ERP/1: Комунікатор

Технічні вимоги

Локальна інфраструктура безпеки,
наскрізного шифрування X.509 CMS
та захищеного обміну повідомленнями

Зміст

Зміст

Анотація

У цьому документі наведено детальні технічні вимоги до підсистеми ERP/1: Комунікатор, яка розробляється як надійна, децентралізована, стійка до відмов платформа безпечного обміну повідомленнями (чат v2) та документами (пошта v3) у захищеному периферійному контурі підприємства чи установи. Система базується на принципах наскрізного шифрування X.509 CMS, кодуванні повідомлень у форматі ASN.1 DER та транспортному протоколі Buddha (X.422). Вона абсорбує існуючі сервіси авторизації, видачі сертифікатів (CA), захищених тунелів (VPN), служби каталогів (LDAP) та забезпечує повну функціональну сумісність без використання екосистеми Rust.

1. Умовні скорочення та визначення

Основні терміни та скорочення підсистеми «Комунікатор»:

Термін / Скорочення	**Значення**
CA	Certificate Authority (Центр сертифікації / засвідчувальний центр)
CMS	Cryptographic Message Syntax (Криптографічний синтаксис повідомлень)
DER	Distinguished Encoding Rules (Правила однозначного кодування ASN.1)
ASN.1	Abstract Syntax Notation One (Абстрактна синтаксична нотація один)
OCSP	Online Certificate Status Protocol (Протокол онлайн-перевірки статусу)
EST	Enrollment over Secure Transport (Реєстрація через безпечний транспорт)
CMP	Certificate Management Protocol (Протокол управління сертифікатами)
TSP	Time-Stamp Protocol (Протокол штампів часу)
IAS	Identity Access Server (Сервер автентифікації та авторизації)
LDAP	Lightweight Directory Access Protocol (Полегшений протокол каталогів)
VPN	Virtual Private Network (Віртуальна приватна мережа / тунель)
E2EE	End-to-End Encryption (Наскрізне шифрування від клієнта до клієнта)
MLS	Messaging Layer Security (Протокол групового шифрування)

2. Загальні відомості

2.1. Передумови

Сучасні виклики безпеки інформаційного обміну в державних установах та на об'єктах критичної інфраструктури потребують відмови від використання публічних та закордонних хмарних месенджерів. Передача службової інформації повинна здійснюватися через локальну інфраструктуру, яка:

1. **Конфіденційність (КСЗІ)**: Гарантує наскрізне шифрування повідомлень і файлів (E2EE) безпосередньо на кінцевих пристроях користувачів.
2. **Автономність (Air-Gapped)**: Здатна функціонувати в умовах відсутності доступу до мережі Інтернет за допомогою локальних каналів маршрутизації та VPN-тунелів.
3. **Стандартизація**: Відповідає міжнародним стандартам ITU-T X.509, IETF CMS (RFC 5652) та вітчизняному ДСТУ 4145 для забезпечення сумісності із державною інфраструктурою ключів.

2.2. Цільові продукти для абсорбції

Підсистема «Комунікатор» абсорбує технічні рішення таких систем:

- **chat.n2o.dev**: асинхронна архітектура швидкої доставки повідомлень на базі Erlang/OTP.
- **x509.chat**: концепція першого покоління месенджера з наскрізною авторизацією за клієнтськими сертифікатами X.509.
- **protocol.zencrypted.uk**: специфікації протоколу Buddha (X.422), призначеного для передачі криптографічно підписаних ASN.1 DER пакетів.

3. Призначення та цілі впровадження

Модуль призначений для розгортання єдиної захищеної системи миттєвого обміну повідомленнями, передачі документів, управління ієрархією користувачів та випуску ключів на базі Erlang/OTP.

Цілі впровадження:

- Локальний запуск месенджера v2 із наскрізним криптографічним шифруванням.
- Запуск поштового клієнта v3 для формалізованого обміну документами у вигляді CMS-пакетів.
- Локальне керування випуском та життєвим циклом сертифікатів за протоколами EST/CMP/OCSP.
- Організація захищених шлюзів зв'язку (VPN/LDAP) на периферії.

4. Класифікація вимог

4.1. Функціональні вимоги

4.1.1. Вимоги до Центру сертифікації (CA ERP/1: Сертифікати)

Сервер CA повинен підтримувати автоматизоване управління сертифікатами X.509:

- Підтримка реєстрації та випуску сертифікатів за протоколом EST (RFC 7030) через HTTPS.
- Підтримка протоколу CMP (RFC 4210) для складних операцій життєвого циклу ключів.
- Перевірка статусів сертифікатів у реальному часі через OCSP (RFC 6960) з часом відповіді не більше 100 мс.
- Надання сервісу міток часу за протоколом TSP (RFC 3161) для юридичного підтвердження часу відправки документів.

4.1.2. Вимоги до VPN (ERP/1: Тунелі)

Модуль тунелювання повинен забезпечувати ізольовані канали:

- Автоматичне підняття тунелю на клієнтських пристроях за допомогою локальних сертифікатів X.509.
- Робота за протоколами з мінімальним накладним оверхедом (WireGuard / UDP тунелі) для стабільності в ненадійних мережах.
- Інтеграція з сервером авторизації для динамічного виділення IP-адрес.

4.1.3. Вимоги до LDAP (ERP/1: Директорія)

Служба каталогів повинна забезпечувати ієрархічний довідник:

- Зберігання профілів користувачів, їх публічних сертифікатів, зв'язків та прав доступу (атрибутів ABAC).
- Асинхронне обслуговування запитів за протоколом LDAPv3 (RFC 4511) через порт 389/636 (LDAPS).
- Підтримка гомотопічного DER кодування та компіляції ASN.1 схем довідника.

4.1.4. Вимоги до IAS (ERP/1: Авторизація)

Сервер авторизації повинен контролювати вхід та сесії:

- Автентифікація за клієнтськими сертифікатами X.509 без використання паролів.
- Підтримка авторизації на базі атрибутів користувача (ABAC), зчитаних з LDAP та сертифіката.
- Контроль статусу відкликання ключів через OCSP перед кожним початком сесії зв'язку.

4.1.5. Вимоги до CHAT (ERP/1: Комунікатор v2)

Сервер CHAT повинен забезпечувати маршрутизацію повідомлень:

- Маршрутизація повідомлень у вигляді DER-кодованих ASN.1 об'єктів без дешифрування контенту на сервері (Zero-Knowledge).

- Підтримка протоколу Double Ratchet для генерації тимчасових ключів сесії на клієнті.
- Тимчасове (транзієнтне) збереження повідомлень в оперативній пам'яті (Mnesia/KVS) до отримання квитанції про доставку, після чого дані повністю знищуються.

4.1.6. Вимоги до MAIL (ERP/1: Документи v3)

Поштовий сервер повинен забезпечувати доставку документів:

- Прийом та відправка документів у вигляді підписаних CMS-конвертів (S/MIME).
- Підтримка протоколів доставки поштових пакетів (SMTP/IMAP) з обов'язковим TLS-захистом.
- Автоматична верифікація підписів відправника та перевірка ланцюжків сертифікатів через локальний CA.

4.2. Нефункціональні вимоги

4.2.1. Вимоги до програмного стеку

- **Заборона Rust**: усі компоненти (CA, VPN, LDAP, IAS, CHAT, MAIL) повинні бути реалізовані на Erlang/OTP, Elixir або C99 для забезпечення сумісності із цільовим середовищем розгортання та спрощення КСЗІ.
- **Erlang/OTP додатки**: кожен сервіс має бути оформлений як окремий OTP-додаток (Application) з супервізорами та процесами-серверами.

4.2.2. Вимоги до безпеки та криптографії

- Використання виключно сертифікованих алгоритмів: ДСТУ 4145-2002 для електронного підпису та ДСТУ 7624 (Калина) / AES для шифрування контенту.
- Повне логування та аудит дій адміністраторів через незмінний журнал подій під захистом апаратного модуля TPM 2.0.

5. Додаток А. Регламент взаємодії за протоколом Buddha (X.422)

Регламент взаємодії визначає транспортні та криптографічні стандарти передачі даних у підсистемі «Комунікатор».

5.1. Транспортний рівень X.422.1

1. **Мережеві сокети**: Обмін пакетами здійснюється через асинхронні TCP сокети або шифровані UDP-канали. Для локального виявлення пристроїв у межах фізичної LAN-мережі підтримується UDP Multicast на виділений порт 4221.
2. **Структура транзиту**: Сервер виконує виключно роль асинхронного брокера (Broker), який пересилає DER-пакети адресатам на основі унікальних ідентифікаторів профілів.

5.2. Криптографічний конверт X.422.2

Кожне інформаційне повідомлення на клієнті упаковується у CMS-конверт відповідно до стандарту RFC 5652 та кодується за правилами DER:

- **SignedData**: містить оригінальне повідомлення (або його хеш), сертифікат відправника та його електронний підпис (ДСТУ 4145 або ECDSA).
- **EnvelopedData**: містить зашифровані за допомогою симетричного ключа (AES-GCM/Калина) дані. Сам симетричний ключ шифрується на публічному ключі отримувача за схемою ECDH (еліптичні криві).
- **Захист метаданих**: заголовки пакетів (ідентифікатор отримувача та пристрою) шифруються на тимчасових серверних ключах для захисту від аналізу трафіку.