ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

Технологія захищеного обміну документами на основі інфраструктури відкритих ключів

Виконав студент 6 курсу, групи БСЗМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Рибаков Артур Юрійович
(прізвище та ініціали)
Керівник Борсуковський Ю.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ **3**

ВСТУП 4

1 АНАЛІЗ ВИКОРИСТАННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ В СУЧАСНОМУ ПІДПРИЄМСТВІ 6

1.1. Аналіз завдань і роль інфраструктури відкритих ключів як основа бізнес-процесів організації 6

1.2. Аналіз стандартів інфраструктури відкритих ключів 9

2 МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ В ОРГАНІЗАЦІЇ 29

2.1 Компоненти інфраструктури відкритих ключів в організації 29

2.2. Центр сертифікації 32

2.3. Складові сертифіката 36

2.4. Ієрархії CA 42

3 РОЗРОБКА РЕКОМДАЦІЙ СТВОРЕННЯ ЦЕНТРУ DIGICERT ONE ENTERPRISE PKI MANAGER 47

3.1 Варіант застосування інфраструктури інфраструктури відкритих ключів на основі інтеграції Microsoft Endpoint Manager і DigiCert ONE 47

3.2 Компоненти корпоративного шлюзу PKI DigiCert ONE Enterprise PKI Manager 52

3.3 Розробка рекомендацій щодо використання PKI DigiCert ONE Enterprise PKI Manager 58

ВИСНОВКИ 60

ПЕРЕЛІК ПОСИЛАНЬ 61

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

TTP - Trusted Third Party

CRL – Certificate Revocation Lists

CA - Certification Authorities

PEM - Internet Privacy Enhanced Mail

PER - Packed Encoding Rules

DER - distinguished encoding rules

PSE - Personal Security Environment

TSA - Time Stamping Authority

ВСТУП

Актуальність дослідження. Керування привілейованими обліковими даними (PAM) — це домен у межах управління ідентифікацією та доступом (IdAM), який зосереджується на моніторингу та контролі використання привілейованих облікових даних. До привілейованих облікових даних належать локальні та доменні адміністративні облікові записи, екстрені облікові записи, облікові записи керування програмами та облікові записи служби. Ці облікові записи забезпечують розширений, часто необмежений, доступ до основних IT-ресурсів і технологій, тому зовнішні та внутрішні зловмисники прагнуть отримати до них доступ. Дуже важливо відстежувати, перевіряти, контролювати та управляти використанням привілейованими обліковими даними.

Організації можуть додати рівень безпеки між користувачами та привілейованими обліковими записами, до яких вони мають доступ, і включає типові сценарії використання для вирішення конкретних проблем, з якими стикається організація. Архітектура PAM показує, як моніторинг, аудит і елементи управління автентифікацією можуть поєднуватися, щоб запобігти несанкціонованому доступу та дозволити швидке виявлення несанкціонованого використання привілейованих облікових даних. Таким чино необхідно визначити методи та засоби управління привілейованими даними інформаційної системи організації. Це дозволить запобігти несанкціонованому доступу до інформаційної системи організації. Вищенаведені аргументи актуалізують дослідження щодо управління привілейованими даними інформаційної системи організації.

Об’єкт дослідження – процес управління привілейованим доступом інформаційної системи організації.

Предмет дослідження – технологія управління привілейованим доступом інформаційної системи організації.

Мета роботи – розробити варіанти технології управління привілейованим доступом інформаційної системи організації та рекомендації щодо застосування технології в організації.

Наукові завдання:

- провести аналіз технології захищеного обміну документами в організації на основі інфраструктури відкритих ключів.;
- проаналізувати методи та засоби управління привілейованими користувачами інформаційної системи організації;
- розробити варіант технології технології захищеного обміну документами в організації на основі інфраструктури відкритих ключів. та розробити рекомендації фахівцям з кібербезпеки щодо застосування обраної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту привілейованих даних користувачів інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці варіанту етапів роботи технології захищеного обміну документами в організації на основі інфраструктури відкритих ключів. а також у розробці рекомендацій щодо використання даної технології в метою виявлення забезпечення цілісності та конфіденційності.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ВИКОРИСТАННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ В СУЧАСНОМУ ПІДПРИЄМСТВІ

1.1. Аналіз завдань і роль інфраструктури відкритих ключів як основа бізнес-процесів організації

Сьогодні існує актуальна проблема створення, впровадження, безпечне і надійне функціонування інфраструктури відкритих ключів для ведення бізнес-процесів організацій. Основним завданням ІВК є надання установам, юридичним та фізичним особам послуг із забезпечення цілісності і достовірності інформації та різних даних, що представлені в електронному вигляді, а саме електронних документів та повідомлень, програмного забезпечення, що ними використовуються.

Відповідно до існуючих міжнародних норм та вимог усім користувачам мають надаватися послуги з забезпечення цілісності та доступності інформації, а в за необхідністю і конфіденційність, на всіх етапах життєвого циклу. Життєвий цикл складається з виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрування, приймання, отримання, передавання Ці процеси здійснюються в системі за допомогою комплексу технічних та/або програмних засобів. [1]

Одним з таки комплексних засобів забезпечення надання вказаних послуг є застосування електронного цифрового підпису (ЕЦП). На світовому рівні та в усіх технологічно розвинутих державах застосування цифрового підпису під час обробки інформації є звичайною практикою. Для розв’язання цих завдань створюється інфраструктура відкритих ключів. Україна в цьому напрямку зробила достатньо важливі кроки. Прийнято закони “Про електронні документи та електронний документообіг”, “Про електронний цифровий підпис”, ряд постанов Кабінету Міністрів та наказів ДСТСЗІ СБ України. Крім того, введено у дію національний

стандарт України ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” (далі – ДСТУ 4145-2002).

Мета та завдання створення інфраструктури відкритих ключів є надання фізичним та юридичним особам, банківським та фінансовим установам, органам місцевого самоврядування та іншим суб’єктам послуг щодо забезпечення цілісності та справжності інформації, документів, повідомлень та програмного забезпечення, які представлені в електронному вигляді та використовуються суб’єктами на усіх етапах життєвого циклу за допомогою використання сертифікатів відкритих ключів. Використання сертифікатів відкритих ключів забезпечує надійний зв’язок відкритих ключів з користувачами, дозволяє іншим користувачам перевірити наявність цього зв’язку та одержати необхідні послуги з управління ключовими даними. У рамках ІВК забезпечується підтвердження цілісності інформації, що підписується особистим ключем користувача та ідентифікація підписувача (підтвердження справжності інформації, яка ним підписана). ІВК має інтегрувати сертифікати відкритих ключів, криптографічні перетворення з відкритими ключами та уповноважені на сертифікацію органи в єдину організаційно-технічну структуру. [1]

Інтеграція ІВК з інформаційною системою організацій дозволить вирішити наступні задачі [1]:

реєстрація користувачів;

реєстрація сертифікатів відкритих ключів користувачів;

реалізація процедури обслуговування сертифікатів, тобто формування та засвідчення чинності відкритого ключа, видача (випуск), розповсюдження, скасування, блокування, поновлення, облік чинних сертифікатів, перевірка статусу сертифікатів та зберігання (архівування) сертифікатів;

об’єднання сертифікатів відкритих ключів у спеціальні довідники сертифікатів та їх обслуговування;

взаємодія з іншими уповноваженими органами системи ЕЦП, у тому числі з відповідними уповноваженими органами інших країн;

надання інших додаткових послуг щодо управління ключовими даними та сертифікатами, в тому числі в частині асиметричного (направленого) шифрування та надання послуг з управління привілеями.

Впровадження послуг ЕЦП у діяльність дозволить організаціям:

впровадити новітні інформаційні технології електронного документообігу у практику повсякденної діяльності;

розширити можливість інтеграції;

підвищити конкурентоспроможність українських організацій;

забезпечити цілісність та справжність (автентичність) інформації, представленої в електронному вигляді;

при затвердженні правових норм використання ЕЦП дозволяє забезпечувати легітимний електронний документообіг та реалізувати правові відносини, такі як при використанні традиційних паперових документів.

Інфраструктура відкритого ключа (PKI) — це механізм, який пов’язує сертифікат відкритого ключа з відповідним ідентифікатором користувача через довірену третю сторону. Основними елементами PKI є:

Центр сертифікації (CA): довірена організація, яка видає сертифікати для використання іншими організаціями. [2]

Сертифікат: електронний документ, який містить цифровий підпис для зв’язування відкритого ключа з ідентифікатором.

Відкритий/приватний ключ: пара ключів, які використовуються в асиметричних криптографічних алгоритмах. Відкритий ключ розповсюджується в сертифікаті, який може бути підтверджений за допомогою ЦС іншими об’єктами. Закритий ключ зазвичай зберігається на локальному комп’ютері власника сертифіката.

У системі програми мають сертифікати користувачів, а кожен менеджер черги має дві пари криптографічних ключів (ключі підпису та ключі шифрування). Система

використовує службу каталогів, а не ЦС, як довірену третю сторону для розповсюдження відкритих сертифікатів і ключів.

Сертифікати користувача

Сертифікат користувача використовується для підпису повідомлення програми, щоб забезпечити функцію захисту цілісності повідомлення на рівні повідомлень.

1.2. Аналіз стандартів інфраструктури відкритих ключів

PKI визначає управління, а не межі управління бізнес-процесами організацій.

З нескінченним збільшенням кількості нових пристроїв, систем і підключень традиційні корпоративні межі більше не існують. Віддалена та гібридна робоча сила робить захист цієї розгалуженої корпоративної інфраструктури ще складнішим. Незважаючи на те, що ініціативи Cybersecurity Mesh і Zero Trust пропонують схеми для забезпечення відомості та довіри всьому, що підключається до вашого підприємства, вам все одно потрібні правильні інструменти для розгортання великого та складного корпоративного середовища та керування ним. [2]

Основні RFC, пов’язані з PKI.

Голова Робочої групи PKIX IETF назвав їх найважливішими RFC щодо безпеки відкритих ключів. Усі інші RFC, пов’язані з PKI, перераховані нижче.

RFC3820 – Профіль сертифіката проксі-сервера інфраструктури відкритого ключа Інтернету X.509 (PKI)

RFC2560 - Інфраструктура відкритих ключів Інтернету X.509 Онлайновий протокол статусу сертифіката - OCSP

RFC2527 – Структура політики сертифікатів і практики сертифікації інфраструктури відкритих ключів Інтернету X.509. Замінено RFC 3647.

RFC3647 - Інфраструктура відкритих ключів Інтернету X.509. Політика сертифікатів і практика сертифікації. Замінює RFC 2527.

RFC2511 – Формат повідомлення запиту на сертифікат Інтернет X.509

RFC2797 - Повідомлення керування сертифікатами через CMS

RFC3039 - Профіль кваліфікованих сертифікатів інфраструктури відкритих ключів Інтернету X.509

RFC3161 - Протокол міток часу (TSP) інфраструктури відкритих ключів Інтернету X.509

RFC3281 – профіль сертифіката атрибутів Інтернету для авторизації

Стандартизація PKI була проведена кількома різними органами, що розробляють стандарти. Загалом було докладено зусиль для гармонізації результатів цієї роботи. Особливої уваги заслуговують такі.

• ITU-T. Цей орган проклав шлях у стандартизації PKI, опублікувавши в 1988 році перше видання Рекомендації X.509 [5], що надає стандартизований формат для сертифікатів відкритих ключів і списків відкликаних сертифікатів (CRL). У співпраці з ISO/IEC ITU-T продовжив розробку рекомендації X.509 (див. [5]).

• Інженерна робоча група Інтернету (IETF). IETF відповідає за стандарти, що регулюють роботу Інтернету. За останні п'ять років або близько того, IETF розробляє набір стандартів, що регулюють роботу PKI на основі X.509 для використання в Інтернеті. Цей набір стандартів має назву PKIX. Зауважте, що проект в Інтернеті [6] містить корисний загальний вступ до PKIX.

• ISO/IEC. Окрім спільної роботи з ITU-T над X.509 (див. [7]), ISO/IEC також розробляє серію більш загальних стандартів, пов’язаних з PKI, включаючи стандарти щодо управління сертифікатами та служб відміток часу.

Типи стандартів PKI

Перш ніж розглядати окремі стандарти, пов’язані з PKI, спочатку розглянемо, які типи проблем стосуються цих стандартів. Тобто ми розглядаємо, які сфери функціонування PKI охоплюються стандартами.

• Найфундаментальнішим питанням PKI є формат сертифікатів відкритих ключів.

• Керування сертифікатами – це термін, який використовується для охоплення низки різних типів взаємодії між центрами сертифікації (CA) та їхніми клієнтами, включаючи такі питання, як початкова реєстрація, запити на сертифікати та запити на відкликання.

• Після створення сертифікатів необхідно, щоб користувачі сертифікатів могли отримати їх із місця, де вони зберігаються.

• Після сертифікації може виникнути необхідність вилучити відкритий ключ із використання до закінчення терміну дії, зазначеного в сертифікаті – це відомо як відкликання. У результаті виникає потреба в тому, щоб користувач сертифіката міг визначити статус сертифіката, тобто чи був він відкликаний.

• Однією з головних причин для запровадження послуг з відмітками часу була підтримка довгострокового використання підписаних документів, зокрема надання можливості документу з цифровим підписом мати чинність після закінчення терміну дії або відкликання відкритого ключа.

• Існує цілий ряд інших служб довіреної третьої сторони (TTP), пов’язаних із PKI, і деякі з останніх розробок стандартів у цій сфері є предметом розділу 7.

• Нарешті, в основі будь-якого ефективного використання сертифікатів відкритих ключів має бути розуміння того, що означає сертифікат. Це залежить від політики сертифікації та заяв про практику сертифікації ЦС.

Сертифікати стандартів

Розробка стандартів сертифікатів відкритих ключів

Перша робота з розробки стандартів PKI передує терміну PKI на кілька років. Те, що стало відомим як формат сертифіката X.509, було вперше стандартизовано в 1988 році [5] як частину першого видання рекомендацій щодо служб каталогів ITU-T X.500 (зверніть увагу, що тоді їх називали рекомендаціями CCITT).

Перше видання узгодженого стандарту ISO/IEC, ISO 9594-8, було опубліковано через кілька років. Пізніше було опубліковано дві наступні версії узгоджених

рекомендацій ITU-T і стандартів ISO/IEC, і щоб уникнути плутанини, три різні формати сертифікатів, визначені в цих документах, називаються сертифікатами X.509 версії 1, 2 і 3.

Початкова робота над X.509 була виконана в рамках розробки рекомендацій серії каталогів X.500. Основним початковим «замовником» стандартизованих сертифікатів відкритих ключів були паралельні серії рекомендацій X.400, що визначають функціонування системи електронної пошти. Версія стандартів X.400 1988 року включала широкий спектр функцій безпеки, керування ключами для яких базувалося на використанні сертифікатів X.509. Цікаво, що хоча рекомендації X.400 навряд чи запалили світ, сертифікат відкритого ключа X.509 формат домінує в полі.

Після публікації першого видання рекомендації X.509 наступним основним замовником формату сертифіката X.509 знову стала захищена система електронної пошти – цього разу система Internet Privacy Enhanced Mail (PEM) [7]. Ця система знову використовувала сертифікати X.509 як основу для керування ключами – однак PEM вимагав ряд додаткових функцій сертифіката, які були включені у формат сертифіката X.509 версії 2 [8]. Подальший зростаючий інтерес до розгортання X.509 PKI виявив потребу в подальших доповненнях до формату сертифіката, і вони були включені у формат сертифіката версії 3, [5], [7].

Сертифікати X.509

Тепер ми розглянемо трохи докладніше основні елементи в сертифікаті, створеному відповідно до стандарту X.509 версії 3, [5], [7]. Формат сертифіката X.509 визначено мовою під назвою Abstract Syntax Notation One (ASN.1) [9].

ASN.1 широко використовується для специфікації протоколів зв'язку ITU-T і ISO (та інших стандартів). Метою ASN.1 є наявність стандартизованої та незалежної від платформи мови для вираження структур даних, а також стандартизованого набору правил для перетворення значень визначеного типу в потік байтів. Потім цей потік байтів можна надіслати по каналу зв'язку [9] встановлюються нижніми рівнями в стеку протоколів зв’язку, напр. TCP/IP або інкапсульовані в UDP-пакети. В

результаті дві різні програми, написані на двох абсолютно різних мовах програмування, працюють на різних комп'ютерах, різні внутрішні представлення даних можуть обмінюватися екземплярами структурованих типів даних. Це звільняє програміста від великої кількості роботи, оскільки для обробки транспортного формату даних не потрібно писати код.

Коли перша рекомендація ITU-T щодо ASN.1 була опублікована в 1988 році, вона супроводжувалася Базовими правилами кодування (BER) як єдиним варіантом кодування. BER є дещо докладним протоколом. Він використовує так званий підхід TLV (тип, довжина, значення) до кодування, у якому кожен елемент кодування містить певну інформацію про тип, деяку інформацію про довжину, а потім значення цього елемента. Якщо елемент сам по собі структурований, то частина елемента Value сама по собі є серією вбудованих компонентів TLV, будь-якої необхідної глибини. Таким чином, BER не є компактним кодуванням, але його досить швидко та легко створити.

Більш компактне кодування досягається за допомогою Правил упакованого кодування (PER) [8], які були введені разом із переглянутою рекомендацією ASN.1 у 1994 році. PER використовує інший підхід, ніж той, який прийнято BER. Перша відмінність полягає в тому, що частина T (тип) опущена з кодувань, а будь-які теги в нотації повністю ігноруються. Друга відмінність полягає в тому, що PER повністю враховує інформацію про підтип, тоді як BER повністю її ігнорує. PER використовує інформацію підтипу, наприклад, щоб пропускати поля довжини, коли це можливо. Таким чином, використання PER призводить до компактного кодування, для створення якого потрібно набагато більше обчислень, ніж для BER.

Синтаксис сертифіката «верхнього рівня» X.509 v3 наведено нижче (синтаксис однаковий для всіх трьох версій сертифіката X.509). Для обчислення підпису сертифікат кодується за допомогою «тегу, довжини, значення» ASN.1, розрізнених правил кодування (DER), [10].

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate        TBSCertificate,
        signatureAlgorithm    AlgorithmIdentifier,
        signatureValue        BIT STRING  }
```

Поле е містить цифровий підпис, обчислений за ASN.1 DER-кодований Тобто кодований DER tbsCertificate ASN.1 використовується як вхідні дані для функції підпису. Потім це значення підпису кодується як ASN.1 і включається в поле підпису сертифіката. Поле містить ідентифікатор для криптографічного алгоритму, який використовується ЦС для підписання цього сертифіката. Ідентифікатор алгоритму визначається такою структурою ASN.1.

```
AlgorithmIdentifier  ::=  SEQUENCE  {
      algorithm          OBJECT IDENTIFIER,
      parameters         ANY DEFINED BY
            algorithm OPTIONAL  }
```

Ідентифікатор алгоритму використовується для ідентифікації криптографічного алгоритму. Компонент OBJECT IDENTIFIER ідентифікує алгоритм (наприклад, DSA з SHA-1). Вміст поля додаткових параметрів змінюватиметься залежно від визначеного алгоритму. Це поле має містити той самий ідентифікатор алгоритму, що й поле підпису в послідовності tbsCertificate.

Поле . tbsCertificate містить назви суб'єкта та емітента, паблік ключ, пов’язаний із суб’єктом, термін дії та інша пов’язана інформація.

TbsCertificate може також включати розширення (назва, дана додаткові поля, введені в сертифікати версії 3 X.509).

Використання ключа. Розширення використання ключа визначає призначення (наприклад, шифрування, підпис, підпис сертифіката) ключа, що міститься в сертифікаті. Обмеження використання може застосовуватися, коли потрібно обмежити ключ, який можна використовувати для кількох операцій.

• Політики щодо сертифікатів. Політика сертифікатів — це іменований набір правил, який вказує на застосовність сертифіката до певної спільноти та/або класу програм із загальними вимогами безпеки. Наприклад, конкретна політика сертифіката може вказувати на застосовність типу сертифіката для автентифікації електронних транзакцій обміну даними для торгівлі товарами в заданому діапазоні цін.

• Альтернативна назва предмета. Розширення альтернативних імен суб'єктів дозволяє прив'язувати додаткові ідентифікатори до суб'єкта сертифіката. Визначені параметри включають адресу електронної пошти в Інтернеті, ім'я DNS, IP-адресу та уніфікований ідентифікатор ресурсу (URI). Існують інші варіанти, включаючи повністю локальні визначення. Можливе кілька форм імен і кілька екземплярів кожної форми імен бути включені. Кожного разу, коли такі ідентифікаційні дані мають бути прив'язані до сертифіката, необхідно використовувати розширення альтернативного імені суб'єкта (або альтернативного імені емітента).

Профіль сертифіката PKIX

Як має бути зрозуміло з опису вище, формат сертифіката X.509 є дуже гнучким і дозволяє розробнику вибирати велику кількість варіантів, які використовують стандарт. У результаті на практиці необхідно визначити профіль для X.509, вказавши, які параметри слід використовувати. RFC 2459, [8], є профілем PKIX X.509. Метою RFC 2459 є полегшення використання сертифікатів X.509 в Інтернет-додатках для тих спільнот, які бажають використовувати технологію X.509. Такі програми можуть включати Інтернет, електронну пошту, автентифікацію користувачів і IPsec. Щоб усунути деякі перешкоди для використання сертифікатів X.509, RFC 2459 визначає профіль для сприяння розвитку систем керування сертифікатами, розробці інструментів додатків і сумісності, визначеній політикою. Ряд значень AlgorithmIdetifier визначено в профілі PKIX. Приклади комбінацій методів підпису та хеш-функцій, для яких визначено ідентифікатори, включають наступне:

• RSA з MD2,

• RSA з MD5,

• RSA з SHA-1, [41],

• DSA, [42] з SHA- 1.

Власні формати сертифікатів

Крім міжнародних стандартних форматів сертифікатів, існує низка інших форматів сертифікатів, визначених для використання в окремих доменах програм. Перерахувати їх усі вийде за рамки роботи, але згадаємо один, який має певне практичне значення.

Це «сертифікат EMV» [11], визначений у стандартах Europay-MasterCard-Visa (EMV), що регулює обмін даними між платіжною смарт-карткою (наприклад, кредитною або дебетовою карткою) і торговим терміналом. Основною причиною розробки сертифікатів EMV (на відміну від прийняття сертифікатів X.509) була необхідність мінімізації довжини сертифікатів. У середовищі картки/терміналу не вистачає як місця для зберігання, так і пропускної здатності зв'язку.

Сертифікат EMV кодується за допомогою техніки довжини тегу-значення, подібно до BER; однак кількість полів набагато менша, ніж для X.509. Крім того, використаний алгоритм підпису (відповідно до ISO/IEC 9796-2) мінімізує вимоги до зберігання даних/пропускної здатності, дозволяючи відновити якомога більше даних із підпису.

Обговорюючи стандарти, що регулюють створення та формат сертифікатів, варто також коротко згадати стандарти для криптографічних методів, які використовуються як частина процесів створення та перевірки сертифікатів. Основними для створення сертифіката відкритого ключа є два типи криптографічної функції:

• схема цифрового підпису та

• криптографічна хеш-функція (майже незмінно використовується як частина схеми підпису).

Схеми цифрового підпису визначені в ряді різних стандартів, зокрема в IEEE P1363, ISO/IEC 9796, ISO/IEC 14888, [26], NIST FIPS PUB 186-2, PKCS №1, Хеш-

функції також визначені в ряді стандартів, включаючи ISO/IEC 10118 і NIST FIPS PUB 180-1, [12, 13].

Керування сертифікатами

Далі розглянемо стандарти для керування сертифікатами, тобто для протоколів, що керують зв’язком між клієнтом ЦС і самим ЦС. Зауважте, що в середовищах, де роль центру реєстрації (RA) відрізняється від ролі CA, частина цих протоколів може фактично здійснюватися між RA та клієнтом, а не між CA та клієнтом.

Протокол керування сертифікатами

Протокол керування сертифікатами PKIX (CMP) описано в RFC 2510. На високому рівні набір операцій, для яких визначено повідомлення керування в RFC 2510, можна згрупувати таким чином.

1. Створення ЦС: під час створення нового ЦС необхідні певні кроки (наприклад, створення початкових CRL, експорт відкритого ключа ЦС).

2. Ініціалізація кінцевого об’єкта: це включає імпорт відкритого ключа ЦС до кінцевого об’єкта та запит інформації про параметри, які підтримує об’єкт керування PKI.

3. Сертифікація: різні операції призводять до створення нових сертифікатів:

• Первинна реєстрація/сертифікація. Це процес, за допомогою якого кінцева сутність спочатку повідомляє про себе ЦС або RA, перш ніж ЦС видає сертифікат або сертифікати для цієї кінцевої сутності. Кінцевим результатом цього процесу (якщо він є успішним) є те, що ЦС видає сертифікат для відкритого ключа кінцевої сутності, повертає цей сертифікат кінцевій сутності та/або розміщує цей сертифікат у загальнодоступному сховищі.

Цей процес може включати і зазвичай включатиме кілька «етапів», зокрема ініціалізацію обладнання кінцевого суб’єкта. Наприклад, обладнання кінцевого суб’єкта має бути безпечно ініціалізовано відкритим ключем центру сертифікації, який використовуватиметься для перевірки шляхів сертифіката. Крім того, кінцеву сутність зазвичай необхідно ініціалізувати за допомогою власної пари ключів.

• Оновлення пари ключів. Кожну пару ключів потрібно регулярно оновлювати (тобто замінювати новою парою ключів), а також видавати новий сертифікат.

• Оновлення сертифіката. Коли термін дії сертифікатів закінчується, вони можуть бути «оновлені», якщо нічого суттєвого в середовищі не змінилося.

• Оновлення пари ключів CA. Як і у випадку з кінцевими об'єктами, пари ключів ЦС потрібно регулярно оновлювати; однак потрібні інші механізми.

• Запит на перехресну сертифікацію. Один ЦС запитує видачу крос-сертифікату від іншого ЦС. Для цілей цього стандарту визначено такі терміни. «Крос-сертифікат» — це сертифікат, у якому ЦС суб'єкта та ЦС видавця є різними, а SubjectPablicKeyInfo містить ключ перевірки (тобто сертифікат був виданий для пари ключів підпису суб'єкта ЦС). Якщо необхідно більш точно розрізнити, можна використовувати такі терміни: крос-сертифікат називається «міждоменним крос-сертифікатом», якщо ЦС суб'єкта та емітента належать до різних адміністративних доменів; в іншому випадку це називається «внутрішньодоменним крос-сертифікатом».

• Оновлення крос-сертифікату: схоже на звичайне оновлення сертифіката, але включає крос-сертифікат.

4. Операції виявлення сертифікатів/CRL: деякі операції керування PKI призводять до публікації сертифікатів або CRL.

• Публікація свідоцтва. Постаравшись виготовити сертифікат, потрібні певні засоби для його публікації. Це може включати використання LDAPv2.

• Публікація CRL. Щодо публікації свідоцтва.

5. Операції відновлення. Деякі операції керування PKI використовуються, коли кінцевий суб'єкт «втратив» своє середовище персональної безпеки (PSE), тобто локальне сховище для матеріалів, пов'язаних із безпекою.

• Відновлення пари ключів. Як варіант, матеріали ключів клієнта користувача (наприклад, особистий ключ користувача, який використовується для цілей дешифрування) можуть бути резервні копії CA, RA або системи резервного копіювання ключів, пов'язаної з CA або RA. Якщо організації потрібно відновити ці

резервні копії ключових матеріалів (наприклад, через забутий пароль або втрачений файл), для підтримки такого відновлення може знадобитися обмін протоколами.

6. Операції відкликання. Деякі операції PKI призводять до створення нових записів CRL та/або нових CRL:

• Запит на відкликання. Уповноважена особа повідомляє ЦС про нестандартну ситуацію, що вимагає відкликання сертифіката.

7. Операції PSE: Хоча визначення операцій PSE (наприклад, переміщення PSE, зміна PIN-коду тощо) виходить за межі його сфери, RFC 2510 визначає PKIMessag, який може стати основою таких операцій.

Як зазначено в RFC 2510, важливо зазначити, що онлайн-протоколи не є єдиним способом реалізації вищезазначених операцій. Для всіх операцій існують офлайн-методи досягнення того самого результату, а специфікація RFC 2510 не вимагає використання онлайн-протоколів. Наприклад, коли використовуються апаратні маркери, багато операцій можуть бути виконані як частина фізичної доставки маркерів.

RFC 2510 визначає набір стандартних повідомлень, що підтримують описані вище операції. Також визначено протоколи для передачі цих обмінів у різних середовищах (на основі файлів, онлайн, електронною поштою та на основі Інтернету).

Повідомлення із запитом на сертифікат

В основі RFC 2510 лежить визначення повідомлення із запитом на сертифікат (CRM), у якому суб’єкт відкритого ключа запитує в ЦС новий сертифікат. Формат цього повідомлення визначено в окремому документі, RFC 2511, [14].

Повідомлення із запитом на сертифікат складається із запиту на сертифікат, додаткового поля підтвердження володіння (POP) і додаткового поля реєстраційної інформації.

```
CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg

CertReqMsg ::= SEQUENCE {
    certReq   CertRequest,
    pop       ProofOfPossession  OPTIONAL,
    -- content depends upon key type
    regInfo   SEQUENCE SIZE(1..MAX) of AttributeTypeAndValue
OPTIONAL }
```

Поле підтвердження володіння використовується для демонстрації того, що об’єкт, який буде пов’язано із сертифікатом, насправді володіє відповідним закритим ключем. Це поле може обчислюватися через вміст поля CERTREQ і змінюється за структурою та вмістом залежно від типу алгоритму відкритого ключа та режиму роботи.

Щоб запобігти певним атакам і дозволити CA/RA належним чином перевірити дійсність прив’язки між кінцевим об’єктом і парою ключів, описані тут операції керування PKI дають змогу кінцевому об’єкту довести, що він володіє (тобто може використовувати) приватний ключ, що відповідає відкритому ключу, для якого запитується сертифікат. Даний CA/RA може вільно вибирати, як застосовувати POP (наприклад, позасмугові процедурні засоби проти внутрішньосмугового повідомлення CRMF) у своїх обмінах сертифікацією (тобто це може бути проблемою політики). Однак згідно з RFC 2511 центри сертифікації/розпорядження повинні запроваджувати POP певними засобами; зазначеною причиною цього є те, що використовується багато операційних протоколів, відмінних від PKIX, які явно не перевіряють зв’язок між кінцевою сутністю та закритим ключем.

POP можна виконати різними способами залежно від типу ключа, для якого запитується сертифікат. Наприклад, для ключів підпису кінцева сутність може підписати значення, щоб підтвердити володіння закритим ключем.

Поле REGInfo має містити лише додаткову інформацію, пов’язану з контекстом запиту на сертифікацію, якщо така інформація потрібна для виконання запиту на сертифікацію. Ця інформація може містити контактну інформацію абонента, платіжну

інформацію або іншу допоміжну інформацію, корисну для виконання запиту на сертифікацію.

Інформацію, безпосередньо пов’язану із вмістом сертифіката, слід включити до вмісту SertReg. Однак включення додаткового вмісту SertReg за допомогою RA може зробити спливаюче поле недійсним. Тому дані, призначені для вмісту сертифіката, можуть бути надані в REGInfo.

Стандарт менеджменту сертифікатів ISO/IEC

Протоколи, дуже схожі на ті, що визначені в RFC 1510 і 1511, також визначені в проекті міжнародного стандарту ISO/IEC 15945.

Доступ до сертифікатів Зрозуміло, що для користувачів сертифікатів (бажаючих перевірити зв’язок між відкритим ключем і користувачем) буде загальна вимога мати стандартні засоби доступа до сховища сертифікатів. Розглянемо два різні стандартизовані підходи до надання цього доступу. Зауважимо, що більш детальне порівняння двох підходів наведено в [3].

1) Служба довідників

Як уже згадувалося, рекомендація X.509 насправді є лише частиною серії рекомендацій ITU-T X.500, що стосуються Служби каталогів. Ці рекомендації X.500 визначають, як користувачі служби каталогів можуть отримати доступ до цієї служби отримувати інформацію про інші суб’єкти, включно з їхнім сертифікатом відкритого ключа. Рекомендації також визначають, як можна отримати CRL (у форматі, визначеному в X.509).

2) Отримання сертифіката за допомогою LDAP версії 2

Протокол доступу до сертифіката PKIX визначено в RFC 2559, [12] (див. також RFC 2587). Протокол, описаний у RFC 2559, призначений для задоволення деяких робочих вимог до Інтернету X.509 PKI. Зокрема, у цьому документі розглядаються вимоги щодо надання доступу до сховищ PKI для цілей отримання інформації PKI, включаючи сертифікати та CRL. RFC 2559 також розглядає вимоги щодо додавання, видалення та зміни інформації PKI у сховищі.

Механізм базується на протоколі легкого доступу до каталогу (LDAP) v2, визначеному в RFC 1777, і визначає профіль цього протоколу для використання в PKIX, а також оновлює кодування для сертифікатів і списків відкликань, наведених у RFC 1778.

Відкликання та визначення статусу сертифіката

Існують два стандартизовані підходи, які дозволяють користувачеві сертифіката визначити його статус (тобто визначити, чи було його відкликано). По-перше, це використання CRL, а саме списків серійних номерів відкликаних сертифікатів, підписаних ЦС. По-друге, довірена третя сторона (ЦС або агент ЦС) надає он-лайн інформацію щодо статусу сертифіката, а саме, чи було його відкликано. Обидва підходи були предметом стандартизації.

1) Списки відкликаних сертифікатів (CRL) Рекомендація X.509 містить стандартний формат для CRL. Кожен запис CRL містить серійний номер (див. розділ 2.2) сертифіката X.509, який відкликається. Загальною вимогою до CRL є те, що вони оновлюються через регулярні визначені проміжки часу, що дозволяє користувачеві CRL перевірити, чи він володіє «останньою» версією.

2) Он-лайн протокол статусу сертифіката

Альтернативний підхід до відкликання сертифіката визначено в Інтернет-RFC 2560, [14]. У цьому документі визначено протокол онлайнового статусу сертифіката (OCSP), який дозволяє користувачеві визначати поточний статус цифрового сертифіката без запиту CRL. Замість або на додаток до перевірки періодично оновлюваного CRL може знадобитися отримати актуальну інформацію щодо відкликання статусу сертифіката. Приклади включають великі грошові перекази або великі угоди.

OCSP дозволяє програмам визначати стан (відкликання) ідентифікованого сертифіката. OCSP також можна використовувати для отримання додаткової інформації про статус сертифіката. Клієнт OCSP надсилає запит статусу відповідачу OCSP і призупиняє прийняття відповідного сертифіката, доки відповідач не надасть

відповідь. Цей протокол визначає дані, якими необхідно обмінюватися між програмою, що перевіряє статус сертифіката, і сервером, який надає цей статус.

Цей же протокол також визначено в проекті стандарту ISO/IEC 15945 [26].

Послуги штампування часу

На даний момент існують дві паралельні спроби запровадити стандарти для послуг із відмітками часу. Хоча служба відміток часу не є важливою частиною PKI, її можна використовувати для підвищення цінності певних служб безпеки, які підтримуються використанням PKI.

Одне з важливих застосувань, пов’язаних з PKI, стосується використання служби відмітки часу для надання довгострокової чинності підписам. Захищену мітку часу, обчислену для підписаного повідомлення, можна використовувати як доказ того, що підписане повідомлення було створено до дати закінчення терміну дії або відкликання ключа, використаного для підпису повідомлення.

1 Стандарт ISO/IEC про відмітку часу. Проекти міжнародних стандартів ISO/IEC 18014, частини 1-3 стосуються послуг штампування часу. Використання цифрових даних, що зберігаються на легко модифікованих носіях, піднімає питання про те, як сертифікувати, коли ці дані були створені або востаннє змінені.

Цифрове штампування часу допомагає отримати підтвердження своєчасності. Цифровий штамп часу повинен відповідати таким вимогам:

• Варіант часу має бути прив’язаний до даних у спосіб, який неможливо підробити, щоб уникнути заперечення існування даних до певного моменту часу.

• Дані повинні бути надані таким чином, щоб була гарантована їх конфіденційність.

Використовувані методи позначення часу вирішують ці вимоги шляхом позначення часу хеш-значення даних, що дозволяє контролювати цілісність і конфіденційність. Самі дані не розкриваються. Хеш-код даних буде криптографічно прив’язаний до поточного значення часу TSA. Ця прив'язка демонструє цілісність і

автентичність позначки часу. Сертифікат часу, що містить ці елементи, буде надіслано запитувачу позначки часу.

Маркери позначки часу можуть також містити інформацію, що стосується раніше згенерованих маркерів. Тут подання даних і додаткова інформація з даних із міткою часу, поставленою до цього запиту на мітку часу, є вхідними параметрами для процесу мітки часу.

2) Проект стандарту позначок часу в Інтернеті

Паралельний проект Інтернету описує службу відміток часу, яка підтримує твердження про доказ того, що дані існували до певного часу. У цьому документі описано формат запиту, надісланого до органу з відміток часу (TSA), і відповіді, яка повертається. Він також встановлює кілька вимог щодо безпеки для роботи TSA щодо обробки запитів для створення відповідей. TSA може працювати як служба довіреної третьої сторони (TTP), хоча можуть підійти й інші робочі моделі, напр. організації може знадобитися TSA для внутрішніх цілей відмітки часу. Приклад того, як довести, що цифровий підпис було згенеровано протягом терміну дії сертифіката відкритого ключа, наведено в додатку.

Інші довірені сторонні послуги

Завершуємо аналіз технічних стандартів PKI, згадавши про два подальші заходи стандартизації, які ще тривають.

1) Інструкції щодо використання та управління послугами TTP

Використання та управління широким спектром послуг довірених третіх сторін (TTP), багато з яких пов’язані з PKI, описано в технічному звіті ISO/IEC, який наближається до завершення, а саме ISO/IEC TR 14516,

З наданням і роботою довіреної третьої сторони (TTP) пов’язана низка проблем, пов’язаних із безпекою, для вирішення яких необхідні загальні вказівки, щоб допомогти суб’єктам господарювання, розробникам і постачальникам систем і послуг тощо. Це включає вказівки щодо питань щодо ролей , позиції та взаємовідносини TTP та суб’єктів, що використовують послуги TTP, загальні вимоги безпеки, хто повинен

забезпечувати який тип безпеки, які можливі рішення безпеки, а також оперативне використання та управління безпекою послуг TTP.

TR 14516 надає вказівки щодо використання та управління TTP, чітке визначення основних обов'язків і послуг, що надаються, їх опис і призначення, а також ролі та зобов'язання TTP та організацій, які користуються їхніми послугами. Він призначений головним чином для системних менеджерів, розробників, операторів TTP і корпоративних користувачів для вибору тих послуг TTP, необхідних для конкретних вимог, їх подальшого управління, використання та оперативного розгортання, а також встановлення політики безпеки в TTP.

Він не призначений для використання як основи для офіційної оцінки TTP або порівняння TTP. У цьому документі визначено різні основні категорії послуг TTP, зокрема: позначення часу, невідмовність, керування ключами, керування сертифікатами та електронні нотаріальні послуги.

2) SCVP

Перевірка сертифіката є складною проблемою. Якщо обробка сертифікатів має бути широко розгорнута в різноманітних програмах і середовищах, необхідно зменшити кількість обробки, яку має виконати програма, перш ніж вона зможе прийняти сертифікат. Існує безліч програм, які можуть використовувати сертифікати відкритих ключів, але обтяжені накладними витратами на перевірку сертифікатів, коли все, що дійсно потрібно програмі, це відкритий ключ і ім'я з сертифіката, а також щоб дізнатися, чи можна використовувати сертифікат для певної мети. Існують інші програми, які можуть виконувати перевірку шляху сертифіката, але не мають надійного методу отримання поточного ланцюга до надійного сертифіката.

Основними цілями простого протоколу перевірки сертифікатів (SCVP) [16] є спрощення для додатків розгортання систем за допомогою PKI та забезпечення централізації адміністрування політики PKI. Частини SCVP можуть використовуватися клієнтами, які самі виконують більшу частину обробки PKI і просто хочуть корисну, але ненадійний сервер, який збиратиме для них інформацію.

Інші частини можуть використовуватися клієнтами, які повністю довіряють серверу, щоб розвантажити перевірку сертифікатів і забезпечити узгоджене виконання політик на підприємстві.

Ненадійні сервери SCVP можуть надавати клієнтам ланцюжки сертифікатів, необхідні для перевірки шляху. Вони також можуть надавати клієнтам інформацію про відкликання, таку як CRL і відповіді OCSP, які клієнт може використовувати для перевірки шляху клієнта. Ці служби можуть бути цінними для клієнтських систем, які не містять протоколів, необхідних для пошуку та завантажити всі проміжні сертифікати, CRL і відповіді OCSP, необхідні клієнту для виконання повної перевірки шляху.

Довірені сервери SCVP можуть виконати повну перевірку сертифіката для клієнта. Якщо клієнт використовує ці служби, він за своєю суттю довіряє серверу SCVP так само, як і своєму власному програмному забезпеченню перевірки шляху (якби воно містило таке програмне забезпечення). Є дві основні причини, чому клієнт може захотіти довіряти такому серверу SCVP:

• Клієнт не хоче брати на себе накладні витрати на включення програмного забезпечення перевірки шляху та його запуск для кожного сертифіката, який він отримує.

• Клієнт знаходиться на підприємстві, яке хоче централізувати свої політики перевірки PKI, наприклад, які кореневі сертифікати є надійними та які типи перевірки політики виконуються під час перевірки шляху.

Заяви щодо політики та практики сертифікації

RFC 2527, [11], представляє структуру для допомоги розробникам політик сертифікації або заяв про практику сертифікації для CA та PKI. Зокрема, структура надає вичерпний перелік тем, які потенційно повинні бути охоплені у визначенні політики сертифікації або заяві про практику сертифікації.

Ступінь, до якого користувач сертифіката може довіряти прив’язці, втіленій у сертифікаті, залежить від кількох факторів. Ці фактори включають практику, якої

дотримується ЦС під час автентифікації суб’єкта; операційна політика, процедури та засоби контролю безпеки ЦС; обов'язки суб'єкта (наприклад, щодо захисту особистого ключа); і заявлені зобов’язання та юридичні зобов’язання ЦС (наприклад, гарантії та обмеження відповідальності).

Сертифікат версії 3 X.509 може містити поле, яке заявляє, що до цього сертифіката застосовуються одна або кілька конкретних політик щодо сертифікатів [8-11]. Згідно з X.509, політика сертифікатів — це «іменований набір правил, який вказує на застосовність сертифіката до певної спільноти та/або класу програм із загальними вимогами безпеки». Політика сертифіката може використовуватися користувачем сертифіката, щоб допомогти вирішити, чи сертифікат і прив’язка в ньому є достатньо надійними для певної програми. Концепція політики сертифікатів є результатом концепції політики, розробленої для Internet PEM [5].

Більш детальний опис практик, яких дотримується ЦС під час видачі та іншого керування сертифікатами, може міститися в документі про практику сертифікації (CPS), опублікованому ЦС або на який він посилається. Відповідно до Рекомендацій щодо цифрового підпису Американської асоціації юристів, «CPS — це виклад практик, які використовує центр сертифікації для видачі сертифікатів» [1].

Метою RFC 2527 є встановлення чіткого зв’язку між політиками сертифікатів і CPS, а також представлення структури, яка допоможе розробникам політик сертифікатів або CPS у виконанні їхніх завдань. Зокрема, структура визначає елементи, які, можливо, необхідно враховувати при формулюванні політики сертифікатів або CPS. Метою є не визначення конкретних політик сертифікатів або CPS.

Сфера застосування RFC 2527 обмежена обговоренням змісту політики сертифікатів (як визначено в X.509) або CPS (як визначено в Керівних принципах ABA). Зокрема, цей документ описує типи інформації, які слід розглянути для включення у визначення політики сертифікатів або CPS. Хоча структура, як представлено, загалом передбачає використання формату сертифіката X.509 версії 3,

не передбачається, що матеріал обмежується використанням цього формату сертифіката. Швидше, передбачається, що цю структуру можна адаптувати до інших форматів сертифікатів, які можуть увійти до використання.

Сфера застосування не поширюється на визначення політик безпеки в цілому (таких як політика безпеки організації, політика безпеки системи або політика маркування даних), окрім елементів політики, які вважаються особливо важливими для політик сертифікатів або CPS. RFC 2527 не визначає конкретну політику сертифікатів або CPS.

2 МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ В ОРГАНІЗАЦІЇ

2.1 Компоненти інфраструктури відкритих ключів в організації

PKI - це основа сучасної інформаційної безпеки. PKI – це набір практик, політик і технологій, які захищають конфіденційні дані від несанкціонованого доступу або використання [17].

Організації не можуть дозволити собі ризикувати репутацією своєї компанії, дозволяючи кіберзлочинцям викрадати інформацію про клієнтів або комерційну таємницю. Завдяки PKI організації можуть бути спокійні, знаючи, що ваш бізнес працює добре після позитивних результатів оцінки безпеки , захист конфіденційних даних від кібератак та інших загроз.

PKI — це система кібербезпеки, яка надає організаціям відкриті ключі та цифрові сертифікати для шифрування публічних даних. Найпоширенішим використанням PKI є безпечний обмін конфіденційною інформацією через Інтернет та інші загальнодоступні мережі, наприклад державні урядові установи. Відповідність і нормативні вимоги вимагають відповідних технічних і організаційних заходів для захисту даних [17].

Інфраструктура відкритих ключів (PKI) захищає дані, шифруючи їх за допомогою ключів, які складаються з великих чисел, згенерованих із складних математичних задач. Ключ кожної особи є різним і дозволяє лише їм отримати доступ до своїх цифрових файлів (рис.2.1).

Криптографічний захист

Криптографічна система, яка використовується з PKI, відома як криптографія з відкритим ключем, захищає дані в русі, гарантуючи, що вони мають цифровий підпис перед передачею через такі мережі, як Інтернет та інші публічні системи зв’язку. PKI іноді називають інфраструктурою приватного ключа або шифруванням приватного

ключа; однак такої функції не існує. Закритий ключ є компонентом PKI, який пов’язаний із тим, як функціонує асиметричне шифрування.

Криптографія відноситься до вивчення захищених комунікацій – її методів і прийомів, різних основних аспектів безпеки даних, таких як конфіденційність, цілісність, автентифікація та неспростовність.

Інфраструктура відкритих ключів (PKI) захищає дані, шифруючи їх за допомогою ключів, які складаються з великих чисел, згенерованих із складних математичних задач. Ключ кожної особи є різним і дозволяє лише їм отримати доступ до своїх цифрових файлів. Криптографічна система, яка використовується з PKI, відома як криптографія з відкритим ключем, захищає дані в русі, гарантуючи, що вони мають цифровий підпис перед передачею через такі мережі, як Інтернет та інші публічні системи зв’язку [17].

PKI складається з набору відкритих і закритих криптографічних ключів. Відкритий ключ можна надавати без занепокоєння щодо безпеки, тоді як закритий ключ зазвичай секретний. Сертифікати створюються та зберігаються в третій стороні, яка зазвичай називається центром сертифікації (ЦС), створеним для надання цієї послуги. Потім ці сертифікати використовуються особами, яким вони потрібні для шифрування документів, автентифікації електронних повідомлень і цифрового підпису контрактів. Існує багато різних способів (внутрішніх, із центру сертифікації тощо) створення цих ключів і сертифікатів, у кожного з яких є переваги та недоліки.

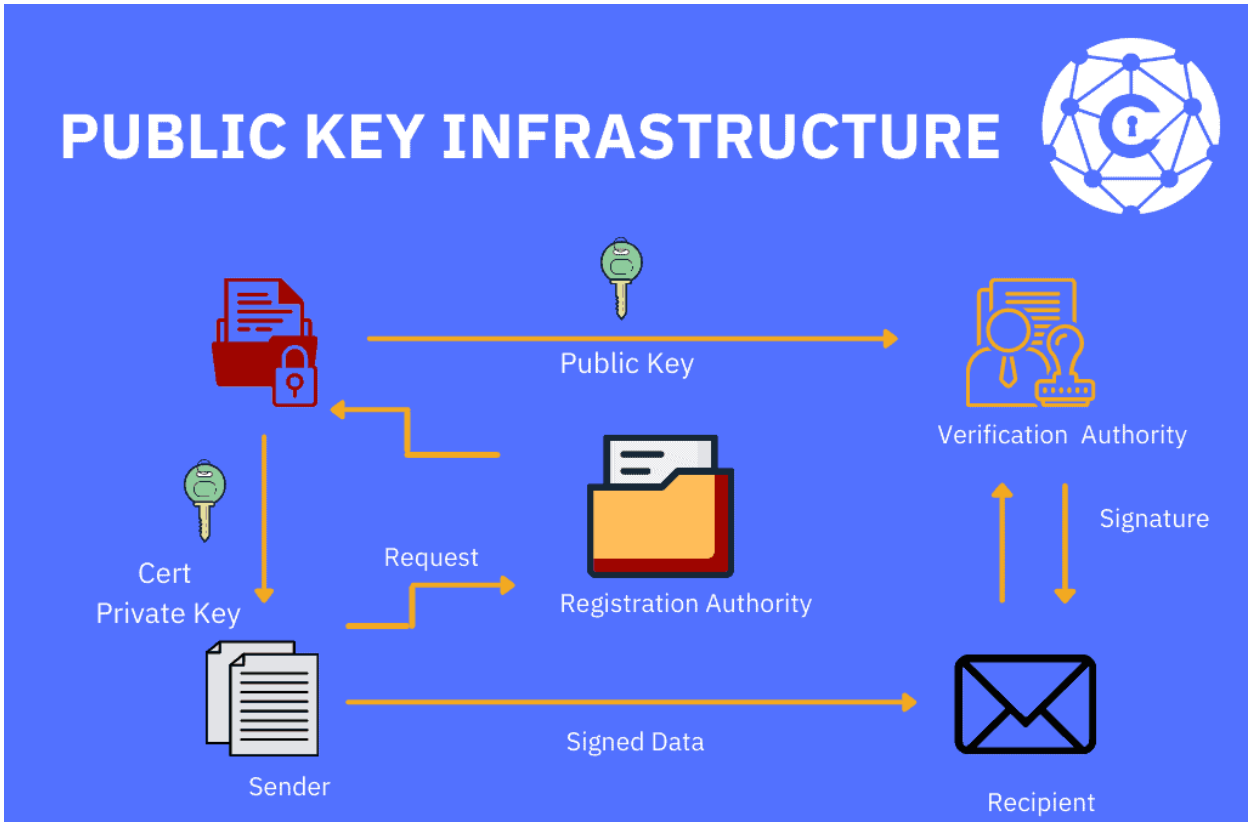

Рис. 2.1. Інфраструктура відкритих ключів [17]

PKI використовується для шифрування та цифрових підписів, гарантуючи, що інформація, яку ви надсилаєте, залишається захищеною від зловмисників. PKI можна використовувати для забезпечення вашої ідентифікації в Інтернеті. Він використовується в кожному випадку шифрування даних, який ви використовуватимете під час користування Інтернетом. Ця форма криптографії захищає електронний зв'язок із такими програмами, як електронна пошта та VPN (віртуальні приватні мережі), і забезпечує безпеку вашої інформації під час перегляду веб-сторінок [17].

PKI використовується в різних системах безпеки, починаючи від автентифікації особи до безпечної доставки у WWW (Всесвітня павутина). Його зазвичай використовують уряди, системи освіти, банки, продавці електронної комерції та інші, які обробляють конфіденційні дані .

PKI використовуються в кількох різних сценаріях, зокрема для шифрування інформації, надісланої електронною поштою та іншими формами цифрового зв'язку. Інтернет-продавці також використовують цей тип шифрування, щоб забезпечити безпеку транзакцій кредитних карток через Інтернет, захищаючи фінансові дані особи від зловмисників. Державні установи також можуть використовувати PKI для шифрування даних, наприклад податкових декларацій.

PKI пропонує набір служб безпеки, які забезпечують основу для електронної комерції, Інтернету та бездротових мереж. Він також забезпечує стабільне бізнес-середовище для нових технологій, включаючи розумні пристрої та Інтернет речей (IoT). Основні переваги PKI для захисту даних:

– Забезпечення довіри між учасниками електронного правочину;

– Забезпечення конфіденційності даних, що передаються по мережах;

– Гарантування достовірності даних, що передаються в електронному вигляді;

– Підтримка невідмовності транзакцій після завершення, а також забезпечення автентифікації та конфіденційності персональних даних [17].

Наведемо основні компоненти PKI:

– Центр сертифікації

– Сертифікат

– Орган реєстрації

– Орган перевірки (OSCP або CRL)

– Безпечне зберігання

– Пара відкритий/приватний ключ

2.2. Центр сертифікації

Центри сертифікації — це надійні треті сторони, які допомагають установлювати та підтримувати цілісність систем PKI, видаючи сертифікати відкритого ключа. Ці організації несуть додаткову відповідальність за перевірку того, що особи, які подають заявку на отримання цифрових ключів, є тими, за кого себе видають (користувачами, пристроями чи послугами), і що надана інформація не була жодним чином змінена з моменту її цифрового підпису. Їх також називають кореневим центром сертифікації або кореневим ЦС або центром реєстрації [17, 18].

Роль центрів сертифікації

Центр сертифікації видає ці цифрові ключі та підписує їх власним закритим ключем, щоб одержувачі знали, що зловмисники не можуть підробити чи змінити особистість відправника. Органи сертифікації (CA) створюють ієрархічну систему довіри на основі кількості різних кореневих сертифікатів CA, які вже існують; це дає змогу поширювати меншу довіру до сертифікатів, кореневі ключі яких мають менше «стрибків» від довірених коренів ЦС.

Центр сертифікації або ЦС – це в основному організація або установа, яка уповноважена та відповідає за розповсюдження цифрових сертифікатів. Видача сертифіката є одним із важливих сегментів безпеки взаємодії, що відбувається через Інтернет.

Основним використанням сертифікатів є шифрування SSL для автентифікації пристроїв, а також людей і легітимізації кодів і документів. Однією з унікальних особливостей довіреного центру сертифікації є «повсюдність». Необхідно, щоб він був максимально сумісний з різними версіями інтернет-браузерів і операційних систем. Важливо розгорнути безперервну перевірку сертифіката для різних користувачів у будь-якій службі чи пристрої. [18]

Якщо говорити простими словами, «що виконують CA (центри сертифікації)?» Вони гарантують, що кожен в Інтернеті є тим, за кого себе видає!

Існує два основних типи центрів сертифікації, які ми збираємося обговорити прямо тут. Один є державним центром сертифікації, а інший – приватним центром

сертифікації. Те, що ми збираємося обговорити нижче, полягає в розмежуванні публічних і приватних центрів сертифікації (рис.2.2).

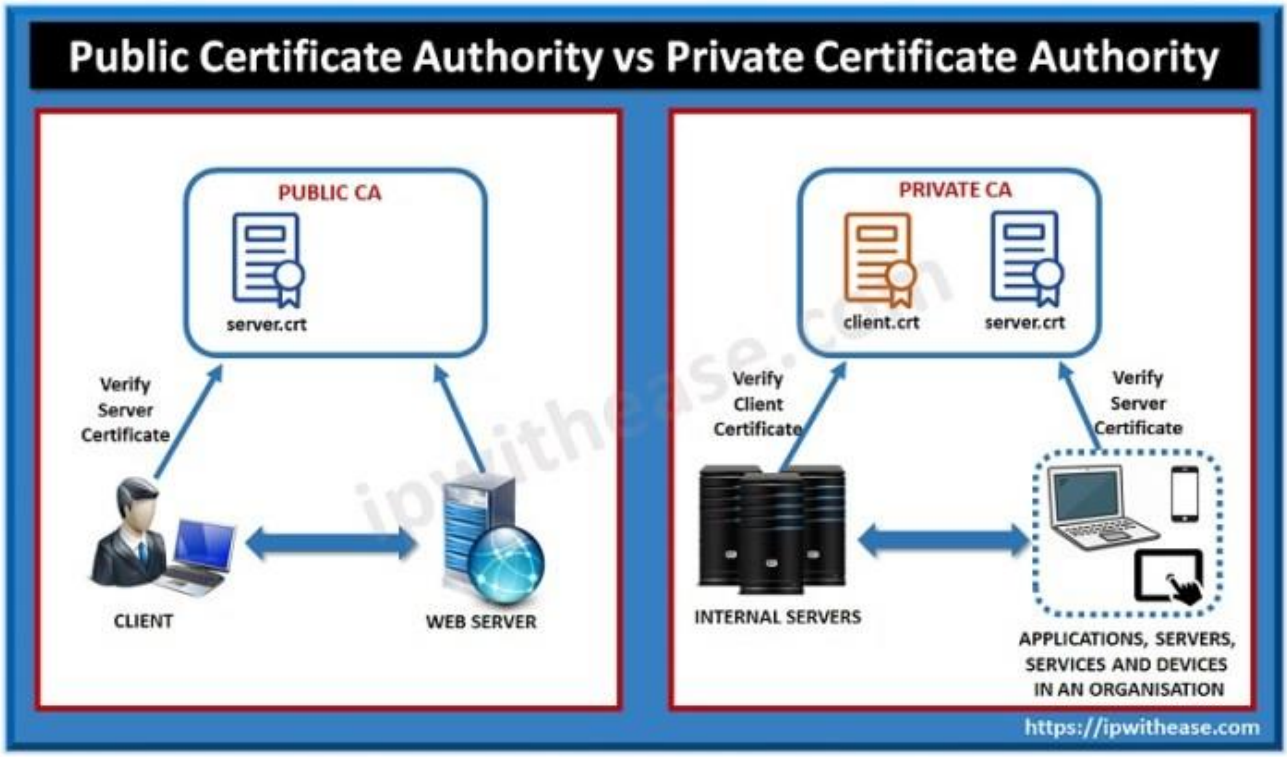

Рис.2.2. Публічний та приватний центр сертифікації [18]

Загальнодоступний центр сертифікації — це центр сертифікації, який надає послуги звичайній громадськості, і будь-яка організація, що пропонує функції та послуги ЦС, з якими ви не пов’язані, є в основному публічним ЦС . Більшість державних центрів сертифікації – це компанії, які заслужили довіру широкої громадськості. Є також деякі державні ЦС, якими керує уряд. З іншого боку, приватний ЦС, які також називають локальними ЦС, є формою автономних центрів сертифікації, призначених лише для внутрішнього використання. Приватним ЦС навмисно було надано обмежений обсяг, який зазвичай використовується в організації, дуже великій компанії чи навіть університеті. Фактом є те, що приватному ЦС «довіряють» лише користувачі всередині організації – і він рідко взаємодіє із зовнішніми мережами. [18]

Оскільки від вас часто вимагається платити за кожен виданий сертифікат, публічні ЦС є улюбленим варіантом, якщо вам потрібно випустити обмежену кількість сертифікатів. З іншого боку, якщо ви прогнозуєте великий обсяг сертифікатів лише через те, що організація є великою, а точніше тому, що сертифікати потрібно періодично перевидавати, може бути розумним і дешевшим керувати власним ЦС замість того, щоб платити за кожен випуск виданий державним СЦ. Іншим аспектом, який відрізняється між обома типами ЦС, є характер комунікації, тобто публічний ЦС є найкращим рішенням у будь-якому випадку, коли ситуація вимагає прозорого спілкування в Інтернеті. У разі будь-якої загальнодоступної послуги чи продукту вам знадобиться загальнодоступний ЦС. Приватний СЦ підхід більш безпечний. Контроль терміну дії сертифіката є важливим фактором для організацій, які мають чутливий до часу або цинічний характер.

Дослідимо, які з наведених ЦС більш захищені – публічний центр сертифікації широко використовується в Інтернеті. Більшість типів конфіденційності чи безпеки так чи інакше включають публічну форму СЦ. Це не стосується приватних ЦС – вони значно безпечніші порівняно з державними аналогами. У державних центрах сертифікації сертифікати видаються кожному, хто платить, приватні центри сертифікації обмежують свої сертифікати лише окремими пристроями чи людьми, як правило, тими, хто входить до складу організації. [18]

Differentiating Factor	Public Certificate Authority	Private Certificate Authority
The Definition	Services to the common public.	Self-hosted certificate authorities for internal usage.
The Type of Companies	Companies that have earned the faith of the public at large.	Functions within an organization, and 'trusted' by users inside that organization.
The Usage	Default common deployment	Specific deployment.
Cost of Certificate Issuance	Higher	Cheaper
Nature of Communication	Transparent	Secured
The Security	Less secured	More secured
The Examples	Implementing SSL, encrypting emails and signing digital documents.	Intranet

https://ipwithease.com

Рис. 2.3. Порівняння центрів сертифікації

Прикладом публічного центру сертифікації включають впровадження SSL, шифрування електронних листів і підписання цифрових документів. З іншого боку, приватний центр сертифікації є важливою частиною побудови захищеної та надійної внутрішньої мережі. [18]

2.3. Складові сертифіката

Багато центрів сертифікації (CA) уже додано до веб-переглядачів і комп'ютерів за замовчуванням. Коли ви купуєте сертифікат X.509 від реєструючого органу, це насправді не просто один сертифікат TLS або SSL, а кілька компонентів [18, 19]:

– Інформація про створення ключа, яка включає відкритий ключ, закритий ключ та інші деталі.

– Сертифікат із цифровим підписом від довіреної третьої сторони, що називається центром сертифікації або ЦС.

– Підпис робить цю інформацію надійною, оскільки лише власник закритого ключа може створити ці підписи (у випадку самопідписаних сертифікатів).

– Доказ володіння сертифікатом (тобто доказ), який зазвичай містить ідентифікаційні дані, такі як назва компанії, адреса тощо.

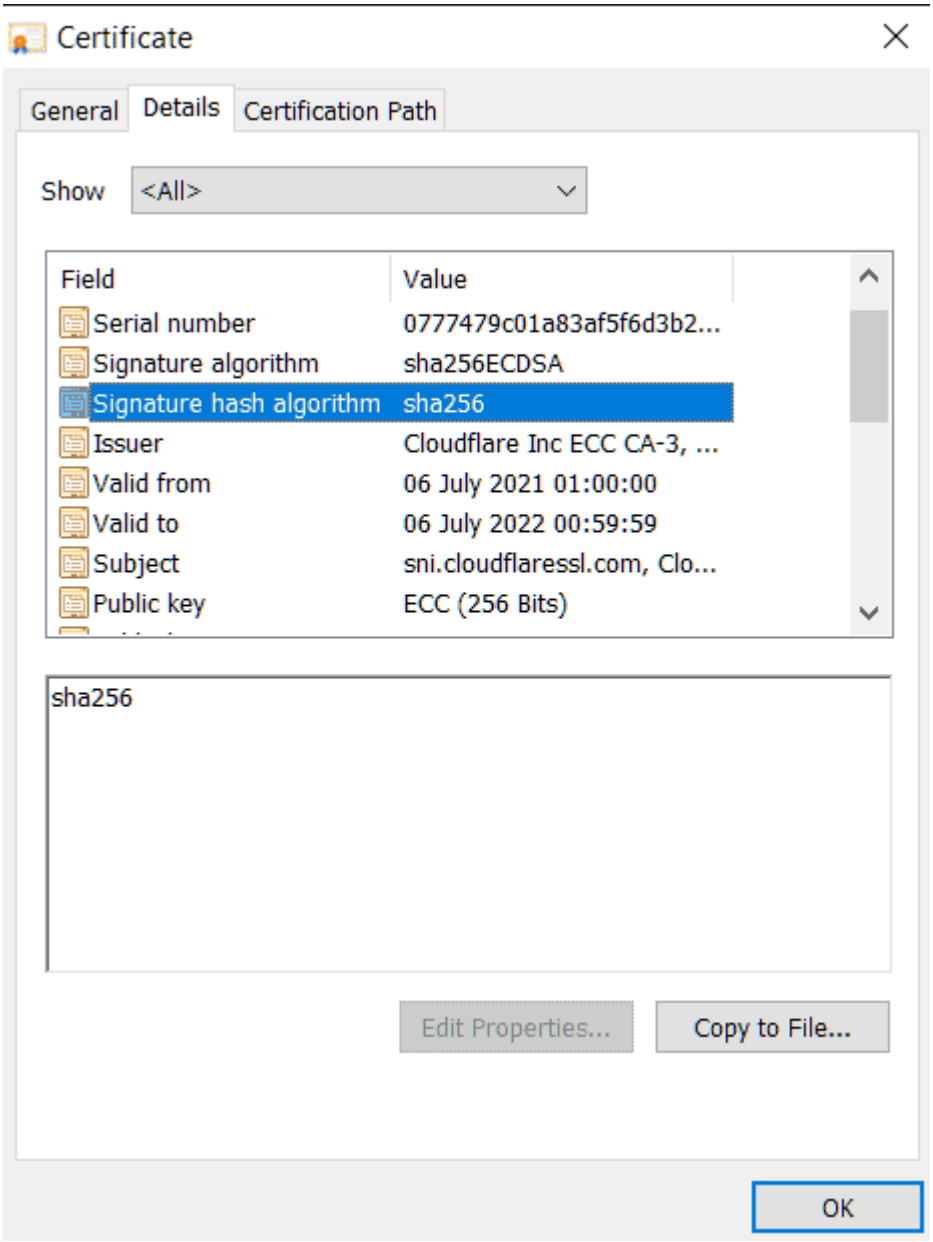

Рис.2.4. Цифровий сертифікат [18]

Властивості цифрового сертифіката

Цифровий сертифікат схожий на ключ, який використовується для шифрування даних. Ці сертифікати підписуються центром сертифікації, який є довіреною третьою стороною.

Стандарт X.509 — це стандарт цифрових сертифікатів, який описує структуру сертифікатів, списки відкликаних сертифікатів і формат сертифікатів для документів сертифікатів. Він був розроблений Міжнародним союзом електрозв'язку (ITU-T) і базується на попередніх стандартах, таких як X.509 v3 та ISO 9594-8 [18].

Призначення X.509

Основною метою цього стандарту є визначення системи для представлення та передачі інформації про цифрову ідентифікацію людей або інших організацій в електронній формі через загальнодоступні мережі, такі як Інтернет.

Ці сертифікати використовують методи криптографії, щоб гарантувати, що лише користувачі, які мають законне володіння, можуть розшифрувати дані, зашифровані їхнім відкритим ключем; це допомагає забезпечити конфіденційність (цілісність даних). Зашифровані дані можна розшифрувати лише за допомогою відповідного закритого ключа.

Люди використовують сертифікати X.509 для різних речей. Ось деякі з причин: шифрування документів, автентифікація електронних повідомлень і цифровий підпис контрактів.

Існує багато різних способів (внутрішніх, із центру сертифікації тощо) створення цих ключів і сертифікатів, у кожного з яких є переваги та недоліки.

Кожна організація має свій сертифікатЦС, який підписали інші ЦС. Ця ієрархія дозволяє здійснити належну перевірку, оскільки кожна особа в ланцюжку, яка підписує, має перевірити, що представлена інформація про особу, яка робить запити на ці запити.

Загрози безпеці, пов'язані з X.509

Уразливі місця безпеки, пов'язані з цифровими сертифікатами, включають файли cookie, які зберігають ключі на жорстких дисках користувачів; Депонування ключа – коли копія вашого закритого ключа існує за межами вашої організації, що створює ризик у разі її втрати або викрадення; Розкриття приватного ключа – коли

хтось отримує доступ до вашого приватного ключа без авторизації; а також спуфінг – коли загроза створює підроблений сертифікат, який підписує законний ЦС.

Існує кілька способів використання цифрового сертифіката: для шифрування звичайних файлів даних, щоб забезпечити безпеку під час передачі інформації через мережі або її зберігання на жорстких дисках; Цифрові підписи електронних документів на основі інфраструктури відкритих ключів (PKI), щоб гарантувати, що вони не були змінені чи підроблені; Вони також можуть забезпечити автентифікацію того, що відправник електронної пошти є тим, за кого себе видає (тобто, що ви надсилаєте електронні листи з веб-сайту свого банку, а не від когось іншого, хто намагається підробити домен).

Щоб бути довіреною стороною, підприємствам рекомендовано використовувати центри сертифікації для перевірки цифрових сертифікатів для підпису своїх електронних листів. Без цього процесу перевірки будь-хто міг би легко створити електронний лист, начебто надісланий вашою компанією, і підробити особу відправника. Нарешті, вони можуть увімкнути електронні підписи, такі як ті, що вимагаються в контрактах, коли транзакції відповідають правовим стандартам.

Сервер каталогів використовує такі типи сертифікатів [19]*:*

Клієнтські сертифікати SSL

Клієнтські сертифікати SSL використовуються для ідентифікації клієнтів на серверах через SSL (автентифікація клієнта). Як правило, припускається, що особа клієнта збігається з особою людини, наприклад, працівника підприємства. Клієнтські SSL-сертифікати також можна використовувати для підписання форм і як частину рішення єдиного входу [19].

Наприклад, банк надає клієнту SSL-сертифікат клієнта, який дозволяє серверам банку ідентифікувати цього клієнта та дозволити доступ до його рахунків. Компанія може надати новому співробітнику клієнтський сертифікат SSL, який дозволяє

серверам компанії ідентифікувати цього працівника та дозволити доступ до серверів компанії.

Сертифікати SSL сервера

Сертифікати SSL сервера використовуються для ідентифікації серверів клієнтам через SSL (автентифікація сервера). Аутентифікацію сервера можна використовувати з автентифікацією клієнта або без неї. Автентифікація сервера є обов'язковою умовою для зашифрованого сеансу SSL[19].

Наприклад, інтернет-сайти, які займаються електронною комерцією, зазвичай підтримують автентифікацію сервера на основі сертифікатів, як мінімум, для встановлення зашифрованого сеансу SSL і для того, щоб переконати клієнтів, що вони мають справу з веб-сайтом, ідентифікованим як певна компанія. Зашифрований сеанс SSL гарантує, що особисту інформацію, надіслану через мережу, наприклад номери кредитних карток, неможливо легко перехопити.

Сертифікати S/MIME

Сертифікати S/MIME використовуються для підписаної та зашифрованої електронної пошти. Як і у випадку з клієнтськими сертифікатами SSL, ідентифікаційна інформація клієнта зазвичай збігається з особою людини, наприклад працівника підприємства. Один сертифікат можна використовувати і як сертифікат S/MIME, і як сертифікат SSL. Сертифікати S/MIME також можна використовувати для підписання форм і як частину рішення єдиного входу [19].

Наприклад, компанія розгортає комбіновані сертифікати S/MIME та SSL виключно з метою автентифікації співробітників, таким чином дозволяючи підписану електронну пошту та автентифікацію SSL клієнта, але не зашифровану електронну пошту. Інша компанія видає сертифікати S/MIME виключно з метою підписання та шифрування електронних листів, які стосуються конфіденційних фінансових або юридичних питань.

Сертифікати підпису об'єктів

Сертифікати підпису об’єктів використовуються для ідентифікації підписувачів коду Java, сценаріїв JavaScript або інших підписаних файлів.

Наприклад, компанія-виробник програмного забезпечення підписує програмне забезпечення, що розповсюджується через Інтернет, щоб надати користувачам певну впевненість, що це програмне забезпечення є законним продуктом цієї компанії. Використання сертифікатів і цифрових підписів у такий спосіб також може дозволити користувачам ідентифікувати та контролювати тип доступу завантаженого програмного забезпечення до своїх комп’ютерів.

Сертифікати ЦС

Сертифікати ЦС використовуються для ідентифікації ЦС. Клієнтське та серверне програмне забезпечення використовує сертифікати ЦС, щоб визначити, яким іншим сертифікатам можна довіряти [19].

Наприклад, сертифікати ЦС, що зберігаються в програмному забезпеченні клієнта, визначають, які інші сертифікати клієнт може автентифікувати. Адміністратор може реалізувати деякі аспекти корпоративної політики безпеки, контролюючи сертифікати ЦС, що зберігаються в клієнті кожного користувача [19].

Список відкликаних сертифікатів (CRL) зазвичай доставляється в цифровому вигляді, хоча їх також можна опублікувати в друкованих каталогах. У CRL перераховуються всі сертифікати, які було відкликано з різних причин, у тому числі коли особа більше не працює в компанії або приватний ключ було зламано. Це також може вказувати на те, що відкритий ключ у сертифікаті недостатній для захисту інформації через підключення до Інтернету, і його потрібно обміняти іншим набором ключів.

База даних сертифікатів підтримує такі запити та інформацію. Усі запити на сертифікати, запити на видачу, відкликані сертифікати та пов’язана інформація зберігається в базі даних сертифікатів.

2.4. Ієрархії CA

У великих організаціях може бути доречним делегувати відповідальність за видачу сертифікатів кільком різним органам сертифікації. Наприклад, кількість необхідних сертифікатів може бути занадто великою для обслуговування одним ЦС; різні організаційні підрозділи можуть мати різні вимоги політики; або для ЦС може бути важливо фізично перебувати в тій самій географічній зоні, що й люди, яким він видає сертифікати. [19]

Є можливість делегувати обов'язки з видачі сертифікатів підлеглим ЦС. Стандарт X.509 містить модель для встановлення ієрархії ЦС (рис 2.5).

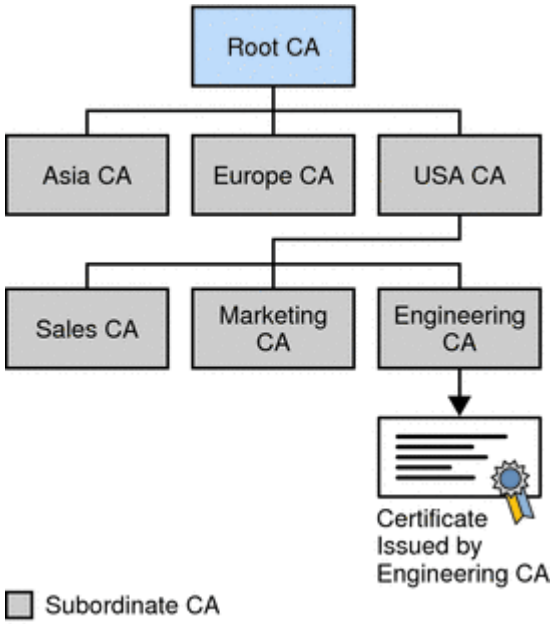

Рис. 2.5–3 Ієрархія центрів сертифікації [19]

У цій моделі кореневий ЦС знаходиться на вершині ієрархії. Сертифікат кореневого ЦС є самопідписаним сертифікатом. Тобто сертифікат має цифровий підпис тією самою сутністю, кореневим ЦС, яку ідентифікує сертифікат. ЦС, які безпосередньо підпорядковані кореневому ЦС, мають сертифікати ЦС, підписані кореневим ЦС. Сертифікати ЦС підлеглих ЦС в ієрархії підписані підпорядкованими ЦС вищого рівня. [19]

Організації мають значну гнучкість щодо того, як вони встановлюють свої ієрархії CA. На рис.2.5 показано лише один приклад; можливі багато інших домовленостей.

Ланцюжки сертифікатів

Ієрархії ЦС відображаються в ланцюжках сертифікатів. Ланцюжок сертифікатів — це серія сертифікатів, виданих послідовними ЦС. На рис. 2.6_показано ланцюжок сертифікатів, що веде від сертифіката, який ідентифікує деяку сутність, через два підпорядкованих сертифікати ЦС до сертифіката ЦС для кореневого ЦС).

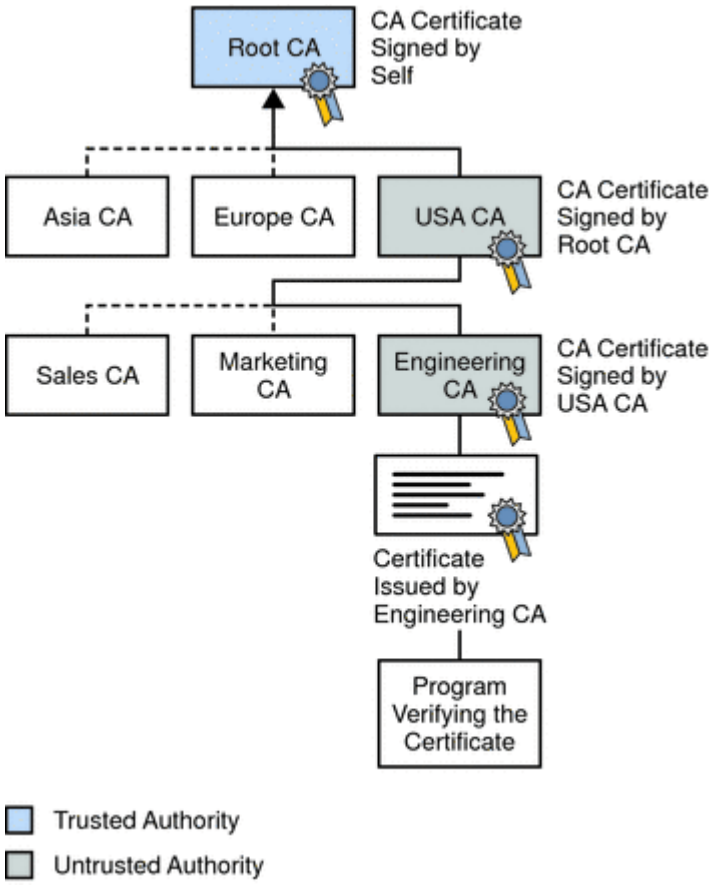

Рис. 2.6. Ланцюжок сертифікатів [19]

Ланцюжок сертифікатів відстежує шлях сертифікатів від гілки в ієрархії до кореня ієрархії. У ланцюжку сертифікатів відбувається таке:

- Після кожного сертифіката додається сертифікат його видавця.

- На рис.2.6 сертифікат інженерного ЦС містить DN ЦС (тобто ЦС США), який видав цей сертифікат. DN CA також є назвою суб’єкта наступного сертифіката в ланцюжку.
- Кожен сертифікат підписується закритим ключем його видавця. Підпис можна перевірити за допомогою відкритого ключа в сертифікаті емітента, який є наступним сертифікатом у ланцюжку.

На рис.2.6 відкритий ключ у сертифікаті для ЦС США можна використовувати для перевірки цифрового підпису ЦС США на сертифікаті для інженерного ЦС.

Перевірка ланцюжка сертифікатів

Перевірка ланцюжка сертифікатів — це процес перевірки того, що даний ланцюжок сертифікатів правильно сформований, дійсний, правильно підписаний і надійний. Програмне забезпечення Directory Server використовує наступні кроки для формування та перевірки ланцюжка сертифікатів, починаючи з того, що сертифікат надається для автентифікації:

1. Період дії сертифіката перевіряється за поточним часом, наданим системним годинником верифікатора.
2. Сертифікат емітента знаходиться. Джерелом може бути або локальна база даних сертифікатів верифікатора (на цьому клієнті чи сервері), або ланцюжок сертифікатів, наданий суб’єктом (наприклад, через з’єднання SSL).
3. Підпис сертифіката перевіряється за допомогою відкритого ключа в сертифікаті видавця.
4. Якщо верифікатор довіряє сертифікату видавця в базі даних сертифікатів верифікатора, тут перевірка успішно зупиняється. В іншому випадку сертифікат видавця перевіряється, щоб переконатися, що він містить відповідну вказівку підлеглого ЦС у розширенні типу сертифіката сервера каталогів, і ланцюгова перевірка повертається до кроку 1, щоб почати знову, але з цим новим сертифікатом [19].

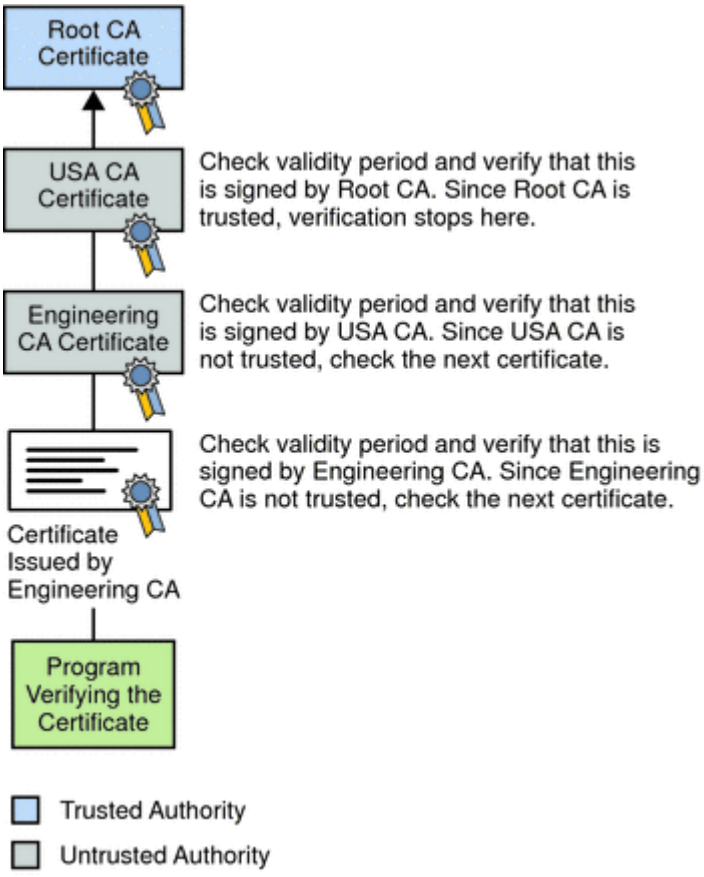

Рис.2.7. Перевірка ланцюжка сертифікатів [19]

На Рис.2.7. показано, що відбувається, коли до локальної бази даних верифікатора включено лише кореневий ЦС. Якщо сертифікат одного з проміжних центрів сертифікації, показаних на Рис.2.8, наприклад інженерного ЦС, знайдено в локальній базі даних верифікатора, перевірка припиняється на цьому сертифікаті, як показано на Рис.2.8. нижче.

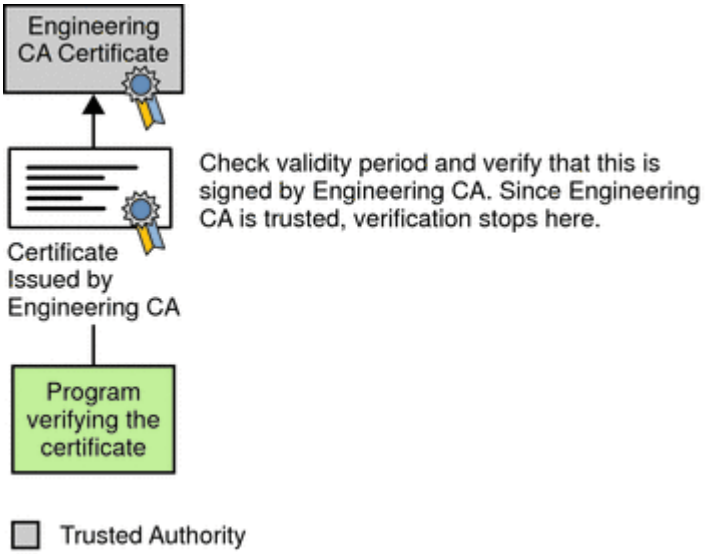

Рис.2.8. Перевірка ланцюжка сертифікатів [19]

Закінчені терміни дії, недійсний підпис або відсутність сертифіката для центру сертифікації, що видав сертифікат, у будь-якій точці ланцюжка сертифікатів призводять до збою автентифікації.

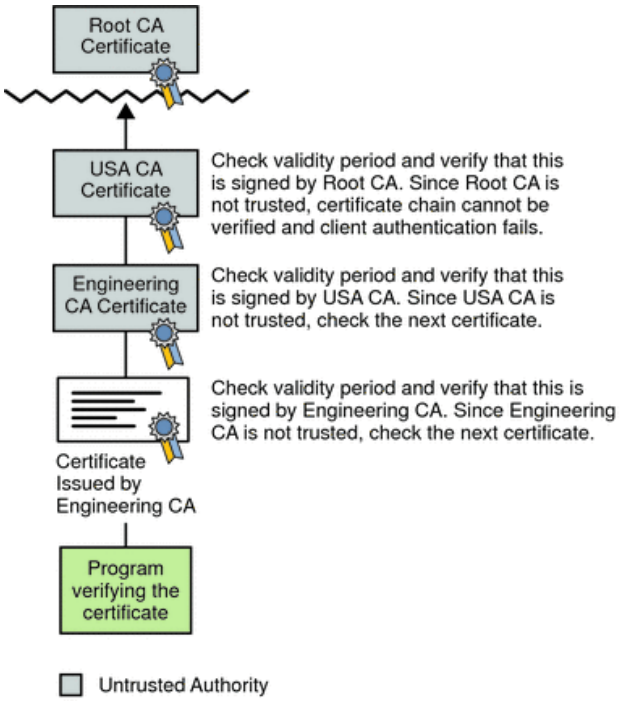

Рис.2.9. Ланцюжок сертифікатів, який не можна перевірити

Наприклад, на Рис.2.9. показано, як не вдається перевірити, якщо ані кореневий сертифікат ЦС, ані будь-який із проміжних сертифікатів ЦС не включено до локальної бази даних верифікатора.

3 РОЗРОБКА РЕКОМДАЦІЙ СТВОРЕННЯ ЦЕНТРУ DIGICERT ONE ENTERPRISE PKI MANAGER

3.1 Варіант застосування інфраструктури інфраструктури відкритих ключів на основі інтеграції Microsoft Endpoint Manager і DigiCert ONE

Етапи життєвого циклу сертифіката, які зазвичай можна автоматизувати, включають:

Створення CSR;

Ключі зберігання;

Повна перевірка сертифікатів;

Створення сертифікатів;

Перевидання ;

Оновлення;

Відкликання.

Microsoft Intune забезпечує керування мобільними пристроями та можливості мобільних програм, які дозволяють визначати, до яких даних мають доступ різні користувачі у вашій організації. Інтегрований захист даних і можливості відповідності визначають, що користувачі можуть робити з даними в Microsoft Office та інших мобільних програмах.

Microsoft Intune безпечно керує ідентифікаторами, програмами та пристроями

Оскільки організації переходять на підтримку гібридної та віддаленої роботи, їм стає важко керувати різними пристроями, які отримують доступ до ресурсів організації. Співробітники та студенти повинні співпрацювати, працювати з будь-якого місця, а також мати безпечний доступ і підключатися до цих ресурсів. Адміністратори повинні захищати дані організації, керувати доступом кінцевих користувачів і підтримувати користувачів, де б вони не працювали.

Щоб допомогти з цими проблемами та завданнямиє можливість використати Microsoft Intune.

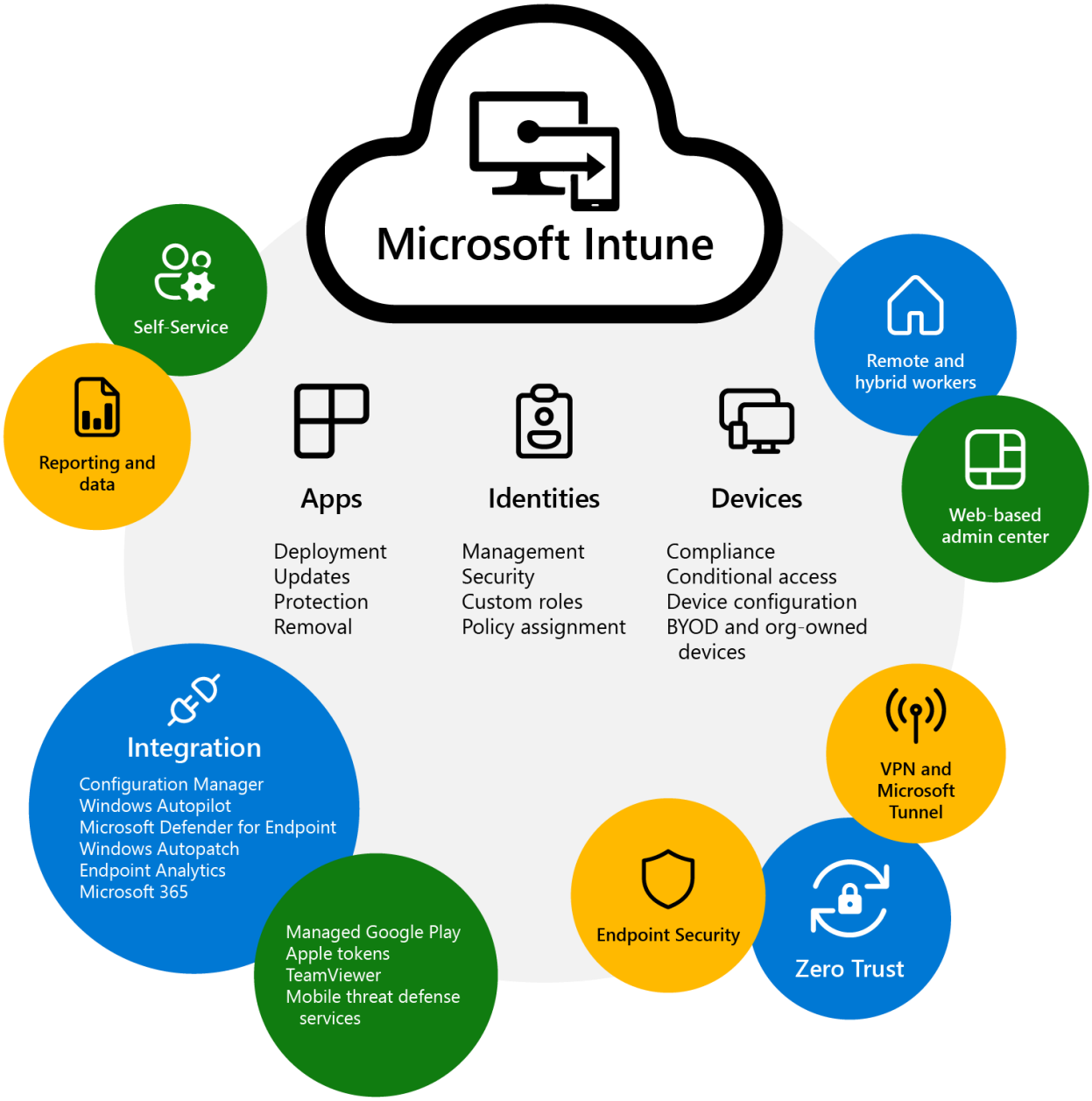

Рис.3.1. Функції Microsoft Intune

Microsoft Intune — це хмарне рішення для керування кінцевими точками. Він керує доступом користувачів і спрощує керування програмами та пристроями на

багатьох ваших пристроях, включаючи мобільні пристрої, настільні комп’ютери та віртуальні кінцеві точки.

Інтеграція Microsoft Intune із DigiCert ONE дозволяє створювати цифрові сертифікати, які забезпечують довіру, без імен користувачів, паролів або додаткових апаратних маркерів. Крім того, DigiCert ONE Enterprise PKI Manager забезпечує швидке розгортання та просте керування.

У наведеній нижче таблиці показано типи сертифікатів, які можна видавати, і методи інтеграції для цього типу сертифіката.

Таблиця 3.1

Тип сертифіката та метод інтеграції

DigiCert тип сертифіката	Microsoft тип профілю	Інтеграція Методу з DigiCert ONE Enterprise PKI Manager	Примітки
пристрій Автентифікація для Microsoft Intune (SCEP)	SCEP сертифікат	Microsoft API	Це інтеграція з хмари в хмару.
Клієнт користувача Автентифікація для Microsoft Intune (SCEP)	SCEP сертифікат	Microsoft API	Це інтеграція з хмари в хмару.

Для успішної роботи необхідно підготовити середовище:

– У вашому клієнті Microsoft Azure увімкнено служби Azure Active Directory.

– Ваш обліковий запис Microsoft Intune налаштовано для Intune MDM Authority.

– Ваш обліковий запис Microsoft Intune налаштовано за допомогою Сертифікат Apple MDM Push , якщо потрібно видати сертифікати для пристроїв Apple iOS.

Популярні протоколи керування сертифікатами включають:

1. SCEP (Simple Certificate Enrollment Protocol)
2. EST (Enrollment over Secure Transport)
3. ACME (Automatic Certificate Management Environment)
4. CMP (Certificate Management Protocol)

Щоб використовувати один із цих протоколів, необхідно встановити клієнт протоколу (наприклад, CertBot для ACME), використовувати систему/програмне забезпечення, яке вже підтримує протокол, або розробити власний клієнт/інтеграцію.

Розглянемо як Microsoft Endpoint Manager інтегрується з DigiCert ONE Enterprise PKI Manager через SCEP (Simple Certificate Enrollment Protocol.

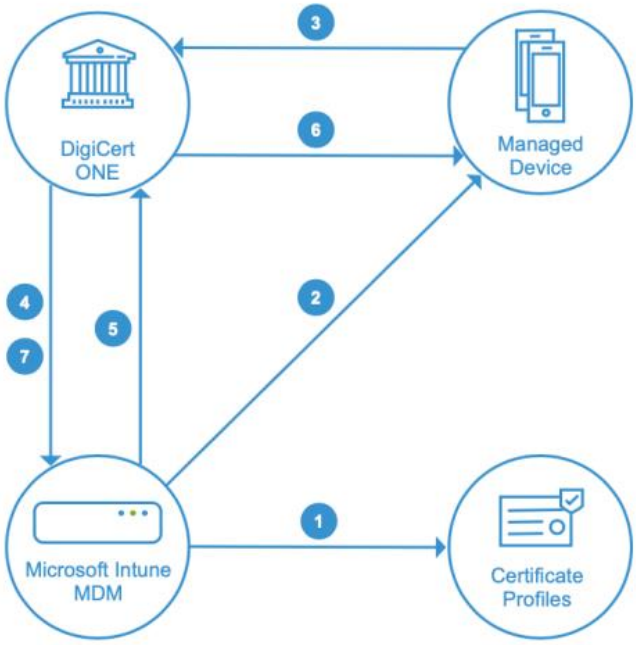

Рис. 3.2. Інтеграція Microsoft Endpoint Manager DigiCert ONE

1. Адміністратор Intune створює шаблони сертифікатів у Microsoft Intune відповідно до профілів сертифікатів, створених у DigiCert ONE Enterprise PKI Manager.

2. Microsoft Intune розгортає профілі конфігурації пристрою (типи довірених сертифікатів і SCEP) для вказаної групи кінцевих пристроїв.

3. Пристрій надсилає запит на сертифікат на основі профілів, розгорнутих у кроці 2, до DigiCert ONE.

4. DigiCert ONE перевіряє запит за допомогою Intune.

5. Microsoft Intune надасть відповідь перевірки службі DigiCert ONE SCEP.

6. DigiCert ONE видасть сертифікат на запитуваний пристрій.

7. Нарешті, DigiCert ONE надасть повідомлення підтвердження в Intune.

Для роботи DigiCert ONE SCEP необхідна реєстрація програми Azure Active Directory.

Її необхідно створити як реєстрацію програми, яку служба DigiCert ONE SCEP використовуватиме для зв’язку з Intune через API.

Метою цієї процедури є отримання ID програми (клієнта). Секрет клієнта (значення, а не ID) і Ім'я клієнта, яке використовуватиметься для налаштування профілю сертифіката в DigiCert ONE Enterprise PKI Manager.

3.2 Компоненти корпоративного шлюзу PKI DigiCert ONE Enterprise PKI Manager

1PKI Enterprise Gateway складається з таких компонентів:

• Служба RA – Служба RA авторизує користувача на основі профілів сертифікатів, які ви налаштували в PKI Manager. Потім він зв’язується з центром сертифікації DigiCert для запиту на видачу сертифіката. Служба RA захищає зв’язок із центром сертифікації DigiCert за допомогою сертифіката RA, щоб увімкнути автентифікацію клієнта SSL. Якщо служба RA налаштована на це, вона також публікує сертифікат у сховищі користувачів.

• RA Agent – RA Agent зв’язується зі службою RA для виконання видачі сертифіката від імені користувача. Агент RA потрібен, якщо ваш профіль сертифіката налаштовано для керування сертифікатами ОС\браузера (реєстрація клієнта без PKI).

• Служба автентифікації. Ця служба автентифікує користувача на основі облікових даних користувача Windows, а потім пересилає запит до служби RA. Це повинно бути встановлено на тому ж сервері, що й агент RA. DigiCert рекомендує захищати зв’язок між службою автентифікації та службою RA за допомогою SSL.

• Служба депонування та відновлення ключів – служба депонування та відновлення ключів отримує запити на реєстрацію для отримання сертифікатів. Служба депонування та відновлення ключів створює та депонує закритий ключ для запиту на реєстрацію сертифіката. Потім він надсилає запит і відкритий ключ до DigiCert CA для реєстрації сертифіката. Потім новий сертифікат із

закритим ключем повертається у відповіді на реєстрацію. Коли служба депонування та відновлення ключів отримує запит на відновлення ключа, вона пересилає запит до DigiCert CA для перевірки. DigiCert CA повертає інформацію, необхідну для отримання ключа з джерела даних депонування ключів. Служба депонування та відновлення ключів відновлює закритий ключ із джерела даних депонування ключів і повертає його у відповідь. Зв'язок зі службою депонування та відновлення ключів захищено за допомогою автентифікації клієнта та SSL. Зв'язок від служби депонування та відновлення ключів до DigiCert CA захищено за допомогою сертифіката RA. Сертифікат зберігається на апаратному модулі безпеки (HSM). Для тестових установок сертифікат RA може зберігатися в програмному сховищі ключів Java

Імпорт зовнішнього ключа – імпорт зовнішнього ключа дозволяє сертифікатам, виданим не DigiCert імпортувати на платформу DigiCert PKI. Ви повинні створити нову політику сертифіката та призначити сертифікати на основі вибраного сховища ключів. Можна зберігати імпортні сертифікати в локальному сховищі ключів або в сховищі ключів DigiCert.

Розглянемо варіанти технології розгортання одного або кількох серверів.

Шлюз PKI Enterprise Gateway можна встановити на одному сервері, де користувачі отримують доступ до PKI.

Служба сертифікації всередині мережі. Або ви можете встановити його на кількох серверах, де користувачі можуть отримати доступ до служби сертифікатів PKI поза межами мережі.

На рисунку 3.2 показано варіант, як PKI Enterprise Gateway зазвичай розгортається на підприємстві сайту в розгортанні одного сервера.

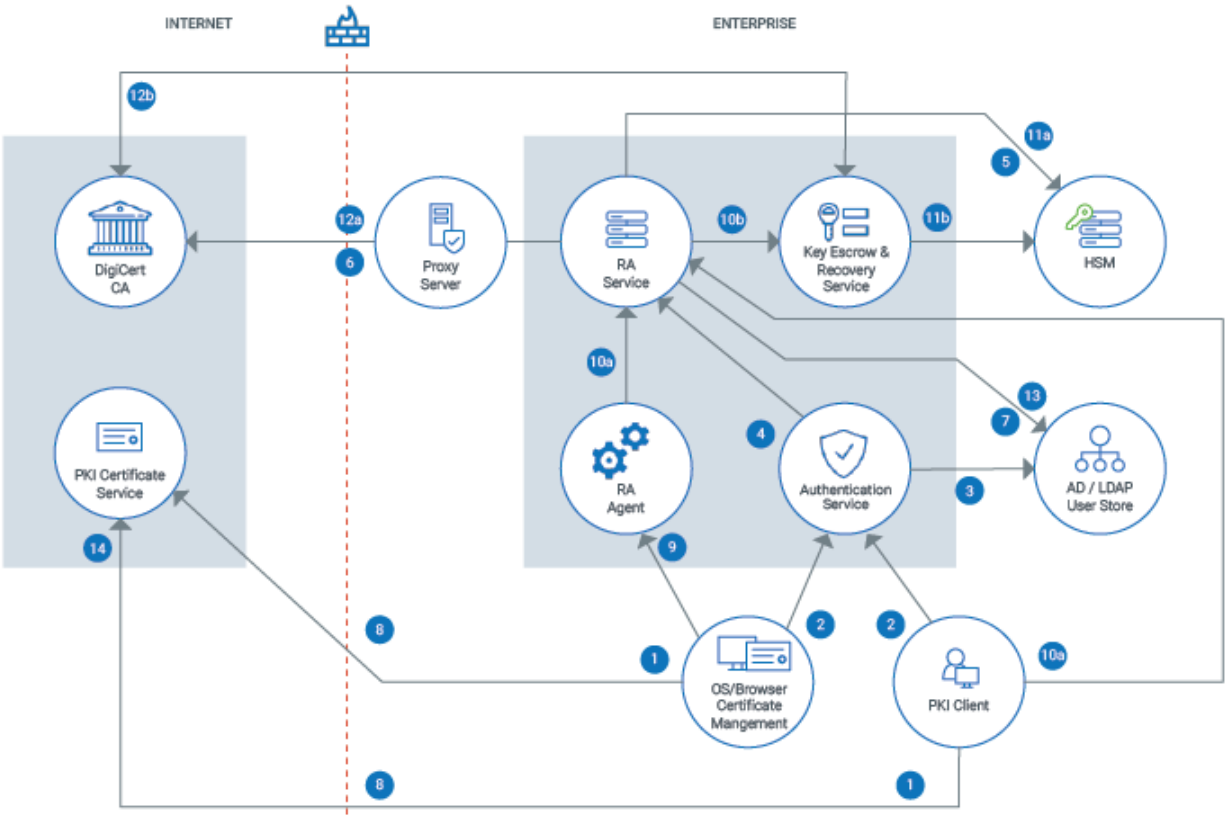

Рис.3.2. Односерверне розгортання корпоративного шлюзу PKI

На рисунку 3.3. показано, як PKI Enterprise Gateway зазвичай розгортається на сайті підприємства в розгортанні кількох серверів. Потоки для користувачів ідентичні як у корпоративній мережі, так і за її межами.

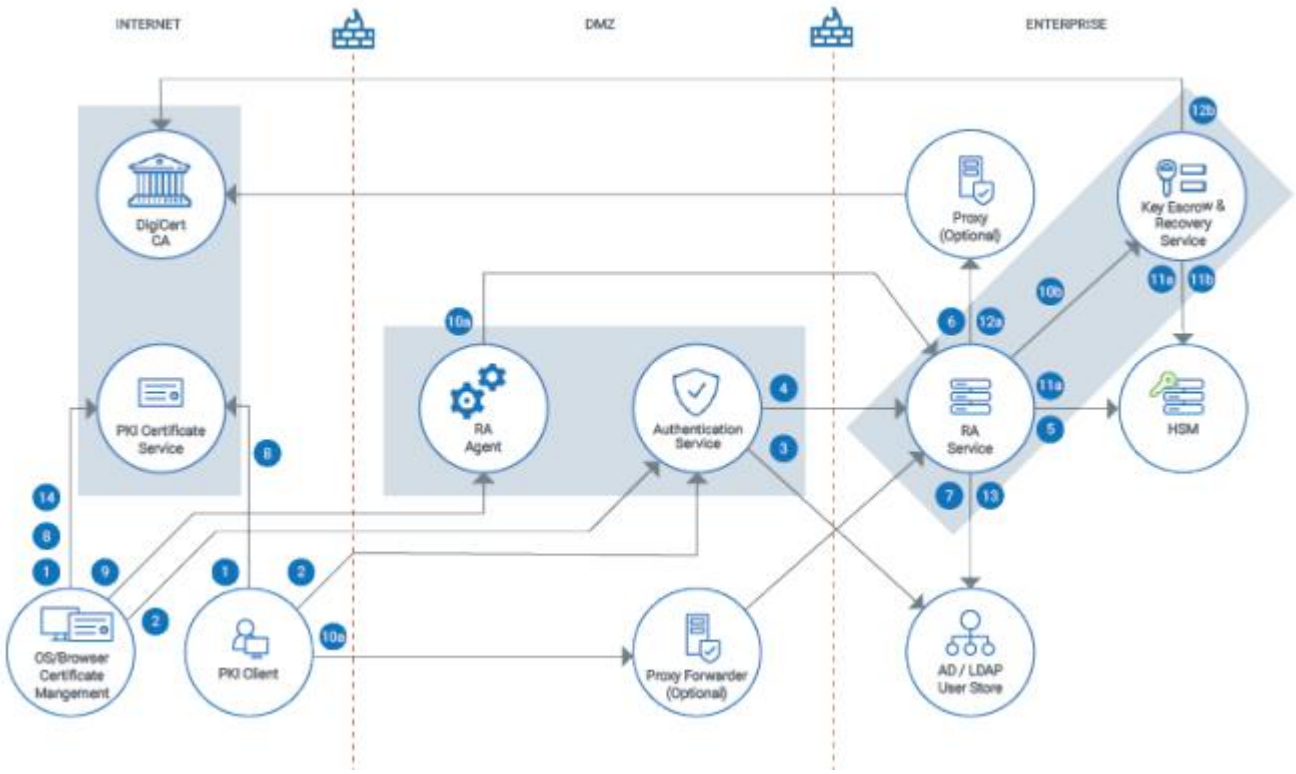

Рис. 3.3. Багатосерверне розгортання

В обох цих розгортаннях типовий процес реєстрації сертифіката буде таким:

1. Користувач отримує доступ до служби сертифікатів PKI, щоб зареєструватися для отримання сертифіката.

2. Облікові дані Windows користувача надсилаються до служби автентифікації.

3. Облікові дані Windows користувача перевіряються в корпоративному сховищі користувачів.

4. Служба автентифікації зв’язується зі службою RA, щоб отримати маркер безпеки. Маркер безпеки використовується для автентифікації для решти потік реєстрації.

5. Служба RA зв’язується з апаратним модулем безпеки (HSM), щоб використовувати сертифікат RA для захисту зв’язку з DigiCert CA.

6. Служба RA зв’язується з DigiCert CA, щоб отримати відповідну політику сертифікатів.

7. На основі політики сертифікатів служба RA отримує дані користувача, необхідні для реєстрації сертифіката, зі сховища користувачів.

8. Користувача буде перенаправлено до служби сертифікації PKI, де йому буде запропоновано надіслати запит на реєстрацію.

9. Лише для керування сертифікатами ОС\браузера користувач перенаправляється до агента RA для виконання запиту на реєстрацію.

10. Система робить запит на видачу сертифіката від DigiCert CA:

a) Або агент RA, або клієнт PKI надсилає запит до служби RA.

b) Якщо послугу депонування та відновлення ключів налаштовано, служба RA надсилає запит до служби депонування та відновлення ключів.

11. Система зв’язується з HSM, щоб використовувати сертифікат RA для захисту зв’язку з DigiCert CA.

a) Служба RA спілкується з HSM.

b) Якщо налаштовано службу депонування та відновлення ключів, служба депонування та відновлення ключа спілкується з HSM.

12. Система зв’язується з DigiCert CA, щоб запитати сертифікат.

a) Якщо службу депонування та відновлення ключів не налаштовано, служба RA зв’язується з ЦС DigiCert.

b) Якщо налаштовано службу депонування та відновлення ключів, служба депонування та відновлення ключа спілкується з центром сертифікації DigiCert.

13. Якщо службу RA налаштовано на це, вона публікує сертифікат у сховищі користувача.

14. Користувача буде перенаправлено до служби сертифікатів PKI для встановлення сертифіката та будь-якої подальшої обробки.

Розгортання відновлення ключів

На рис 3.4. показано, як зазвичай розгортається сервер депонування та відновлення ключів у розгортанні PKI Enterprise Gateway. Хоча на цій діаграмі показано розгортання з одним сервером, розгортання служби депонування ключів і відновлення є ідентичним як для розгортання з одним, так і для кількох серверів.

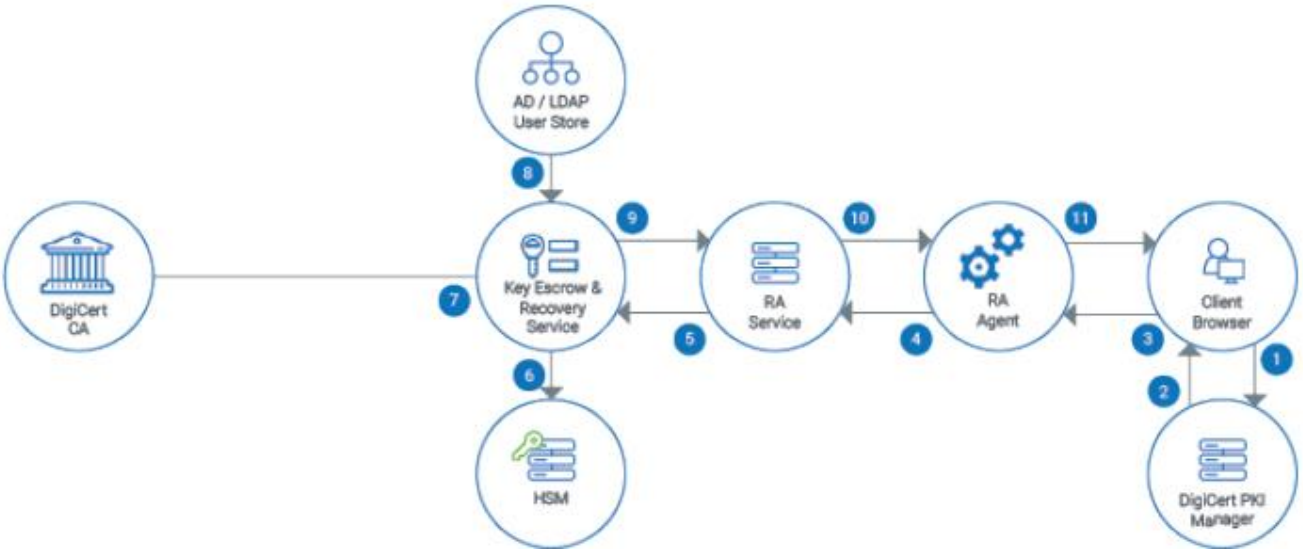

Рис.3.4. Депонування ключів і процес відновлення послуги від PKI Manager

Покажемо типовий процес відновлення сертифіката:

1. Адміністратор отримує доступ до DigiCert PKI Manager, щоб відновити закритий ключ для депонованого профілю сертифіката, який знаходиться на шлюзі підприємства.

2. Менеджер PKI перевіряє автентичність запиту від Enterprise Gateway, перш ніж перенаправляти його на сторінку агента RA.

3. Адміністратор перенаправляється на сторінку RA Agent.

4. Агент RA надсилає запит на відновлення ключа в службу RA.

5. Служба RA пересилає запит до служби депонування та відновлення ключів.

6. Служба депонування та відновлення ключів зв’язується з DigiCert CA за допомогою RA. Сертифікат на HSM.

7. Служба депонування та відновлення ключів зв’язується зі службою сертифікації PKI, щоб отримати облікові дані для зареєстрованого профілю сертифіката.

8. Служба депонування та відновлення ключів зв’язується з налаштованим сховищем даних користувача, щоб створити сертифікат із відновленим закритим ключем.

9. Служба депонування та відновлення ключів повертає сертифікат із відновленим закритим ключем і паролем до служби RA.

10. Служба RA пересилає його на локальну сторінку агента RA. Сертифікат і пароль доступні для завантаження на локальній сторінці.

3.3 Розробка рекомендацій щодо використання PKI DigiCert ONE Enterprise PKI Manager

DigiCert Enterprise PKI Manager є високомасштабованим, гнучким і використовує автоматизовані інструменти, які дійсно працюють у цьому новому світі віддалених і гібридних, асинхронних команд. Захистіть користувачів, електронну пошту, сервери, системи тощо з єдиного скла за допомогою потужних інструментів адміністративного доступу.

Тож основні рекомендації:

Використовуйте комплексний набір профілів сертифікатів, попередньо налаштованих для користувачів, пристроїв і серверів, у тому числі для автентифікації без пароля. Це прискористь швидке розгортання сертифіката.

Застосовуйте параметри ручної та автоматичної реєстрації для PKCS12, CSR, DigiCert Desktop Client, Microsoft Active Directory, автоматичну реєстрації Windows, автентифікації коду та двосторонньої автентифікації сертифіката клієнта TLS.

Уніфікуйте робочі процеси за допомогою контейнерної архітектури:

– Гнучкість розгортання для задоволення локальних, хмарних (публічних і приватних), гібридних і внутрішніх вимог.

– Висока масштабованість із автоматизованою оркестровкою для великого обсягу робочих навантажень.

– Швидкий час отримання вартості завдяки швидкому створенню CA та ICA.

– Уніфіковане керування робочими процесами PKI, що керують TLS, PKI підприємства, підписом коду, підписом документів і довірою пристроїв IoT.

ВИСНОВКИ

В результаті виконання магістерської роботи було отримано наступні наукові результати:

Основні завдання ІВК для надання установам, юридичним та фізичним особам послуг із забезпечення цілісності і достовірності інформації та різних даних, що представлені в електронному вигляді.

В результаті було проаналізовано основні органами, що розробляють стандарти інфраструктури відкритих ключів, а саме ITU-T, який проклав шлях у стандартизації PKI Рекомендації X.509.

В результаті аналізу архітектури інфраструктури відкритих ключів, було визначено що PKI використовується для шифрування та цифрових підписів, гарантуючи, що інформація, яку ви надсилаєте, залишається захищеною від зловмисників. PKI можна використовувати для забезпечення вашої ідентифікації в Інтернеті.

Було визначено що центр сертифікації або ЦС – це в основному організація або установа, яка уповноважена та відповідає за розповсюдження цифрових сертифікатів. Видача сертифіката є одним із важливих сегментів безпеки взаємодії, що відбувається через Інтернет. Як результат було проведено порівняння публічного та приватного центрів сертифікації.

Було досліджено компоненти сертифікатів та особливості їх створення та перевірки.

В результаті роботи отримано варіант інтеграції Microsoft Endpoint Manager DigiCert ONE на основі інфраструктури відкритих ключів та показано етапи їх роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Горбенко І.Д., Потій О.В., Концептуальні підходи до створення, впровадження та функціонування інфраструктури відкритих ключів національного банку україни. Вісник Української академії банківської справи. - № 1(20). - 2006р. – С. 95-100.

2. Enterprise PKI Manager [Електронний ресурс] – Режим доступу: https://www.digicert.com/pki/enterprise-pki-manager

3. Системи інфраструктури відкритих ключів [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/overlay-repository/government-wide-overlay-submissions/pki-systems

4. Архітектура PKI [Електронний ресурс] – Режим доступу: https://pki.com.ua/pki_architecture.html

5. ITU-T Recommendation X.509 (08/97), Information technology – Open Systems Interconnection – The Directory: Authentication framework

6. Internet RFC 2587, *Internet X.509 public key infrastructure – LDAPv2 schema* (by S. Boeyen, T. Howes and P. Richard), June 1999.

7. ISO/IEC 9594-8: 1998 (3rd edition), Information technology – Open Systems Interconnection – The Directory: Authentication framework

8. ITU-T Recommendation X.509 (11/93), *Information technology – Open Systems Interconnection – The Directory: Authentication framework* .

9. ITU-T Recommendation X.680 (12/97), Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

10. ITU-T Recommendation X.690 (12/97), Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

11. EMV ’96, Integrated Circuit Card Specification for Payment Systems. Version 3.1.1, May 31, 1998.

12. NIST FIPS PUB 180-1, *Secure hash standard*, April 1995.

13. NIST PIPS PUB 186-2, *Digital signature standard*, January 2000.

14. Internet RFC 2511, Internet X.509 certificate request message format (by M.Myers, C. Adams, D. Solo and D. Kemp), March 1999.

15. Internet RFC 2587, Internet X.509 public key infrastructure – LDAPv2 schema (by S. Boeyen, T. Howes and P. Richard), June 1999.

16. Internet RFC 2560, X.509 internet public key infrastructure – Online certificate status protocol (OCSP) (by M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams), June 1999.

17. PKI [Електронний ресурс] – Режим доступу: https://thecyphere.com/blog/pki-explained/ /

18. Public vs privat CA [Електронний ресурс] – Режим доступу: https://ipwithease.com/public-vs-private-certificate-authority/ /

19. Складові сертивікату [Електронний ресурс] – Режим доступу: https://docs.oracle.com/cd/E19656-01/821-1507/gdzcw/index.html

20. Digicert-one-enterprise-pki-manager [Електронний ресурс] – Режим доступу: https://knowledge.digicert.com/content/dam/digicertknowledgebase/attachments/pki-platform/microsoft-intune/digicert-one-enterprise-pki-manager-microsoft-intune-scep-integration-guide-v-1-1.pdf .

21. Microsoft Intune [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)