POCA Мессенджер шифрование

POCA

Защищенная коммуникационная платформа Poca Мессенджер имеет многоуровневую архитектуру безопасности. Передаваемые данные шифруются неоднократно. В работе применяется подход защищающий информацию как на пути от устройства к серверу, между серверами и непосредственно между пользователями, так и при хранении на серверах.

1. Сквозное шифрование (End-to-End Encryption—E2EE)

Технология защиты конфиденциальной переписки, гарантирующая, что доступ к содержимому есть только у отправителя и получателя. До момента расшифровки на устройстве адресата сообщение представляет собой нечитаемый набор символов.

Криптографические алгоритмы

Используется комбинация симметричного и асимметричного шифрования. Для сквозного шифрования текстовых сообщений применяется алгоритм AES-256.

Обмен ключами

Для генерации и безопасной передачи сессионных ключей по открытым каналам используется протокол RSA с длиной ключа 4096 бит. Поддерживается возможность смены ключа при необходимости на лету для дополнительной безопасности.

Особенности реализации

Опцию E2EE можно использовать как в личных, так и в групповых чатах. При включенном E2EE новые пользователи не увидят старых сообщений.

2. Транспортное шифрование и защита звонков

Данные шифруются на этапах User-to-Server (пользователь—сервер) и Server-to-Server (между доверенными серверами в распределенной сети компании):

Сигнальный трафик и вызовы:

Для аудио-, видеозвонков и конференций используются технологии WebRTC и протокол SRTP (Secure Real-time Transport Protocol), которые обеспечивают сквозную защиту медиапотока.

Сетевой уровень:

Для защиты каналов связи от перехвата и безопасной доставки push-уведомлений (в которых скрыт сам текст сообщений) задействуются протоколы TLS 1.3 и DTLS.

3. Поддержка ГОСТ-шифрования

В платформу POCA Мессенджер заложена возможность интеграции любых алгоритмов шифрования, включая отечественные. ГОСТ-шифрование подключается по запросу заказчика, что позволяет использовать мессенджер в организациях с повышенными требованиями регуляторов (включая работу с персональными данными и КИИ).

4. Хранение данных на сервере (Данные «в покое»)

Безопасность обеспечивается не только при передаче, но и при хранении данных на сервере:

База данных

На серверах POCA Мессенджер сообщения и файлы зашифрованных чатов хранятся в базе данных в зашифрованном виде.

Безопасность

В случае несанкционированного доступа к базе злоумышленников или даже администраторов компании, все данные остаются в безопасности.

Материал по ссылке >