Національна система PKI України (UaPKI).
Архітектура національної PKI

к.ф.-м.н. Мартиненко С.В.

Анотація

Цей документ відноситься до питань інформаційної безпеки електронного уряду та призначений для викладення питань побудови архітектури національної інфраструктури відкритих ключів (PKI – Public Key Infrastructure) та її реалізації в межах державних структур та їх агентств/установ.

Надається короткий огляд ризиків та переваг різних PKI компонентів та деяких прикладних застосувань, можливих для виконання в межах електронного уряду.

Цей документ розроблений з метою надання практичних рекомендацій та допомоги посадовим особам державних агентств, які приймають рішення щодо питань практичної реалізації функцій електронного уряду: чи відповідає PKI їх агентству, які PKI послуги можуть бути фактично розгорнуті та найбільш ефективно використані в межах державного агентства та електронного уряду в цілому тощо

1. Вступ

1.1. Передумови

Згідно Указу Президента України від 1 серпня 2002 р. №683 «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» та Постанови Кабінету Міністрів України (КМУ) від 24 лютого 2003 р. №208 «Про заходи щодо створення електронної інформаційної системи "Електронний Уряд"» одним з пріоритетних завдань щодо розвитку інформаційного суспільства України визначено надання громадянам та юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи "Електронний Уряд", яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Однією із задач зазначеної постанови КМУ визначено на 2005 рік забезпечити надання громадянам і юридичним особам з використанням електронної інформаційної системи "Електронний Уряд" інформаційних та інших послуг, які потребують ідентифікації суб'єктів правових відносин і забезпечення цілісності та достовірності інформації (з використанням електронного цифрового підпису).

Закон України «Про електронні документи та електронний документообіг», від 22.05.2003 №851-IV визначає юридичний (законодавчий) статус електронних документів та звітів.

Державні агентства зобов’язані використовувати методи електронної ідентифікації та перевірки тотожності відправника (аутентифікації) і цілісність електронного повідомлення.

Закон України «Про електронний цифровий підпис» від 22 травня 2003 року №852-IV визначає електронний цифровий підпис як метод підписання електронного повідомлення, що ідентифікує та підтверджує дійсність особи, яка є джерелом повідомлення та забезпечує цілісність (незмінність) повідомлення.

Законом України «Про електронний цифровий підпис» від 22 травня 2003 року №852-IV та «Порядком засвідчення наявності електронного документа (електронних даних) на певний момент часу», затвердженого постановою КМУ 26 травня 2004 р. №680, «Порядком акредитації центру сертифікації ключів», затвердженого постановою КМУ від

13 липня 2004 р. №903, визначено загальні функції та встановлено загальні вимоги до центру сертифікації ключів, акредитованого центру сертифікації ключів, центрального засвідчувального органу, засвідчу вального центру органу виконавчої влади або іншого державного органу.

За основу побудови архітектури UaPKI в цій публікації взято рекомендації та стандарти **EuroPKI** Європейсько Співтовариства [«EuroPKI Certificate Policy», жовтень 2000 р.] та Федеральний PKI Національного Інституту Стандартів і Технології США [*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] (Federal PKI, NIST - National Institute of Standards and Technology) та інші.

1.2. Ціль

Ціль документу – визначити архітектуру центрів сертифікації **UaPKI,** зокрема, складові елементи структури **UaPKI** та їх взаємодію.

1.3. Межі застосування

Враховуючи те, що Національна PKI повинна об'єднати державний та недержавний сектори інфраструктури PKI України, в цій публікації обговорюються питання вибору варіанту побудови Національної PKI, - створення сертифікаційних шляхів між різними державними відомствами (установами, агентствами) та недержавними організаціями, в тому числі банківським сектором, так, щоб забезпечити високий рівень довірчих відносин, інтеграцію і одночасно криптографічну самостійність/незалежність кожного з відомств/організацій.

В цьому документі не розглядаються питання політики сертифікатів, але вважається, що використовується формат X.509 версії 3. Зміст документу не поширюється на визначення політики захисту інформації взагалі.

Вважається, що читач ознайомлений з загальними поняттями цифрового підпису, сертифікатів та інфраструктури відкритих ключів, що використовується в X.509.

2. Визначення

До усіх терміни надаються також англійською мовою для того, щоб встановити їх відповідність європейським та міжнародним стандартам і можливості взаємодії Національної PKI з іншими національними чи міжнародними PKI.

Держатель сертифікату (Certificate Holders) – суб'єкт чи об'єкт, якому випущено сертифікат і який на законних підставах володіє особистим ключем цифрового підпису. Вживається також еквівалентний термін **Клієнт CA (Customer CA)**.

Довірчий домен (Trust Domain) - частина *Національної PKI*, яка працює під управлінням одного Центру управління політикою домену (***Domain Policy Management Authority - DPMA***). В межах *Довірчого домену* існують один чи більше CA. Кожен *Довірчий домен* має єдиний *Основний CA*, але може мати багато інших CA.

Ізольований/Одноранговий CA (Isolate/Peer CA) – CA, що має само-підписаний сертифікат, який розсилається його держателям сертифікатів та використовується ними для ініціалізації шляху сертифікації. Цей же CA випускає сертифікати своїм клієнтам. Частіше зустрічаються термін „Одноранговий".

Ієрархічний домен PKI (Hieratic Domain PKI) – домен із структурою зв'язного графа, тобто «дерева» (будь-які дві вершини графа можна з'єднати ланцюгом), яке має одну головну вершину, «корінь» (*Кореневий CA*), з якої будується структура *Підпорядкованих CA*.

Координуючий/Шлюзовий СА (Bridge/ Gateway Certification Authorities - BCA) – СА, єдиною задачею якого є встановлення довірчих однорангових відносин з PKI доменами. Сам *BCA* не використовується як точка довіри. Усі СА вважають BCA довірчим посередником.

Компонентний домен PKI (Mesh Domain PKI) – домен, який складається із окремих незалежних *Ізольованих* та *Ієрархічних доменів* (часткових графів, окремих «дерев»), тобто компонент, які об'єднані довірчими відносинами через довірчого посередника чи механізми кросс-сертифікації. Інший термін – „*мережений домен*".

Кореневий СА (Root CA) - в ієрархічному Довірчому домені Кореневий СА – це СА, з якого починаються всі довірчі шляхи сертифікації. Держателям сертифікатів та пов'язаним сторонам само-підписаний сертифікат Кореневого СА видається будь-яким способом, що забезпечує достовірність цього сертифікату. Для Довірчих доменів ієрархічної структури Кореневий СА – це перший (початок «дерева») СА для цього домену.

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)".**

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

Національний Центр управління політикою (National Policy Management Authority - NPMA) – центр управління, який визначає усі політики Національної PKI та затверджує політики і процедури Довірчих доменів в межах Національної PKI. Використовує Національний *Координуючий СА* та архів.

Національний Координуючий СА (NBCA) – це *Координуючий СА*, що використовується *NPMA*. Його ціль – створити «міст» довір'я, який забезпечить довірчі шляхи (відносини) між різними Довірчими доменами *Національної PKI*, а також між Національним PKI та зарубіжними Довірчими доменами PKI. Право *кросс-сертифікації* з Національним NBCA мають NPMA-затверджені Довірчі домени через свій Основний СА (Принципал-СА). NBCA - не є Кореневим СА, так як не є початком/вершиною шляху сертифіката (вершиною ланцюга сертифікатів).

Одноранговий СА (Peer CA) – див. *Ізольований СА*.

Одноранговий домен PKI (Peer Domain PKI) - домен із структурою мережі, який має в своїй структурі рівноправні *Ізольовані СА*, які встановлюють між собою довірчі відносини безпосередньо через механізм кросс-сертифікації. Тобто немає СА вищого рівня чи будь-якого іншого довірчого посередника.

Основний СА (Принципал-СА, Principal CA) – СА в Довірчому домені, який здійснює кросс-сертифікацію з Національним NBCA. Кожен Довірчий домен має один Основний СА. В домені з ієрархічним шляхом сертифікатів це буде Кореневий СА домену. В доменах із структурою мережі (mesh domain) Основним СА може бути будь-який СА в домені. Звичайно це буде той, який використовується чи пов'язаний з DPMA.

Підпорядкований СА (Subordinate CA) – СА в ієрархічному домені, з якого не починаються Довірчі шляхи сертифікації. В ієрархічному довірчому домені

Підпорядкований СА отримує свій СА-сертифікат від СА вищого рівня. Підпорядкований СА може мати власні Підпорядковані СА, яким він видає СА-сертифікат.

Політика сертифікату (Certificate Policy) – визначений набір правил, який встановлює можливість застосування сертифікатів в специфічній групі та/чи класі додатків (прикладних програм) з загальними вимогами захисту.

СА домен (CA Domain) – частина *Національної PKI*, яка працює під управлінням одного СА. В СА домен входять усі користувачі (клієнти) цього СА.

СА-сертифікат (CA-certificate) – сертифікат відкритого ключа одного СА, випущений іншим СА вищого рівня або само-підписаний сертифікат. СА сертифікат призначається для підпису сертифікатів, випущених цим СА.

Сторона, що довіряє (Relying party) – користувач сертифікату, який діє у впевненості щодо цього сертифікату та/чи цифрових підписів, перевірених з використанням цього сертифікату. В цьому документі терміни „**Користувач сертифікату**" та „**Сторона, що довіряє**" використовуються як синоніми. Особа/ суб'єкт, яка підписує документ, називається **Підписувач** або **Власник** чи **Держатель** сертифікату.

Центр реєстрації (Registration Authority - RA) – об'єкт, що відповідає за ідентифікацію та аутентифікацію суб'єктів сертифікатів, але не підписує і не випускає сертифікати (тобто, RA делегуються деякі задачі від імені СА).

Центр сертифікації ключів (CA – Certificate Authority) - юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги щодо сертифікації відкритих ключів.

Шлях сертифікації (Certification path) – впорядкована послідовність сертифікатів, які, разом із відкритим ключем початкового об'єкта в низці сертифікатів може бути оброблений (перевірений підпис) так, щоб перевірити кінцевий об'єкт в низці сертифікатів. Синонімом терміну „шлях сертифікації" є термін „Низка сертифікатів" (**Certificate chain**).

3. Архітектура Національної PKI

3.1. Головна задача Національної PKI

Звичайно PKI складається з багатьох СА, зв'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 переконатися в законності сертифікату при його використанні. Наприклад, одержувач підписаного повідомлення (Користувач сертифіката), який не має відносин з СА, що випустив цей сертифікат для Підписувача (відправника повідомлення), може перевірити чинність сертифіката Підписувача, використовуючи довірчий шлях до цього СА.

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

3.2. PKI підприємства чи державного агентства

Розгортання PKI може починатись з будь-якого підприємства, компанії чи державного агентства/ відомства.

Конфігурація PKI архітектури підприємства чи окремого державного відомства доцільно будувати, виходячи з структури їх управління. Архітектура PKI для окремого підприємства, відомства тощо може бути однією з двох можливих конфігурацій:

- Ізольований/Одноранговий CA (Isolate/Peer CA)
- Одноранговий домен PKI (Peer Domain PKI)
- Ієрархічний домен PKI (Hieratic Domain PKI)
- Компонентний домен PKI (Mesh Domain PKI)

3.2.1. Ізольований/Одноранговий CA (Isolate/Peer CA)

Ізольований/Одноранговий CA – це CA, що має само-підписаний CA-сертифікат (self-signed CA-certificate), який не завіряється (не підписується) будь-яким іншим CA вищого рівня (рис.1). Шлях сертифікації у цьому випадку дорівнює 2 (двом), тобто CA-сертифікат та сертифікат клієнта цього CA. Ізольований CA не видає сертифікати іншим CA (не має підпорядкованих CA).

Тут CA домен складається тільки з Ізольованого CA та Держателів сертифікатів, яким видано сертифікати цим CA. Такий домен ще називають Одноранговим доменом PKI з одним Ізольованим CA.

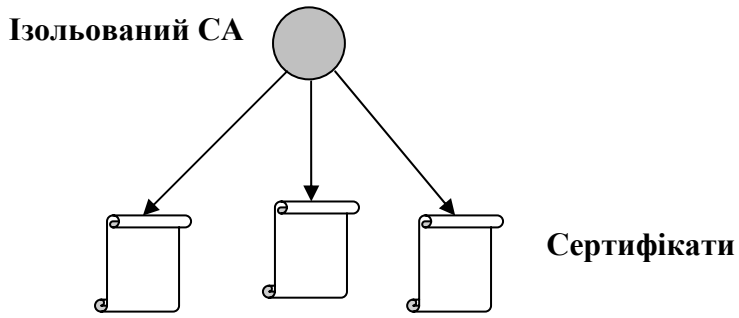

Рис.1. Ізольований CA домен

Приєднати Ізольований CA домен до іншої PKI (CA домену) можна двома основними способами:

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

В першому випадку вимагається обов'язково перевипуск CA-сертифіката (самого CA), а отже й повний перевипуск сертифікатів усіх клієнтів CA.

В другому випадку не вимагається – усі сертифікати клієнтів залишаються чинними після приєднання Ізольованого CA до деякого довірчого Однорангового домену PKI через механізм кросс-сертифікації.

Переваги Ізольованого CA:

- мінімальна вартість та простота впровадження.

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

Недоліки Ізольованого CA:

- усі Клієнти CA з однаковим профілем сертифікату мають однакові довірчі відносини. Це важливо, якщо необхідно мати декілька груп Клієнтів CA, які повинні мати різні довірчі відносини. Наприклад, якщо необхідно видавати сертифікати для декількох груп, наприклад, працівники організації та клієнти (що має місце, зокрема, в банківському секторі), то з точки зору безпеки ці

групи необхідно розмежовувати, що можна здійснити на рівні розмежування СА (див. Нижче Ієрархічний домен СА);

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

3.2.2 Одноранговий домен PKI (Peer Domain PKI)

Домен PKI, в який входять тільки Однорангові СА, між якими встановлено довірчі відносини через кросс-сертифікацію, називають Одноранговим доменом PKI (рис.2).

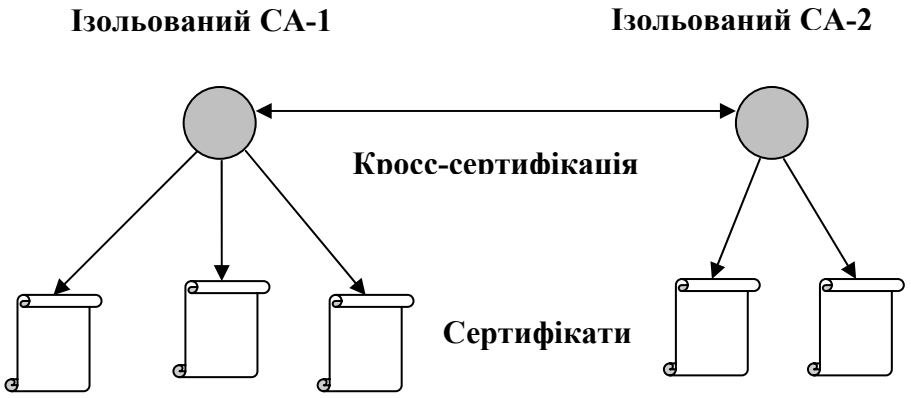

Рис.2. Одноранговий домен PKI

Переваги Однорангового домену PKI:

- відносна простота встановлення довірчих відносин – досить застосувати механізм кросс-сертифікації між Ізольованими СА в домені, не торкаючись при цьому Клієнтів СА, тобто не вимагаються будь-які зміни в середині кожного СА домену.

Недоліки Однорангового домену PKI:

- механізм кросс-сертифікації вимагає встановлювати довірчі відносини між усіма СА по-парно, тобто кожна пара СА встановлює довірчі відносини між собою безпосередньо. Таким чином, якщо в Довірчому домені є вже ***N*** Ізольованих СА, то при підключенні нового СА цьому СА необхідно встановити ***N*** довірчих відносин (з кожним СА в домені окремо).

- Відповідно, якщо один із СА виходить із Довірчого домену (виключається через компрометацію тощо), то усі інші члени цього Довірчого домену повинні внести у себе відповідні «виправлення». При цьому немає в домені такого центрального органу – довірчої особи, яка б була зобов'язана повідомити всіх членів домену про вихід (втрату довір'я) одного із членів.

3.2.3. Ієрархічний домен СА (Hieratic CA)

Ієрархічний домен СА (Hieratic Domain CA) – домен із структурою зв'язного графа, тобто «дерева» (будь-які дві вершини графа можна з'єднати ланцюгом), яке має одну головну вершину (Кореневий СА), з якої будується структура Підпорядкованих СА (рис.3).

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

Кожен з Підпорядкованих СА може випустити сертифікат як своїм Клієнтам, так і йому підпорядкованому СА (**Підпорядковані СА другого рівня**).

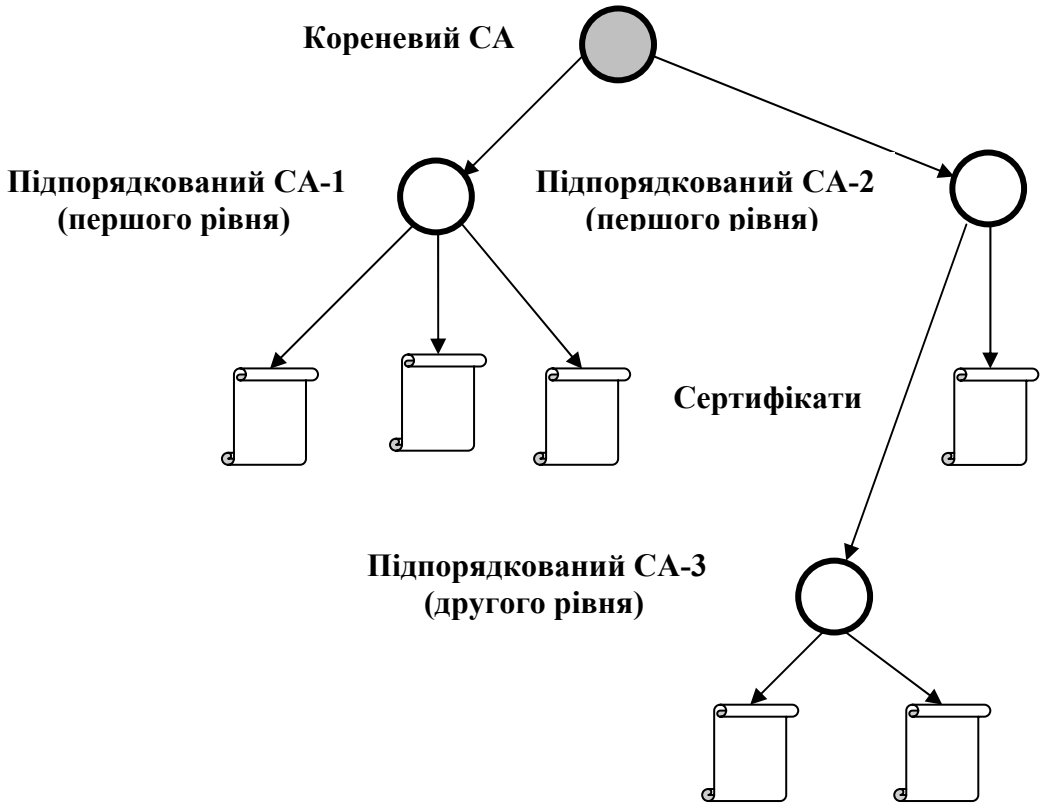

Рис.3. Ієрархічний домен PKI

В Ієрархічному PKI довірчі відносини визначені лише в одному напрямку – від вищого рівня до нижчого рівня СА, тобто Підпорядковані СА не випускають сертифікати для СА вищого рівня.

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

Довірчі відносини між держателями сертифікатів різних під-доменів будуються так

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

- але 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 СА 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 СА.

Переваги Ієрархічної структури PKI:

- наявність Кореневого СА, який видає сертифікати виключно Підпорядкованим СА, тобто «працює» періодично, що дозволяє «замурувати його у сейф» та забезпечити високий рівень безпеки;
- дозволяє довірчі відносини між держателями та дозволяє розмежувати повноваження (права) доступу груп користувачів до сервісів;
- ієрархічна структура дозволяє просто добавляти нові довірчі групи держателів сертифікатів шляхом підключення нового Підпорядкованого СА (будь-якого нижнього рівня) та його під-домену;
- користувачі ієрархії знають явно чи неявно (встановлюється через політику сертифікату) для яких прикладних додатків (програм) може використовуватися сертифікат, що базується на позиції (рівні) СА в межах ієрархії.

Недоліки Ієрархічної структури PKI є наслідками довіри єдиній точці (вищому рівню – Кореневому СА) в структурі ієрархії:

- компрометація «кореня» (ключа Кореневого СА) призводить до компрометації усього Ієрархічного домену та необхідності перегенерації усіх без виключення ключів держателів усіх під-доменів, що може мати фатальні наслідки для організації. Ніяких інших безпечних методів відновлення роботи домену і під-доменів не існує.
- єдиний Кореневий СА може бути неможливим із «політичних» міркувань – конкуренція, міжвідомчі перепони тощо.
- перехід як від Ізольованих СА, так і від інших окремих Ієрархічних доменів до єдиної Ієрархічної PKI є логічно непрактичним, так як усі користувачі сертифікатів вже існуючих доменів повинні внести зміни до їх довірчих точок (шляхів), а усі держателів сертифікатів замінити свої сертифікати та відповідно ключі підпису на нові, які відповідають новій ієрархічній структурі PKI.

3.2.4. Компонентний домен PKI (Mesh Domain PKI)

Компонентний домен PKI (Mesh Domain PKI) – це домен, який складається із окремих Ізольованих СА, Однорангових та Ієрархічних доменів (часткових графів, окремих «дерев»), тобто окремих компонент, які об'єднані довірчими відносинами через **довірчого посередника** чи механізми кросс-сертифікації. Інший термін – „мережений домен". Головна особливість цього домену – можливість підключати до домену через довірчого посередника Однорангові PKI та Ієрархічні PKI, а також наявність довірчого посередника, відмінного від Кореневого СА (рис.4).

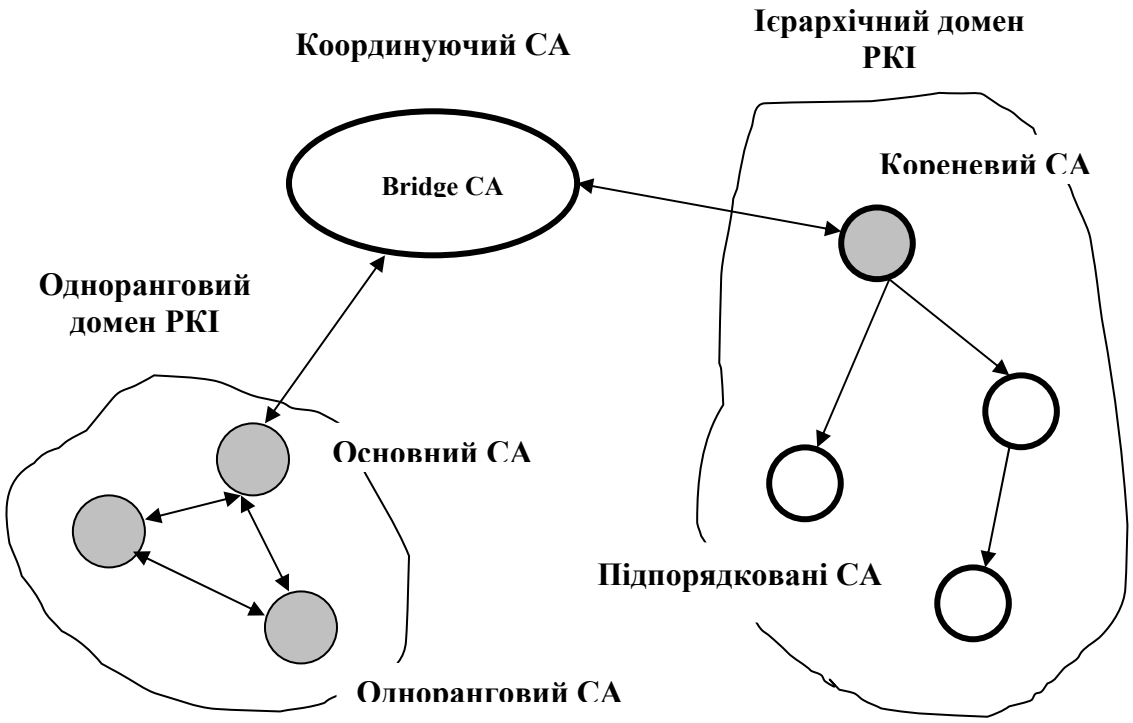

Рис.4. Компонентний домен PKI

Переваги Компонентного домену PKI:

- дозволяє легко підключити новий домен – будь-який CA-домен просто встановлює довірчі відносини с іншими CA-доменами, членами Компонентного домену;
- дуже еластична структура щодо того, що існує багато точок довіри (не єдина);
- компрометація окремого CA не може скомпрометувати усю структуру PKI. CA, які випустили сертифікати скомпрометованому CA просто відкликають їх, видаляючи скомпрометований CA з PKI. Держателі та користувачі сертифікатів, які зв'язані з іншими CA, все ще будуть мати допустимі точки довіри, і, відповідно, можуть спілкуватися надійно з держателями сертифікатів інших CA, які не скомпрометовані;
- відновлення після компрометації більш просте в CA Компонентного домену PKI, ніж для Ієрархічного PKI, хоча б тому, що це стосується меншого числа держателів;
- може бути легко створена з набору ізольованих CA чи доменів різної структури, так як держателі та користувачі сертифікатів не повинні змінювати їх точку довіри (чи будь-що іще). Вимагається лише, щоб CA випустили сертифікати не менше ніж одному CA в межах Компонентного домену PKI. Це дуже бажано навіть в межах однієї організації, яка хоче об'єднати окремо розроблені та впроваджені PKI, не порушуючи їх роботи.

Недоліки Компонентного домену PKI пов'язані із дво-направленністю моделі довіри (на відміну від одно-направленої моделі у Ієрархічному домені PKI):

- розширення шляху сертифікації більш складний процес, ніж в ієрархічній моделі. На відміну від ієрархії, побудова шляху сертифікації від сертифіката держателя до точки довіри не детермінована (не жорстко встановлена). Це робить встановлення шляху сертифікації більш складним, так як є альтернативні шляхи. Деякі з них приведуть до допустимого шляху, а інші до глухого кута. Навіть гірше – Компонентному домені

можуть створюватися «петлі» (*цикли*, які починаються та закінчуються на одному і тому ж СА).

Ця проблема має математичне пояснення, як і розв'язок, у термінах математичної *теорії графів*, як розділу дискретної математики (точніше теорії множин). Визначення графа – це система, яка складається із обмеженої множини елементів, які називаються *вершинами* (зображаються кружками або точками) та обмеженої множини елементів, які називаються *ребрами* (зображаються лініями, які з'єднують вершини), аналогічно домену PKI на рис.4. Лінії з одно-направленими стрілками називаються *дугами*, без стрілок (ненаправлені або з дво-направленими стрілками) – *ребрами*. Граф називається *зв'язним*, якщо він не має *ізольованих* (відкремлених) вершин.

Вершинами графу є СА-сертифікати та сертифікати держателів. Дуги мають місце в ієрархічних доменах і визначають напрямок передачі довіри - від того хто (емітент) видав, до того кому (держатель) видано сертифікат, тобто від емітента до держателя. Ребра – це кросс-сертифікаційні відносини між СА.

Тут наведено деякі визначення та співставлення з теорією графів з метою показати, що ця задача, а саме побудова шляху сертифікації в Компонентному домені має математичний розв'язок, отже недолік, зазначений вище не є принциповим.

Задачею побудови Національної PKI є побудова *дерева*, як *зв'язного ациклічного* графа та визначення *шляху* (від сертифікату будь-якого держателя до довірчого СА-сертифікату) з мінімальною довжиною.

3.3. Вибір моделі довірчих відносин

Довірчі відносини, як випливає із зазначеного вище, можуть бути встановлені одно-направленими (підпорядковано-залежними) чи дво-направленими (одноранговими, незалежними). Вибір типу відносин залежить від відносин між групами держателів (клієнтів СА).

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

У сценарії (1) ця фундаментальна реорганізація PKI може бути здійснена – тут існує єдина організаційна структура, розпорядження та накази якої будь (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 не здатні домовитися про прийнятну єдину третю особу, щоб встановити Кореневий СА нової PKI ієрархії, особливо, якщо одна із компаній (відомств) хоче перейняти цю функцію на себе, що може розглядатися іншими, як деяка підпорядкованість цій компанії

(відомству), тобто втрата деяких елементів самостійності та управляємості. У цьому випадку заміна довірчої точки може стати конфліктом між цими організаціями (групами).

Для цього сценарію більш прийнятним є встановлення дво-направлених довірчих відносин через взаємну кросс-сертифікацію або довіреного посередника (*Координуючий CA*).

3.4. Конфігурація Національної PKI

Національна PKI є об'єднанням PKI недержавних підприємств та державних відомств (агентств), до складу якої можуть входити:

- Одноранговий домен (Peer Domain);
- Ієрархічний домен (Hieratic Domain);
- Компонентний домен (Mesh Domain)..

Треба розмежовувати два терміни:

- Державна PKI, та
- Національна PKI

Державна PKI призначається для взаємодії в межах державних структур чи між ними (тобто обмежена кордонами та державними структурами). *Національна PKI* призначена для створення шляхів сертифікації між різними відомствами та організаціями як державними, так комерційними, як України, так і інших держав (Інтернет не має кордонів).

Основними задачами Національної PKI є:

- створення шляхів сертифікації, які не мають циклів, між різними відомствами та організаціями, які будуть забезпечувати високий рівень довірчих відносин;

- забезпечення можливості функціонування та взаємодії в межах Національної PKI при використанні декількох алгоритмів цифрового підпису та шифрування;

- створення Політики Сертифікатів (CP) Національної PKI та технічні специфікації, даючи можливість відомчим державним та недержавним CA складати їх власну Інструкцію з технології сертифікації (Certification Practice Statement, CPS).

4. Висновки

4.1. Ієрархічна модель Національної PKI

В ієрархічній моделі є єдина перша точка довіри - один центральний Центр сертифікації ключів (*Центральний засвідчувальний орган*).

Перевагою ієрархічної моделі є простота її початкової побудови. *Головним недоліком* ієрархічної моделі є наслідками довіри єдиній точці в структурі ієрархії (*Центральному засвідчувальному органу*) – компрометація ключа «кореня» *призводить до компрометації усіх підпорядкованих центрів сертифікації* та необхідності генерації заново усіх без виключення ключів ЕЦП (в масштабах України), що може мати фатальні наслідки для електронної Держави. Ніяких інших безпечних методів відновлення роботи після компрометації «кореня» *не існує*.

Шлюзова модель

Шлюзова модель (Bridge/Gateway Model) складається із окремих ізольованих CA та ієрархічних доменів CA, які об'єднані довірчими відносинами через *довірчого посередника*. На відміну від Ієрархічної моделі вона не має таких великих ризиків у разі компрометації ключа Bridge CA.

Ця модель прийнята за основну для побудови Національної (Федеральної) структури Цифрового підпису США, Канади та ін., а також для Європейського співтовариства.

Сергій В. Мартиненко

Digitally signed by Сергій В. Мартиненко
DN: cn=Сергій В. Мартиненко, ou=BKP-consulting Ltd., dc=org
Reason: Я автор цього документу
Location: Kiev, Ukraine
Date: 2005.11.28 08:34:38 +02'00'