**ASN.1****ARCH****Вступ**

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

**Бізнес**

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

**Суспільство****Протокол****Компанія****OCSP****TSP****CMP/CMS****NS****CA****CHAT****LDAP**

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

**CLIENT**

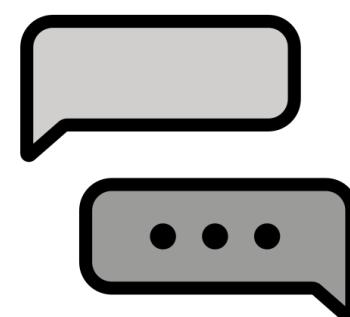
:1030:1070

**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.





## ASN.1

## PROTOCOL

Вступ

Принципи

Бізнес

Суспільство

Протокол

Компанія

Топіки

Записи

Модулі

Додатки

Ключі

Відкритість

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, іо 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 ЧАТ покладається лише на підключення ISO/IETF, такі як DNSSEC, X.509 CSR, LDAP, QUIC, WebSocket, MQTT.

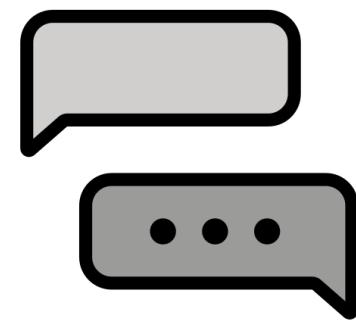
**Додатки.** ЧАТ — це простий сервер обміну миттєвими повідомленнями на основі стандартів ISO. Він використовує протокол MQTT і бінарну серіалізацію ETF від Erlang/OTP у різних своїх додатках: MQTT, LDAP, DNS, CA. Безпечний за замовчуванням. Додаток ЧАТ має функцію підпису/підтвердження, шифрування/розшифрування, 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/СА; 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 ЧАТ X509. Таким чином клієнт підтримує довільну кількість ключів та довільну кількість серверів. І вся ця інформація зберігається тільки на клієнти.



**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<sup>509</sup>), ДСС3І: #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<sup>431</sup>), GF(2<sup>509</sup>)

Похідні ключі

KDF, PBDF2,  
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

**ASN.1/BER**

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

**CA/CMP/CMC/TSP/TLS**

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

**LDAP/TLS**

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**

DNS

**NS/DNSSEC/TLS**

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

Compatibility: BIND.