УДК 004.056.55

Г.О.Кравцов, м.Київ

ОЦІНКА ОБМЕЖЕНЬ У ВИКОРИСТАННІ ЕЦП ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ МЕРЕЖАХ

Abstract. In this article author shows the condition for effective implementation of method of distributed storage in electronic signature subsystems and implementation of reconfigured algorithms for cryptographic evaluations. This is possible if the algorithm is based on reconfigurable logic composition of elementary modules that implement the primitive mathematical operations. The research results are reflected in the patents for useful models.

Актуальність

На початку 80-их років В.М. Глушков запропонував концепцію ЗДАС – загальнодержавної автоматизованої системи збору та обробки інформації для обліку, планування і управління народним господарством [1]. В наші часи його ідеї знаходять своє відлуння, зокрема, в розвитку інтелектуальних електроенергетичних систем (Smart Grid).

Відповідно до технічного завдання Європейським організаціям зі стандартизації на розробку стандартів для забезпечення впровадження європейської інтелектуальної електромережі [2] одним з основних механізмів Smart Grid є електронний підпис.

Пошук оптимального за економічними показниками способу забезпечення гарантованого захисту інформації при використанні електронного цифрового підпису у відповідності до [3] приводить до ідеї розподіленого зберігання, яка полягає в необхідності поряд зі сховищем підписаних даних (електронних документів) штучно утворювати сховище списків відкликаних сертифікатів та ланцюжка сертифікатів у відповідності до моделі інфраструктури відкритих ключів в залежності від країни.

Постановка задачі

Прийняття рішення щодо впровадження механізму розподіленого зберігання як інновації пов’язане з визначенням структури ефекту, насамперед економічного.

Складність структури ефекту інновацій, в свою чергу, проявляє себе в двох основних формах. По-перше, окремі компоненти такого ефекту не завжди можуть бути виміряні в однакових універсальних одиницях (наприклад - вартісних), що дозволяють взаємно інтегрувати одержувані окремі оцінки. По-друге, здійснення процедур подібної інтеграції вимагає наявності кількісних оцінок відносної значущості кожного з компонентів ефекту, які індивідуальні в кожному конкретному випадку і можуть бути визначені тільки суб'єктивно.

Розходження в ступені прояву ефекту інновацій в рамках кожного конкретного відрізка часу також істотно обмежують можливість отримання точної оцінки такого ефекту. Основою таких відмінностей є відмінності в природі ефекту інновацій, який може бути як явним, так і потенційним. Явний ефект має конкретні результати свого прояву в діяльності підприємства і може бути об'єктивно оцінений за цими результатами. Потенційний же ефект, на відміну від явного, на момент оцінки не має вимірних результатів свого прояву і, отже, не може бути оцінений будь-якими формалізованими методами. Разом з тим, величина такого прихованого ефекту може бути істотно більшою величини явного ефекту і по закінченню певного проміжку часу потенційний ефект може реалізуватися.

В зв'язку з цим постає питання оцінки обмежень у використанні ЕЦП для забезпечення цілісності інформації в інтелектуальних електроенергетичних мережах. В розумінні цієї статті під обмеженнями будемо розуміти такі показники, за яких впровадження способу розподіленого зберігання призводить до збільшення економічної вартості використання ЕЦП.

Вирішення задачі

Слід звернути увагу, що стандарт [3] визначає шість профілів електронного підпису в залежності від необхідного рівня захисту.

Кожен профіль включає і розширює попередній: XAdES - базова форма для посиленого підпису; XAdES-T - додавання мітки часу для захисту від відмови; XAdES-C - додавання посилань на перевірку даних (сертифікати і списки відгуку) до підписаного документу для автономної перевірки та перевірки в майбутньому; XAdES-X - додавання мітки часу на посилання, введені XAdES-C для захисту від можливого компромісу сертифікатів в ланцюжку в майбутньому; XAdES-XL - додавання сертифікатів та списку відкликаних сертифікатів до підписаного документу для перевірки в майбутньому, навіть якщо їх первісного джерела немає; XAdES-A - додавання можливості для періодичного штампування часу (наприклад, кожен рік) для архівних документів, аби запобігти компроміс, викликаний послабленням підпису протягом тривалого часу зберігання.

Спираючись на відомі матеріали ряду засвідчувальних центрів, центрів сертифікації ключів (Apple Root Certificate Authority, Boeing Company Root CA, Центральний засвідчувальний орган України, Засвідчувальний центр МВС Росії) ми можемо вважати, що середній розмір сертифіката становить 1 Кбайт (1024 байти), займаючи при цьому 4 Кбайт дискового простору.

Для обраної Україною моделі «Центральний засвідчувальний орган - Засвідчувальний центр органів державної влади - центр сертифікації ключів - клієнт», розміри підпису будуть відповідно становити: XAdES - 1 Кбайт, XAdES-T - 2 Кбайта, XAdES-C - 2 Кбайт, XAdES-X - 7 Кбайт, XAdES-XL - 8 Кбайт і XAdES-A - більше 8 Кбайт (враховується тільки розмір сертифікатів без урахування довжини підпису, атрибутів підпису та розміру списків

відкликаних сертифікатів).

Розглянемо в якості домену споживання електроенергії, наприклад, місто Київ. Компанія «КиївЕнерго» на 1 січня 2013 року обслуговувала більше 1 мільйона побутових споживачів [4]. Результати розрахунку дискового простору для зберігання даних домену за рік, при обліку електроенергії виходячи з профілю підпису та періоду звітності, наведені в Таблиці 1 (в Гбайт).

Таблиця 1

Підпис		Період (1 раз в/на)				
Профіль	Мін. розмір, Кбайт	рік	місяць	день	годину	в 10 хвилин
XAdES	1	0,95	11,44	320,43	7690,43	46142,58
XAdES-T	2	1,91	22,89	640,87	15380,86	92285,16
XAdES-C	2	1,91	22,89	640,87	15380,86	92285,16
XAdES-X	7	6,68	80,11	2243,04	53833,01	322998,05
XAdES-XL	8	7,63	91,55	2563,48	61523,44	369140,63
XAdES-A	9	8,58	103,00	2883,91	69213,87	415283,20

«Київенерго» не може відповідати за зобов'язаннями Центрів сертифікації ключів, тому слід використовувати профіль XAdES-XL протягом одного року, а з урахуванням позовної давності 3 роки - XAdES-A. Очевидно, що моніторинг мережі в реальному масштабі часу спричинить значне збільшення необхідного дискового простору і за три роки позовної давності показники, наведені в Таблиці 1, можуть перевищити петабайт. (Для порівняння експерименти на Великому адронному колайдері виробляють дані для подальшої обробки об'ємом 4 петабайта на рік [5].)

Очевидно, що розв'язання завдання збереження конкретних даних істотно залежить не тільки від опцій їх безпосереднього використання, але й від застосовуваних методів і алгоритмів обробки. І також очевидно, що у зв'язку з великими обсягами вихідних даних методи і алгоритми їх обробки будуть безперервно удосконалюватися. Отже, елементи інтелектуальних електроенергетичних систем повинні мати можливість оновлення, що особливо важливо для так званих, польових елементів, що знаходяться «на місцях».

У цьому зв'язку слід особливо відзначити, що технічна база інфраструктури ЕЦП на стороні клієнта повинна мати можливість поновлення своєї алгоритмічної складової. Таке оновлення технічно можливо, що підтверджується рішеннями, заявленими, наприклад, у патентах [6-8].

Відповідно до [9] центри сертифікації емітують: сертифікати користувачів (certificate), списки відкликаних сертифікатів (CRL) і свіжіші списки відкликаних сертифікатів (Freshest CRL (a.k.a. Delta CRL Distribution

Point, RFC 2459)).

З точки зору розподіленого зберігання нас буде цікавити інтенсивність емісії списків відкликаних сертифікатів та свіжіших списків відкликаних сертифікатів. У відповідності до [9] Центри сертифікації ключів визначають інтенсивність емісії свіжіших списки відкликаних сертифікатів.

З огляду на те, що інформаційна система може оперувати підписаними даними, в яких підпис отримано за допомогою сертифікатів від різних центрів сертифікації ключів, то загальна інтенсивність емісії свіжіших списків відкликаних сертифікатів буде дорівнювати сумі інтенсивностей, яку позначимо як λ_{Δ}.

Припустимо, що в систему надходять документи, які підписувалися з інтенсивністю λ_C. Відповідно до [3] кожен підпис в форматах XAdEX-XL та XAdEX-A містить список відкликаних сертифікатів та найсвіжішій список відкликаних сертифікатів на момент часу підписання.

Вочевидь, що застосування методу роздільного зберігання доцільне за умови

$$\lambda_{\Delta} < \lambda_C ,$$

що випливає безпосередньої з самої ідеї розподіленого зберігання, що гарантує зберігання тільки унікальних даних (списків відкликаних сертифікатів та свіжіших списків відкликаних сертифікатів) без дублювання.

Постає питання однозначної ідентифікації сертифікатів та списку відкликаних сертифікатів. Це питання може розглядатися як проблема з огляду на те, що центри сертифікації ключів можуть емітувати сертифікати з однаковими серійними номерами. Але серійні номери емітованих сертифікатів в межах центру сертифікації є унікальними, тому якщо до серійного номера сертифікату додати серійний номер кореневого сертифікату центру сертифікації ключів, то такої проблеми не існує.

Списки відкликаних сертифікатів є унікальним за URL та серійним номером сертифіката кореневого сертифікату центру сертифікації ключів з урахуванням часу емісії.

Висновок

Метод розподіленого зберігання виявляє економічний ефект за умови, що кількість підписаних документів в автоматизованій системі зростає скоріше, ніж кількість сертифікатів, що задіяні у процесі легалізації електронного документообігу. Застосування методу розподіленого зберігання можливе лише при вирішенні задачі однозначної ідентифікації сертифікату та списку відкликаних сертифікатів. Вирішення задачі однозначної ідентифікації є виключно технологічною задачею, що може бути вирішена на рівні програмного забезпечення. Таким чином, єдиним обмеженням до застосування методу розподіленого зберігання є співвідношення між кількістю підписаних документів та кількістю сертифікатів.

1. *В.М.Глушков, В.Я.Валах*. Что такое ОГАС? – М. Издательство «Наука», - 1980.

2. Европейская комиссия Генерального директората по энергетике. Директорат B. Техническое задание Европейским организациям по стандартизации (EOC) на разработку стандартов для обеспечения внедрения европейской интеллектуальной электросети. M/49 EN. – c.10. - 2011. – Режим доступу: http://www.smartgrid.ru/smartgrid/analytics/2012/analytics56/centercolumn/permanent/SmartgridArticleBrief/SmartgridArticleInnerCollection/0/0/text_files/file/tech.pdf . - Дата доступу: листопад 2012. – Назва з екрану.

3. ETSI TS 101 903 (v.1.4.1) XML Advanced Electronic Signatures (XAdES) – 2009. – Режим доступу: http://uri.etsi.org/01903/v1.4.1/ts_101903v010401p.pdf . - Дата доступу: грудень 2012. – Назва з екрану.

4. Офіційний сайт «Київенерго». Виробництво та реалізація електроенергії. Режим доступа: http://kyivenergo.ua/ua/production/power - Дата доступу: грудень 2012. – Назва з екрану.

5. Let the number-crunching begin: the Worldwide LHC Computing Grid celebrates first data. (Interaction News Wire #79-08, 3 October 2008). Режим доступа: http://www.interactions.org/cms/?pid=1027032 - Дата доступу: грудень 2012. – Назва з екрану.

6. Пат.66790 Україна, МПК (2012.01) H04L 9/00. Спосіб застосування криптографічних алгоритмів у криптографічних засобах захисту інформації. / *Мартиненко С.В., Бєлов С.В., Ромін О.О., Кравцов Г.О., Зубарева О.О.*; заявники та патентовласники. № u 2011 13881; заявл.25.11.2011, опубл. 10.01.2012, Бюл.№1.

7. Пат.67369 Україна, МПК H04L 9/14 (2006.01) Пристрій криптографічного захисту інформації для реалізації криптографічних алгоритмів з використанням математичних примітивів. / *Мартиненко С.В., Бєлов С.В., Ромін О.О., Кравцов Г.О., Зубарева О.О;* заявники та птантовласники. № u 2011 15298; заявл.23.12.2011, опубл. 10.02.2012, Бюл.№3.

8. Пат.68956 Україна, МПК H04L 9/14 (2006.01) . Пристрій криптографічного захисту інформації з реалізацією криптографічного алгоритму ДСТУ 4145-2002») / *Мартиненко С.В., Бєлов С.В., Ромін О.О., Кравцов Г.О., Лясковський А.В., Суховієв О.В., Квіта Г.І., Андреєв Ю.Ю., Яременко О.В., Зубарева О.О.;* заявники та патентовласники. № u 2012 02032; заявл.22.02.2012, опубл. 10.04.2012, Бюл.№7.

9. RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Режим доступу - http://tools.ietf.org/html/rfc5280. Дата доступу: грудень 2012. – Назва з екрану.

Поступила 14.03.2013р.