CHAT X.509

PITCH

INTRO

ЧАТ X.509 — це безпечна програма обміну повідомленнями з відкритим кодом на основі відкритого ключа, яка використовує сервери лише для маршрутизації для надсилання наскрізних зашифрованих повідомлень без доступу до переписки та метаданих користувачів. Програмне забезпечення засноване на принципах конфіденційності, для нього не потрібен номер телефону чи будь-яка інша особиста інформація.

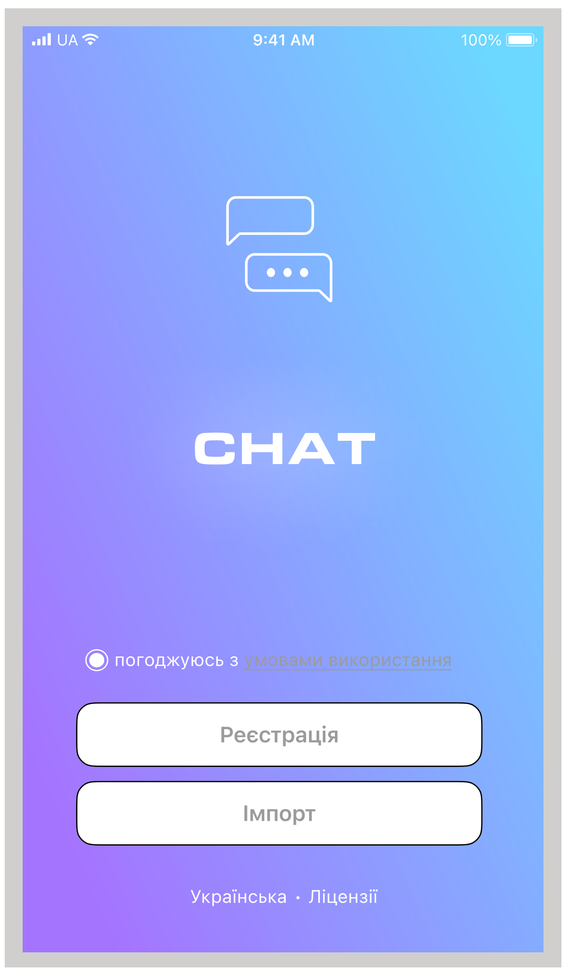
ЧАТ X.509 належить до класу мультипрофільних, захищених за допомогою ECC PKI сертифікатів, федеративних месенжерів на MQTT брокері та побудований на Erlang/OTP для державних та комерційних підприємств з глобальною доступністю.

Реалізація. Імплементація виглядає як простий сервер доставки миттєвих повідомлень розроблений для ненадійних мереж та у відповідності до стандартів ISO/IETF.

- Етап 0 - протокол X.509, iOS клієнт, P2P чати;
- Етап 1 - групові чати, голосові чати;
- Етап 2 - P2P відео чати;
- Етап 3 - групові відеочати RTP.

Він використовує шину та брокер MQTT, LDAP сервер для корпоративних ієрархічних конфігурацій, та бінарну серіалізацію ETF (Erlang Term Format). ЧАТ складається з наступних додатків:

- MQTT у якості Pub/Sub ABAC брокера;
- LDAP для директорії користувачів;
- DNS для безпеки іменного простору;
- CA для видачі клієнтських сертифікатів.



CHAT X.509

PITCH

PRINCIPLES

Компанія користується наступними принципами які формують цілі продукта:

Конфіденційність. Розмови у ЧАТ X.509 завжди наскрізно зашифровані, їх можуть прочитати або почути лише призначені одержувачі.

Прозорість. Повний вихідний код ЧАТ X.509 клієнтів і серверних рішень доступний на GitHub. Це дає змогу зацікавленим сторонам перевірити код на безпеку та правильність.

Відповідність світовим та державним телекомунікаційним та криптографічним стандартам.

Акредитовані Центр Сертифікації Ключів. ЧАТ має власний X.509 центр видачі сертифікатів з використанням еліптичної криптографії ECC CA. Кожен раз при реєстрації нового користувача генерується PKCS-10 X.509 запит на створення сертифікату. Це також може бути зроблено за допомогою консольної утіліти. Підтримання сертифікатів сторонніх АЦСК.

Ієрархічні домени. ЧАТ має власний DNS сервер NS з підтримкою DNSSEC. Структура використаних сервісів та їх імена записані зберігаються в DNS сервері;

Директорія підприємства як розподілена база. В складних розподілених ієрархія підпорядкування з двома видами адміністраторів (безпеки і операційний) підтримка крос-DMZ реплікації регулюється глобальними правилами системи для авторизації пошукових LDAP запитів. Топ-левел LDAP сервери вибирають адміністраторів безпеки LDAP серверів другого рівня, і т.д.;

Всі повідомлення шифруются завжди. Кожне повідомлення шифрується за допомогою моделей полів Галуа GF(2^m) GCM або з використанням еліптичних кривих та їх модулярних форм CCM, які зберігаються в X.509 конфертах як JKS. Нешифровані месаджі заборонені в системі.

CHAT X.509

PITCH

PRINCIPLES

Повідомлення не зберігаються на сервері. Транзієнта оперативна черга доставки повідомлень MQTT, сертифіковані сервери: MQ: Mosquitto через TLSv1.3 та EMQX через QUIC (HTTP/3). Кожне повідомлення після останнього кроку отримання квитанції про доставку кореспондентом знищується на сервері і залишається відтепер тільки на клієнті. Так працювали перші версії Viber;

Не збираєм метадані. Месенжер не зберігає ніяких метаданих, як то локація, IP адреса, інформація про апаратуру клієнта, тощо. ЧАТ використовує тільки наступні внутрішнін ідетифікатори: client, device, profile, roster виключно для роутінга повідомлень. Користувач також має змогу обрати зберігати контактну книгу (ростер) не на сервері, а на клієнті;

Ростер на клієнті. Вся контактна інформація про ваші підписки, чати, канали, та компанії може зберігатися ексклюзивно на клієнті. Після логіна на іншому присторії користовач має змогу отримати (по MQTT) контактну книгу (ростер) з іншого клієнта, який працює на іншому пристрої;

Ростер на сервері. Вся контактна інформація про ваші підписки, чати, канали та компанії зберігається в корпоративній LDAP дерикторії яка має багато каналів реплікації;

Багато контактних книг. Для ведення подвійного та багааватарного життя на платній основі та для корпоративних акаунтів клієнт підтримує мульті-ростерність та верифікує акаунти за допомогою phone та mail способів верифікації клієнта;

Відкритий код. Імплементація Erlang SSL пережила heartblead тому була вибрана як основа безпеки TLS з'єднань в архітектурі ЧАТ. Всі серверні субкомпоненти системи написані на Erlang та доступні для верифікації та ліцензування публічно. Єдиний і повний автор усіх компонент системи який здійснює свою політику згідно BDFL собору є Максим Сохацький.

CHAT X.509

PITCH

BUSINESS

Мотивація

Принципи

Бізнес

Суспільство

Протокол

Компанія

Форми співробітництва:

— Автономні впровадження на ВАШИХ потужностях;
— Хостинг сервісу по підписці на НАШИХ потужностях;
— Багато-ростерні конфігурації по підписці;
— Інтеграційне API SDK для партнерських програм;
— Конфігурація під потреби бізнесу.

SOCIAL

Зроблено для людей:

— Безкоштовний захищений анонімний месенджер;
— Безкоштовний захищений веріфікований месенджер;
— Безпека персональних даних при спілкуванні в Інтернеті;
— Цифровізація держпослуг та звернень громадян;
— Використання електронного підпису документів онлайн;
— Інтегровані системи масового оповіщення;
— B2C сервісні канали для бізнесу і ОВВ;
— Календар iCal та Контакт vCard органайзер;
— Референсний iOS UI дизайн, додаток без залежностей;
— Відкритий консольний клієнт;
— Державний або корпоративний ДСТУ 4145 логін.

CHAT

X.509

CLIENT

CERTIFY

Запрошення

Реєстрація

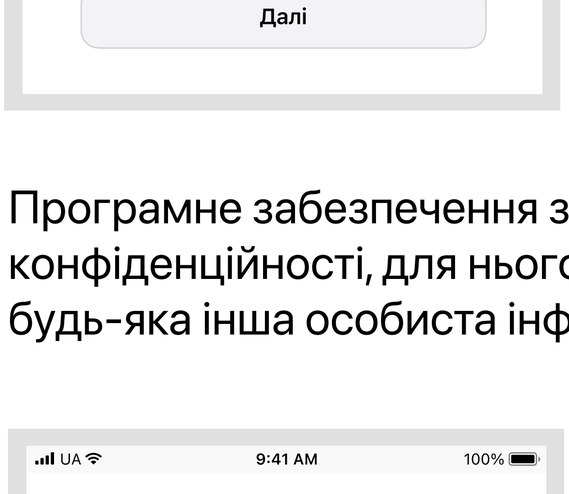
Імпорт

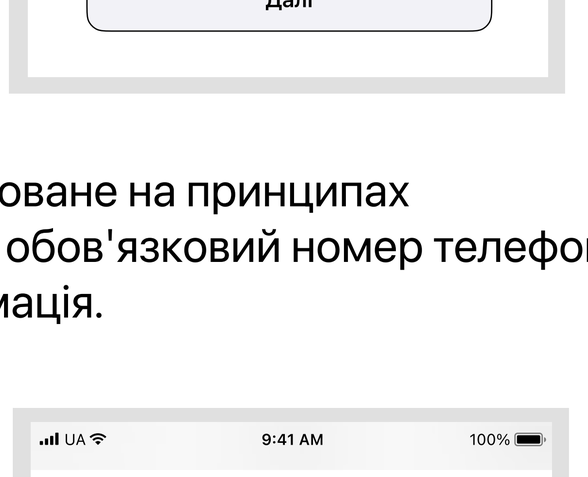
Мобільний

Пошта

Ключі

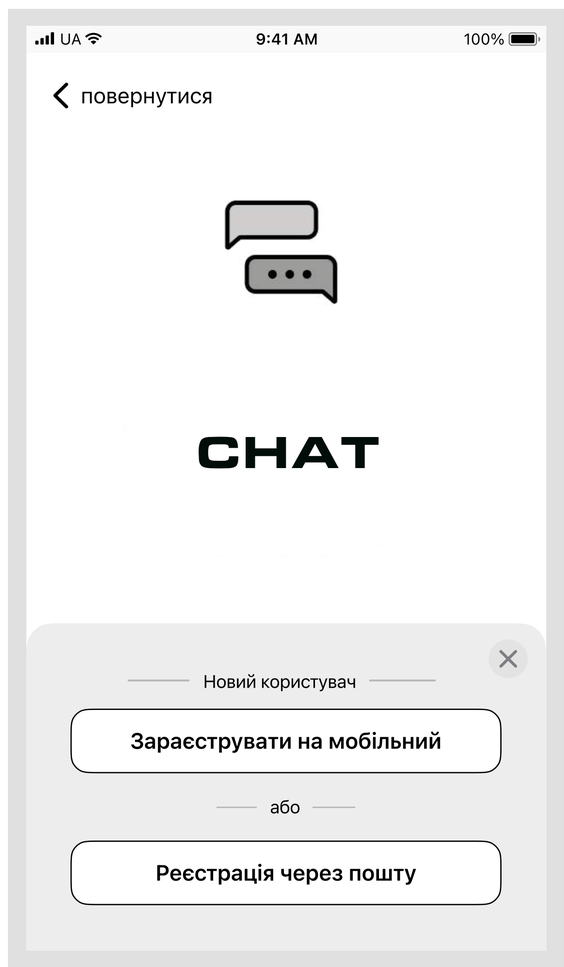
Шифри

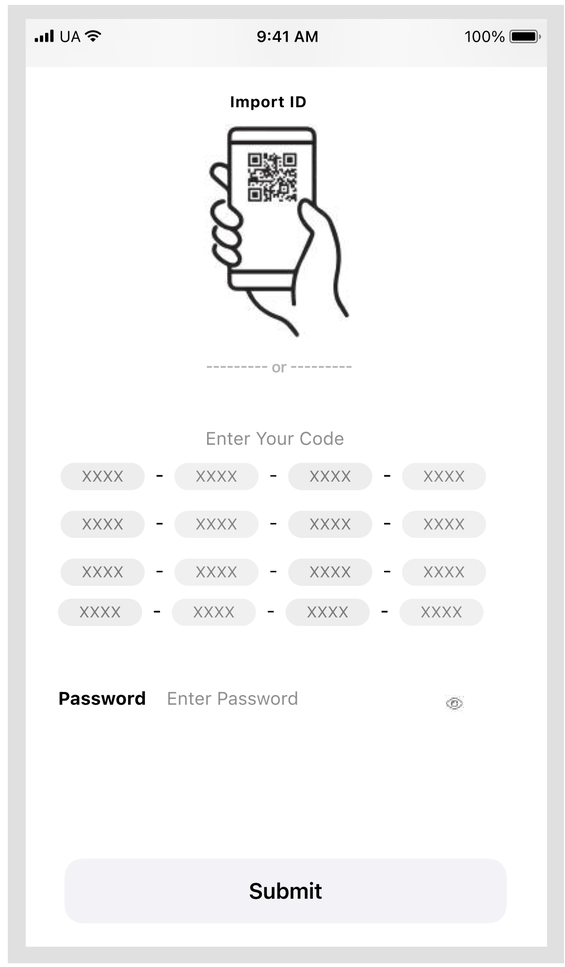




Чати

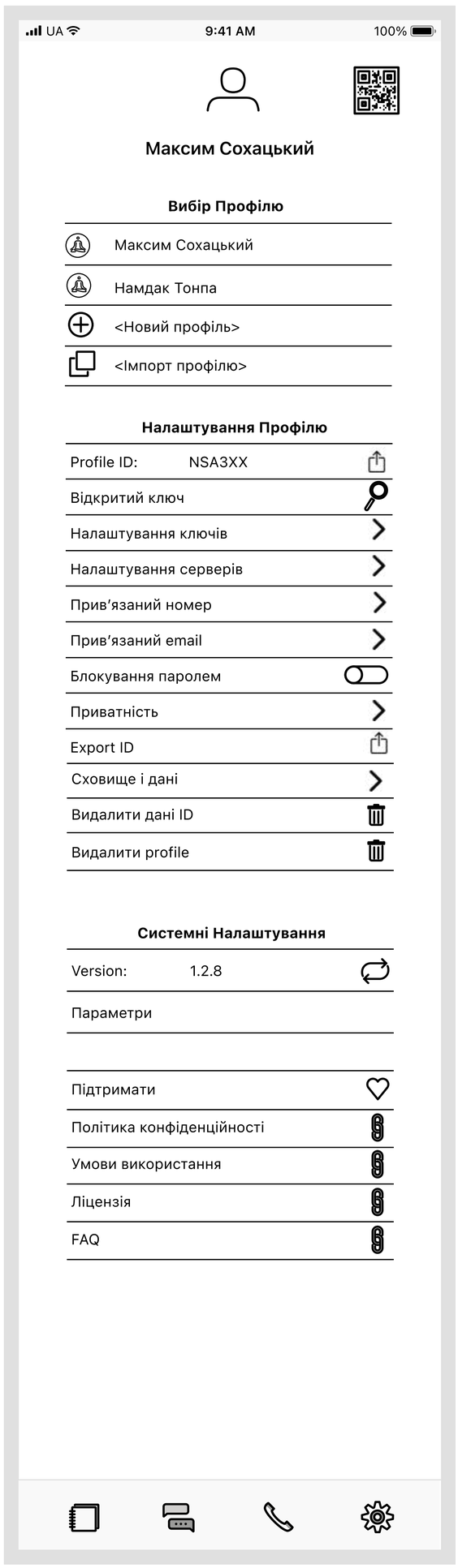
Програмне забезпечення засноване на принципах конфіденційності, для нього не обов'язковий номер телефону чи будь-яка інша особиста інформація.





CHAT X.509

CLIENT PROFILE



Мультипрофільність на одному клієнті - для кожного профілю свої ключі, контакти та топіки.

Безпека - розмови у ЧАТ X.509 завжди наскрізно зашифровані, їх можуть прочитати або почути лише призначені одержувачі.

Анонімність - налаштування бажаної видимості профілю в загальноому каталозі.

Приватність - налаштування захисту персональних даних та встановлення меж для захисту від необґрунтованого втручання сторонніх, що дозволяє керувати бажаною взаємодією з навколишнім світом.

Дані профілю - захищений доступ до профілю. Розмежоване зберигання даних кожногоо профілю та гарантоване видалення данних без можливості відновлення. Експорт профілю для відновлення при необхідності.

Ключі які використовують користувачі складаються з трьох типів-пар (можна більше, але типів всього три):

- Перша пара ключів SECP384R1 забезпечує безпеку каналу TLS;
- Друга пара ключів ED25519 забезпечує безпеку повідомлень;
- Третя пара ключів забезпечує доступ до державних та юридичних сервісів ДСТУ-4145.

Кожен учасник системи перед комунікацією здійснює реанонс своїх публічних частин цих асиметричних ключів.

Шифри на вибір користувача - AES-CBC, AES-GCM, AES-CCM, ДСТУ-КАЛИНА.

CHAT X.509

CLIENT

CHATS

Контакти

Текст

Аудіо

Відео

Файли

Топіки

Папки

ЧАТ — це простий сервер обміну миттєвими повідомленнями на основі стандартів ISO. Він використовує протокол MQTT і бінарну серіалізацію ETF від Erlang/OTP у різних своїх додатках: MQTT, LDAP, DNS, CA.

Безпечний за замовчуванням. Додаток ЧАТ має функцію підпису/підтвердження, шифрування/розшифрування, увімкнену для кожного окремого переданого повідомлення. Доставлені повідомлення видаляються з MQTT сервера після підтвердження отримки одержувачем.

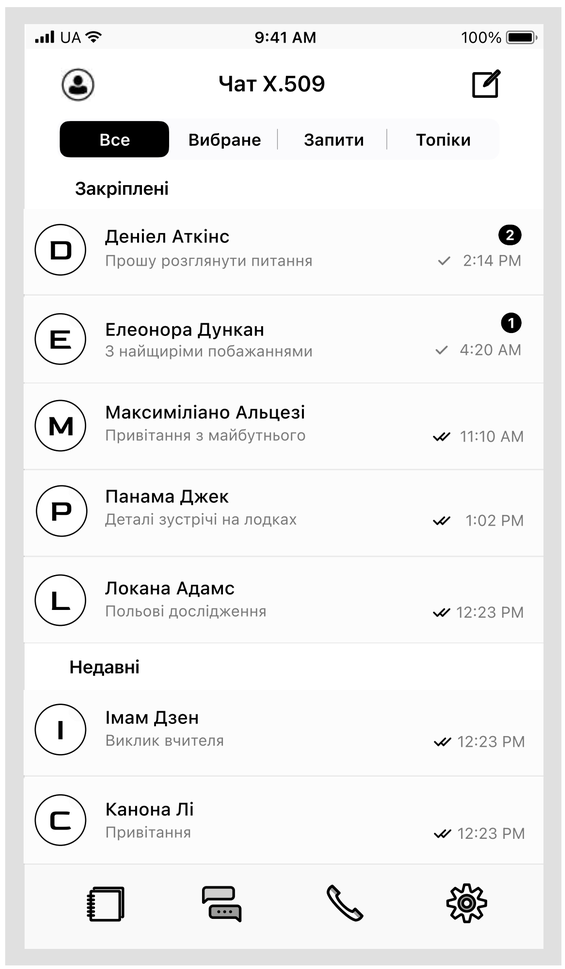
Конфіденційність. Дані у ЧАТ X.509 завжди наскрізно зашифровані, їх можуть прочитати або почути лише призначені одержувачі.

Формати данних. Текст, аудіо, відео, файли, фото, локація. Управління папками чатів та додавання власних під свої потреби.

Перегляд запитів від інших контактів: видалити, заблокувати, прийняти.

Топіки - створення та підписка на групові чати з налаштуваннями щодо приватності та управління прівілеями підписників.

Групові чати. Програми обміну повідомленнями все частіше використовують наскрізні механізми безпеки, щоб гарантувати, що повідомлення доступні лише кінцевим точкам зв'язку, а не будь-яким серверам, які беруть участь у доставці повідомлень. MLS визначаємо протокол встановлення ключа, який забезпечує ефективне асинхронне встановлення ключа групи з прямою секретністю (FS) і посткомпромісною безпекою (PCS) для груп розміром від двох до тисяч.



CHAT X.509

CLIENT

CONTACTS

Синхронізація

Блокування

Видимість

Приватність

Ростер на клієнті. Вся контактна інформація про ваші підписки, чати, канали, та компанії може зберігатися ексклюзивно на клієнті. Після логіна на іншому пристрої користувач має змогу отримати (по MQTT) контактну книгу (ростер) з іншого клієнта, який працює на іншому пристрої;

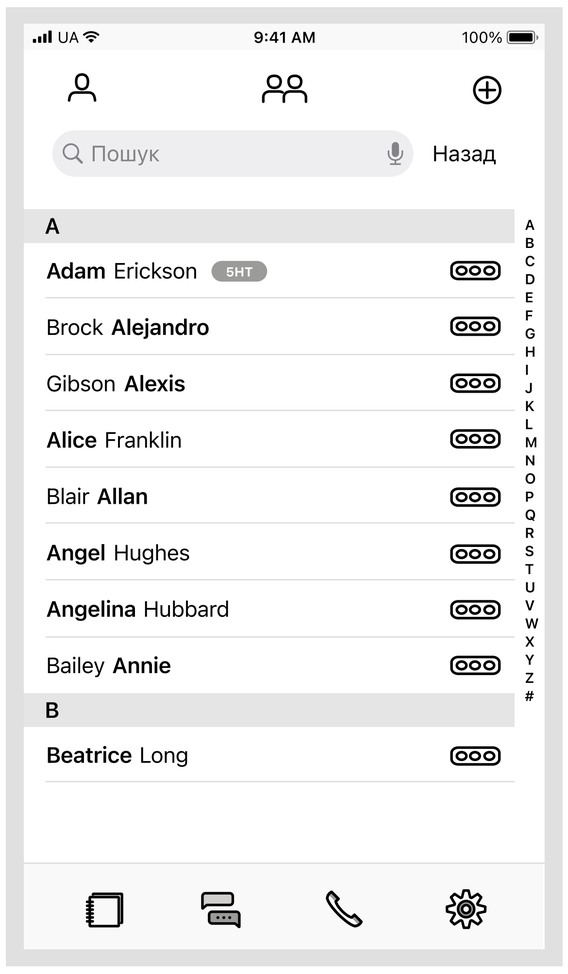
Ростер на сервері. Вся контактна інформація про ваші підписки, чати, канали та компанії зберігається в корпоративній LDAP дерикторії яка має багато каналів реплікації;

Управління доступом до контактної книги iOS. Доступ до існуючих контактів та додавання нових контактів до власної контактної книги. Пошук відкритих контактів в загальному каталозі та власній контактній книзі.

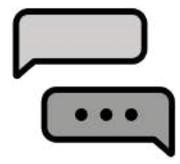
Відправка запитів на встановлення контакту та приймання запрошення від довірених контактів. Перегляд рівня взаємної верифікації контакту.

Налаштування взаємодії. Додавання: видалення, блокування, оповіщення. Управління сумісними даними що зберігаються на клієнті: перегляд, редагування, бекапування, видалення.

Встановлення функції зникаючих повідомлень.



CHAT X.509



ASN.1

ARCH

ЧАТ X.509 належить до класу захищених за допомогою ECC PKI сертифікатів, федеративних месенжерів на MQTT брокері та побудований на Erlang/OTP для державних та комерційних підприємств з глобальною доступністю.

Як імплементація ЧАТ реалізований як простий сервер доставки миттєвих повідомлень розроблений для ненадійних мереж та у відповідності до стандартів ISO/IETF.

OCSP TSP CMP/CMS

NS CA CHAT LDAP

:18:53:443:636:829:1030:1070

CLIENT

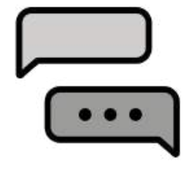
:1030:1070

CZO/CA

Він використовує шину та брокер MQTT, LDAP сервер для корпоративних ієрархічних конфігурацій, та бінарну серіалізацію ETF (Erlang Term Format). ЧАТ складається з наступних додатків:

- MQTT у якості Pub/Sub ABAC брокера;
- LDAP для директорії користувачів;
- DNS для безпеки іменного простору;
- CA для видачі клієнтських сертифікатів.

CHAT X.509



ASN.1 PROTOCOL

Поняття протоколу:

Топіки. ЧАТ протокол використовує наступні MQTT топіки, перелік яких зберігається на клієнті: 1) actions/:client; 2) events/:client; 3) devices/:phone; 4) contacts/:roster; 5) private/:roster/:roster; 6) room/:room.

Записи. По цим топікам передаються наступні Erlang записи (records): Index, Typing, Search, Feature, Service, Presence, Friend, Tag, Link, Message, Member, Room, Contact, Star, Ack, Auth, Roster, Profile, History, push, io закодовані ETF серіалізатором.

Модулі. Протокол ЧАТ реалізований у наборі модулів-підпротоколів: ФАЙЛ, ІСТОРІЯ, ПОСИЛАННЯ, ПОВІДОМЛЕННЯ, ПРИСУТНІСТЬ, ПРОФІЛЬ, PUSH, КІМНАТА, РЕСТЕР, ПОШУК, АУТ. Щоб отримати повну специфікацію, перейдіть до папки priv/proto. Реалізація сервера CHAT покладається лише на підключення ISO/IETF, такі як DNSSEC, X.509 CSR, LDAP, QUIC, WebSocket, MQTT.

Додатки. ЧАТ — це простий сервер обміну миттєвими повідомленнями на основі стандартів ISO. Він використовує протокол MQTT і бінарну серіалізацію ETF від Erlang/OTP у різних своїх додатках: MQTT, LDAP, DNS, CA. Безпечний за замовчуванням. Додаток ЧАТ має функцію підпису/підтвердження, шифрування/розшифрування, увімкнену для кожного окремого переданого повідомлення. Доставлені повідомлення видаляються з MQTT сервера після підтвердження отримки одержувачем. Це заміна Keybase, OTR, PGP (називайте як хочете) для безпечних комунікацій, визначених X.509 ASN.1.

Ключі. Ключі які використовують користувачі складаються з трьох типів-пар (можна більше, але типів всього три): 1) Перша пара ключів SECP384R1 забезпечує безпеку каналу TLS 1.3 засобами еліптичної криптографії власного АЦСК/CA; 2) Друга пара ключів ED25519 забезпечує безпеку повідомлень; 3) Третя пара ключів забезпечує доступ до державних та юридичних сервісів ДСТУ-4145. Кожен учасник системи перед комунікацією здійснює реанонс своїх публічних частин цих асиметричних ключів.

Відкритість платформи. Єдиний додаток як в часи IRC та XMPP забезпечує доступ до всіх серверів сумісних з CHAT X509. Таким чином клієнт підримує довільну кількість ключів та довільну кількість серверів. І вся ця інформація зберігається тільки на клієнті.

CHAT

X.509

ASN.1/BERT

CHAT

CHAT/CMS/MQTT/TLS

NIST: 800-38D 800-56A 800-57 800-162 P-384 P-571, ISO: 20922 15946 10646 8824 8825, FIPS: PUB 180-4, ДСТУ: 4541 28147 GF(2^509), ДССЗІ: #112 14.05.2010 #1236/5/453 20.08.2012 #687 27.10.2020

PKIX CRYPTO

Протоколи ключів	ED-25519, X25519, X448, SECP-384r1, SECP-571r1, ДСТУ-ГАЛУА-GF(2^431), GF(2^509)
Похідні ключі	KDF, PBDKF2, AES-KW
Шифри	AES-CBC, AES-GCM, AES-CCM, ДСТУ-КАЛИНА
Хеші	SHA-2, POLY-1305, AES-CMAK, ДСТУ-КУПИНА, CAdES
Протоколи груп	MLS
PQC	CMS, IBE, KYBER

CHAT

X.509

ASN.1/BER

CA/CMP/CMC/TSP/TLS

CMS-AES-CCM-AND-AES-GCM-2009
CMSAESRSAESOAEP-2009
CMSECCALGS-2009-02
CMSECDHALGS-2017
CRYPTOGRAPHICMESSAGESYNTAX-2009
CRYPTOGRAPHICMESSAGESYNTAX-2010
ENROLLMENTMESSAGESYNTAX-2009
PKCS-10
PKCS-7
PKIX1EXPLICIT-2009
PKIX1IMPLICIT-2009
PKIXALGS-2009
PKIXCMP-2009
PKIXCRMF-2009
AUTHENTICATIONFRAMEWORK
INFORMATIONFRAMEWORK
KEP

SMIME-WG: 5990, 5911, 5750—5754, 5652, 5408, 5409, 5275, 5126, 5035, 4853, 4490, 4262, 4134, 4056, 4010, 3850, 3851, 3852, 3854, 3855, 3657, 3560, 3565, 3537, 3394, 3369, 3370, 3274, 3114, 3278, 3218, 3211, 3217, 3183, 3185, 3125—3126, 3058, 2984, 2876, 2785, 2630, 2631, 2632, 2633, 5083, 5084, 2634.

PKIX: 7030, 6960, 6818, 6844, 6712, 6664, 6402, 6277, 6170, 6024, 6025, 5934, 5912—5914, 5877, 5816, 5755, 5756, 5758, 5697, 5636, 5480, 5272—5274, 5280, 5055, 5019, 4985, 4683, 4630, 4476, 4387, 4325, 4158, 4210, 4211, 4055, 4043, 3874, 3779, 3820, 3739, 3709, 3628, 3161, 3029, 2797, 2559, 2587, 3039, 3029, 2511, 2510.

Compatibility: LibreSSL CMS, OpenSSL CMS, GnuPG S/MIME, OpenSSL, Cisco, Red Hat, Siemens, Nokia, IBM.

ASN.1/BER

LDAP/TLS

LDAP

LDAP: 2849, 3296, 3671—3673, 3866, 4511—4518, 4522, 4525, 4526, 4529, 1823, 2377, 2820, 3352, 3384, 3494, 4510, 4520, 4521, 2589, 2649, 2696, 2891, 3062, 3829, 3876, 3909, 3928, 4370, 4373, 4527, 4527, 4531—4533, 5805, 6171, 2247, 2798, 2926, 2985, 3045, 3112, 3687, 3698, 4517, 4519, 4524, 4530, 5020, 2079, 2307, 2713, 2714, 2739, 3641, 3642, 3703, 3727, 4104, 4403, 4523, 4792, 4876, 5803, 7612, 8284.

Compatibility: Apache Directory Studio, OpenLDAP.

ASN.1/BER

NS/DNSSEC/TLS

DNS

NS: Name Server IETF 1034, 1035, 1101, 2065, 2535, 2539, 4033-4035 4398, 6944

Compatibility: BIND.

PITCH COMPANY

Структура виробничого процесу компанії:

Маркетинговий відділ: Threema, Signal, WhatsApp, Session, Element, Wire, Wickr. Займається дослідженням найкращих практик та адаптацією їх до дизайну месанжера;

Клієнтський сектор розробки. Відділ розробки iOS клієнта на мові програмування Swift 5.8 Chat X.509, разом з дизайном та ігровою ергономікою в Figma та Swift;

Серверний сектор розробки. Займається як розвитком сервера на Erlang/OTP так і розробкою інших серверів в інфраструктурі системи: CA NS LDAP AUTH MQTT [mac] CHAT CLI;

Відділ по роботі з корпоративними клієнтами. Відділ займається підтримкою та комунікацією з органами державної влади, партнерами, провайдерами та зовнішніми контрагентами. [SYNRC.PEM] [SYNRC.LDIF] [SYNRC.DNS];

Відділ впровадження, супроводу і підтримки. Відділ займається інсталяціями під ключ та супроводом існуючої публічної клієнтської бази користувачів месенжера для операційних систем NetBSD і Linux. Головний продукт компанії — X.509 чат месенжер;

Відділ проектної документації. займається розвитком та підтримкою протоколу, дидактичних матеріалів та технічної докментації. Описує протокол SYNRC CHAT в BERT/MQTT контексті для мов Swift і Erlang. Відділ публікує наступні публікації.

1) Технічні характеристики (Datasheet);
2) Брошура та головний сайт (Whitepaper);
3) Посібник користувача (Manual);
4) Слайди презентації (Slides);
5) Діаграми Ґанта (Gantt);
6) Вимоги та технічне завдання (Requirements);
7) Публікації (Publications);
8) Архітектура та програмування (Book);
9) Ліцензії та угода користувача (EULA);
10) Субліцензії (Licenses);
11) Контракти (ЄДРПО);
12) Контракти (ФОП);
13) Комплекс систем захисту інформації (КЗЗІ).