УДК 681.3

Ю.В. Морозов, В.М. Сокіл
Національний університет "Львівська політехніка",
кафедра "Електронні обчислювальні машини"

ЦИФРОВІ СЕРТИФІКАТИ – ОСНОВА СИСТЕМ ІДЕНТИФІКАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Запропоновано новий підхід для зберігання конфіденційної інформації, що поєднує надійну ідентифікацію об'єкта та надання додаткової інформації про об'єкт.

New solution proposes for saving confidence information, which join trust identification and giving additional information of object.

Більшість людей вважають, що достатньо зашифрувати повідомлення одним із відомих алгоритмів, і інформація буде надійно захищена від зловмисників. Але при отриманні будь-якої інформації (не обов'язково зашифрованої) виникає ще одне дуже важливе запитання – а чи справді отримана інформація прийшла звідти, звідки вказано в повідомленні? Тобто чи є автор повідомлення тим, за кого він себе видає?

Розглянемо іншу ситуацію. Нехай є закрита інформаційна система, в якій міститься будь-яка захищена (секретна) інформація. При отриманні доступу до системи треба перевірити, чи має об'єкт право на доступ до системи і чи є об'єкт тим, за кого він себе видає.

Тобто в обох випадках виникає проблема ідентифікації об'єкта.

Ідентифікація на основі паролів – це найпростіший інтуїтивний метод розпізнавання, проте він не є найкращим. Система з використанням паролів – це симетрична система з усіма її недоліками. Для ідентифікації користувача комп'ютерних мереж на основі паролів використовують такі протоколи, як PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) та протокол ідентифікації на основі одноразових паролів S/Key. Альтернативою ідентифікації на основі паролів є механізм ідентифікації об'єкта з використанням цифрових сертифікатів.

При використанні цифрових сертифікатів окрім сторони, яка перевіряє та сторони, яку перевіряють, в процесі ідентифікації бере участь третя сторона, так званий "арбітр", якому довіряють обидві сторони. "Арбітр" зберігає відкриті ключі клієнтів і на основі механізму цифрових сертифікатів гарантує відповідність відкритого ключа суб'єкту. Така схема використовується в асиметричних системах, коли ідентифікація виконується на основі відкритих ключів користувачів, що пересилаються за допомогою цифрових сертифікатів.

Міжнародним союзом телекомунікації в 1988 році був опублікований стандарт ITU-T X.509 (раніше CCITT X.509) або ISO/IEC/ITU 9594-8 як частина рекомендацій Каталогів X.500. Він визначав стандартний формат сертифікатів X.509.

Цифровий сертифікат – це структура певного формату, що однозначно ідентифікує об'єкт. Він містить необхідну стандартну інформацію про організацію, що видала сертифікат, деяку службову інформацію та певні відомості про суб'єкт, якому видається сертифікат. На рис. 1 показана базова структура сертифіката. Такий сертифікат відповідає вимогам стандарту X.509v3.

tbsCertificate містить всю інформацію, що має бути присутня в сертифікаті, тобто версія сертифіката, його унікальний номер, відомості про організацію, що видала сертифікат та про суб'єкт, якому видали цей сертифікат, час дії сертифіката, відкритий ключ суб'єкта та деяку іншу додаткову інформацію.

Окрім того, передбачено можливість використання додаткових типів розширень, в яких також може зберігатись потрібна інформація.

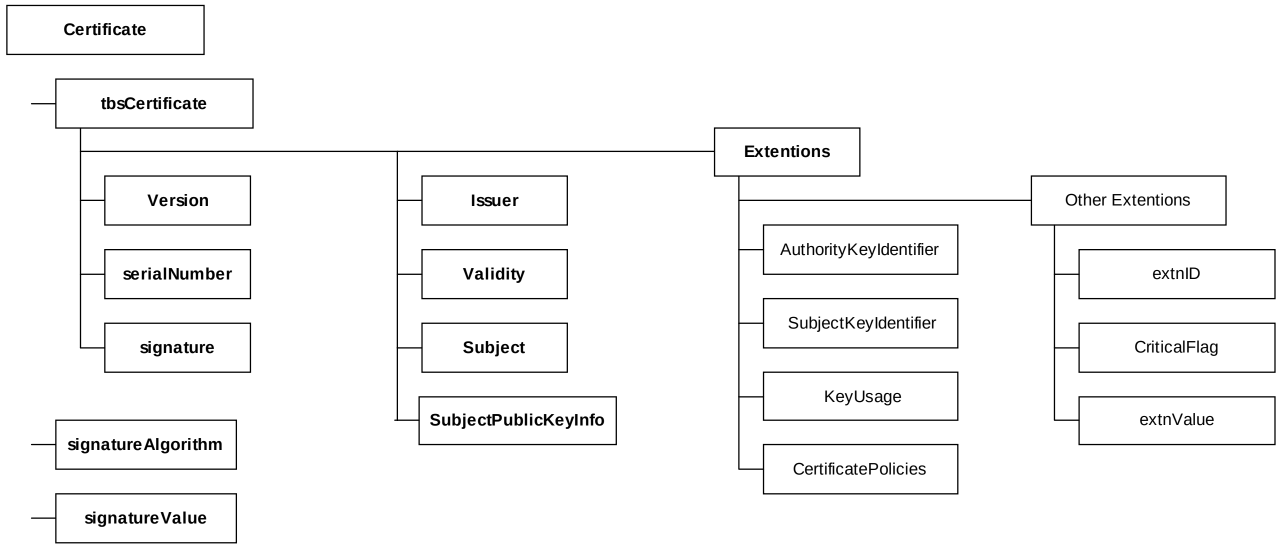

Рис. 1. Структура сертифіката

signatureAlgoritm містить інформацію про алгоритм, за допомогою якого організація

підписує цифровим підписом даний сертифікат, та його параметри (якщо вони необхідні). Для формування цифрового підпису використовується односторонній алгоритм хешування інформації SHA1 в поєднанні з алгоритмом ECDSA.

signatureValue – це безпосередньо значення цифрового підпису у форматі бітового рядка.

При побудові комп'ютерних мереж "закритого" типу, як правило, окремо реалізується система ідентифікації об'єктів та база для зберігання захищених даних. Структурна схема такої системи показана на рис. 2.

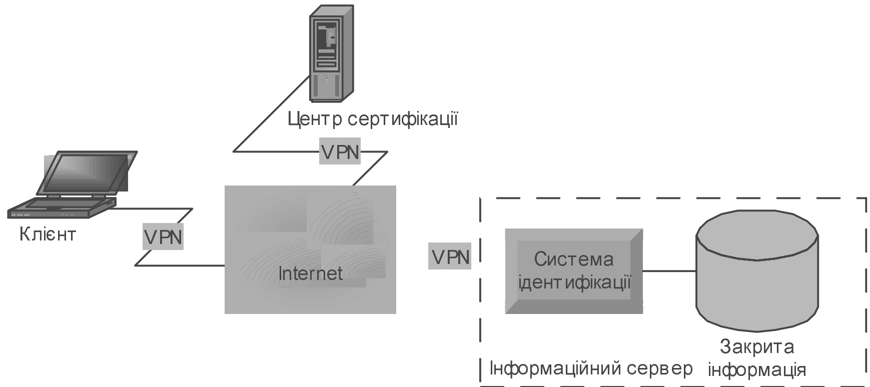

Рис. 2. Класична схема побудови захищеної комп'ютерної мережі

При такій реалізації клієнт спочатку отримує сертифікат в окремому центрі сертифікації. Водночас для нього мають бути встановлені права доступу до захищеної інформації, що зберігається в іншій базі даних (на іншому сервері). Після цього він відправляє запит на потрібну інформацію разом з отриманим сертифікатом. Сертифікат перевіряється на сервері системою ідентифікації. За умови успішного завершення перевірки по захищеному каналу видається потрібна інформація.

В основу запропонованої системи покладено можливість зберігання та передачі потрібної інформації в додатково визначених та створених розширеннях базового сертифіката. Тобто центр сертифікації та сервер бази даних захищеної інформації об'єднуються в одну систему.

Структурна схема системи показана на рис. 3.

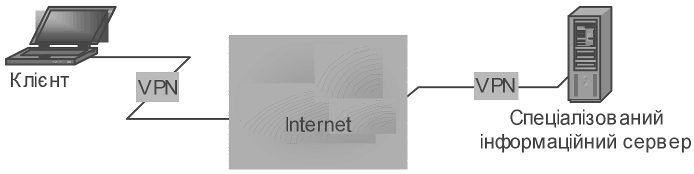

Рис. 3. Структура запропонованої комп'ютерної системи

Розглянемо детальніше структуру та огранізацію роботи спеціалізованого інформаційного сервера. Логічна структура сервера показана на рис. 4.

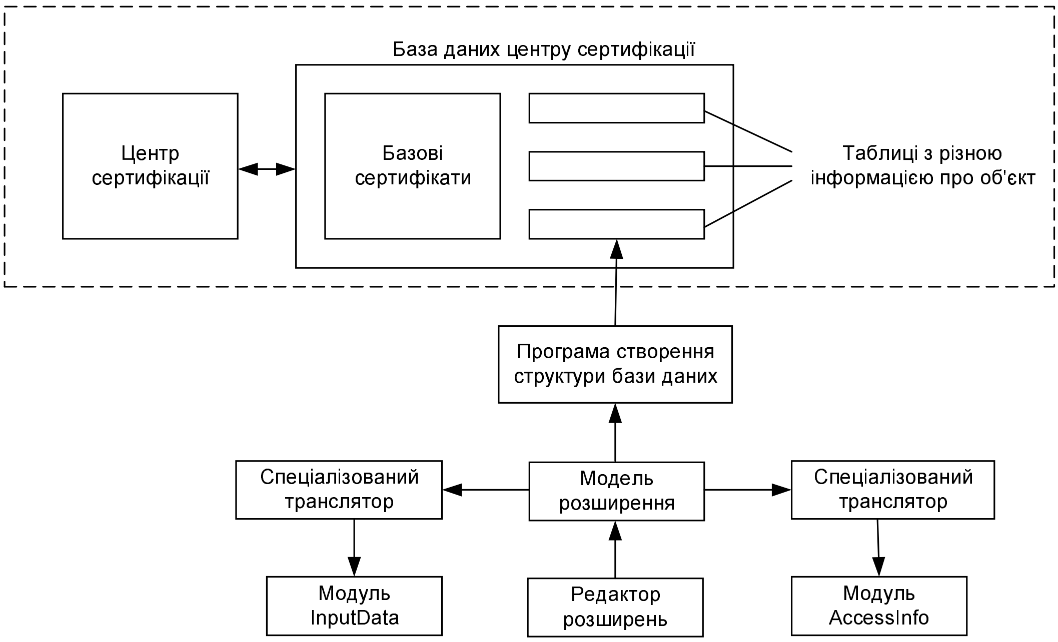

Рис. 4. Спеціалізований інформаційний сервер

При ініціалізації на початку роботи інформаційний сервер працює в режимі стандартного сервера сертифікації. Для кожного об'єкта, інформація про який має зберігатись в системі, створюється стандартний сертифікат. Він містить мінімальний набір даних про об'єкт. Причому ці дані є несекретними, тобто доступними в звичайному режимі функціонування сервера як центра сертифікації.

Для введення нових даних, доступ до яких має бути обмеженим, використовується редактор розширень, побудований як система візуального проектування. Редактор генерує модель розширення цифрового сертифіката. Модель розширення містить: назву розширення, перелік нових даних, спосіб подання цих даних, правила їх обробки, статус цих даних та службову інформацію.

На основі отриманої моделі розробленими засобами трансляції генерується програма створення структури нового розширення в базі даних цифрових сертифікатів. Вона передається на виконання СКБД цифрових сертифікатів. Результатом роботи програми є певні об’єкти бази даних цифрових сертифікатів, за допомогою яких забезпечується зберігання нового розширення в базі даних. Окрім того, інформації призначається певний рівень конфіденційності.

Окрім того, спеціалізованими трансляторами створюються два додаткові програмних модулі. Перший модуль – InputData – стає частиною засобів адміністрування сервера. За його допомогою вводиться закрита інформація, що пов’язана з певним об’єктом і має структуру нового розширення. Другий модуль – AccessData – це спеціалізований клієнт для доступу до захищеної інформації.

Отже, спеціалізований інформаційний сервер може працювати у двох режимах. Перший – це режим сервера сертифікації. В цьому випадку на запит на сертифікат певного суб’єкта видається стандартний сертифікат.

Коли приходить запит на якусь інформацію від клієнта AccessData, сервер починає працювати в іншому режимі. У запиті міститься сертифікат автора і вказується суб’єкт та тип потрібної інформації. Центр сертифікації перевіряє дійсність поданого сертифіката автора запиту та відповідність прав доступу запитувача рівню захисту потрібної інформації. Якщо перевірка завершується успішно, з бази даних зчитується базовий сертифікат суб’єкта. В нього у вигляді розширень вводиться потрібна інформація. Після того сертифікат підписується та по захищеному каналу відправляється автору запиту. Клієнт AccessData відображає отриману від сервера цифрових сертифікатів інформацію.

Отже, сервер цифрових сертифікатів, крім своєї основної функції – надійної ідентифікації об’єктів, виконує функцію захищеного сервера інформації про даний об’єкт. Даний підхід дозволяє значно зменшити час відклику і збільшити надійність системи збереження захищеної інформації за рахунок вбудованої ідентифікації. Уся конфіденційна інформація про об’єкт може зберігатись централізовано, що пропорційно зменшує вартість зберігання інформації і вартість експлуатації системи зберігання конфіденційної інформації.

Розглянутий підхід може використовуватись у системах цифрового підпису, електронного посвідчення особи, інформації про підприємства, у розподілених вимірювальних системах, дозвільних системах, а також всюди, де необхідна ідентифікація джерела інформації та/або отримувача інформації.

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – Спб., 2000. – 320 с. 2. Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January 1999. 3. ITU-T Recommendation X.509 : Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, January 2001.