

## ABSTRACT

Explanatory note size – 130 pages, contains 10 illustrations, 36 tables, 2 applications, 27 references.

**Topicality.** The relevance of developing a software library for reliable and secure processing of API keys is due to the need to improve the security of machine authorization in distributed and microservice systems. Modern services require effective solutions for storing, updating and revoking keys without system downtime. There is also a need to improve the efficiency of key verification to avoid accessing a centralized database. The proposed library is aimed at eliminating the shortcomings of traditional approaches, which have limited scalability and an insufficient level of protection

**The aim of the study.** Improve the reliability and efficiency of API key processing by using extended JWT tokens with proof of ownership and without the use of centralized database checks.

The object of research: the process of creating a software library for reliable and secure processing of API keys.

The subject of research: methods for secure and scalable API key processing.

To achieve this goal, the **following tasks** were formulated:

- analyze existing libraries for processing API keys;
- analyze existing engineering solutions for processing API keys;
- formulate requirements for a software library to ensure the reliability and security of processing API keys;
- modify existing engineering solutions to increase the speed and reliability of processing API keys;
- develop the architecture of an API key processing library with support for confirming token ownership;
- implement key processing using a distributed cache, avoiding constant access to a centralized database;

- implement a key rotation mechanism without system downtime;
- ensure the ability to integrate the library into the Spring framework ecosystem;
- evaluate the effectiveness and security of the proposed approach experimentally.

**The scientific novelty** of the results of the master's dissertation lies in the fact that engineering solutions for the effective representation of API keys in the form of extended JWT tokens that support proof of ownership have been improved, as well as the API key revocation algorithm based on the epochal mechanism and the use of Bloom filters has been improved.

**The practical value** of the obtained results is that the developed Java library can be integrated into any machine authorization system for secure processing of API keys in the Spring framework ecosystem. It provides fast revocation, continuous rotation, and scalable interaction between services, which increases the level of security and reliability of the system.

**Relationship with working with scientific programs, plans, topics.** Work was performed at the Department of Informatics and Software Engineering of the National Technical University of Ukraine «Kyiv Polytechnic Institute. Igor Sikorsky».

**Approbation.** The scientific provisions of the dissertation were tested at the The scientific provisions of the dissertation were tested at the scientific and practical conference of young scientists and students "SOFTWARE ENGINEERING AND ADVANCED INFORMATION TECHNOLOGIES" (SoftTech-2025).

**Publications.** The scientific provisions of the dissertation were published in:

1) Moskalenko V. U., Golovchenko M.M., Pavlov O.A. Software library for reliable and secure API-key processing // Software engineering and advanced information technologies (SoftTech-2025 Autumn): materials of abstracts of reports of the IX International Scientific and Practical Conference of Young Scientists and Students (Kyiv, November 26-28, 2025). – K.: Igor Sikorsky Kyiv Polytechnic Institute, 2025.

**Keywords:** API KEY, MACHINE AUTHORIZATION, JWT, TOKEN OWNERSHIP PROOF, KEY REVOCATION, KEY ROTATION, SCALABILITY, SECURITY.