MSC: 68P20; 68U35 Original article

Development of an approach to ensuring information security in web-based information systems when transferring data using the Web Cryptography API interface

M.V. Stupina

Don State Technical University
344003, Russia, Rostov-on-Don, 1 Gagarina square

Abstract. The aim of the research is to formulate general principles for ensuring information security in web-oriented information systems. The paper describes the main concepts of the Web Cryptography API interface, as well as presents practical aspects of using cryptographic methods to ensure data security in web-oriented information systems. The proposed approach, based on the introduction of a secure system for generating and storing users private keys through the use of the asynchronous ECDSA encryption algorithm via the Web Cryptography API interface, combined with encrypting private keys with passphrases and additional user authentication, allows a high level of protection of private keys from unauthorized access.

Keywords*:* Web Cryptography API, cryptography, electronic signature, electronic document management, ECDSA

REFERENCES

1. Mekhdiev E.T., Plekhanova E.A. Development of electronic document management systems in the digital economy. *Diskussiya* [Discussion]. 2023. No. 1(116). Pp. 58–70. DOI: 10.46320/ 2077-7639-2022-6-115-52-70. (In Russian)

2. Goncharov E.I., Shatkovskaya T.V. Problems of using digital signatures in electronic document management in Russia. *Severo-Kavkazskiy yuridicheskiy vestnik* [North Caucasian Legal Bulletin]. 2020. No. 2. Pp. 97–103. DOI: 10.22394/2074-7306-2020-1-2-97-103. (In Russian)

3. Baranov A.S. Use of cryptographic information protection tools in organizations. *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal* [International Scientific Research Journal]. 2020. No. 6-1 (96). Pp. 131–133. DOI: 10.23670/IRJ.2020.96.6.023. (In Russian)

4. Bylinskiy M.D. Protecting JavaScript applications using the Web Cryptographs Api. *Vestnik Baltiyskogo federal'nogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskie i tekhnicheskie nauki* [Bulletin of the Baltic Federal University. I. Kant. Series: Physics, mathematics and technical sciences]. 2022. No. 1. Pp. 53–60. (In Russian)

5. Cairns K., Halpin H., Steel G. Security Analysis of the W3C Web Cryptography API. *Proceedings of Security Standardisation Research (SSR).* Gaithersberg. 2017. Pp. 112–140. DOI: 10.1007/978-3-319-49100-4_5

6. Wichmann P., Blochberger M., Federrath H. Web Cryptography API. Prevalence and Possible Developer Mistakes. *In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22).* Association for Computing Machinery. New York. 2022. Pp. 1–10. DOI: 10.1145/3538969.3538977

1. Samir A., Abo-Taleb M., Shalaby et al. A Side-Channel Attack Resistive ECDSA. *International Conference on Advanced Information Systems and Engineering. Journal of Physics: Conference Series.* Cairo, Egypt. 2019. Pp. 112–140. DOI: 10.1088/1742-6596/1454/1/012003

Information about the author

Maria V. Stupina, Candidate of Pedagogical Sciences, Associate Professor, Department of Information Technology, Don State Technical University;

344003, Russia, Rostov-on-Don, 1 Gagarina square;

masamvs@bk.ru, ORCID: https://orcid.org/0000-0002-6394-6966