УДК 004.056.006.1

ПРИНЦИПИ ТА ПІДХОДИ ЩОДО СЕРТИФІКАЦІЇ ЕЛЕКТРОННОГО ПІДПИСУ

К.Л. Шевченко, доктор технічних наук, професор
Київський національний університет технологій та дизайну
І.І. Карпенко, магістрант
Київський національний університет технологій та дизайну

Ключові слова: електронний підпис, сертифікація, нормативно правова база, перевірка, накладання.

Розвиток суспільних відносин і ринкової економіки в Україні зумовлює збільшення кількості договорів, які укладаються в електронній формі. Можливість їх укладення залежить від ефективного правового регулювання використання електронних підписів. Варто зазначити, що 3 вересня 2015 року прийнято Закон України «Про електронну комерцію», яким установлено порядок учинення електронних правочинів, при цьому визначено види електронних підписів. Закон України «Про електронний цифровий підпис» прийнятий ще 22 травня 2003 року. Проте ці законодавчі акти не конкретизують механізм використання електронних підписів, містять суперечності. Тому наукові дослідження із цієї проблеми є актуальними.

Перевірка електронного цифрового підпису – це операція, яка виконується отримувачем захищеного електронного документу з використанням відкритого ключа підписувача (відправника). Для виконання цієї операції необхідно отримати відкритий ключ відправника (наприклад, із довідника) та захищеного документа (тобто даних документа та даних ЕЦП). Відповідний програмний модуль перевіряє, чи дійсно цифровий підпис відповідає документу та відкритому ключу. Якщо в документ або у відкритий ключ внесено будь-які зміни, перевірка закінчиться із негативним результатом. Для повноцінного функціонування систем ЕЦП необхідно забезпечити доступ отримувача до достовірної копії відкритого ключа відправника (підписувача) та можливість перевірити, що це копія відкритого ключа належить саме цьому підписувачу. Для виконання цієї процедури створюються спеціальні захищені довідники ключів, які ведуться спеціальними установами – центрами сертифікації ключів.

Центри сертифікації ключів перевіряють дані власника відкритого ключа та видають захищені електронні документи спеціального зразка – сертифікати відкритих ключів, в яких міститься відкритий ключ та перевірена центром сертифікації інформація про власника ключа. Сертифікат відкритого ключа підписується електронним цифровим підписом центру сертифікації ключів. Таким чином, достатньо отримати достовірним каналом лише один електронний документ – сертифікат самого центру сертифікації ключів, щоб мати можливість перевірити достовірність будь-якого сертифікату, що виданий цим центром сертифікації ключів.

Правила сертифікації – документ, у якому описані індивідуальні для кожного центру сертифікації правила, за якими перевіряються відомості, що знаходяться у сертифікаті. Тобто, не всі центри сертифікації ключів діють за однаковими правилами та вимогами при перевірці документів, що встановлюють особу-власника ключа (ці правила також називаються «політикою сертифікації»). Правила сертифікації, якими користується центр сертифікації, та клас сертифікату безумовно безпосередньо впливають на рівень довіри до сертифікатів ключів, які видані такими центрами сертифікації. Тобто, довіра до сертифікату відкритого ключа залежить не тільки від того факту, що відкритий ключ сертифіковано, а також від того, ким (яким центром сертифікації) сертифіковано та за якими правилами.

За даними останніх досліджень впровадження технологій шифрування з відкритими ключами на корпоративному рівні без використання цифрових сертифікатів представляється малоефективним. Внаслідок необхідності сертифікатів, що підтверджують особу власника відкритого ключа, керування сертифікатами є невід'ємною частиною системи з відкритими ключами. Подібно до аналогової системи сертифікації, внутрішня система керування (така, як система e-Lock фірми Frontier Technologies, що містить компоненти для обробки цифрового підпису, Secure MIME і управління сертифікатами) видає сертифікати на відкриті ключі, перевіряючи спочатку особу користувача.

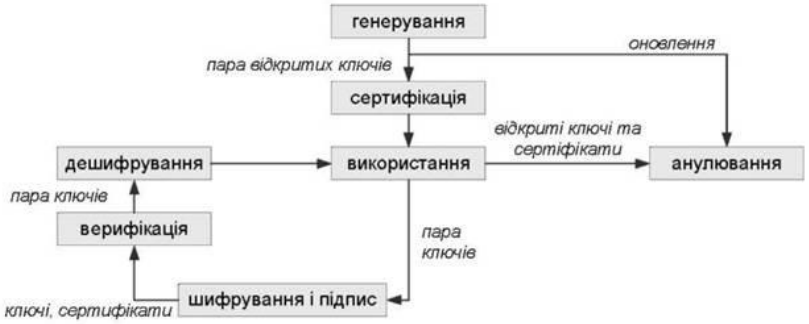

Рис. 1 - Схема життєвого циклу ключів

Таким чином ефективне рішення питання управління сертифікатами також має передбачати спосіб ведення списку анульованих сертифікатів з оновленням в режимі реального часу, оскільки відкритий ключ може використовуватись для шифрування окремо від сертифікату, отже, представляється необхідним одночасне видалення із системи пари відкритих ключів разом із відповідними сертифікатами.

Список використаних джерел

1.Закон України «Про електронні довірчі послуги» від 05.10.2017 р. №2155-VIII [Електронний ресурс] // Офіційний веб-портал Верховної Ради України - Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n534

2. Закон України « Про електрону комерцію» від 03.09.2015 № 675-VIII [Електронний ресурс] // Офіційний веб-портал Верховної Ради України - Режим доступу: https://zakon.rada.gov.ua/laws/show/675-19