УДК 681.3:002.651.028(083.73)

П. С. КЛІМУШИН

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ДОВІРИ В НАЦІОНАЛЬНІЙ СИСТЕМІ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

***В**изначено основні механізми довіри в інфраструктурі відкритих ключів: ізольований, кореневий, мережевий, шлюзовий, списком статусу, списком сертифікатів та управління якістю сертифікатів; практичні рекомендації щодо запровадження європейської системи QPKI для забезпечення єдиного інформаційного простору, розвитку інвестицій, впровадження інновацій та підвищення якості життя і послуг.*

Ключові слова: механізми довіри, електронний цифровий підпис, інфраструктура відкритих ключів, засвідчувальний центр, орган сертифікації.

***B**asic mechanisms of trust in the public key infrastructure - peer, root, network, bridge, by status list, by certificates list, and certificates quality control – have been determined; practical recommendations are given as to introduction of the pan-European QPKI system for providing a common information area, development of investments, introduction of innovations, and improving life and services standards.*

Key words: mechanisms of trust, electronic digital signature, public key infrastructure, certification center, certification authority.

Концепція розвитку електронного урядування в Україні до 2015 р. є одним із пріоритетних завдань побудови інформаційного суспільства. Цією концепцією визначено надання фізичним та юридичним особам юридично значимих послуг шляхом використання електронних комунікацій на основі впровадження механізмів довіри між суб'єктами правових відносин і забезпечення цілісності та достовірності інформації.

Основою довіри в сучасній концепції електронного урядування є електронний цифровий підпис (ЕЦП), технологічно підтриманий інфраструктурою відкритих ключів (PKI).

Сьогодні національна система ЕЦП (НСЕЦП) як організаційно-технічна система інтегрує сертифікати відкритих ключів, засоби ЕЦП (криптографічних перетворень), центри сертифікації ключів (ЦСК) і власників сертифікатів в єдину структуру і гарантує від імені держави якість послуг ЕЦП. Якість послуг ЕЦП регулює Центральний засвідчувальний орган (ЦЗО), якій є органом акредитації та державного нагляду за діяльністю центрів сертифікації ключів, акредитованих (АЦСК) і зареєстрованих (ЦСК).

Проте НСЕЦП поки відстає від світового рівня розвитку на 8 – 10 років [5]. Так, відповідно до європейської бізнес-моделі ЕЦП, кваліфікована інфраструктура відкритих ключів (QPKI) реалізує три виду кваліфікованих підписів на відміну від

прийнятої в Україні інфраструктури PKI, що реалізує тільки один, найпростіший та неінтероперабельний різновид підпису [4].

Окрім того, Єврокомісія за підтримкою Європарламенту запропонувала стратегію розвитку інформаційного простору Євросоюзу до 2020 р. Ця стратегія спрямована на досягнення трьох головних цілей на створення: єдиного європейського інформаційного простору, умов для інвестицій та інновацій у сфері інформаційних технологій, а також повсюдно охоплення інформаційними технологіями всіх структур суспільства, що сприятиме підвищенню якості життя і послуг.

Таким чином, для України актуальна проблема вдосконалення внутрішній та зовнішньою політики у сфері інтеграції національних систем ЕЦП до міжнародних систем.

Розробці практичних рекомендацій щодо розвитку національних інфраструктур ЕЦП присвячено багато праць вітчизняних науковців і дослідників різних структур суспільства. Значний вклад знань з питання впровадження інфраструктур ЕЦП у банківській сфері внесли такі дослідники: І. Івченко [6], С. Левшаков [3], А. Савченко [6], В. Степаненко [7]. Дослідженню питань теорії та практики аналізу, синтезу та застосування ЕЦП присвячено роботи науковців: М. Бондаренко, І. Горбенко [2], Ю. Горбенко [2], В. Онопрієнко, А. Потій, С. Черних. У роботах науковців С. Бєлова і С. Мартиненка [1] обґрунтовано моделі побудови національної інфраструктури центрів сертифікації ключів та аналізуються їх ризики. Особливу значимість мають роботи науковців А. Мелащенка і О. Перевозчикової [4; 5], де розглянути проблеми крос-сертифікації, інтероперабельності НСЕЦП та запровадження міжнародних стандартів в сфері QPKI в систему національних стандартів.

Подальший розвиток національної PKI вимагає визначення механізмів довіри. Проте практика крос-сертифікації (процес установлення довірчих відносин між органами сертифікації в інфраструктурі відкритих ключів), упровадження інтероперабельних компонент ЕЦП, установлення політик безпеки, розробка організаційно-технологічних заходів і технічних регламентів для запровадження європейської системи QPKI недостатнє досліджена і набуває актуальності в умовах економічної інтеграції Україні до ЄС.

Мета статті є встановлення довірчих відносин у сфері інтеграції національних електронних комунікацій до світових тенденцій для забезпечення єдиного інформаційного простору, розвитку інвестицій, упровадження інновацій та підвищення якості життя і послуг.

В основу національного законодавства забезпечення впровадження ЕЦП закладено такі основні принципи:

– відсутність дискримінації електронної форми документа щодо його паперової форми;

– визначення загальних правил і умов прирівнювання ЕЦП до власноручного підпису;

– можливість на договірних основах визначати інші умови застосування й визнання ЕЦП, ніж ті, які визначені законом;

– добровільна акредитація провайдерів послуг із сертифікації ключів;

– створення системи контролю над діяльністю інфраструктур сертифікації ключів.

Відповідно до прийнятої системи сертифікації ключів законодавством застосовано гнучкий підхід у питанні юридичної сили ЕЦП і прирівнювання її до власноручного підпису. На підставі цього підходу можливі дві основні схеми правових взаємин у разі використання ЕЦП:

1) за використання посиленого сертифікату АЦСК – ЕЦП автоматично прирівнюється в юридичній силі до власноручного підпису, і попередній вступ до договірних відносин суб'єктів електронного документообігу про визнання ЕЦП один одного не є обов'язковим;

2) за використання механізмів ЕЦП на основі сертифікатів ключів ЦСК або без використання їхніх послуг правові взаємини регулюються цивільно-правовими договорами між суб'єктами електронної взаємодії, в яких обумовлюється порядок визнання юридичної сили електронного документа і власноручного підпису.

Гарантоване забезпечення рівня довіри і надійності до НСЕЦП у контексті цих правових взаємин вимагає строгого опису і підтримки політик безпеки, створення інтелектуальних систем, здатних аналізувати, порівнювати і виконувати різновиди політик безпеки згідно з вимогами забезпечення транзакцій у процесі електронного урядування.

Одна зі складових політики безпеки є політика підписання – набір правил для створення і валідації ЕЦП, використовуючи який, ЕЦП можна визначити як валідною (дійсною, підленною). Політику підписання потрібно відрізняти від іншої складової політики безпеки – політики сертифікації, що містить правила, які серед іншого визначають, яка політика сертифікації прийнятна під конкретною політикою підписання.

Політика підписання як механізм дозволяє пов'язати значущість документа з ЕЦП, таким чином підвищуючи довіру і надійність процесу електронного урядування.

Оскільки політика підписання може задавати вимоги, що асоціюються з трансакціями електронного урядування, необхідно пов'язати її зі специфічними базовими елементами політики підписання, призначеними для такої формалізації. Контекст транзакції може включати комерційний, адміністративний, приватні аспекти або їх комбінації. Контекст транзакції визначає загальні прийнятні правила, що асоціюються з процедурами підписання. Такі правила можуть статися зі станів, наприклад дія має бути зроблена при заповненні певної форми згідно з корпоративними умовами.

Наприклад, центри сертифікації ключів в Україні продають клієнтам ЕЦП, що асоціюються з різним рівнем криптозахисту і, зрозуміло, з різною вартістю: електронна печатка компанії, ЕЦП менеджера компанії, бухгалтера і інших

службовців. Зрозуміло, види електронних документів, що витікають з компанії, слід підписувати різними ЕЦП згідно зі строгими процедурами організації електронного документообігу як основи політик підписання.

Один з недоліків національної реалізацій ЕЦП – відсутність прямого зв'язку семантики процесів електронного урядування з ЕЦП, оскільки семантика розпізнається побічно, через контекст транзакції. Такий механізм недопустимий у системах з підвищеними вимогами до надійності і безпеці транзакцій, наприклад, державних закупівель, банківських транзакцій тощо.

Для прив'язки семантики до додаткових правил верифікації (перевірка істинності) і валідації ЕЦП розроблена концепція політики підписання, що передбачає її різновиди.

Національні політики підписання – досі слаборозвинене поле, в першу чергу зважаючи на нечіткість кордонів їх використання і недоліки досвіду стандартизації. А механізм опису політики підписання – критично важливий інструмент для підтримки валідації ЕЦП на етапі підписання і прив'язки чіткого семантичного навантаження ЕЦП.

Другим із недоліків НСЕЦП є невизначеність механізмів внутрішньої і зовнішної крос-сертифікації ЦСК для забезпечення довіри між користувачами різних систем. На національному рівні забезпечення крос-сертифікації із закордонними системами законодавча надано ЦЗО, а внутрішня крос-сертифікація між ЦСК відсутня, що привело до відомчого формування розрізнених НСЕЦП. У результаті користувачі зобов'язані використовувати ключі за кожним відомством, що стримує розвиток систем електронної взаємодії.

Аналіз існуючих моделей організації взаємодії органів сертифікації (CA – Certification authority) QPKI дозволив виділити основні механізми довіри в інфраструктурі відкритих ключів: ізольований, кореневий, мережевий, шлюзовий, списком статусу, списком сертифікатів та управління якістю сертифікатів.

Ізольований – це механізм довіри на основі самопідписаного сертифікату CA (self-signed CA-certificate), який не завіряється будь-яким іншим CA. Шлях сертифікації в цьому випадку дорівнює двом рівням, тобто CA-сертифікат та сертифікат користувача цього CA.

Прикладом організації такої інфраструктури використання сертифікатів і ключів може послужити досвід співтовариства S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication – Товариство Світових Міжбанківських Фінансових Телекомунікацій). Це некомерційна акціонерна структура, яке не є платіжною системою і надає телекомунікаційні послуги різним національним і міжнаціональним платіжним системам, банкам, біржам, корпораціям та іншим нефінансовим організаціям. Користувачі об'єднані в єдину закриту мережу з використанням служби SWIFTNet, через яку виповняються трансакції фінансових операції [3]. В основі захисту інформації в SWIFT лежить принцип використання асиметричного алгоритму RSA, при якому використовуються дві пари особистих і відкритих ключів, які заздалегідь засвідчуються SWIFT. Одна пара (особистий + відкритий) використовується для ЕЦП у фінансових трансакціях, друга – для їх шифрування.

Кореневий – це механізм довіри на основі ієрархічно засвідчувального ланцюгу сертифікатів від кореневого СА до кінцевого підлеглого СА, за якими будується довіра до сертифікатів кінцевих користувачів підлеглих СА (шлях сертифікації починається з трьох рівнів – кореневий, підлеглий (може бути декілька), користувач). У декількох країнах засновано загальний кореневий СА: у Германії RegTP (лише для акредитованих провайдерів послуг сертифікації), в Нідерландах (лише для урядового використання), в Польщі, Бельгії і Україні [5]. У банківській системі електронних платежів (СЕП) Україні використовується чотирирівнева ієрархія сертифікації ключів: ЦЗО, засвідчувальний центр Національного банку України (ЗЦ НБУ), ЦСК або АЦСК, кінцевий користувач. У державному управлінні (подання електронної звітності) упроваджена трирівнева ієрархія: ЦЗО, АЦСК, користувач.

Описана ієрархічна модель PKI, України визначає довірчі відносини лише в одному напрямі – згори – вниз. Підлеглі СА не випускають сертифікатів своїх вищестоящих СА і вищестоящий СА нав'язує умови підлеглим СА, що стосується політики сертифікації. Держави ЄС однозначно відмовилися від цієї моделі, в Україні вона доречна, зважаючи на свою тривіальність і відсутність корисного досвіду реалізації PKI як у розробників, так і у клієнтів ЦСК. Європейський досвід у процесі реалізації бізнес-додатків орієнтується на визначення безпосередньо надійних СА, замість того, щоб покладатися на автоматизований ланцюжок сертифікатів, який є грубим механізмом для визначення надійності і статусу СА, що видає сертифікати.

Мережевий – це механізм установлення довірчих взаємин між рівноправними СА (СА-доменами) на основі взаємної крос-сертифікації без довірчого посередника, тобто СА випускають сертифікати один одному, і така пара сертифікатів описує їх двосторонні відносини довіри. Проте кожному СА необхідно встановити таки відносини з усіма іншими СА, що нагромаджує схему взаємодії кожного СА. Через це мережеві механізми довіри найбільш ефективні на верхніх рівнях ієрархії, коли необхідно організувати крос-сертифіковану взаємодію між декількома учасниками, наприклад країнами союзу або структурами суспільства.

Для розвантаження мережевої схеми взаємодії, з одного боку, і відходу від жорсткої ієрархії – з іншого, використовують шлюзові механізми довіри. У цій схемі технологія забезпечення довіри будується через єдиний вузол довіри – шлюзовий СА, якій бере на себе функцію крос-сертифікації кінцевих СА. При цьому користувач використовує власний СА як якір довіри і будує ланцюжок довіри сертифікатів від власного СА, через шлюзовий СА, до сертифікату будь-якого другого кінцевого користувача.

Нині реалізовані відомі проекти: шлюзовий СА (bridge/gateway CA – BGCA) у рамках програми IDABC для використання державними адміністраціями держав-членів ЄС і Федеральний єднальний засвідчуючий орган (FBCA) США. Для України актуальний досвід BGCA, оскільки він створений згідно з положеннями Директиви 1999/93/ЕС, зокрема відносно управління посиленими сертифікатами відкритих ключів. Уже розроблено ряд нормативних документів

(зокрема ETSI TS 102 231 v3.1.1 від 2009 р.) для проведення крос-сертифікації і раціональні технологічні схеми організації трансграничного визнання сертифікатів і архітектурної моделі національного шлюзового СА. Ці схеми повною мірою підходять для організації відносин НСЕЦП України з BGCA в рамках програми IDABC електронної взаємодії адміністрацій країн – членів ЄС.

Слід зазначити, що шлюзовий СА не вирішує потреби в детальній інформації про статус окремого СА. Для вирішення цієї проблеми використовують модифікацію шлюзового СА, який підтримує механізм довіри списком статусу. Список статусу довіри – це підписаний список даних про СА і його статус. Реалізація даного механізму використовується на основі захищеного он-лайн-протоколу OCSP (Online certificate status protocol), за допомогою якого з сервера підтверджуючого органу (VA) запрошується статус сертифіката, що перевіряється. Для збору потрібної інформації VA повинен опитувати інші сервери, можливо, розташовані в інших державах-членах, тому доцільний центральний VA, аби забезпечувати інформацією підтвердження кожен сервер.

Механізм довіри зі списком сертифікатів, оснований на моделі довіри Web/ Інтернета і на списках CTL (Certificate trust list) довіри сертифікатів, які підписані структурами даних PKCS #11. PKCS#11 (Public-Key Cryptography Standard #11), це платформо незалежний програмний інтерфейс для роботи з апаратнореалізованими ЗКЗІ (засоби криптографічного захисту інформації): криптографічні токени (token – флеш-пам'ять), смарт-картки, HSM (Hardware Security Module – пристрої для зберігання ключів). Інколи PKCS#11 використовується для доступу до програмно реалізованих криптографічних бібліотек.

У PKCS#11 чітко прописані правила (набір функцій, механізмів, алгоритмів і їх параметрів для роботи з криптографічними пристроями або бібліотеками), відповідно до яких працюватиме прикладне програмне забезпечення при виклику криптографічних функцій за стандартом підпису RSA. Даний стандарт підтримується в багатьох OpenSource-проектах, у тому числі проектах компанії Microsoft, що використовують криптографію. З метою уніфікації доступу до криптографічних функцій компанія Microsoft розробила пропрієтарний інтерфейс програмування додатків (API): Microsoft Crypto API, який базується на використанні криптопровайдерів. Специфікації Crypto API описують набір функцій, які повинна надавати бібліотека криптопровайдера операційної системі, способи інтеграції з нею і специфікації викликів. Отже, національні виробники ЗКЗІ, що виконують правила Crypto API, мають можливість інтеграції свого рішення в операційну систему Microsoft Windows, а прикладне програмне забезпечення реалізує доступ до криптографічних функцій за допомогою уніфікованого інтерфейсу.

Багато держав – членів ЄС зацікавлено у використанні CTL як альтернативному механізмі крос-сертифікації в мережевих моделях, маючи можливість зберегти контроль над тим, яким сертифікатам вони довіряють. Також CTL містить ідентифікатори політик безпеки і підтримують розширення. З позицій внутрішньодоменної інтероперабельності по суті CTL замінює пари крос-

сертифікатів, тобто конкретна сторона довіряє видавцеві CTL, значить, довіряє CA, вказаному в CTL.

Нарешті, механізм управління якістю сертифікатів упроваджується як результат модифікованої моделі BGCA, тобто комбінації моделі довіри Web/Інтернету і моделі шлюзового CA. Причому держави-члени можуть доповнювати цю інфраструктуру відкритим для держслужбовців національним засвідчуючим органом, якщо це допускають технічні можливості.

Названа модифікація забезпечує реалізацію таких можливостей: шлюзовий CA розподіляє список CTL надійних кореневих сертифікатів, що виконують загальні вимоги, і підписує список довірчих сертифікатів своїм сертифікатом; деякі держави-члени просто на довірі сприймають цей список, а інші держави-члени можуть створювати власний список коріння, якому вони довіряють, видаляючи деякі сертифікати і перепідписуючи оновлений список власними сертифікатами.

Таким чином, за результатами проведених досліджень визначено структуру політик безпеки (політика підпису, політика сертифікації) та основи механізми довіри в інфраструктурі відкритих ключів: ізольований, кореневий, мережевий, шлюзовий, статусом довіри, списком сертифікатів та управління якістю сертифікатів.

Основна проблема впровадження запропонованих механізмів довіри в НСЕЦП пов'язана з неінтероперабельністю електронної цифрової підписі до QPKI. Базовою складовою кваліфікованих підписів ЄС є комплекти підпису, які складаються з трьох елементів: геш-функція, метод доповнення, алгоритм підписування з широким набором параметрів. Геш-функція пов'язана зі схемою підписування і забезпечує підписування документів довільної довжини, а її вибір встановлюється потрібним рівнем безпеки. Метод доповнення залежить від обраного алгоритму підписування. Зокрема алгоритми за міжнародним стандартом DSA, ECDSA, ECGDSA не потребують доповнення, а алгоритм RSA потребує нетривіального доповнення для завдання методу кодування документу в цілочислове подання.

Комплекти підпису будують за модульним принципом, що сприяє розвитку конкуренції серед розробників компонентів. При цьому для побудови надійних ЕЦП необхідно використовувати тільки у визначених комбінаціях сертифіковані комплекти підпису.

Проте в Україні не регламентовано використання й опис компонентів підпису. Унаслідок цього засоби ЕЦП будуються під ключ без організації їх модульної структури на основі національних алгоритмів підписування й геш-функції, які не дають змоги крос-сертифікуватися з жодною країною світу.

Також національна система ЕЦП неінтероперабельна через відсутність профілів (єдиного набору опцій) на два базових криптоалгоритму: ДСТУ 4145-2002 і ГОСТ 34.310-95, відсутність стандартів на формати їх базових компонентів, невідповідність міжнародному стандарту формату сертифіката на ЕЦП, що існує, відсутність органу штемпелювання часу. Упровадження же прийнятих у 2009 р.

на Україні сучасних європейських стандартів ETSI у сфері електронних підписів і розвитку їх інфраструктури обмежено структурою PKI, що діє.

У цих умовах потрібно комплекс організаційно-технологічних заходів і технічний регламент для запровадження європейської системи QPKI.

Поки НСЕЦП неінтероперабельна з організаційних причин, переважно через слабку координацію дій ЦЗО та контролюючого органа як головних суб'єктів Закону України про електронний цифровий підпис.

Головними завданнями цих органів є запровадження крос-сертифікаційних механізмів у політику підпису, задіювання жорсткої процедури акредитації, яка відкидає неінтероперабельні реалізації програмно-технічних комплексів, бібліотек, сприяння розвитку системи незалежних оцінщиків, упровадження сучасних тестових стендів для контролю базових показників політики безпеки, ініціювання нової редакції Закону України про ЕЦП для введення сертифікатів відповідності в визнанні зрілості всіх складових НСЕЦП у замін діючого лише на території України позитивного експертного висновку та підпису міждержавної угода з ЄС про взаємне визнання цих сертифікатів відповідності.

Література:

1. *Бєлов С. В.* Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики / С. В. Бєлов, С. В. Мартиненко // Зб. наук. праць ІПМЕ ім. Г. Є. Пухова, НАН України. – 2005. – Вип. 28. – С. 68–79.

2. *Горбенко Ю. І.* Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія / Ю. І. Горбенко, І. Д. Горбенко. – Х. : Форт, 2010. – 608 с.

3. *Левшаков С. Ф.* Проблеми становлення інфраструктури електронних цифрових підписів в банківській системі України / С. Ф. Левшаков // Вісник Української академії банківської справи. – 2010. – № 2. – С. 80–85.

4. *Мелащенко А. О.* Проблемы интероперабельности Национальной системы электронных цифровых подписей / А. О. Мелащенко, О. Л. Перевозчикова // Кибернетика и системный анализ. – 2009. – № 3. – С. 55–63.

5. *Мелащенко А. О.* Кроссертификация Украины / А. О. Мелащенко, О. Л. Перевозчикова // Проблемы программирования. – 2010. – № 2–3. – С. 299–308.

6. *Савченко А С.* Електронна Україна: міф чи реальність? / А. С. Савченко, І. С. Івченко // Вісник НБУ. – 2010. – № 3 (169). – С. 3–6.

7. *Степаненко В.* Электронная цифровая подпись / В. Степаненко // Сети и бизнес. – 2006. – № 6 (31). – С. 82–91.

Надійшла до редколегії 18.02.2013 р.