УДК 681.3.06

І.Д. ГОРБЕНКО, П.О. КРАВЧЕНКО

Харківський національний університет радіоелектроніки, Україна

КОМБІНОВАНА ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ ТА ЇЇ ЗАСТОСУВАННЯ

Проведений аналіз вимог до комбінованих інфраструктур відкритих ключів (ІВК), що поєднують у собі як традиційну ІВК, так і ІВК на ідентифікаторах. Висунуті безумовні та умовні критерії, що будуть застосовані для порівняння існуючих розробок у цій галузі. Запропонована схема комбінованої інфраструктури дозволяє налагодити взаємодію між користувачами з сертифікатами та користувачами інфраструктури на ідентифікаторах, причому взаємодія можлива не тільки у межах інформаційної системи. Порівняльний аналіз запропонованої комбінованої інфраструктури з іншими рішеннями дозволяє зробити висновок про її найбільшу відповідність висунутим критеріям.

Ключові слова: *інфраструктура відкритих ключів, ідентифікатор, таємний ключ, уповноважений на генерацію ключів.*

Вступ

Дослідження інфраструктур відкритих ключів показує, що для вирішення проблем, пов'язаних з високою вартістю та складністю їх застосування, необхідно використовувати інноваційні підходи. Звичайна оптимізація не призводить до суттєвого підвищення ефективності, тому що витрати на апаратну частину, обслуговуючий персонал та інші статті перевищують прибуток від послуг надання сертифікатів [1].

Використання інфраструктури відкритих ключів на базі ідентифікаторів дозволяє вирішити певні протиріччя [7], але існують деякі проблеми, що не дозволяють використовувати цю інфраструктуру у глобальному масштабі. У роботі [4] був розглянутий підхід, що намагається вирішити проблемні питання інфраструктур відкритих ключів за допомогою застосування комбінованих інфраструктур. Були розглянуті декілька схем, що ставлять за мету об'єднати переваги традиційної інфраструктури та інфраструктури на ідентифікаторах.

Але, як було показано у [4], реальні переваги цих комбінованих схем занадто малі (а іноді їх зовсім немає), тому необхідно продовжувати дослідження цієї сфери.

Метою нашого дослідження є розробка та аналіз такої комбінованої схеми, яка б задовольнила хоча б частині вимог, що будуть наведені нижче. Тобто необхідно побудувати таку інфраструктуру відкритих ключів, яка б володіла високою ефективністю та низькою вартістю впровадження, була б психологічно прийнятною для користувачів та могла бути інтегрована у існуючу традиційну ІВК.

Аналіз переваг традиційної інфраструктури відкритих ключів та інфраструктури на іденитфікаторах показує, що традиційна ІВК ефективна для використання на рівні держави та організацій, а ІВК на ідентифікаторах – на рівні локальних мереж організацій, тобто на рівні кінцевих користувачів.

1. Розробка комбінованої архітектури

Зважаючи на особливості розглянутих інфраструктур відкритих ключів, ми робимо спробу побудувати таку схему взаємодії, яка б володіла перевагами обох інфраструктур. Ця схема повинна відповідати деяким безумовним та умовним критеріям, за якими можна буде порівнювати її ефективність та вартість.

До безумовних критеріїв віднесемо:

1. Програмно-апаратний рівень гарантій, що надаються ІВК;
2. Безпечність протоколів;
3. Уніфікація протоколів;
4. Криптоживучість.

Сформулюємо умовні критерії до комбінованої інфраструктури відкритих ключів:

1. Ступінь довіри користувачів традиційної ІВК до уповноваженого на генерацію ключів (УГК);
2. Необхідність обов’язкового використання сертифікатів для усіх користувачів системи;
3. Наявність механізмів взаємодії користувачів традиційної ІВК та ІВК на ідентифікаторах;
4. Стан впровадження.

Сутність схеми дуже проста — до уведеної в дію традиційної ІВК на рівні організацій буде застосовуватися ІВК на ідентифікаторах. Таким чином, буду-

ється ще один рівень захищеної взаємодії – рівень кінцевих користувачів. Він поєднується з існуючою ІВК за допомогою шлюзів, які перетворюють повідомлення, зашифроване за допомогою ІВК на ідентифікаторах у повідомлення традиційної ІВК.

Тобто, як і раніше, організація володіє декількома сертифікатами відкритих ключів (найчастіше сертифікат директора, головного бухгалтера та печатки). За допомогою цих сертифікатів здійснюється взаємодія між різними організаціями – податковою, пенсійним фондом та ін.

У рамках запропонованої схеми у локальній мережі організації розгортається інфраструктура на ідентифікаторах, яка буде використовуватися для захищеного документообігу як усередині організації, так і поза її межами (рис. 1).

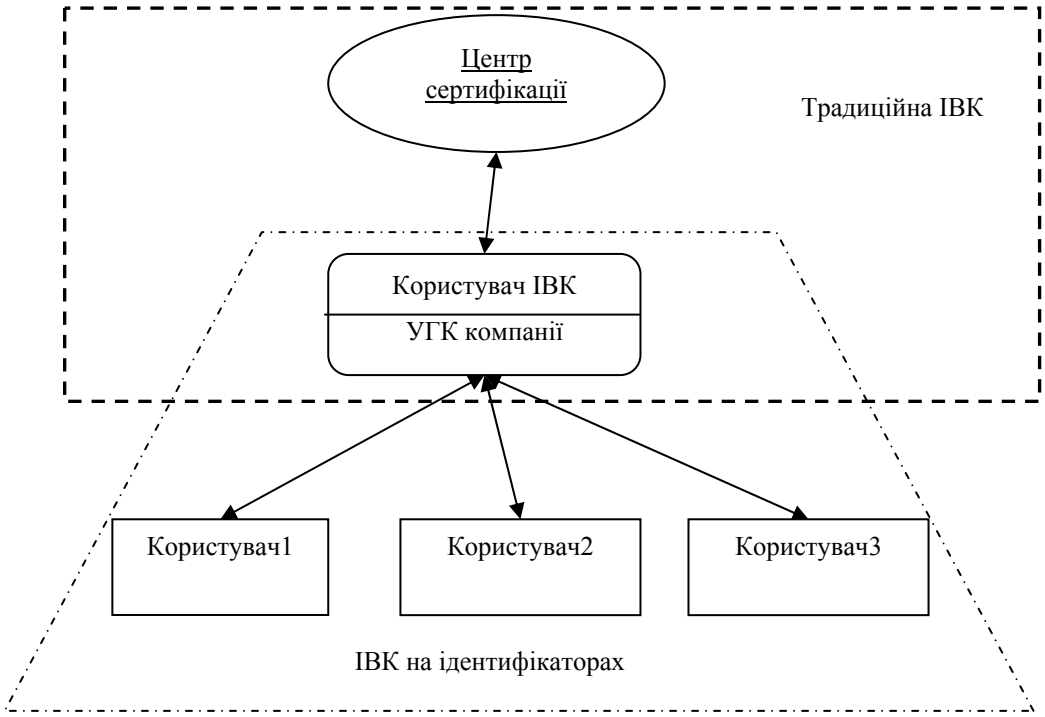

Рис. 1. Загальна схема запропонованої архітектури

2. Схема комбінованої архітектури та протокол взаємодії користувачів

До цього моменту схема нічим не відрізняється від звичайної агрегації обох інфраструктур. Тому тепер ми розглянемо, як за її допомогою можна налагодити взаємодію між кінцевими користувачами різних організацій, які використовують ІВК на ідентифікаторах.

Розглянемо приклад. Нехай користувач Аліса працює у компанії „Альфа”, користувач Боб – у компанії „Бета”. Припустимо, що ці організації є суб'єктами традиційної ІВК, а на рівні їх локальних мереж використовується ІВК на ідентифікаторах, тобто у кожній існує уповноважений на генерацію ключів, який генерує таємні ключі для кожного користувача та опубліковує відкриті загальні параметри системи. Процес взаємодії між кінцевими користувачами організацій буде складатися з виконання наступного протоколу:

1. Користувач Аліса направлено зашифровує повідомлення M, вважаючи, що одержувач Боб належить тій же компанії, що і він сам (тобто використовуючи відкриті параметри своєї системи).

2. Аліса відправляє зашифроване повідомлення на сервер своєї компанії.

3. Сервер розшифровує його (тому що він володіє майстер-ключем і може розшифровувати усі повідомлення, що були зашифровані з використанням його відкритого ключа та загальних параметрів).

4. Сервер зашифровує направлено повідомлення M на відкритому ключі компанії „Бета” (цей ключ він отримує з сертифікату, доступ до сертифікату здійснюється шляхом запиту до відкритого каталогу сертифікатів засвідчувального органу, який сертифікував відкритий ключ компанії „Бета”).

5. Сервер компанії „Бета” розшифровує повідомлення M, та знову зашифровує його, але вже на відкритому ключі користувача B (використовуючи вже власні загальні параметри) та надсилає його Бобу.

6. Користувач Боб розшифровує повідомлення за допомогою свого таємного ключа.

Цей протокол схематично зображений на рис. 1.

Схему взаємодії можна трохи спростити, якщо припустити, що УГК компанії „Альфа” має доступ до цілісних та справжніх відкритих параметрів компанії „Бета”. В такому випадку УГК компанії „Альфа” відразу направлено зашифрує повідомлення М на відкритому ключі Боба (рис. 2). Також, якщо кінцевий адресат володіє власним сертифікатом, УГК компанії «Альфа» може безпосередньо зашифрувати повідомлення на його відкритому ключі.

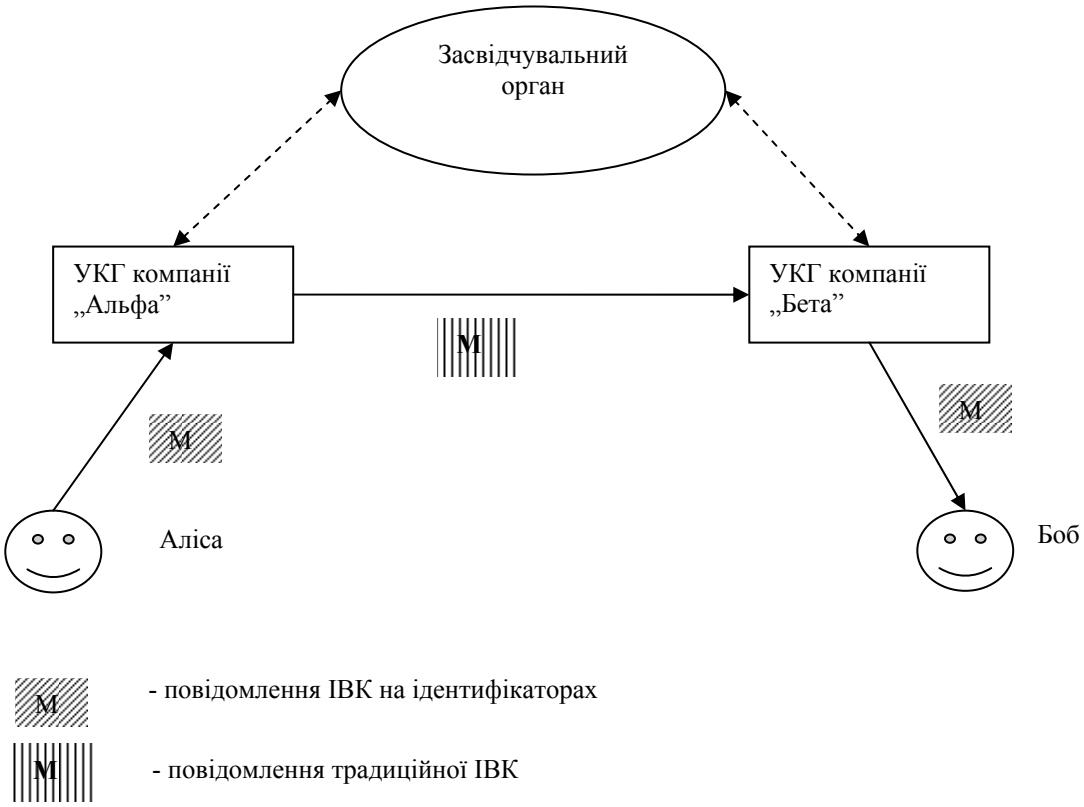

Рис. 2. Схема запропонованої архітектури

Цей різновид основної схеми демонструє роботу традиційної ІВК та ІВК разом.

Взагалі, відмітимо, що така модель взаємодії дозволить побудувати досить велику систему, використовуючи обидві інфраструктури.

Проаналізуємо переваги та недоліки розробленої моделі взаємодії.

До переваг можна віднести наступні особливості:

1. Можливість побудови досить великої інфраструктури з використанням принципів ІВК на ідентифікаторах;

2. Немає необхідності у використанні сертифікатів для кожного користувача.

3. Прозорість для кінцевих користувачів у процесі захищеного документообігу.

4. Захищеність даних в процесі передачі в каналах Інтернет (за рахунок використання сертифікатів).

5. Можливість підключення додаткових сервісів (антивірус, антиспам тощо).

6. Можливість контролю кореспонденції з боку керівництва (якщо є потреба).

7. Система може працювати і в тому випадку, якщо одна з компаній не користується ІВК на ідентифікаторах.

Тобто, можна говорити, що усі кінцеві користувачі фактично користуються інфраструктурою на ідентифікаторах (і їм доступні усі її переваги). Причому взаємодія користувачів з різних організацій, що мають різні загальні параметри буде такою ж прозорою, як і у межах тільки своєї організації. Механізми традиційної ІВК будуть використовуватися для підпису звітності, цифрових печаток та захисту документообігу між компаніями, співробітники яких використовують ІВК на ідентифікаторах.

Щодо недоліків, можна зазначити наступні:

1. Порівняно з традиційною схемою збільшено навантаження на центральний сервер компанії (йому необхідно виконувати шифрування/розшифрування для кожного електронного листа).

2. У схемі є дві критичні точки – сервери компаній, на яких повідомлення M з'являється у відкритому вигляді. Атака на будь-який з цих серверів виведе з ладу усю систему.

Користувачі можуть працювати тільки з серверами їхніх компаній, тобто вони повинні надсилати електронні листи лише на ці сервери. Крім того, ця система використовується лише для ділового листування (тобто користувач повинен довіряти УГК своєї компанії).

3. Порівняння комбінованих ІВК

Проведемо порівняння описаних архітектурних рішень за критеріями, що були визначені вище.

Порівняння будемо проводити за умовними критеріями, тому що безумовним критеріям відповідають усі рішення (якщо вважати, що розробники відповідних систем використовують надійні протоколи)(табл. 1).

Таблиця 1

Порівняння архітектурних рішень ІВК за умовними критеріями

Критерій\Інфраструктура	Запропонована схема	Система Voltage	Схема Джо Калласа	ІВК на ідентифікаторах
Ступінь довіри до УГК користувачів традиційної ІВК	не потрібна	повна	повна	–
Необхідність використання сертифікатів	–	+	– (але необхідно підписувати відкриті ключі)	–
Можливість взаємодії користувачів різних інфраструктур	+	+	–	–
Стан впровадження	–	+	–	–

З таблиці видно, що запропонована схема найбільш повно відповідає висунутим критеріям ніж усі інші. Комбіновані схеми, які пропонуються компанією Voltage [6] та Дж. Калласом [5], потребують процедури сертифікації (або підпису) відкритих ключів, що не може бути прийнятно для повноцінних ІВЕ схем.

Висновки

Запропонована схема комбінації традиційної та ІВК на ідентифікаторах, на наш погляд, володіє перевагами обох архітектур і може бути застосована при побудові реальних систем.

Щодо критеріїв, які були висунуті до комбінованих схем, ця схема задовольняє усім безумовним критеріям, та більшості умовних, за виключенням стану впровадження.

Але потрібно зазначити, що для прийняття кінцевого рішення щодо впровадження системи, що буде базуватися на даній схемі, необхідно проаналізувати недоліки цієї моделі, та встановити їх важливість у конкретному випадку. Наприклад, якщо сервер генерації досить потужний, захищений від фізичних та мережевих атак, перші два недоліки є несуттєвими.

Література

1. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах / І.Д. Горбенко, Т.О. Гріненко. – Х., 2004. – 222 с.

2. Билинейное спаривание эллиптических кривых и его теоретические основы. / И.Д. Горбенко, А.П. Мелецкий, К.А. Погребняк, Д.В. Шевченко // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 3-12.

3. Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів./ М.Ф. Бондаренко, І.Д. Горбенко, О.П. Мелецький, П.О. Кравченко // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 3. – С. 356-362.

4. Горбенко І.Д. Аналіз існуючих досліджень в галузі побудови комбінованої ІВК. / І.Д. Горбенко, П.О. Кравченко // Прикладная радиоэлектроника. – 2008. – Т. 7. – №3. – С. 267-270.

5. Callas Jon. Identity-Based Encryption with Conventional Public-Key Infrastructure. / Jon Callas. – PGP Corporation, USA. – 2005

6 . Voltage Security. Identity-Based Encryption and PKI Making Security Work [Электронный ресурс]. – Режим доступа к ресурсу: http://www.itsecurity.com/whitepaper/whitepaper-identity-based-encryption.

7. Menezes A. An Introdution to Pairing-based Cryptography / A. Menezes // Recent Trends in Cryptography. – AMS-RSME, 2009. – Vol. 477. – P. 47-65.

Поступила в редакцию 3.02.2009

Рецензент: д-р техн. наук, проф. кафедри БІТ О.В. Потій, Харківський національний університет радіоелектроніки, Україна.

КОМБИНИРОВАННАЯ ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ И ЕЕ ПРИМЕНЕНИЕ

И.Д. Горбенко, П.А. Кравченко

Проведен анализ требований к комбинированным инфраструктурам открытых ключей (ИВК), соединяющим в себе как традиционную ИВК, так и ИВК на идентификаторах. Предложены безусловные и условные критерии, которые будут применяться для сравнения существующих разработок в этой области. Предложенная схема комбинированной инфраструктуры позволяет наладить взаимодействие между пользователями с сертификатами и пользователями ИВК на идентификаторах, причем взаимодействие возможно не только в рамках информационной системы. Сравнительный анализ предложенной комбинированной ИВК с другими разработками позволяет сделать вывод про ее наибольшее соответствие выдвинутым критериям.

Ключевые слова: инфраструктура открытых ключей, идентификатор, секретный ключ, уполномоченный на генерацию ключей.

COMBINED PUBLIC KEY INFRASTRUCTURE AND IT'S USE

I.D. Gorbenko, P.O. Kravchenko

We have made the analysis of requirements of the combined public key infrastructures, that combines public key infrastructures, to combine traditional public key infrastructure and identity-based infrastructure. We suggest absolute and conditional criteria which will be used for comparison of existing developments in this area. Our scheme allows establishing the cooperation of public key infrastructure users and identity-based infrastructure users, moreover it is possible in global informational system. Comparative analysis of our scheme makes a conclusion about its compliance with the requirements.

Keywords: public key infrastructure, identity, private key, public key generator.

Горбенко Іван Дмитрович – доктор технічних наук, професор, завідуючий кафедрою БІТ, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: gorbenko@kture.kharkov.ua.

Кравченко Павло Олександрович – аспірант кафедри БІТ, Харківський національний університет радіоелектроніки, Харків, Україна.