КРИПТОТЕЛЕФОН X-Telecom

Надежная защита ваших разговоров и тестовых сообщений от прослушки.

X-TELECOM SECURE MOBILE

Представляем Вашему вниманию закрытую связь X-Telecom. “Закрытая”- означает, что связь осуществляется только между абонентами внутренней сети. Все переговоры и передача сообщений внутри сети происходит с помощью криптотелефонов (iPhone/iPad или Android устройств с установленным специальным приложением) в защищенном режиме.

Для шифрования данных в наших криптотелефонах используются криптографические протоколы ZRTP и TLS, ICE + STUN + TURN при сеансах связи. Два уровня надежной защиты от атак "человек посередине": аутенфикация SAS и непрерывность ключевого материала. При использование приложения происходит шифрование каждого звонка End-to-End, т.е. ключи генерируются на телефонах и безопасно передаются по протоколу Диффи-Хеллмана другому абоненту.

+7 (495) 649-98-53, +7 (985) 182-03-61

БЕЗОПАСНОСТЬ ЗВОНКОВ

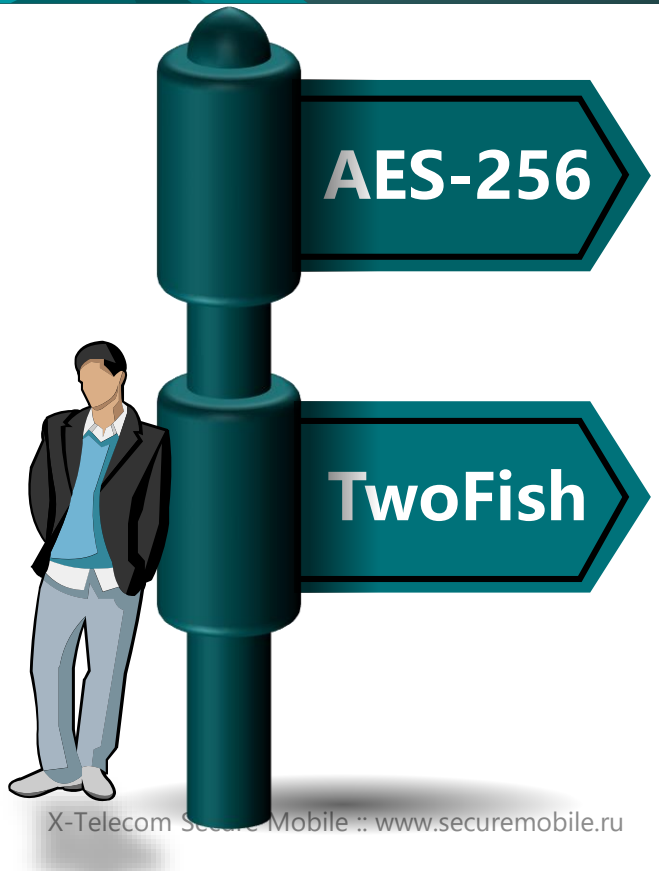
Функциональность и безопасность голосовых звонков обеспечивается при помощи комбинации нескольких технологий и протоколов.

Для сигнализации (например, о начале звонка) используется протокол SIP TLS. Звуковой канал защищен при помощи симметричного шифра AES/Twofish с длиной ключа 256 бит, который выводится при помощи ZRTP. Протокол ICE решает, какой метод использовать для связи абонентов: если подключение через STUN удалось, то используется P2P с ZRTP, если из-за прокси подключение напрямую не удается, то используется TURN с ZRTP.

Для назначения ключа используется протокол ZRTP. ZRTP инициализирует уникальный ключ шифрования для каждого разговора. Ключи генерируются на телефонах и безопасно передаются по протоколу Диффи-Хеллмана другому абоненту.

ZRTP надежно защищен от так называемой "man-in-the middle" атаки при помощи значения SAS hash. SAS - это короткая текстовая цепочка, которая устно засвидетельствована обеими сторонами во время начала разговора. После такой верификации обе стороны могут быть уверены, что между ними нет хакера.

АЛГОРИТМЫ ШИФРОВАНИЯ



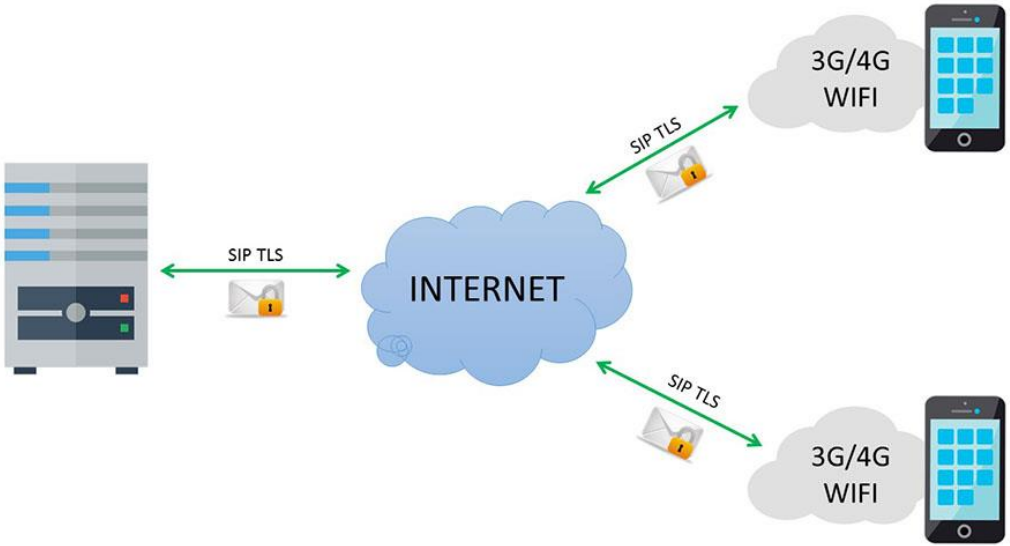
AES - Advanced Encryption Standard — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется в государственных структурах США и других западных стран для засекреченной информации с грифами SECRET и TOP SECRET. Даже если взломщик располагает огромными ресурсами, множеством суперкомпьютеров, то при усердном старании доступ к зашифрованным данным он мог бы получить через десятки лет.

Twofish — симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит, разработанный на основе алгоритмов Blowfish, SAFER и Square. Его отличительными особенностями являются использование предварительно вычисляемых и зависящих от ключа узлов замены и сложная схема развёртки подключений шифрования. Половина n-битного ключа шифрования используется как собственно ключ шифрования, другая — для модификации алгоритма (от неё зависят узлы замены).

Каждый из данных алгоритмов является неуязвимым на сегодняшний день, и в ближайшей, и в дальней перспективе не представляется возможным расшифровать ни один из них. А каскадное (наложенное друг на друга) исполнение их в совокупности дает возможность иметь гарантию неуязвимости на десятки лет вперед, даже невзирая на то, что человечество приобретет новые сверхсовременные технологии.

БЕЗОПАСНОСТЬ СООБЩЕНИЙ

Текстовые сообщения работают по типу PGP - используется шифрование end-to-end. Тип шифра AES-256 mod GCM, который одновременно гарантирует аутентичность и достоверность сообщения.



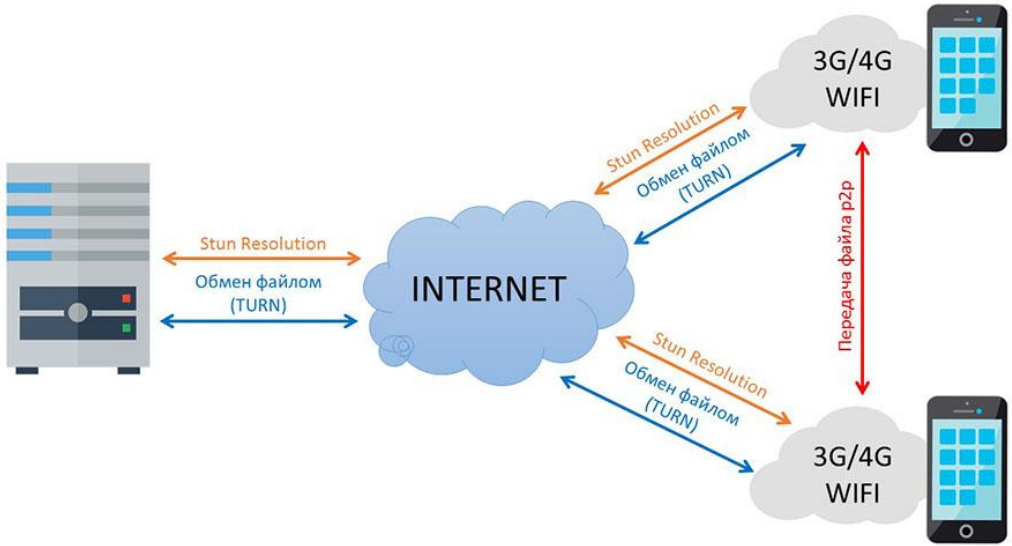
Текстовые сообщения доставляются при помощи протокола SIP TLS. Также поддерживаются оффлайн-сообщения и подтверждения о прочтении сообщений.

Приложение также обеспечивает еще один уровень безопасности для обмена сообщениями. Если обе стороны имеют предыдущий сеанс вызова (ZRTP), то будет использоваться ключ вторичного уровня, добавляющий дополнительный уровень защиты.

То есть сообщения будут шифроваться еще и сгенерированным ключом SAS, затем передаваться по TLS. Таким образом, если ваш сервер скомпрометирован и кто-то наблюдает за вашим сообщением, они не смогут читать, поскольку сообщение зашифровано вашим собственным SAS-кодом.

БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ФАЙЛОВ

При передаче файлов (аудиозаписей, фото и видео) используются технологии RFC 5245 (ICE, механизм обхода NAT) и RFC 5766 (TURN сервера-помощники для обхода NAT или в наихудших случаях TURN сервер используется как посредник (relay) – в этом случае p2p превращается в связь клиент-сервер-клиент).



Сначала собирается информация о доступных IP адресах, а также информация о настроенных IP адресах на сетевых интерфейсах абонентов, с которых они могут получать сетевой трафик. Протокол ICE объединяет полученную информацию о доступных IP и строит наиболее удобные маршруты к этим IP адресам.

Далее устанавливается связь между абонентами либо напрямую – p2p, либо с использованием TURN релея (в случае использования прокси и т.п.)

При передаче пакетов используется технология "Pseudo TCP", которая накладывается на отправку пакетов по UDP. После передачи данных проверяется целостность файла и получателя, таким образом гарантируется, что файл передался целиком и по назначению.

Одновременно можно отправлять и получать несколько файлов, т.к. используется отдельный сеанс для каждого сеанса передачи.

НАДЕЖНАЯ ЗАЩИТА

Криптотелефон X-Telecom надежная защита от прослушки и перехвата сообщений!

Вся передаваемая информация **надежно шифруется** – это защитит от перехвата интернет трафика.

Коммуникации происходят не по GSM каналу – это защитит от фиксировании сообщений и разговоров на стороне оператора связи.

Программное обеспечение - мы предоставляем собственные, специально разработанные приложения для iOS и Android, которые поддерживают ZRTP шифрование. Отсутствуют "программные закладки" для слежения и сбора данных о пользователе телефона.

Собственный SIP сервер - вы можете использовать свой сервер для коммуникации! При общении обмен ключами проходит напрямую между абонентами, поэтому даже в случае компрометации вашего сервере нельзя прослушать разговоры или прочитать переписку.

Полная анонимность - в отличие от популярных мессенджеров нет никакой идентификации пользователя по номеру телефона или email. На сервере хранится только "внутренний" номер абонента и пароль в зашифрованном виде. Нет логов звонков и т.д.

+7 (495) 649-98-53, +7 (985) 182-03-61

ОСНОВНЫЕ ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ И СТАНДАРТЫ

Advanced Encryption Standard, https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard
Twofish, https://ru.wikipedia.org/wiki/Twofish
P2P – peer-to-peer, https://ru.wikipedia.org/wiki/Одноранговая_сеть
SIP – Session Initiation Protocol, https://ru.wikipedia.org/wiki/SIP
ZRTP – Zimmermann Real-time Transport Protocol, https://ru.wikipedia.org/wiki/ZRTP
TLS – Transport Layer Security, https://ru.wikipedia.org/wiki/TLS

RFC 5245 – Interactive Connectivity Establishment (ICE), https://tools.ietf.org/html/rfc5245
RFC 5389 – Session Traversal Utilities for NAT (STUN), https://tools.ietf.org/html/rfc5389
RFC 5766 – Traversal Using Relays around NAT (TURN), https://tools.ietf.org/html/rfc5766
RFC 5768 – Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP), https://tools.ietf.org/html/rfc5768
RFC 6544 – TCP Candidates with Interactive Connectivity Establishment (ICE), https://tools.ietf.org/html/rfc6544

КОНТАКТНАЯ ИНФОРМАЦИЯ

01 Телефоны

+7 (495) 649-98-53

+7 (985) 182-03-61

02 E-mail

sg@opengsm.ru

support@opengsm.ru

03 Россия

Ленинский пр. 41/2

г.Москва, Россия

04 Казахстан

пр. Аль-Фараби 71/10

г.Алматы, Казахстан