УДК 004.414.22:004.056:004.413.4

Сергій Валентинович Бєлов, Сергій Васильович Мартиненко

АРХІТЕКТУРА ЗАГАЛЬНОЄВРОПЕЙСЬКОЇ СТРУКТУРИ PKI. АКТУАЛЬНІ ПИТАННЯ ПОБУДОВИ BGCA В УКРАЇНІ

Анотація: Розглядається актуальне питання побудови національної інфраструктури електронного підпису з використанням моделі державного шлюзового центру сертифікації (**BGCA)**. Сформульовані функції та загальні вимоги до шлюзового центру сертифікації, використання списків довір'я, вимоги до використання стандартів та висвітлені деякі проблеми сумісності.

З розвитком програми електронного уряду в країнах Європейського співтовариства (ЄС) органи державного управління ЄС все ширше використовують електронні сертифікати для безпеки комунікацій, шифрування та електронного підпису, в тому числі в міждержавних відносинах в межах ЄС. Виникла необхідність встановлення відносини довір'я між центрами сертифікації ключів (ЦСК або англ. CA), які використовуються національними органами державного управління. Це необхідно для того, щоб державні службовці держав ЄС могли використовувати електронні сертифікати, випущені їх національними ЦСК, в зальноєвропейській (pan-European) державній мережі.

В зв'язку з цим виникають такі задачі:

1. Встановлення системи взаємного довір'я між ЦСК європейських державних органів.
2. Встановлення системи взаємного довір'я між ЦСК європейських недержавних органів. Це надасть можливість підприємствам і громадянам, які володіють електронними сертифікатами, випущеними національними ЦСК (державними та недержавними), взаємодіяти в межах ЄС як між собою, так і з державними органами та в електронній комерції ЄС.

Аналогічні задачі виникають і при побудові національної системи ЦСК в Україні, яка має поєднувати в собі функції обслуговування громадян та організацій України та забезпечувати можливість їх взаємодії з громадянами та організаціями ЄС. В ці завдання входить також і забезпечення взаємодії державних органів України з офіційними органами та недержавними організаціями держав ЄС. Тому дуже важливо вивчити досвід інших держав та запроваджувати в Україні найбільш перспективні моделі побудови національної інфраструктури електронного підпису.

Традиційна модель інфраструктури з відкритими ключами (PKI – Public Key Infrastructure) дозволяє вирішити питання щодо встановлення відносини довір'я між ЦСК через механізм «крос-сертифікації» («cross-certification»). Такий механізм - це «*Bridge CA*» або «*Gateway CA*» (Шлюзовий ЦСК), який

використовується, зокрема, в США, Канаді, ЄС [1]÷[4] та інш. для побудови Національних PKI. В ЄС ініціатива "European Bridge-CA" була ініційована Дойче банком (Deutsche Bank) та Дойче Телекомом (Deutsche Telekom).

Державний Шлюзовий ЦСК, «Bridge CA» (BGCA – Bridge Government Certificate Authority), призначений забезпечити такий ступінь довір'я, який необхідний для використання електронних сертифікатів як на національному, так і на європейському рівні.

Відповідна робоча програма ЄС щодо створення «Bridge CA» (BCA) на рівні ЄС була розпочата на запит Членів Співтовариства в 2001 році. Базою для програми «Bridge CA» був проект PKI для замкнутих груп (PKICUG - Public Key Infrastructure for Closed User Groups) користувачів ЄС [4]-[6], який був розпочатий в січні 1999, як частина програми Обміну Даними між Урядами (IDA - Interchange of Data between Administrations), що призначена для розвитку та виконання між урядами країн ЄС електронного обміну даними через транс-європейські мережі.

Використовуючи напрацьований досвід ЄС, розглянемо актуальні питання побудови BGCA в Україні. Для реалізації проекту необхідно розглянути відповідну політику, організаційні та технічні проблеми, а саме:

- еквівалентність політик сертифікатів;
- забезпечення зразкової технічної архітектури BGCA;
- створення та управління BGCA;
- вимоги щодо сумісності.

Основою державної інфраструктури PKI, якщо визначити в термінах ЄС, є PKI для *замкнутих груп користувачів* (CUG) [1]. Тобто створення окремих підсистем PKI для груп користувачів, якими є, наприклад, працівники підприємства (організації, відомства) або клієнти. Переваги створення CUG - більш прості та більш гнучкі процедури управління сертифікатами, чітко окреслена група користувачів, для яких ці процедури придатні. Створення CUG означає, що суворі вимоги, які висуваються до державних Центрів Реєстрації, можуть ослаблятися за потребами CUG, щоб уникнути пересторог користувачів через надмірні та невідповідні процедури. Архітектура PKI для CUG [2] – це однорангові структури/моделі PKI (Peer PKI) та ієрархічні структури/моделі PKI (Hierarchic PKI).

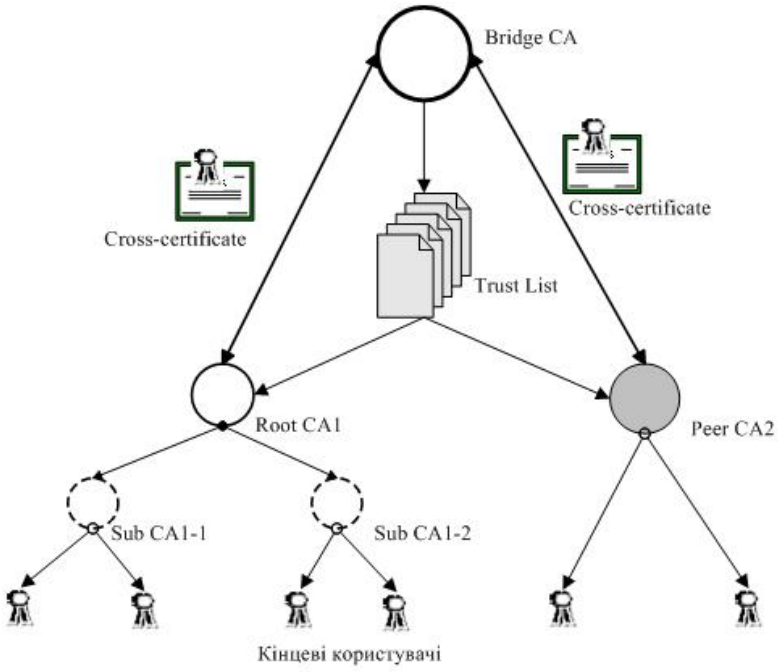
Шлюзова модель BCA PKI (Bridge CA PKI) складається з поєднання так званої Web/Internet довірчої моделі (Web/Internet Trust Model) та Шлюзової моделі (Bridge/Gateway Model). У термінах UML (Unified Modelling Language), яка є визнаним засобом при розробці програмних проектів, «Акторами» (*Actors)* в межах цієї моделі є :

- Шлюзовий ЦСК (Bridge/Gateway CA);
- окрема інфраструктура PKI сектору CUG.

У цій моделі Шлюзовий ЦСК виконує дві ролі :

- кросс-сертифікація з іншими ЦСК замкнутих груп CUG;
- випуск «Списків Довіри» (Trust Lists) для різних груп та/або різних секторів.

Будь-яка окрема інфраструктура PKI в межах об'єднання в шлюзову модель BCA PKI має можливість завантажити Список Довіри, випущений Шлюзовим ЦСК або завантажити кросс-сертифікати для того, щоб дозволити відносини довір'я з іншою PKI інфраструктурою, яка є членом BCA PKI (мал.1). Позначення на мал.1: «Peer CA» - ізольований ЦСК однорангової структури; «Root CA1» - кореневий ЦСК ієрархічної структури; «Sub CA1-1» - перший підпорядкований ЦСК ієрархічної структури з коренем Root CA1 і т.ін.



Мал.1. BCA PKI модель

Загальні вимоги до Шлюзового ЦСК (BCA)

Шлюзовий ЦСК(BCA) повинен забезпечити:

- випуск перехресних кросс-сертифікатів, обмін і оновлення належним чином сертифікатів з «Головним ЦСК» («Principal CA») кожного члену PKI;
- регулярне розсилання сертифікатів *Списків довіри* (CTL - Certificates Trust Lists) членам PKI;

- ведення служби каталогу (репозиторію) випущених BCA сертифікатів кожному члену PKI, а також відповідні Списки анулювання сертифікатів (CRL - Certificate Revocation Lists); які потрібно регулярно оновлювати;
- підтримання веб-вузла, що публікує CTL, CRL, MoU (Меморандум про згоду - Memorandum of Understanding) та документи щодо політик CP (Certificate Policy);
- (необов'язково) on-line відповіді щодо статусу сертифікату через OCSP (Online Certificate Status Protocol).

Крім того, державний орган повинен опублікувати для членів PKI:

- технічні інтерфейси взаємодії з державним шлюзом BGCA;
- базові основи тестування інтерфейсу з вузлом BGCA, призначенні для нових претендентів на підключення.

Використання Списків довіри

Кожен користувач навігатора операційної системи має локальний файл «кореневих довірчих» (Trust Root) сертифікатів. Зазначений файл називають «*Списки довіри*». Навігатори звичайно поставляються з початковим набором кореневих сертифікатів від виробника/постачальника системи. Контроль за цим файлом може здійснюватись користувачем індивідуально, або організації можуть централізовано поставляти їх для завантаження чи здійснювати управління цим файлом централізовано через мережу управління.

Термін «використання Списку довіри» означає:

- розповсюдження в межах моделі BCA Списків довіри Головним ЦСК (Принципалам) груп CUG, які є членами цієї інфраструктури;
- використання Списку довіри прикладними програмами (додатками) клієнтів або серверів для того, щоб визначати легітимність електронних операцій (затвердження операцій або відмова в затвердженні). Таким чином, вимагається інтеграція в межах додатків, які фактично відповідальні за затвердження електронної операції.

Термін «*Інтерфейс списку довіри*» використовується для описання інтерфейсу між Списком Довіри, що розповсюджується («*Список довіри розповсюдження*» - Distribution Trust List), який завірений BCA та призначений для загального вжитку в домені, та «*Списком довіри локального зберігання*» (Local Storage Trust List), який використовуються локальними додатками членів BCA для затвердження операцій. Отже може використовуватись два формати – для списків, які розповсюджуються та для списків, які локально зберігаються.

Можна умовно виділити дві моделі інтеграції Списків довіри з додатками, що використовуються для затвердження операцій:

1. Список довіри використовується виключно для розповсюдження **і**нформації про довір'я для окремої організації-учасника ВСА. Структура (формат) локального зберігання цього Списку довіри відмінна від структури Списку довіри, який розповсюджується відповідним ВСА. У цьому випадку структура зберігання «*Списку довіри локального зберігання*» повинна відповідати правилам електронного додатку або серверу, який затверджує операції.

Розповсюдження може здійснюватися вручну або автоматично. В обох випадках необхідна повторна структуризація всіх даних, які знаходяться в Списку довіри. Таким чином, «*Інтерфейс списку довіри*» повинен визначати механізм транспортування Списку довіри, а також перетворення від «*Списку довіри розповсюдження*» до «*Списку довіри локального зберігання*».

2. Формат Списку довіри використовується як стандарт локального зберігання для усіх учасників ВСА. Таким чином, «*Інтерфейс списку довіри*» у цьому випадку повинен визначати тільки механізм транспортування Списку довіри. Всі додатки клієнтів використовують в даному випадку одні й ті ж стандарти формату Списку довіри.

Головні недоліки першої моделі інтеграції Списків довіри з додатками затвердження операцій:

- Якщо місцеві (локальні) стандарти «*Списку довіри локального зберігання*» не пов'язані з деяким мінімальним рівнем вимог, то не вся інформація, що присутня в «*Списках довіри розповсюдження*», може зберігатися в «*Списку довіри локального зберігання*» і це зменшує рівень безпеки.
- У випадку використання ручного процесу розповсюдження (наприклад, завантаження оператором/адміністратором з веб-вузла), збільшується ризик помилок. Також треба додати сюди необхідність перетворення формату (перекодування) інформації, що ще збільшує ризик помилок.
- Необхідно визначити та підтримувати окремий «*Інтерфейс списку довіри*» між стандартом «*Списку довіри розповсюдження*» та іншим стандартом «*Списку довіри локального зберігання*». Тестування та виконання змін програмного забезпечення значно ускладнюється.
- Формальна акредитація програмного забезпечення затвердження операції буде більш складною, тому що мають місце різні стандарти Списків довіри.
- Неможливість використовувати стандартне програмне забезпечення чи спеціалізовані додатки, які підтримують єдиний стандарт «*Списку довіри локального зберігання*».

Таким чином, для мінімізації ризику безпеки та ризику помилок, необхідно обмежити використання місцевих/відомчих форматів «*Списку довіри локального зберігання*». Отже, необхідно затвердити (прийняти) та

використовувати стандарти, єдині для усіх сторін – розробників PKI та додатків, урядових органів та неурядових підприємств і організацій тощо.

Вимоги до використання стандартів

З метою досягнення сумісності в контексті послуг електронного уряду (eGovernment) між державами ЄС, необхідно особливо зосередитися на *відкритих стандартах*. Стандарти, для того щоб вважатися *відкритими стандартами*, повинні задовольняти таким мінімальним вимогам [7]:

- Стандарт повинен бути прийнятий та підтримуватися некомерційною організацією, а його розробка повинна здійснюватися на основі відкритої процедури ухвалення та доступності для зацікавлених сторін (консенсус або рішення більшості тощо).
- Стандарт повинен бути повністю опублікованим і ця публікація повинна бути вільно доступною, або за номінальну оплату. Повинно бути дозволено повне копіювання стандарту, розповсюдження та використання без будь-якого грошового збору або в мінімальному грошовому зборі.
- Інтелектуальна власність (тобто можлива наявність патенту щодо стандарту, або його частини) – остаточно робиться на без-гонорарній (royalty-free) основі при розповсюдженні/тиражуванні.
- Немає ніяких обмежень на повторне використання стандарту.

Таким чином, розробляючи проект реалізації Національного Шлюзового ЦСК (BCA PKI), треба врахувати ці вимоги ЄС щодо *відкритості стандартів*.

Наведемо мінімальні вимоги ЄС щодо стандартів і специфікацій для BCA [4]:

- Послуги (сертифікації та CRL) BCA PKI повинні відповідати стандартам IETF PKIX і специфікаціям (специфікації - [8]÷[10]).
- Служби каталогу домену BCA повинні бути як мінімум X.500 сумісні та підтримувати LDAP запити.
- CRL та CTL формати повинні бути визначені експертною групою безпеки BCA.
- Вимоги щодо послуги запиту статусу сертифікату через OCSP не пред’являються. Члени ЄС можуть це робити, так як прийнято на їх місцевому рівні.
- Не надається ніяких рекомендацій щодо веб-вузла BCA.
- Обов’язковим є дотримання стандартів ETSI щодо центрів сертифікації ключів, які випускають «прості» сертифікати відкритих ключів [11] та кваліфіковані сертифікати [12].

Деякі проблеми сумісності

Проблеми сумісності стосуються BCA стандартів. Розглянемо особливі питання, від яких залежить безпека BCA.

1. Основним фактором безпеки будь-якої PKI є політика сертифікатів (CP). Одним із перших кроків розробки PKI повинно бути формування CP. Документ CP повинен відповідати [13].

2. Політика CP повинна бути офіційно зареєстрована та мати Ідентифікатор Об'єкту (OID) ([14]).

3. Стандарт CTL, що використовується сьогодні, - це стандарт специфікації Microsoft. Він використовує стандарт PKCS #7 [15]-[17] як стандарт формату файлу для передачі Списку довіри («*Списки довіри розповсюдження*»). Стандарт CTL не пов'язаний із якимсь специфічним додатком Microsoft і придатний для використання у всіх додатках Microsoft, які використовують PKI. До того ж, використання CTL в додатках Microsoft не зв'язується обов'язково з постачальником CTL тільки від цієї фірми. Завдяки тому, що формат файлу передачі CTL стандартизований за PKCS #7 та підтримується майже всіма розробниками програмного забезпечення, інтерфейси його використання в додатках інших виробників не є складними в реалізації. Той факт, що CTL є поки що виключно стандартом Microsoft може бути «політичною» проблемою щодо повної згоди з цією специфікацією інших продавців програмного забезпечення.

Висновки та пропозиції:

1. Вважаємо, що при побудові Національної інфраструктури ЕЦП (PKI) базовою архітектурою має бути Шлюзова модель. Порівняння вимог ЄС та законодавства України в галузі застосування інфраструктури ЕЦП приводить до висновку, що Центральний засвідчувальний орган (ЦЗО) за Законом «Про ЕЦП» має бути створений саме за цією моделлю, як Шлюзовий ЦСК, та відповідати вимогами до технології «Bridge CA» програми ЄС. Головним завданням ЦЗО має бути виконання кросс-сертифікації між іншими Головними ЦСК в Україні та за її межами, формування та підтримка Списків довіри за правилами постійної доступності та граничної достовірності.
2. Відповідно до завдань національної системи ЦСК мають бути обов'язково офіційно підтримані діючі відкриті Європейські стандарти щодо створення та використання інфраструктури ЕЦП, гармонізовані технічні вимоги щодо застосування криптографічних модулів, політик безпеки додатків, застосувань, форматів та інших елементів технічної інфраструктури в рамках інформаційної політики для програми «Електронного Уряду». Розроблені ЄС мінімальні вимоги до BCA мають бути обов'язково визнані та застосовані і в Україні. Національний ЦЗО має керуватись визнаними мінімально необхідними правилами і стандартами щодо побудови та обслуговування учасників національної системи, підтримки їх взаємодії з зовнішніми абонентами.
3. Для застосування вказаних моделей, стандартів, врахування мінімальних вимог щодо використання стандартів та необхідних послуг національного «Bridge CA» необхідно провести аналіз щодо внесення необхідних змін в

законодавчі акти України.

4. Особливу увагу при розробці нормативних документів слід звернути на Політику сертифікатів, яка є базовою в питаннях безпеки інформації. Документ щодо Політики сертифікатів є одним з головних та одним з перших при розробці нормативної бази національної інфраструктури ЕЦП.

Література

1. William T. Polk and Nelson E. Hastings. National Institute of Standards and Technology. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures.
2. David Drucker, Test Show PKI Promise: 'Bridge' architecture links certificates from multiple vendors, Internet Week, April 17, 2000.
3. X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA). - National Institute of Standards and Technology, September 10, 2002.
4. IDA PKICUG. Public Key Infrastructure for Closed User Groups. A bridge CA for Europe's Public Administrations Feasibility study. - European Commission, Enterprise General, Final report, July 2002.
5. IDA PKICUG. Public Key Infrastructure for Closed User Groups. Description of Current Architecture and Operations. – IDA, April 2001.
6. PKICUG, Public Key Infrastructure for Closed User Groups. - ATA proposal, Ref. DCS/SXP/PRP/98/003, 1 September 1998.
7. European Interoperability Framework for pan-European eGovernment Services. - Luxembourg: Office for Official Publications of the European Communities, ISBN 92-894-8389-X, 2004.
8. RFC 2459. Certificate and CRL Profile. - January 1999.
9. RFC 2630. Cryptographic Message Syntax. - June 1999.
10. RFC 3852. Cryptographic Message Syntax (CMS) - July 2004.
11. ETSI TS 102 042 – Policy requirements for Certification Authorities issuing public key certificates, v. 1.1.1. - April 2002.
12. ETSI TS 101 456 – Policy requirements for Certification Authorities issuing qualified certificates, v. 1.2.1. - April 2002.
13. RFC 3647. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - November 2003.
14. Interoperability sub-project, final report, minimum standards and profiles for interoperability, ref. 3AT 05025 AAAA DTZZA, version 3, dated 12 November 2001.
15. PKCS #7: Cryptographic Message Syntax Standard. - RSA Laboratories, Version 1.5, Revised November 1, 1993.
16. RFC 2630: Cryptographic Message Syntax. – June 1999.
17. RFC 3852: Cryptographic Message Syntax (CMS). - July 2004.