Інфраструктура відкритих ключів

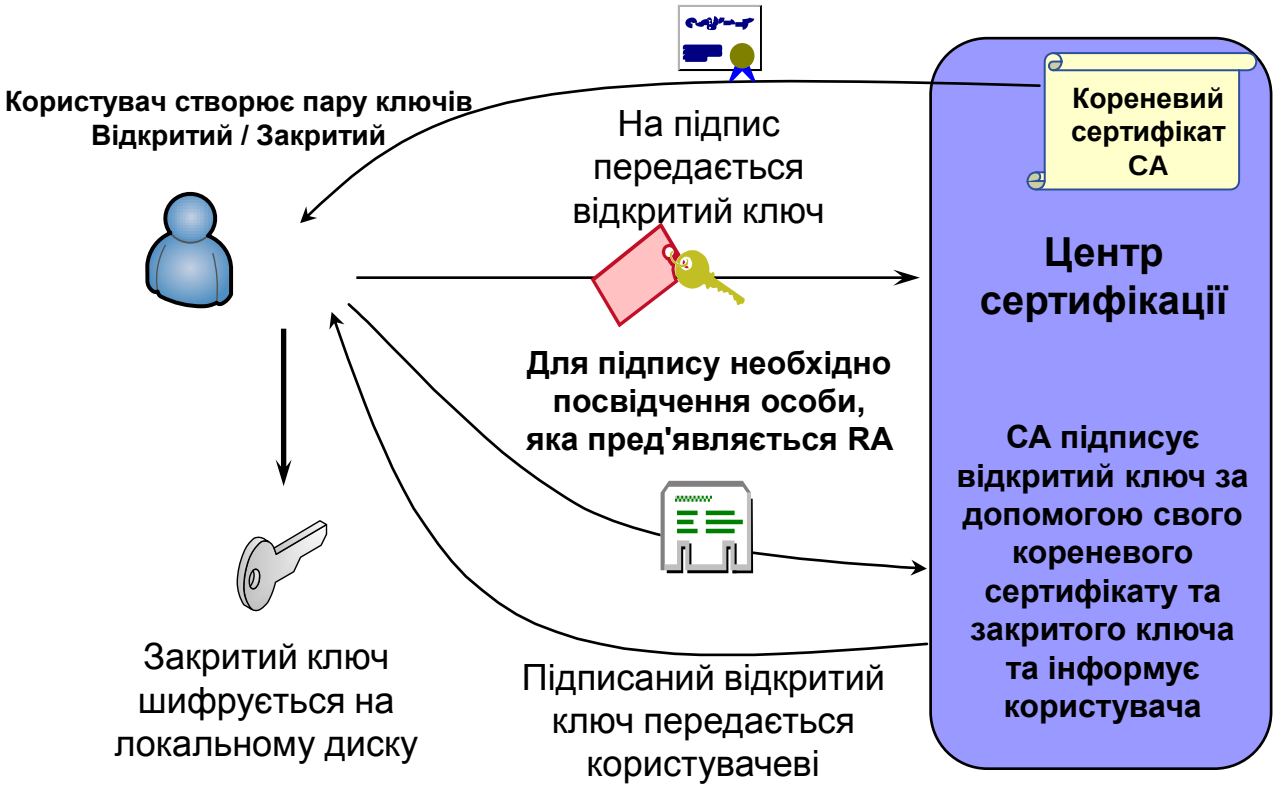
План лекції

- Можливості PKI
- Основні компоненти інфраструктури відкритих ключів
- Цифровий сертифікат
- Електронний цифровий підпис
- Автентифікація за допомогою сертифікатів

Інфраструктура відкритих ключів

- Інфраструктура відкритих ключів (PKI - Public Key Infrastructure) - це технологія аутентифікації, що використовує для ідентифікації суб'єктів криптографію з відкритими ключами разом з наступними механізмами
  - Механізмом встановлення довіри на базі певної моделі довіри
  - Механізмом присвоєння суб'єктам імен, унікальних в даному середовищі
  - Механізмом поширення інформації, що характеризує правильність зв'язування певної пари ключів (відкритого та закритого) з певним ім'ям суб'єкта в даному середовищі (така інформація фіксується і надається центром, якому довіряє верифікатор інформації)
- Інфраструктура відкритих ключів являє собою комплексну систему, сервіси якої реалізуються та надаються з використанням технології відкритих ключів. Мета PKI полягає в управлінні ключами та сертифікатами

Отримання сертифікату



Основні компоненти PKI

- Засвідчувальний центр (Центр сертифікації)
- Реєстраційний центр
- Репозиторій сертифікатів
- Архів сертифікатів
- Кінцеві суб'єкти

Засвідчувальний центр (ЗЦ) сертифікує зв'язування пари ключів з суб'єктом, завіряє цифровим підписом структуру даних, яка містить деяке уявлення суб'єкта і відповідного відкритого ключа. Ця структура даних називається **сертифікатом відкритого ключа.**

Засвідчувальний центр відомий суб'єктам PKI за двома атрибутам: назвою і відкритим ключем. Засвідчувальний центр включає своє ім'я в кожен випущений їм сертифікат і в список відкликаних сертифікатів і підписує їх за допомогою власного закритого ключа. Користувачі можуть ідентифікувати сертифікати за ім'ям засвідчувального центру і переконатися в їх достовірності, використовуючи його відкритий ключ.

Функції засвідчувального центру

- Формує власний закритий ключ; якщо є головним ЗЦ, то видає і підписує свій сертифікат, називається **самовиданний** або **самоподпісанний**
- Випускає (тобто створює і підписує) сертифікати відкритих ключів підлеглих засвідчувальних центрів та кінцевих суб'єктів PKI; може випускати крос-сертифікати, якщо пов'язаний відношеннями з іншими PKI
- Підтримує реєстр сертифікатів (базу всіх виданих сертифікатів) і формує списки відкликаних сертифікатів з регулярністю, визначеної регламентом ЗЦ
- Публікує інформацію про статус сертифікатів і список відкликаних сертифікатів

Функції компонент PKI

- **Реєстраційний центр (РЦ)** є обов'язковим компонентом PKI. Зазвичай РЦ отримує від засвідчувального центру повноваження реєструвати користувачів, забезпечувати їх взаємодію з ЗЦ і перевіряти інформацію, яка заноситься в сертифікат.
- **Репозиторій** - спеціальний об'єкт інфраструктури відкритих ключів, база даних, в якій зберігається реєстр сертифікатів.
- На **архів сертифікатів** покладається функція довгочасного зберігання (від імені ЗЦ) та захисту інформації про всі видані сертифікати.
- **Кінцеві суб'єкти**, і користувачі, PKI діляться на дві категорії: власники сертифікатів і сторони які довіряють. Власником сертифіката може бути фізична або юридична особа, додаток, сервер і т.д. Сторони з довірою запитують і покладаються на інформацію про статус сертифікатів і відкритих ключах підписи своїх партнерів по діловому спілкуванню.

Формат сертифікатів відкритих ключів X.509

- **Сертифікат відкритого ключа** являє собою структурований двійковий запис у форматі абстрактної синтаксичної нотації ASN.1. Сертифікат містить елементи даних, супроводжувані цифровим підписом **видавця сертифіката**. У сертифікаті є десять основних полів: шестеро обов'язкових і чотири опціональних. Велика частина інформації, що вказується в сертифікаті, не є обов'язковою, а зміст обов'язкових полів сертифіката може варіюватися.
- **Обов'язкові поля сертифіката**
  - Серійний номер сертифіката.
  - Ідентифікатор алгоритму підпису.
  - Ім'я видавця.
  - Період дії.
  - Відкритий ключ суб'єкта.
  - Ім'я суб'єкта сертифіката.

Додаткові поля сертифіката

- Опціональне поле **Доповнення** з'являється у сертифікатах третьої версії. Кожне доповнення складається з **ідентифікатора типу доповнення, ознаки критичності** і власне **значення доповнення**.
- Всі доповнення можна розділити на дві категорії: **обмежуючі** та **інформаційні**. Перші обмежують область застосування ключа, визначеного сертифікатом, або самого сертифіката. Другі містять додаткову інформацію, яка може бути використана в прикладному програмному забезпеченні користувачем сертифіката
- **Обмежуючі доповнення**
  - Основні обмеження
  - Призначення ключа
  - Розширене призначення ключа
  - Політики застосування сертифіката
  - Обмеження на імена
- **Інформаційні доповнення**
  - Ідентифікатори ключів
  - Альтернативні імена
  - Пункт поширення списку анульованих сертифікатів
  - Спосіб доступу до інформації ЗЦ

Структура сертифіката

Структура сертифіката (RFC3280)

Distinguished Name (DN) – унікальне ім'я суб'єкта, оформлене в стилі X.500:

/C=UA/O=UGrid/CN=UGrid CA

Області використання :
аутентифікація, перевірка цілісності, цифровий підпис, non-repudiation.

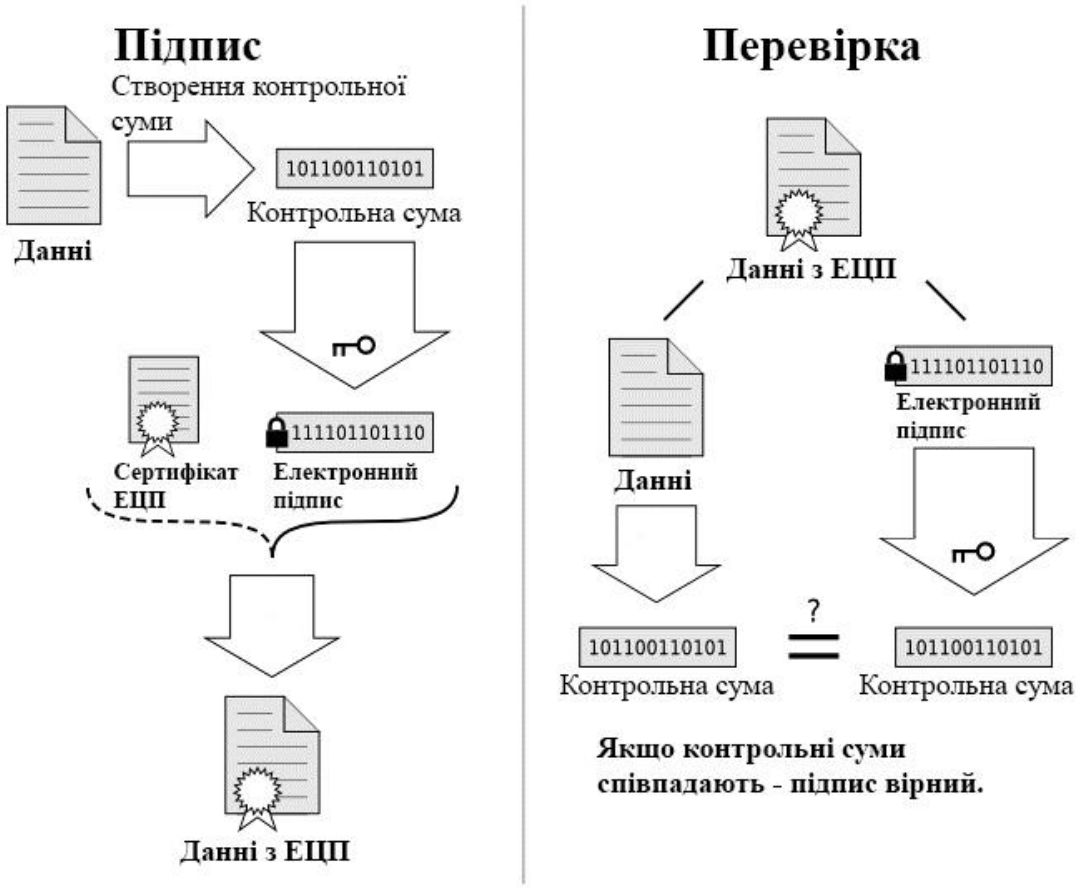
Цифровий підпис - геш (hash) даних, зашифрований закритим ключем.

Підпис можна перевірити за допомогою відкритого ключа.

Третя довірена сторона (CA) засвідчує приналежність сертифіката певної сутності, визначеної DN.

Довіра до сертифікату будується на довірі третій стороні, що підписала цей сертифікат.

Цифровий підпис



Електронний цифровий підпис

- Електронний цифровий підпис (ЕЦП) - реквізит електронного документа, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа підпису, що дозволяє встановити відсутність спотворення інформації в електронному документі з моменту формування підпису та перевірити приналежність підпису власнику сертифіката ключа підпису.
- Процедура формування цифрового підпису документа
  - Обчислюється значення хеш-функції від даних, що знаходяться в документі.
  - За допомогою закритого ключа суб'єкта, що формує цифровий підпис, значення хеш-функції зашифровується.
  - До вихідного документу приєднується отримане на попередньому кроці значення.

Перевірка цифрового підпису документа

- У документі виділяється цифровий підпис, визначається ідентифікатор суб'єкта, згенерованого цифровий підпис і алгоритм її генерації.
- За допомогою відкритого ключа суб'єкта розшифровується значення цифрового підпису.
- Обчислюється значення хеш-функції від даних, що знаходяться в документі.
- Порівнюються значення, отримані на двох попередніх етапах, якщо вони збігаються, робиться висновок про те, що документ від автора до кінцевого користувача був переданий без модифікації, тобто, підтверджена його цілісність.

Центри сертифікації

https://www.comodo.com/

https://www.symantec.com/

https://ca.godaddy.com

https://www.globalsign.com

https://www.digicert.com

Інструменти для генерації та перевірки цифрових сертифікатів

- Основним інструментом, який виконує повний набір функцій для інфраструктури відкритих ключів, є застосування OpenSSL.
- Можливості OpenSSL :
  - Симетричне шифрування/дешифрування
  - Реалізація S/MIME для підписування і шифрування в електронній пошті
  - Асиметричне шифрування/дешифрування
  - Реалізація функцій для інфраструктури відкритих ключів
  - Генерація ключів для асиметричних алгоритмів шифрування
  - Генерація цифрового підпису
  - Реалізація SSL/TLS клієнта/сервера
  - Кодування/декодування
  - Перетворення форматів зберігання ключів, сертифікатів
  - Гешування