ПРИКЛАДНА МАТЕМАТИКА, ІНФОРМАТИКА ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА

УДК 004.056.55 https://doi.org/10.31713/vt320217

Джоші А., аспірант (Національний університет водного господарства та природокористування, Рівне, dzhoshi_ak17@nuwm.edu.ua)

ТЕХНОЛОГІЯ ТОКЕНІЗАЦІЇ КАРТКОВИХ ДАНИХ В ОНЛАЙН-ПЛАТЕЖАХ

Проведено огляд теоретичних відомостей технології токенізації карткових даних. Проаналізовано доцільність створення системи токенізації карткових даних.

Розглянуто переваги та недоліки алгоритмів токенізації карткових даних.

Описано можливість використання математичних методів захисту інформації для реалізації алгоритмів токенізації карткових даних. Розглянуто основні алгоритми вирішення даної проблеми, описано алгоритм токенізації та детокенізації даних.

Описано методи перевірки коректності токенізації для найбільш поширених алгоритмів.

Також наведено реалізацію системи токенізації та детокенізації карткових на персональних даних, наведені особливості реалізації, принципи вибору конкретної реалізації в залежності від зовнішніх умов та вимог, що ставляться до системи.

Ключові слова: **карткові дані; токенізація; шифрування.**

Постановка проблеми. По мірі росту популярності онлайн-покупок, безпека онлайн-платежів стає важливим питанням. Мільйони номерів кредитних карток зберігаються та надсилаються по Інтернету щодня. Проте, це призводить до великої небезпеки, якщо ці дані зберігаються або надсилаються небезпечно. Зловмисники можуть проникнути на сервер онлайн-продавця і отримати доступ до великої кількості номерів кредитних карток, а також до відповідної конфіденційної інформації – ім'я власника картки, дата закінчення строку дії та перевірочні коди. Платіжна індустрія передбачила цю проблему, тому було розроблено стандарт під назвою PCI DSS, що покликаний забезпечувати основу для розробки надійного процесу

захисту даних платіжних карток у всіх організаціях, що беруть участь в обробці платіжних даних, включаючи продавців, процесорів, еквайерів та емітентів. Існують сторонні постачальники послуг, що займаються обробкою конфіденційних персональних даних для онлайн-продавців. Токенізація – одна з найбільш широко використовуваних технологій, тому виникає необхідність аналізу алгоритмів токенізації, що наразі використовуються.

Мета і завдання дослідження. Метою дослідження є аналіз алгоритмів токенізації та оцінка надійності токенізації як методу зберігання карткових даних. З метою досягнення поставленої мети було передбачено розв'язання наступних завдань:

- огляд теоретичних відомостей, що стосуються токенізації;
- аналіз сучасних алгоритмів токенізації на предмет їх застосовності для збереження карткових даних;
- побудова системи токенізації карткових даних.

Виклад основного матеріалу. Номера кредитних карток або первинні номера рахунків складаються максимум з 22 цифр, що ідентифікують емітента картки та її власника. Як показано на рис. 1, номер картки складається з трьох основних елементів:

- ідентифікаційний номер емітента, що відповідає першим 8 цифрам
- номер індивідуального рахунку, що може бути різної довжини – від 1 до 10 цифр
- контрольна цифра, що обчислюється із всіх попередніх цифр за допомогою алгоритма Луна.

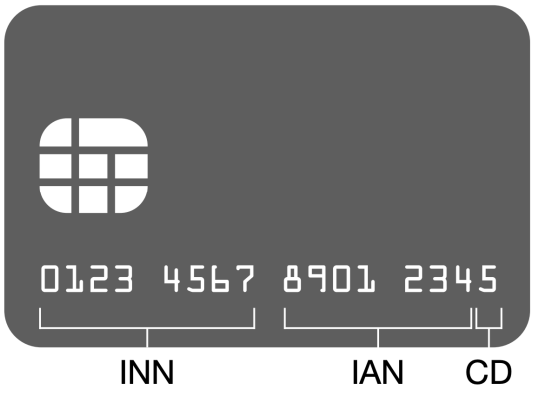

Рис. 1. Формат номеру кредитної картки

Що стосується платіжного токену, то в ньому можна прийняти

структуру, що дещо відрізняється від традиційного формату. Наприклад, перші 4 цифри можуть використовуватися для ідентифікації картки емітента. Останні ж 4 цифри можуть бути фіксованими та використовуватися для перевірки цілісності або для виявлення помилок в токені в якості контрольної суми. 8 цифр, що залишилися всередині ідентифікують токен (рис. 2).

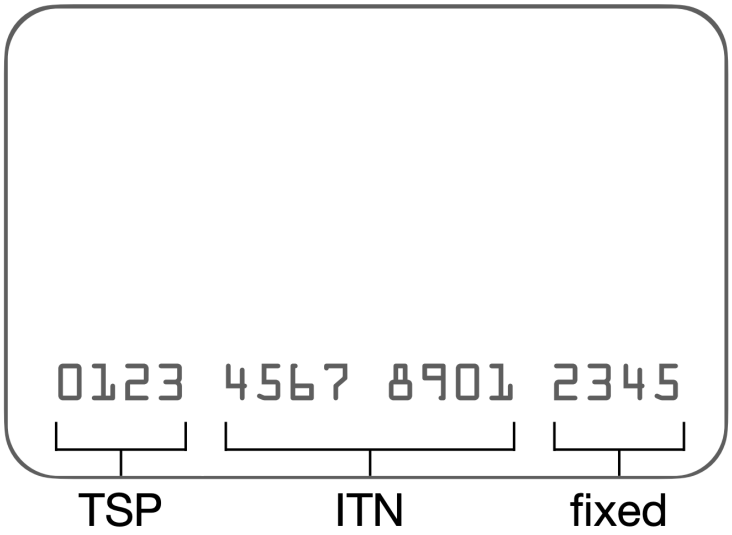

Рис. 2. Формат токену номеру кредитної картки

На зворотній стороні фізичної картки три додаткові цифри утворюють код CVV (Card Verification Value). Їх призначення полягає в тому, щоб гарантувати фізичне володіння карткою в момент оплати. Більше того, по стандарту PCI DSS, не може зберігатися ніде, крім емітента картки [2].

На даний момент для підвищення рівня безпеки онлайн- транзакцій, багато платіжних систем використовують тимчасову ідентифікацію. Це зменшує можливість відстеження, обмежує ризики витоку даних.

Розповсюдженим підходом є токенізація – цей процес замінює існуючий номер платіжної картки значенням-замісником, що називається токеном, котрий випускається довіреною третьою стороною – Token Service Provider. Цей сервіс слугує проксі, що маскує справжню особу користувача. Пізніше токен використовується під час платіжних операцій та дозволяє обробляти платіж без використання реальних банківських реквізитів [1]. Служба токенів зв'язує оригіналь-

ний номер картки з токенами і надійно зберігає всі необхідні дані. Типовий сценарій життєвого циклу токену зображений на рис. 3.

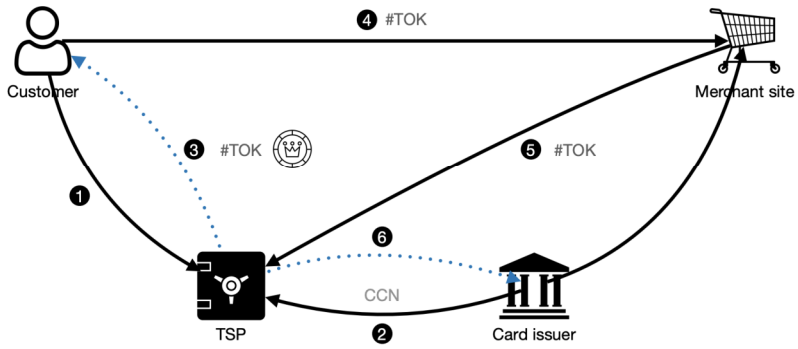

Рис. 3. Життєвий цикл токена карткових даних

Алгоритм використання токена для проведення платежу складається з наступних кроків:

1. Запит на отримання токена. Клієнт запитує токен в TSP.
2. Запит – TSP запитує всі необхідні дані для створення токену у емітента картки.
3. Токенізація – TSP створює токен із номеру кредитної картки і відправляє його клієнту.
4. Покупка – клієнт купує товар чи послугу в інтернет-магазині і передає токен.
5. Запит на проведення платежу – сайт продавця повертає токен в TSP і підтверджує платіж.
6. Детокенізація – TSP перетворює токен в номер карти і передає запит на проведення платежу емітенту карти.
7. Платіж – емітент карти підтверджує платіжний запит від сайту продавця.

Основна роль TSP полягає в збереженні токена та встановленні відповідності між токеном і номером кредитної картки. TSP може взяти на себе додаткові обов'язки такі як управління доменами (забезпечення додаткової захищеності шляхом обмеження використання токенів окремими каналами) та автентифікація (забезпечення в процесі детокенізації того, що токен був законно використаний правильним клієнтом). Для цього можна перевірити особу користувача, попросивши підтвердити свою особу за допомогою пароля, багатофакторної автентифікації або за допомогою криптографічного підпи-

су по стандарту ECDSA. Емітенти карт можуть підтвердити роль TSP, дозволяючи повний контроль над процесом токенізації. Відповідно до цього, емітенти карт можуть використовувати сторонній TSP та інтегрувати його в свої платіжні системи [1].

Процес токенізації заключається в генерації токена TOK із номера карти CN. Він також передбачає збереження даних користувача для майбутньої детокенізації. Алгоритм Tokenziation(Tab, CN, num_uses, exp_date, auth, sk) приймає на вхід таблицю Tab, номер кредитної карти, максимальну кількість використань, мітку часу, додаткову авторизаційну інформацію (наприклад – відкритий ключ) и приватний ключ. Потім алгоритм обирає випадковий 32-бітний масив: hash32 = SHA224(CN,expiry,auth,rand). Потім, враховуючи nmax – максимальну кількість рядків, обраховується s tok = hash32 mod nmax. Таким чином токен (відкриті 8 цифр) генеруються рівномірно шляхом хешування даних. Якщо токен вже існує, то процес перезапускається и токенізація повторюється з новим значенням rand.

Процес детокенізації полягає в отриманні номера кредитної карти CN з токену tok. При необхідності (наприклад для виявлення зловмисних запитів) алгоритм зберігає виклик детокенізації у зовнішній базі даних). Алгоритм Detokenization(Tab, tok, debit, verif, sk) приймає на вхід таблицю Tab, токен, дані для перевірки автентифікації и приватний криптографічний ключ. Перевіряється, чи існує рядок таблиці, що індексується tok. Якщо ні – це означає, що токен не дійсний і алгоритм зупиняється. В іншому випадку рядок розшифровується за допомогою приватного ключа, а значення num_uses зменшується на 1.

Висновки. Розглянуто рішення для системи токенізації номерів кредитних карт. Система базується на можливості збереження повної таблиці токенів в оперативній пам'яті так, щоб обчислення були достатньо швидкими. Зовнішня база даних може використовуватися для транзакцій токенізації та детокенізації для проведення аудиту. Оперативна пам'ять системи токенізації може бути репліковаою для підвищення доступності розподіленої системи. Крім того, для збереження більшої кількості даних та швидкого пошуку, можна використовувати двійкове дерево або інші методи збереження даних.

1. Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh, Yris Brice Wandji Piugie. An Upcycling Tokenization Method for Credit Card Numbers. Normandie Universite. 2021. 12 p. **2.** Gabriel Babatunde

Iwasokun, Taiwo Gabriel Omomule, Raphael Olufemi Akinyede. Encryption and Tokenization-Based System for Credit Card Information Security. The Society of Digital Information and Wireless Communications. 2018. 11 p.

REFERENCES:

1. Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh, Yris Brice Wandji Piugie. An Upcycling Tokenization Method for Credit Card Numbers. Normandie Universite. 2021. 12 p. **2.** Gabriel Babatunde Iwasokun, Taiwo Gabriel Omomule, Raphael Olufemi Akinyede. Encryption and Tokenization-Based System for Credit Card Information Security. The Society of Digital Information and Wireless Communications. 2018. 11 p.

Dzhoshi A., Post-graduate Student (National University of Water and Environmental Engineering, Rivne, dzhoshi_ak17@nuwm.edu.ua)

CARD DATA TOKENIZATION TECHNOLOGY USED IN ONLINE PAYMENTS

As the popularity of online shopping grows, the security of online payments is becoming an important issue. Millions of credit card numbers are stored and sent online every day. However, this leads to great danger if this data is stored or sent dangerously. Attackers can hack into an online merchant's server and gain access to a large number of credit card numbers, as well as relevant confidential information such as the cardholder's name, expiration date, and verification codes. A review of theoretical information about tokenization technology of card data was done. The expediency of creating a card data tokenization system was analyzed.

The advantages and disadvantages of card data tokenization algorithms are considered.

Tokenization is important for all organizations involved in the processing of payment data, including sellers, processors, acquirers and issuers. There are third-party service providers that process sensitive personal information for online sellers. Tokenization is one of the most widely used technologies, so there is a need to analyze the tokenization algorithms currently in use. The possibility of using mathematical methods of information protection to implement card data tokenization algorithms is described. The basic algorithms for

solving this problem are considered, and the algorithm of tokenization and data detokenization is described. Improved data storages as binary trees are also described for quicker search and optimized data storage.

Tokenization correctness checking methods for the most common algorithms are described.

Also we present the implementation of the tokenization and detokenization system of card data, the peculiarities of implementation, principles of choosing the particular implementation, depending on external conditions and requirements to the system.

***Keywords*: card data; tokenization; encryption.**

Джоши А., аспирант (Национальный университет водного хозяйства и природопользования, Ровно, dzhoshi_ak17@nuwm.edu.ua)

ТЕХНОЛОГИЯ ТОКЕНИЗАЦИИ КАРТОЧНЫХ ДАННЫХ В ОНЛАЙН-ПЛАТЕЖАХ

Проведен обзор теоретических сведений технологии токенизации карточных данных. Проанализирована целесообразность создания системы токенизации карточных данных.

Рассмотрены преимущества и недостатки алгоритмов токенизации карточных данных.

Описаны возможность использования математических методов защиты информации для реализации алгоритмов токенизации карточных данных. Рассмотрены основные алгоритмы решения данной проблемы, описан алгоритм токенизации и детокенизации данных.

Описаны методы проверки корректности токенизации для наиболее распространенных алгоритмов.

Также приведены реализацию системы токенизации и детокенизации карточных на персональных данных, приведены особенности реализации, принципы выбора конкретной реализации в зависимости от внешних условий и требований, предъявляемых к системе.

***Ключевые слова:* карточные данные; токенизация; шифрование.**
