УДК 004

О.Лаврусенко, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЗОРОГО ШИФРУВАННЯ ДАНИХ З ЗАСТОСУВАННЯМ ЗАСОБІВ PKI

У статті програмне забезпечення, яке призначено для системи прозорого шифрування даних з застосуванням засобів PKI. Метою розробки є дослідження та програмна реалізація системи прозорого шифрування даних з застосуванням засобів PKI. Об'єктом дослідження є процес прозорого шифрування даних з застосуванням засобів PKI. Предметом дослідження є методи прозорого шифрування даних з застосуванням засобів PKI. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи прозорого шифрування даних з застосуванням засобів PKI. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, шифрування даних, PKI

Постановка проблеми. На сьогоднішній день уже кожний чув повідомлення про те, як особисті або конфіденційні дані були втрачені через крадіжку або втрату портативного комп'ютера. Портативні комп'ютери пропадають постійно. З ростом числа розкрадань особистих даних і при більш ніж будь-коли високою важливістю дотримання нормативних вимог ретельний захист даних на мобільних комп'ютерних системах украй важливий.

Одним з рішень є використання файлової системи EFS (Encrypting File System – шифрована файлова система), що забезпечує убудоване високоефективне шифрування диска. Система EFS працює однаково добре із власними технологіями перевірки дійсності й контролю доступу системи Windows, так що користувачам не потрібно запам'ятовувати для доступу до своїх даних окремі паролі. І, нарешті, система EFS забезпечує зручні варіанти відновлення даних у випадку втрати користувачем доступу до своїх ключів шифрування (наприклад у випадку видалення або ушкодження профілю користувача або у випадку втрати смарт-карти).

Для генерування, зберігання й розгортання ключів для захисту даних у системі EFS використовується технологія відкритих ключів шифрування (PKI). У даному магістерському проекті для шифрування даних на диску у файловій системі EFS використовується алгоритм стандарту DES. Ці симетричні ключі потім захищаються асиметричною парою ключів (RSA). У системі EFS кожний файл шифрується своїм власним ключем DES, потім цей ключ шифрується користувальницьким ключем RSA і результат зберігається у файл.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи прозорого шифрування даних з застосуванням засобів PKI.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи прозорого шифрування даних з застосуванням засобів PKI.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем прозорого шифрування даних з застосуванням засобів PKI.
- Дослідження системи прозорого шифрування даних з застосуванням засобів PKI.

– Програмна реалізація системи прозорого шифрування даних з застосуванням засобів PKI.

Об'єктом дослідження є процес прозорого шифрування даних з застосуванням засобів PKI.

Предметом дослідження є методи прозорого шифрування даних з застосуванням засобів PKI.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу

PKI, або інфраструктура відкритих ключів, охоплює все, що використовується для встановлення та керування шифруванням відкритих ключів. Це включає програмне забезпечення, апаратне забезпечення, політики та процедури, які використовуються для створення, розповсюдження, керування, зберігання та відкликання цифрових сертифікатів.

Цифровий сертифікат криптографічно пов'язує відкритий ключ із пристроєм або користувачем, який ним володіє. Це допомагає автентифікувати користувачів і пристрої та забезпечити безпечний цифровий зв'язок.

PKI є однією з найпоширеніших форм шифрування в Інтернеті, яка використовується для захисту та автентифікації трафіку між веб-браузерами та веб-серверами. Його також можна використовувати для захисту доступу до підключених пристроїв і внутрішніх комунікацій в організації.

Інфраструктура відкритих ключів має довгу історію захисту та автентифікації цифрових комунікацій з двома основними цілями: забезпечити конфіденційність повідомлення, що надсилається, і перевірити, чи відправник є тим, за кого себе видає.

Що таке інфраструктура відкритих ключів (PKI)?

Інфраструктура відкритих ключів є важливим аспектом безпеки в Інтернеті. Це набір технологій і процесів, які складають основу шифрування для захисту та автентифікації цифрових комунікацій.

PKI використовує криптографічні відкриті ключі, пов'язані з цифровим сертифікатом, який автентифікує пристрій або користувача, який надсилає цифрове повідомлення. Цифрові сертифікати видаються надійним джерелом, центром сертифікації (CA), і діють як тип цифрового паспорта, щоб гарантувати, що відправник є тим, за кого себе видає.

Інфраструктура відкритого ключа захищає та перевіряє зв'язок між серверами та користувачами, наприклад між вашим веб-сайтом (розміщеним на вашому веб-сервері) та вашими клієнтами (користувач, який намагається підключитися через свій браузер. Її також можна використовувати для безпечного зв'язку всередині організації, щоб забезпечити що повідомлення бачать лише відправник і одержувач, і вони не були змінені під час передачі.

До основних компонентів інфраструктури відкритих ключів належать:

– Центр сертифікації (ЦС): ЦС є довіреною організацією, яка видає, зберігає та підписує цифровий сертифікат. Центр сертифікації підписує цифровий сертифікат власним закритим ключем, а потім публікує відкритий ключ, до якого можна отримати доступ за запитом.

– Орган реєстрації (RA): RA перевіряє особу користувача або пристрою, що запитує цифровий сертифікат. Це може бути третя сторона, або ЦС також може діяти як RA.

– База даних сертифікатів: у цій базі даних зберігається цифровий сертифікат і його метадані, які включають тривалість дії сертифіката.

– Центральний каталог: це безпечне місце, де індексуються та зберігаються криптографічні ключі.

– Система керування сертифікатами: це система для керування доставкою сертифікатів, а також доступом до них.

– Політика щодо сертифікатів: ця політика описує процедури PKI. Його можуть використовувати сторонні особи для визначення надійності PKI.

Розуміння того, як працює PKI

Інфраструктура відкритих ключів використовує асиметричні методи шифрування, щоб гарантувати, що повідомлення залишаються приватними, а також для автентифікації пристрою або користувача, який надсилає передачу.

Асиметричне шифрування передбачає використання відкритого та закритого ключів. Криптографічний ключ – це довгий рядок бітів, який використовується для шифрування даних.

Відкритий ключ доступний кожному, хто його запитує, і видається довіреним центром сертифікації. Цей відкритий ключ перевіряє та автентифікує відправника зашифрованого повідомлення.

Другим компонентом пари криптографічних ключів, що використовується в інфраструктурі відкритих ключів, є приватний або секретний ключ. Цей ключ зберігається одержувачем зашифрованого повідомлення та використовується для розшифровки передачі.

Складні алгоритми використовуються для шифрування та дешифрування пар відкритих/приватних ключів. Відкритий ключ засвідчує автентичність відправника цифрового повідомлення, тоді як закритий ключ гарантує, що лише одержувач може відкрити та прочитати його.

Сертифікати PKI

Основою інфраструктури відкритих ключів є довіра. Організації-одержувачу важливо безсумнівно знати, що відправником цифрового сертифіката є саме той, за кого вони себе видають.

Довірені сторонні ЦС можуть поручитися за відправника та допомогти довести, що він справді є тим, за кого себе видає. Цифрові сертифікати використовуються для перевірки цифрової ідентифікації.

Цифрові сертифікати також називаються сертифікатами PKI або сертифікатами X.509 . Сертифікат PKI пропонує підтвердження особи суб’єкту, який надіслав запит, який перевіряється третьою стороною та працює як цифровий паспорт або водійське посвідчення.

Сертифікат PKI міститиме наступне:

- Помітне ім'я (DN) власника
- Відкритий ключ власника
- Дата видачі
- Термін придатності
- DN видавця ЦС
- Видача цифрового підпису ЦС

Чому використовується PKI?

Одним із найпоширеніших застосувань PKI є TLS/SSL (рівень безпеки транспортного рівня/рівень захищених сокетів), який захищає зашифрований зв’язок HTTP (протокол передачі гіпертексту).

Власники веб-сайтів отримають цифровий сертифікат від довіреного ЦС. Щоб отримати CA, власник веб-сайту повинен буде довести, що він справді є справжнім власником. Після перевірки власник веб-сайту може придбати сертифікат SSL для встановлення на веб-сервері. Це повідомляє браузеру, що це законний веб-сайт, до якого він намагається отримати доступ.

Протокол TLS/SSL покладається на ланцюжок довіри, де користувач має довіряти органу, що надає кореневий сертифікат. Альтернативною схемою є мережа довіри, яка використовує самопідписані сертифікати, перевірені третьою стороною. Мережа довіри часто використовується в невеликих спільнотах користувачів, наприклад, у самодостатній мережі організації.

Додаткові способи використання PKI включають наступне:

- Шифрування електронної пошти та аутентифікація відправника
- Підписання документів та програмного забезпечення
- Використання серверів баз даних для захисту внутрішніх комунікацій

– Захист веб-комунікацій, наприклад електронної комерції
– Аутентифікація та шифрування документів
– Захист локальних мереж і автентифікація смарт-карт
– Шифрування та дешифрування файлів
– Обмежений доступ до VPN та корпоративних інтрамереж
– Безпечний зв'язок між взаємно довіреними пристроями, такими як пристрої Інтернету речей (Інтернет речей).

Типи відкритих PKI

Інфраструктура відкритого ключа з відкритим кодом є загальнодоступною. Приклади PKI з відкритим кодом:

– EJBCA Enterprise: розроблено на Java як повнофункціональна реалізація CA корпоративного рівня, вона може налаштувати CA як службу або для внутрішнього використання.
– OpenSSL: повнофункціональний інструментарій комерційного рівня, він включений до всіх основних дистрибутивів Linux і розроблений на C. Він може використовувати PKI-додатки та використовуватися для створення простого ЦС.
– CFSSL: це набір інструментів PKI/SSL від Cloudflare для підписання, перевірки та об'єднання сертифікатів TLS і створення спеціальних інструментів TLS PKI
– XiPKI: високопродуктивний і масштабований відповідач CA та OCSP, реалізований на Java з підтримкою SHA-3.
– Система сертифікатів Dogtag: це повнофункціональний ЦС корпоративного класу, який підтримує всі аспекти керування життєвим циклом сертифікатів.

EJBCA® Enterprise

У зв'язаному суспільстві, оскільки потреба в надійних даних зростає, стає все більш очевидним, що безпека та PKI мають вирішальне значення для всіх видів бізнесу та організацій. Багатоцільове програмне забезпечення з відкритим кодом EJBCA Enterprise підтримує багато можливостей інтеграції та автоматизації та видає сертифікати людям, серверам і пристроям Інтернету речей.

EJBCA підтримує широкий спектр варіантів використання, сценаріїв і інтеграцій інфраструктури відкритих ключів (PKI) в інші екосистеми додатків і підтверджено у великих розгортаннях по всьому світу.

Побудований на основі відкритих стандартів і платформи з відкритим кодом, сертифікованої Common Criteria, EJBCA забезпечує прозорість і зобов'язання, необхідні для довгострокового рішення безпеки.

Розгорніть EJBCA відповідно до ваших потреб – як готове програмне чи апаратне забезпечення, або як хмару чи SaaS PKI.

Платформа PKI EJBCA Enterprise пропонує видачу сертифікатів і керування ними, щоб надати вам надійні ідентифікатори та безпечний зв'язок для будь-якого сценарію використання. EJBCA Enterprise є багатокористувачем і підтримує кілька центрів сертифікації (CA) і рівні центрів сертифікації в одному екземплярі програмного забезпечення.

Економічна безпека

Програмне забезпечення EJBCA Enterprise, здатне захистити практично будь-який варіант використання та сферу технології, відповідає всім вашим потребам щодо інфраструктури відкритих ключів (PKI) і надає різні варіанти, які дозволять вам знайти найбільш економічно ефективне рішення. PrimeKey пропонує EJBCA як готове програмне чи апаратне забезпечення, або як хмару чи SaaS PKI.

Масштабований

Гнучкість і надійність EJBCA Enterprise забезпечує можливість обслуговувати як маломасштабні, так і великомасштабні корпоративні впровадження з мільйонами користувачів або пристроїв у середовищах високої доступності, завдяки підтримці різних варіантів розгортання, централізованих операцій і високого рівня автоматизації.

Забезпечує відповідність

EJBCA Enterprise дотримується найкращих практик із детальними, підписаними журналами аудиту та транзакцій, авторизацією на основі ролей і розширеною підтримкою апаратних модулів безпеки. Він сертифікований Common Criteria і вже розгорнутий у численних ETSI/eIDAS- і WebTrust-аудитованих клієнтів і клієнтів ePassport.

Добре інтегрується

Завдяки перевіреній інтеграції в екосистеми додатків, включаючи пристрої IoT та інструменти DevOps, завдяки підтримці багатьох протоколів і форматів, EJBCA Enterprise є на вашому шляху цифровізації.

Параметри розгортання EJBCA

Щоб врахувати унікальні бізнес-завдання вашої організації, включаючи безпеку, бюджет і доступність внутрішніх ресурсів, PrimeKey пропонує комбінацію варіантів розгортання, які відповідають вашим потребам сьогодні та дозволяють вам гнучко розвиватися з часом.

Програмний пристрій

Розгорніть PKI у власному центрі обробки даних, використовуючи власні ресурси віртуалізації. Виберіть HSM і модель приладу, яка найкраще відповідає вашим потребам.

Апаратний пристрій

Виберіть EJBCA Hardware Appliance, якщо ви шукаєте локальне рішення PKI-in-a-box. EJBCA Hardware Appliance – це надійний, високопродуктивний сервер, який постачається з повним апаратним і програмним забезпеченням і HSM.

Хмара EJBCA

Насолоджуйтеся швидким розгортанням за допомогою PKI у загальнодоступній хмарі без необхідності купувати та підтримувати апаратне забезпечення або будь-які попередні витрати на ліцензію на програмне забезпечення. Наші хмарні рішення PKI доступні в AWS і Azure.

Програмне забезпечення EJBCA як послуга

Якщо ви шукаєте повністю розміщене та кероване рішення PKI, то EJBCA SaaS – це ваш вибір. Це допомагає обмежити ризики розгортання та збільшити швидкість виходу на ринок.

Компоненти продукту EJBCA

EJBCA постачається або може використовуватися разом із такими розширеними інструментами для реєстрації та перевірки сертифікатів:

Реєстраційний орган EJBCA

Центр реєстрації EJBCA (RA) є зовнішньою організацією для центру сертифікації (CA) для реєстрації будь-якого типу сертифіката, що забезпечує додатковий рівень безпеки навколо центру сертифікації.

Орган перевірки EJBCA

EJBCA Validation Authority (VA) дозволяє онлайн-перевірку сертифіката за допомогою OCSP або CRL.

Автоматична реєстрація сертифіката

Завдяки функції автоматичної реєстрації сертифіката в EJBCA Enterprise ви можете позбутися будь-якої необхідності використовувати центри сертифікації Microsoft і повністю використовувати повну гнучкість EJBCA Enterprise і Active Directory.

Менеджер повноважень ідентифікації

Обладнання промислового класу PKI Registration Authority (RA), яке можна використовувати разом з EJBCA для видачі сертифікатів продукту безпосередньо на виробництві.

Видання EJBCA eIDAS

З випуском EJBCA eIDAS як апаратним або програмним пристроєм ви отримуєте повний набір функцій для роботи повномасштабної інфраструктури відкритих ключів (PKI), сумісної з eIDAS.

Набір інструментів PKI/TLS CloudFlare

CFSSL – це швейцарський армійський ніж PKI/TLS від CloudFlare. Це як інструмент командного рядка, так і сервер HTTP API для підписання, перевірки та об'єднання сертифікатів TLS. Для створення потрібен Go 1.16+.

Зауважте, що певні дистрибутиви Linux видаляють певні алгоритми (зокрема дистрибутиви на основі RHEL), тому golang з офіційних репозиторіїв не працюватиме. Користувачі цих дистрибутивів повинні інсталювати go вручну, щоб інсталювати CFSSL.

CFSSL складається з:

– набір пакетів, корисних для створення спеціальних інструментів TLS PKI;

– програма cfssl, яка є канонічною утилітою командного рядка, що використовує пакети CFSSL;

– програму multirootca, яка є сервером центру сертифікації, який може використовувати кілька ключів підпису;

– програма mkbundlevикористовується для створення пулів сертифікатів;

– програма cfssljson, яка отримує вихідні дані JSON з cfsslпрограм multirootcai записує сертифікати, ключі, CSR і пакети на диск.

XiPKI

XiPKI (e X tensible s Imple Public Key I nfrastructure) – це високомасштабована та високопродуктивна PKI з відкритим кодом (відповідач CA та OCSP) .

Ліцензія

– Ліцензія на програмне забезпечення Apache, версія 2.0.

Система сертифікації Dogtag

истема сертифікації Dogtag – це центр сертифікації корпоративного класу з відкритим вихідним кодом (CA). Це повнофункціональна система, яка була посилена розгортанням у реальному світі. Він підтримує всі аспекти керування життєвим циклом сертифіката, включаючи архівування ключів, OCSP і керування смарт-картами, а також багато іншого. Систему сертифікатів Dogtag можна завантажити безкоштовно та налаштувати менш ніж за годину.

На цьому сайті є все, що вам потрібно, щоб приєднатися до спільноти Dogtag. Незалежно від того, чи вам потрібна допомога та порада щодо розгортання та використання компонентів Dogtag, чи ви хочете взяти на себе більш активну роль і допомогти сформувати майбутнє PKI, є посилання на документацію, списки розсилки та канали обговорень, які ви можете прочитати або приєднатися:

– Онлайн-документація.
– Посилання на додаткову документацію.
– Списки розсилки.
– Сайти онлайн-чату через канали IRC.

Ключові особливості

Dogtag – це набір технологій, які дозволяють підприємствам розгортати PKI у великих масштабах. Він має такі функції, як:

– Видача, відкликання та відновлення сертифіката.
– Створення та публікація списку відкликаних сертифікатів (CRL).
– Профілі сертифікатів.
– Простий протокол реєстрації сертифікатів (SCEP).
– Місцевий орган реєстрації (LRA) для автентифікації та політики організації.
– Архівація та відновлення ключа шифрування.
– Управління життєвим циклом смарт-карт:

- Профілі токенів.
- Реєстрація маркерів, утримання, відновлення ключа та форматування.
- Особиста реєстрація за допомогою інтерфейсу робочої станції офіцера безпеки.

– Велика документація.

EFS

Перед використанням можливостей шифрування EFS варто визначитися чи буде використовуватися Агент відновлення даних. Агентом відновлення називається користувач, уповноважений розшифровувати дані, зашифруванні іншим користувачем, якщо користувач втратив закриті ключі сертифіката шифрування або обліковий запис користувача віддалений і потрібно відновити зашифруванні дані. Як правило, Агентом відновлення вказується Адміністратор, але може бути призначений і інший користувач. Може бути створене трохи Агентів відновлення. Щоб призначити користувача Агентом відновлення, необхідно спочатку створити сертифікати Агента відновлення.

Шифрувати можна як окремі файли, так і цілі папки, при цьому якщо шифрується папка вже утримуюча файли, тобто можливість вибору, шифрувати тільки папку або папку й вкладені файли. Шифрування папки не означає що інші користувачі не зможуть переглядати вміст папки – вони лише не зможуть відкривати зашифруванні файли. Всі нові файли, збережені в зашифруванній папці або скопійовані в неї будуть автоматично зашифруванні. Шифрувати папки більш зручно, і крім того безпечно, оскільки EFS має схему відновлення після аварійного збою (наприклад якщо під час операції шифрування відбулася критична помилка) яка передбачає створення незашифрованної архівної копії вихідного файлу – при успішному завершенні операції шифрування архівна копія віддаляється, але може бути відновлена спеціальними програмами відновлення віддалених даних, що створює потенційну погрозу інформаційної безпеки. А при збереженні файлу в зашифруванній папці шифрування відбувається без створення такої резервної копії. Якщо все-таки шифрувалися одиночні файли, тобто можливість перезаписати кластери, що залишилися після зміни або видалення файлів на томах NTFS випадковими значеннями – для цього може бути використана команда cipher /w:шлях запущена з командного рядка (докладніше про використання цієї команди дивитеся в довіднику по командному рядку) або програми сторонніх розроблювачів.

Із усього перерахованого вище можна зробити наступні висновки:

−Система EFS надає користувачам можливість зашифровувати каталоги NTFS, використовуючи стійку, засновану на загальних ключах криптографічну схему, при цьому всі файли в закритих каталогах будуть зашифруванні. Шифрування окремих файлів підтримується, але не рекомендується через непередбачене поводження додатків.

−Система EFS також підтримує шифрування віддалених файлів, доступ до яких здійснюється як до спільно використовуваних ресурсів. Якщо мають місце користувальницькі профілі для підключення, використовуються ключі й сертифікати віддалених профілів. В інших випадках генеруються локальні профілі й використовуються локальні ключі.

−Система EFS надає можливість встановити політику відновлення даних таким чином, що зашифруванні дані можуть бути відновлені за допомогою EFS, якщо це буде потрібно.

−Політика відновлення даних убудована в загальну політику безпеки Windows. Контроль за дотриманням політики відновлення може бути делегований уповноваженим на це особам. Для кожного підрозділу організації може бути зконфігурована своя політика відновлення даних.

−Відновлення даних в EFS – закрита операція. У процесі відновлення розшифровуються дані, але не ключ користувача, за допомогою якого ці дані були зашифруванні.

−Робота із зашифруванними файлами в EFS не жадає від користувача яких-небудь спеціальних дій по шифруванню й дешифруванню даних. Дешифрування й шифрування відбуваються непомітно для користувача в процесі зчитування й запису даних на диск.

−Система EFS підтримує резервне копіювання й відновлення зашифруванних файлів без їхньої розшифровки. Програма NtBackup підтримує резервне копіювання зашифруванних файлів.

–Система EFS убудована в операційну систему таким чином, що витік інформації через файли підкачування неможливий, при цьому гарантується, що всі створювані копії будуть зашифруванні

–Передбачено численні запобіжні заходи для забезпечення безпеки відновлення даних, а також захист від витоку й втрати даних у випадку фатальних збоїв системи.

Опис PKI

Розглянемо технологію PKI. Задачею PKI є визначення політики випуску цифрових сертифікатів, видача їх і анулювання, зберігання інформації, необхідної для наступної перевірки правильності сертифікатів. PKI використовується в EFS. Діяльність інфраструктури керування відкритими ключами здійснюється на основі регламенту системи. Інфраструктура відкритих ключів ґрунтується на використанні принципів криптографічної системи з відкритим ключем. Інфраструктура керування відкритими ключами складається із центра сертифікації, кінцевих користувачів, і опціональних компонентів: центра реєстрації й мережного довідника.

Зрозуміло, що PKI оперує в роботі сертифікатами. Але у зв'язку з тим, що в PKI використовуються сертифікати, виникає множина нюансів, без яких будь-яка PKI не буде працювати коректно.

По суті, сертифікат – це ключова пара, що складається із двох ключів – зазвичай перший ключ називається закритим ключем (private key), а другий ключ – відкритим ключем (public key). Ці ключі створюються тільки в парі й мають однаковий електронний відбиток. По електронному відбитку можна визначити, чи відповідає даний відкритий ключ своєму закритому ключу.

Створює ці ключі якийсь центр, що зазвичай називається центром видачі сертифікатів або центром, що засвідчує, по запиті користувача. Користувач робить запит на сертифікат, після чого, після деяких процедур ідентифікації користувача, центр видає йому сертифікат зі своїм підписом (цей підпис свідчить про те, що даний сертифікат виданий саме цим центром видачі сертифікатів і ніким іншим), після чого користувач має в наявності свій закритий ключ і відповідний йому відкритий ключ.

Закритий ключ використовується для підпису даних, відкритий ключ у свою чергу використовується для шифрування даних. Відкритий ключ відомий усім, а закритий ключ зберігається в таємниці. Власник закритого ключа завжди зберігає його в захищеному місці й ні за яких умов не повинен допустити того, щоб цей ключ став відомим зловмисникам або іншим користувачам.

Якщо ж закритий ключ усе таки стане відомий зловмисникам, необхідно терміново сповістити про це колег, щоб запобігти витоку важливої інформації. Тільки власник закритого ключа може підписати дані, а також розшифрувати дані, які були зашифровані відкритим ключем, що відповідає закритому ключу власника.

Тому що закритий ключ використовується для підпису даних – його можна назвати своєрідним ідентифікатором передплатника. Підпис на даних або листі гарантує цілісність отриманої інформації.

Термінологія PKI

Із усього вище сказаного можна виділити деякі пункти, а також додати нові, для того щоб визначити основні терміни, використовувані в PKI.

Отже, в PKI використовуються терміни:

–Сертифікат – це ключова пара (складається з відкритого й закритого ключів), до якої приписаний її унікальний номер, ім'я власника сертифіката, а також ім'я центра видачі, що видав цей сертифікат.

–Закритий ключ – ключ, що зберігається в таємниці, створений з використанням PKI алгоритмів, що має свій унікальний електронний помилок і, що використовується для одержання зашифрованих даних і підпису даних.

–Відкритий ключ – ключ, створений у парі із закритим ключем, що має такий же електронний відбиток, як і закритий ключ, якому він відповідає, використовується для шифрування даних і перевірки підпису

–Підписані дані – дані, підписані за допомогою закритого ключа користувача.

–Зашифровані дані – дані, зашифровані за допомогою відкритого ключа користувача.

Терміни, які необхідні для загального розуміння:

–Мережа довіри – або ланцюжок сертифікацій, необхідна й потрібна для тих випадків, коли є множина різних центрів, що засвідчують, і виникають ситуації, коли один УЦ (удостовірюючий центр), не довіряє якомусь іншому, але при цьому може покластися на те, що загальний дружній УЦ довіряє обом

–Особисті сертифікати – сертифікати які зберігаються в користувача в особистому сховищі сертифікатів.

–Кореневі центри сертифікації – центри сертифікації, яким довіряють споконвічно всі, наприклад після установки ОС. У ці центри сертифікації можна в будь-який час додавати нові центри, яким Ви хочете довіряти

–Довірені центри сертифікації – список центрів сертифікації, яким довіряєте особисто. Щоб зробити любий УЦ довіреним, досить одержати від нього сертифікат і внести його в довірені центри Також важливо знати про поняття центра сертифікації й про кінцевих користувачів.

–Центр сертифікації (удостоверяючий центр) – є основною структурою, що формує цифрові сертифікати підлеглих центрів сертифікації й кінцевих користувачів. Центр сертифікації сам формує власний секретний ключ і сертифікат, що містить відкритий ключ даного центра. Засвідчує автентичність відкритого ключа користувача своїм електронно-цифровим підписом. Формує список відкликаних сертифікатів. Веде бази всіх виготовлених сертифікатів і списків відкликаних сертифікатів. Відкритий ключ, підписаний центром сертифікації, називається сертифікатом відкритого ключа.

–Кінцеві користувачі – є користувачі, додатки або системи, що є власниками сертифіката й використовують інфраструктуру керування відкритими ключами

–Центр Реєстрації – опціональна компонента інфраструктури, призначена для реєстрації кінцевих користувачів і забезпечення їхньої взаємодії із центром сертифікації.

–Мережний довідник – опціональна компонента інфраструктури, що містить сертифікати й списки відкликаних сертифікатів і, що служить для мети поширення цих об'єктів серед користувачів.

Впровадження інфраструктури керування відкритими ключами з урахуванням зниження витрат і строків впровадження здійснюється протягом семи етапів.

– Етап 1. Аналіз вимог до системи.
– Етап 2. Визначення архітектури.
– Етап 3. Визначення регламенту.
– Етап 4. Огляд системи безпеки. Аналіз і мінімізація ризиків.
– Етап 5. Інтеграція.
– Етап 6. Розгортання.
– Етап 7. Експлуатація.

Деякі основні моменти

Двома словами вже було сказано, для чого потрібні закритий і відкритий ключі, що таке сертифікат і центри, що засвідчують. Але тому що це основні компоненти PKI, розберемо докладніше наступні моменти:

– у чому полягає робота УЦ

– як відбувається видача сертифіката, обмін відкритими ключами і як зрозуміти, що відкритий ключ, що перебувати перед моїми очами, не фальшивий

– а також те, які бувають PKI.

УЦ і його робота

Основна робота центра, що засвідчує, полягає в ідентифікації користувачів і їхніх запитів на сертифікати, у видачі користувачам сертифікатів, у перевірках автентичності сертифікатів, у перевірці за сертифікатом, чи не видає користувач сертифіката себе за інший, в анулюванні або відкликанні сертифікатів, у веденні списку відкликаних сертифікатів.

Розробка структурної схеми

На рисунках 1 та 2 показані структурні схеми шифрування та дешифрування EFS.

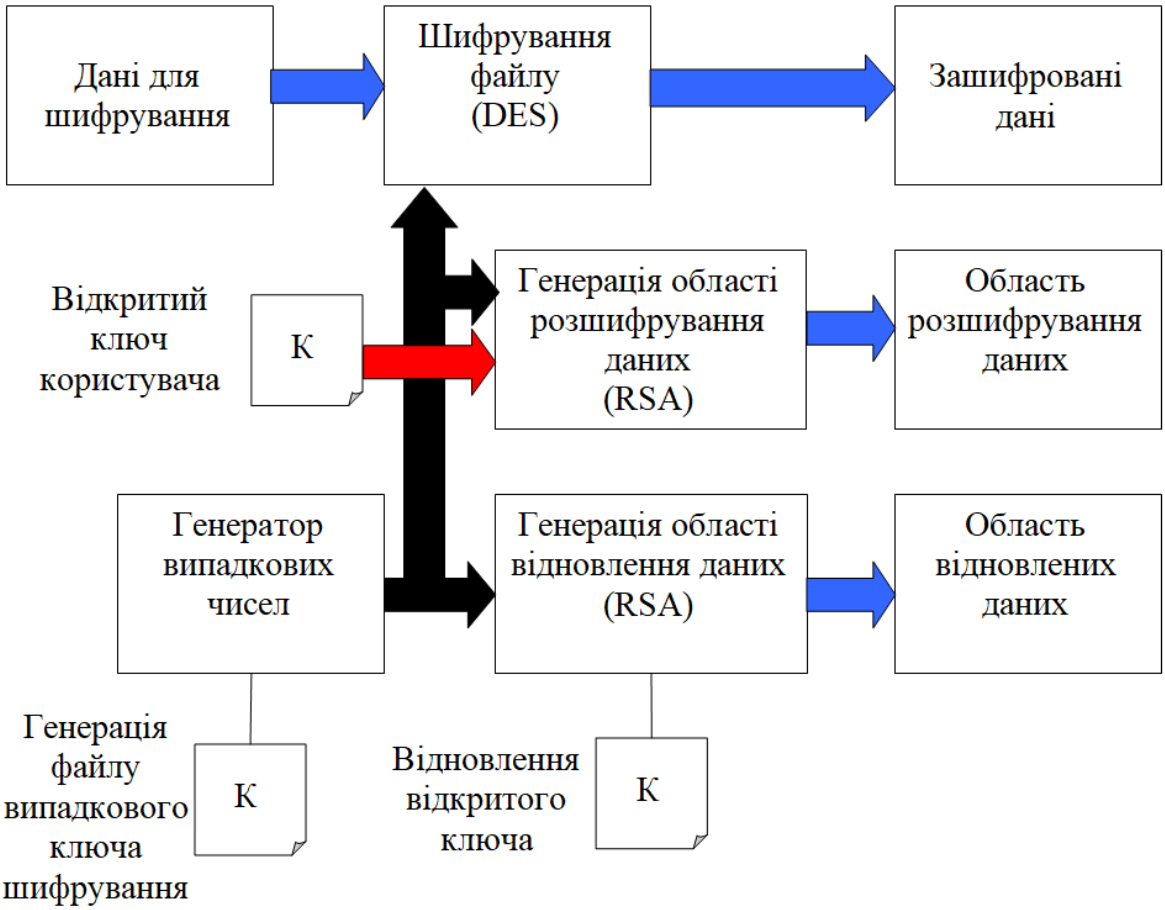

Рисунок 1 – Структурна схема шифрування EFS

Якщо коротко, то можливо сказати, що робота системи відбувається наступним чином. EFS працює, шифруючи кожний файл за допомогою алгоритму симетричного шифрування, що залежить від версії операційної системи й настроювань.

При цьому використовується випадково-згенерований ключ для кожного файлу, називаний **File Encryption Key** (FEK), вибір симетричного шифрування на даному етапі пояснюється його швидкістю й більшою надійністю стосовно асиметричного шифрування. У данному магістерському проекті у якості симетричного алгоритму шифрування вибраний DES, у зв'язку з тим, що він є достатньо стійким та швидким.

FEK (випадковий для кожного файлу ключ симетричного шифрування) захищається шляхом асиметричного шифрування, що використовує відкритий ключ користувача файл, який шифрує, і алгоритм RSA (теоретично можливе використання інших алгоритмів асиметричного шифрування).

RSA обраний тому, що він достаньо стійкий , для цих потреб, та виконується більш швидко, ніж інші алгоритми симметричного шифрування. Зашифрований у такий спосіб ключ FEK зберігається в альтернативному потоці $EFS файлової системи NTFS.

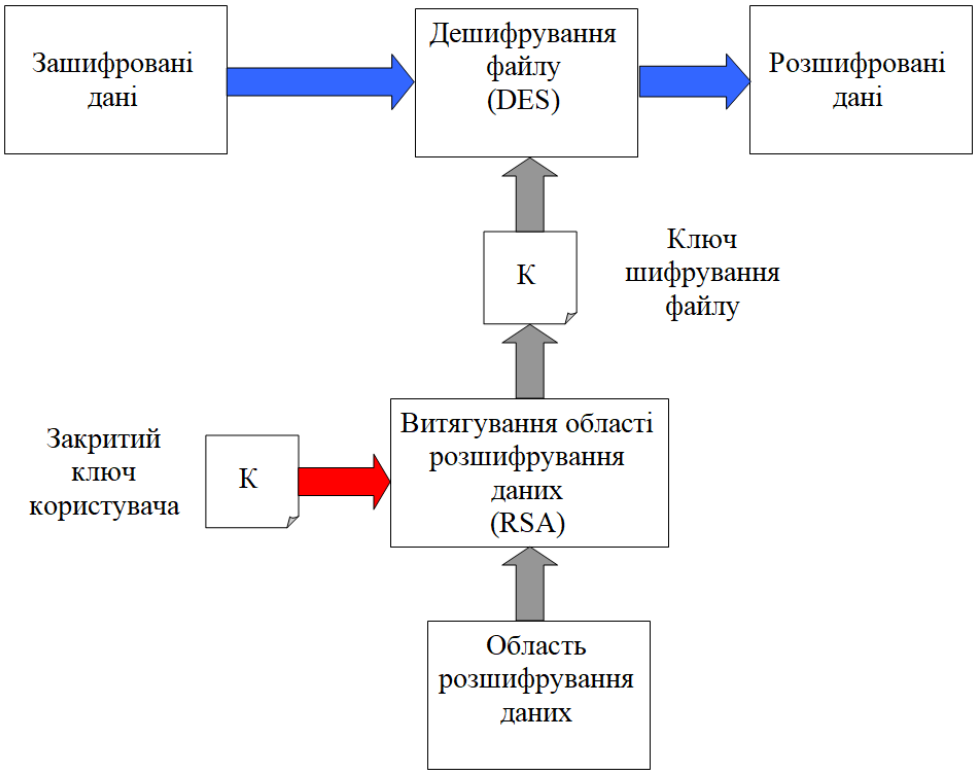

Рисунок 2 – Структурна схема дешифрування EFS

Для розшифрування даних, драйвер шифруванної файлової системи, прозоро для користувача, розшифровує FEK використовуючи закритий ключ користувача, а потім і необхідний файл за допомогою розшифруванного файлового ключа.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів прозорого шифрування даних з застосуванням засобів PKI. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем прозорого шифрування даних з застосуванням засобів PKI. Досліджена система прозорого шифрування даних з застосуванням засобів PKI. На основі отриманих результатів досліджень створена програмна реалізація системи прозорого шифрування даних з застосуванням засобів PKI. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання прозорого шифрування даних з застосуванням засобів PKI. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
2. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
3. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
4. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. – практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

5. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. – № 2 (46). – С. 146-149.
6. Смирнов С. А. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2016. – Вип. 3 (140). – С. 36-39.
7. Смирнов С. А. Метод безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы / В. Л. Бурячок, С. А. Смирнов // Системи управління, навігації та зв'язку. – Полтава, 2016. – Вип. 4(40). – С. 57-62.
8. Смирнов С. А. Способ контроля линий связи телекоммуникационной системы облачного антивируса / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2016. – № 2 (47). – С. 148-152.
9. Смирнов С. А. Дослідження та реалізація GERT-моделі технології розповсюдження комп'ютерних вірусів для захисту телекомунікаційних систем / В. Л. Бурячок, Мохамад Абу Таам Гани, С. А. Смирнов // Інформаційні технології та комп'ютерна інженерія: зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 грудня 2014 р. – Кіровоград: КНТУ, 2014. – С. 168.
10. Смирнов С. А. Исследование математических моделей технологии распространения компьютерных виру сов / А. А. Смирнов, Мохамад Абу Таам Гани, С. А. Смирнов // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: зб. наук. праць міжнар. наук.-практ. конф., м. Київ, 25-28 лютого 2015 р. – К.: Європейський університет, 2015. – С. 90-91.
11. Смирнов С. А. Метод управления доступом к «облачным» ресурсам для защиты телекоммуникационных систем / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Всеукраїнська науково-практична конференція «Інформаційна безпека держави, суспільства та особистості», м. Кіровоград, 16 квітня 2015 р.: зб. тез доп. – Кіровоград: КНТУ, 2015. – С. 50-52.
12. Смирнов С. А. Разработка метода управления доступом в интеллектуальных узлах коммутации / А. А. Смирнов, Мохамад Абу Таам Гани, С. А. Смирнов // Проблеми і перспективи розвитку ІТ-індустрії: зб. тез VII міжнар. наук.-практ. конф., м. Харків, 17-18 квітня 2015 р. – Х.: ХНЕУ, 2015. – С. 14.
13. Смирнов С.А. Реализация метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Абу Таам Гани, С.А. Смирнов // Збірник тез XVII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 17-18 квітня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 91-92.
14. Смирнов С. А. технология передачи сигнатур в облачные антивирусные системы для обеспечения защищенности телекоммуникационных сетей / А. А. Смирнов, С. А. Смирнов // Збірник тез V міжнародної науково-технічної конференції «ITSEC», Київ, 19-22 травня 2015 р. – К.: НАУ 2015. – С. 12-13.
15. Смирнов С. А. Реализация математической модели интеллектуального узла коммутации для обеспечения защищенности телекоммуникационной сети / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Інформаційна та економічна безпека (INFECO-2015): зб. тез II Міжнар. наук.-практ. Інтернет-конф., м. Харків, 21-22 травня 2015 р. – Х.: ХІБС УБС НБУ, 2015. – С. 20-24.
16. Смирнов С. А. Разработка математической модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Сборник тезисов XI международной конференции «Стратегия качества в промышленности и образовании», г. Варна, Болгария, 01-06 июня 2015 г. – Варна: ТУВ, 2015. – С. 488-491.
17. Смирнов С. А. Метод управления доступом к облачным телекоммуни-кационным ресурсам для обеспечения защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Комп'ютерні технології та інформаційна безпека: зб. тез доп. міжнар. наук.-практ. конф., м. Кіровоград, 2-3 липня 2015 р. – Кіровоград: КНТУ, 2015. – С. 4-5.
18. Смирнов С. А. Имитационная модель системы управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Збірник тез першої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації» (м. Затока, 7-9 вересня 2015 р.). – Одеса: ОНАЗ, 2015. – С. 90-94.
19. Смирнов С. А. Разработка комплекса gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційні технології та взаємодії» (IT & I): зб. тез II міжнар. наук.-практ. конф., м. Київ, 3-5 листопада 2015 р. – К.: КНУ ім. Тараса Шевченка, 2015. – С. 65-67.
20. Смирнов С. А. Разработка моделей телекоммуникационной системы формирования и обработки метаданных в облачных антивирусных системах / А.А. Смирнов, С.А. Смирнов, А. К. Дидык // Информационные и телекоммуникационные технологии: образование, наука, практика: сб. тезисов II междунар. научно-практ. конф., г. Алматы, Казахстан, 3-4 декабря 2015 г. – Алматы: КазНИТУ им. К.И. Сатпаева, 2015. – С. 309-313.