УДК 004.056.5 **DOI:10.30837/rt.2023.3.214.02**

М. О. БОДНЯ, М. В. ЄСІНА, канд. техн. наук, В. А. ПОНОМАР, канд. техн. наук

ОСНОВНІ ОСОБЛИВОСТІ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Вступ

На сьогодні широко застосуються засоби мережевої інфраструктури та інформаційно-комунікаційні системи для організації спілкування та обміну даними між користувачами. Внаслідок цього виникло питання – як забезпечити автентифікацію всіх авторизованих користувачів. Сучасні криптографічні протоколи автентифікації базуються на криптографії з відкритим ключем. Системи захисту інформації та технічні засоби захисту не можуть повністю гарантувати запобігання несанкціонованому доступу до каналу зв'язку, внаслідок цього реалізовуються різноманітні протоколи та системи автентифікації, що ґрунтуються на асиметричній криптографії. Застосування технологій та процедур, що засновані на криптографії з відкритим ключем, широко впроваджуються в системи комерційних організацій та урядових установ, тому що вони забезпечують надійний механізм, який дозволяє підтвердити, що особа є тим, за кого себе видає, та реалізувати конфіденційність, цілісність, неспростовність та автентичність інформації.

Як показує практика, застосування асиметричної криптографії є недостатнім комплексом методів та технологій для забезпечення процедури достовірної автентифікації та обміну інформацією між авторизованими користувачами. Суб'єкти комунікації гіпотетично можуть використовувати паперові документи, які містять персональні дані та відкриті ключі авторизованих користувачів, підписані рукописним підписом та завірені нотаріусом. Але в такому випадку виникає проблема масштабності: проведення нотаріального завірення документів для великої множини суб'єктів спілкування потребує великої кількості аркушів паперу та займає багато часу. Інфраструктура відкритих ключів (ІВК) є надійним інструментом для розв'язання задач, пов'язаних з автентифікацією користувачів та визначенням легітимності, справжності відкритих ключів користувачів у цифровому середовищі.

Структура ІВК складається зі спеціалізованих компонентів, кожен з яких має власний напрям діяльності та фіксований спектр задач. При цьому забезпечуються всі процеси відносно управління цифровими сертифікатами, які включають: видачу, перевипуск, відкликання сертифікатів, управління життєвим циклом та ключами сертифікатів тощо. Такі сертифікати підтверджують факт належності певного відкритого ключа конкретному суб'єкту та наявності у відповідного суб'єкта секретного ключа. Завдяки цифровим сертифікатам всі сторони можуть ідентифікувати один одного та безпечно обмінюватись інформацією через мережу. Фальсифікувати облікові дані цифрового сертифіката, видані центром сертифікації, дуже важко, адже цифровий сертифікат підписується особистим ключем центру сертифікації, який відомий лише йому. Цифровий підпис забезпечує цілісність, автентичність та неспростовність відповідного сертифікату.

ІВК є комплексною системою, яка має раціональну структуру та широкий набір функцій, які спрощують процедуру автентифікації та забезпечують її справжність на підставі цифрових сертифікатів. Суб'єкти комунікації можуть повністю не довіряти один одному, але довіряти третій незалежній стороні, яка регулює механізм встановлення довіри між ними. Цей механізм базується на використанні цифрових сертифікатів і криптографії з відкритим ключем та є важливим елементом для забезпечення безпеки та конфіденційності інформації в Інтернеті та інших цифрових середовищах.

ІВК широко застосовується для проведення безпечних електронних транзакцій, банківських операцій, цифровізації та трансформації уряду, державних установ та організацій задля підвищення рівня якості надання послуг та організації комунікації між суспільством та державними органами. Міжнародна спільнота розгортає та модернізує ІВК у вигляді надійного механізму для забезпечення процесу обміну інформацією та комунікації.

Мета статі - аналіз можливих зовнішніх загроз сторонам комунікації в інформаційному просторі, методології їх виявлення та захисту за допомогою ІВК, концепції ІВК, дослідження компонентів ІВК, методів та апаратних засобів захисту інформації, які застосовуються в парадигмі ІВК.

1. Зовнішні загрози та методи їх вирішення за допомогою використання ІВК

1.1. Атака «людина посередині»

Атака «людина посередині» – це тип кібератаки, при якій зловмисник прослуховує та перехоплює інформацію суб'єктів комунікації, через отримання несанкційованого доступу до каналу зв'язку. Зловмисник симулює себе як суб'єкта комунікації та шляхом маніпуляцій нав'язує власний відкритий ключ сторонам комунікації. Всі сторони вважають, що вони здійснюють обмін інформацією один з одним, але насправді весь потік інформації проходить через зловмисника, який може вносити зміни та пересилати викривлену інформацію з метою обману. При передачі відкритого ключа від одного суб'єкта до іншого, зловмисник може перехопити відкритий ключ отримувача та надіслати власний відкритий ключ адресанту, як наслідок він зможе розшифрувати шифртекст власним особистим ключем та отримати доступ до інформації.

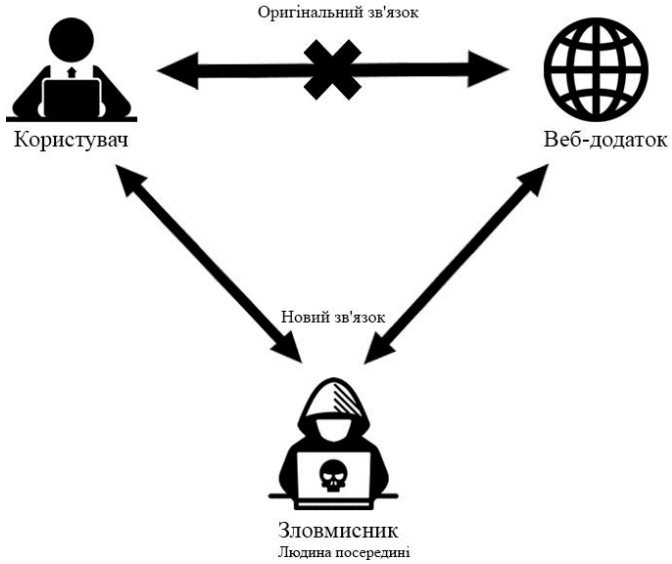

Рис. 1. Модель атаки «людина посередині»

Кібератака «людина посередині» представляє вагому загрозу для користувачів, адже сторони комунікації навіть не підозрюють, що їх прослуховує зловмисник. Механізм управління відкритими ключами ІВК дозволяє захиститися від атаки «людина посередині». Зловмисник може непомітно підмінити відкритий ключ сторони комунікації на свій відкритий ключ [1]. Ця проблема вирішується за допомогою цифрових сертифікатів. Кожна сторона має цифровий сертифікат, у якому наведено основні відомості про сторону та її відкритий ключ. Цифровий сертифікат підписується цифровим підписом центру сертифікації для забезпечення цілісності та справжності документа. Внаслідок цього одна сторона може однозначно ідентифікувати та автентифікувати іншу сторону, перевірити сертифікат на справжність відкритим ключем центру сертифікації та на основі цього вибудовувати довірчі відносини. ІВК допомагає виявити атаку типу «людина посередині». У разі виявлення кібератаки рекомендується використовувати альтернативний канал зв'язку для продовження комунікації. ІВК сприяє встановленню ланцюжка довіри між суб'єктами комунікації. Людина посередині не зможе сформувати цифровий сертифікат для заміни або підробки вихідного сертифіката, оскільки він не має відповідного особистого ключа для створення справжніх сертифіка-

тів. Крім того, зловмисник не зможе представитися однією з легітимних сторін, оскільки він не має доступу до їх особистих ключів. При передачі пакетів через мережу рекомендується використовувати цифровий підпис для забезпечення цілісності та автентичності даних. Якщо підпис перевіряється успішно, це свідчить про те, що переданий пакет не був модифікований.

1.2. Негативні аспекти самопідписаних сертифікатів, фальсифікація цифрових сертифікатів, компрометація особистого ключа

Самопідписаний сертифікат підписується не центром сертифікації, а самим суб'єктом, з використанням особистого ключа. Кожна зацікавлена сторона може перевірити справжність цифрового підпису за допомогою відкритого ключа підписника. Самопідписані сертифікати мають ряд обмежень та недоліків:

1. Відсутність довіри: сертифікат підписується суб'єктом, а не незалежним уповноваженим органом, тому немає гарантії, що сертифікат справжній, дійсний та належить очікуваному власнику.

2. Обмежена сфера застосування: більшість веб-браузерів і програм, які сприймають та довіряють цифровим сертифікатам не допускають самопідписані сертифікати придатними для використання в захищених з'єднаннях по протоколу безпечної передачі даних HTTPS.

3. Ризик безпеки: якщо зловмисник отримає доступ до секретного ключа, він матиме можливість видавати власні сертифікати за сертифікати очікуваного суб'єкта, що несе потенційну загрозу для конфіденційності інформації.

Недоліки самопідписаних сертифікатів доводять їх малоефективність, цим документам не можна повністю довіряти внаслідок відсутності стовідсоткової гарантії їх справжності. Зловмисник може використовувати самопідписані сертифікати, щоб імітувати себе як легітимну сторону. Рекомендується використовувати цифрові сертифікати, сформовані та підписані центром сертифікації, вони гарантують високий рівень довіри та безпеки. Реалізувати фальсифікацію цифрових сертифікатів виданих центром сертифікації дуже складно, бо вони підписані особистим ключем центру сертифікації. Сертифікат вказує на те, що суб'єкт володіє відкритим та особистим ключами, а також надає основні відомості про власника сертифіката. Цифровий підпис центру сертифікації гарантує цілісність, автентичність та справжність цифрового сертифіката.

Фальсифікація цифрових сертифікатів – це створення та використання сфабрикованих сертифікатів для представлення себе як легітимної сторони. Такі сертифікати можуть становити серйозну загрозу для конфіденційності та безпеки інформації. Зловмисники застосовують фальсифіковані сертифікати для кібератаки типу «людина посередині», перехоплення сертифікати, видані центром сертифікації, а також регулярно оновлювати сертифікати.даних, підміни ключів, шахрайства та інших видів атак, підмінюючи свою легітимність. Для запобігання подібним загрозам необхідно перевіряти ланцюжки довіри, використовувати

Компрометація особистого ключа означає, що зловмисник отримав несанкціонований доступ до особистого ключа, який використовується в криптографічних операціях. Коли зловмисник отримує доступ до особистого ключа, він може використовувати його для розшифрування зашифрованих даних, підпису повідомлень та документів від імені власника ключа, а також для інших махінацій. Зловмисник може видавати себе за власника особистого ключа та легітимну сторону, маючи доступ до особистого ключа. Для запобігання загрозі несанкціонованого доступу до особистого ключа неавторизованими користувачами, власнику особистого ключа потрібно використовувати захищені апаратні модулі, сховища та електронні пристрої, які містять блоки пам'яті для зберігання інформації. В ІВК передбачена процедура відкликання сертифікатів, якщо користувач втратив особистий ключ. Відкликання сертифіката автоматично зробить його недійсним, а також не придатним для побудови ланцюжка довіри. Механізм ІВК побудований таким чином, що виключається ймовірність підробки сертифіката або використання зловмисником сертифіката іншого суб'єкта.

2. Концепція ІВК та її компоненти

Інфраструктура відкритих ключів (ІВК) – сукупність процедур, методів, людського контингенту, програмного та апаратного забезпечення, які формують загальну систему, яка підтримує застосування криптографії з відкритим ключем для забезпечення безпеки комунікації. ІВК реалізує механізм, який включає комплекс процедур, алгоритмів, процесів та систему надання послуг. Для створення безпечного простору, в якому суб'єкти можуть в спрощеному порядку ідентифікувати один одного та обмінюватися інформацією між собою. ІВК являє собою надійну структуру третьої незалежної сторони, яка називається центром сертифікації [2]. ІВК складається з профільованих служб та матеріальних компонентів, які взаємодіють між собою та з користувачами або потенційними клієнтами. Всі складові ІВК функціонують та діють відповідно до регламенту системи. Механізм ІВК дозволяє регулювати управління відкритими ключами, цифровими сертифікатами та сприяє зменшенню кількості випадків фальсифікації сертифікатів. Методологія ІВК відносно створення, видачі та відкликання цифрових сертифікатів побудована таким чином, щоб мінімізувати ризики безпеки. ІВК є багатогранною структурою, яка охоплює не лише різноманітні інформаційні технології та електронні пристрої. Вона включає [3]: центр реєстрації, центр сертифікації, стратегії та підходи до забезпечення безпеки, системи поширення та зберігання цифрових сертифікатів, додатки та програми, які підтримують ІВК.

Рис. 2. Компоненти інфраструктури відкритих ключів

До складових ІВК відносяться наступні елементи:

1. Центр сертифікації (ЦС) – ключовий компонент ІВК, який відповідає за видання, керування та валідацію цифрових сертифікатів. ЦС може формувати цифрові сертифікати для кінцевих користувачів та підлеглих ЦС. ЦС є невід'ємною складовою ІВК, яка асоціюється з арбітром, якому повністю довіряють учасники комунікації. Основною метою ЦС є валідація та автентифікація різних сутностей [4], таких як веб-сайти, домени, сервери, організації або фізичні особи для забезпечення їхньої легітимності та безпеки. ЦС проводить перевірку ідентичності суб'єктів та сутностей, які подають запит на видачу сертифікатів. В ІВК, де присутній реєстраційний центр, саме він відповідає за перевірку ідентичності суб'єктів та сутностей, які подають запит на видачу сертифікатів. Після успішної перевірки ідентичності суб'єкта ЦС видає цифровий сертифікат, який містить відкритий ключ та інформацію про його власника. ЦС має наступні функції:

- створює, видає та перевидає цифрові сертифікати;
- здійснює управління цифровими сертифікатами: веде реєстр сертифікатів, відповідає за оновлення та відкликання сертифікатів;

- здійснює перевірку облікових даних суб'єктів для підтвердження їх ідентичності;
- проводить валідацію сертифікатів;
- виконує комплекс процедур та операцій, з метою встановлення довіри між суб'єктами.

2. Реєстраційний центр (РЦ) – компонент ІВК, який перевіряє ідентичність суб'єкта, надає дозвіл на створення цифрового сертифіката, збирає та передає ЦС необхідну інформацію для подальшої видачі сертифіката. ЦС та РЦ є структурами ІВК, які відокремлені одна від одної, але вони взаємодіють між собою та довіряють один одному. РЦ приймає запити, які надходять від серверів, користувачів та організацій на створення нового сертифікату або подовження сертифіката, після перевірки облікових даних та ідентифікації суб'єкта запит надходить до ЦС, який здійснює видачу сертифіката [5, 6]. По завершенню перевірки облікових даних суб'єкта РЦ підписує перевірену інформацію особистим ключем та передає ЦС, після чого ЦС перевіряє відповідну інформацію відкритим ключем РЦ [7]. Підписання даних цифровим підписом здійснюється з метою забезпечення цілісності, автентичності та неспростовності інформації.

3. Сутності з підтримкою ІВК – об'єкти, які підтримують та застосовують систему ІВК [3]. До таких сутностей відносяться: банкомати, платіжні термінали, системи електронного доставлення та платежів, державні установи, технологічні компанії, міжнародні корпорації, сервери, комп'ютерні й мережеві пристрої тощо. Копії цифрового сертифіката ЦС мають бути поширені серед усіх сутностей, які підтримують ІВК для встановлення довірчих взаємовідносин у цифровому просторі. Цифровий сертифікат ЦС є ознакою, яка визначає, що ЦС – це надійний та легітимний орган, який спеціалізується на сертифікації та не залежить від жодної сутності.

4. Сховище сертифікатів – це база даних, яка містить видані сертифікати, включаючи сертифікати, у яких закінчився термін дії, а також запити на отримання цифрового сертифіката, які очікують на розгляд або відхилені [3]. Захист сховища сертифікатів забезпечується шифруванням та різноманітними фізичними методами захисту інформації.

5. Політики сертифікатів – документи, спрямовані на визначення різних об'єктів ІВК, їх компетенцій та обов'язків в рамках здійснення етапів робочого процесу ІВК.

6. Список відкликаних сертифікатів (СВС) містить перелік цифрових сертифікатів, які відкликані ЦС до фактичної дати закінчення терміну дії [8].

7. Online Certificate Status Protocol (OCSP) [9] є альтернативою СВС, замість того, щоб завантажувати та перевіряти наявність конкретного цифрового сертифіката в повному СВС, протокол OCSP дозволяє запитувати сервер щодо статусу дійсності конкретного цифрового сертифіката в режимі реального часу.

3. Методи та засоби захисту інформації в парадигмі ІВК

3.1. Цифровий підпис та сертифікат

ІВК складається з різноманітних компонентів, які взаємодіють між собою. Центри, які входять до складу ІВК, використовують цифровий підпис, який базується на криптографії з відкритим ключем для побудови довірчих відносин. Цифровим підписом підписуються та завіряються цифрові сертифікати, електронні документи та списки, що надаються іншим організаціям для перевірки конкретних сертифікатів. Застосування цифрового підпису забезпечує безпеку взаємовідносин між внутрішніми структурами та зовнішніми сутностями. Цифровий підпис гарантує забезпечення цілісності, автентичності та неспростовності інформації, що є фундаментальними атрибутами для забезпечення безпеки та довіри в цифровому середовищі. Він є електронним аналогом рукописного підпису в паперовому документі. Основна роль цифрового підпису – підтвердити походження документа від першоджерела та зафіксувати вміст документа на момент підписання, тим самим забезпечити його цілісність. Цифровий підпис є ключовим елементом цифрового сертифіката, на базі якого суб'єкти встановлюють довірчі взаємовідносини в інформаційному середовищі.

Цифровий сертифікат є електронним документом, який містить ідентифікаційну інформацію щодо власника цього сертифікату, його відкритий ключ та цифровий підпис ЦС. Сертифікати використовуються сторонами комунікації для перевірки особистості один одного та для встановлення довіри між сторонами в інформаційному просторі. Також вони дозволяють захистити інформацію від несанкціонованого доступу або модифікації. Ідентифікаційна інформація щодо власника сертифіката та його відкритий ключ перетворюються в геш-значення за допомогою геш-функції. Особистим ключем ЦС виконується операція підписання геш-значення. Процес підписання здійснюється шляхом застосування криптографічної функції до геш-значення для створення цифрового підпису. Алгоритм підпису використовує особистий ключ ЦС для формування унікального цифрового підпису. Згенерований цифровий підпис додається до вихідних даних у цифровому сертифікаті.

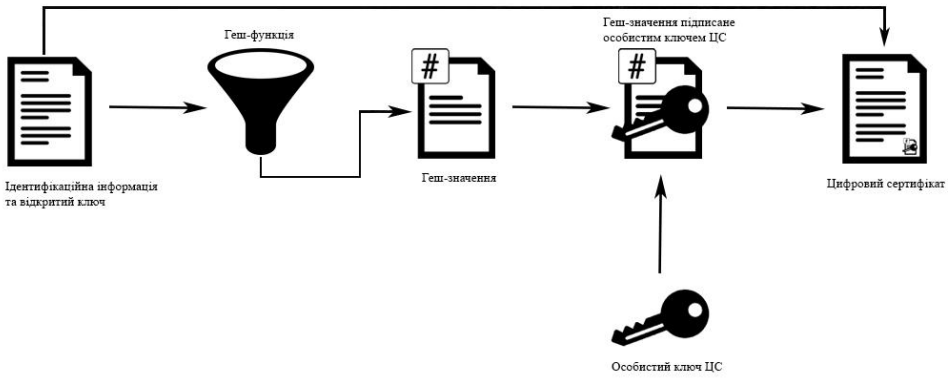

Рис. 3. Схема процедури підписання цифрового сертифіката

Цифровий підпис ЦС гарантує цілісність даних, наведених в сертифікаті, та підтверджує належність відкритого ключа конкретному суб'єкту. Формат та структура цифрових сертифікатів, використовуваних в ІВК, визначені в стандарті X.509. Цифровий сертифікат X.509 містить інформацію про суб'єкта, відкритий ключ, а також організацію, яка видала сертифікат та інші метадані. ЦС створює та підписує цифровий сертифікат, тому в сертифікаті містяться основні дані щодо ЦС, включаючи назву та відкритий ключ. При отриманні цифрового сертифіката інші сторони можуть перевірити справжність цифрового підпису, використовуючи відкритий ключ ЦС. Цифровий сертифікат містить дати початку та закінчення строку дії сертифіката. Після закінчення терміну дії сертифікат стає недійсним. Кожному цифровому сертифікату присвоюється унікальний ідентифікатор. Він дозволяє відрізнити сертифікати один від одного. В цифровому сертифікаті вказується криптографічний алгоритм, використаний для генерації цифрового підпису.

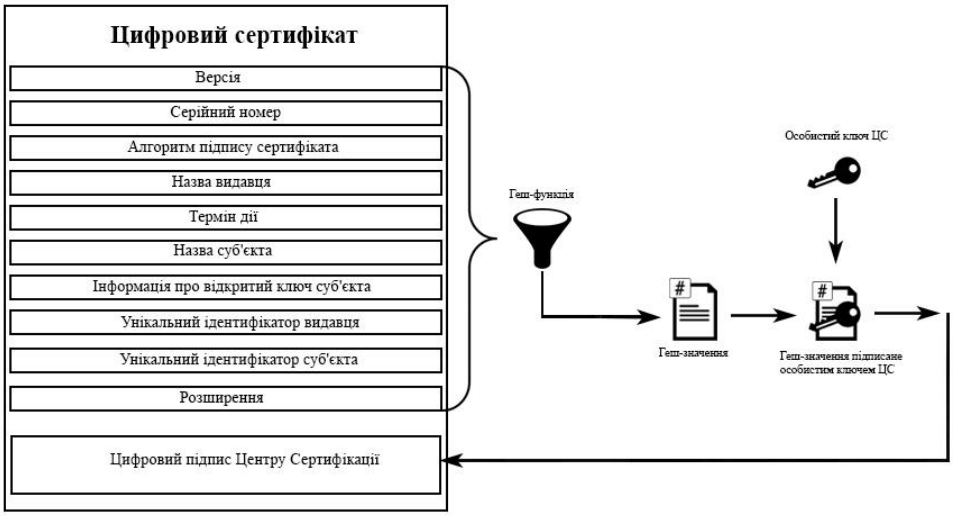

Рис. 4. Формат цифрового сертифіката X.509 V3 та модель побудови цифрового підпису

3.2. Смарт-карти

Смарт-карти – це маленькі пластикові карти, які оснащені вбудованим мікропроцесором, який здатний виконувати різноманітні обчислювальні та криптографічні операції. Смарт-карти також оснащені пам'яттю, що дозволяє зберігати відкриті, секретні ключі та цифрові сертифікати. Смарт-карта надає сховище для секретних ключів, які в більшості випадків використовуються виключно на смарт-карті й ніколи не залишають її для забезпечення максимальної безпеки. Смарт-картка застосовується для генерації цифрового підпису, обчислене геш-значення зберігається на смарт-карті та підписується особистим ключем. Криптографічні операції для валідації цифрового підпису, також проводяться на смарт-карті.

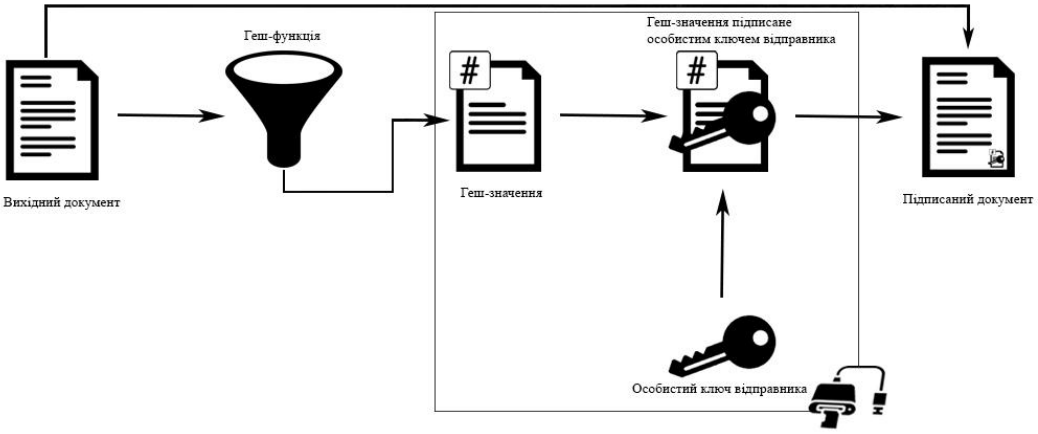

Рис. 5. Схема процедури підписання електронного документа за допомогою смарт-карти

Смарт-карти можуть генерувати відкритий та особистий ключі та здатні зберігати обмежені обсяги пам'яті. Смарт-карти використовуються для генерації цифрових сертифікатів, можна виділити два методи генерації цифрових сертифікатів [10]:

1. ЦС створює відкритий та особистий ключі в захищеному середовищі, формує, підписує цифровий сертифікат та імпортує його на смарт-карту (рис. 6).

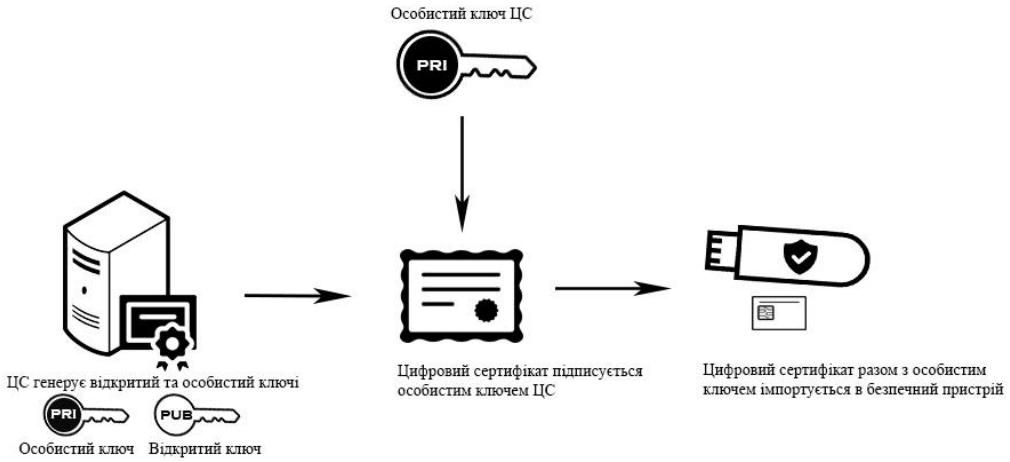

Рис. 6. Схема першого методу генерації цифрових сертифікатів

2. Генерація відкритого та особистого ключів здійснюється всередині смарт-карти (рис. 7).

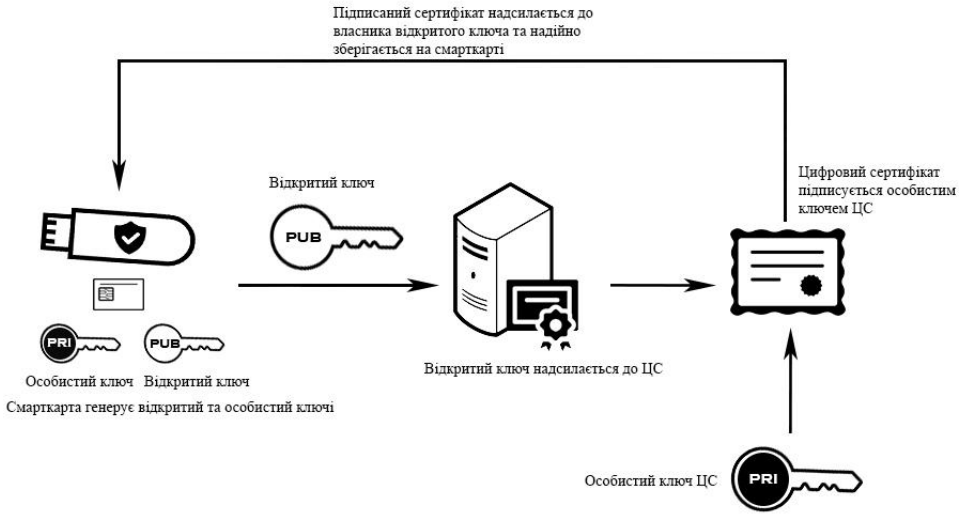

Рис. 7. Схема другого методу генерації цифрових сертифікатів

Смарт-карти є мобільними та компактними пристроями, оскільки за розмірністю відповідають стандартним банківським картам. Смарт-карта оснащена вбудованим механізмом безпеки для забезпечення конфіденційності, цілісності та автентичності даних, які зберігаються на смарт-карті. ПІН є важливим компонентом для забезпечення безпеки, він необхідний для отримання доступу до функцій смарт-карти та конфіденційної інформації. Здебільшого, ПІН – це послідовність цифр в діапазоні від 0 до 9 [11]. Користувач матиме можливість повторно ввести ПІН, якщо він неправильне ввів значення ПІН. Кількість спроб введення ПІН обмежена в основному до трьох спроб, щоб уникнути вичерпного пошуку. Смарт-карта переходить в режим блокування у випадку, якщо максимальна кількість спроб введення перевищується. Розробниками смарт-карт передбачено додатковий механізм для розблокування смарт-карти. Користувачу необхідно ввести правильну комбінацію числового коду, яка називається персональний ключ розблокування (ПКР) для зняття режиму блокування. Система, також встановлює обмежену кількість спроб для введення значення ПКР. Порівняно з числовою послідовністю ПІН, яка складається з 4–6 цифр, ПКР представляє собою довгу послідовність, яка переважно складається з 10–20 цифр, яку дуже складно зафіксувати в пам'яті. Для використання особистого ключа, який міститься на смарт-карті, користувач повинен володіти двома компонентами: послідовністю ПІН та смарт-картою. У деяких смарт-картах біометрична авторизація використовується як альтернатива до авторизації за допомогою ПІН. Біометрична авторизація підвищує рівень безпеки особистих ключів, бо біометричні параметри не можуть бути передані іншим особам.

Висновки

1. Механізм управління відкритими ключами ІВК дозволяє виявити та захиститися від атаки типу «людина посередині» завдяки застосуванню криптографії з відкритими ключем та цифрових сертифікатів. Використання криптографії з відкритими ключами та цифрових сертифікатів грає ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних та сприяє уникненню широкого спектра зовнішніх загроз, таких як кібератака типу «людина посередині», компрометація особистого ключа, фальсифікація цифрових сертифікатів тощо.

2. ІВК є комплексною системою, ключовим елементом якої є ЦС, який виконує роль третьої сторони в комунікаційному процесі групи сторін. ЦС сприяє встановленню ланцюжка довіри між сторонами для подальшої взаємодії в інформаційному просторі. Довірчі відносини між сторонами встановлюються на основі цифрових сертифікатів, виданих ЦС.

3. ІВК є рішенням для організації процедури ідентифікації та автентифікації конкретного суб'єкта в режимі онлайн. Цифровий сертифікат виконує роль посвідчення суб'єкта, яке

дозволяє іншим сторонам ідентифікувати та перевірити особистість в цифровому світі. ІВК регулює механізм управління цифровими сертифікатами, які є невід'ємним елементом для встановлення довіри та інформаційної безпеки в мережевих комунікаціях.

4. Сертифікати X.509 є структурованими, надійними та широко використовуються для забезпечення безпеки та автентифікації в мережевих протоколах та інформаційних системах.

5. Компоненти ІВК складають комплексну структуру та взаємодіють між собою, використовуючи різні механізми на основі криптографії з відкритим ключем для забезпечення інформаційної безпеки.

6. Всі процеси та процедури проходять згідно зі встановленим регламентом системи ІВК.

7. ІВК є регулятором процесів, пов'язаних з управлінням відкритими ключами та встановленням довіри між сторонами, які ініціюють комунікацію через мережу.

8. Для підвищення рівня безпеки необхідно використовувати апаратні засоби та електронні пристрої, які надають безпечне сховище для відкритих і особистих ключів та цифрових сертифікатів.

Список літератури:

1. Інфраструктура управління відкритими ключами PKI. [Електронний ресурс]. Режим доступу: http://infoprotect.net/varia/infrastruktura-otkrytyh-klyuchey-pki.

2. CCNA Cyber Ops (Version 1.1). Chapter 9: Cryptography and the Public Key Infrastructure. [Електронний ресурс]. Режим доступу: https://itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-9-cryptography-and-the-public-key-infrastructure.html.

3. PKI for EMV cards compliant to PCI DSS. [Електронний ресурс]. Режим доступу: https://www.cryptomathic.com/news-events/blog/pki-for-emv-cards-compliant-to-pci-dss.

4. Certificate authority (CA). [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/certificate-authority.

5. PKI Fundamentals. [Електронний ресурс]. Режим доступу: https://pki.treas.gov/pki_funds3.htm.

6. What is a Registration Authority? [Електронний ресурс]. Режим доступу: https://www.primekey.com/wiki/what-is-a-registration-authority/.

7. Інфраструктура відкритих ключів. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Інфраструктура_відкритих_ключів.

8. Certificate Revocation List (CRL). [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/Certificate-Revocation-List.

9. Online Certificate Status Protocol. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Online_Certificate_Status_Protocol

10. Cryptography and Public Key Infrastructure. Режим доступу: https://downloads.acs.com.hk/technology/494-09-pki-and-middleware.pdf.

11. Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier. Introduction to Public Key Infrastructures. 2013. P. 68–70.

Надійшла до редколегії 05.08.2023

Відомості про авторів:

Бодня Микита Олегович – Харківський національний університет імені В. Н. Каразіна, студент факультету комп'ютерних наук; Україна; e-mail: bodnia2020kb12@student.karazin.ua

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Пономар Володимир Андрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, інженер-конструктор АТ "Інститут Інформаційних Технологій"; Україна; e-mail: Laedaa@gmail.com; ORCID: https://orcid.org/0000-0001-5271-2251