УДК 004.056.2

О.Ю. Юдін, С.М. Красніков, Київ

ВАРІАНТИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ ПРИ ВЗАЄМОДІЇ SMART GRID СИСТЕМ НА МІЖДЕРЖАВНОМУ РІВНІ

Abstract. The materials are for the ways of establishing relations with other certification authorities that are used outside the boundaries of Ukraine's information space.

Вступ

На теперішній час електроенергетичні системи (ЕС) України, Російської Федерації, Республіки Молдова, Республіки Білорусь, Польщі, Словаччини, Угорщини, Румунії дуже тісно пов'язані між собою та працюють разом з електроенергетичними системами інших країн [1]. Враховуючи цей факт можливо припустити, що майбутня Smart Grid система буде створюватись на базі фрагментів ЕС між якими необхідно забезпечити захищений оперативний обмін інформацією.

В той же час слід зазначити на існування ризику щодо неможливості легітимного обміну інформацією в Smart Grid системі у зв'язку з виконанням вимог національних нормативно-правових актів в галузі захисту інформації. Цей ризик пов'язаний з відсутністю реалізованого на міждержавному рівні механізму підтвердження цілісності та достовірності інформації. Збільшує цей ризик той факт, що в Україні прийнята ієрархічна модель електронного цифрового підпису [2] (далі – ЕЦП) яка є замкненою системою. В цій моделі всі центри сертифікації ключів (далі – ЦСК) є доменами об'єднаними в структуру зв'язного графа, що має одну головну вершину (кореневий ЦСК), з якої будується структура підпорядкованих ЦСК. Звідси випливає проблема щодо неможливість встановлення довірчих відносин з іншими ЦСК які існують поза межами інформаційного простору України. Також означена проблема пов'язана з використання національних алгоритмів ЕЦП й геш-функції (ДСТУ 4145-2002 та ДСТУ ГОСТ 34.310-95) які не сумісними з міжнародними алгоритмами DSA, RSA, ECDSA та ін. [2, 3].

Можливі шляхи розв'язання проблеми

Варіант 1

Забезпечення крос-сертифікації між Кореневим ЦСК України (Центральний засвідчувальний орган [2]) та Кореневими ЦСК інших держав.

Крос-сертифікацією називається процес, який використовується в інфраструктурі відкритих ключів (PKI), для встановлення довірчих відносин. Це процес взаємної (перехресної) сертифікації двох рівноправних ЦСК доменів, яка використовується одним ЦСК, щоб сертифікувати будь-який інший ЦСК [4, 5, 7].

Для реалізації механізму крос-сертифікації необхідно вирішити наступні завдання:

– реєстрація національних стандартів ДСТУ 4145-2002 та ДСТУ ГОСТ 34.310-95 як міжнародних (ISO/IEC) та створення і закріплення на міжнародному рівні комплекту підписування;

– розробка профілю на криптоалгоритми визначені ДСТУ. Під профілем розуміється деякий набір опцій, які визначають обмеження на використання алгоритмів. Профіль закріплюється об'єктним ідентифікатором OID (Object IDentifier) [6].

Варіант 2

Іншим варіантом розв'язання проблеми є створення Мостового ЦСК, який може функціонувати в межах міждержавних домовленостей. Основним завданням Мостового ЦСК є одночасна робота з двома алгоритмами цифрового підпису [8-9]. Опишемо процес роботи Мостового ЦСК.

Нехай існують два суб'єкти, які є користувачами різних ЦСК (наприклад, знаходяться в різних країнах), позначимо їх через А (перший суб'єкт) та В (другий суб'єкт). Для А використання алгоритму цифрового підпису В вважається нелегітимним і відповідно навпаки. Враховуючи викладені обмеження весь процес підтвердження легітимності ЕЦП суб'єктів можливо викласти у вигляді послідовності дій, а саме:

- відправлення повідомлення від А до В;
- проходження суб'єктом В верифікації повідомлення, отриманого від суб'єкта А;
- відправлення повідомлення від В до А;
- проходження суб'єктом А верифікації повідомлення, отриманого від суб'єкта В.

Розглянемо детально запропонований алгоритм.

Відправлення повідомлення від А до В. Послідовність дій схематично наведена на рис. 1.

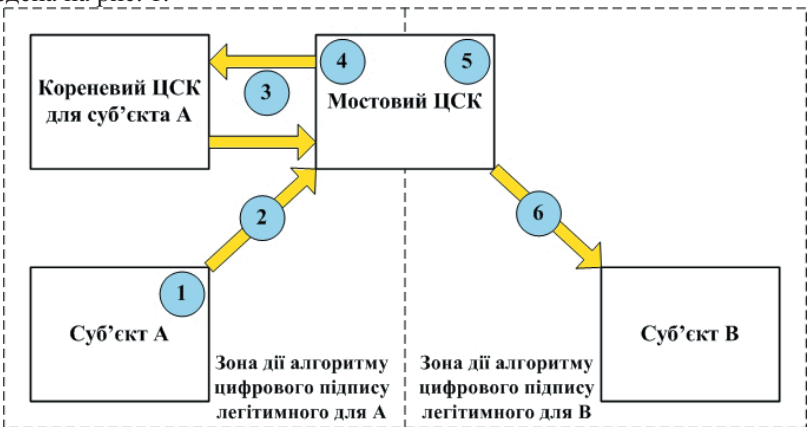

Рис. 1. Процес відправлення повідомлення від А до В

Викладемо опис зазначеного процесу.

1. Формування цифрового підпису до повідомлення створеного суб'єктом А, має наступний вигляд

$$Sign_1 := S(M_A, PriK_A, UI_A, DSA_A) \quad (1)$$

де S – функція формування цифрового підпису повідомлення;

DSA_A – алгоритм цифрового підпису легітимний для А;

UI_A – службова інформація об'єкта А;

$PriK_A$ – особистий ключ об'єкта А, відповідно до DSA_A;

M_A – повідомлення від об'єкта А;

$Sign_1$ – утворене значення цифрового підпису.

2. Відправлення $M_A \,||\, Sign_1$ до Мостового ЦСК (далі – CA_{Bridge}).

3. CA_{Bridge} здійснює виділення підпису ($Sign_1$) з повідомлення. На основі отриманої інформації він формує запит до ЦСК об'єкта А (далі – CA_A) з метою одержання необхідної інформації для процесу верифікації повідомлення.

4. CA_{Bridge} після отримання від CA_A необхідної інформації ($PubK_A$, UI_A) проводить процес верифікації повідомлення:

$$V(Sign_1, M_A, PubK_A, UI_A, DSA_A) \quad (2)$$

де V – функція верифікації цифрового підпису повідомлення;

$PubK_A$ – відкритий ключ об'єкта А, відповідно до DSA_A.

5. У випадку позитивного проходження верифікації отриманим повідомленням, CA_{Bridge} виконує процес перепідпису повідомлення

$$Sign_2 := S(M_A \,||\, Sign_1, PriK_{BridgeB}, UI_A, DSA_B) \quad (3)$$

де DSA_B – алгоритм цифрового підпису легітимний для В;

$PriK_{BridgeB}$ – особистий ключ CA_{Bridge}, відповідно до DSA_B;

$Sign_2$ – утворене значення цифрового підпису.

6. Відправлення до суб'єкту В $M_A \,||\, Sign_1 || \, Sign_2$

Проходження суб'єктом В верифікації повідомлення, отриманого від суб'єкта А. Послідовність дій схематично наведена на рис. 2.

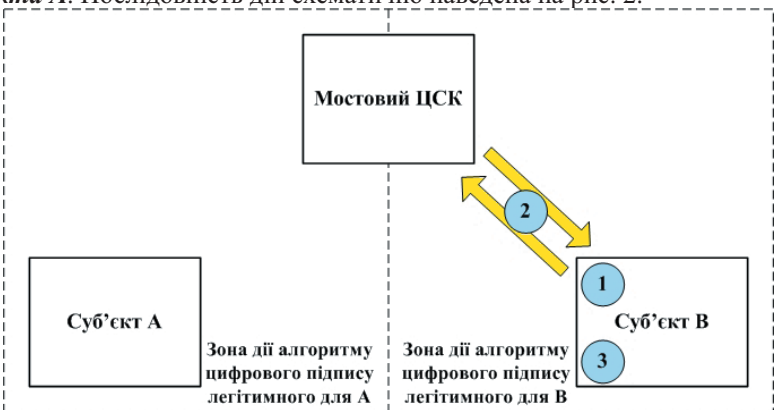

Рис. 2. Процес проходження суб'єктом В верифікації повідомлення, отриманого від суб'єкта А

Викладемо опис зазначеного процесу.

1. Виділення підпису ($Sign_2$) з повідомлення (M_A || $Sign_1$|| $Sign_2$). На основі отриманої інформації формується запит до CA_{Bridge} з метою одержання необхідної інформації для процесу верифікації повідомлення.

2. Після отримання від CA_{Bridge} необхідної інформації (UI_A, $PubK_{BridgeB}$) проводиться процес верифікації

$$V\ (Sign_2,\ M_A,\ PubK_{BridgeB},\ UI_A,\ DSA_B) \qquad (4)$$

де $PubK_{BridgeB}$ – відкритий ключ CA_{Bridge}, відповідно до DSA_B.

3. У випадку позитивного проходження верифікації, повідомлення (M_A) вважається підписаним суб'єктом А.

Відправлення повідомлення від В до А. Послідовність дій схематично наведена на рис. 3.

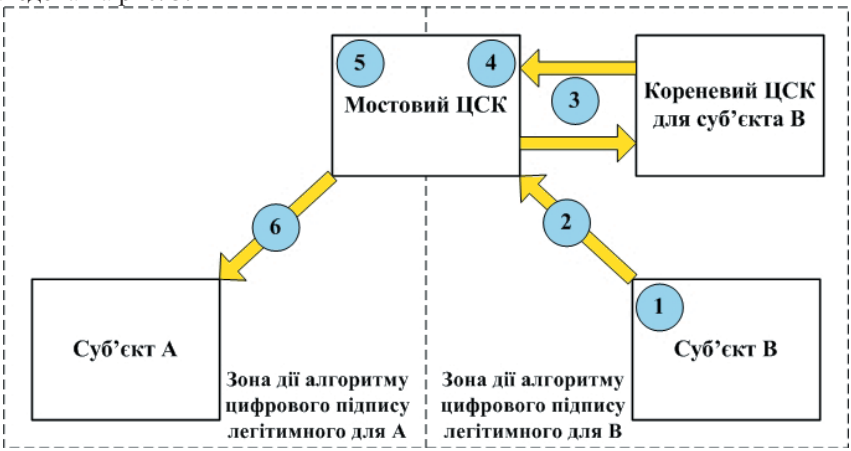

Рис. 3. Процес відправлення повідомлення від В до А

Наведемо опис зазначеного процесу.

1. Формування цифрового підпису до повідомлення створеного суб'єктом В, має наступний вигляд

$$Sign_3 := S\ (M_B,\ PriK_B,\ UI_B,\ DSA_B) \qquad (5)$$

де M_B – повідомлення від об'єкта В;

$PriK_B$ – особистий ключ об'єкта В, відповідно до DSA_B;

UI_B – службова інформація об'єкта В;

$Sign_3$ – утворене значення цифрового підпису.

2. Відправлення до CA_{Bridge} M_B || $Sign_3$

3. CA_{Bridge} здійснює виділення підпису ($Sign_3$) з повідомлення. На основі отриманої інформації він формує запит до ЦСК об'єкта В (далі – CA_B) з метою одержання необхідної інформації для процесу верифікації повідомлення.

4. CA_{Bridge} після отримання від CA_B необхідної інформації (UI_B, $PubK_B$) проводить процес верифікації одержаного повідомлення:

$$V\ (\ Sign_3,\ M_B,\ PubK_B,\ UI_B,\ DSA_B) \quad (6)$$

де $PubK_B$ – відкритий ключ об'єкта А, відповідно до DSA_B.

5. У випадку позитивного проходження верифікації отриманого повідомлення, CA_{Bridge} виконує процес перепідпису повідомлення

$$Sign_4 := S\ (M_B\ ||\ Sign_3,\ PriK_{BridgeA},\ UI_B,\ DSA_A) \quad (7)$$

де $PriK_{BridgeA}$ – особистий ключ CA_{Bridge}, відповідно до DSA_A;

$Sign_4$ – утворене значення цифрового підпису.

6. Відправлення до суб'єкту А $M_B\ ||\ Sign_3\ ||\ Sign_4$.

Проходження суб'єктом А верифікації повідомлення, отриманого від суб'єкта В. Послідовність дій схематично наведена на рис. 4.

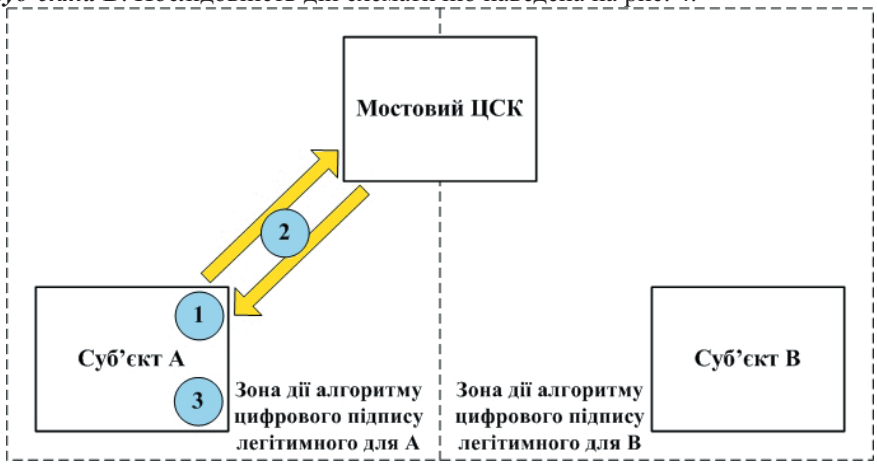

Рис. 4. Процес проходження суб'єктом А верифікації повідомлення, отриманого від суб'єкта В

Здійснімо опис цього процесу.

1. Виділення підпису ($Sign_4$) з повідомлення ($M_B\ ||\ Sign_3||\ Sign_4$). На основі отриманої інформації формується запит до CA_{Bridge} з метою одержання необхідної інформації для процесу верифікації повідомлення.

2. Після отримання від CA_{Bridge} необхідної інформації ($UI_B,\ PubK_{BridgeA}$), проводиться процес верифікації

$$V\ (Sign_4,\ M_B,\ PubK_{BridgeA},\ UI_B,\ DSA_A) \quad (8)$$

де $PubK_{BridgeA}$ – відкритий ключ CA_{Bridge}, відповідно до DSA_A.

3. У випадку позитивного проходження верифікації, повідомлення (M_B) вважається підписаним суб'єктом В.

Висновки

За результатами розгляду двох варіантів розв'язання проблеми найбільш проблематичним є перший варіант. В першу чергу це пов'язано з тим, що процедура визнання державних стандартів України (ДСТУ 4145-2002, ДСТУ ГОСТ 34.310-95) як міжнародних може зайняти багато часу. Як приклад можна навести ситуацію з ГОСТ 28147-89. Зазначений стандарт з 2010 року

знаходиться на розгляді 27-го підкомітету 1-го об'єднаного технічного комітету Міжнародної організації по стандартизації (ISO/IEC JTC 1/SC 27) з метою визначення як міжнародного та викладення його в ISO/IEC 18033 "Information technology. Security techniques. Encryption algorithms". На теперішній час, зазначений стандарт так і не прийнятий.

Другий варіант є більш реалістичний, тому що для його реалізації необхідно:

1. Розробити технічну реалізацію мостового ЦСК.

2. Закріпити можливість використання мостового ЦСК на міждержавному рівні шляхом прийняття відповідних угод з урядами зацікавлених країн. При цьому сферу застосування та необхідні обмеження можливо закріпити тими ж угодами.

Таким чином інтероперабельність Smart Grid систем, в частині забезпечення цілісності та достовірності інформації, доцільно забезпечити шляхом побудови мостових ЦСК.

1. Україна. Розпорядження Кабінету Міністрів України. Про схвалення Енергетичної стратегії України на період до 2030 року : офіц. текст : [схвалена розпорядженням Кабінету Міністрів України від 15 березня 2006 р.].
2. Україна. Закони. Про електронний цифровий підпис : офіц. текст : [прийнятий Верховною Радою 22 травня 2003 р.]. - К.: Відомості Верховної Ради України, 2003, №36.
3. Україна. Закони. Про електронні документи та електронний документообіг : офіц. текст : [прийнятий Верховною Радою 22 травня 2003 р.]. - К.: Відомості Верховної Ради України, 2003, №36.
4. SP800 – 32. Introduction to Public Key Technology and the Federal PKI Infrastructure / D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk // NIST. – 2011. – 54 p.
5. X.509. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks // ITU-T. – 2008. – 186 p.
6. *Мелащенко А.О.* Комплекти підписів для інтероперабельності Національної системи електронних цифрових підписів / *А.О. Мелащенко, О.Л. Перевозчикова, О.С. Скарлат, К.С. Криворучко* // Наукові записки, Том 99, Комп'ютерні науки. - К.: Києво-Могилянська академія, 2009. - С. 70-77.
7. *Горбенко І.Д.* Захист інформації в інформаційно-телекомунікаційних системах : навч. посібник. Ч.1 / *І.Д. Горбенко, Т.О. Гріненко*. –Х.: ХНУРЕ, 2004. – 368 с.
8. Identity-Based Encryption with Conventional Public-Key Infrastructure [Електронний ресурс] / Jon Callas // PGP Corporation, USA. – 2005. Режим доступу: http://middleware.internet2.edu/pki05/proceedings/callas-conventional_ibe.pdf. - Назва з екрану.
9. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures [Електронний ресурс] / William T. Polk and Nelson E. Hastings // National Institute of Standards and Technology – 14 p. - 2000. Режим доступу: http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/B2B-article.pdf. - Назва з екрану.

Поступила 18.02.2013р.