ERP/1: Авторизація

Технічні вимоги

до системи керування цифровими ідентичностями,
сертифікатами та політиками безпеки

Зміст

Зміст

Анотація

У цьому документі наведено детальні технічні вимоги до підсистеми ERP/1: Служба ідентифікації та авторизації (Identity and Authorization Service — IAS), яка розробляється як центральний компонент безпеки інфраструктури Zencrypted на базі Erlang/OTP. Вимоги розроблено згідно з Політиками Технічних вимог, ТЗ та ТД (ДСТУ 3973-2000, ДСТУ 3008:2015 та ISO/IEC/IEEE 42010). Документ визначає перелік довідників, реєстрових сутностей, життєві цикли сертифікатів (включаючи CMP/EST/CMC), рольову модель доступу на базі ABAC, принципи інтеграції з Центром сертифікації (CA) та шлюзами VPN, а також нефункціональні вимоги до архітектури, безпеки (КЕП CAdES-X Long та ДСТУ 4145-2002), продуктивності та логування.

1. Умовні скорочення та визначення

Терміни та скорочення, що використовуються в цьому документі:

Термін / Скорочення	Значення
IAS	Identity and Authorization Service (Служба ідентифікації та авторизації)
CA	Certificate Authority (Центр сертифікації)
VPN	Virtual Private Network (Віртуальна приватна мережа)
PKI	Public Key Infrastructure (Інфраструктура відкритих ключів)
КЕП / QES	Кваліфікований електронний підпис / Qualified Electronic Signature
CSR	Certificate Signing Request (Запит на підписання сертифіката)
CMP	Certificate Management Protocol (RFC 4210)
EST	Enrollment over Secure Transport (RFC 7030)
CMC	Certificate Management over CMS (RFC 5272)
BPE	Business Process Engine (Рушій бізнес-процесів)
KVS	Key-Value Storage (Універсальна бібліотека сховища даних)
ABAC	Attribute-Based Access Control (Контроль доступу на основі атрибутів)
RBAC	Role-Based Access Control (Рольовий контроль доступу)
FSM	Finite State Machine (Скінченний автомат)
OTP	Open Telecom Platform (Набір бібліотек для Erlang)

2. Загальні відомості

2.1. Передумови

Проект ERP/1: Служба ідентифікації та авторизації (IAS) створюється як центральна ланка безпеки Zencrypted-середовища. Вона призначена для адміністрування та координації життєвого циклу цифрових ідентичностей, пристроїв, сертифікатів, профілів безпеки, VPN-сервісів та графів зв'язків між ними. IAS виступає центральною консоллю управління, яка взаємодіє з автономними компонентами: Центром сертифікації (CA) для підписання сертифікатів та шлюзами VPN, які виконують отримані від IAS рішення з авторизації.

2.2. Питання, що вирішуються

Платформа вирішує такі ключові завдання:

- Ведення єдиного реєстру користувачів, пристроїв та їх зв'язків у вигляді графу відношень.
- Управління життєвим циклом криптографічних сертифікатів (від запиту CSR до випуску, оновлення та відкликання).
- Генерація та дистрибуція конфігураційних файлів VPN (включаючи провіженінг OVPN профілів).
- Оцінка статусу довіри пристроїв та користувачів на основі ABAC-політик безпеки.
- Односторонній провіженінг конфігурацій (IAS → VPN) через розподілений Erlang RPC без прямого зворотного зв'язку під час обробки трафіку шлюзами.
- Узгодження (reconciliation) та виявлення розбіжностей між запланованим станом IAS та фактичним станом шлюзів VPN.

2.3. Вимоги законодавства та міжнародних стандартів

Система повинна розроблятися та функціонувати відповідно до:

- Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закону України «Про електронні довірчі послуги» (впровадження КЕП);
- Закону України «Про захист персональних даних»;
- Закону України «Про основні засади забезпечення кібербезпеки України»;
- Постанови Кабінету Міністрів України № 205 від 21.02.2025 «Про затвердження Порядку використання засобів інформатизації»;
- Нормативних стандартів ДСТУ 3973-2000, ДСТУ 3974-2000 та ДСТУ 3008:2015;
- Національних стандартів криптографічного захисту ДСТУ 4145-2002 та ДСТУ ГОСТ 28147:2009;
- Міжнародних стандартів ISO/IEC/IEEE 42010 (опис архітектури), ISO/IEC/IEEE 29148 (інженерія вимог), рекомендацій NIST та стандартів RFC (RFC 4210, RFC 7030, RFC 5272).

3. Призначення та цілі впровадження

Основною метою впровадження ERP/1: IAS є забезпечення найвищого рівня кібербезпеки інфраструктури Zencrypted за рахунок централізації управління доступами, автоматизації випуску сертифікатів через CMP/EST протоколи, ізоляції приватних ключів на стороні клієнтських пристроїв, та забезпечення повного аудиторського контролю за доступом до корпоративних VPN-мереж.

4. Класифікація вимог

4.1. Простежуваність вимог (Traceability)

Для забезпечення прозорості проектування та відповідності вимогам міжнародного аудиту, в системі реалізується наскрізна простежуваність вимог (traceability). Кожне архітектурне рішення, сутність та бізнес-процес повинні мати чітко визначене простежуване посилання (lineage):

- Від Політик до Технічних вимог: Політики безпеки, визначені в `policy.tex`, безпосередньо транслюються у функціональні та нефункціональні вимоги цього документу.
- Від Технічних вимог до Технічного завдання (ТЗ): Кожна вимога, описана в `ias.tex`, деталізується в `ias_pro.tex` у вигляді конкретних структур даних (Erlang records), алгоритмів та BPE бізнес-процесів.
- Від Технічного завдання до Реалізації та Тестування: Кожне поле сутності та крок процесу пов'язуються з відповідними тестовими сценаріями (Common Test), забезпечуючи повне покриття вимог і запобігаючи впровадженню незатвердженої або надлишкової функціональності.

4.2. Обмеження архітектури: відмова від JWT та OpenID Connect

З метою забезпечення відповідності вимогам національного законодавства та стандартам безпеки державних інформаційних систем високого рівня захисту (assurance), архітектура Модуля IAS категорично відкидає використання JSON Web Tokens (JWT) та OpenID Connect (OIDC) як основних або самостійних механізмів автентифікації та авторизації.

Основні причини та технічні передумови цього рішення базуються на детальному аналізі вразливостей та регуляторних вимог:

- Неприпустимість використання JWT як первинного механізму: Відповідно до аналізу технічних вимог щодо безпеки державних реєстрів [1], JWT є анонімним bearer-токеном (stateless), який пред'являється без повторного криптографічного підтвердження володіння оригінальним приватним ключем. Це суперечить вимогам стандарту NIST SP 800-53 (контроль AU-10 та серія IA) щодо невідкликаності (non-repudiation) та повної підзвітності. Стандартні JWT-бібліотеки мають відомі криптографічні слабкості (вразливості до `alg:none`, key-confusion та header injection), а також не забезпечують нативного зв'язку та логування серійного номера й відбитка сертифіката X.509 на всіх етапах сесії.
- Неприпустимість OpenID Connect (OIDC): Як зазначено у специфікаціях щодо архітектури європейської цифрової ідентичності (EUDI) та регламенту eIDAS [2], стандартний OIDC побудований на централізованій моделі Identity Provider, що створює ризики витоку метаданих та стеження за активністю користувача з боку провайдера ідентифікації. Крім того, OIDC не підтримує вимоги децентралізації, селективного розкриття атрибутів (selective disclosure) та використання криптографічних доказів без використання протоколів CRL/OCSP на стороні верифікатора, що робить його несумісним із регламентом eIDAS 2.0.

Замість цього, у Модулі IAS використовується виключно криптоцентрична архітектура на базі інфраструктури відкритих ключів (PKI) з автентифікацією пристроїв через двосторонній TLS (mTLS) на основі кваліфікованих сертифікатів X.509 відповідно до RFC 5280, з обов'язковою фіксацією унікальних ідентифікаторів сертифіката (серійний номер, SKI, public key) у журналах аудиту.

4.3. Функціональні вимоги

4.3.1. Опис довідників

Система повинна підтримувати систему довідників для класифікації та уніфікації даних авторизації:

- Типи VPN-сервісів (VPNServiceType): OpenVPN (ovpn), WireGuard (wg), IPsec.
- Класи сертифікатів (CertificateClass): Імпортований OVPN (imported_ovpn), Сертифікат запиту (enrollment_certificate), Випущений ідентифікаційний сертифікат (issued_identity_certificate).
- Статуси довіри сертифікатів (TrustStatus): Довірений (trusted), Деградований (degraded), Блокований (blocked), Невідомий (unknown).
- Статуси авторизації пристроїв (DeviceAuthorizationStatus): Готовий (ready), Деградований (degraded), Блокований (blocked), Неповний (incomplete).
- Режими доставки провіженінгу (DeliveryMode): Портативний (portable), Прив'язаний до пристрою (device_bound).
- Статуси транзакцій провіженінгу (ProvisioningStatus): Очікує матеріалів (awaiting_material), Публічний бандл готовий (public_bundle_ready), Готовий до імпорту (ready_for_device_import), Доставлений (delivered).
- Типи інцидентів узгодження (ReconciliationIncidentType): Сирітська конфігурація (orphan_vpn_config), Невідповідність відбитку (fingerprint_mismatch), Застаріла версія ревізії (stale_revision), Несанкціоноване підключення (unauthorized_peer).
- Ролі операторів IAS (IASRole): Адміністратор безпеки (Security Admin), Operator системи (Operator), Аудитор (Auditor), Користувач/Співробітник (User).
- Типи подій логування (LogEventType): Генерація CSR, Випуск сертифіката, Зміна статусу довіри, Провіженінг конфігурації, Інцидент узгодження, Вхід оператора, Блокування доступу.

4.3.2. Опис реєстрових сутностей та їх станів

Основними реєстровими сутностями системи IAS є:

- User (Користувач): Ідентичність співробітника. Стани: Активний, Блокований.
- Device (Пристрій): Опис клієнтського обладнання. Стани: Активний, Непідтверджений, Виведений з експлуатації (Decommissioned).
- Certificate (Сертифікат): Криптографічний сертифікат X.509. Стани: Активний, Прострочений, Відкликаний, Замінений (Superseded).
- SecurityProfile (Профіль безпеки): Набір дозволів та обмежень для ролей. Стани: Активний, Чернетка, Архівний.
- SecurityPolicy (Політика безпеки): Правила авторизації доступу (наприклад, обов'язковість КЕП, обмеження за часом/мережею). Стани: Активний, Чернетка.
- VPNService (VPN-сервіс): Опис конфігурації конкретного шлюзу VPN. Стани: Активний, Зупинений.
- CertificateEnrollment (Запит на випуск): Стан процесу CMP/EST випуску сертифіката. Стани: Створено, Надіслано до CA, Підписано, Відхилено.
- CertificateVerification (Перевірка сертифіката): Результати валідації сертифіката пристрою під час підключення. Стани: Успішно, Помилка валідації.
- ProvisioningTransaction (Транзакція провіженінгу): Стан підготовки та доставки конфігурації на VPN-шлюз. Стани: Створено, Готово до доставки, Доставлено.

4.3.3. Опис бізнес-процесів

Основні процеси системи ідентифікації та авторизації:

1. Процес «Імпорт та аналіз конфігурацій OVPN» (OVPN Import):

- Крок 1: Оператор завантажує існуючий файл конфігурації OpenVPN (.ovpn) для аналізу.
- Крок 2: Система розбирає конфігураційний файл, виділяє сертифікат CA, клієнтський сертифікат, TLS-auth ключ та параметри підключення.
- Крок 3: Система генерує прев'ю-план імпорту (сутності Device, Certificate, VPN Service).
- Крок 4: Оператор затверджує план імпорту.
- Крок 5: Система створює відповідні записи в стійкому сховищі KVS та встановлює зв'язки між ними.

2. Процес «Випуск сертифіката через CMP/EST» (Certificate Enrollment):

- Крок 1: Користувач або пристрій ініціює запит на новий сертифікат, локально генеруючи пару ключів та підписуючи CSR.
- Крок 2: CSR передається в IAS.
- Крок 3: IAS перевіряє права користувача/пристрою згідно з діючим профілем безпеки.
- Крок 4: IAS надсилає запит до CA через протокол CMP або EST.
- Крок 5: CA підписує сертифікат та повертає його в IAS.
- Крок 6: IAS імпортує сертифікат без збереження приватного ключа, реєструє його та пов'язує з відповідним пристроєм.

3. Процес «Оцінка довіри та авторизація пристрою» (Trust Evaluation):

- Крок 1: Пристрій намагається встановити з'єднання з VPN або оновити конфігурацію.
- Крок 2: IAS перевіряє статус сертифіката пристрою (чи не закінчився термін дії, чи не відкликаний через CRL/OCSP).
- Крок 3: IAS аналізує зв'язки пристрою з користувачем та діючі політики безпеки (ABAC).
- Крок 4: Визначення ефективного статусу довіри сертифіката (Trusted, Degraded, Blocked).
- Крок 5: Формування остаточного статусу авторизації пристрою (Ready, Blocked).

4. Процес «Односторонній провіженінг конфігурацій та реконсиляція» (Provisioning and Reconciliation):

- Крок 1: IAS формує канонічні команди провіженінгу з унікальною ревізією.
- Крок 2: IAS доставляє команди на шлюз VPN через розподілений Erlang RPC.
- Крок 3: VPN-шлюз застосовує зміни локально та надсилає повідомлення про виконання через шину подій.
- Крок 4: IAS зчитує статус та оновлює статус транзакції провіженінгу.
- Крок 5: Періодичний фоновий процес звіряє стан наявних конфігурацій шлюзу з базою IAS, виявляючи сирітські профілі (orphans) або застарілі ревізії, та створює інциденти узгодження.

4.3.4. Вимоги до протоколів взаємодії

- Взаємодія IAS → VPN: Розподілений Erlang RPC з використанням механізмів ревізій та транзакційних логів.
- Взаємодія IAS ↔ CA: Протоколи CMP (RFC 4210) через TCP 8829 або EST (RFC 7030) через HTTP 8047 для автоматичного випуску сертифікатів.
- Внутрішні інтерфейси: TLS X.690 DER та серіалізація Erlang External Term Format для процесів авторизації.
- Зовнішні API: REST API (JSON) для інтеграції з корпоративними системами та консолями управління.

4.3.5. Опис прав та привілеїв (ABAC)

Доступ до операцій IAS повинен контролюватися за допомогою моделі ABAC (Attribute-Based Access Control) на основі наступних атрибутів:

- Суб'єкт: роль оператора, посада, ЄДРПОУ підприємства, наявність сертифіката КЕП.
- Об'єкт: рівень чутливості даних (SensitivityLevel), приналежність пристрою до конкретного користувача чи сервісу.
- Умови: поточний час, геолокація запиту, статус довіри пристрою.

4.3.6. Опис валідацій

Система повинна забезпечувати обов'язкову валідацію:

- Відповідності публічного ключа в CSR та випущеному сертифікаті.
- Цілісності ланцюжка сертифікатів CA під час імпорту.
- Термінів дії сертифікатів та перевірки за списками відкликання CRL.
- Відповідності ревізій команд провіженінгу для уникнення race conditions.

4.3.7. Шаблони сповіщень

IAS повинен підтримувати шаблони сповіщень для операторів про критичні події:

- Сповіщення про відкликання сертифіката: надсилання детального звіту аудитору.
- Інцидент узгодження: сповіщення про виявлення несанкціонованої конфігурації на VPN-шлюзі.
- Завершення терміну дії: попередження користувача про необхідність оновлення сертифіката пристрою за 30 днів.

4.3.8. Вимоги до серіалізації

Серіалізація даних у каналах зв'язку повинна підтримувати:

- JSON — для зовнішніх REST API та веб-інтерфейсів.
- ASN.1 / DER (X.690) — для роботи з криптографічними об'єктами та сертифікатами.
- Erlang External Term Format — для швидкої та безпечної взаємодії між Erlang-нодами IAS та VPN.

4.3.9. Вимоги до транспорту

Транспортний рівень взаємодії повинен базуватися на:

- Distributed Erlang RPC — для прямої доставки конфігурацій.
- TLS v1.3 — як обов'язковий протокол для всіх мережевих з'єднань HTTP/REST та CMP/EST.

4.4. Нефункціональні вимоги

4.4.1. Вимоги до архітектури

- Побудова архітектури відповідно до стандарту ISO/IEC/IEEE 42010.
- Розгортання компонентів на базі віртуальної машини Erlang/OTP для забезпечення високої доступності (99.99%) та відмовостійкості.
- Використання бібліотеки KVS для абстракції сховища (сумісність з Mnesia, RocksDB та RocksDB на NVMe).
- Забезпечення агностичності архітектури до моменту затвердження конкретних технічних рішень у ТЗ.

4.4.2. Вимоги до безпеки

- Повна відповідність Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (рівень захисту Г3).
- Використання засобів КЕП формату CAdES-X Long для засвідчення критичних змін та дій операторів.
- Підтримка національних стандартів ДСТУ 4145-2002 для цифрових підписів та ДСТУ ГОСТ 28147:2009 для шифрування.
- Приватні ключі користувачів та пристроїв ніколи не повинні передаватися або зберігатися в системі IAS.

4.4.3. Вимоги до потужності і ємності

- Підтримка одночасної роботи до 100,000 активних пристроїв.
- Час відповіді системи на запити авторизації не повинен перевищувати 50 мс.
- Об'єм сховища повинен розраховуватися з урахуванням збереження логів аудиту протягом щонайменше 3 років.

4.4.4. Вимоги до функціональності логування

- Логування всіх дій користувачів та операторів у захищеному журналі аудиту (Write-Once storage).
- Запис подій у форматі, сумісному зі стеками ELK / Grafana Loki.
- Заборона на запис конфіденційних даних або частин ключів у лог-файли.

4.4.5. Адміністративні вимоги

- Наявність повної настанови адміністратора та оператора безпеки.
- Підтримка автоматичного тестування життєвого циклу без реального підключення зовнішніх сервісів КЕП (через механізми моків/заглушок у тестовому середовищі).

4.4.6. Загальні вимоги до документації та артефактів

- Документування коду та API за допомогою стандартів EDoc та OpenAPI/Swagger відповідно до ДСТУ 3008:2015.

4.4.7. Юридичні вимоги

- Забезпечення ліцензійної чистоти: всі системні компоненти, бібліотеки та їх залежності повинні мати відкритий вихідний код (Open Source) з ліцензіями типу Apache 2.0, MIT або BSD, що не накладають додаткових фінансових зобов'язань на Замовника.

5. Додаток А. Специфікація реєстрових сутностей (для ТЗ)

5.1. А.1. Сутність «Користувач» (User)

Довідкова сутність, що містить ідентифікаційні дані оператора або кінцевого користувача системи.

- Унікальний ідентифікатор користувача.
- Прізвище, ім'я, по батькові.
- Посада та табельний номер.
- Код ЄДРПОУ підприємства.
- Статус облікового запису (активний, заблокований).
- Список призначених ролей та атрибутів доступу.

5.2. А.2. Сутність «Пристрій» (Device)

Реєстрова сутність, що представляє кінцеву VPN-клієнтську точку.

- Унікальний ідентифікатор пристрою.
- Тип пристрою (мобільний, робоча станція, шлюз).
- Посилання на пов'язаний сертифікат доступу.
- Посилання на активний VPN-сервіс.
- Статус пристрою (активний, тимчасово заблокований, виведений з експлуатації).
- Відносне посилання на файл приватного ключа на пристрої (без самого тіла ключа).

5.3. А.3. Сутність «Криптографічний сертифікат» (Certificate)

Реєстрова сутність, що містить метадані сертифіката X.509.

- Унікальний ідентифікатор сертифіката (серійний номер).
- Тема сертифіката (Subject Distinguished Name).
- Відбиток сертифіката (SHA-256 fingerprint).
- Публічний PEM-блок сертифіката.
- Клас сертифіката (imported, enrollment, issued).
- Дати початку та закінчення дії сертифіката.
- Статус довіри сертифіката (trusted, degraded, blocked).

5.4. A.4. Сутність «Транзакція провіженінгу» (ProvisioningTransaction)

Об’єкт, що описує підготовку та хід доставки конфігурації.

- Унікальний ідентифікатор транзакції.
- Посилання на пристрій та користувача.
- Посилання на сертифікат та VPN-сервіс.
- Режим провіженінгу (portable, device_bound).
- Номер ревізії конфігурації.
- Статус доставки команди (awaiting_material, ready_for_delivery, delivered).

6. Додаток Б. Технічні деталі реалізації процесів та валідацій

6.1. Б.1. Алгоритм перевірки статусу довіри пристрою (Trust Evaluation Logic)

Вхідними даними для оцінки є об'єкти `Device` та `Certificate`.

1. Перевірка терміну дії: Якщо поточний час $T >$ expires_at, статус довіри сертифіката встановлюється в Blocked, а статус пристрою в Incomplete.
2. Перевірка за списками CRL/OCSP: Сервіс перевіряє статус серійного номера сертифіката. У разі наявності в списку відкликаних — статус довіри стає Blocked.
3. Аналіз деградації пристрою: Якщо пристрій не виходив на зв'язок більше 30 днів або зафіксовано спробу підключення з нетипової геолокації, статус довіри встановлюється в Degraded.
4. Оцінка ABAC-правил: Перевіряються атрибути суб'єкта. Якщо користувача заблоковано в кадровій системі — статус пристрою стає Blocked.

6.2. Б.2. Алгоритм узгодження станів (Reconciliation Loop)

Регулярний фоновий процес виконує порівняння конфігурацій:

1. Запит списку активних пірів та їх ревізій із шлюзів VPN через Erlang RPC.
2. Порівняння списку пірів зі списком пристроїв, які мають статус авторизації Ready в IAS.
3. Якщо пір присутній на VPN, але відсутній або заблокований в IAS — генерується інцидент узгодження типу orphan_vpn_config.
4. Якщо версії ревізії конфігурації на VPN та IAS відрізняються — генерується інцидент типу stale_revision.
5. Автоматичне виправлення (auto-reconciliation) запускається оператором або за політикою системи, надсилаючи відповідні команди `decommission` або `upsert`.

Література

[1] Технічні вимоги: Про неприпустимість використання JWT токенів як самостійного механізму в державних системах, 2026. `https://5ht.co/jwt.pdf`

[2] Технічні вимоги: Щодо неприпустимості використання OpenID Connect токенів при наявності eIDAS/EUDI у вимогах, 2026. `https://5ht.co/openid.pdf`