АО «Концерн ГРАНИТ»

Россия, 119019, г. Москва, ул. Гоголевский бульвар, д. 31, стр. 2, эт. 2, пом.1
т. +7 495 642 97 42, ф. +7 499 558 15 29
office@granit-concern.ru, granit-concern.ru

QUANTUM SECURE STORAGE

Описание технической архитектуры

Листов 15

2023

Акционерное общество «Концерн ГРАНИТ»
ОКПО 78089277 к/с 30101810400000000225, БИК 044525225
, ОГРН 1055011347093, ИНН/КПП 5003056699/770401001
р/с 40702810738000014569 в ПАО «Сбербанк России»,

АННОТАЦИЯ

Настоящий документ содержит сведения по структуре и зависимостям «Quantum Secure Storage» (далее QSS, Программа), предназначенной для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

Программа предназначена для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных, и представляет собой программный продукт на языке Rust со встроенной библиотекой шифрования, консольными и программными интерфейсами. Криптографическая защита должна соответствовать требованиям ГОСТ: ГОСТ Р 34.13-2015, ГОСТ 34.13-2018, ГОСТ Р 34.12-2015, ГОСТ 34.12-2018, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018 и стандартам: Р 1323565.1.026–2019, Р 50.1.111-2016, Р 50.1.113-2016. Система предназначена для защиты конфиденциальности и целостности информации, не содержащей сведений, составляющих государственную тайну.

2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

В данном разделе под случайными данными подразумеваются данные, сгенерированные физическим датчиком случайных чисел (далее, ФДСЧ) , имеющий сертификат соответствия ФСБ России по классу не ниже 2Б, а под псевдослучайными – данные, сгенерированные генератором Xorshift, инициазированным с помощью случайных данных, сгенерированных ФДСЧ и производящем повторную инициализацию после каждых 32 МиБ сгенерированных данных.

2.1. Постановка задачи и выбор методов решения

Программный комплекс должен обладать набором следующих функциональных характеристик:

1) аутентификацию при установлении административного соединения по паролю и дополнительной случайной информации (с опциональным её хранением на внешнем носителе) с использованием алгоритма выработки ключа из пароля по алгоритму «PBKDF2» в соответствии с «Р 50.1.111-2016»;
2) диверсификацию ключей с использованием алгоритма KDF_GOSTR3411_2012_256 в соответствии «Р 50.1.113-2016»;
3) аутентифицированное шифрование/расшифрование данных (с использованием разделяемой памяти/ через сокеты) в соответствии с «Р 1323565.1.026—2019» (алгоритмом «Кузнечик» в соответствии «ГОСТ 34.12—2018»);
4) формирование и проверку электронной подписи в соответствии с «ГОСТ 34.10-2018» и параметрами эллиптических кривых, определёнными в «Р 1323565.1.024-2019»;
5) формирование общих ключей по алгоритму «VKO» в соответствии с «Р 50.1.113-2016»;
6) вычисление хеш-суммы от блока данных в соответствии с «ГОСТ 34.11-2018»;
7) управление ключевой информацией;

8) хранение ключей в зашифрованном и имитозащищенном виде в долговременном хранилище (диске);
9) стирание из оперативной памяти ключевой информации после окончания её использования путем перезаписи псевдослучайной последовательностью;
10) защиту ключевой информации в оперативной памяти путем ее маскирования;
11) контроль жизненного цикла ключа: запрет техническими средствами на использование ключа для шифрования и формирования цифровой подписи после истечения времени его жизни (не может составлять более 15 месяцев) и заблаговременное уведомление администраторов о необходимости смены ключа.
12) управление администраторами.

Все функциональные характеристики были реализованы в полном объеме.

Функции авторизации клиентской библиотекой не предусмотрены.

Функциональные требования по шифрованию реализованы в соответствии с ГОСТ: ГОСТ Р 34.13-2015, ГОСТ 34.13-2018, ГОСТ Р 34.12-2015, ГОСТ 34.12-2018, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018, и стандартами: Р 1323565.1.026–2019, Р 50.1.111-2016, Р 50.1.113-2016.

Реализовано использование алгоритма Multilinear Galous Mode, описанного в Р 1323565.1.026–2019, в комбинации с шифром Кузнечик, описанного в ГОСТ Р 34.12-2015 и ГОСТ 34.12-2018. При шифровании данных используется вектор инициализации (nonce), сгенерированный на основе псевдослучайного датчика случайных чисел на основе блочного шифра «Кузнечик» в режиме гаммирования, инициализированном с помощью случайных данных, сгенерированных ФДСЧ и производящем повторную инициализацию после каждых 32 МиБ сгенерированных данных.

2.2. Структура и зависимости QSS

Программный комплекс представляет собой программный продукт, реализованный на языке Rust, со встроенной библиотекой, реализующей

криптографические алгоритмы, консольным и программными интерфейсами, опционально использующим в качестве внешней библиотеки решения поставщиков ФДСЧ (например, ПАК «Соболь»).

Структура Программы и используемых внешних решений включает в себя такие элементы, как:

1. qss-server (файл qss) – элемент выступает в роли сервера, отвечающего на команды, посылаемые пользователем;
2. qss-client – элемент представляет собой пользовательский консольный интерфейс для работы с серверной частью;
3. libqss.so – пользовательская библиотека для работы с qss-server через API;
4. qss-admin – элемент представляет собой административный консольный интерфейс для работы с серверной частью;
5. libgostcrypto.so – динамическая библиотека, реализующая криптографические алгоритмы;
6. config.yml – файл с настройками;
7. storage.bin – файл с реестром пользователей, зашифрованными рабочими ключами, счетчиками попыток входа;
8. bin_integrity.streebog512 — файл с эталонными значениями хеш-кодов библиотек и исполняемых файлов являющихся частью СКЗИ;
9. журналы регистрации событий;
10. (опционально) внешние библиотеки:
    a. libsobol.so – используется для получения случайных последовательностей, сгенерированных на ПАК «Соболь»;
    b. libtmdrv.so – используется для получения случайных последовательностей, сгенерированных на СЗИ НСД «Аккорд-АМДЗ»;
    c. иные библиотеки для получения случайных последовательностей.

Структурная схема зависимостей представлена на рисунке 1.

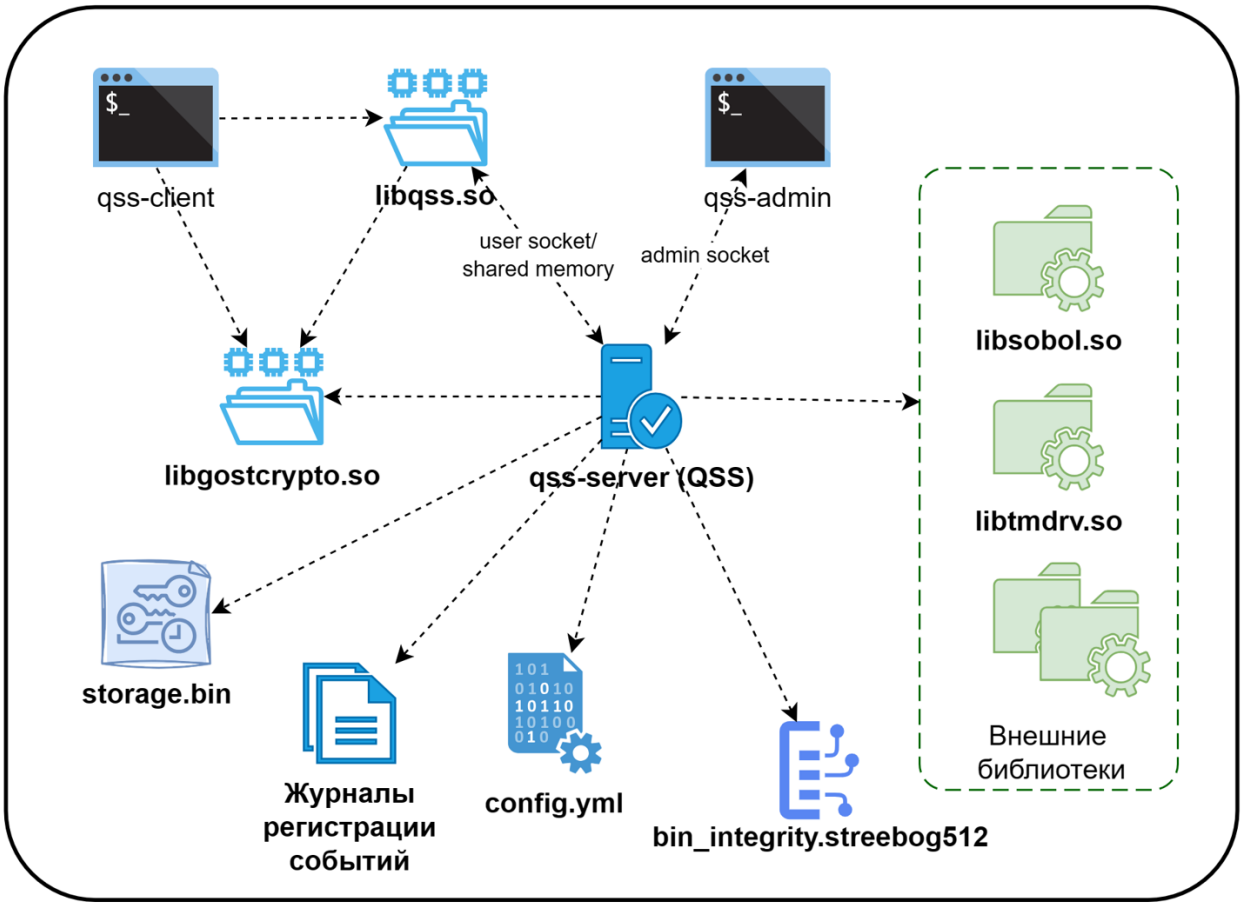

Рисунок 1 - Зависимости QSS

Исходя из рисунка 1 видно, что qss-server (файл qss) и интерфейсы пользователя и администратора (библиотека libqss.so и консольный интерфейс qss-admin) взаимодействуют между собой по клиент-серверной модели посредством двух UNIX сокетов: пользовательского и административного. Кроме того, при шифровании и расшифровании имеется возможность использовать разделяемую память. Настройки для qss-server хранятся в файле config.yml. В качестве элемента, реализующего криптографические алгоритмы, используется библиотека libgostcrypto.so. Кроме вышеперечисленных элементов рисунка qss-server использует storage.bin для хранения рабочей информации о пользователях и рабочих ключах и (опционально) внешние библиотеки (например, libsobol.so, libtmdrv.so) для доступа к физическому датчику случайных чисел (далее ФДСЧ), поставляемые вместе со сторонними решениями, такими как ПАК «Соболь», СЗИ НСД «Аккорд-АМДЗ».

Работа пользователя с Программным комплексом предусмотрена через CLI администратора для административных задач и через API для прямого обращения приложений к криптографическим функциям.

СКЗИ представляет собой готовый продукт. Имеется возможность использовать СКЗИ в качестве встраиваемого решения путем обращения к функциям программного комплекса через библиотеки libqss.so и libgostcrypto.so, минуя qss-client.

Дл8я обеспечения доверенной загрузки совместно с СКЗИ QSS необходимо использовать механизм доверенной загрузки, имеющий сертификат соответствия ФСБ России по классу не ниже 2Б.

Для генерации случайных последовательностей СКЗИ QSS использует ФДСЧ, имеющий сертификат соответствия ФСБ России по классу не ниже 2Б (ФДСЧ из состава механизмов доверенной загрузки, имеющих сертификаты соответствия ФСБ России по классу 2Б и выше).

2.3. Взаимодействие с СУБД «Квант-гибрид»

Система управления базами данных «Квант-гибрид» представляет собой объектно-реляционную систему управления базами данных общего и специального назначения с возможностью расширения функциональности при помощи встраиваемых модулей, применимую для широкого круга разработчиков государственных информационных систем, приложений, а также для корпоративных отделов по цифровой трансформации предприятий крупного и среднего бизнеса.

СУБД «Квант-гибрид» реализована в архитектуре клиент-сервер и представляет собой общесистемное программное обеспечение, обслуживающее запросы клиентов на языке SQL. Приложения пользователя (клиенты создаются сторонними разработчиками), желающее исполнить операции на языке SQL взаимодействуют с СУБД по сетевому протоколу, или при помощи механизмов межпроцессного взаимодействия операционной системы и СУБД. Клиент и сервер

могут находиться как на одном, так и на разных компьютерах, которые должны располагаться в защищенном контуре.

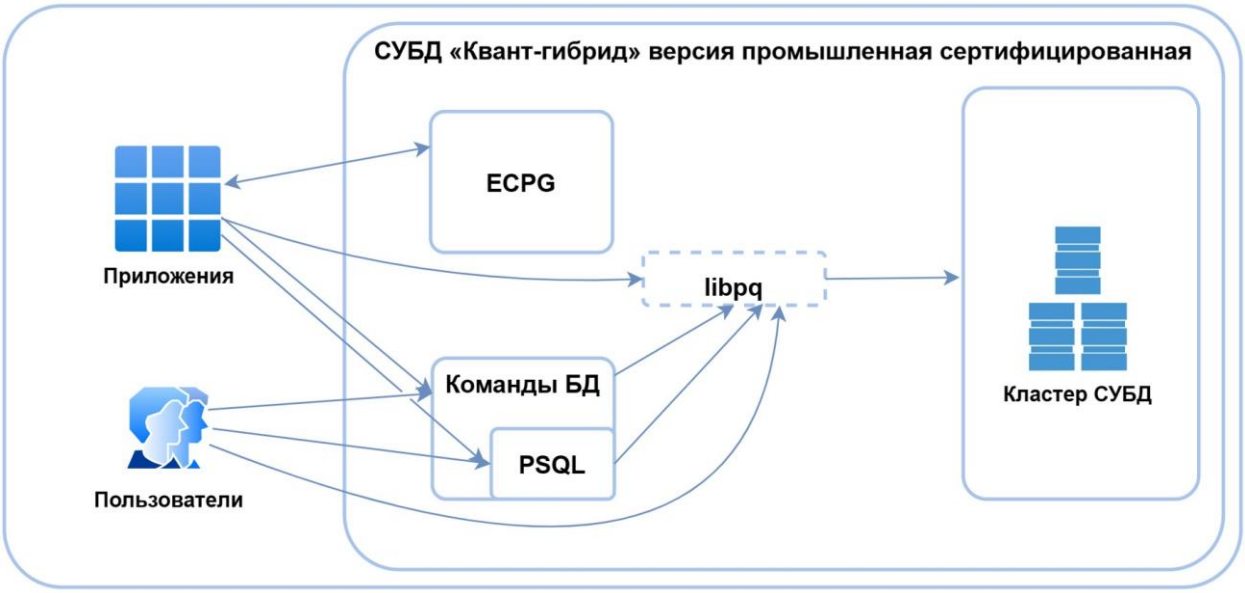

Рисунок 2 - Структурная схема СУБД

При штатном функционировании, компонент кластера СУБД «Квант-гибрид» Хранилище взаимодействует через «библиотеку-обертку» client-qss с библиотеками СКЗИ QSS libqss и libgostcrypto (отражено на рисунке 3). Совместное использование ПО и СКЗИ используется для шифрования и расшифрования информации СУБД.

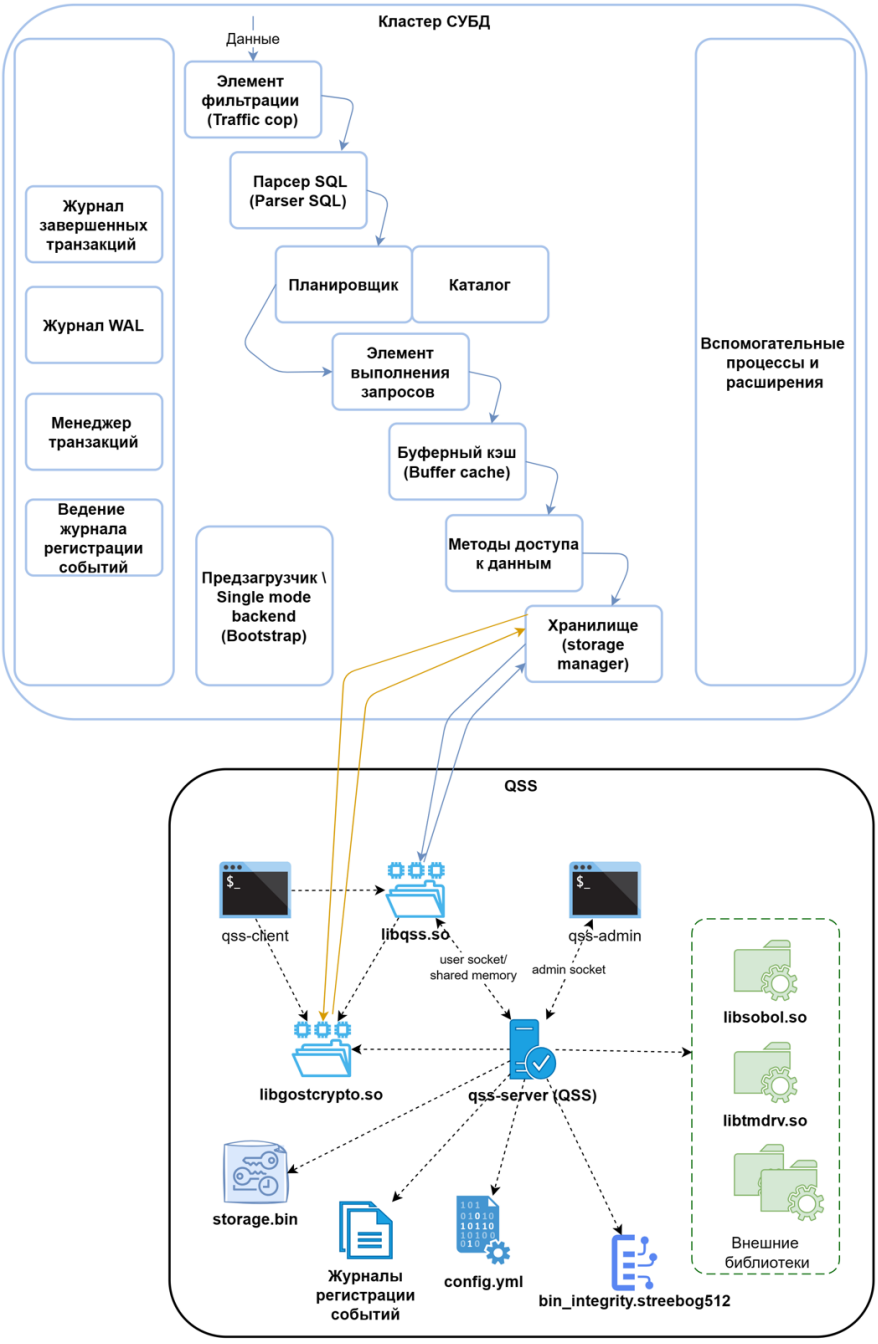

Рисунок 3 – Взаимодействие СУБД «Квант-гибрид» и СКЗИ QSS

2.4. Выбор состава технических и программных средств

Программа функционирует на ЭВМ. В таблице (Таблица 1) представлены требования к Программе и программному обеспечению.

Таблица 1 - Требования к Системе

№ п/п	Техническое средство	Требования
1	Процессор	Процессоры архитектуры (только для 64 битных CPU): x86-64 с тактовой частотой 2 ГГц
2	Оперативная память	Не менее 4 Гб оперативной памяти
3	Жесткий диск	Не менее 1 Гб (не учитывая требования ОС)

QSS функционирует на всех вышеуказанных архитектурах в среде ОС на базе Linux:

- CentOS 7 и 8;
- РЕД ОС;
- ROSA Enterprise Linux Server (RELS);
- РОСА «Кобальт»;
- Альт 8 СП;
- Альт Сервер 9;
- Fedora 33, 34 и 35;
- Debian 9 и 10;
- Astra Linux Special Edition «Смоленск» 1.6, 1.7;
- Ubuntu 18.04 LTS и 22.04 LTS;
- openSUSE 15.4.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Термин/ Сокращение, обозначение	**Расшифровка**
CPU	Центральный процессор (с англ. «Central processing unit»)
QHB	Система управления базами данных «Квант-гибрид»
QSS	Quantum Secure Storage Программа, предназначенная для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных
Гб	Гигабайт, единица измерения количества информации
ГОСТ	Государственный стандарт
ГОСТ Р 34.11-2012	ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ 34.11-2018	ГОСТ 34.11-2018 Информационная технология. Криптографическая защита информации. Функция хэширования.
ГОСТ Р 34.12-2015	ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.
ГОСТ 34.12-2018	ГОСТ 34.12-2018 Информационная технология. Криптографическая защита информации. Блочные шифры.
ГОСТ Р 34.13-2015	ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
ГОСТ 34.13-2018	ГОСТ 34.13-2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
Ключ хранения	Ключ, которым производится зашифрование рабочего ключа
МДЗ	Модуль доверенной загрузки
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение

Термин/ Сокращение, обозначение	**Расшифровка**
Пользовательский ключ, ключи пользователей	Ключи, хранимые на отчуждаемых носителях, которыми производится зашифрование ключа хранения
ПС	Программные средства
Рабочий ключ	Ключ, которым производится зашифрование/расшифрование информации
Р 1323565.1.026–2019	Р 1323565.1.026–2019 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицирующее шифрование.
Р 50.1.111-2016	Р 50.1.111-2016 Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации.
Р 50.1.113-2016	Р 50.1.113-2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.
ТЗ	Техническое задание
ФСБ	Федеральная служба безопасности
ЭВМ	Электронно-вычислительная машина
ЭЦП	Электронная цифровая подпись

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в документе*	*Номер документа*	*Входящий номер сопроводительного документа и дата*	*Подпись*	*Дата*
	измененных	*замененных*	*новых*	*аннулированных*					