AUTHENTICATION ALGORITHM FOR SMART POWER GRID SYSTEMS

V. A. Dokuchaev [1,2], **I. A. Safonov** [3], **J. Rahmani** [4],
[1] Network Information Technologies and Services, MTUCI, Moscow, Russia, v.a.dokuchaev@mtuci.ru
[2] International Telecommunication Union (GCBI ITU), Geneva, Switzerland
[3] Network Information Technologies and Services, MTUCI, Moscow, Russia
[4] Network Information Technologies and Services, MTUCI, Moscow, Russia
j.rahmani@mtuci.ru

ABSTRACT

The paper describes an authentication algorithm structure and key stages of its application for smart power grid systems, its advantages over traditional solutions, and practical application scenarios. An authentication algorithm based on a combination of verifiable encryption and one-time keys, designed to ensure high cryptographic strength in demanding security environments. Particular attention is paid to adapting the algorithm to critical infrastructures such as energy grids, where delays and data compromise can lead to catastrophic consequences.

DOI: 10.36724/2664-066X-2025-11-3-22-28

Received: 12.06.2025
Accepted: 25.07.2025

KEYWORDS: *smart power; authentication; verifiable encryption; one-time keys; security; smart grid; energy systems*

Citation: V.A. Dokuchaev, I.A. Safonov, J. Rahmani, "Authentication algorithm for smart power grid systems", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 22-28.

Introduction

Modern authentication systems face numerous challenges related to increasing security and user experience requirements [1, 2]. Communication networks continue to evolve, and with the support of comprehensive long-term development programs, quality standards can be expected to improve [3-5]. These issues are particularly pressing in the context of critical infrastructures such as energy grids. Energy systems, the backbone of the economy and everyday life, are increasingly becoming targets for sophisticated cyberattacks capable of causing large-scale outages, financial losses, and threats to national security [6]. Protecting such systems requires not only resilience to external threats but also ensuring uninterrupted operation, which challenges developers to combine high security with minimal delays in authentication processes.

With the growing number of cyberattacks and the increasing sophistication of hacking methods, traditional approaches such as passwords and static keys are becoming increasingly less reliable. Passwords are often vulnerable to phishing, brute-force attacks, and data leaks, while static keys, while providing a higher level of security, are vulnerable to compromise over long periods of use—especially in systems where regularly changing keys is difficult, as is the case with distributed power grid nodes. These issues are driving the search for new solutions that can provide both a high level of security and the operational efficiency critical to energy facilities.

One of the most promising areas in this area is the use of one-time keys in combination with verifiable encryption. One-time keys, generated dynamically for each session or transaction, minimize the risks associated with their interception or reuse by attackers, which is especially relevant for power grids with their vast number of devices. However, one-time keys alone do not solve all problems, such as verifying the integrity of authentication processes in real time. Verifiable encryption comes to the rescue, ensuring that all authentication stages are completed correctly without malicious intervention, which is critical for preventing man-in-the-middle attacks in power facility control systems [7, 8].

The purpose of this article is to present an authentication algorithm based on these technologies and demonstrate its advantages in the context of protecting energy infrastructures. The proposed solution is aimed not only at increasing cryptographic strength but also at optimizing computing resources, making it applicable even in power system networks with limited network bandwidth.

The concept of verifiable encryption

Verifiable encryption is a cryptographic method that encrypts a message in such a way that a verifier can verify that certain conditions for the encrypted data are met without decrypting it. This approach is based on the use of zero-knowledge proofs and cryptographic protocols that guarantee data integrity.

One of the key properties of verifiable encryption is transparency. This means that an encrypted message can be verified against specified parameters without having to disclose it. For example, it can be verified that a message was signed by a specific user or contains certain attributes while remaining encrypted.

Preserving confidentiality is also an important aspect. The message content remains protected, which is achieved through the use of strong cryptographic algorithms such as RSA, elliptic curve algorithms, or homomorphic encryption [9]. Data integrity is ensured by digital signature mechanisms or hash functions.

One-time keys, as their name suggests, are used only for a single operation or session. One-time keys minimize the risks associated with compromise, as even if leaked, the key cannot be reused. These keys are generated for each client-server interaction and are then destroyed.

One-time keys play an important role in preventing replay attacks, in which an attacker intercepts data and attempts to reuse it [10]. The temporary nature of the keys and their uniqueness make these attacks ineffective. Using one-time keys also reduces the risk of leaking long-term keys, as compromising one temporary key does not reveal information about other sessions.

Using verifiable encryption with one-time keys offers a number of advantages. First and foremost, it offers a high level of security. One-time keys eliminate the possibility of reusing compromised data, and verifiable encryption guarantees the confidentiality of the information. The algorithm's flexibility allows it to be adapted to various tasks and conditions. Verification parameters can be configured to meet the requirements of a

specific system or organization. Another important aspect is user convenience, as the method can be integrated with other authentication methods, including biometric technologies and token devices [11]. A comparison with other authentication methods is presented in Table 1.

Table 1

Comparison with other authentication methods

Method	Security level	Usability	Resilience to attacks
Passwords	Low [12]	Medium (requires memorization)	Low (vulnerable to phishing, brute force, and dictionary attacks) [13]
Multi-factor authentication (MFA)	High (combination of factors) [14]	Low (requires additional devices/actions)	High (complicates attacks, but vulnerable to SIM-swap) [15]
Magic Link	Average (depending on the security of the delivery channel) [16]	High (no password required)	Medium (vulnerable to email/SMS interception)
Verifiable encryption	Very high (one-time keys + cryptography) [17]	High (automatic key generation)	Very high (non-reuse by design, protection against MITM) [18]

Authentication algorithm based on verifiable encryption using one-time keys

Authentication algorithm based on verifiable encryption using one-time keys The complexity of attacks aimed at compromising user data is growing, requiring developers to create innovative approaches to ensure the confidentiality and integrity of information. Algorithms based on a combination of verifiable encryption and one-time keys represent one of the most promising technologies. One of the algorithms is presented below:

Registration:

The user sends their digital identity p_1 to the device.

The device generates two keys:

Primary key k_1 for encryption.

Auxiliary key k_2 for hashing.

The device calculates the hash of p_1 using GOST 34.11-20181: $h_2 = H(p_2)$.

The device encrypts the hash h_1 using the key k_1 and the block cipher:

$$c_1 = E_{k_1}(h_1) = h_1 \oplus k_1.$$

The device calculates the hash from the key k_2 and adds it to the encrypted hash h_1:

$$c_1^{'} = c_1 \oplus H(k_2).$$

The device sends $c_1^{'}$ to the server, which stores it in the database.

Verification:

The user sends their digital identity p_1 to the device.

The device generates two one-time keys:

Primary key $k_1^{'}$ for encryption.

Secondary key $k_2^{'}$ for hashing.

The device calculates the hash of p_2 using GOST 34.11-2018:

$$h_2 = H(p_2).$$

The device encrypts the hash h_2 using key $k_1^{'}$ and the block cipher:

$$c_2 = E_{k_1^{'}}(h_2) = h_2 \oplus k_1^{'}.$$

The device calculates the hash of key $k_2^{'}$ and adds it to the encrypted hash h_2:

$$c_2^{'} = c_2 \oplus H(k_2^{'}).$$

The device sends $c_2^{'}$ to the server.

The server calculates the encrypted distance between $c_1^{'}$ and $c_2^{'}$ using function *F*:

$$F(c_1^{'}, c_2^{'}) = c_1^{'} \oplus c_2^{'} = c_d.$$

The server sends the encrypted distance c_d back to the device.

The device decrypts c_d using keys k_1, $k_1^{'}$, k_2 and $k_2^{'}$:

$$D_{k_1,k_1^{'},k_2,k_2^{'}}(c_d) = (c_1 \oplus H(k_2)) \oplus (c_2 \oplus H(k_2^{'})) \oplus (k_1 \oplus k_1^{'}) =$$
$$= (h_1 \oplus H(k_2)) \oplus (h_2 \oplus H(k_2^{'})) \oplus (k_1 \oplus k_1^{'}).$$

The device calculates the final value:

$$h_1 \oplus h_2 = D_{k_1,k_1^{'},k_2,k_2^{'}}(c_d) \oplus H(k_2) \oplus H(k_2^{'}).$$

The device compares $h_1 \oplus h_2$ with the threshold value *s*. If $h_1 \oplus h_2 \le s$, the device returns "OK", otherwise "NG".

Authentication algorithm based on verifiable encryption using one-time keys

In the era of digital transformation, smart technologies are increasingly being implemented in various industries [19]. In recent years, the development of grid technologies has received a strong boost during the pandemic, affecting virtually all industries, including industrial and manufacturing sectors [20]. The energy sector is a critical element of the infrastructure of any country. The operational efficiency of an energy company depends largely on the reliability of corporate information and communication systems and networks. However, these systems also create new data security risks [21].

Modern energy systems, such as smart grids and power generation networks, require a high level of security and reliability [22]. These systems integrate complex infrastructure, including control centers, generators, distribution nodes, smart meters, sensors, and control devices. Interaction between these elements occurs through digital communication channels, which creates risks of cyberattacks, ranging from data interception to command spoofing [23]. The implementation of Smart Grid technology in the electric power industry increases economic efficiency, its use significantly reduces the costs of production, distribution and consumption of electricity [24].

To protect such systems, an authentication algorithm based on verifiable encryption with one-time keys is proposed, ensuring the integrity and confidentiality of critical information [25]. Such tools help mitigate emerging risks in the information and communication systems of energy generating companies
[26, 27].

Power systems are based on data transmission networks controlled by SCADA (Supervisory Control and Data Acquisition) systems. These systems are responsible for collecting information, remotely controlling equipment, and monitoring parameters in real time [28]. Smart Grid SCADA controls smart meters, transformers, and circuit breakers, and in large energy companies, it regulates generator operating modes, balances loads, and monitors the status of power lines [29]. Data is transmitted between field devices such as RTUs (Remote Terminal Units) and PLCs (Programmable Logic Controllers), servers, and dispatch interfaces via wired and wireless channels.

However, many communication protocols, including Modbus and DNP3, are not designed to protect against modern cyberthreats, making them vulnerable to attack. The implementation of verifiable encryption is particularly relevant for IEC-61850, which is used in digital substations, and IEEE C37.118, where data integrity is critical for real-time network management [30, 31].

The proposed method is adapted not only for classic SCADA systems but also for new architectures, including distributed substations, where the method protects control commands during high-voltage line switching; hybrid microgrids (Microgrids), ensuring data authentication between solar farms, wind turbines, and energy storage systems in standalone mode; and automatic load shedding (ALS) systems, verifying the authenticity of load balancing commands during power grid failures [32]. For decentralized networks with intermittent connections to the control center, such as remote wind farms, the algorithm implements local verification via pre-established keychains, minimizing dependence on centralized infrastructure and maintaining security even under limited connectivity.

The main problem with such systems is the lack of guarantees of the authenticity of transmitted commands. An attacker can infiltrate the communication channel, spoof parameters, or resend an intercepted command, causing equipment to malfunction. This can lead to accidents, consumer outages, or infrastructure damage. Traditional encryption methods are not always effective: long sessions with persistent keys facilitate replay attacks, and the lack of verification mechanisms allows data manipulation [33].

Each command, such as "disable overloaded section" or "adjust generator frequency," is encrypted with a unique key that is destroyed after use. This eliminates the possibility of reusing intercepted data. Verifiable encryption simultaneously ensures that the command has not been altered during transmission: any attempt to tamper with it results in automatic message rejection. When sending an instruction to shut down a transformer, the system generates a one-time key, encrypts the command, and transmits it to the recipient. Even if the communication channel is compromised, an attacker will be unable to inject false instructions or reproduce previously sent data.

With the growing number of IoT devices, the issue of compatibility with resource-intensive algorithms arises. The proposed method is optimized for low-power processors. Key generation requires less than 5% of the computing power of a typical protection and automation device [34]. The authentication latency does not exceed 2 ms, which meets the requirements of GOST R IEC 61850-5-2011222 for critical commands. To minimize the load, messages are grouped with a single verification key.

Special attention is paid to the protection of emergency notification systems. Messages about overloads, power line failures, or abnormal voltage surges require instant delivery and absolute reliability. The algorithm ensures their integrity through verifiable encryption, and one-time keys prevent blocking or delays of notifications. Upon detecting generator overheating, the system generates a key, encrypts the message, and sends it to the control center. The recipient verifies the authenticity of the data and the validity of the key, eliminating false alarms or the concealment of an emergency.

Thus, the authentication algorithm based on verifiable encryption with one-time keys offers a universal solution for power systems. It protects control commands, monitoring data, and emergency messages, minimizing the risk of cyberattacks. Implementing this approach increases the resilience of Smart Grids and power networks, ensuring the security of critical infrastructure in the face of growing digital threats.

Conclusion

The proposed authentication algorithm, based on verifiable encryption and one-time keys, represents a significant advance in security and usability for modern systems. In an era of increasingly sophisticated cyberthreats and ever-increasing data protection requirements, this approach offers a reliable solution capable of minimizing the risks associated with information leaks and key compromise.

An important aspect of the proposed algorithm is its versatility. Its adaptability to various application areas, including financial services, corporate networks, government platforms, and even the Internet of Things (IoT), opens up new possibilities. In each of these areas, the algorithm is capable of providing a high level of security while maintaining simplicity and user convenience. This is especially important in an environment where users increasingly prefer systems that are not only secure but also intuitive to use. However, despite all its advantages, the algorithm requires further development and optimization.

One area for future research could be improving its performance, especially when working with large data volumes or in systems with high loads. Furthermore, it is important to explore the possibilities of integrating the algorithm with other technologies.

REFERENCES

[1] S. V. Pavlov, E. V. Leonovich, V. V. Maklachkova, V. A. Dokuchaev, “Networks 2030: prospects and challenges,” *REDS: Telecommunications Devices and Systems*, 2022, vol. 12, no. 2, pp. 17-23.

[2] V. A. Dokuchaev, S. S. Mytenkov, D. D. Rakhmani, I. A. Safonov, “Analysis of vulnerabilities and risks of traditional password systems in the context of corporate distributed systems and critical infrastructures,” *Economics and quality of communication systems*. 2025. No. 2 (36), pp. 135-147.

[3] R. Jahed, “Analysis of trends in the development of the communications industry in the Islamic Republic of Iran,” *Information Society Technologies: Proceedings of the XIV International Industry Scientific and Technical Conference*, Moscow, March 18-19, 2020. Moscow: Media Publisher, 2020, pp. 300-301.

[4] V. A. Dokuchaev, “Digital twins: new opportunities, new risks,” *Innovations for building a digital future: Proceedings of the XXIX International Forum IAS' 2025*, Moscow, April 25, 2025. Moscow: State University of Education, 2025, pp. 82-89.

[5] V. A. Dokuchaev, Yu. I. Vedeneeva, “Security and trust in digital twin technologies,” *Theory and practice of economics and entrepreneurship: Proceedings of the XXII International scientific and practical conference*, Simferopol – Gurzuf, April 24-26, 2025. Simferopol: IP Zueva TV, 2025, pp. 269-271.

[6] V. A. Dokuchaev, “Artificial Intelligence and Energy: New Drivers, New Risks,” *Trends in the Development of the Internet and Digital Economy: Proceedings of the VIII International Scientific and Practical Conference*, Simferopol-Alushta, May 29-31, 2025. Simferopol: IP Zueva T.V., 2025, pp. 16-17.

[7] R. L. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120-126.

[8] S. Goldwasser, S. Micali, “Probabilistic Encryption,” *Journal of Computer and System Sciences*, 1984, vol. 28, no. 2, pp. 270-299.

[9] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, “Handbook of Applied Cryptography,” Boca Raton: CRC Press, 1996, p. 816.

[10] D. Boneh, M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *Advances in Cryptology – CRYPTO 2001*. Berlin: Springer, 2001, pp. 213-229.

[11] M. Kihara, S. Iriyama, “New Authentication Algorithm Based on Verifiable Encryption with Digital Identity,” *2019 International Conference on Information Security*, Tokyo, 2019, pp. 1-8.

[12] Verizon. Data Breach Investigations Report [Electronic resource]. Mode of access: https://www.verizon.com/business/resources/reports/dbir (Date of access: 20.10.2025)

[13] OWASP. Authentication Cheat Sheet [Electronic resource]. Mode of access: https://cheatsheetseries.owasp.org (Date of access: 20.10.2025).

[14] Google Security Blog [Electronic resource]. Mode of access: https://security.googleblog.com (Date of access: 20.10.2025).
[15] NIST. Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Electronic resource]. Mode of access: https://doi.org/10.6028/NIST.SP.800-63b (Date of access: 20.10.2025).
[16] FIDO Alliance. Whitepaper [Electronic resource]. Mode of access: https://fidoalliance.org (Date of access: 20.10.2025).
[17] IETF. RFC 6238: Time-Based One-Time Password Algorithm [Electronic resource]. Mode of access: https://tools.ietf.org/html/rfc6238 (Date of access: 20.10.2025).
[18] Forrester Research. Zero-Trust Network Architecture [Electronic resource]. Mode of access: https://www.forrester.com (Date of access: 20.10.2025).
[19] V. A. Dokuchaev, "Digital transformation: New drivers and new risks*," 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH 2020)* Proceedings, Vienna, October 20-22, 2020. New York: IEEE, 2020, p. 9261544. DOI: 10.1109/EMCTECH49634.2020.9261544.
[20] J. Rahmani, "Trends in the development of network technologies in 2022," *Information Society Technologies: Proceedings of the XVI International Industry Scientific and Technical Conference*, Moscow, March 2-3, 2022. Moscow: Media Publisher, 2022, pp. 30-31.
[21] V. A. Dokuchaev, "Typical structure of a corporate infocommunication system of an energy-producing company of the IRI," *III Scientific Forum "Telecommunications: Theory and Technology (TTT-2019)": Proceedings of the XXI International Scientific and Technical Conference*, Kazan, November 18–22, 2019. Vol. 1. Kazan: KNRTU-KAI, 2019, pp. 298-299.
[22] NIST. Special Publication 1108R3. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2020.
[23] G. Liang, et al., "Cybersecurity for Power Grids: Challenges and Solutions," *IEEE Transactions on Smart Grid*, 2017, vol. 8, no. 5, pp. 2446-2455.
[24] M. S. Kozhanov, "Analysis of the economic efficiency of Smart Grid implementation in the electric power industry and its impact on electricity prices," *Theory and Practice of Economics and Entrepreneurship: Proceedings of the XX International Scientific and Practical Conference*, Simferopol – Gurzuf, April 20-22, 2023. Edited by N. V. Apatova. Simferopol: V. I. Vernadsky Crimean Federal University, 2023, pp. 318-322.
[25] M. Bellare, V. T. Hoang, P. Rogaway, "Foundations of garbled circuits," *CRYPTO 2013: Proceedings of the 33rd Annual Cryptology Conference*, Santa Barbara, 2013, pp. 784-807.
[26] J. Rahmani, "Study of risk management methods in the infocommunication system of an energy-producing company of the Islamic Republic of Iran," *T-Comm*, 2022, vol. 16, no. 8, pp. 30-37. DOI: 10.36724/2072-8735-2022-16-8-30-37.
[27] J. Rahmani, "The main approaches to evaluating the effectiveness of applying the risk analysis and management methodology at an energy company," *T-Comm*, 2022, vol. 16, no. 9, pp. 46-55. DOI: 10.36724/2072-8735-2022-16-9-46-55.
[28] IEEE. IEEE Std C37.1-2007. IEEE Standard for SCADA and Automation Systems. New York: IEEE, 2007.
[29] IEC. IEC 61850-7-420:2021. Communication networks and systems for power utility automation – Part 7-420: Basic communication structure — Distributed energy resources logical nodes. Geneva: IEC, 2021.
[30] IEC. IEC 61850-5:2020. Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models. Geneva: IEC, 2020.
[31] IEEE. IEEE C37.118.2-2011. IEEE Standard for Synchrophasor Data Transfer for Power Systems. New York: IEEE, 2011.
[32] A. Ulbig, et al., "Impact of Grid Integration of Wind Power on Power System Stability," *Applied Energy*, 2014, vol. 123, pp. 145-153.
[33] ENISA. Report on ICS Security [Electronic resource]. Mode of access: https://www.enisa.europa.eu (Date of access: 10.01.2025).
[34] M. Usman, et al., "IoT-Based Secure Energy Management for Smart Grids," *IEEE Internet of Things Journal*, 2021, vol. 8, no. 10, pp. 7892-7905.