

ВИКОРИСТАННЯ ГРУПОВИХ ПІДПИСІВ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Вінницький національний технічний університет

Анотація

Розглянуто застосування групових підписів у системах електронного документообігу та наведено приклади їх використання у таких системах. Наведено результати дослідження популярних українських і іноземних систем електронного документообігу, розглянуто їх основні особливості та функціональні можливості, отримано інформацію щодо використання групових підписів у їх роботі. Виходячи із результатів, отриманих протягом цього дослідження, зроблено висновок, щодо в собі результати про доцільність використання таких підписів та їх потенціал використання у система електронного документообігу.

Ключові слова: анонімність, електронний цифровий підпис, групові підписи, система електронного документообігу, кібербезпека, неув'язність.

Abstract

This study explores the application of group signatures, in electronic document management systems, and examples of their implementation in such systems. The study presents the results of an analysis of popular Ukrainian and foreign electronic document management systems, highlighting their key features and functional capabilities, as well as gathering information on the use of group signatures in their operation. Based on the findings of this research, a conclusion has been drawn regarding the feasibility of the such signatures usage and their potential application potential in electronic document management systems.

Keywords: anonymity, electronic digital signature, group signatures, electronic document management system, cybersecurity, documents, unlinkability.

Вступ

Рух документів у великих державних та приватних підприємствах відіграє критичну роль у їх функціонуванні та потребує додаткових рішень безпеки. Щоб задовільнити цю потребу зазвичай використовують електронні цифрові підписи, однак їх функціональність є досить обмеженою у випадках потреби анонімності підписанта або підпису документа декількома особами одночасно, щоб задовільнити такі потреби доцільним рішенням є використання групових підписів.

Метою роботи є покращення захисту приватності у системах електронного документообігу на основі використання групових підписів, доцільності та ефективності їх використання.

Аналіз групових підписів

Груповий підпис – це примітив з відкритим ключем, який дозволяє членам групи генерувати підписи від імені групи, до якої вони належать. Таким чином при потребі перевірки згенерованого підпису, можна впевнитися у його коректності, не розкриваючи особу, що його згенерувала, або взагалі не маючи можливості його ідентифікації [1,2]. Виходячи із таких його властивостей, цей метод електронного підпису найкраще підійде у випадках коли потрібно забезпечити анонімність підписанта або при необхідності підпису документа певною довіреною групою людей. Наприклад під час перевірки та тестуванні якості написаного програмного коду в організації, під час підписання робочих звітів, було б доречно приховувати особистість людини, що виконувала цю перевірку, задля уникнення суперечок серед персоналу підприємства. Також це буде корисним при завантаженні файлів у систему із певним рівнем безпеки, що потребує підтвердження приналежності особи до організації або під час голосування, коли потрібно забезпечити анонімність та запобігти подвійному голосуванню.

Початкову реалізацію такого підпису було запропоновано Девідом Чаумом та Юджин ван Гейстом (David Chaum, Eugene van Heyst) [2]. Загальний процес створення підпису виглядає таким чином: формується група осіб, після чого адміністратор групи генерує приватний та публічний ключ групи після чого кожному із членів видається свій особистий приватний ключ, далі при необхідності підписання

підписант повинен використати свій приватний ключ та публічний ключ групи для створення підпису. Існує велика кількість видів методів підписів, кожен із яких має свої функціональні особливості так і методику реалізації. Так є можливість створити підписи для генерування яких потрібна певна кількість членів групи, а не лише одна особа, підписи із можливістю, відстеження підписанта, так і її відсутності, підписи публічний ключ яких змінюється при зміні складу початкової групи.

Аналіз систем електронного документообігу

Було досліджено низку систем електронного документообігу: flydoc [3], vchasno [4], medoc [5], box [6], m-files [7], revverdocs [8]. Кожна із систем має свої переваги та недоліки, функціональні особливості. Таким чином flydoc виділяється можливістю створення документів на основі облікових документів «BAS». Vchasno має високу гнучкість налаштування, що дозволяє налаштувати робочі процеси відповідно до потреб компанії. Medoc є лідером українського ринку, широко інтегрований із державними службами, box орієнтується на хмарне зберігання файлів та зручний доступ до документів з будь-якого пристрою. M-files виділяється використанням метаданим, що дозволяє оптимізувати процеси пошуку, класифікації та управління документами в складних бізнес-середовищах. Revverdocs орієнтований на автоматизацію документообігу з акцентом на гнучке налаштування робочих процесів. Однак не зважаючи на всі їх переваги отриманий результат показав що ні одна із наведених вище систем не має у своєму функціоналі можливість створення та використання групових підписів.

Одними із головних причин відсутності цього метода безпеки є і його головні недоліки так і переваги. Стандартні цифрові підписи регулюються відповідними законами та міжнародними нормами, однак у випадку групових підписів постає проблема їх юридичного урегулювання. Залежно від конфігурації підпису можуть виникнути певні проблеми, такі як анонімність підписанта не завжди можна виявити через адміністратора групи, постає питання способу організації такої групи, хто і як буде її регулювати. Також відсутність функцій групового підпису може бути спричиненим, використанням окремого програмного засобу для його створення та регулювання.

Висновки

Як висновок, груповий підпис є чудовим інструментом для забезпечення безпеки та анонімності автора документів, із наявністю гнучкого налаштування його властивостей, відповідно до вимог його використання у системі. Такі підписи мають можливість забезпечення неув'язності підписанта, що може значно вплинути на взаємини колективу, так як людина підписант може не перейматися про її репутації серед цієї групи людей, як наслідок таких змін, ефективність та точність прийнятих рішень буде значно покращено. Також вони можуть бути ефективні при застосуванні під час контролю доступу у системі та при проведенні анонімних голосувань.

Так як групові підписи не мають широкого застосування у системах електронного документообігу, реалізація система із такими особливостями безпеки є одним із майбутніх шляхів розвитку безпеки у багатьох їх сферах роботи. Таким чином створення цих систем мають як високу практичну та інтелектуальну цінність так і високу перспективність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. M. Laurent, S. Belguith. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. Journal of Network and Computer Applications, Volume 171, 2020, URL: <https://doi.org/10.1016/j.jnca.2020.102807>. (accessed: 18.03.2025).
2. D. Chaum, E. van Heyst. Group Signatures. Advances in Cryptology - EUROCRYPT '91, LNCS 547, 1991, pp. 257-265. URL: https://link.springer.com/content/pdf/10.1007/3-540-46416-6_22.pdf (accessed: 18.03.2025).
3. FlyDoc. Підписання документа ЕП. URL: <https://flydoc.ua/help/userguide/index.html> (дата звернення: 18.03.2025).
4. Вчасно.ЕДО. Як підписати вхідний документ. URL: <https://help.vchasno.com.ua/signdoc/> (дата звернення: 18.03.2025).
5. Medoc. Робота з КЕП (ЕЦП) та захищеними носіями особистих ключів. URL: <https://medoc.ua/faq/category/robota-z-ecp> (дата звернення: 18.03.2025).
6. Box Sign. URL: <https://www.box.com/esignature> (accessed: 18.03.2025).

7. M-files. E-Signatures. URL: <https://www.m-files.com/m-files-platform/integrations/e-signatures/> (accessed: 20.03.2025).
8. Revverdocs. How to Use eSignature with Revver. URL: <https://www.revverdocs.com/how-to-use-esignature-with-revver/> (accessed: 20.03.2025).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Лобай Дмитро Віталійович — студент групи ІБК-216, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: dimastudl1@gmail.com

Yurii Baryshev — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua

Lobai Dmytro — student of ІБК-24m group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: dimastudl1@gmail.com