одновременного подключения нескольких клиентов. Максимальное число одновременно подключенных клиентов: 100.
- Возможность управления устройством с удаленной рабочей станции посредством REST API. В текущей версии доступны следующие операции:
    - Получение данных о настройках сетевого подключения.

- Изменение настроек сетевого подключения.
- Просмотр количества и параметров доступных наборов ключей шифрования.
- Добавление, удаление и изменение параметров наборов ключей шифрования.
- Обновление ПО устройства с просмотром данных о прогрессе обновления.
- Просмотр ошибок, возникших в процессе обновления ПО устройства.
- Просмотр сведений о версиях компонентов ПО устройства.
- Смена паролей пользователей устройства.
- Перезагрузка устройства.
- Сброс устройства к заводским настройкам.

- Полномочия по управлению устройством разделены для 3 пользователей. Каждый пользователь имеет изменяемый пароль и фиксированный логин:
  - *configure* - работа с настройками и обновлением устройства.
  - *keyholder* - работа с ключами шифрования.
  - *monitor* - мониторинг текущих параметров.
- Возможность просмотра настроек устройства, возникших ошибок, а также перезагрузки устройства на передней панели корпуса.
- Возможность перезагрузки устройства и сброса к заводским настройкам с использованием кнопок внутри корпуса устройства.

3.3. Безопасность

Ниже перечислены меры, примененные в устройстве для повышения безопасности данных:

- Удаленное управление осуществляется по защищенному протоколу HTTPS.
- Для удаленного управления устройством пользователю требуется знать логин и пароль.
- Файлы с наборами ключей, передаваемые на устройство, снабжены подписью, а значения ключей зашифрованы.
- Набор данных устройства хранится в постоянной памяти в зашифрованном виде.
- Устройство имеет защиту от "отката" версии ПО.

3.4. Взаимодействия

Пример взаимодействий устройства в составе системы CAS DREGUARD приведен на рисунке:

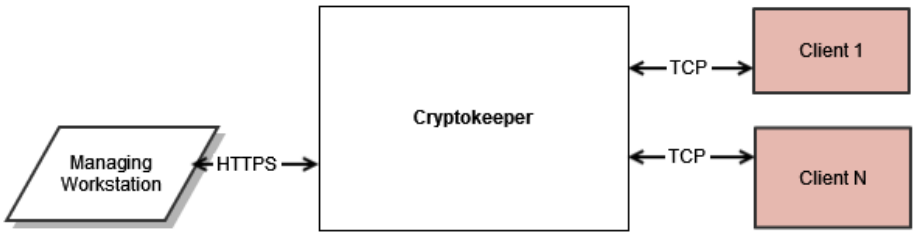

Рис. 3.1. Обобщенная схема взаимодействий ПАК "Криптокипер" с внешними компонентами.

На рисунке показаны:

- **Cryptokeeper** - устройство ПАК "Криптокипер".
- **Managing Workstation** - рабочая станция, с которой осуществляется удаленное управление устройством. Управление может осуществляться с нескольких станций.

- **Client 1 … Client N -** клиенты устройства. В частности, клиентами, использующими устройство, являются компоненты системы CAS DREGUARD:
    - ECMG - отвечает за генерацию сообщений ECM. Использует Устройство для шифрования, либо подписи данных.
    - EMMG - отвечает за генерацию сообщений EMM. Использует Устройство для шифрования, либо подписи данных.

4. Архитектура ПО

Общая схема архитектуры ПО Устройства представлена на рисунке:

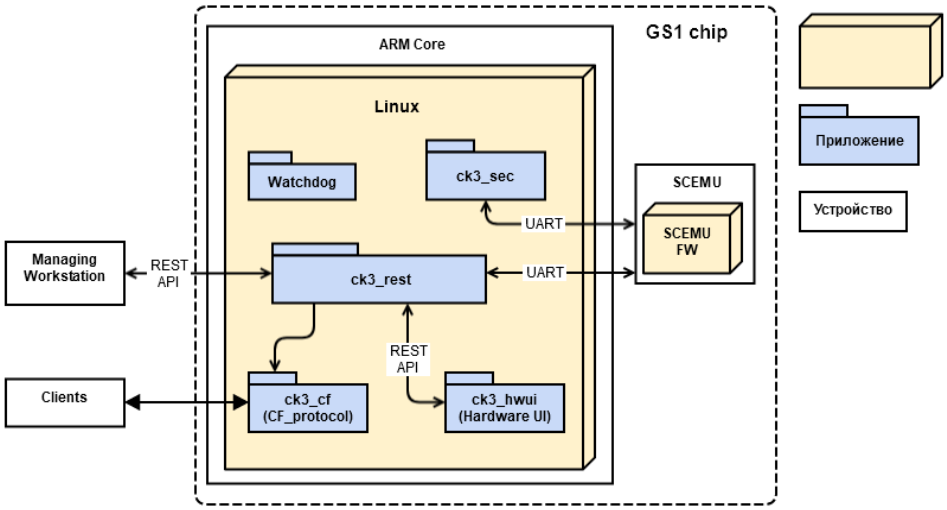

Рис. 4.1. Схема взаимодействия компонентов ПАК "Криптокипер".

Ниже приведено описание основных компонентов ПО устройства, показанных на рис. 4.1.

- **Watchdog**
  Приложение для мониторинга работы остальных компонентов.
- **ck3_sec**
  Приложение, отвечающее за проверку номера защитной версии ПО Устройства, сохраняемой с помощью компонента SCEMU.
- **ck3_rest**
  Приложение, отвечающее за управление Устройством через управляющий протокол, выставление правил для файрвола и обновление ПО.
- **ck3_cf**
  Приложение реализует функциональность рабочего протокола (CF-protocol), через который происходит вся криптографическая работа Устройства.
- **ck3_hwui**
  Приложение обеспечивает управление Устройством на корпусе и плате, а также просмотр информации на двухстрочном дисплее.
- **SCEMU**
  Компонент SCEMU с его ПО (**SCEMU FW**) используется в Устройстве для работы с параметром "защитная версия ПО", служащим для защиты от "отката" прошивки устройства.