УДК 681.3:002

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПІД ЧАС ЗБЕРІГАННЯ, ОБРОБКИ ТА ПЕРЕДАЧІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Леляк А.В., Астраханцев А.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lelyak.andrey@gmail.com

ENSURING PROTECTION DURING STORAGE, PROCESSING AND TRANSMISSION OF ELECTRONIC DOCUMENTS

Electronic documents security principles are analyzed for three main implementation options: foreign passport with embedded chip, mobile driving license on a smartphone and server-based solution with a “thin” client on smartphone.

Електронне посвідчення особи – це цифрове рішення, що дозволяє громадянам підтвердити свою особистість без використання паперових документів. Основними варіантами імплементації електронних документів є імплементація згідно зі стандартом ICAO Doc 9303 [1] (закордонний паспорт з інтегрованим чіпом), імплементація згідно зі стандартом ISO/IEC 18013-5 [2] (електронне посвідчення водія) та внутрішні рішення всередині окремих країн, як-от Дія, що не забезпечують міжнародної сумісності. Рівень безпеки електронних документів є одним з вирішальних факторів [3] для переходу від паперових документів, оскільки конфіденційність, цілісність та стабільність доступу є гарантією взаємної довіри між громадянином та державою. Наприклад, для уніфікованого розв'язування типових задач безпеки електронних документів був створений регламент Європейського Союзу про електронну ідентифікацію та довірчі послуги для електронних транзакцій (eIDAS), і велика кількість країн докладають суттєвих зусиль для сумісності з цим стандартом [4].

Для порівняння шляхів розв'язання задач безпеки розглянемо три імплементації електронних документів:

1. Класичний закордонний паспорт з чіпом згідно зі стандартом ICAO Doc 9303
2. Електронне посвідчення водія в Google Wallet чи Samsung Wallet згідно зі стандартом ISO/IEC 18013-5
3. Рішення «Дія» від Міністерства цифрової трансформації України

Закордонний паспорт реалізований у вигляді пластикової картки з інтегрованим чіпом, де паспортні дані дублюються в надрукованому та електронному вигляді. Мобільне посвідчення водія реалізоване у вигляді застосунку для iOS чи Android, чутливі дані якого зберігаються на окремому захищеному чипі всередині телефону. «Дія» теж реалізована як застосунок для iOS чи Android, але дані зберігаються на віддаленому захищеному сервері.

Основними компонентами будь-якої системи електронних документів є орган видачі, тримач та зчитувач документа. Орган видачі зберігає та керує документами, і видає їх тримачу документа. Тримач документа зберігає

документ у себе на пристрої та надає його зчитувачу на вимогу. Зчитувач отримує документ від тримача та перевіряє його.

Розглянемо наступні задачі безпеки для електронних документів:

1. Уникнути несанкціонованої вичитки даних документа
2. Уникнути підслуховування каналу зв'язку
3. Автентифікувати сховище документа
4. Автентифікувати дані документу
5. Автентифікувати зчитувач
6. Отримати згоду тримача документа на передачу даних

Уникнення несанкціонованої вичитки закордонного паспорта забезпечується використанням гаманця з RFID-захистом, як і для банківських карт, що використовують схожий чіп. Для водійського посвідчення в телефоні використовуються засоби контролю доступу операційної системи такі, як вимкнення NFC, направлення NFC запитів лише до авторизованих додатків та додаткова автентифікація користувача на початку обробки повідомлень в додатку. Для рішень, що ґрунтуються на збережені даних на захищеному сервері, ця задача безпеки виконується через посилання документа лише після двосторонньої автентифікації сервера з додатком.

Основним способом захисту від підслуховування каналу зв'язку є шифрування цього каналу. Для закордонних паспортів використовується механізм PACE (Password Authenticated Connection Establishment), що формує сесійні AES ключі за допомогою даних з зони машинного зчитування (Machine Readable Zone, MRZ), надрукованої на пластику документа. Схожим чином працює шифрування каналу зв'язку для передачі електронного посвідчення водія, де AES ключі формуються з сесійних даних, унікальних для кожної передачі даних між тримачем документа та зчитувачем. Для шифрування передачі даних між «Дією» та сервером використовується протокол TLS, як і для більшості застосунків.

Для автентифікації сховища документа у випадку закордонного паспорта використовується механізм Chip Authentication, за допомогою якого формуються нові симетричні сесійні ключі на базі асиметричного статичного ключа з чіпа та асиметричного сесійного ключа зчитувача. У випадку електронного посвідчення водія використовуються механізм mDoc Authentication, під час якого тримач документа накладає електронний підпис чи рахує Message Authentication Code (MAC) на метадані документа і передає його зчитувачу разом зі своїм сертифікатом. Для рішень, що базується на збереженні даних документа на сервері, використовується класичний підхід Public Key Infrastructure (PKI), в якому застосунок та сервер обмінюються сертифікатами та перевіряють їх.

Для автентифікації даних документа у всіх рішеннях використовується цифровий підпис, що накладається органом видачі на дані документа, зберігається разом з документом, і передається разом з документом зчитувачу, щоб підтвердити автентичність цих даних.

Для автентифікації зчитувача закордонного паспорта виконується процедура Terminal Authentication, під час якої зчитувач підписує своїм приватним асиметричним ключем довільні дані, надіслані тримачем документа, а тримач має змогу перевірити цей підпис за допомогою надісланого сертифіката зчитувача з асиметричним публічним ключем. Для електронного

водійського посвідчення використовується механізм Reader Authentication, під час якого схожим чином зчитувач підписує дані, що унікальні для поточної сесії передачі даних, а зчитувач перевіряє валідність цього підпису за допомогою сертифіката зчитувача. «Дія» використовує схожий власний механізм.

Для отримання згоди тримача документа на передачу даних чи їх частини потрібен факт свідомого вибору та підтвердження користувача. Для закордонного паспорта це є демонстрація документа особі, що його перевіряє, та прикладання документа до зчитувача. Для мобільного водійського посвідчення це вибір потрібного UI елемента в застосунку на екрані телефону, а для «Дії» це демонстрація QR-коду особі, що перевіряє документ. Також протоколи зі специфікації мобільного водійського посвідчення дозволяють тримачу документа обирати, які поля документа повернути з тих, що запросив зчитувач, що поки не реалізоване в інших варіантах імплементації.

Було розглянуто три варіанти безпечного сховища електронних документів – чіп, вбудований в картку, окремий процесор в мобільному пристрої та сервер. Для розв'язання задач безпеки використовуються різні технічні засоби та протоколи, але всі перераховані рішення є в середньому достатньо безпечними для використання державними структурами. Вибір між цими варіантами імплементації електронних документів повинен базуватися на потребах держави та технічних можливостях держави та мобільних пристроях більшості громадян. Перевагою рішення з чіпом в картці є повний контроль центра видачі над комплексним рішенням електронного документа, що забезпечує високий рівень безпеки при дотриманні всіх протоколів. Рішення з захищеним процесором в телефоні є компромісним варіантом, що дозволяє зберігати електронний документ на будь-якому сучасному мобільному пристрої з високим рівнем безпеки. В такому підході можуть використовуватися більш сучасні та складні підходи до безпеки, але незахищений телефон користувача може бути використаний як додаткова точка входу в систему для нападника. Рішення зі збереженням документа на сервері є найменш вибагливим до користувацьких пристроїв, і дозволяє зосередити більшість зусиль з підвищення безпеки на віддаленому сервері. Але таке рішення потребує зв’язку з сервером як для тримача документа, так і для зчитувача для будь-якої операції.

Література

1. Machine Readable Travel Documents, ICAO Doc 9303 v8, 2021.
2. Personal identification — ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application, ISO/IEC 18013-5:2021, 2021.
3. V. Tsap, “eID Public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity,” Ph.D. dissertation, Tallinn University of Technology, Tallinn, Estonia, 2022.
4. A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, and S. Ranise, “The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes,” *Applied Sciences*, vol. 12, no. 24, p. 12679, Dec. 2022, doi: https://doi.org/10.3390/app122412679.