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».

Передавання електронних документів. Зберігання електронних документів. Забезпечення конфіденційності електронних документів. Електронний офіс.

Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання.

Вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону.

Одержання електронних документів

Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

Якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження.

У разі ненадходження до автора підтвердження про факт одержання цього електронного документа вважається, що електронний документ не одержано адресатом.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, електронний документ вважається відправленим автором та одержаним адресатом за їх місцезнаходженням (для фізичних осіб — місцем проживання), у тому числі якщо інформаційна, телекомунікаційна, інформаційно-телекомунікаційна система, за допомогою якої одержано документ, знаходиться в іншому місці. Місцезнаходження (місце проживання) сторін визначається відповідно до законодавства.

Зберігання електронних документів

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;
2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;
3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така установа додержується вимог цієї статті. Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

Кожен одержаний адресатом електронний документ перевіряється на цілісність і справжність усіх накладених на нього електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки (далі - електронні печатки). При цьому необхідно, щоб:

- кожен електронний цифровий підпис був підтверджений з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідав відкритому ключу, зазначеному у сертифікаті;
- на час перевірки був чинним посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

Електронний офіс – система всебічного використання в управлінській діяльності засобів обчислювальної техніки і телекомунікацій.

Електронний офіс втілює концепцію всебічного використання в офісній діяльності засобів обчислювальної техніки та зв’язку з одночасним збереженням та підсиленням переваг традиційного та виробничого офісу.

Етапи розвитку концепції електронного офісу:

- електронні засоби опрацювання текстів;
- локальні комп’ютерні мережі і автоматизація робіт з документаційного забезпечення управління;
- розвиток телекомунікаційних систем і автоматизовані робочі місця персоналу офісу;
- електронні архіви і сховища даних;
- регіональні і глобальні комп’ютерні мережі.

Практичне втілення концепції електронного офісу - це трудомісткий, багатоетапний процес, який умовно можна розділити на дві стадії:

- електронізація;
- організація.

На офіс покладають основні функції організації та управління зрегулювання діяльності підприємства уцілому.

Основні функції електронного офісу:

- реалізація можливості ефективно підтримувати і розвивати зв'язки з партнерами, успішно пристосовуватись до швидкозмінюваної економічної ситуації;
- включення фірми до інформаційних структур ринкової економіки країни та світу, доступ до комерційних баз даних, проведення електронного маркетингу, рекламних та інформаційних заходів;
- координація діяльності всередині і зовні організації;
- допомога у виробленні і прийнятті ефективних рішень;
- виключення затримок і помилок при опрацюванні інформації, документів.

Текстові редактори (або сучасні текстові процесори) є першим компонентом електронного офісу, оскільки проблема обробки тексту і його перетворення є одним із основних завдань діловодства.

Поява наступного компонента дозволила реалізувати за допомогою комп'ютера функцію інформаційного обміну, що належала системі телефонного і поштово-телеграфного зв'язку. Таким компонентом стала система електронної пошти для обміну інформацією між користувачами на багатокористувацьких комп'ютерах, а потім і в мережах.

Значно пізніше стали використовуватися системи розробки баз даних, а також електронні таблиці для виконання різних розрахунків.

Надалі в офісах стали використовуватися системи ділової графіки, необхідні для наочності виконуваних офісних процедур.

Усі перераховані компоненти службової діяльності персоналу офісу відповідають спеціалізованим пакетам, призначеним для комплексної автоматизації згаданих функцій. Одним із таких пакетів є офісна система Microsoft Office. Усі програмні продукти цієї системи не тільки уніфіковані, але й інтегровані між собою, що дає змогу в рамках рішення певної ділової проблеми здійснювати інформаційний обмін незалежно від того, який тип документа опрацьовується.

Використання ПК в офісі не виключає, а, навпаки, підсилює роль засобів організаційної техніки, розробленої на основі застосування новітніх досягнень електроніки.

На сучасному етапі розвитку інформаційних технологій до структури системи автоматизації документообігу електроного офісу традиційно включають наступні підсистеми:

- технології обробки зображень документів (Imaging System);
- системи оптичного розпізнання символів (Optical Character Recognition System, OCR);
- системи керування документами, СКД (Document Management System, DMS);
- повнотекстові бази даних (Full-Text System);
- системи автоматизації ділових процедур, АДП (Workflow System);
- програмне забезпечення для робочих груп (Groupware),
- елементи та зв'язки між ними.

Впровадження електронних офісів стало реальністю завдяки досягненням в галузях виробництва комп'ютерної техніки та високоефективних засобів організаційної техніки.

Не дивлячись на короткий термін існування електронний офіс вже пройшов три стадії розвитку.

Для ***першого етапу*** була характерною орієнтація на автоматизацію рутинних, часто повторюваних операцій, яка здійснювалась секретарями або технічним персоналом організації. Характерним прикладом таких робіт є машинописні роботи. Для підвищення продуктивності праці при їх виконанні були створені, так звані пристрої обробки текстів, які дозволили швидко виправляти та редагувати різні документи, а також створювати і використовувати шаблони при підготовці документів також створювати і використовувати шаблони при підготовці документів.

На ***другому етапі*** розвитку електронних офісів окремі пристрої об'єднувалися за допомогою внутрішніх ліній в єдину мережу, що дозволяло виконувати ряд додаткових функцій, таких, як автоматизований зв'язок між різними робочими місцями, сумісна робота над документами, автоматизований контроль за виконанням документів і т.д.

Третій етап розвитку електронних офісів пов'язаний з широким застосуванням персональних комп'ютерів і створенням на їх основі автоматизованих робочих місць. Ці автоматизовані робочі місця об'єднувалися за допомогою комутаційних засобів в єдину систему (мережу), яка забезпечувала загальний доступ до всіх обчислювальних ресурсів офісу, баз даних, а також зовнішніх джерел інформації. Це дозволило значно прискорити інформаційний обмін між користувачами мережі,

автоматизувати деякі традиційні операції, зв’язані з прийомом та відправленням кореспонденції та іншої документації по каналах зв’язку.

У той же час впровадження електронних офісів має і деякі негативні наслідки. Основним з них є негативний вплив на організм людини електронної техніки, яка інтенсивно використовується на робочих місцях. Крім того, погіршуються можливості особистих контактів персоналу офісу, що впливає на загальний психологічний клімат у колективі. Слід зазначити, що в результаті електронізації офісу змінюються кваліфікаційні вимоги до персоналу, що може створити конфліктні ситуації.

Нові технічні засоби й інформаційні технології покликані забезпечити підвищення продуктивності праці в офісній і адміністративній діяльності. Поряд із цим технічні засоби і комп'ютерні технології, адміністративні й офісні системи виконують, по суті, допоміжні роботи, зв'язані з обробкою інформаційних масивів. Процес прийняття рішень залишається прерогативою людини. Але завдяки автоматизації деяких процесів керування персонал офісу звільняється від виконання рутинних операцій і приділяє більше часу аналітичним та творчим процесам