Сучасний стан наукових досліджень та технологій в промисловості. 2021. № 4 (18)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

UDC 621.3.01+621.38
DOI: https://doi.org/10.30837/ITSSI.2021.18.031

P. KLIMUSHYN, T. SOLIANYK, O. MOZHAEV, V. NOSOV, T. KOLISNYK, V. YANOV

HARDWARE SUPPORT PROCEDURES FOR ASYMMETRIC AUTHENTICATION OF THE INTERNET OF THINGS

Subject of research: procedures of asymmetric authentication of Internet of Things nodes to ensure the highest level of security using cryptographic chips. The **aim** of the article is to study the ways of potential use of cryptographic chips to ensure secure authentication of Internet of Things sites using asymmetric cryptography procedures. The article solves the following **tasks:** analysis of hardware support technologies for asymmetric cryptography of the Internet of Things; definition of secure procedures for asymmetric authentication of Internet of Things sites and their constituent elements: creation of certificates, verification of public and private keys. Research **methods:** method of structural and functional analysis and design of complex systems, methods of identification and authentication of information objects, cryptographic methods of information protection, methods of security analysis of distributed information systems. The **novelty** of the study is the analysis of hardware support technologies for asymmetric cryptography of Internet of Things with cryptographic chips and the definition of structural and functional schemes for the implementation of procedures for asymmetric authentication of Internet of Things. Distinctive features of the provided asymmetric authentication schemes and procedures are: ensuring an increased level of information security through secure storage of cryptographic keys, digital signatures, certificates, confidential data in a **novelty** security environment protected from external attacks and no need to store private keys on the host side. The **results** of the work are procedures and schemes of application of cryptomicrops of asymmetric authentication to ensure the protection of Internet of Things. Analysis of the functioning of the presented schemes allowed to draw the following **conclusions.** The proposed structural and functional schemes for the implementation of procedures for asymmetric authentication of Internet of Things using cryptographic chips give the user an easy opportunity to implement cryptography without expertise in this field. These chips use the ECDSA digital signature computing and verification hardware with elliptical curve advantages, as a proven and reliable authentication algorithm, and the ECDH symmetric encryption session key generation unit. The provided schemes and procedures support three components of information security, namely: confidentiality, integrity and authenticity of data. Examples of potential applications of the provided schemes and procedures can be implemented using any asymmetric authentication chip, but it is recommended that they be used to generate encryption session keys and where digital signatures are required to verify data and code for integrity and authenticity.

Keywords: Internet of Things; asymmetric authentication; encryption algorithms; cryptographic keys; electronic certificates; digital signatures; cryptographic chips.

Introduction

The Internet of Things (IoT) contributes to the challenges of humanity in areas such as public safety, process management, human life services, health services, productivity and business competitiveness.

The security of the Internet is based on the identification and authentication of its elements, i.e. on the identification of the subjects of connection to the network. Identification provides a unique name to the entity – user, process or hardware and software component, and authentication is associated with the actions of entities on the other side of the network, which determines that the entity of the first party is really the one for whom he pretends to be. That is, a synonym for the word "authentication" is the phrase "validation" of the subject.

The operation of the Internet of Things is based on personalization of entities using unique IDs, MAC addresses, keys and certificates. The use of a certain scheme of personalization has its difficulties in the process of connecting the Internet of Things, because its implementation determines the specified level of security and costs. Therefore, this article is devoted to the study of technical solutions for the implementation of identification and authentication procedures to ensure the highest level of security of the Internet of Things at minimal cost.

Literature analysis

Implementing identification and authentication procedures to ensure the Internet of Things is an urgent task in many environments, such as public order, energy efficiency, health, residential and office space, industry, transportation, agriculture, and more.

The following developments are important in these areas: multifactor and continuous IoT authentication [1], development of mutual authentication protocols [2], IoT authentication based on block chain technology [3, 4], etc.

Much attention in the IoT network is paid to the security of stored, processed and transmitted data, protection against cloning of end IoT devices [5, 6], as well as protection against copying of intellectual property and digital content. A critical factor in protecting the Internet of Things is the authentication of the site when accessing it. Here is a new network paradigm, which is based on interaction without human participation, based on the following features of the IoT: compactness, limited energy and computing resources.

The solution to the problem of providing access to IoT objects in the new paradigm is possible with the use of modern microcontrollers and additional cryptographic accelerators with hardware support for protocols and cryptographic algorithms.

The aim of the article is to investigate the ways of potential use of cryptographic chips of the CryptoAuthentication family for secure authentication of Internet of Things sites using asymmetric cryptography procedures.

It should be noted that in accordance with this goal, this article is a continuation of the study [7], which was devoted to the potential use of cryptographic chips of the

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2021. No. 4 (18)

CryptoAuthentication family using symmetric cryptography procedures, but this study focuses on chips of the CryptoAuthentication family of asymmetric cryptography.

1. Hardware support for Internet of Things security technologies.

The Internet of Things is a network of physical objects that interact with the local or global computing environment according to possible models of interaction: 1) " Thing-Thing"; 2) "Thing-User"; 3) "Thing-Web Object" [8, 9].

Physical objects are IoT nodes and have built-in control microcontrollers that provide interaction with the environment through wired and wireless lines.

The IoT network is based on fog computing and cloud computing models, in which data is computed and stored by IoT nodes (fog nodes) and cloud computing centers.

Computing centers are called "hosts", which include: 1) a computer system or computing device connected to the Internet or a local area network; 2) a server that operates in a client-server format; 3) a computer program that provides services to other programs and applications. Hosts interact with IoT endpoints (called "clients") to solve their functional tasks.

IoT security includes three main components (Confidentiality, Integrity, Authenticity – CIA) [5]: *Authenticity* – validation of the IoT node; *Integrity* – verification of the invariability of the message during transportation to the destination; *Confidentiality* – availability of data only to designated objects or authorized persons.

Network security is provided by network technologies at different levels, sets of protocols used in the network. It should be remembered that the level of security of the entire network is determined by the level of security of the weakest link [7, 10].

The main threats to the security of IoT nodes are: violation of security at the transport layer of cryptographic protocols SSL / TLS; updating the original software with malicious code; non-qualitative generation of random numbers in cryptographic algorithms; violation of access to cryptographic keys; weak protection of IoT ports; physical penetration to the contents of the built-in memory.

Integrated security of IoT nodes must protect evenly from all these threats. Keep in mind that the consequences of a successful attack can put the network as a whole at risk, that is, everything connected to it.

Support for important components of the CIA is achieved in a number of ways [11]: Authenticity – identification and authentication of network nodes; Integrity – formation of the message authentication code (MAC) of the transmitting and receiving parties, followed by their comparison by coincidence to confirm the invariability of the message along the route; Confidentiality – encryption and decryption of messages.

In addition, to protect against contactless attacks use practical measures: storage of cryptographic keys in secure memory chips without the possibility of electrical access to them; shielding IoT nodes or their individual elements to limit electromagnetic radiation; introduction of special power supply circuits to prevent attempts to control voltage or other signals; encryption of key information in the repository; reducing the number of external ports.

It is extremely important to use the tested methodology – to store and use cryptographic keys throughout their life cycle in encrypted form and in secure equipment, i.e. Hardware Security Module (HSM). HSM hardware modules provide all data encryption and decryption operations inside the module, i.e. cryptographic keys do not leave a secure perimeter of the module.

The method of protection of the highest level of information is the use of cryptographic protocols using digital signatures (DS). They are the main mechanisms for authentication, management and certification of keys, as well as for the direct protection of information in the IoT network.

Cryptographic protocols have a number of complex requirements to ensure the required level of security. Recent research has confirmed the fact that authentication mechanisms need to be used for reliable authentication, primarily using DS.

As a rule, cryptographic protocols are implemented based on the use of symmetric and asymmetric cryptocurrencies. The difference between them is the use of secret keys. If the same key is used on both sides (receiving and transmitting), the authentication is symmetric. If a mathematically related pair of public and secret keys is used, the authentication is asymmetric.

Asymmetric authentication method does not distribute all the information that requires protection between the parties to the interaction, so you need reliable protection on one side, which saves hardware and other resources in the authentication process. In addition, the use of asymmetric methods provides the creation of secure DS algorithms, and DS is one of the important cryptographic transformations used to ensure the integrity, authenticity (authenticity), authentication, irrefutability of messages.

The main advantages of the *symmetric block encryption algorithm* (Advanced Encryption Standard – AES) include: 1) scattering of ciphertext characters; 2) mixing statistical dependencies between open and closed text; 3) byte-oriented structure; 4) high speed on different platforms; 5) resistance to many types of cryptanalytic attacks.

There are three ways to implement encryption according to the AES algorithm [12]: 1) software implementation – focused on the bit rate of the platform and uses mathematical optimizations and calculated substitution tables; 2) hardware implementation – uses an extension of the instruction system and special instructions for modern microprocessors, which allow you to perform some hardware operations, which significantly speeds up the process; 3) implementation with the use of video cards – the resources of graphics accelerators are used to perform parallel encryption or decryption.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2021. № 4 (18) ISSN 2524-2296 (online)

Asymmetric cryptography is implemented on the basis of *public-key cryptographic algorithms* built on elliptical curves over finite fields. These algorithms are a powerful tool, but require more computing resources to implement compared to symmetric algorithms. Therefore, the use of asymmetric cryptography algorithms is limited to the exchange and calculation of symmetric session keys in the IoT network [13].

The construction of cryptographic systems of the IoT network is based on the generation of random sequences that are used to generate cryptographic keys, key information and system parameters of the cryptographic system. The cryptographic stability of the system as a whole significantly depends on the quality of these sequences.

There are two classes of random sequence generation: 1) hardware (physical), which provides the formation of sequences with high-quality randomness; 2) software (algorithmic), which allows you to form pseudo-random sequences with a certain period of repetition. That is, the creation of efficient hardware random sequence generators is an important and separate area of cryptography research.

Thus, hardware protection of information using cryptochips is much more expensive than similar software, but they allow you to achieve the highest level of information protection and are now increasingly used in the IoT network. The advantages of hardware protection of the IoT network are: hardware method of forming random sequences; methodology of HSM security hardware modules – execution of cryptographic operations in the environment of protected cryptographic chips (security on the chip); delimitation and unloading of the CPU functions of the IoT node using a specialized cryptoprocessor to perform cryptographic transformations; guaranteeing the integrity of cryptographic data transformations; increasing the speed of cryptographic data transformations.

These advantages have determined the development of hardware for the protection of the Internet of Things: built-in random sequence generators, cryptographic accelerators and cryptographic modules in general-purpose microprocessor kits [9, 15].

It should be noted that the trend towards integrated security solutions is observed in 32-bit microcontrollers with additional cryptographic information protection features that provide secure key generation and storage, support for electronic certificates and electronic signatures, secure download and update applications.

The procedures of asymmetric cryptography with the use of cryptographic chips of the CryptoAuthentication family in the security of the Internet of Things should include: pairing (public and private) of asymmetric encryption keys; calculation of digital signature and its verification; generating session (secret) keys of symmetric encryption; creation of client and enterprise certificates; verification of public keys of the client and the enterprise; verification of the private key of the client and the enterprise; secure download of updated software.

2. Asymmetric cryptography procedures in the Internet of Things

The advantage of public key cryptosystems is the ability to use digital signatures. A digital signature is a means of authenticating the author of a message and controlling the integrity of the data. In addition, the DS carries the principle of "non-disclaimer", i.e. the author of the message cannot deny the fact of his authorship of the information signed by him.

A digital signature of a message is a sequence of fixed-length bits generated for a message using the author's private key. The identification of the author of the signature is verified using a public key. The DS is sent with the message and becomes an integral part of it. The recipient of the message must have the sender's public key. Public key distribution schemes can vary from simple personal key exchange to a complex multi-level public key infrastructure (PKI).

The Elliptic Curve Digital Signature Algorithm (ECDSA) based on elliptic curves, adopted as an ISO standard, contains two separate procedures (fig. 1): 1) digital signature calculation algorithm; 2) digital signature verification algorithm. The digital signature calculation algorithm uses a private key, and the verification algorithm uses a public key. Digital signature calculation / verification is an authentication procedure that involves creating a data digest that is then encrypted with the sender's private key. The result is a digital signature. To verify the digital signature, the recipient independently hashes the received source data using the hash algorithm SHA (Secure Hash Algorithm), decrypts the digital signature with the sender's public key, retrieving the sent digest, and compares it with the calculated one. If there is a match, the digital signature is considered valid.

Hardware cryptographic chips of asymmetric authentication have: 1) built-in random sequence generator; 2) protected Electrically Erasable Programmable Read-Only Memory (EEPROM) for storing cryptographic keys, digital signatures, certificate data on public keys, confidential data. These chips support full 256-bit cryptography on elliptical curves: they perform ECDSA algorithms for digital signature calculation and verification algorithms and the Diffie-Hellman Session key (Elliptic Curve Diffie-Hellman ECDH) encryption algorithm for encryption.

Cryptographic chips support three components of information security, namely: confidentiality, integrity and authenticity of data to protect IoT network nodes, so there is no need to organize secure storage of confidential data on the host side. This is achieved by the fact that the cryptographic chip of asymmetric authentication stores keys, signatures, certificates, confidential data on the chip in a hardware environment protected from external attacks. It is a great addition to any microcontroller capable of performing symmetric encryption (such as AES), thanks to the built-in ECDH algorithm. The asymmetric authentication cryptographic chip implements secure firmware download during the initial download or

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2021. No. 4 (18)

update (including remote) stages, using the ECDSA digital signature verification algorithm.

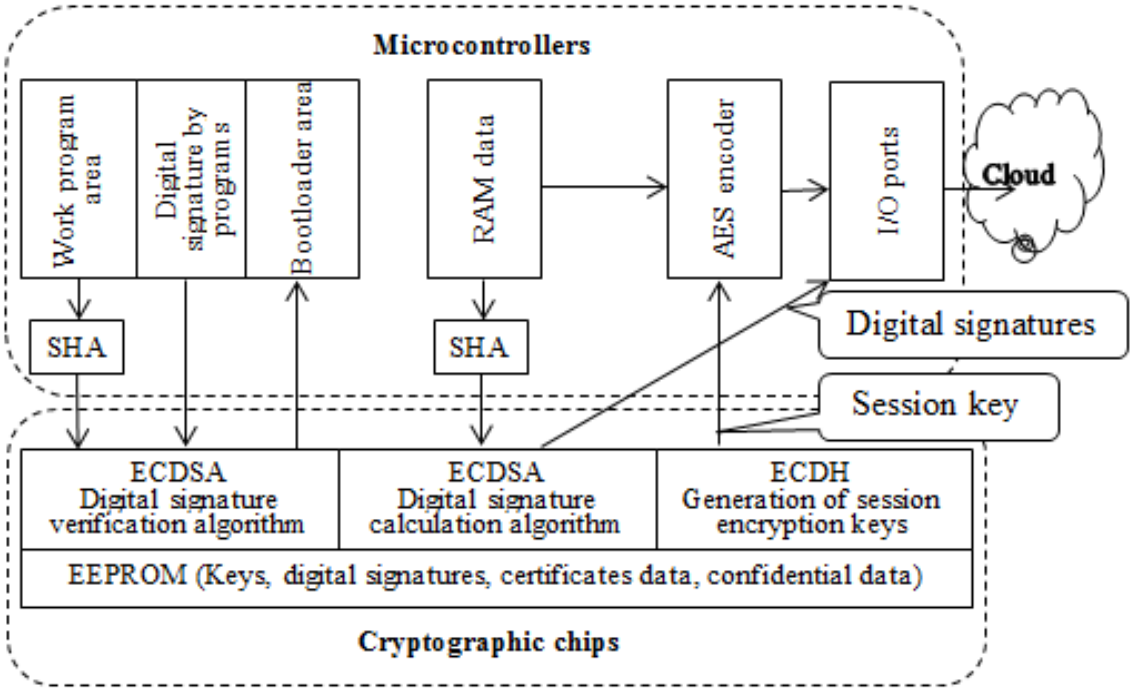

Fig. 1. Scheme of interaction of cryptographic chip and host microcontroller

A useful option for cryptographic chips of asymmetric authentication is a flexible number of usage functionality based on secure final counters. The main application of this feature is to count or limit the number of uses of the final product, such as a printer cartridge or smartphone battery. The current value of the counter can also be associated with the cryptographic key by hashing. Since the meter is monotonous, i.e. works only in one direction and is never reset, the calculated digest (MAC) will always be different.

Another application of total counters is to limit the amount of work in the pair system (one server – one client). This enhances information security: if a client is already working with a particular host, it cannot be used by another host.

In asymmetric cryptography compared to symmetric cryptography in the authentication of users and end devices there is a problem of public key ownership, i.e. secure distribution of public keys. Since the public key can be exchanged during the transfer process, it is very important to convince users that, firstly, the key is genuine and, secondly, it was obtained from the party from whom it was intended. To secure the distribution of public keys among a large number of users, a special mechanism has been developed, which is based on public key certificates.

The interaction between the client and the host in general is carried out according to the scheme: 1) the client requests a connection; 2) the host sends its certificate with a public key; 3) the client sends his certificate with a public key; 4) calculation of the session key of the closed session; 5) exchange of messages that are protected by a shared secret key (encryption – integrity). As you can see from the diagram, the client and host do not send their public keys in their pure form, they send certificates that contain public keys.

This is done so that the client must be able to distinguish a real host from a fake one. In order to carry out such inspections, Certificate Authorities (CAs) have been established as independent corporations that issue digital certificates certifying the public key of the organization whose name is indicated in the certificate. Upon receipt, the client will verify the signature of the certificate using the public key of the certification authority, which allows you to ensure the security of Internet connections.

To simplify the description of the process of asymmetric authentication with ECDSA for chips of the CryptoAuthentication family, on the example of the potential use of cryptographic chips APESSx08A, it can be divided into two successive stages [6, 15].

At the first stage the client's public key is checked. This is done by the host-side digital signature verification algorithm, obtaining the necessary information from the certificate provided by the client. Only if the verification result is successful does the authentication process continue.

In the second stage, the already private key of the client is checked. To do this, the host sends a request (random number) to the client, which he signs with his private key. The generated digital signature is sent back to the host, which starts the algorithm to verify it. If successful, the client is considered genuine.

Distinctive features of the asymmetric authentication process are: providing an increased level of information security, as it does not require secure storage of the private key on the host side (only on the client side); CryptoAuthentication chips have an ECDSA hardware unit, which makes them very light and easy to use.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2021. № 4 (18) ISSN 2524-2296 (online)

3. Creating client and host certificates

The creation of the client's certificate takes place on the host, which produces the final products (hereinafter referred to as the enterprise). The client certificate consists of two components (fig. 2): 1) Certificate data and 2) Digital signature of the enterprise. The process of its creation begins in a special tester (programmer), which personalizes the cryptographic chip. The data of the future certificate is transferred to the tester. Certificate data consists of three blocks: 1) statistical data – is basic information about the product, such as the name and composition of the product, the name and address of the company, etc.; 2) Dynamic data – is variable information: for example, serial number, date and time of programming, expiration date, etc.; 3) Public key of the client (generated together with the private key in advance). The private key is securely kept secret and programmed into a protected area of the cryptographic chip memory at the enterprise during the production of finished products.

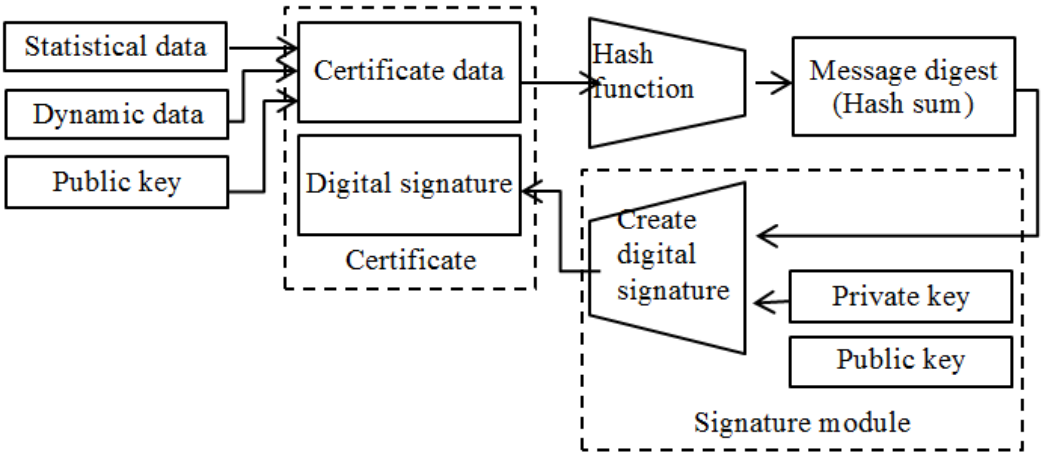

Fig. 2. Creating a client certificate

The second half of the client's certificate – digital signature of the company – is used in two ways: in open unencrypted form as part of the certificate and in the form of digital signature, which is created by hashing (Hash function) certificate data followed by a digest in the signature module module) of the enterprise through the algorithm for calculating the digital signature (Create digital signature). This uses the Private key (Private key) of the enterprise, stored in the signature module. The generated digital signature is sent to the tester, where it is combined with the original (i.e. non-hashed) data, thus completing the process of creating the Certificate of the client (final product) and the finished certificate can now be downloaded to the cryptographic chip.

To confirm the authenticity of the company that produces the finished product, you may also need a certificate. It is issued by one of the CA certification centers that certify the keys of the enterprise.

The procedure for creating an enterprise certificate is similar to the procedure for creating a client certificate. Initially, static and dynamic data and the public key of the enterprise come to the tester. In the tester, all three components are combined to form certificate data, hashed in the tester. The received digest is sent to the certification center, where it is signed with a private key certifying. The received digital signature is sent back to the enterprise, where in the tester it is combined with the data of the enterprise certificate, thus forming a completed certificate. The public key of the certification authority is also sent to the enterprise and programmed into the control microcontroller of the system (on the host).

Finally, both the finished product certificate and the enterprise are loaded by the tester into the protected independent programmable memory of the cryptographic chip.

4. Verification of public keys of the client and the enterprise

At this stage, the host requests from the client information about its authenticity, which is part of the certificates of the client (Certificate Client) and the enterprise (Certificate Enterprises) (fig. 3). After receiving both documents, the host reads from the client's certificate his data (Certificate data) and public key (Public key Client), as well as a digital signature (Digital signature), made in the signature module at the enterprise.

The host also retrieves its data and the public key Enterprises from the Certificate Enterprises, as well as the CA's signature. The host then separately hashes the certificate dataset, creating two digests – the Message digest Client and the Message digest Enterprises. The public key removed from the enterprise certificate is fed to the input of the ECDSA digital signature verification algorithm together with the client certificate data digest and the enterprise digital signature. The task of these calculations is to verify the client's public key.

If successful, the host proceeds to the next step of verifying the authenticity of the enterprise (fig. 3). Without such verification, the client's public key cannot be considered genuine. This is done by verifying the signature of the CA certification authority, which certifies the keys of the enterprise, which is part of the enterprise certificate.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2021. No. 4 (18)

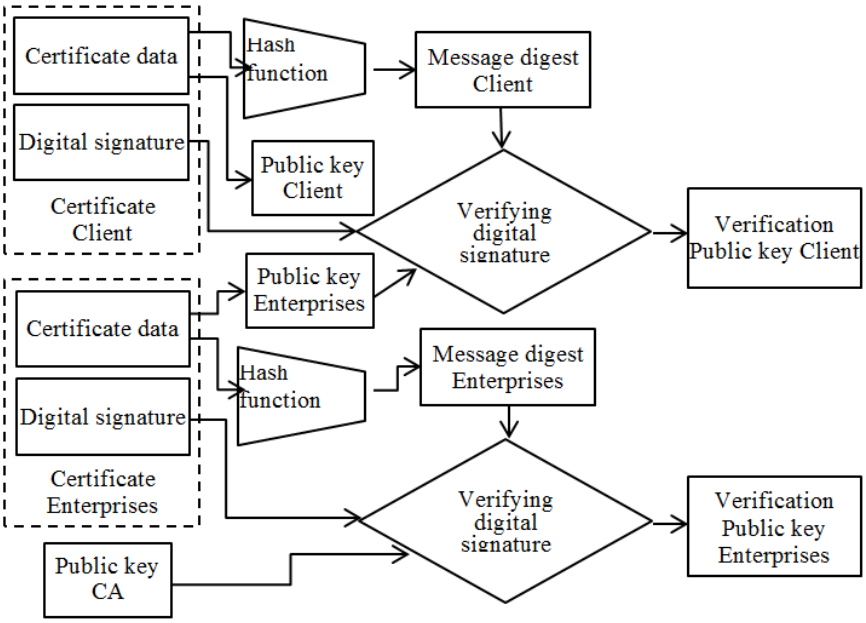

Fig. 3. Verification of the public key of the client and the enterprise

The digital signature of the CA certificate is submitted to the input of the second cycle of the ECDSA digital signature verification algorithm together with the enterprise certificate data digest (calculated in the previous step) and the public key CA, which was preloaded into the host microcontroller memory.

If both successive ECDSA verification cycles are performed without errors, then the client's public key is considered valid and verified all the way from the product (through the enterprise) to the CA certifying center.

5. Private key verification. After successful completion of the first stage of ECDSA calculations, the second stage begins – verification of the client's private key (fig. 4). It will be recalled that the ultimate goal of the entire asymmetric authentication process is mathematical proof that the client's public and private keys are indeed a real key pair.

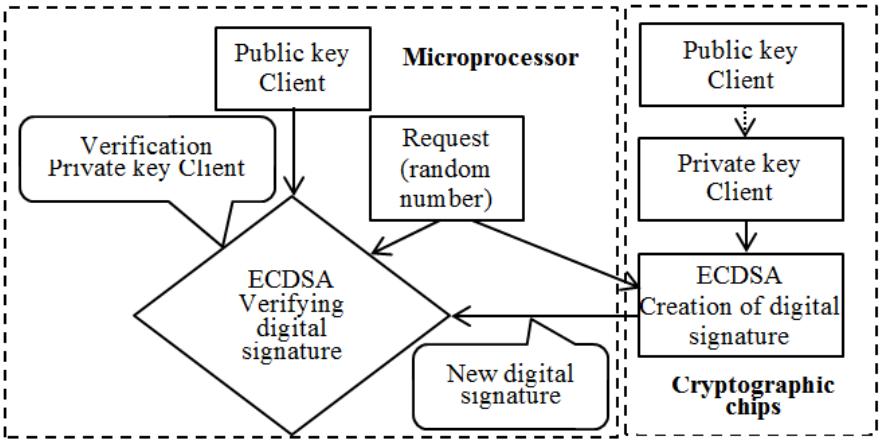

Fig. 4. Private key verification scheme

Conclusions

The main threats to the security of IoT nodes are: violation of the protection of cryptographic protocols SSL / TLS at the transport level; updating the original software with malicious code; non-qualitative generation of random numbers in cryptographic algorithms; violation of access to cryptographic keys; weak protection of IoT ports; physical penetration to the contents of the built-in memory.

The level of complex security of the Internet of Things on the route "client-host" solves the following tasks: symmetric or asymmetric authentication of interacting system devices; creation and exchange of session encryption keys; storage of encryption keys; data integrity; data confidentiality; software and data download protection.

With the asymmetric authentication method, all the information that requires protection is not distributed between the subjects of interaction, and therefore requires reliable protection on one side, which saves hardware and other resources in the authentication process. In addition, the use of asymmetric methods provides the creation of secure DS algorithms, and DS is one of the important

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2021. № 4 (18) ISSN 2524-2296 (online)

cryptographic transformations used to ensure the integrity, authenticity (authenticityConclusions), authentication and irrefutability of messages. But this method requires much more computing power to encrypt and decrypt data compared to symmetric block encryption algorithms.

It is extremely important to use the tested methodology – to store and use cryptographic keys throughout their life cycle in encrypted form and in secure equipment, i.e. hardware security modules HSM. These modules provide all encryption and decryption operations within the module, i.e. cryptographic keys do not leave the protected perimeter of the module.

To protect against contactless attacks, use practical measures: storage of cryptographic keys in secure memory chips without the possibility of electrical access to them; shielding IoT nodes or their individual elements to limit electromagnetic radiation; introduction of special power supply circuits to prevent attempts to control voltage or other signals; encryption of key information in the repository; reducing the number of external ports.

Algorithms of asymmetric cryptography have been thoroughly studied by cryptanalysts for vulnerabilities, and it is often assumed a priori that the systems that use these algorithms are secure by default. But this assumption is not always true.

First, like all cryptographic systems and algorithms, the cryptographic stability of cryptographic algorithms depends on the keys. If an attacker can get the key, he is able to pretend to be authentic, decrypt all network messages and, in general, destroy the security of the system. That is, the key to Internet security is key security. The problem is that not all systems have a really secure place to store keys, protected from attacks.

Secondly, like all cryptographic algorithms, asymmetric algorithms can be used in many variants and ways, as a result, the security system can be broken through the wrong or ill-conceived interface, organization of the device, data exchange procedures and more. This is obvious in theory, but not always easy to put into practice.

Third, when something needs to be encrypted using cryptographic algorithms, most modes require an initial sequence. This sequence should never be repeated and in many modes must be a random number. The problem is that if the same message is processed with the same initial sequence, the encrypted text will be exactly the same, which is important information for calculating the encryption key by the cryptanalyst.

Many developers now rely on specialized cryptographic hardware, including end devices and protected integrated circuits of various classes. Hardware-protected chips of the CryptoAuthentication family belong to the following specialized cryptographic tools.

The CryptoAuthentication family of chips solves system problems: secure key storage and built-in cryptoaccelerators that perform standard cryptographic procedures.

The motto of the CryptoAuthentication family is "Crystal Security". The chips include voltage, frequency and temperature sensors, a protective metal screen over the entire surface of the crystal and other methods of counteracting various attacks. When detecting attempts to penetrate the chip, the secret data contained in it is destroyed.

Examples of potential applications can be implemented using any chip of the CryptoAuthentication family. However, the main feature of APESSx08A is the built-in algorithm for calculating and verifying the digital signature ECDSA and hardware encoder ECDH. Therefore, it is recommended that they be used to generate encryption session keys and where digital signatures are required to verify data and code for integrity and authenticity.

There are many suggestions for improving the Internet connection system based on solutions for secure device personalization, which includes: the use of cryptographic algorithms with shorter keys instead of long keys; smaller certificates; extended validity of the key certificate; the ability of the device to verify the host certificate "offline"; a secure and easy way to personalize and store certificates along with keys directly on your device; services of the certification center for the issuance and verification of ordered certificates; mutual authentication of the client and the host; simple and automated allocation of device resources in a remote application on the host, etc.

References

1. Falk, R., Fries, S. (2016), "Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things", *CYBER 2016: The First International Conference on Cyber-Technologies and Cyber-Systems*, P. 69–74.
2. Wu, D. J., Taly, A., Shankar, A., Boneh, D. (2017), "Privacy, Discovery, and Authentication for the Internet of Things", *Computer Science. Cryptography and Security*, available at: https://arxiv.org/abs/1604.06959 (last accessed 21.05.2021).
3. Yavari, M., Safkhani, M., Kumari, S., Kumar, S., Chen, C.-M. (2020), "An Improved Blockchain-Based Authentication Protocol for IoT Network Management", *Security and Communication Networks*, Vol. 2020, P. 16. DOI:10.1155/2020/8836214.
4. Tian, Z., Yan, B., Guo, Q., Huang, J., Du, Q. (2020), "Feasibility of Identity Authentication for IoT Based on Blockchain", *Procedia Computer Science*, Vol. 174, P. 328–332. DOI: 10.1016/j.procs.2020.06.094.
5. CryptoAuthentication™ Family, available at: https://www.microchip.com/en-us/products/security-ics/cryptoauthentication-family (last accessed 21.11.2021).
6. Krivchenko, I. (2015), "Hardware-protected microcircuits of the CryptoAuthentication family: potential applications of ATECCx08A", *Components and technologies*, No. 11, P. 57–64.
7. Klimushin, P., Solianyk, T., Kolisnyk, T., Mozhaev, O. (2021), "Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things", *Advanced Information Systems*, Vol. 5, No.3, P. 103-111.
8. Puleko, I. V., Chumakevich, V. O. (2019), "IoT sensors with time representation of measuring information", available at: https://conf.ztu.edu.ua/wp-content/uploads/2019/06/44.pdf (last accessed 21.11.2021).
9. Sovin, Y. R., Nakonechny, Y. M., Opirsky, I. R., Stakhiv, M. Yu. (2018), "Analysis of hardware support for cryptography in IoT

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2021. No. 4 (18)*

devices", *Ukrainian Scientific Journal of Information Security*, Vol. 24, Issue 1, P. 36–48.
10. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M. (2020), "IoT Privacy and Security: Challenges and Solutions", *Appl. Sci.*, No. 10 (12), P. 17. DOI: 10.3390/app10124102.
11. Asangkhanwa, Y., Ii, R., Syrov, A. (2019), "Improving the security level of the edge nodes of the Internet of things using microchip ATECC608A microcircuits", *Electronics NTB*, No. 7 (00188), P. 60-64. DOI: 10.22184/1992-4178.2019.188. 7.60.64.
12. Shlykov, D. I. (2018), "About the fast implementation of the AES cipher in the Sdicrypt library", *Information systems*, No. 3 (53), P. 34–40.
13. Crinon, G. (2021), "Internet of Things security: existing problems and their solutions", available at: https://controleng.ru/wp-content/uploads/In_08.pdf (last accessed 21.11.2021).
14. Gnusov, Y. B., Klimushin, P. S., Kolisnyk, T. P., Mozhayev, M. O. (2020), "Analysis of microcontroller modeling systems with additional modules of cryptographic information protection", *Bulletin of the National Technical University "KhPI". Series: Systems Analysis, Management and Information Technology: Coll. Science. etc.*, No. 1 (3), P. 79–84. DOI: 10.20998 /2079-0023.2020.01.14.
15. Microchip Technology (2017), "ATECC508A CryptoAuthentication Device Complete Data Sheet", available at: https://seltok.com/ upload/iblock/ 217/2177fef7a5c972d17d5781fce434236b.pdf

Received 30.11.2021

Відомості про авторів / Сведения об авторах / About the Authors

Клімушин Петро Сергійович – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: klimushyn@ukr.net; ORCID: https://orcid.org/0000-0002-1020-9399.

Климушин Петр Сергеевич – кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Petro Klimushyn – Candidate of technical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Соляник Тетяна Миколаївна – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: t.solianyk@khai.edu; ORCID: https://orcid.org/0000-0003-3695-0019.

Соляник Татьяна Николаевна – кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Tetiana Solianyk – Candidate of technical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Можаєв Олександр Олександрович – доктор технічних наук, професор, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: mozhaev1957@gmail.com; ORCID: https://orcid.org/0000-0002-1412-2696.

Можаев Александр Александрович – доктор технических наук, профессор, профессор кафедры кибербезопасности и DATA-технологий, Харьков, Украина.

Oleksandr Mozhaev – Doctor of technical science, professor, professor of Cyber Security and DATA-Technologies Department, Kharkiv, Ukraine.

Носов Віталій Вікторович – кандидат технічних наук, доцент, професор кафедри и протидії кіберзлочинності, Харків, Україна; e-mail: vitnos.g@gmail.com; ORCID: https://orcid.org/0000-0002-7848-6448.

Носов Виталий Викторович – кандидат технических наук, доцент, профессор кафедры и противодействия киберпреступности, Харьков, Украина.

Vitalii Nosov - Candidate of technical science, associate professor, professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Колісник Тетяна Петрівна – кандидат педагогічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: ktp201505@gmail.com; ORCID: https://orcid.org/0000-0002-7442-8136.

Колесник Татьяна Петровна – кандидат педагогических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Tetiana Kolisnyk – Candidate of pedagogical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Янов Василь Вікторович – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: vasiliyyanov@gmail.com; ORCID: https://orcid.org/0000-0002-0696-7728.

Янов Василий Викторович - кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Vasily Yanov – Candidate of technical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

АПАРАТНА ПІДТРИМКА ПРОЦЕДУР АСИМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ІНТЕРНЕТ РЕЧЕЙ

Предмет дослідження: процедури асиметричної автентифікації вузлів інтернет речей для забезпечення найвищого рівня безпеки з використанням криптографічних мікросхем. **Метою** статті є дослідження способів потенційного застосування криптографічних мікросхем для забезпечення безпечної автентентифікації вузлів інтернет речей з використанням процедур

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2021. № 4 (18) ISSN 2524-2296 (online)

асиметричної криптографії. У статті вирішуються наступні **завдання**: аналіз апаратних засобів підтримки технологій асиметричної криптографії інтернет речей; визначення безпечних процедур асиметричної автентифікації вузлів інтернет речей та їх складових елементів: створення сертифікатів, верифікація відкритих та закритих ключів. **Методи** дослідження: метод структурно-функціонального аналізу і проектування складних систем, методи ідентифікації та автентифікації інформаційних об'єктів, криптографічні методи захисту інформації, методи аналізу безпеки розподілених інформаційних систем. **Новизною** проведеного дослідження є аналіз апаратних засобів підтримки технологій асиметричної криптографії інтернет речей з допомогою криптографічних мікросхем та визначення структурно-функціональних схем для реалізації процедур асиметричної автентифікації вузлів інтернет речей. Відмінними характеристиками наданих схем та процедур асиметричної автентифікації є: забезпечення підвищеного рівня інформаційної безпеки за рахунок захищеного зберігання криптографічних ключів, цифрових підписів, сертифікатів, конфіденційних даних в захищеному від зовнішніх атак апаратному оточенні та не потрібності зберігання закритих ключів клієнтів на стороні хоста. **Результатами** роботи є процедури та схеми застосування криптомікросхем асиметричної автентифікації для забезпечення захисту вузлів інтернет речей. Аналіз функціонування представлених схем дозволив сформувати наступні **висновки**. Запропоновані структурно-функціональні схеми для реалізації процедур асиметричної автентифікації вузлів інтернет речей з використанням криптографічних мікросхем надають користувачеві легку можливість реалізувати криптографію без експертних знань в цій галузі. У цих мікросхемах застосовується апаратний блок обчислення і перевірки цифрового підпису ECDSA з перевагами криптографії на еліптичних кривих, як перевірений і надійний алгоритм автентифікації, та блок генерування сеансових ключів симетричного шифрування ECDH. Надані схеми та процедури підтримують три складові інформаційної безпеки, а саме: конфіденційність, цілісність та автентичність даних. Приклади потенційних застосувань наданих схем та процедур можуть бути реалізовані за допомогою будь-якої мікросхеми асиметричної автентифікації, але їх рекомендується застосовувати для генерації сеансових ключів шифрування і там, де для перевірки даних і коду на цілісність і автентичність потрібні цифрові підписи.

Ключові слова: інтернет речі; асиметрична автентифікація; алгоритми шифрування; криптографічні ключі; електронні сертифікати; цифрові підписи; криптографічні мікросхеми.

АППАРАТНАЯ ПОДДЕРЖКА ПРОЦЕДУР АСИММЕТРИЧНОЙ АУТЕНТИФИКАЦИИ ИНТЕРНЕТ ВЕЩЕЙ

Предмет исследования: процедуры ассиметричной аутентификации узлов интернет вещей для обеспечения высокого уровня безопасности с использованием криптографических микросхем. **Целью** статьи является исследование способов потенциального применения криптографических микросхем для обеспечения безопасной аутентификации узлов интернет вещей с использованием процедур асимметричной криптографии. В статье решаются следующие задачи: анализ аппаратных средств поддержки технологий асимметричной криптографии веб вещей; определение безопасных процедур ассиметричной аутентификации узлов интернет вещей и их составляющих элементов: создание сертификатов, верификация открытых и закрытых ключей. **Методы** исследования: метод структурно-функционального анализа и проектирования сложных систем, методы идентификации и аутентификации информационных объектов, криптографические методы защиты информации, методы анализа безопасности распределенных информационных систем. **Новизной** проведенного исследования является анализ аппаратных средств поддержки технологий асимметричной криптографии интернет вещей с использованием криптографических микросхем и определения структурно-функциональных схем для реализации процедур асимметричной аутентификации узлов интернет вещей. Отличительными характеристиками схем и процедур асимметричной аутентификации являются: обеспечение повышенного уровня информационной безопасности за счет защищенного хранения криптографических ключей, цифровых подписей, сертификатов, конфиденциальных данных в защищенном от внешних атак аппаратном окружении и не потребность хранения закрытых ключей клиентов на стороне хоста. **Результаты** работы: процедуры и схемы применения крипто микросхем асимметричной аутентификации для обеспечения защиты узлов интернет вещей. Анализ функционирования представленных схем позволил сформировать следующие **выводы.** Предложенные структурно-функциональные схемы для реализации процедур асимметричной аутентификации узлов интернет-речей с использованием криптографических микросхем предоставляют пользователю легкую возможность реализовать криптографию без экспертных знаний в этой области. В этих микросхемах применяется аппаратный блок вычисления и проверки цифровой подписи ECDSA с преимуществами криптографии на эллиптических кривых, как проверенный и надежный алгоритм аутентификации, и блок генерирования сеансовых ключей симметричного шифрования ECDH. Указанные схемы и процедуры поддерживают три составляющие информационной безопасности, а именно: конфиденциальность, целостность и аутентичность данных. Примеры потенциальных применений схем и процедур могут быть реализованы с помощью любой микросхемы асимметричной аутентификации, но их рекомендуется применять для генерации сеансовых ключей шифрования и там, где для проверки данных и кода на целостность и аутентичность нужны цифровые подписи.

Ключевые слова: интернет вещи; асимметричная аутентификация; алгоритмы шифрования; криптографические ключи; электронные сертификаты; цифровые подписи; криптографические микросхемы.

Бібліографічні описи / Bibliographic descriptions

Клімушин П. С., Соляник Т. М., Можаєв О. О., Носов В. В., Колісник Т. П., Янов В. В. Апаратна підтримка процедур асиметричної автентифікації інтернет речей. *Сучасний стан наукових досліджень та технологій в промисловості*. 2021. № 4 (18). С. 31–39. DOI: https://doi.org/10.30837/ITSSI.2021.18.031

Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov V. (2021), "Hardware support procedures for asymmetric authentication of the internet of things", *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (18), P. 31–39. DOI: https://doi.org/10.30837/ITSSI.2021.18.031