УДК 004.056

М.М. Поліщук, В.П. Пасько, С.Ф. Погляд

РОЗШИРЕННЯ ФУНКЦІОНАЛУ ЕЛЕКТРОННОГО БІОМЕТРИЧНОГО ПАСПОРТА ДЛЯ ЗАСТОСУВАННЯ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

Анотація: У статті проаналізовано концепцію застосування електронного біометричного паспорта як засобу електронного цифрового підпису і описано прототип такого паспорта. Отримані результати дозволяють спростити доступ громадян до послуг електронного цифрового підпису та прискорити процес впровадження системи електронного урядування на території України.

Ключові слова: Ключові слова: захист інформації, електронний біометричний паспорт, електронний цифровий підпис, інфраструктура відкритих ключів.

Вступ

Протягом першої половини 2014 р. уряд України неодноразово наголошував про необхідність якнайшвидшого переходу до електронного документообігу в державних структурах. Важливою складовою електронного документообігу є електронний цифровий підпис (далі – ЕЦП). Саме тому, з'являється необхідність у поширенні дешевих та надійних засобів ЕЦП, а враховуючи тенденцію економії бюджетних коштів, такі рішення будуть одночасно дешевими та ефективними.

На даний момент найпоширенішими засобами ЕЦП є спеціалізовані програмні продукти криптографічного захисту інформації, які як носій особистого ключа використовують накопичувачі інформації (CD, DVD, USB-drive) із записаним на нього зашифрованим файловим сховищем особистого ключа. Для посилення безпеки може застосовуватись захищений носій особистого ключа, який унеможливлює копіювання закритої інформації підписувача. Через брак довіри з боку споживачів, дані рішення не набули широкого поширення. Для функціонування повноцінного електронного документообороту в державних структурах з перспективою формування системи електронного урядування необхідно, щоб переважна більшість громадян України володіли послугою ЕЦП. На важливості впровадження ефективної системи ЕЦП вже було наголошено у багатьох дослідженнях та документах [1–4].

Авторами запропоновано використовувати електронні біометричні паспорти (далі – ЕБП) у якості засобу ЕЦП. Для цього необхідно провести модифікацію програмного забезпечення, яке здійснює взаємодію з ЕБП. У цій статті визначено складові ЕБП, які необхідно розширити для отримання очікуваного результату та подано опис прототипу програмного забезпечення *ePassSign* для роботи з ЕБП як засобами ЕЦП.

ISSN 1560-8956

Вибір технічної платформи

Для реалізації ЕЦП необхідна підтримка ЕБП процесорних можливостей асиметричного шифрування. Цьому критерію відповідають ЕБП, які передбачають процедуру активної автентифікації.

В даному випадку термінал взаємодії з ЕБП посилає на "чіп" запит. Далі запит підписується особистим ключем активної автентифікації. Підпис перевіряється терміналом за допомогою відкритого ключа активної автентифікації, який зберігається серед біометричних даних, захищених методом пасивної автентифікації видавцем ЕБП.

Згідно з рекомендаціями Міжнародна організація цивільної авіації (МОЦА [5] необхідно обмежити доступ до неперсоналізованих (таких, на які не записано особисті дані про особу) електронних паспортів. Тому як платформу для розробки електронного паспорта з функцією накладання ЕЦП доцільно скористатись емулятором другого покоління електронних посвідчень. Для забезпечення криптографічного захисту інформації в електронних паспортах використовується технологія *Java card virtual machine* (JCVM) [6]. Це середовище забезпечує можливість програмування поведінки електронної картки в умовах обмежених процесорних можливостей та розмірів оперативної пам'яті. Для емуляції JCVM обрано *jCardSim* [7] як найпопулярнішу систему даного класу.

Вибір програмних інструментів

У процесі розробки програмного забезпечення для електронних паспортів використано кілька відкритих програмних продуктів:

- *Java Machine Readable Travel Documents* (JMRTD) [8] – імплементація вимог МОЦА до реалізації електронних паспортів [5]. Першою частиною проекту є "паспортний аплет" – реалізація електронного паспорта на основі Java card. Другою частиною є термінальний інтерфейс, що дозволяє взаємодіяти з електронною карткою. Для реалізації прототипу необхідно тільки "паспортний аплет".
- *Legion of the Bouncy Castle* (Bouncy Castle) [9] – бібліотека криптографічних перетворень, що може використовуватись у JCVM. Передбачає як реалізацію міжнародних криптографічних алгоритмів [10], так і об'єктів інфраструктури відкритих ключів, які необхідні для роботи системи електронних паспортів та електронного урядування. Дозволяє розширювати функціонал шляхом наслідування класів. Так, за допомогою наслідування і розширення класу, що імплементує асиметричні алгоритми підписання на еліптичних кривих, реалізується імплементація ДСТУ 4145.
- *PKCS#11 Signer For Java* [11] – бібліотека-обгортка, що надає високорівневий доступ до платформо незалежного інтерфейсу

криптографічних засобів (використання процесорних можливостей мікросхеми електронного паспорта).

Оскільки в JMRTD вже реалізовано логічну структуру даних (далі – ЛСД) ЕБП та інтерфейс взаємодії з карткою, то для реалізації поставленого завдання, а саме: імплементації на основі електронного паспорта особистого ЕЦП для використання в системі електронного урядування, необхідно реалізувати інтерфейс взаємодії з процесорними можливостями асиметричного шифрування (ключ активної автентифікації) та забезпечити зберігання посиленого сертифікату відкритого ключа активної автентифікації пам'яті електронного паспорта.

Розробка програмного продукту

Авторами статті розроблено програмний продукт *ePassSign* за допомогою якого вирішуються проблеми, які описані вище. Програмний продукт складається з трьох модулів (рис. 1):

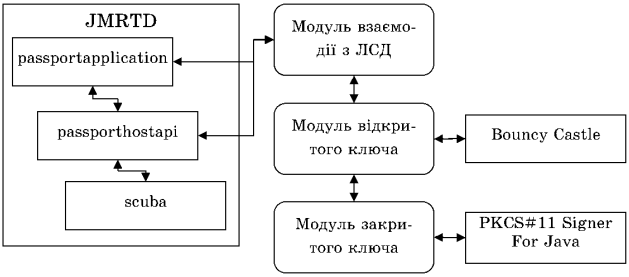

Рис. 1 – Рисунок 1. – Структурна схема ePassSign

- Модуль взаємодії з ЛСД. Зручний інтерфейс для роботи користувача з електронним паспортом.
- Модуль взаємодії з відкритим ключем активної автентифікації. Забезпечує запис і зчитування сертифікату відкритого ключа активної автентифікації.
- Модуль взаємодії з особистим ключем активної автентифікації. Забезпечує підписання документів особистим ключем, який знаходиться у захищеній ділянці електронного паспорта.

Модуль взаємодії з ЛСД базується на основі форми *org.jmrtd.app.DocumentEditFrame* (проект JMRTD). Зовнішній вигляд модуля показано на рис. 2. Основні поля форми перекладено на українську мову та додано кнопки взаємодії з двома іншими модулями (рис. 3).

Для накладання ЕЦП електронним паспортом необхідно реалізувати роботу з посиленим сертифікатом відкритого ключа,

Рис. 2 – Форма модуля взаємодії з ЛСД

який видається акредитованим центром сертифікації ключів (далі – АЦСК) у відповідності до чинного законодавства [12]. Оскільки особистий ключ генерується і зберігається у захищеній ділянці електронного паспорта, етап отримання сертифікату повинен передбачати генерацію запиту на сертифікат відкритого ключа. Запит генерується у форматі PKCS#10 за допомогою класу бібліотеки *Bouncy Castle "org.bouncycastle.jce.PKCS10CertificationRequest"* (або аналогічних засобів криптографічного захисту інформації). Запит є підписаним документом, який містить інформацію про особу, що здійснює запит на отримання сертифікату відкритого ключа (Subject), та відкритий ключ, на основі якого необхідно генерувати сертифікат.

Кожен АЦСК надає інструменти для генерації запитів на сертифікат відкритого ключа, тому буде доцільно скористатись програмним продуктом конкретного обраного довіреного органу. Наприклад АЦСК *UPG PKI-UA* розповсюджує безкоштовний *Клієнт UPG PKI*, який дозволяє формувати PKCS#10 запити на сертифікат. В такому випадку немає необхідності передбачати функціонал запитів на сертифікат відкритого ключа у програмному продукті *ePassSign*.

Для забезпечення зберігання посиленого сертифікату відкритого ключа можна скористатись двома різними механізмами.

Перший механізм – це зберігання сертифікату у спеціальному розділі пам'яті електронного паспорта. Доступ до цієї області пам'яті здійснюється за допомогою інтерфейсів, які визначені в PKCS11, або при безпосередній роботі з платформозалежними драйверами електронної картки, що буде нераціональним у разі застосування ЕБП від різних виробників, оскільки необхідно підтримувати драйвери кожного виробника.

Другий механізм – це зберігання сертифікату відкритого ключа у ЛСД. Згідно зі специфікаціями МОЦА [5] передбачено групу даних DG13 "Факультативні дані", яка може містити додаткові дані. Кожна країна (організація-видавець електронного паспорта) може визначити свій власний формат в DG13. Сертифікат відкритого ключа доцільно зберігати у DER-кодуванні у відповідності з вимогами до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису [13]. В програмному продукті *ePassSign* реалізовано другий механізм зберігання посиленого сертифікату відкритого ключа.

У модулі взаємодії з відкритим ключем активної автентифікації для зберігання сертифікату відкритого ключа розроблено клас *org.jmrtd.lds.LDSFileUtil. DG13File*, який розширює клас *org.jmrtd.lds.DataGroup* (підклас *org.jmrtd.lds.AbstractLDSFile*), та здійснено відповідні модифікації методів JMRTD, у яких передбачено повернення об'єкту DG13File, бо за замовчуванням у коді встановлено програмні заглушки виду:

case PassportService.EF_DG13: throw new IllegalArgumentException ("DG13 files are not yet supported").

До модуля взаємодії з ЛДС додано модуль взаємодії з сертифікатом відкритого ключа через кнопку *Імпорт сертифікату АА* (рис. 3).

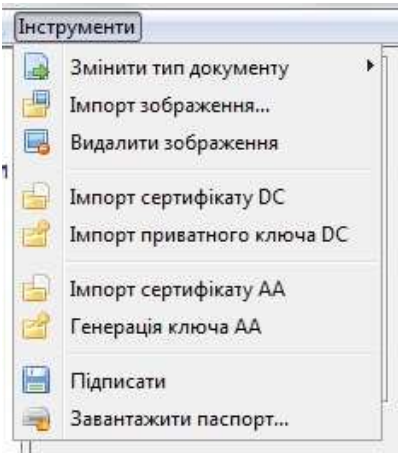

Рис. 3 – Кнопки взаємодії з модулями для управління особистим та відкритим ключами активної автентифікації

Особистий ключ активної автентифікації зберігається у захищеній ділянці електронного паспорта. Завантажити ключ у пам'ять та скопіювати його неможливо. Це дозволяє припускати, що електронний паспорт з конкретним особистим ключем є оригіналом

(дублювання неможливе). Для перевірки оригінальності паспорта використовується процедура автентифікації за допомогою відкритого та закритого ключів активної автентифікації.

Для взаємодії з особистим ключем електронного паспорта JMRTD передбачає тільки процес активної автентифікації (метод *org.jmrtd.Passport.verifyAA()*), за допомогою якого неможливо підписати довільний масив байтів (встановлено обмеження в 8 байт).

Для здійснення процедури накладання ЕЦП розроблено модуль взаємодії з особистим ключем активної автентифікації. За основу взято інтерфейс *PKCS#11*. Бібліотека *PKCS#11 Signer For Java* дозволяє легко взаємодіяти з особистим ключем електронного паспорта. Фрагмент коду підписання документу:

```
CertificateInformer informer = new CertificateInformer();
certs = informer.getCertificates();
CertificateInfo cert = certs.get(0);
// отримуємо сертифікат відкритого ключа активної аутентифікації
PKCS11Signer signer = new PKCS11Signer(cert.getSlotId(), cert.getDriverPath());
//ініціалізація підписувача на основі інформації про відкритий ключ
signer.login(passwordStr);
byte[] signedData = signer.signAsCMSEncoded(dataToSign.getBytes(), true);//підписання
CMSSignedData cmsSignedData = new CMSSignedData(signedData);
signer.logout();//завершення сесії роботи з особистим ключем (знімається блокування на ресурс)
```

До модуля взаємодії з ЛДС додано модуль взаємодії з особистим ключем через кнопки *Генерація ключа АА* та *Підписати* (рис. 3).

Програмний продукт *ePassSign* дозволяє накладати ЕЦП за допомогою модифікованого (підтримка DG13) електронного паспорта. Верифікація ЕЦП здійснюється за допомогою спеціалізований програмних продуктів таких, як *Клієнт UPG PKI*.

Обмеження даної версії програмного продукту, які необхідно усунути в остаточній реалізації *ePassSign* (release) :

- підтримуються тільки міжнародні криптографічні стандарти RSA та SHA-1 (для підписання на основі стандарту ДСТУ-4145 необхідно усунути деякі юридичні обмеження);
- формат групи даних DG13 потребує визначення у нормативній документації;
- необхідно генерувати запит на сертифікат відкритого ключа у програмному забезпеченні АЦСК.

Висновки

Розглянуто концепцію застосування ЕБП як засобів ЕЦП. Подальший розвиток цієї концепції потребує вирішення організаційних юридичних та технологічних питань. Проте розроблений авторами прототип дозволяє стверджувати, що ЕБП останніх поколінь можливо застосовувати для накладання ЕЦП.

Дане рішення має перспективу у поширенні технології ЕЦП. Однак, для того, щоб аргументувати доцільність матеріальних витрат з боку центрів сертифікації ключів та уряду, необхідні інструменти, які дозволять порівняти спосіб застосування ЕБП як засобу ЕЦП з іншими способами формування ЕЦП, що є предметом подальших досліджень.

Список використаних джерел

1. Об организации предоставления государственных и муниципальных услуг: Федеральный закон Российской Федерации от 27.07.2010 г. N 210-ФЗ // Российская Газета - Федеральный выпуск. 30.07. 2010. №5247.
2. Электронное голосование в Эстонии: https://www.valimised.ee/ru/uldkirjeldus.
3. Закон Естонии об удостоверяющих личность документах от 12.01.2012г.: http://mvd.riga.lv/uploads/documents/152.Personu_apliecinosu_rus.pdf.
4. E-Government Survey 2012. E-Government for the People // United Nations, New York, 2012: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf.
5. Машиносчитываемые проездные документы. Часть 1. Машиносчитываемые паспорта. Том 2. Спецификации на электронные паспорта со средствами биометрической идентификации. Издание шестое – 2006 // Международная организация гражданской авиации. – ИКАО: http://www.icao.int/publications/Documents/9303_p1_v2_cons_ru.pdf.
6. Java Card: http://www.oracle.com/us/technologies/java/embedded/card/overview/index.html.
7. jCardSim – Java Card Runtime Environment Simulator: http://jcardsim.org/.
8. JMRTD: An Open Source Java Implementation of Machine Readable Travel Documents: http://jmrtd.org.
9. The Legion of the Bouncy Castle: http://www.bouncycastle.org/.

10. Електронні підписи й інфраструктури (ESI) алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми (ETSI TS 102 176-1 V2.0.0 (2007-11), IDT): ДСТУ ETSI TS 102 176-1:2009 (Проект): http://dep145.org.ua/uk/node/96.

11. PKCS#11 Signer For Java: http://sourceforge.net/projects/pkcs11signer.

12. Про електронний цифровий підпис: Закон України від 22.05.2003р № 852-IV // Голос України. Від 27.06.2003. № 119.

13. Наказ міністерства юстиції України від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису зареєстрований в Міністерстві юстиції України від 20 серпня 2012 р. За № 1398/21710: http://zakon1.rada.gov.ua/laws/show/z1398-12.

Отримано 13.09.2014 р.