УДК 681.3

Кулажський В.І., к.т.н., доцент;
Берестов Д.С.;
Кульчицький О.С.

Центр воєнно-стратегічних досліджень Національного університету оборони України

Аналіз можливих шляхів реалізації електронно-цифрового підпису в ERP-системі

Резюме. У статті розглядаються можливі механізми та технічні рішення з реалізації електронно-цифрового підпису в ERP-системі, а також можливі варіанти зберігання закритого ключа асиметричних криптосистем.

Ключові слова: електронний документ, ERP-система, аутентифікація, електронно цифровий підпис, закритий ключ, відкритий ключ, криптосистема, пінкод.

Анализ возможных путей реализации электронно-цифровой подписи в ERP-системе

Резюме. В статье рассматриваются возможные механизмы и технические решения, с помощью которых может осуществляться реализация электронно-цифровой подписи в ERP-системе, а также возможные варианты хранения закрытого ключа асимметричных криптосистем.

Ключевые слова: электронный документ, ERP-система, аутентификация, электронно-цифровая подпись, закрытий ключ, открытый ключ, криптосистема, пінкод.

Analysis of possible ways of realizing the electronic digital signature in ERP-systems

Resume. The article discusses the possible mechanisms and technical solutions with which may be implementation of digital signatures in the ERP-system, as well as possible options for storing the private key asymmetrical cryptosystems.

Keywords: electronic document, ERP-system, authentication, electronic digital signature, private key, public key, cryptosystem.

Постановка проблеми.

Використання електронного документообігу в ERP-системі суттєво прискорює проведення паперової документації та скорочує її обсяги, економить час користувачів і витрати установ, які пов'язані з оформленням документів, поданням звітності в контролюючі органи, отриманням довідок від різних держустанов тощо. Але при цьому виникає проблема захисту учасників електронного документообігу від нав'язування їм хибної інформації, встановлення факту модифікації документів, які передаються по інформаційно-телекомунікаційнім каналам або зберігаються у базі даних ERP-системи, та отримання гарантії їх справжності [1].

На сьогодні вирішення цієї проблеми в ERP-системі здійснюється шляхом використання електронно-цифрового підпису (ЕЦП), який дозволяє здійснювати аутентифікацію як автора електронного документа так і самого документа. Це дає можливість використовувати ЕЦП в якості аналога власноручного підпису для надання електронним документам юридичної сили. Тому захист ЕЦП є одним з актуальних питань при впровадженні та супроводженні ERP-системи.

Ступінь розробленості проблеми.

При створенні ЕЦП, як правило, використовується асиметричне шифрування. Для його реалізації в мережі ERP-системи необхідно розгорнути інфраструктуру відкритих ключів, яка відповідає вимогам даної системи. Ключі в асиметричних криптосистемах завжди генеруються парами і складаються з двох частин – відкритого ключа та закритого ключа. Відкритий ключ використовується для шифрування інформації, є доступним для всіх користувачів і може бути опублікований в загальнодоступному місці для використання всіма користувачами криптографічної мережі. Дешифрування інформації за допомогою відкритого ключа неможливо. Закритий ключ використовується для дешифрування інформації і зберігається тільки в одного користувача, який згенерував

ключову пару. Ці два ключі володіють наступними характеристиками: ключі складають пару і функціонують разом. Неможливо розрахувати один із ключів, використовуючи інший.

Сам по собі ЕЦП являє собою відносно невелику кількість додаткової цифрової інформації, яка передається разом з документом, що підписується. У зв'язку з тим створення ЕЦП складається з двох процедур: процедури постановки підпису та процедури перевірки підпису, де відкритий ключ використовується при процедурі постановки підпису, а закритий ключ при процедурі перевірки підпису. Однак шифрування з відкритим ключем створює велике навантаження на процесор, тому при формуванні ЕЦП відправник насамперед обчислює хеш-функцію документа, який підписується. Її значення являє собою один короткий блок інформації, яка характеризує весь документ у цілому. Потім цей блок інформації шифрується ключем відправника. Одержувана при цьому пара чисел являє собою ЕЦП для даного документа. Це здійснюється з метою стиснення документа, який підписаний, до декількох десятків або сотень біт.

Мета статті.

Аналіз сучасних механізмів та технічних рішень щодо захисту ЕЦП, які можуть бути використані при впроваджені та супроводжені ERP-системи.

Виклад основного матеріалу.

Використання в електронному документообігу ERP-систем асиметричних криптосистем дозволяє забезпечити не тільки конфіденційність, але також достовірність і цілісність переданого електронного документа, де достовірність і цілісність електронного документа забезпечується формуванням ЕЦП і відправкою цього документа у зашифрованому вигляді. Перевірка відповідності підпису отриманого електронного документа після його попереднього розшифрування являє собою перевірку цілісності та автентичності прийнятого документа. В електронному документообігу ERP-системи ЕЦП враховується рівнозначним власноручному підпису при дотриманні наступних умов:

- сертифікат ключа підпису, що відноситься до даного ЕЦП, не втратив дії на момент перевірки або на момент підписання електронного документа за наявності доказів, які визначають момент підпису. Сертифікат ключа підпису засвідчує користувачу інформаційної системи дійсність ЕЦП та ідентифікує власника сертифіката ключа підпису;
- підтверджена достовірність ЕЦП в електронному документі. Підтвердженням достовірності ЕЦП в електронному документі є позитивний результат перевірки відповідним сертифікованим засобом ЕЦП із використанням сертифіката ключа підпису приналежності ЕЦП в електронному документі власникові сертифіката ключа підпису і відсутності спотворень у підписаному електронному документі;
- ЕЦП використовується відповідно до відомостей, зазначеними в сертифікаті ключа підпису.

Сучасні механізми захисту ЕЦП базуються на таких асиметричних криптосистемах: криптосистема RSA; криптосистема ECC; криптосистема Ель-Гамалі.

Криптосистема RSA [2, 3, 4] є широким прикладом криптосистеми з відкритим ключем. Вона всебічно досліджена і визнана криптостійкою при достатній довжині ключів. Її стійкість заснована на трудомісткості розкладанні на множники великих чисел. Однак зі зростанням потужності процесорів криптосистема RSA може втратити стійкість до атаки повного перебору, тому збільшення потужності процесорів приводить до застосування більш довгих ключів, що підвищує її стійкість.

Криптосистема RSA – дозволяє вирішити завдання підтвердження істинності електронного документа. Ця можливість заснована на тому, що зашифрувати дані, використовуючи закритий ключ замість відкритого ключа може тільки той, кому закритий ключ відомий. При цьому існує можливість перевірки застосування закритого ключа до даних без його розкриття. На сьогодні RSA є найбільш поширеною криптосистемою – стандартом для багатьох криптографічних додатків.

Криптосистема ECC [5,6,7] – система з відкритим ключем, що використовує алгебраїчну систему, яка описується в термінах точок еліптичних кривих, для реалізації асиметричного алгоритму шифрування. Широкому впровадженню ECC довго заважала слабка вивченість її математичного фундаменту криптосистеми, але проведені дослідження не виявили в її технології серйозних недоліків.

Стійкість шифрування системи ECC базується на складності задачі дискретного логарифмування, при цьому висока стійкість криптосистеми досягається при значно менших довжинах ключів, ніж у RSA. Згідно з рекомендаціями Національного інституту стандартів і технологій США, еквівалентом

1024-бітного ключа RSA, наприклад, є ECC-ключ довжиною всього 163 біта (співвідношення 6:1). Причому ця залежність нелінійна, тому для 512-бітного ключа ECC розмір аналога в системі RSA складає вже 15360 біт (співвідношення 30:1). Її сучасні реалізації показують, що вона набагато ефективніша, ніж інші системи з відкритими ключами. На сьогодні стандарт електронного цифрового підпису України ґрунтується на еліптичних кривих (ДСТУ 4145-2002 який набув чинності з 1 липня 2003 року).

Криптосистема Ель-Гамалі [6] – система з відкритим ключем, яка заснована на обчисленні дискретних логарифмів у кінцевому полі та складається з алгоритму шифрування і алгоритму ЕЦП. Головною перевагою схеми цифрового підпису Ель-Гамалі є можливість виробляти цифрові підписи для великого числа повідомлень з використанням тільки одного закритого ключа. Щоб порушнику підробити підпис, йому потрібно вирішити складні математичні завдання із знаходженням логарифма в кінцевому полі. Недоліком цієї системи є відсутність семантичної стійкості. На відміну від RSA алгоритм Ель-Гамалі не був запатентований і, тому, став більш дешевою альтернативою, оскільки не вимагалася оплата внесків за ліцензію. Схема Ель-Гамалі полягає в основі стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

Розглядаючи вищезазначені асиметричні криптосистеми слід відмітити, що перспективним напрямком їх розвитку є квантова криптографія [7]. Вона дозволяє забезпечити безпечну передачу ключових даних по волоконно-оптичному кабелю. Суть полягає в наступному: інформація про ключі кодується в одному-єдиному фотоні світла, який потім передається одержувачу. Згідно законам квантової фізики, неможливо виміряти один параметр фотона, не спотворивши при цьому інший. Тому спроба перехоплення ключа неминуче спровокує порушення в квантовій системі та призведе до спотворення переданої інформації. Таким чином, факт проникнення в систему легко встановлюється, а сторонам, які обмінюються інформацією доведеться тільки повторити сеанс зв'язку з іншим ключем.

Сучасні технічні рішення ЕЦП. В ERP-системах існують інтерфейси для підключення засобів ЕЦП. Наприклад у SAP NetWeaver таким інтерфейсом є Secure Store & Forward (SSF) [8, 9]. При роботі з електронним документом SSF дозволяє реалізовувати процедури обробки і підписання документа, які застосовуються для паперових документів. Також SSF здійснює захист даних за допомогою так званих цифрових конвертів. Цифрові конверти гарантують, що дані, які захищаються, будуть доступні тільки тому, для кого вони призначені. Механізм створення ЕЦП та цифрових конвертів засновано на технології відкритих ключів. У користувача, який створює електронні підписи або цифрові конверти, є пара ключів – відкритий і закритий.

При створені ЕЦП відкритий ключ використовується для того, щоб підписати документ. Після того, як документ був підписаний, для його прочитання користувач-одержувач повинен володіти закритим ключем, необхідним для доступу до зашифрованої інформації. Даний механізм може додавати одну або декілька цифрових підписів до будь-якого набору даних, будь то файл або таблиця в базі даних системи.

Щоб створити цифровий конверт, використовується закритий ключ повідомлення для "упаковки" документа в "конверт". Одержувач повідомлення повинен знати цей ключ, щоб розшифрувати документ. Тому ключ повідомлення зашифровується з використанням відкритого ключа одержувача і відправляється разом з документом.

Таким чином за допомогою SSF в ERP-системі можливо:

- здійснювати аутентифікацію як автора електронного документа так і самого документа;
- забезпечити цілісність даного документа;
- пересилати та зберігати зашифровані дані.

Програмне забезпечення "КАРМА" [10, 11]. Воно призначено для реалізації функцій криптографічного захисту інформації та застосування ЕЦП, а також для безпосереднього захисту файлів і документів від несанкціонованого доступу. Може використовуватися у будь-яких системах різного рівня та призначення, які потребують використання засобів електронного підпису та шифрування. З її допомогою користувачі можуть працювати з електронним підписом файлів безпосередньо з провідника Windows.

У "КАРМІ" використовується високорівневий інтерфейс, не вимагає умінь оперувати спеціальними криптографічними об'єктами, наприклад, ключовими контейнерами, хеш-функціями й іншими – усе це система робить сама. Таким чином, до переваг "КАРМИ" можна віднести простоту використання: системі достатньо надати оброблюваний файл, сертифікат відкритого ключа та вказати, яку дію потрібно зробити. Всі

необхідні параметри криптопровайдера і послідовність операцій будуть визначені автоматично. “КАРМА” може працювати в стандартних операційних сісемах Microsoft Windows. В системі реалізований механізм додавання до складу ЕЦП факсиміле - графічного зображення власноручного підпису. Зображення може бути сформовано безпосередньо в момент підписання за допомогою планшета або тач-скрін, або завантажене з файла.

Програмне забезпечення “КАРМА” застосовується разом з програмою EDSIGN [10, 12], яка являє собою програмну надбудову над Microsoft Office Word 2007 і використовується для створення електронного документа у форматі приєднаного ЕЦП. Застосовуючи Edsign, можна підписувати будь-які текстові документи і замінити паперовий документообіг електронним. Процес підписання електронних документів простий і відбувається у звичному інтерфейсі текстового редактора Microsoft Word.

На сам кінець слід відмітити що реалізація ЕЦП на базі асиметричних криптосистем передбачає високий рівень захисту закритих ключів. У сучасних ERP-системах з електронним документообігом такий захист може здійснюватися за допомогою спеціальних сховищ, наприклад e-Token і Rutoken. (або просто “токен”). Це захищені сховища у вигляді USB-брелоків та смарткарт, доступ до яких здійснюється тільки за пінкодом. При введенні невірного пінкоду більше трьох разів сховище блокується, запобігаючи спроби доступу до ключа шляхом підбору необхідного значення пінкоду. Всі операції з ключем здійснюються в пам’яті сховища, тобто ключ ніколи його не покидає. Таким чином, виключається перехоплення ключа з оперативної пам'яті.

Крім вищезазначених переваг при використанні захищених сховищ можна виділити ще такі:

- гарантується збереження закритого ключа, в тому числі при втраті носія на час, необхідний для відкликання сертифіката;
- немає необхідності встановлювати сертифікат закритого ключа на кожен комп'ютер, з якого працює користувач;
- “токен” можна одночасно використовувати для авторизації при вході в операційну систему комп’ютера і в систему електронного документообігу. Тобто він стає персональним засобом аутентифікації.

Використання в ERP-системі спеціалізованих сховищ передбачає додаткові витрати, але при цьому значно збільшується як рівень безпеки закритих ключів так і самої системи в цілому.

Висновки

1. Використання в електронному документообігу ERP-системи асиметричних криптосистем дозволяє забезпечити не тільки конфіденційність, але й достовірність і цілісність переданого електронного документа, де його достовірність і цілісність забезпечується формуванням ЕЦП. Сучасні механізми захисту ЕЦП базуються на наступних асиметричних криптосистемах : криптосистема RSA; криптосистема ECC; криптосистема Ель-Гамалі.

2. Криптосистема RSA використовується для шифрування даних і ЕЦП. Вона визнана криптостійкою при достатній довжині ключів. Її стійкість заснована на трудомісткості розкладання на множники великих чисел. Однак із зростанням потужності процесорів криптосистема RSA може втратити стійкість до атаки повного перебору. Тому збільшення потужності процесорів приводить до застосування більш довгих ключів.

3. Криптосистема ECC використовує алгебраїчну систему, яка описується в термінах точок еліптичних кривих, для реалізації асиметричного алгоритму шифрування. Стійкість шифрування системи ECC базується на складності задачі дискретного логарифмування, при цьому висока стійкість криптосистеми досягається при значно менших довжинах ключів, ніж у RSA. На сьогодні стандарт ЕЦП України грунтується на еліптичних кривих (ДСТУ 4145-2002 який набув чинності з 1 липня 2003 року).

4. Криптосистема Ель-Гамалі заснована на обчисленні дискретних логарифмів у кінцевому полі. Вона включає як алгоритм шифрування так і алгоритм ЕЦП. Головною перевагою схеми цифрового підпису Ель-Гамалі є можливість виробляти цифрові підписи для великого числа повідомлень з використанням тільки одного закритого ключа. Щоб порушнику підробити підпис, йому потрібно вирішити складні математичні завдання із знаходженням логарифма в кінцевому полі. Недоліком цієї системи є відсутність семантичної стійкості. Схема Ель-Гамалі полягає в основі стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

5. У сучасних ERP-системах існують інтерфейси для підключення засобів ЕЦП. Наприклад, у SAP NetWeaver таким інтерфейсом є Secure Store & Forward (SSF). При роботі з електронним документом SSF

дозволяє реалізовувати ті самі процедури обробки й підписання документа, які застосовуються для паперових документів. Також SSF здійснює захист даних за допомогою цифрових конвертів. Механізм створення ЕЦП та цифрових конвертів заснован на технології відкритих ключів.

6. Програмне забезпечення "КАРМА" призначено для реалізації функцій криптографічного захисту інформації та застосування ЕЦП, а також для безпосереднього захисту файлів і документів від несанкціонованого доступу. Воно дає можливість працювати з електронним підписом файлів безпосередньо з провідника Windows. Програмне забезпечення "КАРМА" застосовується разом з програмою EDSIGN, яка являє собою програмну надбудову над Microsoft Office Word 2007 і використовується для створення електронного документа у форматі приєднаної ЕЦП.

7. Реалізація в електронному документообігу ERP-систем ЕЦП на базі криптосистем із відкритим ключем передбачає високий рівень захисту закритих ключів. У сучасних ERP-системах такий захист може здійснюватися за допомогою спеціальних сховищ, наприклад e-Token і Rutoken. Це захищені сховища у вигляді USB-брелоків та смарткарт, доступ до яких здійснюється тільки за пінкодом.

Напрямки подальших наукових досліджень доцільно зосередити на подальшому удосконаленню механізмів та технічних рішень щодо створення ЕЦП в ERP-системах.

СПИСОК ЛІТЕРАТУРИ

1. Ю.Г. Платонов. Анализ требований к системе "электронный документооборот" на предприятии с высокой степенью ответственности с точки зрения применения современных информационных систем. Институт систем информатики СО РАН, 630090, Новосибирск, Россия. http://www.problem-info.ru/2011-1/5.pdf.
2. Харин Ю.С. и др. Математические основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Мн.: БГУ, 1999. -319 с.
3. Современные алгоритмы шифрования, BYTE/Россия № 8, 2003.
4. Криптосистема RSA. http://onlinesrv.ru/31-kriptosistema-rsa.html.
5. Астапенко Г.Ф. Аппаратно-программные методы и средства защиты информации / Г.Ф. Астапенко. – Минск : БГУ, 2008. 188с.
6. Бабичев С.Г., Серов Р.Е. Основы современной криптографии. http://window.edu.ru/resource/005/24005/files/crypto1-3.pdf.
7. Перспективы развития современной криптографии. http://www.deltann.ru/10/d-102007/p-22.
8. Обеспечение информационной безопасности в решениях SAP. http://www.sap.com/cis/pdf/sap_security.pdf.
9. Шония О., Цомая Н. ERP-система: прикладная безопасность и защита электронных документов. Automated control systems – № 2(9), 2010. http://www.gtu.edu.ge/jurnalebi/mas/Referat/2010(2-9)/12_78-81%20ComaiaOtto-2+--.pdf.
10. Электронная подпись и защита информации. http://www.eos.ru/eos_products/solution/elektronnaya_podpis_i_zashchita_informatsii/.
11. Внедорожный П. "Карма" от ЭОС: защищаем е-документы. http://www.infobez.com/article.asp?ob_no=7343.
12. Новые версии систем КАРМА и EDSIGN. http://www.eos.ru/eos_support/news/detail.php?ID=96574.

Рецензент: Рибидайло А.А. – к.т.н.,с.н.с., ЦВСД НУО України.
Поступила в редакцію 25.03.13