Embedding Algorithms for Generating and Verifying Eds in A Cryptographic Information Security Tool

Nurullaev Mirkhon Muhammadovich

Department of Information Communication Technology, Bukhara Engineering Technological Institute, Uzbekistan
nurullayevmirxon@gmail.com

ABSTRACT

In this article, we will discuss the functions of embedding algorithms for generating and verifying EDS in a cryptographic information security tool. Electronic Data Signatures (EDS) are crucial components of modern cryptographic information security tools. They provide authentication, integrity, and non-repudiation of electronic data, ensuring that the data has not been tampered with during transmission or storage. EDS are generated using a combination of hashing algorithms and digital signatures, which are then embedded into the electronic data.

Keywords: EDS, cryptographic information security tool, functions of EDS, generating and verifying EDS, embedding algorithms EDS

Introduction.

In today's digital age, the secure transmission and storage of information are crucial. Cryptographic information security tools play a crucial role in ensuring that sensitive information remains secure and protected from unauthorized access or interception. One of the key components of these tools is the use of electronic digital signatures (EDS).

1. Data authenticity: One of the primary functions of EDS is to provide data authenticity. An EDS is a digital signature that verifies the identity of the sender and the integrity of the data. This ensures that the data received is exactly the same as the data that was sent, and that it was sent by an authorized party.
2. Non-repudiation: EDS also provides non-repudiation, meaning that the sender cannot deny sending the data. The recipient can verify the EDS to ensure that it was sent by the claimed sender. This is particularly important in legal or financial transactions, where it is necessary to prove the identity of the sender.
3. Key management: Effective key management is crucial in embedding algorithms for generating and verifying EDS in a cryptographic information security tool. Key management includes key generation, distribution, storage, usage, and lifecycle management. The secure management of EDS keys is essential in ensuring that only authorized parties can generate and verify EDS.
4. Digital certificates: EDS is issued using digital certificates, which are issued by trusted third-party authorities. The digital certificate contains information about the sender, such as their name and public key, which is used to verify the EDS. The use of digital certificates is essential in ensuring the authenticity of the EDS.

5. Verification process: The verification process is a critical function in the use of EDS. The verification process involves using the public key contained in the digital certificate to decrypt the EDS and verify its authenticity. The verification process must be carefully implemented to ensure that it is not vulnerable to attacks such as a man-in-the-middle attack.

To generate and verify EDS, various embedding algorithms are used. Embedding algorithms are mathematical techniques that enable the integration of EDS into electronic data. These algorithms are essential to ensure that the EDS can be efficiently generated and verified by cryptographic information security tools [1].

In the algorithm, the sender creates an EDS by encrypting a hash of the data with their private key. The receiver then verifies the EDS by decrypting it with the sender's public key and comparing the decrypted hash with the original data.

The effectiveness of embedding algorithms in generating and verifying EDS depends on several factors. These factors include the complexity of the algorithm, the length of the key, and the security of the cryptographic tool [2]. For example, longer keys and more complex algorithms offer a higher level of security, but may also require more computational power, which can slow down the EDS generation and verification process.

To ensure the security of electronic data, it is crucial to use a reliable and secure cryptographic information security tool. This tool should be designed to incorporate the most effective embedding algorithms, such as the RSA [3], O`z DSt 1092:2009 [4],[5] and ECDSA [6] algorithms, to generate and verify EDS. Additionally, the cryptographic tool should be regularly updated and tested to ensure that it is robust and secure against potential cyber threats.

Materials and methods.

An EDS is an electronic analogue of a written signature and therefore an EDS can be used by the recipient or a third party to verify that the message was actually signed by the sender [7].

Two algorithms are used to describe the formation and authentication of EDS (Algorithm 1, Algorithm 2).

Algorithm 1 is considered in two basic modes:

- without a session key;
- with a session key.

Algorithm 2 is used in the classic (without a session key) mode. Algorithm 1 provides a backup way to detect EDS forgery by introducing a session key procedure into the EDS formation process used in the EDS authentication process (Fig. 1. and Fig. 2.).

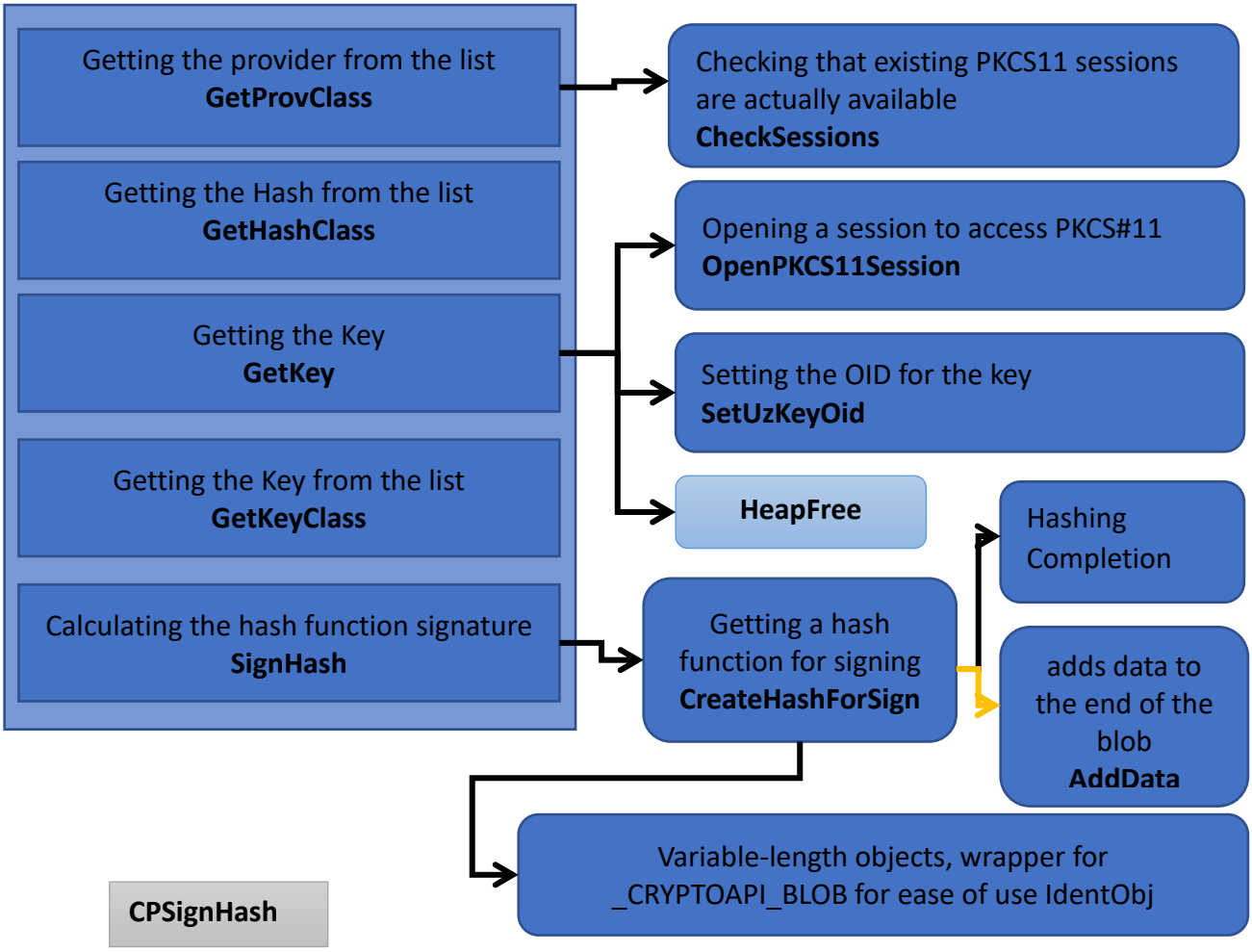

Fig. 1. The function of forming an EDS CPSignHash

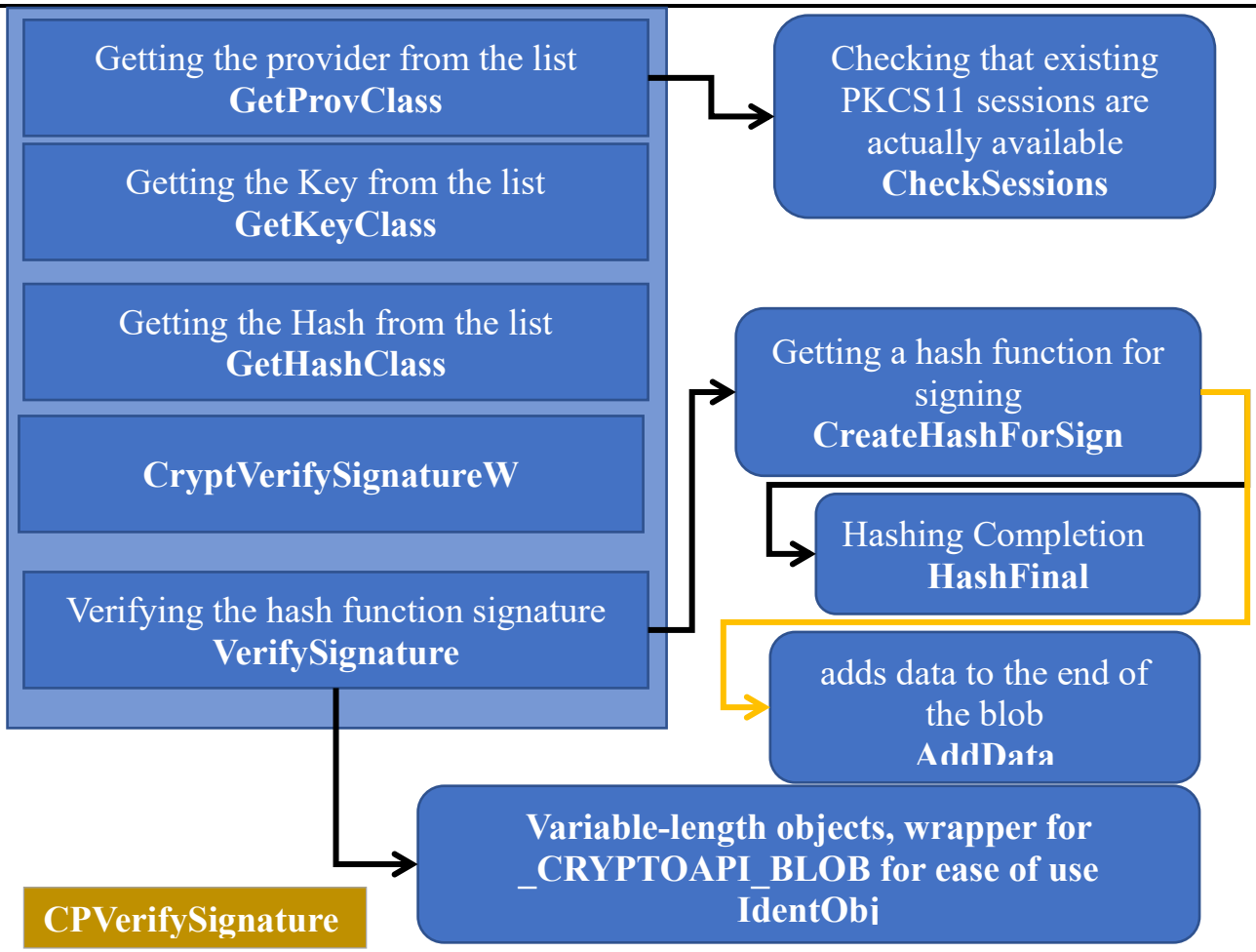

Fig. 2. The function of verifying an EDS CPVerifySignature

Results and discussions.

To ensure the safe use of the cryptographic information protection tool installed on the computer, organizational measures are provided, as well as software and hardware methods and means of information protection are used to ensure the secret of secret keys placed in the computer's RAM during the operation of the cryptographic information protection tool, as well as service parameters of the cryptographic information protection tool stored on the hard drive [8],[9]. The cryptographic information security tool contains a component that allows you to check the operability of cryptographic algorithms implemented in it [10]. The health check is carried out on the basis of test examples. To ensure the safe use of an application with a built-in cryptographic information protection tool, mechanisms for monitoring the integrity of libraries are provided for cryptographic information protection. A biophysical random number sensor is used as a means of cryptographic information protection to generate random binary sequences, which implements a mechanism for generating secret EDS keys, encryption keys [11], initialization vectors using various algorithms.

Conclusion. In conclusion, embedding algorithms are critical components of cryptographic information security tools that enable the efficient generation and verification of EDS. The effectiveness of these algorithms depends on various factors, such as complexity and key length. The use of reliable and secure cryptographic information security tools incorporating the most effective embedding algorithms is essential to ensure the security of electronic data.

Embedding algorithms for generating and verifying EDS in a cryptographic information security tool is crucial in ensuring the authenticity and non-repudiation of sensitive

information. The use of EDS provides a high level of security in legal, financial, and other transactions, where the identity of the sender must be verified. Effective key management and the use of digital certificates are essential components of EDS, and the verification process must be carefully implemented to ensure its security. As technology continues to evolve, the continued development and refinement of EDS algorithms will ensure their effectiveness and reliability in securing our digital world.

References

1. Subramanya, S.R. & Yi, B.K. (2006). Digital signatures. Potentials, IEEE. 25. 5 - 8. doi: 10.1109/MP.2006.1649003.
2. Нуруллаев М. М. Моделирование информационных процессов в интегрированных системах безопасности // Молодой ученый. – 2018. – №. 17. – С. 26-27.
3. Nisha, Shireen & Farik, Mohammed. (2017). RSA Public Key Cryptography Algorithm – A Review. International Journal of Scientific & Technology Research. 6. 187-191.
4. Aloev R.D., Nurullaev M.M. Software, algorithms and methods of data encryption based on national standards // IIUM Engineering Journal 21 (1), pp. 142–166, 2020. doi: 10.31436/iiumej.v21i1.1179.
5. "Cryptographic protection of information. The formation and verify digital signatures," O'z DSt 1092:2009. 2009. Accessed: Mar. 16, 2023 [Online]. Available: https://tace.uz/ru/docs/OzDSt_1092.pdf
6. Johnson, D., Menezes, A. & Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). doi: 10.1007/s102070100002
7. Aloev R.D., Nurullaev M.M. Development of the Software Cryptographic Service Provider on the Basis of National Standards // Journal of Systemics, Cybernetics and Informatics, 17 (1), pp. 260–272, 2019.
8. Muhammadovich N. M. The need to implement cryptographic information protection tools in the operating system and existing solutions // Central Asian Journal of Mathematical Theory and Computer Sciences. – 2023. – Т. 4. – №. 3. – С. 1-4. doi: 10.17605/OSF.IO/J4U89
9. Aloev R.D., Nurullaev M.M. Cryptography Service Provider – Data Encryption // in Proc. Conference on Complexity, Informatics and Cybernetics, Orlando, Florida, USA, pp.127–131, 2019.
10. Nurullaev M.M. Random number generation to ensure information security on mobile phones // International Journal of Contemporary Scientific and Technical Research, 1(1) pp.12-16, 2022. doi: 10.5281/zenodo.7238632
11. Mukhammadovich N. M., Djuraevich A. R. Working with cryptographic key information. // International Journal of Electrical and Computer Engineering. – 2023. – Т. 13. – №. 1. – С. 911. doi: 10.11591/ijece.v13i1.pp911-919