

Костенко О.В.^{1,2} Капшук О.О.²

¹Міністерство юстиції України, Київ, Україна; ²Інститут прикладного системного аналізу НТУУ "КПІ", Київ, Україна

Проблеми інтероперабельності Національної системи електронного цифрового підпису в Україні та шляхи їх вирішення

Метою роботи є дослідження проблем створення інтероперабельної Національної системи електронного цифрового підпису в Україні (НСЕЦП) та інтеграції її з Європейським та світовим співтовариством. Для інтеграції та вигідної співпраці України з Європейським та світовим співтовариством, з метою євроінтеграції та розвитку експорту продукції всіх вітчизняних галузей виробництва, необхідно запровадити в нашій державі відповідні норми ООН, СОТ та ЄС, забезпечивши технологічну та юридичну підтримку при обміні електронними документами, засвідченими електронним цифровим підписом. Однією з ключових проблем, які постали сьогодні перед державою у сфері надання послуг електронного цифрового підпису (ЕЦП), є відсутність інтероперабельності Національної системи електронного цифрового підпису як у межах України, так і з іншими державами [1].

Слід значити, що інтероперабельність становить одну із найважливіших властивостей відкритих систем, і в даний час все більша увага приділяється саме питанням забезпечення інтероперабельності для інформаційних систем (ІС) різного масштабу і призначення (від пано- до GRID і більш складних систем) і НСЕЦП, зокрема. Тривалий час регулювання у сфері ЕЦП здійснювалось в «ручному режимі», а просування нових форматів і технологій було ситуативним, що спричинило технологічну несумісність програмно-технічних комплексів, нерівнозначність різних електронних цифрових підписів у системі та унеможливило інтеграцію до європейської системи електронного цифрового підпису.

З розвитком програми електронного урядування 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 довіри між центрами сертифікації ключів іноземних держав (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 зальоєвропейській (pan-European) державній мережі.

Майбутнє розширення сфери використання ЕЦП в Україні та відповідне зростання кількості користувачів ставить також завдання кластеризації (спеціальні програмно – апаратні рішення для балансування навантаження доступу користувачів, підвищення доступності та зменшення часу відгуку), надійності, резервування до обладнання центрального засвідчувального органу. Ці завдання одночасно із створенням спеціального депозитарію списків довіри, а також веденням бази сертифікатів та списків відкликаних сертифікатів пропонується вирішувати в межах функціонування Довірчого Центру Міністерства юстиції України. До завдань, які вимагають виконання, для вирішення проблеми інтероперабельності НСЕЦП можна віднести необхідність вироблення єдиного підходу до її забезпечення шляхом створення єдиної технічної, організаційної та інтеграційної моделі НСЕЦП, уніфікації термінології та ключових інтерфейсів, визначення ключових інтерфейсів (об'єктів) стандартизації, а також створення нормативно-технічних документів, стандартів, профілів, рекомендацій, методик, правил тощо.

В роботі розглядаються алгоритми функціонування одного із ключових елементів в структурі сучасної інтероперабельної НСЕЦП (рис.1) - довірчого центру (ДЦ) міністерства юстиції, який сприятиме досягненню сумісності технічних рішень у сфері використання електронного цифрового підпису шляхом технологічної уніфікації компонентів НСЕЦП з використанням як міжнародних стандартів з національними особливостями, так і вітчизняних національних стандартів, а також взаємного визнання сертифікатів за двосторонніми та багатосторонніми угодами.

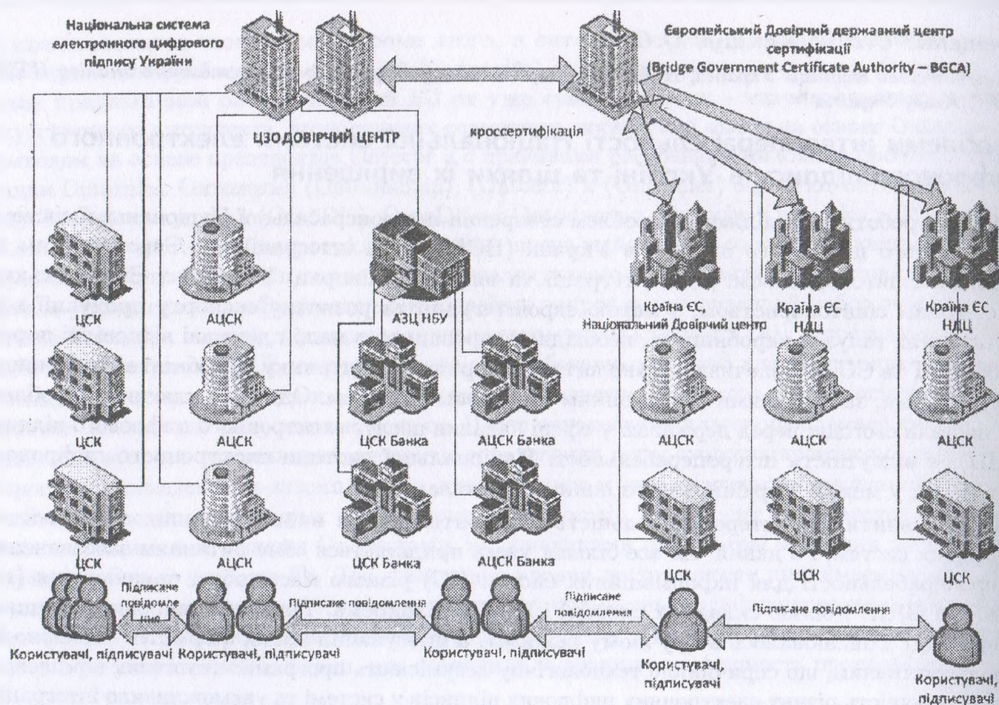


Рис. 1. Національна система електронного цифрового підпису України (ЦЗО - центральний засвідчувальний орган, АЦСК - акредитований центр сертифікації ключів, ЗЦ - засвідчувальний центр, АЗЦ - акредитований засвідчувальний центр)

Довірчий центр повинен забезпечити:

- випуск перехресних кросс-сертифікатів, обмін і оновлення належним чином сертифікатів з «Головним ЦСК» кожного члена РКІ;
- регулярне розсилання сертифікатів «Списків довіри» членам РКІ;
- ведення служби каталогу (репозиторію) випущених головних сертифікатів кожному члену РКІ, а також відповідні Списки анулювання сертифікатів, які потрібно регулярно оновлювати;
- підтримання веб-вузла, що публікує меморандуми та інші документи щодо політик;
- on-line квітування статусу сертифікату через OCSP (Online Certificate Status Protocol);
- технічні інтерфейси взаємодії з Довірчим Центром;
- базові основи тестування інтерфейсу з вузлом BGCA, призначенні для нових претендентів на підключення.

Таким чином, Довірчий Центр Міністерства юстиції України об'єднує не тільки суб'єктів Національної системи електронного цифрового підпису але й вирішить головне питання інтегрованості - адаптацію НСЕЦП України в європейську та світову систему електронного документообігу та електронного цифрового підпису.

Література. 1. Мелашенко А. О., Перевозчикова О. Л. Проблемы интероперабельности Национальной системы электронных цифровых подписей // Кибернетика и системный анализ. - 2009. - № 3. - с. 55-63.