ООО «КуАпп»
121205, Москва г., тер. Сколково
Инновационного Центра, б-р. Большой,
дом 30, строение 1, ЭТ 3 ПОМ 33 РБ 33-1
ИНН/КПП: 9731047258 / 773101001
ОГРН: 1197746410278
e-mail: request@qapp.tech
Телефон: +7 991 282 71 82, +7 925 537 71 53
Сайт: https://qapp.tech/

Программное обеспечение «PQC GATE»

Описание функциональных характеристик

Генеральный директор
ООО «КуАпп»

_____/Гугля А.П.
14.10.2024г.

2024

АННОТАЦИЯ

Настоящее описание содержит основные сведения о характеристиках ПО «PQC Gate», разработанного ООО «КуАпп». В описании содержится информация о назначении ПО, используемых языках программирования при его разработке, поддерживаемых протоколах и алгоритмах, системные требования и описание функциональных характеристик ПО «PQC Gate».

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины с соответствующими определениями:

Квантово-устойчивый (или постквантовый) канал передачи данных	— канал передачи данных, обеспечение конфиденциальности в котором достигается путем применения квантово-устойчивых (или постквантовых) алгоритмов
Квантово-устойчивые (или постквантовые) алгоритмы	— асимметричные алгоритмы, стойкие как относительно классических атак, так и атак с применением квантового вычислителя (квантовых атак)
Постквантовый TLS туннель	— TLS соединение, в котором используются постквантовые алгоритмы инкапсуляции ключа. На текущий момент ПО «PQC Gate» не поддерживает постквантовые алгоритмы электронно-цифровой подписи
x509	— стандарт ИОК, который определяет формат цифровых сертификатов. Эти сертификаты используются для управления идентификацией и аутентификацией в сетевых протоколах, таких как TLS

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем документе применяют следующие сокращения и обозначения:

CRLDP — certificate revocation list distribution point

HTTP — hypertext transfer protocol

IMAP — internet message access protocol

POP3 — post office protocol 3

SMTP — simple mail transfer protocol

TLS — transport layer security

ИОК — инфраструктура открытых ключей

МИК — механизм инкапсуляции ключа

ООО — общество с ограниченной ответственностью

ОС — операционная система

ПО — программное обеспечение

1. ОПИСАНИЕ ПО «PQC GATE»

1.1. Назначение

«PQC Gate» — это ПО, обеспечивающее квантово-устойчивый канал передачи данных между узлами компьютерной сети. В клиент-серверной модели взаимодействия выступает в роли прокси, предоставляя возможность клиенту и серверу обмениваться данными посредством постквантового TLS туннеля. ПО «PQC Gate» состоит из трех компонентов: «PQC Gate Server», «PQC Gate Client», «PQC Gate Extension».

«PQC Gate Server» — это компонент ПО «PQC Gate», выступающий в виде обратного прокси-сервера, устанавливаемого, как правило, в демилитаризованной зоне на стороне web-сервера в виде службы ОС Windows. Является точкой выхода из TLS «туннеля», здесь весь входящий трафик расшифровывается и направляется на соответствующий web-сервер.

«PQC Gate Client» — это компонент ПО «PQC Gate», который работает в фоновом режиме на стороне клиента. Приложение не имеет интерфейса или настраиваемых параметров и управляется расширением браузера. Все вызовы на удаленные веб-серверы осуществляются через этот прокси-сервер, который выполняет дополнительное квантово-безопасное шифрование всех данных перед передачей их на удаленный веб-сервер.

«PQC Gate Extension» — это компонент ПО «PQC Gate», расширение для браузера. Оно управляет параметрами браузера — для выбранных доменных имен принудительно используется прокси-сервер.

1.2. Используемые языки программирования

При разработке ПО «PQC Gate» использовались следующие языки программирования:

- C;
- JavaScript;
- Golang.

1.3. Поддерживаемые версии протокола TLS

ПО «PQC Gate» поддерживает следующие версии протокола защиты транспортного уровня (TLS):

- v1.2;
- v1.3.

1.4. Поддерживаемые асимметричные алгоритмы

ПО «PQC Gate» поддерживает следующие постквантовые механизмы инкапсуляции ключа (МИК):

- Kyber;
- Saber;
- NewHope;
- McEliece (только для TLS v1.2).

2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Для эксплуатации ПО к системам предъявляются следующие требования:

1. Операционные системы:
   - Windows 10 и выше;
   - Windows Server 2019 и выше;
   - Ubuntu 22.04 и выше.
2. Архитектура процессора: x86_64.
3. Оперативная память: минимум 64 МБ.
4. Дисковое пространство: минимум 20 МБ.

3. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПО «PQC GATE»

ПО «PQC Gate» обладает следующими функциональными характеристиками:

1) Защита данных.

ПО «PQC Gate» упрощает сохранение конфиденциальности и целостности информации с применением протокола TLS, что позволяет дополнительно квантово-устойчиво защитить информацию от перехвата и несанкционированного доступа.

2) Поддержка прикладных протоколов.

ПО «PQC Gate» может быть использовано для дополнительной квантово-устойчивой защиты таких прикладных протоколов, как: SMTP, POP3, IMAP, HTTP и так далее.

3) Кросс-платформенность.

Поддерживаемые платформы:

- Windows;
- Linux.

4) Гибкость конфигурации.

Пользователь имеет возможность настраивать:

- параметры соединения;
- параметры логирования;
- параметры управления инфраструктурой открытых ключей (ИОК).

5) Прозрачность для приложений.

ПО «PQC Gate» выступает в роли прокси между клиентом и сервером, не требуя при этом никаких модификаций в исходном коде приложений, для которых обеспечивается защита.

6) Поддержка CRLDP.

CRLDP — важный элемент ИОК, который позволяет проверять актуальность сертификатов, предотвращая использование

скомпрометированных или недействительных по каким-либо другим причинам сертификатов.

7) Аутентификация.

ПО «PQC Gate» позволяет проводить аутентификацию как серверной, так и клиентской стороны взаимодействия, с применением X.509 сертификатов.

8) Возможность работы в виде службы/демона.

ПО «PQC Gate» устанавливается на устройство в виде службы и работает в фоновом режиме, что упрощает его использование как на клиентской, так и на серверной части.

4. ПОДДЕРЖКА И ОБСЛУЖИВАНИЕ

По техническим вопросам, связанным с установкой ПО «PQC Gate», можно обращаться it@qapp.tech.