УДК 004.056:004.7

ПІДХІД ЩОДО ПЕРЕВІРКИ ЦИФРОВИХ СЕРТИФІКАТІВ З ВИКОРИСТАННЯМ BLOCKCHAIN

DOI 10.36994/2707-4110-2020-1-28-17

Ільєнко А. В., к.т.н., доц., Національний авіаційний університет, Київ, Україна.
Ilyenko.a.v@nau.edu.ua

Ільєнко С. С., к.т.н., доц., Національний авіаційний університет, Київ, Україна.
Ilyenko.s.s@nau.edu.ua

Куліш Т. М., Національний авіаційний університет, Київ, Україна.
teti98kulish@gmail.com

Анотація. Стаття присвячена реалізації власного підходу щодо перевірки цифрових сертифікатів з використанням Blockchain напрямку для захисту операційної системи Windows. У роботі розглянуті питання передачі цифрових сертифікатів, проблеми SSL/TLS -протоколів. Проаналізовані та запропоновані методи підвищення рівня захисту операційної системи Windows, що можуть бути використані при верифікації сертифікатів.

Запропоновано новий напрям Blockchain для реалізації перевірки, за рахунок введення різних перевірок, що дозволяє проводити якісну оцінку достовірності цифрових сертифікатів. На сьогодні Blockchain технологія прекрасно підходить для перевірок, обмінів і захисту цифрових сертифікатів. Зберігається список емітента і одержувача, підпис документа у відкритій базі даних, що такий же і у комп'ютерах у відкритій мережі. У порівнянні із звичайними цифровими сертифікатами, сертифікати сформовані з використанням blockchain технології мають такі переваги: немає необхідності у посередниках; перевірку сертифіката реалізовуватиме програма, що має відкритий код; можна точно впевнитися ким і кому був виданий сертифікат; зберігається конфіденційність документу, що підписується. Як бачимо, дана технологія здатна створити потужну, захищену, довірену і надійну структуру, що не потребує для роботи ні посередників, ні чергових перевірок. Завдяки різноманітності методів перевірок, ресурсів, що цей напрямок надає, можна досягнути максимум підтвердження дійсності як одиноких сертифікатів так і цілого їх ланцюжка.

Практична цінність дослідження полягає в наступному: авторами запропоновано власний підхід, що дозволяє перевіряти одинокі сертифікати і ланцюги сертифікатів завдяки напрямку Blockchain, що дозволяє встановити надійде з'єднання і надійну передачу даних. Завдяки тому, що запропонований підхід дозволяє здійснювати декілька перевірок сертифікатів, він у подальшому може бути інтегрованим в операційну систему Windows і може використовуватись із ціллю захисту персонального комп'ютера або ж використовуватись у корпоративних структурах.

Ключові слова: *Blockchain, Цифрові сертифікати, Верифікація, Windows, SSL/TLS.*

APPROACH FOR VERIFICATION OF DIGITAL CERTIFICATES USING BLOCKCHAIN

Ilyenko A.V., Ph.D., Ass. Prof., National Aviation University, Kyiv, Ukraine.
ilyenko.a.v@nau.edu.ua

Ilyenko S.S., Ph.D., Ass. Prof., National Aviation University, Kyiv, Ukraine.
ilyenko.s.s@nau.edu.ua

Kulish T.M., National Aviation University, Kyiv, Ukraine. teti98kulish@gmail.com

Abstract. *The article is devoted to the implementation of its own approach to the verification of digital certificates using Blockchain direction to protect the Windows operating system. The methods of increasing the level of protection of the Windows operating system that can be used for certificate verification are analyzed and proposed.*

A new direction of Blockchain is proposed for the implementation of verification, due to the introduction of various verifications, which allows for a qualitative assessment of the authenticity of digital certificates. Today, Blockchain technology is perfect for checking, exchanging and protecting digital certificates. The list of the issuer and the recipient, the signature of the document in an open database, which is the same as in the computers on the open network, is stored. Compared to conventional digital certificates, certificates generated using blockchain technology has the following advantages: no need for intermediaries; certificate verification will be performed by an open source program; you can be sure exactly who and to whom the certificate was issued; the confidentiality of the document being signed is preserved. As you can see, this technology is able to create a powerful, secure, trusted and reliable structure that does not require any intermediaries or regular inspections. Due to the variety of inspection methods, the resources that this area provides, you can achieve maximum validation of both individual certificates and entire chain. Blockchain network is a guarantee of reliability and validity of data, but if someone still wants to confirm the validity of the certificate, you must obtain the public key of the person who signed it. Due to the lack of constant confirmation of certificates, this approach simplifies the administration of the network.

The practical value of the study is as follows: the authors have proposed their own approach, which allows you to check single certificates and certificate chains thanks to the Blockchain direction, which allows you to establish a secure connection and reliable data transmission. Because the proposed approach allows multiple certificate checks, it can be further integrated into the Windows operating system and can be used to protect a personal computer or used in corporate structures.

Keywords: *Blockchain, Digital Certificates, Verification, Windows, SSL/TLS.*

Вступ

Щоденний обмін інформацією між користувачами і веб-сторінками вимагає підвищених вимог щодо захищеної передачі призначених для користувача даних.

На сьогодні HTTPS став стандартом одним із основних стандартів при побудові та організації секретного зв'язку. Також не менш популярними є

HSTS (HTTP Strict Transport Security) - механізм, який активує форсоване захищене з'єднання через протокол HTTPS, а також Certificate pinning (зберігання списку дозволених для домена сертифікатів у вихідних текстах браузера) і HTTP Public Key Pinning. Ці методи дозволяють уникнути непомітну підміну сертифіката за рахунок порівняння з еталонними в захищеному сховищі браузера.

Однак, проблема використання цифрових сертифікатів для підтвердження автентичності інформації все одно залишається актуальною, так як далеко не всі сайти використовують цифрові сертифікати і якщо і використовують, то їх перевірка не завжди є коректною, або ж неповною. Як приклад, CVE-2019-13050 - сертифікований напад спаму на ключові сервери SKS та GnuPG, що відбулась у 2019 році.

Оскільки основною і найбільш частою проблемою цифрових сертифікатів є саме не коректний спосіб їх верифікації, то метою роботи стала є розробка нового підходу щодо верифікації сертифікатів з використанням підходу blockchain, що являє собою комплекс декількох перевірок сертифікатів. Подальші результати роботи можуть здобути широке застосування як у звичайних користувачів так і на корпоративному рівні з ціллю захисту операційної системи Windows від вразливостей, пов'язаних із передачею цифрових сертифікатів.

Теоретичні основи дослідження

В даному розділі розглянемо основні недоліки та вразливості використання операційної системи Windows пов'язаної із передачею цифрових сертифікатів. На сьогоднішній день після тривалого використання SSL, були виявлені значні ризики, особливо для операційної системи Windows. У 2015 році SSL версія v3 протоколу була знята через виявлення критичного недоліку, який дозволив зловмисникам вилучати секретну інформацію з зашифрованих повідомлень. Як його альтернативою можна використовувати спадкоємця – TLS [1-3].

Розглянемо далі основні вразливості, які пов'язані із передачею цифрових сертифікатів та можливі шляхи вирішення проблем. До основних вразливостей відносяться використання ненадійного сертифікату, закінчення терміну дії сертифікату, використання ненадійного криптографічного алгоритму, неправильно підписані сертифікати SSL

Ненадійний сертифікат. Сертифікати з простроченим або ненадійним сертифікатом є проблемою, оскільки ними можуть скористатися зловмисники. Наприклад, якщо користувачі звикли бачити сертифікат з простроченим терміном дії і зазвичай їх ігнорують, існує ймовірність, що під час перегляду вашого сайту ваші дані будуть викрадені. Рішення: усі сертифікати повинні бути підписані довіреним органом сертифікації. Це може бути авторитетний сертифікаційний орган третьої сторони, або використання інфраструктури відкритих ключів, що існує в організації. Останнє вимагає встановлення кореневого сертифіката на всіх підключених клієнтах, що можна зробити за

допомогою зміни групової політики Windows: відкрити відповідний об'єкт групової політики (GPO); у дереві консолі натисніть Довірені органи кореневої сертифікації: Ім'я об'єкта політики / Конфігурація комп'ютера / Налаштування Windows / Налаштування безпеки / Політика відкритого ключа / Довірені органи кореневої сертифікації; у меню Дія вкажіть на Усі завдання, а потім натисніть Імпортувати, щоб додати кореневий сертифікат

Термін дії просрочених сертифікатів. Як і ненадійні сертифікати, користувачеві, який підключається до служби SSL із сертифікатом просроченого терміну, подається повідомлення про помилку, в якому повідомляється про те, що термін дії сертифікату минув. Зазвичай це означає, що Орган сертифікації більше не звітує про цілісність сертифіката. Рішення: вести запис про терміни дії сертифіката та забезпечити, щоб процес поновлення розпочався за тридцять днів до закінчення терміну дії сертифіката.

Використання ненадійного криптографічного алгоритму. Алгоритм хешування використовується для надання сертифікату цифрового підпису, щоб переконатися, що його вміст не було змінено. Алгоритми хешування бувають різних типів, деякі з яких криптографічно зламані і піддаються хеш-зіткненням; напад, який сприяв би формуванню шахрайських сертифікатів. Якщо такі атаки вдаються, зловмисна група чи особа можуть маскуватися під надійну послугу і бути прихованими до всіх даних, переданих між користувачем та цією службою. Рішення: рекомендується, щоб усі сертифікати, підписані за допомогою слабких алгоритмів хешування, таких як SHA-1 і MD5, були переоформлені і використовувались сімейство алгоритмів хешування SHA-2 (SHA-224, SHA-256, SHA-384 і SHA- 512) [4-8].

Сертифікати SSL, підписані за допомогою ключів RSA менше 2048 біт, вважаються слабкими, оскільки, враховуючи прогрес у обчислювальній потужності, вони стають все більш вразливими до злому в розумні часові рамки. Успішна атака подібного характеру забезпечить зловмиснику чіткий доступ до тексту до зашифрованих даних, оскільки він перебуває між транзитом між клієнтом та сервером. Рішення: пошкоджені сертифікати в ланцюзі з ключем RSA довжиною менше 2048 біт замінюються більш довгим ключем, а будь-які сертифікати, підписані старим сертифікатом, видаються повторно.

Неправильно підписані сертифікати SSL. Неправильно підписані сертифікати X.509 містять одне або більше порушень обмежень, накладених на нього RFC 5280. Це означає, що або кореневий, або проміжний Сертифікаційний орган підписав сертифікат неправильно. Сертифікати, які не дотримуються обмежень у своїх розширеннях, можуть бути відхилені певним програмним забезпеченням. Наявність таких сертифікатів свідчить або про напад у процесі підписання, або про зловмисні наміри. Рішення: змінення розширення сертифікатів-порушників, і їх перепідписання або перевидання [9-10].

Підсумовуючи викладене у розділі, можна зробити висновки, що безпека комунікацій цілком залежить від адекватності перевірки криптографічного сертифікату, наданого сервером під час активного з'єднання. У тому числі від адекватності реалізації набору шифрів (cipher suite), якими клієнт і сервер користуються при обміні даними.

На основі проведеного аналізу сучасних засобів передачі цифрових сертифікатів, було зроблено висновок що у теорії, захищене SSL/TLS-протоколом з'єднання повинно забезпечувати конфіденційність, достовірність і цілісність комунікацій клієнтського і серверного програмного забезпечення, навіть якщо в мережу проник активний зловмисник, однак у багатьох додатках і бібліотеках, для яких безпека комунікацій дуже критична, процедура перевірки SSL/TLS-сертифіката, і навіть EV-SSL, сертифіката з розширеною перевіркою, повністю провальна, причому це справедливо для такої операційної системи як Windows.

Саме тому було поставлено завдання реалізувати власну перевірку цифрових сертифікатів, що може бути використана на операційній системі Windows, врахувавши уразливості, які наявні у сучасних методах верифікації цифрових сертифікатів.

Реалізація підходу щодо перевірки цифрових сертифікатів з використанням blockchain напрямку

Для досягнення поставленої цілі був запропонований напрям blockchain для передачі цифрових сертифікатів, був детально представлений принцип роботи запропонованого рішення.

Blockchain – це особлива технологія, на якій засновані платформи для проведення операцій між рівноправними учасниками, які діють без посередників, і в якій застосовується децентралізоване зберігання інформації для відображення всіх даних про операції. Вперше технологія «блокчейн» була використана в фінансовому секторі, де вона послужила основою для створення криптовалюти «біткойн». Останнім часом з'являється все більше додатків, розширюють ключову функцію цієї технології - децентралізоване зберігання даних про транзакції за рахунок інтеграції механізмів, що дозволяють децентралізовано проводити реальні угоди. Дані механізми, які отримали назва «розумних контрактів», працюють на основі правил, встановлених в індивідуальному порядку (наприклад, конкретні вимоги щодо кількості, якості, ціни) і дозволяють в автоматичному режимі підбирати потенційних споживачів для постачальників і навпаки на основі розподілених реєстрів. Blockchain – це технологія, яка дозволяє проводити транзакції між рівноправними учасниками єдиної мережі (P2P-мережі). Транзакції даного виду припускають, що кожен учасник мережі може здійснювати транзакцію безпосередньо з будь-яким іншим учасником мережі без залучення стороннього посередника.

Як згадувалось у першій частині даної роботи, один з загальнопоширених допоміжних інструментів, без якого неможливий захист даних у відкритих

мережах, - це технологія цифрових сертифікатів. Втім, не є секретом і те, що головний недолік цієї технології - безумовна довіра до центрів, що випускають цифрові сертифікати.

У даній роботі автори пропонують новий підхід до організації інфраструктури загальнодоступних ключів (Public Key Infrastructure, PKI), який допоможе усунути існуючі нині недоліки та який використовує технологію розподіленого реєстру (блокчейна) і дозволяє створити децентралізовану інфраструктуру відкритих ключів.

Основними компонентами Blockchain є книги обліку (реєстраційні книги), що дозволяють відслідкувати активність учасників у певний момент часу. Під поняттям книги обліку будемо розуміти послідовний список груп транзакцій з часовою міткою. Технологія Blockchain використовує криптографічні хеш-функції для унікального ідентифікатора учасників інформаційного обміну, що гарантує забезпечення цілісності даних. Транзакції в технології Blockchain підписуються приватними і публічними ключами. Публічний ключ є відкритим і доступним для всіх. Іншим елементом ідентифікування є приватний ключ, або ж пароліні дані, які прив'язуються до публічного. Маючи таку пару ключів, користувач проходить автентифікацію. Перевірка математичного зв'язку цих ключів відбувається на стороні програмного коду після введення приватного ключа у програмі.

Далі опишемо децентралізовану інфраструктуру загальнодоступних ключів, яка пропонується на базі технології Blockchain. Наприклад, є сервер баз даних, де зберігаються загальнодоступні ключі, де кожен ключ – це якась транзакція, яка зберігається в реєстрі. В даному випадку під поняттям нульової транзакції будемо розуміти таку транзакцію, до якого будуть прикріплюватися наступні транзакції з даними про загальнодоступні ключі. Кожна така транзакція містить спеціалізовану структуру даних, або по-іншому - нотифікат.

Під поняттям нотифікату будемо розуміти структурований набір даних, що складається з функціональних полів і включає інформацію про загальнодоступні ключі власника, персистентність якого гарантується розміщенням в одному з пов'язаних записів розподіленого реєстру. Під поняттям нульова транзакція будемо розуміти агрегацію шести полів даних. В ході формування нульової транзакції задіяна криптографічна ключова пара (загальнодоступний і парний секретний ключ). Ця пара ключів з'являється в той момент, коли користувач реєструється в системі та проходить процедуру автентифікації та авторизації.

Як показано на рис.1., дайджест загальнодоступного ключа буде формуватися шляхом послідовного застосування хеш-функцій SHA256 і RIPEMD160. Тут RIPEMD160 відповідає за компактне представлення даних, розрядність яких не перевищує 160 біт. Сам загальнодоступний ключ заноситься до п'ятого поля. У першому полі містяться дані, які встановлюють зв'язок з попередньою транзакцією. У нульовій транзакції це поле нічого не містить, що відрізняє її від подальших транзакцій. Друге поле - це дані для перевірки зв'язності транзакцій. Дані першого і другого полів назовемо для

стислості "зв'язкою" і "перевіркою" відповідно. Вміст цих полів формується методом ітеративного хешування на прикладі зв'язування другої і третьої транзакцій на рис. 2., що нижче. Дані з перших п'яти полів завіряються електронним-цифровим підписом (ЕЦП), який формується за допомогою секретного ключа. Далі нульова транзакція відправляється в пул і після успішної перевірки заноситься до реєстру.

Тепер до неї можна "підв'язувати" такі транзакції. Формування транзакцій, відмінних від нульової наведено на рис.2. Крім ключової пари використовуються ординарна і службова ключові пари.

Під поняттям ординарний загальнодоступний ключ будемо розуміти ключ, який задіяний в різних процедурах і процесах. Наприклад, секретний ключ з ординарної пари може використовуватися для формування ЕЦП різних документів, а загальнодоступний - для перевірки цієї ЕЦП з подальшим виконанням цих доручення за умови її валідності.

Службова пара видається зареєстрованому суб'єкту децентралізованої інфраструктури відкритих ключів DPKI (*Decentralized Public Key Infrastructure*). Назва цієї пари відповідає її призначенню. При формуванні/перевірці нульової транзакції службові ключі не застосовуються.

Таким чином, є дві групи ключів. У першу входять службові ключі і ключова пара – мають сенс тільки в контексті DPKI. До другої групи входять ординарні ключі - їх область застосування може відрізнитися і обумовлена тими прикладними завданнями, в яких вони використовуються. При цьому DPKI забезпечує цілісність і автентичність відбитку ординарних загальнодоступних ключів.

Рис. 1. Схема формування цифрового підпису

Рис. 2. Формування транзакцій, відмінних від нульової

Усі транзакції, які йдуть слідом за нульовою, формуються схожим чином: загальнодоступний ключ (але не ключової пари, як у випадку з нульовою транзакцією, а з ординарної ключової пари) проходить через дві хеш-функції SHA256 і RIPEMD160. Так формуються дані третього поля. В четверте поле заноситься супроводжує інформація (наприклад, інформація про поточний статус, терміни дії, тимчасова відмітка, ідентифікатори використовуваних криптоалгоритмів та ін.). У п'ятому полі - загальнодоступний ключ зі службової ключової пари. З його допомогою потім буде перевірятися ЕЦП, тому він тиражується.

Транзакція заноситься в пул і зберігається там до тих пір, поки не буде оброблена. Зберігання в пулі пов'язано з певним ризиком - дані транзакції можуть бути фальсифіковані. Власник запевняє дані транзакції ЕЦП. Загальнодоступний ключ для перевірки цього ЕЦП вказується в одному з полів транзакції в явному вигляді і згодом заноситься до реєстру. Особливості обробки транзакції такі, що зломисник здатний змінити дані на свій розсуд і потім завірити їх за допомогою свого секретного ключа, а парний загальнодоступний ключ для перевірки ЕЦП вказати в транзакції. Якщо справжність і цілісність забезпечується виключно за допомогою ЕЦП, то такий фальсифікація залишиться непоміченим. Однак, якщо крім ЕЦП існує додатковий механізм, що забезпечує одночасно архівування та персистентність інформації, що зберігається, то фальсифікацію можливо

виявити. Для цього достатньо занести до реєстру справжній загальнодоступний ключ власника.

Отже, при обробці даних найпершої транзакції власника необхідно підтвердити справжність занесеного до реєстру загальнодоступного ключа. Для цього слід прочитати ключ з реєстру і виконати його звірення з істинним загальнодоступним ключем власника в межах периметра безпеки (область відносної невразливості). Якщо справжність ключа підтверджена і його персистентність гарантується за фактом розміщення, то справжність ключа з подальшою транзакцією легко підтвердити/спростувати шляхом його звірення з ключем з реєстру. Іншими словами, ключ з реєстру використовується в якості еталонного зразка. Аналогічно обробляються всі інші транзакції власника.

Транзакція завіряється ЕЦП - тут-то і знадобляться секретні ключі, і не один, а відразу два - службовий і ключова пара. Завдяки використанню двох секретних ключів забезпечується необхідний рівень безпеки - адже службовий секретний ключ може бути відомий іншим користувачам, тоді як секретний ключ ключової пари відомий тільки власнику ординарної ключової пари. Такий дво ключовий підпис можна назвати "консолідованим" ЕЦП.

Перевірка транзакцій, відмінних від нульової, виконується з використанням двох загальнодоступних ключів: ключової пари і службового. Процес перевірки можна розділити на два основних етапи: перший - це перевірка дайджесту загальнодоступного ключа ключової пари, а другий - перевірка ЕЦП транзакції, тієї самої, консолідованої, яка була сформована за допомогою двох секретних ключів (ключової пари і службового). Якщо валідність ЕЦП підтверджено, то після додаткової перевірки транзакція заноситься до реєстру. Дана схема наведена на рис. 3.

Щоб перевірити чи належить транзакція конкретному ланцюжку з "коренем" у вигляді нульової транзакції, процес перевірки доповнений ще однією стадією - перевіркою зв'язності. Тут і знадобляться дані з перших двох полів.

Припустимо, що нам треба перевірити, чи дійсно транзакція №3 йде після транзакції №2. Для цього методом комбінованого хеширования обчислюється значення хеш-функції для даних з третього, четвертого і п'ятого полів транзакції №2. Потім виконується конкатенація даних з першого поля транзакції №3 і раніше отримане значення комбінованої хеш-функції для даних з третього, четвертого і п'ятого полів транзакції №2. Все це теж проходить через дві хеш-функції SHA256 і RIPEMD160. Якщо отримане значення збігається з даними другого поля транзакції №2, то перевірка пройдена і зв'язність підтверджена.

У загальному технологія формування та занесення нотифіката в реєстр виглядає саме таким чином. У цьому тексті ми не будемо зупинятися на деталях, які, безсумнівно, існують, і повернемося до обговорення самої ідеї децентралізованої інфраструктури загальнодоступних ключів.

Отже, оскільки заявник сам відправляє заявку на реєстрацію нотифікатів, які зберігаються не в базі даних, а в реєстрі, то основними архітектурними

компонентами DPKI слід вважати: Реєстр чинних нотіфікатів (РЧН); реєстр відкликаних нотіфікатів (РВН); реєстр призупинених нотіфікатів (РПН).

Рис.3. Перевірка транзакцій, відмінних від нульової

Інформація про загальнодоступні ключі зберігається в РЧН / РВН / РПН у вигляді значень хеш-функції. Варто також зауважити, що це можуть бути як різні реєстри, так і різні ланцюжки або навіть один ланцюжок в складі єдиного реєстру, коли інформація про статус ординарного загальнодоступного ключа (відгук, припинення дії та ін.) Заноситься в четверте поле структури даних у вигляді відповідного кодового значення. Існує безліч різних варіантів архітектурної реалізації DPKI і вибір того, чи іншого, залежить від ряду факторів, наприклад такого критерію оптимізації як витрати довготривалої пам'яті для зберігання загальнодоступних ключів та ін.

Таким чином, DPKI може виявитися якщо не простіше, то щонайменше порівнянню з централізованим рішенням за складністю архітектури.

Головна вимога до реєстру – можливість формування транзакцій довільного типу. Найвідоміший приклад застосування реєстру - це мережа біткойнів. Але в ній при реалізації описаної вище технології виникають певні труднощі: виявляється обмеженість існуючого мови сценаріїв, відсутність необхідних механізмів для обробки довільних наборів даних, способів формування транзакцій довільного типу, а також багато іншого.

Вирішити сформовані вище проблеми і може реєстр, який включає наступне:

- підтримує декілька типів транзакцій: в ньому можна як обмінюватися активами (тобто виконувати фінансові транзакції), так і формувати транзакції з довільною структурою;

- розробникам доступна пропріетарна мова програмування PrismLang, що забезпечує необхідну гнучкість при вирішенні різних технологічних завдань;

- передбачений механізм обробки довільних наборів даних.

Якщо підходити спрощено, то має місце наступна послідовність дій:

- Заявник реєструється в DPKI і отримує цифрову ключову пару. Адреса її - значення хеш-функції від загальнодоступного ключа пари. Секретний ключ пари відомий тільки замовнику.

- Зареєстрованому суб'єкту надається доступ до службового секретного ключа.

- Суб'єкт формує нульову транзакцію і запевняє її ЕЦП з використанням секретного ключа пари.

- Якщо формується відмінна від нульової транзакція, то підтверджує її ЕЦП з використанням двох секретних ключів: ключової пари і службового.

- Суб'єкт відправляє транзакцію в пул.

- Вузол мережі ENCRY зчитує транзакцію з пулу і перевіряє ЕЦП, а також зв'язність транзакції.

- Якщо ЕЦП валідний і зв'язність підтверджена, то готує транзакцію для занесення до реєстру.

- Тут реєстр виступає в ролі розподіленої бази даних, в якій зберігається інформація про діючі, анульовані і призупинені нотифікати.

Звичайно, децентралізація не повноцінне вирішення проблеми забезпечення коректної перевірки цифрових сертифікатів. Фундаментальна проблема первинної автентифікації користувачів нікуди не зникає: якщо в даний час перевіркою сертифікатів займаються централізовані системи, то в DPKI перевірку пропонується делегувати учасникам спільнот.

Висновки

Отже, підсумовуючи вище викладене, варто відмітити результати досліджень:

1. На сьогодні важливе місце у забезпеченні безпеки комунікацій у мережі посідає процес верифікації цифрових сертифікатів. Аналіз вразливостей у механізмі верифікації, що виявлені на сьогоднішній день,

дозволяє сформулювати новий підхід щодо перевірок цифрових сертифікатів і пересвідчитись у їх справжності і дійсності.

2. Одним з актуальних способів підвищення рівня захисту операційної системи Windows є використання нового напрямку Blockchain для здійснення верифікації цифрових сертифікатів.

Література

1. The Secure Sockets Layer (SSL)/ T. Dierks. // 1-st. — RTFM, Inc., August 2008. — № 1. — P. 207.
2. SSL & TLS Essentials: Securing the Web/ Stephen Thomas. — 1-st. — Wiley, 2000. — Т. 1. — 224 p.
3. Computer Security and Industrial Cryptography/ Joris Claessens, 2002. —P. 253–265. — 287 p.
4. Discovery and Exploitation of New Biases in RC4/ Pouyan Sepehrdad, 2011 – 24 p. — 91 p.
5. The Secure Sockets Layer (SSL) Protocol Version 3.0 / P. Karlton, 2011. — P. 67.
6. The Transport Layer Security (TLS) Protocol Version 1.2/ E. Rescorla. 2008. — № 1. — P. 101.
7. Stephen Thomas. SSL & TLS Essentials: Securing the Web. — 1-st. — Wiley, February 11, 2000. — Т. 1. — 224 p.
8. John Viega. Network Security with OpenSSL. — 1-st. — O'Reilly Media, USA, June 15, 2002. — Т. 1. — 386 p.
9. The AWS SDK for Java. [Електронний ресурс]. – Режим доступу до ресурсу: <https://github.com/aws/aws-sdk-java>.
10. Introduction to Public Key Technology and the Federal PKI Infrastructure / D. Richard Kuhn Vincent, C. Hu, W. Timothy Polk, Shu-Jen Chang, 2001. - 16p.

References

1. The Secure Sockets Layer (SSL)/ T. Dierks. // 1-st. — RTFM, Inc., August 2008. — № 1. — P. 207.
2. SSL & TLS Essentials: Securing the Web/ Stephen Thomas. — 1-st. — Wiley, 2000. — Т. 1. — 224 p.
3. Computer Security and Industrial Cryptography/ Joris Claessens, 2002. —P. 253–265. — 287 p.
4. Discovery and Exploitation of New Biases in RC4/ Pouyan Sepehrdad, 2011 – 24 p. — 91 p.
5. The Secure Sockets Layer (SSL) Protocol Version 3.0 / P. Karlton, 2011. — P. 67.
6. The Transport Layer Security (TLS) Protocol Version 1.2/ E. Rescorla. 2008. — № 1. — P. 101.
7. Stephen Thomas. SSL & TLS Essentials: Securing the Web. — 1-st. — Wiley, February 11, 2000. — Т. 1. — 224 p.
8. John Viega. Network Security with OpenSSL. — 1-st. — O'Reilly Media, USA, June 15, 2002. — Т. 1. — 386 p.
9. The AWS SDK for Java. [Online]. – Available: <https://github.com/aws/aws-sdk-java>.
10. Introduction to Public Key Technology and the Federal PKI Infrastructure / D. Richard Kuhn Vincent, C. Hu, W. Timothy Polk, Shu-Jen Chang, 2001. - 16p.