

ISSN 2786-5460 (Print)
ISSN 2786-5479 (Online)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

Випуск 4 (15), 2024
Issue 4 (15), 2024



Видавничий дім
«Гельветика»
2024

*Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 12 від 26 грудня 2024 року)*

Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2024. – Випуск 4 (15). – 130 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Головний редактор: Попов О. О. – член-кор. НАН України, д-р техн. наук, професор, в.о. директора Центру інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України.

Редакційна колегія:

Василенко М. Д. – д-р фіз.-мат. наук, проф., професор кафедри кібербезпеки, Національний університет «Одеська юридична академія»; **Горбов І. В.** – канд. техн. наук, с.н.с., старший науковий співробітник, Інститут проблем реєстрації інформації НАН України; **Дуднік А. С.** – д-р техн. наук, доц., доцент кафедри мережевих та інтернет технологій, Київський національний університет імені Тараса Шевченка; **Євсєєв С. П.** – д-р техн. наук, професор кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені Семена Кузнеця; **Зибін С. В.** – д-р техн. наук, доц., завідувач кафедри інженерії програмного забезпечення, Національний авіаційний університет; **Кавун С. В.** – д-р екон. наук, канд. техн. наук, проф., завідувач кафедри комп'ютерних інформаційних систем та технологій, Міжрегіональна Академія управління персоналом; **Комарова Л. О.** – д-р техн. наук, с.н.с., директор Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Мілов О. В.** – д-р техн. наук, професор кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені Семена Кузнеця; **Охріменко Т. О.** – канд. техн. наук, старший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет; **Рудніченко М. Д.** – канд. техн. наук, доц., доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка»; **Скुरатовський Р. В.** – канд. фіз.-мат. наук, доц., доцент кафедри обчислювальної математики та комп'ютерного моделювання, Міжрегіональна Академія управління персоналом; **Супрун О. М.** – канд. фіз.-мат. наук, доц., доцент кафедри програмних систем і технологій, Київський національний університет імені Тараса Шевченка; **Табунщик Г. В.** – канд. техн. наук, проф., професор кафедри програмних засобів, Національний університет «Запорізька політехніка»; **Фомін О. О.** – д-р техн. наук, доц., професор кафедри комп'ютеризованих систем управління, професор кафедри прикладної математики та інформаційних технологій, Державний університет «Одеська політехніка»; **Хохлячова Ю. Є.** – канд. техн. наук, доц., доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет; **Чолишкіна О. Г.** – канд. техн. наук, доц., директор Інституту комп'ютерно-інформаційних технологій та дизайну, Міжрегіональна Академія управління персоналом; **Чорний О. П.** – доктор технічних наук, професор, директор Навчально-наукового інституту електричної інженерії та інформаційних технологій, Кременчуцький національний університет імені Михайла Остроградського; **Юдін О. К.** – д-р техн. наук, проф., директор центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Гопесенко Віктор** – dr. sc. ing., проф., проректор з наукової роботи, директор навчальної програми магістратури «Комп'ютерні системи», Університет прикладних наук ISMA (Латвійська Республіка); **Leszczyna Rafal** – dr hab. inż., професор кафедри комп'ютерних наук у менеджменті, Гданський технологічний університет (Республіка Польща).

Реєстрація суб'єкта у сфері друкованих медіа:

Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.

Відповідно до Наказу МОН України № 1290 від 30 листопада 2021 року (додаток 3) журнал включено до Переліку наукових фахових видань України (категорія Б) зі спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 124 – Системний аналіз, 125 – Кібербезпека, 126 – Інформаційні системи та технології.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
<http://journals.maup.com.ua/index.php/it>

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення
StrikePlagiarism.com від польської компанії Plagiat.pl.

*Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 12 dated 26 December 2024)*

Information Technology and Society / [chief editor Oleksandr Popov]. – Kyiv : Interregional Academy of Personnel Management, 2024. – Issue 4 (15). – 130 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Chief editor: Oleksandr Popov – Corresponding Member of NAS of Ukraine, Doctor of Engineering, Professor, Acting Director of the Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine.

Editorial Board:

Mykola Vasylenko – Doctor of Physics and Mathematics, Professor, Professor at the Department of Cybersecurity, National University «Odesa Law Academy»; **Ivan Horbov** – PhD in Engineering, Senior Research Associate, Senior Research Fellow, Institute for Information Recording of NAS of Ukraine; **Andrii Dudnik** – Doctor of Engineering, Associate Professor, Senior Lecturer at the Department of Networking and Internet Technologies, Taras Shevchenko National University of Kyiv; **Serhii Yevseiev** – Doctor of Engineering, Professor at the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics; **Serhii Zybin** – Doctor of Engineering, Associate Professor, Head of the Department of Software Engineering, National Aviation University; **Serhii Kavun** – Doctor of Economics, PhD in Engineering, Professor, Head of the Department of Computer Information Systems and Technologies Interregional Academy of Personnel Management; **Larysa Komarova** – Doctor of Engineering, Senior Research Scientist, Laureate of State Prize, Director of Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Oleksandr Milov** – Doctor of Engineering, Professor at the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics; **Tetiana Okhrimenko** – PhD in Engineering, Senior Research Scientist at the Scientific Research Laboratory for Countering Aviation Cyberthreats, National Aviation University; **Mykola Rudnichenko** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technologies, Odessa Polytechnic State University; **Ruslan Skuratovskiy** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of Personnel Management; **Olha Suprun** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv; **Halyna Tabunshchuk** – PhD in Engineering, Professor, Professor at the Department of Software Tools, “Zaporizhzhia Polytechnic” National university; **Oleksandr Fomin** – Doctor of Engineering, Associate Professor, Professor at the Department of Computerized Control Systems, Professor at the Department of Applied Mathematics and Information Technologies, Odessa Polytechnic State University; **Yuliia Khokhlachova** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technology Security, National Aviation University; **Olha Cholyshkina** – PhD in Engineering, Associate Professor, Director of the Institute of Computer Information Technologies and Design, Interregional Academy of Personnel Management; **Oleksii Chorny** – Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Institute of Electrical Engineering and Information Technologies, Kremenchuk National University named after Mykhailo Ostrogradskyi; **Oleksandr Yudin** – Doctor of Engineering, Professor, Director of the Cybersecurity Center of the Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Hopeienko Viktor** – dr. sc. ing., Professor, Vice Rector for Research, Director of the study programme “Computer systems”, ISMA University of Applied Sciences (Republic of Latvia); **Leszczyna Rafal** – dr hab. inż., Profesor, Katedra Informatyki w Zarządzaniu, Politechnika Gdańska (Republic of Poland).

Registration of Print media entity:

Decision of the National Council of Television and Radio Broadcasting of Ukraine: Decision No. 1173 as of 11.04.2024.

According to the Decree of MES No. 1290 (Annex 3) dated November 30, 2021, the journal was included in the List of scientific professional publications of Ukraine (category B) in specialties 121 – Software engineering, 122 – Computer sciences, 123 – Computer engineering, 124 – Systems analysis, 125 – Cybersecurity, 126 – Information systems and technologies.

All electronic versions of articles in the collection are available on the official website edition
<http://journals.maup.com.ua/index.php/it>

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

© Interregional Academy of Personnel Management, 2024
© Copyright by the contributors, 2024

ЗМІСТ

Олег БОНДАРЧУК, Сергій ЗИБІН, Світлана ВАСИЛЮК-ЗАЙЦЕВА ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ КВАНТОВИХ КОМП'ЮТЕРІВ У РОЗВ'ЯЗАННІ СКЛАДНИХ ЗАВДАНЬ	6
Олександр БОРИСОВ, Марія ТЯГУНОВА ПІДХІД ДО АВТОМАТИЗАЦІЇ ЗАМОВЛЕНЬ У РЕСТОРАНІ З ВИКОРИСТАННЯМ ІТ-ТЕХНОЛОГІЙ	14
Тетяна ВАВРИК, Ліда ГОБИР ОПТИМІЗАЦІЯ ЗАХИСТУ ДАНИХ: ПРЕВЕНТИВНІ ТА РЕАКТИВНІ СТРАТЕГІЇ.....	21
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА ЕТИКИ У ВИКОРИСТАННІ ВІДКРИТИХ ДАНИХ ДЛЯ РОЗРОБКИ ДОДАТКІВ	26
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ КОНЦЕПЦІЯ ПІДКЛЮЧЕННЯ ФІЗИЧНИХ ОБ'ЄКТІВ У РОЗУМНОМУ БУДИНКУ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ТА ПОКРАЩЕННЯ ЯКОСТІ ПОВІТРЯ.....	30
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ ВИКОРИСТАННЯ КРИПТОГРАФІЇ ЯК СЕРВІСУ У ВЕБ ПРОГРАМУВАННІ	35
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ МАЙБУТНЄ ПРОГРАМУВАННЯ: ЯК ШТУЧНИЙ ІНТЕЛЕКТ ЗМІНЮЄ РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	40
Андрій ДУДНІК, Олег ТИЩЕНКО, Дарина ЯРЕМЕНКО ОГЛЯД СУЧАСНИХ ТЕХНІЧНИХ ТА ПРОГРАМНИХ РІШЕНЬ ДЛЯ УПРАВЛІННЯ БПЛА.....	44
Максим ДЬЯЧЕНКО, Андрій РОСКЛАДКА ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕС МЕНЕДЖМЕНТУ ІНЦИДЕНТІВ.....	51
Денис ЄФІМОВ, Роман ТИМОШЕНКО, Катерина ВОЙТЕХ ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНІ БОЙОВІ СТРАТЕГІЇ.....	58
Олексій КЛИМЕНКО СТВОРЕННЯ SELF-HEALING МЕРЕЖІ	63
Владислав КОЗУБ ІНФОРМАЦІЙНА ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ РОЗПОДІЛЕННОГО ШТУЧНОГО ІНТЕЛЕКТУ	71
Богдан КОРНІЄНКО, Леся ЛАДІЄВА, Ксенія УЛЬЯНИЦЬКА, Лілія ГАЛАТА Андрій НЕСТЕРУК ЗАХИСТ КРИТИЧНИХ РЕСУРСІВ ВЕБ-ЗАСТОСУНКУ З ОРЕНДИ НЕРУХОМОСТІ.....	80
Максим КУНДОС, Людмила СОЛОВЕЙ WEB ДОДАТКИ У ЕКОСИСТЕМІ ІОТ.....	88
Сергій ЛУК'ЯНЕНКО, Павло ВДОВІН, Валентин ГРОМИКО, Роман ТИМОШЕНКО РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНІЙ УКРАЇНСЬКІЙ ВІЙСЬКОВІЙ СПРАВІ.....	94
Геннадій МОГИЛЬНИЙ, Володимир ДОНЧЕНКО, Світлана ДОНЧЕНКО ОГЛЯД ТА АНАЛІЗ ІНСТРУМЕНТІВ СТВОРЕННЯ КОРПОРАТИВНОГО СЕРЕДОВИЩА.....	99
Олександр ПСАРЬОВ, Євген ДРУЖИНІН AGILE-ФРЕЙМВОРК ЯК КАТАЛІЗАТОР ЕФЕКТИВНОГО ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЄЮ.....	108
Денис РЕДЬКО, Альона ДЕСЯТКО, Байтума БІСАРІНОВ, Айгуль БІСАРІАНОВА ОГЛЯД МЕТОДІВ АНАЛІЗУ ТРАФІКУ КОМПАНІЇ НА ОСНОВІ АНСАМБЛЕВОЇ КЛАСТЕРИЗАЦІЇ.....	115
Олександр СТОРОЖУК, Квітослава-Ольга ЯЦИНА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ AR У ВІЗУАЛІЗАЦІЇ ТА АНАЛІЗІ АНАТОМІЧНИХ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ЕВКЛІДОВОЇ МЕТРИКИ В НАВЧАЛЬНОМУ ПРОЦЕСІ ПІДГОТОВКИ МЕДИЧНИХ ФАХІВЦІВ	125

УДК 004.8:004.42

DOI <https://doi.org/10.32689/maup.it.2024.4.6>**Олександр ГОРДІЄНКО**

кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», oleksandr.m.hordienko@gmail.com

ORCID: 0009-0002-7764-8668

Аліна КОВАЛЬ

викладач кафедри комп'ютерних інформаційних систем та технологій

Інститут комп'ютерно-інформаційних технологій та дизайну

ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», sora9393@gmail.com

ORCID: 0009-0001-7379-5065

ВИКОРИСТАННЯ КРИПТОГРАФІЇ ЯК СЕРВІСУ У ВЕБ ПРОГРАМУВАННІ

Анотація. Стаття присвячена дослідженню використання криптографії як сервісу (Cryptography as a Service, CaaS) у веб-програмуванні, що є важливою складовою сучасних підходів до забезпечення безпеки веб-додатків. Зважаючи на постійний ріст кількості онлайн-сервісів і зростаючу важливість захисту персональних даних, необхідність у надійних методах криптографії є незаперечною. Веб-розробники часто стикаються з проблемою інтеграції криптографічних функцій у свої додатки, що потребує значних витрат часу, зусиль та ресурсів. Криптографія як сервіс надає зручну і ефективну альтернативу, дозволяючи швидко інтегрувати захист даних через API, без необхідності глибоких знань у сфері криптографії.

Мета статті. Дослідити концепцію використання криптографії як сервісу CaaS, Cryptography у веб-програмуванні, визначити її переваги, обмеження та перспективи для забезпечення безпеки веб-додатків, а також розробити рекомендації щодо інтеграції CaaS у сучасні веб-розробницькі процеси.

Методологія. Проведено огляд існуючих сервісів CaaS (наприклад, AWS Key Management Service, Azure Key Vault). Проаналізовано технічні аспекти інтеграції криптографічних сервісів у веб-додатки на прикладах популярних мов програмування (JavaScript, Python, Java). Виконано порівняльний аналіз ефективності та безпеки CaaS у порівнянні з традиційними методами реалізації криптографії в веб-програмуванні. Проведено тестування практичного використання CaaS у моделюванні сценаріїв для шифрування даних, управління ключами та автентифікації.

Наукова новизна. Представлено систематизований аналіз можливостей CaaS у веб-програмуванні, зокрема для шифрування даних, цифрового підпису, автентифікації та управління ключами. Описано нові підходи до зниження навантаження на розробників шляхом делегування складних криптографічних операцій хмарним сервісам. Запропоновано рекомендації щодо вибору та інтеграції CaaS з урахуванням специфіки веб-додатків.

Висновок. Криптографія як сервіс пропонує розробникам ефективні інструменти для підвищення безпеки веб-додатків, дозволяючи делегувати складні криптографічні завдання спеціалізованим платформам. Це спрощує впровадження надійних механізмів шифрування, автентифікації та управління ключами, що є критично важливими для сучасних веб-систем. Однак для ефективного використання CaaS необхідно враховувати специфіку додатків, забезпечувати відповідність нормативним вимогам і мінімізувати залежність від зовнішніх сервісів шляхом впровадження резервних механізмів.

Загалом, стаття пропонує комплексний огляд криптографії як сервісу в контексті веб-програмування та демонструє, як цей підхід може значно полегшити розробку безпечних веб-додатків, зберігаючи при цьому високу ефективність і надійність системи.

Ключові слова: Цифровий підпис, PKI (Public Key Infrastructure), Digital Certificates, CA, Certification Authority, (RA, Registration Authority), (DB, Database), (CMS, Certificate Management System), (CRL, Certificate Revocation List), (Public and Private Keys), ECDSA, RSA, SHA-2.

Oleksandr HORDIENKO, Alina KOVAL. USING CRYPTOGRAPHY AS A SERVICE IN WEB PROGRAMMING

Abstract. The article is devoted to the study of the use of Cryptography as a Service (CaaS) in web programming, which is an important component of modern approaches to ensuring the security of web applications. Given the constant growth of the number of online services and the growing importance of protecting personal data, the need for reliable cryptography methods is undeniable. Web developers often face the problem of integrating cryptographic functions into their applications, which requires significant expenditure of time, effort and resources. Cryptography as a service provides a convenient and effective alternative, allowing you to quickly integrate data protection via API, without the need for in-depth knowledge in the field of cryptography.

The purpose of the article. To investigate the concept of using cryptography as a CaaS service, Cryptography in web programming, to determine its advantages, limitations and prospects for ensuring the security of web applications, as well as to develop recommendations for integrating CaaS into modern web development processes.

Methodology. A review of existing CaaS services (for example, AWS Key Management Service, Azure Key Vault) was conducted. The technical aspects of integrating cryptographic services into web applications were analyzed using examples of popular programming languages (JavaScript, Python, Java). A comparative analysis of the effectiveness and security of CaaS was performed in comparison with traditional methods of implementing cryptography in web programming. The practical use of CaaS was tested in modeling scenarios for data encryption, key management and authentication.

Scientific novelty. A systematic analysis of the capabilities of CaaS in web programming, in particular for data encryption, digital signature, authentication and key management, is presented. New approaches to reducing the burden on developers by delegating complex cryptographic operations to cloud services are described. Recommendations for the selection and integration of CaaS are proposed, taking into account the specifics of web applications.

Conclusion. Cryptography as a service offers developers effective tools for improving the security of web applications, allowing them to delegate complex cryptographic tasks to specialized platforms. This simplifies the implementation of reliable encryption, authentication, and key management mechanisms, which are critical for modern web systems. However, for effective use of CaaS, it is necessary to take into account the specifics of applications, ensure compliance with regulatory requirements, and minimize dependence on external services by implementing backup mechanisms.

Overall, the article offers a comprehensive overview of cryptography as a service in the context of web programming and demonstrates how this approach can significantly facilitate the development of secure web applications, while maintaining high system performance and reliability.

Key words: Digital Signature, PKI (Public Key Infrastructure), Digital Certificates, CA, Certification Authority, (RA, Registration Authority), (DB, Database), (CMS, Certificate Management System), (CRL, Certificate Revocation List), (Public and Private Keys), ECDSA, RSA, SHA-2.

Вступ. Цифровий підпис – це електронний аналог власноручного підпису, який використовується для автентифікації та забезпечення цілісності електронних документів. Він дозволяє підтвердити, що документ не було змінено після підписання, а також, що підписант є автором цього документа.

Цифровий підпис базується на криптографії з відкритим ключем і використовує пару ключів: приватний і публічний [1-3, 7, 12, 13].

Криптографія з відкритим ключем.

PKI (Public Key Infrastructure) – це система, яка використовує криптографію з відкритим ключем для забезпечення безпеки в електронному середовищі, а також для управління та обміну електронними підписами, сертифікатами та іншими безпечними елементами. PKI дозволяє здійснювати автентифікацію, шифрування та забезпечення цілісності даних, використовуючи пару ключів: публічний і приватний [1, 2].

Основні компоненти PKI:

1. *Сертифікати (Digital Certificates)* – це електронні документи, які містять публічний ключ і інформацію про власника цього ключа (наприклад, ім'я, організація, термін дії тощо). Сертифікати підписуються центром сертифікації (CA), що гарантує їх достовірність. Вони використовуються для підтвердження ідентичності суб'єктів і для забезпечення довіри до публічного ключа.

2. *Центр сертифікації (CA, Certification Authority)* – це організація або служба, яка видає сертифікати та перевіряє особу або організацію перед видачею сертифікату. CA підписує сертифікати, підтверджуючи їх дійсність і зв'язок з певною особою чи організацією. Прикладом CA може бути компанія, що надає послуги цифрових підписів (наприклад, VeriSign, DigiCert або Національний центр сертифікації ключів в Україні).

3. *Реєстраційний орган (RA, Registration Authority)*. RA працює в тісній взаємодії з центром сертифікації. Це орган або служба, яка відповідає за прийом запитів на сертифікати, перевірку особи та передачу запитів в CA для видачі сертифікатів. RA може здійснювати перевірку особи за допомогою документів, особистої перевірки тощо.

4. *Реєстраційна база даних (DB, Database)* – це база даних, де зберігаються сертифікати, статуси сертифікатів, ключі та інша важлива інформація для підтримки PKI-системи.

5. *Система управління сертифікатами (CMS, Certificate Management System)*. CMS використовує сертифікати та допомагає у їх створенні, обміні, оновленні, відкликанні тощо.

6. *Система відкликання сертифікатів (CRL, Certificate Revocation List)* – це список сертифікатів, які були відкликані до завершення терміну їх дії. Відкликання сертифікатів може відбуватися з різних причин: наприклад, якщо приватний ключ був скомпрометований, чи користувач припинив свою діяльність. CRL допомагає визначити, чи є сертифікат недейсним.

7. *Пара публічного і приватного ключів (Public and Private Keys)*. Приватний ключ використовується для підписання документів і повинен бути захищений. Лише підписант має доступ до свого приватного ключа. Публічний ключ використовується для перевірки підпису. Він може бути доступний будь-кому, хто хоче перевірити достовірність підписаного документа.

Функції PKI для безпеки даних у цифровому середовищі [1].

1. *Аутентифікація*. Завдяки використанню сертифікатів, PKI дозволяє перевіряти, що обидві сторони (наприклад, підписувач та отримувач) є тими, за кого вони себе видають. Це важливо для онлайн-транзакцій, електронних підписів та інших операцій, що вимагають верифікації особи.

2. *Шифрування*. Для шифрування даних використовується публічний ключ: будь-хто може зашифрувати інформацію за допомогою публічного ключа, але тільки власник відповідного приватного ключа може її дешифрувати.

3. *Цілісність і підписання.* За допомогою криптографічних підписів з використанням приватного ключа можна гарантувати цілісність документа (що документ не був змінений після підписання) та підтвердження, що підпис стався від конкретної особи.

4. *Відкликання сертифікатів.* Якщо приватний ключ стає скомпрометованим або з іншої причини сертифікат більше не є дійсним, то він може бути відкликаний через CRL, що дає змогу уникнути зловживань.

Генерація ключів:

Спочатку підписант створює пару ключів: приватний ключ та публічний ключ. Приватний ключ зберігається в безпечному місці (наприклад, на токени або смарт-карті), тоді як публічний ключ може бути наданий для перевірки підписів.

Пара ключів генерується за допомогою криптографічних алгоритмів, таких як RSA або ECDSA (Elliptic Curve Digital Signature Algorithm).

Процес підписання:

1. Підписант створює хеш (унікальне цифрове представлення) документа:

– Для підписання документа спочатку обчислюється його хеш – це цифровий відбиток документа, що дозволяє зменшити його розмір. Зазвичай використовуються хеш-алгоритми, такі як SHA-256 або SHA-3.

– Хеш є унікальним для кожного документа, і будь-які зміни в документі призведуть до зміни хешу.

2. Цей хеш шифрується приватним ключем підписанта, створюючи цифровий підпис:

– Після того, як хеш обчислений, він шифрується за допомогою приватного ключа підписанта. Цей процес створює цифровий підпис, який додається до документа.

– Шифрування хешу гарантує, що підпис може бути перевірений тільки за допомогою відповідного публічного ключа.

Перевірка підписаного документу:

1. Для перевірки підпису отримувач документу використовує публічний ключ підписанта, який можна отримати через сертифікат (наприклад, X.509).

2. Спочатку обчислюється хеш документа, який перевіряється з хешем, що знаходиться в цифровому підписі.

3. Якщо хеші збігаються і підпис можна правильно розшифрувати за допомогою публічного ключа, це підтверджує автентичність підпису і те, що документ не був змінений після підписання.

Хешування має кілька важливих властивостей:

1. *Детермінованість.* Для однакових вхідних даних хеш-функція завжди генерує однакове хеш-значення.

2. *Неможливість відновлення (односторонність).* З хеш-значення неможливо відновити оригінальні вхідні дані. Це робить хешування корисним для зберігання паролів, оскільки навіть якщо хеш буде вкрадений, не можна безпосередньо дізнатися сам пароль.

3. *Маленька зміна вхідних даних викликає великі зміни в хеші.* Якщо навіть одна літера у вхідних даних зміниться, хеш-значення зміниться кардинально.

4. *Унікальність.* Добре спроектовані хеш-функції повинні мінімізувати ймовірність того, що два різних набори даних дадуть однакові хеші. Такий випадок називається колізією.

Найпоширеніші криптографічні алгоритми [17]:

RSA (Rivest–Shamir–Adleman). Один з найпоширеніших алгоритмів для підписів і шифрування, використовується з хеш-функцією (наприклад, SHA-256) для створення цифрових підписів.

ECDSA (Elliptic Curve Digital Signature Algorithm). Використовується в рамках алгоритмів на основі еліптичних кривих. Він надає більшу безпеку при меншому розмірі ключа в порівнянні з RSA.

SHA-2 (Secure Hash Algorithm 2). Використовується для обчислення хешу документів. SHA-256 є однією з найбільш поширених функцій хешування для підписів.

Цифрові підписи використовуються в багатьох сферах:

- Юридичні документи: Контракти, угоди, та інші юридичні документи.
- Фінансові транзакції: Банківські та фінансові звіти, податкові декларації.
- Урядові послуги: Подача заявок на отримання ліцензій або взаємодія з урядовими установами.
- Медицина: Електронні медичні записи та рецепти.
- В Україні для використання цифрових підписів є державні сертифікаційні центри, які надають послуги:

- Видача сертифікатів електронного підпису.
- Перевірка дійсності підпису.
- Використання ключів для криптографічних операцій.
- Сервіси для зберігання і управління ключами.

Кваліфікований електронний підпис (КЕП) – це електронний підпис, який має юридичну силу, що прирівнюється до власноручного підпису, відповідно до законодавства. Для того, щоб підпис був кваліфікованим, він повинен відповідати певним вимогам, встановленим національними або міжнародними стандартами (зокрема, Регламентом ЄС № 910/2014, який визначає принципи використання електронних підписів в ЄС). У більшості країн, зокрема в Україні, цей підпис регулюється законодавством, яке забезпечує його юридичну значимість.

Генерація ключів в Україні:

- Для кожного користувача сертифікаційний центр генерує пару криптографічних ключів – публічний і приватний.
- Приватний ключ залишається в безпеці на сервері сертифікаційного центру або в апаратних засобах (токенах, смарт-картах).
- Публічний ключ надається у вигляді сертифіката користувача, який може бути використаний для перевірки підписів.

Використання електронного підпису на веб-сайті.

В Україні, приватний ключ недоступний для передачі на сервер – це правильна і безпечна практика. Приватний ключ не повинен залишати клієнтську сторону, де він зберігається. Це важливо для забезпечення конфіденційності та цілісності електронного підпису. В такому випадку, підписування виконується на клієнтській стороні, а сервер тільки перевіряє підпис та зберігає [14, 15].

Створення документу, який буде збережений на веб сервері разом із підписом та статусом перевірки підпису:

1. Створимо HTML-форму, шаблон документа, яку клієнт буде заповнювати. Кожне поле відповідає певному полю в базі даних для конкретного шаблону документа.
2. Після заповнення форма зберігається у базі даних. Кожен шаблон документа має свою таблицю, а кожен запис в таблиці – це дані з конкретної форми.
3. Клієнт завантажує документ із сервера. Перетворимо документ, який розташований у базі даних, у формат JSON, та повернемо клієнту.
4. Отриманий документ підписується клієнтом. Отриманий підпис клієнт завантажує назад на сервер.
5. Підпис зберігається на сервері в базі даних, і створюється зв'язок між документом і підписом.
6. Сервер перевіряє підписаний документ та встановлює мітку-результат до підпису.

Автоматизація підписання документа.

Щоб спростити алгоритм підписання документа можна використати систему вебхуків. Вебхук – спосіб інтеграції, де один сервіс або система може автоматично сповіщати іншу систему про події (наприклад, про запит на підписання документа), щоб виконати певні дії [14, 15]. Щоб реалізувати таку систему необхідно:

1. Сервер, який містить документ, генерує JSON файл та надсилає запит на сторонній сервіс (наприклад, сервіс для електронного підпису або іншу зовнішню систему), щоб підписати цей документ. В запиті є реквізити отримувача та реквізити сервера, якому необхідно повернути підпис.
2. Клієнт, користуючись стороннім сервісом, підписує документ. Сервіс повертає підпис назад на сервер, який вказаний у реквізитах.
3. Отримавши сповіщення, сервер збереже підпис у базі даних та виконає перевірку підписаного документа.

Висновки. У результаті дослідження використання криптографії як сервісу у веб-програмуванні можна зробити висновок, що цей підхід є перспективним інструментом для забезпечення високого рівня безпеки веб-додатків. Завдяки PKI розробники можуть інтегрувати складні криптографічні алгоритми без необхідності глибоких знань у цій галузі, що дозволяє зменшити час на розробку та підвищити надійність систем. Використання хмарних криптографічних сервісів дозволяє оптимізувати процеси обробки даних, зменшити навантаження на сервери та забезпечити більшу гнучкість у масштабуванні веб-додатків. Проте важливо враховувати можливі ризики, такі як безпека зберігання ключів та залежність від постачальника PKI. Для максимізації ефективності необхідно ретельно обирати постачальників послуг, враховуючи їх репутацію, рівень захисту даних і відповідність стандартам безпеки.

Список використаних джерел:

1. "Secure Electronic Signature Regulations SOR/2005-30". Justice Laws Website. 10 March 2011. Archived from the original on 28 February 2020. Retrieved 19 May 2020.
2. "US ESIGN Act of 2000" (PDF). Archived (PDF) from the original on 2011-05-22. Retrieved 2006-05-10.
3. Bellare, Mihir; Goldwasser, Shafi (July 2008). "Chapter 10: Digital signatures". Lecture Notes on Cryptography (PDF). p. 168. Archived (PDF) from the original on 2022-04-20. Retrieved 2023-06-11.

4. Ellis, James H. (January 1970). "The Possibility of Secure Non-Secret Digital Encryption" (PDF). Archived from the original (PDF) on 2014-10-10.
5. Hash_RC6 – Variable length Hash algorithm using RC6 <https://ieeexplore.ieee.org/document/7164747>
6. JSON – Introduction https://www.w3schools.com/js/js_json_intro.asp
7. Katz Jonathan, Lindell Yehuda. "Chapter 12: Digital Signature Schemes". Introduction to Modern Cryptography. 2007. p. 399.
8. RSA Security's Official Guide to Cryptography by Steve Burnett, Stephen Paine, ISBN-13:978-0072131390, April 19, 2001.
9. Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar, ISBN-13: 978-3642041006, November 27, 2009.
10. Webhooks <https://developer.atlassian.com/server/jira/platform/webhooks/>.
11. What is PKI? <https://www.digicert.com/what-is-pki>.
12. Winn, Jane K. Wright, Benjamin "Digital Signatures: A Survey of Law and Practice in Global Perspective". Journal of Information Technology Law, 2021. Volume 25, Issue 3, pp. 45–60.
13. Головий Л. В., Янчук Ю. В. Правове регулювання інформаційних відносин у сфері електронної комерції. *Право. Людина. Довкілля*. 2020 Том 11, №2. С. 150–157.
14. ЗАКОН УКРАЇНИ Про електронну ідентифікацію та електронні довірчі послуги <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
15. Роз'яснення законодавства у сфері ЕДП <https://czo.gov.ua/edp-legislation-clarification>.
16. Що таке КЕП та ЕЦП?. 17Якими бувають електронні підписи? <https://ca.dii.gov.ua/faq17>