Аналітика 2011. Сучасний стан цифрового підпису в Україні

к.ф.-м.н. Мартиненко С.В.
Белов С.В.

З часу прийняття Закону України «Про електронний цифровий підпис» (надалі - ЕЦП) минуло більше 8-ми років. В електронному світі – це термін життя одного покоління. Отже, маючи вже досить зрілий вік, ЕЦП в Україні вже досягнуло рівня зрілості та мудрості? Зробимо аналіз сучасного стану ЕЦП в Україні у таких площинах:

- Законодавство;
- Стандартизація;
- Сучасна практика ЕЦП.

Законодавство

Ще на етапі проекту Закону про ЕЦП Міністерством юстиції надано висновок, відповідно до якого цей проект було розроблено з порушенням вимог Тимчасового регламенту Кабінету Міністрів України. Оскільки предмет правового регулювання цього проекту закону віднесено до пріоритетних сфер адаптації законодавства України до законодавства ЄС і він був внесений до Плану роботи з адаптації законодавства на 2000 рік, головний розробник відповідно до пункту 14 розділу 6 Тимчасового регламенту Кабінету Міністрів України був зобов'язаний перевірити цей проект на відповідність основним положенням законодавства ЄС у порядку, передбаченому пунктами 27-29 цього ж розділу Тимчасового регламенту. Така перевірка в порушення вимог Тимчасового регламенту не була проведена і результати перевірки проекту не були відображені у довідці про його відповідність основним положенням законодавства ЄС, яка повинна подаватися головним розробником до Мінюсту разом із проектом Закону.

На етапі проекту Закону про ЕЦП нами також були надані зауваження до проекту, де, зокрема, зазначено, що викладена у пояснювальній записці до проекту закону думка головного розробника про те, що „… *створити проект Закону України про цифровий підпис, який би повністю відповідав вимогам законодавства ЄС, неможливо*” є необгрунтованою та абсолютно безпідставною. Окремі надані до проекту зауваження були враховані під час другого читання, але в цілому **Закон про ЕЦП і на поточний момент не відповідає законодавству ЄС**, зокрема:

- Директиві Європейського Парламенту та Ради Міністрів ЄС 1999/93/ЄС від 13.12.99 р. щодо системи електронних підписів Європейського Співтовариства (далі - Директива 1999/93/ЄС); далі – **Директива ЄС**;
- Рішенню Комісії 2000/709/ЄС Європейського парламенту та Ради від 6 листопада 2000р. Про мінімальні критерії, які враховуватимуться Державами-членами під час визначення органів, згідно статті 3(4) Директиви 1999/93/ЄС Європейського парламенту та Ради про систему електронних підписів, що застосовуються в межах Співтовариства, Офіційний журнал L 289, 16.11.2000 с.42; далі - **Рішення Комісії ЄС.**

Підкреслимо лише одну з ключових проблем – невідповідність національного терміну «посилений» (а отже і суті безпеки цифрового підпису) до терміну (і чітких вимог) «advanced electronic signatures» (посилений електронний підпис) Директиви ЄС. Тобто безпека ЕЦП в Україні, що базується на посилених сертифікатах, не відповідає (а саме - нижче) рівню безпеки цифрового підпису в ЄС. А отже, і правовий статус ЕЦП України, виконаний з використанням «посиленого сертифікату», не відповідає правовому статусу посиленого (advanced) цифрового підпису в ЄС, виконаного з застосуванням кваліфікованого сертифікату ЄС (qualified certificate).

Невже й на сьогодні комусь вигідно підтримувати твердження, що «„… *створити проект Закону України про цифровий підпис, який би повністю відповідав вимогам законодавства ЄС, неможливо*”?

Стандартизація

Стандартизація є головним чинником як надійності/ безпеки, так і сумісності рішень різних виробників, а отже «прозорого» використання цих рішень у великих системах електронного документообігу (платежів, звітності, електронних послуг тощо).

Стандартизація - це складова частина політики Ради і Комісії ЄС, щоб здійснювати краще регулювання, збільшувати конкурентоспроможність підприємств і виключати бар'єри в торгівлі як на міжнародному, так і внутрішньому ринку товарів та послуг:

- Резолюція Ради "Роль стандартизації в Європі" від 28 жовтня 1999, OJ C141 2000 05-19;
- Рішення Ради із стандартизації від 2002-03-01, OJ C66 2002-03-15.
- Повідомлення Комісії до Європейського Парламенту та Ради про роль європейської стандартизації у структурі європейських політик і законодавства, Brussels, 18.10.2004, COM(2004) 674 final.

Як зазначено у Повідомлення Комісії COM(2004)674, Комісія продовжуватиме просувати міжнародні стандарти, прийняті міжнародними органами стандартизації (ISO, IEC, ITU) і підтримувати їх трансформацію в ЄС. Одним із пріоритетних напрямків стандартизації ЄС є інформаційно-телекомунікаційні технології.

Таким чином, стандартизації в галузі ЕЦП слід приділяти значну увагу, як пріоритетному напрямку стандартизації ЄС. Це повинно реалізовуватися через:

- Адаптацію (прийняття) в Україні відповідних міжнародних та європейських стандартів (це близько 40 стандартів);
- Прийняття технічних специфікацій щодо застосування національних криптографічних алгоритмів (ДСТУ 4145-2002, ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-85).

Необхідність технічних специфікацій випливає з того, що діючі національні стандарти з криптографічних алгоритмів відрізняються від міжнародних, і тому прийняття міжнародних стандартів в деяких випадках потребує уточнень, які врегульовуються вказаними технічними специфікаціями.

За період розвитку ЕЦП в Україні було зроблено станом на поточний момент:

- 5-ть Технічних специфікацій;
- Адаптовано кілька десятків міжнародних та європейських технічних стандартів.

Звичайно, що цих заходів занадто мало, а тому голову ціль «виключати бар'єри» (досягти сумісності рішень) не було досягнуто (про це детальніше буде сказано нижче).

Відповідно до Указу Президента України «Про затвердження Положення про Міністерство юстиції України» від 6 квітня 2011 року №395/2011З 2001 року на поле «гри» ЕЦП вийшов новий учасник – Міністерство юстиції України. І тут згідно з класикою жанру «у семи няньок …» новий учасник відміняє усі прийняті Технічні специфікації, нічого не надаючи натомість – тепер кожен може «грати» як він це розуміє?...

Питання, чи збільшить це рівень стандартизації, можна і не ставити – відповідь очевидна!

Друге питання, яке виникає: чи є в Міністерство юстиції України відповідного рівня фахівці, які будуть (відповідно до зазначеного Указу, п.4, 65):

«забезпечувати розроблення норм, стандартів і технічних регламентів у сфері електронного цифрового підпису;».

Третє питання: яка роль (щодо норм, стандартів і технічних регламентів) залишається у *спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації,* який відповідає за криптографічний захист інформації, тобто і цифровий підпис у тому числі? Причому враховуючи, що це прямо визначено у діючому Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»?

Отже, через вісім років «зростання» ЕЦП в Україні питань із стандартизації не стало менше.

Сучасна практика

Сучасна практика є дзеркалом законодавства та стандартизації. Щоб це показати, розглянемо кілька ключових питань.

1. Чи є сумісними різні рішення, що відповідають прийнятим свого часу (і відмінених тепер) Технічних специфікацій? Відповідь: НІ.

Причина – недостатній рівень прийнятих свого часу Технічних специфікацій, та недостатня їх кількість взагалі (не охоплювали усі питання, які вимагаються для сумісності). Відмінені Технічні специфікації, звичайно, є кроком уперед на шляху стандартизації, адже навіть повне прийняття (адаптація) міжнародних/ європейських технічних стандартів не може забезпечити сумісність, бо національні стандарти в них жодним чином не відображені. А отже, технічні особливості національних стандартів можуть і повинні бути відображені у окремих Технічних специфікаціях. Таким чином, Технічні специфікації обов'язково повинні бути затверджені, але, що також обов'язково, із внесенням відповідних правок.

Слід зазначити ще один суттєвий фактор сумісності – це якість тестування (експертизи) рішень. Якість тестування досягається якістю методик тестування.

Для прикладу, одна із найбільш поширених сьогодні методик тестування правильності реалізації цифрового підпису ДСТУ 4145-2002 містить 266 тестових векторів, але:

- із 266 тестових векторів реально використовуються лише 153 вектори для поліноміального базису, так як операції в оптимальному базисі майже ніхто не реалізує (чи обов'язковим це є для реалізації, - невідомо);
- усі 153 вектори використовують лише дві стандартизовані для реалізації криві (із десяти, які повинні реалізовуватися), а тому сумісність на інших восьми кривих не гарантується;
- зовсім відсутні будь-які тести структури/ форматів відкритих ключів у двох системах кодування (Big-Endian, Little-Endian);
- майже відсутнє тестування ГОСТ 34.311-95, що реалізується для цифрового підпису з ДСТУ 4145-2002
- та інш.

Це є наслідком того, що методики тестування не є предметом стандартизації – кожна тестова лабораторія розробляє власні тести, не маючи жодних обов'язкових чи рекомендованих мінімальних вимог. Для прикладу, американський інститут NIST розробляє та публікує тестові вектори для перевірки реалізації крипто алгоритмів, що можна розглядати як мінімальні вимоги. Чи не слід в Україні запровадити такий підхід?

Те саме стосується й тестування на відповідність Технічним специфікаціям (які донедавна існували). На жаль, рівень такого тестування ще нижчий, ніж тестування на відповідність стандартам. Так зокрема, відомим є той факт, що такий поважний в Україні орган, як «Центральний засвідчу вальний орган», тривалий час (до 2011 року) «працював», формуючи списки відкликаних сертифікатів з помилками ASN.1 структури, що не давало можливості скористатися цими списками взагалі.

Відсутність певних Технічних специфікацій створює взагалі хаос у використанні засобів ЕЦП. Так, одним з ключових питань засобів криптографічного захисту інформації (КЗІ) є безпечне зберігання та використання закритих/ секретних ключів (цифрового підпису, шифрування тощо). На поточний момент в Україні не існує жодних вимог (Технічних специфікацій чи адаптованих/ рекомендованих стандартів) з цих питань. А тому кожен розробник засобів КЗІ створює сховище ключів на свій розсуд (як він розуміє). Кожен розробник засобів КЗІ створює функції використання ключів (такі, як підписати, зашифрувати тощо) на свій розсуд (як він розуміє) із власним форматом та власною назвою цієї функції, і т.д.

Поглянемо на це з точки зору прикладних програм, наприклад, електронна звітність, яка повинна обробляти цифрові підписи різних розробників. Така прикладна програма повинна:

1. Працювати із сховищами ключів кожного розробника КЗІ (створеного на його «розсуд»).
2. Працювати (викликати, передавати параметри, отримувати результат) із функціями використання ключів кожного розробника КЗІ (створеного на його «розсуд»).
3. У разі виходу на ринок послуг нового розробника КЗІ додавати до прикладної програми нові модулі цього розробника, та відповідно тестувати тощо, і головне – надати усім користувачам нову версію прикладної програми.

Як видно, процес нескінчений.

Крім того, використовуючи зазначені проблеми із додаванням до прикладної програми електронної звітності модулів нового розробника КЗІ, власник/ замовник/ розробник цієї прикладної програми може легко «не допустити» нові засоби КЗІ до впровадження, у тому числі, із конкурентних та/чи корупційних підстав.

Чи можна ліквідувати цей хаос у використанні засобів ЕЦП різних виробників? Так!

Загальновизнаним універсальним засобом взаємодії прикладних програм із засобами КЗІ (як програмними, так і апаратними) є використання міжнародного стандарту PKCS#11. Цей стандарт слідує об'єктно-орієнтованому підходу, відповідає цілі незалежності від технології (від будь-якого типу пристрою) та відповідає цілі спільного використання/ розподілу ресурсів (доступ декількох прикладних програм до декількох пристроїв), надаючи прикладним програмам загальний абстрактний пристрій під назвою «криптографічний токен».

Прийняття Технічної специфікації відповідно до стандарту PKCS#11, та визначення її як обов'язкової для усіх систем електронної звітності дозволить припинити хаос у використанні засобів ЕЦП.

2. Як сьогодні на практиці державні органи працюють із створення електронної звітності.

Чи забезпечують державні органи, які, працюють з електронною звітністю, здійснювати краще регулювання, збільшувати конкурентоспроможність підприємств і виключати бар'єри в торгівлі як на міжнародному, так і внутрішньому ринку товарів та послуг?

Для прикладу розглянемо систему електронної звітності Державної податкової адміністрації України (ДПА).

Як державний орган, ДПА повинно працювати лише з акредитованими центрами сертифікації ключів (ЦСК). Таких на поточний момент 18 (станом на 20.09.2011), але ДПА працює лише з 5-ма (http://www.dpi0609.houa.org/elzvit/elzvzv.htm#zak5). Про причини такої «вибірковості» сказано вище.

Для роботи з різними ЦСК ДПА використовує «шлюз», який «розуміє» підключені до нього ЦСК. Фактично, цей шлюз є програмно-фізичним поєднанням сховищ ключів та бібліотек функцій різних виробників КЗІ.

На перший погляд (не спеціаліста з цих питань), усе ніби то урегульовано - затверджено «Уніфікований формат транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису» (наказом ДПА України від 12.07.2010 № 499). Отже, достатньо виконати вимоги «Уніфікованого формату»? Так, але трошечки не так.

В «Уніфікованому форматі» сказано, що:

- Уніфікований формат транспортного повідомлення для обміну інформацією між платниками податків і податковими органами в електронному вигляді з використанням електронного цифрового підпису (далі – Уніфікований формат транспортного повідомлення) застосовується для організації обміну електронними документами між платниками податків і податковими органами безпосередньо і телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису (далі – ЕЦП).
- Обмін електронними документами здійснюється за допомогою транспортного повідомлення (далі – ТП), складається з реквізитів ТП та транспортного контейнера, що містить зашифровані дані (електронні звіти, квитанції тощо).

Але технічний формат електронного цифрового підпису (далі – ЕЦП) та технічний формат зашифровані дані не визначено. Існує дві групи стандартизованих міжнародними стандартами форматів підписані та зашифровані дані – це ASN.1 формат та XML формат, у який є «під-формати» (attached, detached, enveloped, enveloping …). Який же із них треба реалізувати для «Уніфікованого формату»?..

По-друге, у п.2. («Вимоги до криптографічного захисту інформації») наказу ДПА сказано, що криптографічні перетворення виконуються засобами систем криптографічного захисту інформації (СКЗІ), які повинні відповідати таким вимогам:

- реалізовувати процедури формування й перевірки ЕЦП відповідно до національного стандарту ДСТУ 4145-2002;
- реалізовувати процедури відкритого розподілу ключів відповідно до національного стандарту ДСТУ ISO IEC 15946-3:2006;
- реалізовувати процедури симетричного шифрування відповідно до регіонального ГОСТ 28147-89;
- бути сертифікованими відповідно до законодавства України.

Очевидно, що ці «вимоги» виписані для «аби було хоч щось», бо ДСТУ ISO IEC 15946-3:2006 не містить єдиного конкретно визначеної «*процедури відкритого розподілу ключів*». Маємо те ж саме питання: Яку ж із них треба реалізувати для «Уніфікованого формату»?..

По-третє, вимоги, викладені офіційно у наказі ДПА, не відповідають дійсності. Зокрема, фактична структура *UACertInfo* відрізняється від описаної у специфікації (http://www.sta.gov.ua/control/uk/publish/article?art_id=249334&cat_id=249325), та містить ще (додатково) параметр ***Issuer*.** Також відрізняється функція створення підпису *MakeSign* (додатку 3 наказу ДПА)**,** яка в специфікації має 6 параметрів, а фактично їх 7. Не відповідає і функція перевіряння підпису *VerifySign* (додатку 3 наказу ДПА), і т.д. і т.п.

По-четверте, у п.2. наказу ДПА вимагається: функції бібліотек криптографічних перетворень, що надаються центрами сертифікації ключів для інтеграції у систему приймання та обробки податкової звітності, повинні відповідати специфікаціям криптографічних перетворень, викладених у додатку 3 (наказу ДПА).

Звернімося до додатку 3 (наказу ДПА). Зазначені в Уніфікованому форматі функції **не повинні допускатися до застосування як криптографічно небезпечні**. Так зокрема, функція

накладання підпису повинна отримати «секретний ключ» (йдеться певно про особистий ключ, бо термін «секретний ключ» відсутній для алгоритму підпису, а є в алгоритмах шифрування). Отже, будь-який розробник прикладного програмного забезпечення (у даному випадку – податкової звітності) може мати доступ до особистого ключа підписувала, що є неприпустимим.

Практика показує, що для того, щоб досягти кінцевого результату – забезпечити обробку документів податкової звітності в електронному вигляді шлюзом ДПА, необхідно виконати вправу «поклон до самої землі» декілька разів: спершу – для отримання реальних технічних специфікацій «Уніфікований формат транспортного повідомлення..», які відповідають діючим на шлюзі ДПА, бо опубліковані на сайті ДПА не відповідають тим, які технічно реалізовані; вдруге – щоб отримати можливість спілкування з розробником вказаного шлюзу ДПА та тестування реалізації програмних бібліотек, оскільки ці програмісти не є співробітниками ДПА, а комерційної структури; втретє – після завершення тестування з розробником шлюзу ДПА вже самому ДПА, який може допустити або ні до свого шлюзу додаткову реалізацію програмних засобів для приймання електронних документів платників податків, з використанням ключів та сертифікатів, які випускаються акредитованими центрами сертифікації відкритих ключів України. А між цими «земними поклонами» необхідно буде ще багато разів вклонитися для вирішення поточних питань з технічної реалізації підключення до шлюзу ДПА. Виникає питання – навіщо створено ці штучні складнощі?

Таким чином, для того, щоб підключити новий акредитований ЦСК до ДПА слід пройти занадто невизначений ні по складності, ні по термінах такого «підключення» шлях.

Як сказано і вище, використовуючи зазначені проблеми із додаванням до прикладної програми електронної звітності модулів нового розробника КЗІ, власник/ замовник/ розробник цієї прикладної програми може легко «не допустити» нові засоби КЗІ до впровадження, у тому числі, із конкурентних та/чи корупційних підстав.

Така ситуація не є унікальною, а характерна для більшості технічних реалізацій, які функціонують у державних органах України, які обробляють документи в електронному вигляді з електронними цифровими підписами.

Приклади можна було б продовжити (інші державні органи, та системи звітності), але картина й так очевидна.

Така на сьогодні практика державних органів із створення електронної звітності. За відсутності Технічних специфікацій, які розроблені фахівцями з цих питань, створюються вимоги через підзаконні акти (накази тощо) особами, які є далеко не фахівцями. Повнота цих «вимог» низька, а фактично інформаційна безпека тим паче.

Останнє риторичне питання: Так куди ж ми йдемо? У Європу? Чи за висловом Олександра Волкова…