УДК 004.414.22:004.056:004.413.4

Сергій Валентинович Бєлов, Сергій Васильович Мартиненко

Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики

Анотація: в статті розглядаються моделі побудови та питання інформаційної безпеки і ризиків національної *інфраструктури відкритих ключів* при її реалізації для електронного уряду, державних та комерційних структур та їх установ. Дослідження ризиків показує, що прийнятною є шлюзова модель національної інфраструктури центрів сертифікації з використанням механізмів крос-сертифікації.

Програму створення електронної інформаційної системи «Електронний Уряд» на державному рівні (Постанова Кабінету Міністрів України №208 від 24.02.2003 та інші) визнано одним з пріоритетних завдань щодо розвитку інформаційного суспільства України. Цією програмою визначено надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання інформаційної системи, яка забезпечує взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій. Такі технології в системі потребують ідентифікації суб'єктів правових відносин і забезпечення цілісності та достовірності інформації з використанням *електронного цифрового підпису* (далі - ЕЦП).

Законодавством України визначено правовий статус електронного цифрового підпису та електронного документу [1],[2]. Для забезпечення використання електронного підпису необхідно створення інфраструктури Центрів сертифікації ключів (далі – ЦСК). Ця інфраструктура також має загальновизнану назву **інфраструктури відкритих ключів** (Public Key Infrastructure, PKI). В Законі «Про електронний цифровий підпис» [1] та постанові Кабінету Міністрів України [2] визначено загальні функції та встановлено загальні вимоги до ЦСК, акредитованого ЦСК, центрального засвідчувального органу, засвідчувального центру органу виконавчої влади або іншого державного органу.

При побудові Національної інфраструктури центрів сертифікації ключів (далі – Національна інфраструктура ЕЦП) важливим є питання вибору варіанту її моделі, а саме моделі створення сертифікаційних шляхів між різними державними відомствами (установами, агентствами) та недержавними організаціями, в тому числі банківським сектором, таким чином, щоб забезпечити високу надійність та високий рівень довірчих відносин, інтеграцію і одночасно криптографічну самостійність/незалежність кожного з відомств/організацій.

Треба зазначити, що побудова Національної інфраструктури ЕЦП є не тільки технічним питання, а й *питанням національної безпеки*.

Крім того, необхідно створювати Національну інфраструктуру ЕЦП таким чином, щоб вже діючі системи різних форм власності, а особливо – фінансові структури, могли працювати стабільно, не зазнали великих збитків через неможливість використання електронного документообігу у своїй повсякденній діловій діяльності з клієнтами та партнерами у зв'язку з розгортанням національної системи. Звичайно, при аналізі можливих варіантів побудови Національної інфраструктури ЕЦП, слід враховувати наявність відповідних міжнародних технічних стандартів та вже діючих структур, що використовують такі системи, або компоненти таких систем. Не менш важливим є і те, що бізнес-сектор (та його користувачі-клієнти) здебільшого не мають іншої альтернативи, ніж використання інформаційних технологій, у тому числі технологій захисту інформації, розпорядниками яких є Європейські, міжнародні організації, наприклад – платіжні системи.

Для однозначності розуміння подальшого тексту наведемо визначення окремих термінів:

ЦСК-домен – об'єкти одного ЦСК, яким видано сертифікати цим ЦСК.

Модель архітектури ЕЦП (PKI) **–** модель об'єднання довірчими відносинами різних ЦСК-доменів.

Кросс-сертифікація (Cross-certification) – процес, який використовується в PKI, щоб встановити довірчі відносини. Це процес взаємної (перехресної) сертифікації двох рівноправних ЦСК доменів, яка використовується одним ЦСК, щоб сертифікувати будь-який другий ЦСК, окрім безпосередньо суміжного ЦСК (вищого рівня чи підпорядкованого). Це дозволяє держателям сертифікатів цих ЦСК доменів перевірити легальність (валідність) сертифікатів одне одного. Механізм кросс-сертифікації встановлює довірчі відносини між *рівноправними* ЦСК доменами через незалежну взаємну кросс-сертифікацію адміністраторів Основних ЦСК (тобто призначених для таких дій) в цих доменах.

Користувач сертифікату (Certificate User) - суб'єкт чи об'єкт, які перевіряють чинність цифрового підпису підписувача та низки сертифікатів. Синонімом цього терміну є «**Сторона, що довіряє**» (Relying party).

Архітектура Національної інфраструктури ЕЦП

Власники сертифікатів можуть отримати свої сертифікати в різних ЦСК (CA – Certificate Authority), в залежності від організації чи співтовариства, членами якого вони є.

Звичайно інфраструктура ЕЦП складається з багатьох ЦСК, пов'язаних довірчими шляхами. Довірчий шлях дозволяє **користувачеві сертифіката,** який перевіряє чинність цифрового підпису та низки сертифікатів, зв'язатися з однією чи більше довірених третіх осіб так, що користувач може бути впевнений в законності сертифікату при його використанні. Наприклад,

одержувач підписаного повідомлення (користувач сертифіката), який не має відносин з ЦСК, що випустив цей сертифікат для підписувала повідомлення, може перевірити чинність сертифіката підписувача, використовуючи довірчий шлях сертифікату.

Головна задача Національної інфраструктури ЕЦП – об'єднати різноманітні відомчі PKI (не державних підприємств чи державних організацій) в одну довірчу структуру, створивши довірчі шляхи сертифікації.

Для організації електронного документообігу слід враховувати **необхідність** спілкування користувачів ЦСК як державних, так (і особливо) недержавних організацій з іншими, у тому числі закордонними організаціями та громадянами, що використовують в своїй практиці міжнародні технічні стандарти та правила. Отже, необхідно врахувати наявний досвід розвинених країн, який викладений в рекомендаціях та стандартах **EuroPKI** Європейсько Співтовариства [5], Федерального PKI Національного Інституту Стандартів і Технології США [6] (Federal PKI, NIST) тощо.

Типи ЦСК

Побудова ЦСК-доменів базується на таких типах ЦСК:

- Ізольований/Одноранговий ЦСК (Isolate/Peer CA)
- Кореневий ЦСК (Root CA)
- Підпорядкований ЦСК (Subordinate CA)
- Шлюзовий ЦСК (Bridge/Gateway CA)

Це базові елементи різних моделей інфраструктури ЕЦП, які розглядаються далі.

Інфраструктура ЕЦП окремого підприємства, відомства тощо може бути однією з можливих моделей:

- Одноранговий ЦСК-домен (Peer Domain PKI);
- Ієрархічний ЦСК-домен (Hieratic Domain PKI)

Реалізації таких моделей часто утворюють Замкнуту групу, утворену в межах одного підприємства/організації та призначену для відокремленого від інших ЦСК застосування локальної інфраструктури ЕЦП.

Архітектура ЕЦП для об'єднання окремих ЦСК-доменів підприємств, відомств тощо в одну довірчу інфраструктуру може бути однією з можливих моделей:

- Ієрархічна модель (Hieratic model)
- Мережена модель (Mesh model)
- Шлюзова модель (Bridge model)

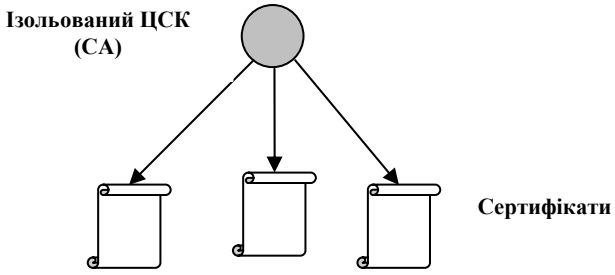
Проаналізуємо особливості таких моделей архітектури ЕЦП.

Ізольований/Одноранговий ЦСК-домен

Ізольований/Одноранговий ЦСК – це ЦСК, що має само-підписаний ЦСК-сертифікат (self-signed CA-certificate), який не завіряється (не

підписується) будь-яким іншим ЦСК вищого рівня (мал.1). Шлях сертифікації у цьому випадку дорівнює 2, тобто ЦСК-сертифікат(CA-certificate) та сертифікат клієнта цього ЦСК. Ізольований ЦСК не видає сертифікати іншим ЦСК (не має підпорядкованих ЦСК).

Тут ЦСК-домен складається тільки з Ізольованого ЦСК та Клієнтів-держателів сертифікатів, яким видано сертифікати цим ЦСК. Такий домен ще називають **Ізольованим/Одноранговим ЦСК-доменом** (Peer Domain PKI).



Мал.1. Ізольований ЦСК-домен

Приєднати Ізольований ЦСК-домен до деякої інфраструктури ЕЦП (до іншого ЦСК-домену) можна двома способами:

- Через ієрархічні відносини, як Підпорядкований ЦСК (див. нижче Ієрархічний ЦСК-домен);
- Через відносини рівноправних ЦСК (peer-to-peer кросс-сертифікацію).

В першому випадку вимагається обов'язково перевипуск (заміна) ЦСК-сертифіката, а отже повний перевипуск усіх сертифікатів держателів.

В другому випадку це не вимагається – усі сертифікати держателів залишаються чинними після приєднання Ізольованого ЦСК до деякого довірчого ЦСК-домену через механізм кросс-сертифікації.

Переваги Ізольованого ЦСК:

- мінімальна вартість та простота впровадження.

Особливо приваблива така структура для малих та середніх організацій, у яких усі клієнти ЦСК належать до однієї групи/категорії, наприклад, працівники організації.

Недоліки Ізольованого ЦСК:

- усі Клієнти ЦСК з однаковим профілем сертифікату мають однакові довірчі відносини. Це важливо, якщо необхідно мати декілька груп Клієнтів ЦСК, які повинні мати різні довірчі відносини та права. Наприклад, якщо необхідно видавати сертифікати для декількох груп, зокрема, це можуть бути працівники організації та клієнти (що має місце в банківському секторі), то з точки зору безпеки ці групи необхідно розмежовувати, що можна здійснити на рівні розмежування ЦСК (див. Ієрархічний домен ЦСК);

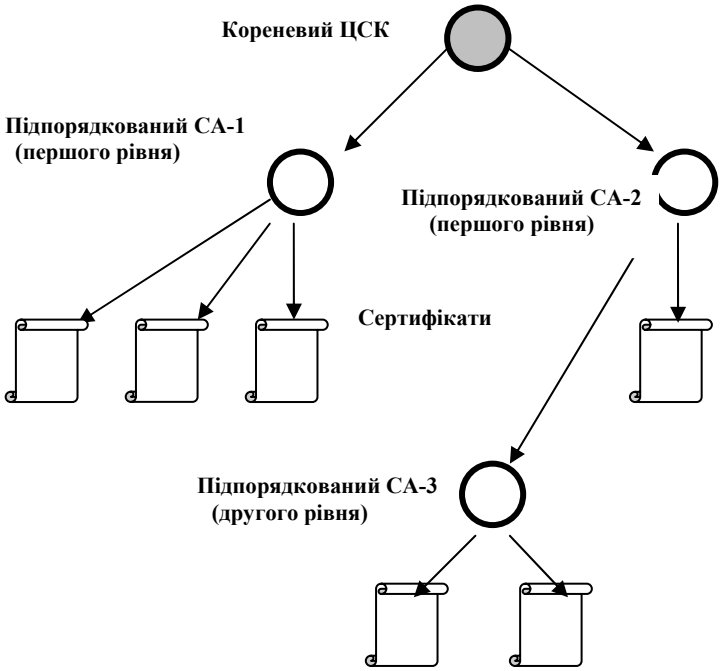
- не можна «відокремити» довірчий сертифікат, початок довірчого шляху сертифікації (ЦСК-сертифікат), який є найбільш важливим з точки зору безпеки домену, від сертифікатів інших користувачів. Усі сертифікати видаються одним ЦСК, який повинен бути постійно доступний. З точки зору безпеки само-підписанного ЦСК-сертифікату, його треба «замурувати у сейф» та зробити недоступним для будь-яких несанкціонованих дій, що для Ізольованого ЦСК забезпечити неможливо;
- компрометація ЦСК-сертифікату чи приєднання Ізольованого ЦСК до Ієрархічного домену приводить до необхідності повного перевипуску усіх сертифікатів цього ЦСК;
- деякі стандарти PKI (наприклад, стандарт банківського PKI Європейського Співтовариства Identrus) не допускають видачу сертифікатів клієнтам Ізольованими ЦСК. Цими стандартами встановлюється, що ЦСК з само-підписаним ЦСК-сертифікатом може використовуватися виключно для видачі сертифікатів Підпорядкованим ЦСК. Такий ЦСК з само-підписаним ЦСК-сертифіктом називається Кореневим ЦСК.

Ієрархічна модель

Ієрархічна модель – це об’єднання ЦСК-доменів в структуру зв’язного графа, тобто «дерева, що має одну головну вершину (Кореневий ЦСК), з якої будується структура Підпорядкованих ЦСК (мал.2).

В Ієрархічній моделі є один головний ЦСК, якому довіряють усі користувачі – це Кореневий ЦСК, тобто для усіх держателів сертифікатів ієрархічної моделі шлях сертифікації починається є одного Кореневого ЦСК. Кореневий ЦСК не випускає сертифікатів для Клієнтів, окрім виключно Підпорядкованих ЦСК.

Кожен з Підпорядкованих ЦСК може випустити сертифікат як своїм Клієнтам, так і підпорядкованому йому іншому ЦСК - **Підпорядковані ЦСК другого рівня**.



Мал.2. Ієрархічний домен ЦСК

В Ієрархічній моделі довірчі відносини визначені лише в одному напрямку – від вищого рівня до нижчого рівня ЦСК, тобто Підпорядковані ЦСК не випускають сертифікати для ЦСК вищого рівня.

Політики сертифікатів визначаються Кореневим ЦСК для усього домену, і можуть додатково визначатися (у межах, що не суперечать політиці вищого рівня ЦСК) Підпорядкованими ЦСК для своїх ЦСК-доменів (на мал.2 є три ЦСК -домени - СА-1, СА-2, СА-3).

Довірчі відносини між держателями сертифікатів різних ЦСК-доменів Підпорядкованих ЦСК будуються таким чином:

- *держатель сертифікату* ієрархічного домену сприймає сертифікат іншого держателя з цього домену, як такий, що заслуговує довір'я, тому що вони мають один «корінь» довір'я, тобто один і той же Кореневий ЦСК;

- *сервіс*, який встановлено в одному із під-доменів і який вимагає сертифікат держателя (наприклад, аутентифікація з сертифікатом по SSL-протоколу), довіряє лише держателю свого під-домену (Клієнту ЦСК цього домену). Це дозволяє розмежувати права користувачів різних під-доменів.

Наприклад, СА-1 видає сертифікати клієнтам організації (банку), а СА-2 – працівникам організації. Тоді сервіс (програма бухгалтерського обліку), який встановлено в домені СА-2, не буде довіряти сертифікатам домену СА-1, не дивлячись на те, що у обох під-доменів один корінь – Кореневий ЦСК.

Переваги Ієрархічної моделі:

- головною перевагою ієрархічної моделі є простота її початкової побудови;
- наявність Кореневого ЦСК, який видає сертифікати виключно Підпорядкованим ЦСК, тобто «працює» періодично, що дозволяє «закрити його у сейф» та забезпечити високий рівень безпеки;
- дозволяє довірчі відносини між держателями та дозволяє розмежувати повноваження (права) доступу груп користувачів до сервісів;
- дозволяє просто добавляти нові довірчі групи держателів сертифікатів шляхом підключення нового Підпорядкованого ЦСК (будь-якого нижнього рівня);
- користувачі ієрархії знають неявно, для яких прикладних додатків (програм) може використовуватися сертифікат, що базується на позиції (рівні) ЦСК в межах ієрархії.

Недоліки Ієрархічної моделі є наслідками довіри єдиній точці (вищому рівню – Кореневому ЦСК) в структурі ієрархії:

- компрометація «кореня» (ключа Кореневого ЦСК) призводить до компрометації усього Ієрархічного «дерева» та необхідності заміни (перегенерації) усіх без виключення ключів держателів, причому не віддалено, а згідно з процедурою видачі першого сертифікату (особистий контакт), що може мати фатальні наслідки для організації. Ніяких інших безпечних методів відновлення роботи домену і усіх підпорядкованих йому під-доменів не існує;
- якщо в державі буде впроваджена жорстка ієрархічна модель та на цій базі в перспективі сформований електронний документообіг, який значною мірою (чи повністю) витисніть звичайний паперовий документообіг, то *компрометація «кореня» системи ЕЦП* приведе до блокування будь-яких урядових справ (від фінансових операцій до розпорядчих документів) в Державі;
- єдиний Кореневий ЦСК може бути неможливим із «політичних» міркувань – конкуренція, міжвідомчі перепони тощо;
- перехід як від Ізольованих ЦСК, так і від інших окремих Ієрархічних доменів до єдиної Національної ієрархічної моделі інфраструктури ЕЦП є логічно непрактичним, так як усі користувачі сертифікатів вже існуючих ЦСК-доменів повинні внести зміни до їх довірчих точок (шляхів), а усі держателі сертифікатів замінити їх та відповідно ключі підпису на нові, які відповідають новій ієрархічній структурі.

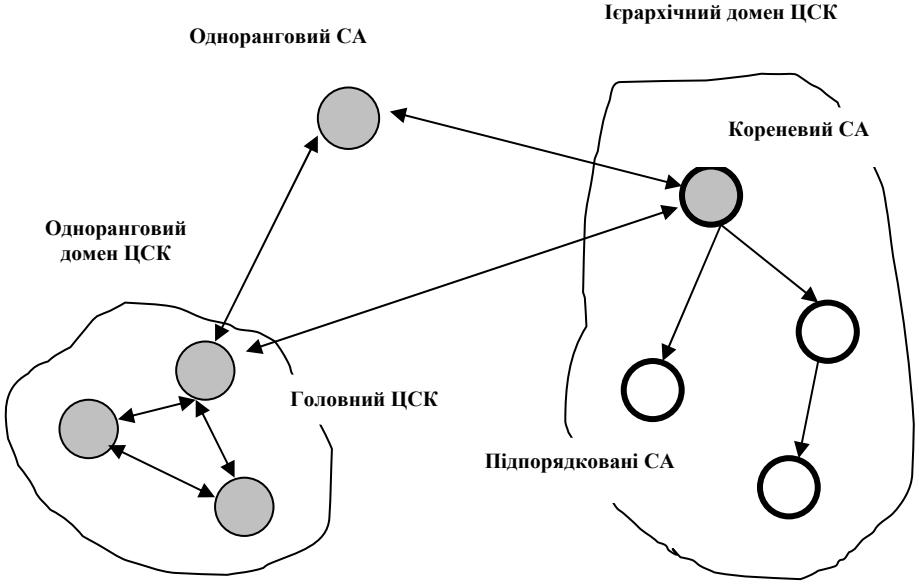
Додатково необхідно підкреслити, що в ієрархічній структурі при перевірці ланцюжків сертифікатів не передбачається перевірка сертифікату «кореня» домену, бо він є само-підписаним, а тому при компрометації ключа кореня публікація списку анульованих сертифікатів (CRL) стає неможливою,

оскільки цей список необхідно підписати вже скомпрометованим ключем, до якого немає довіри.

Мережева модель

Мережева модель PKI – це модель встановлення довірчих відносин між окремими Ізольованими та Ієрархічними ЦСК-доменами без довірчого посередника. Довірчі відносини встановлюються через механізм кросс-сертифікації.

Довірчі відносини встановлюються між Головними ЦСК (Principal CA) в уожному з доменів. Для Однорангового ЦСК-домену Головним ЦСК є сам Ізольований ЦСК; для об'єднання Ізольованих ЦСК із їх числа може бути призначений (на договірних засадах) один Ізольований, який є Головним у цій групі; для Ієрархічної моделі – це Кореневий ЦСК (мал.3).



Мал. 3. Мережена модель PKI

Переваги мереженої моделі:

- відносна простота встановлення довірчих відносин: достатньо застосувати механізм кросс-сертифікації між Головними ЦСК в існуючому домені ЦСК, не торкаючись при цьому Клієнтів ЦСК, тобто не вимагаються будь які зміни в середині кожного ЦСК-домену.
- дуже еластична структура щодо того, що існує багато точок довіри (не єдина);

- компрометація окремого ЦСК не може скомпрометувати усю структуру. ЦСК, які випустили кросс-сертифікати скомпрометованому Головному ЦСК, просто відміняють (анулюють) їх, видаляючи скомпрометований ЦСК з інфраструктури. Держателі та користувачі сертифікатів, які зв'язані з іншими ЦСК, все ще будуть мати допустимі точки довіри, і, відповідно, можуть спілкуватися надійно з держателями сертифікатів інших ЦСК, які не скомпрометовані;

- відновлення після компрометації більш просте, ніж для Ієрархічної моделі, хоча б тому, що це стосується меншого числа держателів;

- може бути легко створена з набору Ізольованих ЦСК чи доменів різної структури, так як держателі та користувачі сертифікатів не повинні змінювати їх точку довіри (чи будь-що іще). Вимагається лише, щоб ЦСК випустили сертифікати не менше ніж одному ЦСК в межах структури цієї моделі. Це дуже бажано навіть в межах однієї організації, яка хоче об'єднати окремо розроблені та впроваджені ЦСК, не порушуючи їх роботи.

Недоліки цієї моделі пов'язані із дво-направленністю моделі довір'я (на відміну від одно-направленої моделі у Ієрархічній моделі):

- при компрометації будь-якого з Головних ЦСК учасників, він самостійно має повідомити всіх інших; це при великій кількості об'єктів зробити досить складно та може зайняти тривалий час (від кількох годин до днів), що для деяких застосувань неприпустимо (наприклад – фінансових взаєморозрахунків);

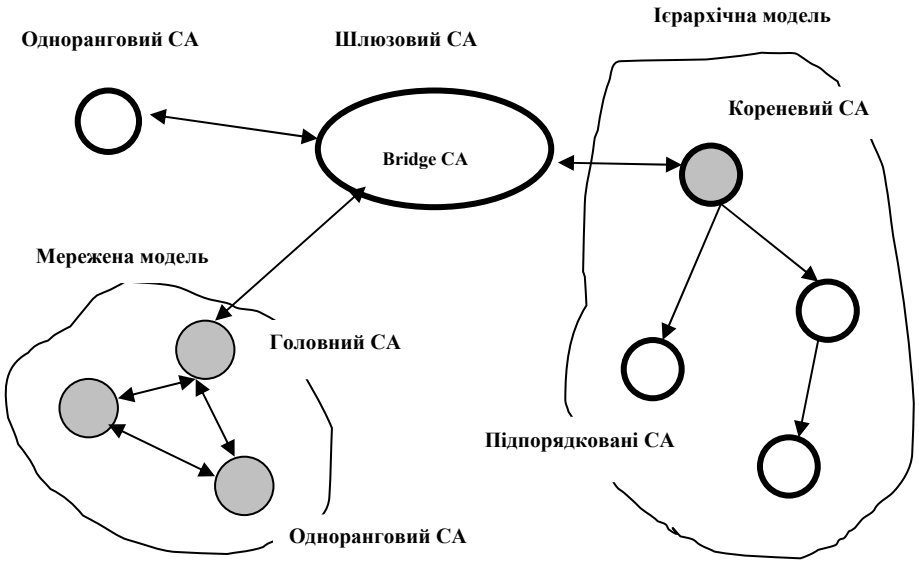
- розширення шляху сертифікації є більш складним процесом, ніж в Ієрархічній моделі. На відміну від ієрархії, побудова шляху сертифікації від сертифіката держателя до точки довіри не детермінована (не жорстко визначено). Це робить встановлення шляху сертифікації більш складним, так як можуть бути альтернативні шляхи. Деякі з них приведуть до допустимого шляху, а інші до глухого кута. Навіть гірше – можуть створюватися «петлі» (*цикли*, які починаються та закінчуються на одному і тому ж ЦСК).

За вказаних недоліків дуже критичним стає питання щодо застосування сертифікатів у програмних додатках (застосуваннях) кожного із учасників структури - обробка шляху сертифіката (перевірка чинності сертифікату) більш складна, а можливо й не однозначна.

Шлюзова модель

Шлюзова модель складається із окремих незалежних *Ізольованих* та *Ієрархічних доменів* (часткових графів, окремих «дерев»), в тому числі інших структур зі шлюзовою моделлю, які об'єднані довірчими відносинами через довірчого посередника, Шлюзовий ЦСК (Gateway CA), за допомогою механізму кросс-сертифікації. Головна особливість цієї моделі – можливість підключати до домену через довірчого посередника, Шлюзовий ЦСК або інша назва - «мост» (Bridge CA), який відмінний від Кореневого ЦСК (мал.4)

.



Мал. 4. Шлюзова модель

Така модель об’єднує переваги Ієрархічної та Мереженої моделей. Шлюзовий ЦСК не випускає сертифікатів для окремих користувачів, а тільки здійснює кросс-сертифікацію між доменами на рівні *однорангових відносин*. Це дозволяє встановити прості та прозорі відносини довіри між різними об’єднаннями користувачів через Шлюзовий ЦСК з визначеним рівнем довіри.

Переваги Шлюзової моделі в порівнянні з Мережаною моделлю:

- можливість застосувати більш сувору процедуру реєстрації учасників, в тому числі з урахуванням вимог для Ієрархічних ЦСК;
- при компрометації будь-якого з ЦСК-учасників, цей ЦСК інформує Шлюзовий ЦСК і йому не потрібно «множити» інформацію на всіх ЦСК-учасників, так як цю функцію виконує Шлюзовий ЦСК.

Інші **переваги** Шлюзової моделі:

- дозволяє легко підключити новий ЦСК; держателі та користувачі сертифікатів не повинні змінювати їх точку довіри чи свої ключі;
- компрометація окремого ЦСК (у тому числі Центрального засвідчувального органу в Україні), не може скомпрометувати усю структуру;
- відновлення після компрометації більш просте в Шлюзовій моделі, ніж в ієрархічній.

Недоліки Шлюзової моделі подібні до тих, які є у Мереженої. Але шляхи сертифікації значно коротші. Проблема появи циклічних шляхів сертифікації в Шлюзовій моделі існує, але вона менш гостра, так як тут є єдина структура (Шлюзовий ЦСК), що може контролювати появу (наявність) циклічних шляхів і відповідно не допускати їх.

Для контролю наявності циклічних шляхів треба сформулювати задачу побудови Національної інфраструктури ЕЦП як побудови *зв'язного ациклічного* графа та визначення *шляху* (від сертифікату будь-якого держателя до довірчого ЦСК-сертифікату) з мінімальною довжиною.

Вибір моделі довірчих відносин

Національна інфраструктура ЕЦП повинна будуватися, виходячи з питання *національної безпеки*, а отже припускаючи можливість (враховуючи ризики) компрометації окремих підсистем ЕЦП.

Як слідує з розглянутого вище, можливі такі моделі побудови Національної інфраструктури ЕЦП:

- ієрархічна модель (планується будувати в Україні);
- шлюзова модель (вибрана як основна в США, ЄС та інш.).

Довірчі відносини можуть бути встановлені одно-направленими (підпорядковано-залежними) чи дво-направленими (одноранговими, незалежними). Вибір типу відносин залежить від відносин між групами держателів (клієнтів ЦСК).

Можливі два сценарії:

(1) Групи держателів сертифікатів належать до різних організацій в межах однієї компанії (відомства) з одним централізованим управлінням усіх організацій.

(2) Групи держателів належать до різних компаній (відомств), кожна з яких є самостійною із своєю структурою управлінням, але ці компанії мають між собою деякі договірні відносини і хочуть встановити довірчі відносини.

Як зазначено вище, створення ієрархії вимагає, щоб кожен держатель та користувач сертифікату з різних груп вніс корективи в його точку довіри відповідно до заново визначеного Кореневого ЦСК. Це є принциповою зміною у довірчих відносинах, так як раніше держателі та користувачі не мали ніяких контактів з цим новим Кореневим ЦСК.

У сценарії (1) ця фундаментальна реорганізація практично може бути здійснена – існує єдина організаційна структура, розпорядження та накази якої будуть (повинні бути) виконані усіма членами та вчасно.

У сценарії (2) така реорганізація приречена на поразку. Відносини між держателями та користувачами не базуються на підпорядкованості, - це окремі компанії, не мається чіткого центрального керівництва. При відсутності центрального керівництва групи часто не здатні домовитися

навіть про прийнятну єдину третю особу, щоб встановити Кореневий ЦСК нової ієрархії, особливо, якщо одна із компаній (відомств) хоче перейняти цю функцію на себе, що розглядається іншими, як деяка підпорядкованість цій компанії (відомству), тобто втрата елементів самостійності та керованості. У цьому випадку заміна довірчої точки може стати конфліктом між цими організаціями (групами).

Для сценарію (2) більш прийнятним є встановлення дво-направлених довірчих відносин через взаємну кросс-сертифікацію або довіреного посередника (*Шлюзовий ЦСК*). Така схема відповідає вимозі універсальності застосування та мінімізації структурно-технічних ризиків [6], [7].

Слід наголосити, що визначена державним регулюючим органом ДСТСЗІ СБУ [4] модель побудування дворівневої моделі ЦСК для недержавних структур створить значні проблеми не тільки для великих корпоративних бізнес-структур, по типу системообразуючих банків або розгалужених торгових мереж, для яких замалою може бути навіть дворівнева система, але й для менших бізнес структур. Тим більш відмова від кросс-сертифікації при визнанні лише ієрархічної архітектури [4] піддає дуже суттєвим ризикам будь-які системи електронного документообігу в загальнонаціональному масштабі: ризики компрометації, технічної ненадійності в національних системах та більшості бізнес-застосувань при використанні вказаної архітектури є неприйнятними як з точки зору національної безпеки, так і можливих збитків абонентів та користувачів.

Таким чином, вибрана в Україні для побудови ієрархічна модель Національної інфраструктури ЕЦП, з точки зору її безпеки та технологічності щодо підключення існуючих структур є гіршою, а найбільш прийнятною можна визнати Шлюзову модель.

Висновки та пропозиції:

1. Вважаємо, що за базову модель побудови Національної інфраструктури ЕЦП необхідно прийняти Шлюзову модель.
2. Необхідним елементом для застосування в національний інфраструктурі ЕЦП є створення довірчих «мостів» - Шлюзових ЦСК, які виконують кросс-сертифікацію між іншими Головними ЦСК різних організацій, установ та відомств.
3. Для розв’язання проблеми виключення можливих «циклів» сертифікаційних шляхів необхідно розробити функціональні вимоги до Шлюзових ЦСК, модель впровадження та контролю використання таких вимог.

Література:

1. Закони України «Про електронний цифровий підпис» №852-IV від 22.05.2003, «Про електронний документообіг» №851-IV від 22.05.2003.

2. Постанови КМУ «Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу» №680 від 26.052004 р., «Порядок акредитації центру сертифікації ключів» №903 від 13.07.2004 р.

3. М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных, А.В. Потий. Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий. УДК 681.322.

4. В.В. Барлабанов. Электронно-цифровая подпись: взгляд из СБУ.- «Компьютеры +Программы», №2 (99), 2003

5. EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000, OID: 1.3.6.1.4.1.5255.1.1.1

6. *D.R. Kuhn, V.C. Hu, W.T. Polk, S.J. Chang.* Introduction to Public Key Technology and the Federal PKI Infrastructure. - NIST SP 800-32, February 2001

7. William T. Polk, Nelson E. Hastings. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures. - NIST, 03/08/2004