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


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