Урок 8. Особистий та відкритий ключі. Сертифікат відкритого ключа OCR-технології для розпізнавання паперових документів

Ключ - параметр криптографічної системи, який використовується для

- шифрування і/або дешифрування повідомлення при шифруванні;
- накладення та перевірки коду автентифікації повідомлень або електронного цифрового підпису.

У асиметричних криптосистемах ключі зазвичай створюються парами: ключ шифрування, та ключ дешифрування. Якщо знаючи один можна легко отримати інший, та навпаки (наприклад вони збігаються), то криптосистема називається шифруванням з симетричними ключами. Якщо ж з одного можна отримати інший, але навпаки дуже важко, то така система називається шифруванням з несиметричними ключами.

Приклади ключів:

- Відкритий ключ - ключ, котрий дозволяється передавати по відкритому каналу зв'язку, а таємний ключ - мусить зберігатися таємно, або передаватися з використанням закритого каналу зв'язку.
- Сеансовий ключ - ключ, що використовується під час сеансу обміну повідомленнями для захисту каналу зв'язку.

Жоден ключ шифрування не можна використовувати нескінченно. Час його дії має минати автоматично, подібно дозвільним документам, оскільки:

- чим довше використовується ключ, тим більша ймовірність його компрометації;
- чим довше використовується ключ, тим більші втрати при компрометації ключа;
- чим довше використовується ключ, тим більша спокуса прикласти необхідні зусилля для його розкриття. Наприклад, розкриття ключа, який використовується протягом доби, дозволить прочитати всі повідомлення, передані протягом доби;
- у низці випадків трудомісткість криптоаналізу визначається кількістю шифротекстів, отриманих у результаті шифрування одним ключем.

Для будь-якого криптографічного додатка необхідна стратегія, що визначає допустимий термін дії ключа. В залежності від застосування, різні ключі можуть мати різні періоди життя. Термін дії ключа не повинен бути надто тривалим та може залежати від важливості та обсягів даних, зашифрованих протягом заданого періоду. При виборі терміну дії ключа слід збалансувати ризики, пов'язані з заміною ключа або використанням фіксованого ключа.

Стандарт ISO/IEC 10770 здійснює класифікацію ключів за такими ознаками:

За типом криптосистеми

- Симетрична (симетричні ключі)
- Несиметрична (особистий (таємний) ключ та відкритий ключ)

За призначенням

- Системи шифрування (ключі шифрування, ключі дешифрування, вектори ініціалізації)
- Системи автентифікації (ключі печаток (MAC), ключі підпису, ключі перевірки підпису)

За ієрархією

- Головні ключі
- Ключі шифрування ключів
- Транспортні ключі
- Ключі даних

За часом використання

- Короткострокові ключі
- Довгострокові ключі.

Генерація ключів повинна здійснюватись апаратними генераторами випадкових чисел або криптографічно стійкими генераторами псевдовипадкових чисел. Якщо можлива атака на генератор псевдовипадкових чисел, то можливе дешифрування криптограм зі складністю, меншою ніж складність атаки грубою силою навіть при відсутності вразловостей у алгоритмах шифрування.

Ключі повинні ***зберігатись і використовуватись*** у апаратних криптографічних модулях, смарт-картках та токенах, які не дозволяють експорт ключа у незашифрованому вигляді.

Після виведення з дії ключі повинні знищуватись способом, який не допускає їх відновлення. Найнадійнішим способом є знищення носія ключів (механічне, термічне тощо). Допускається повний перезапис носія.

Відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Відкритий ключ використовується для перевірки ЕП документів (файлів), які отримані. Він працює тільки в парі з закритим (особистим) ключем.

Відкритий ключ міститься в сертифікаті відкритого ключа, і підтверджує приналежність відкритого ключа ЕП певній особі. Крім самого відкритого ключа, сертифікат відкритого ключа містить в собі персональну інформацію про його власника (ім'я, реквізити), унікальний реєстраційний номер, термін дії сертифіката відкритого ключа.

Для забезпечення безпеки і виключення підміни відкритих ключів Центр «Україна» проводить сертифікацію відкритих ключів ЕП шляхом підписання відкритого ключа користувача своїм секретним ключем - ключем Центру.

Власнику ключа ЕП видається сертифікат відкритого ключа, який містить такі відомості:

- відкритий ключ ЕП;
- ім'я власника, інші ідентифікуючі дані;
- терміни дії ключа;
- унікальний номер сертифіката відкритого ключа ЕП;
- найменування центру, який видав сертифікат.

Сертифікат ключа ЕП в електронному вигляді, підписаний секретним ключем Центру «Україна», направляється користувачу ЕП і вноситься до реєстру сертифікатів Центру, а також за бажанням користувача може бути опублікований на веб-сайті АЦСК «Україна».