DOI: https://doi.org/10.36910/4293-52779-2025-17-02-09
UDC 004.896 (075.8)

[1] Krestyanpol, L.
PhD, Associate Professor
ORCID: 0000-0003-3617-7900
[1] Cheb, D.
student
[2] Kaidyk, O.
PhD, Associate Professor
ORCID: 0000-0002-3620-270X

[1] Lesya Ukrainka Volyn National University / Ukraine
[2] Lutsk NationalTechnical University / Ukraine

CHALLENGES AND ISSUES IN THE USE OF CERTIFICATE FORMATS IN MODERN INFORMATION SYSTEMS: PATHWAYS TO ENHANCING CYBERSECURITY

Abstract: *This article provides an overview of the main digital certificate data formats used to ensure information security and authentication in computer networks. In particular, it examines the most common formats – X.509, PGP, OpenPGP, PKCS – their structure, areas of application, advantages, and disadvantages. The study analyzes how different formats affect compatibility between software tools and presents examples of each format's use in modern security systems. The material may be useful for cybersecurity professionals, system administrators, and software developers working with certificates.*

Keywords**:** *digital certificate, data formats, information security, authentication, cryptography.*

INTRODUCTION, PROBLEM STATEMENT

In today's interconnected digital world, ensuring the security of data and communication is of paramount importance. One of the key elements of modern cybersecurity infrastructures is the use of certificates, which are employed to authenticate users, devices, and services across various networks. Certificates, particularly in the context of public key infrastructure (PKI), provide a critical layer of trust, enabling encrypted communications, secure transactions, and the verification of identity.

These certificates are implemented in various formats, each serving specific purposes and requirements. Among the most common formats are X.509, PGP, OpenPGP, and PKCS, each with its own advantages, limitations, and areas of application. While these formats play a crucial role in ensuring digital security, they also pose challenges for integration, management, and scalability in modern IT environments.

Problem Statement. Despite the widespread adoption of certificate-based security mechanisms, organizations face significant challenges in managing and implementing different certificate formats effectively. Issues such as incompatibilities between systems, the complexity of certificate life cycle

management, difficulties in verifying certificate authenticity, and security risks related to key storage pose substantial obstacles for security administrators. Moreover, the increasing demand for scalability in diverse environments, such as the Internet of Things (IoT) and mobile devices, adds further complexity to the adoption and management of certificates.

Furthermore, with the advent of quantum computing and the evolving threat landscape, the current certificate formats may not be sufficiently resilient to emerging threats, necessitating the development of new standards. In light of these challenges, it is crucial to explore solutions to streamline certificate management processes, enhance compatibility across different platforms, and ensure that the integrity of certificate-based security is maintained.

MAIN ARTICLE

Overview of the Main Certificate Data Formats (X.509, PGP, OpenPGP, PKCS, and Others).

Certificates are a key element of modern security infrastructure. They are used to verify the authenticity of users, servers, and devices in networks and electronic communications. Different certificate formats have their own specific features, standards, and areas of application. Among the most common are X.509, PGP, OpenPGP, PKCS, and others. This section explores their characteristics, advantages, and disadvantages.

The X.509 format is the most widely used certificate standard within the context of Public Key Infrastructure (PKI). It is defined by ITU-T recommendations and is utilized in many protocols, including SSL/TLS, HTTPS, and S/MIME. An X.509 certificate contains information about the public key, the subject's name, the serial number, the validity period, and the digital signature of the certificate authority (CA). The X.509 structure is strictly formalized and based on ASN.1 and DER encoding format.

One of the main advantages of X.509 is its support in most modern systems and software. However, due to its complex structure and centralized trust model, this format has several drawbacks. In particular, certificate chain verification can be challenging, and managing trusted certificate authorities requires significant resources. Despite these limitations, X.509 remains the de facto standard for secure communication on the Internet [1].

PGP (Pretty Good Privacy) is a cryptographic system that ensures data confidentiality and authenticity, especially in the field of email communication. PGP certificates implement the "web of trust" concept, as opposed to the centralized PKI model. In this system, users sign each other’s keys to indicate that they trust their authenticity. This creates a decentralized and flexible structure for interaction.

The main advantage of PGP is its decentralized approach to trust management. Each user independently decides whom to trust and can build their own trust networks. However, such flexibility often complicates automatic certificate verification, especially in corporate environments. Additionally, the interface and logic of PGP can appear complex to beginners [2, 3].

OpenPGP is an open standard based on PGP, defined in RFC 4880. It includes specifications for symmetric and asymmetric encryption, digital signatures, and key

management. OpenPGP supports many cryptographic algorithms, such as RSA, ElGamal, DSA, and others, making it highly flexible. Due to its open specification, there is a wide range of compatible software, such as GnuPG.

The use of OpenPGP is widespread among privacy-focused communities, as well as among journalists, activists, and IT professionals. The standard allows the creation of key pairs with long validity periods and supports the association of multiple identifiers with a single key. A drawback, similar to that of PGP, is the complexity of building and verifying trust chains in large-scale systems [4].

PKCS (Public-Key Cryptography Standards) is a set of standards developed by RSA Security to ensure the interoperability of cryptographic systems. Specifically, the PKCS#7 format (also known as CMS – Cryptographic Message Syntax) is commonly used to store signed and encrypted messages. PKCS#12 is designed to store private keys, certificates, and associated chains in a secure container.

Unlike X.509, PKCS formats are not only focused on certificate structure but also on key and message management. They are supported by most cryptographic libraries, such as OpenSSL, Windows Crypto API, and others. An important feature is the ability to store multiple certificates and keys in a single file, which is convenient for real-world deployment.

In article [5] discusses the challenges of cybersecurity certification for software. The authors address the importance of integrating security into the software development process and ensuring reliable certification for programs used in critical infrastructures. The study explores the difficulty of maintaining software security in an environment of rapidly evolving cyber threats.

The article [6] is a systematic literature review that analyzes the benefits and challenges of information security certification. The article evaluates different methods and approaches to certification in the context of managing the security of information systems, particularly in business environments. It discusses the challenges of implementing certification processes, their impact on organizational strategies, and the advantages of certification in enhancing trust and system security.

Other formats worth mentioning include PEM (Privacy Enhanced Mail), DER (Distinguished Encoding Rules), CER, and CRT. PEM and DER are used for encoding X.509 certificates. PEM is a text-based format that contains base64-encoded data with appropriate headers, while DER is binary. CER and CRT are simply alternative file extensions for X.509 certificates, which may be encoded in either DER or PEM format.

The significance of different certificate formats lies in their compatibility with software and protocols. For example, web browsers and servers support X.509 in PEM and DER formats, while email clients may work with PGP and OpenPGP. Many libraries allow conversion between formats, but understanding each format's specifics is important for maintaining security.

The certificate infrastructure is constantly evolving. With the advent of quantum computing, new cryptographic approaches are needed, which will also affect certificate formats. Active research in post-quantum cryptography is already laying the groundwork for future standards.

In conclusion, the choice of certificate format depends on the specific task, required level of security, software compatibility, and administrative convenience. In some cases, combining different formats and systems is advisable to achieve an optimal balance between security, flexibility, and scalability.

Challenges and Issues Related to the Use of Certificate Formats in Modern Information Systems.

In modern information systems, certificates play a critical role in ensuring authentication, confidentiality, and data integrity. However, despite their widespread use, certificate formats present a number of issues that complicate their implementation and maintenance. These challenges involve not only technical aspects but also organizational, legal, and human factors, creating a complex and dynamic landscape.

One of the main problems is the complexity of formats and the lack of standardization. For instance, even within the X.509 standard, different encoding methods (PEM, DER) can lead to incompatibility between systems. Additionally, some formats, such as PKCS#12, have limited support in certain environments, particularly open platforms. This creates difficulties for developers and administrators who are forced to work with multiple tools and formats simultaneously.

Another serious issue is the management of the certificate lifecycle. This includes certificate creation, distribution, renewal, and revocation. In large organizations, this can be especially challenging due to the high number of devices and users. If a certificate is not renewed or revoked in time, it can cause service disruptions or significant security breaches.

The complexity of certificate validation is also a challenge. In the case of X.509, for example, the entire trust chain must be verified, including intermediate and root certificate authorities. If an intermediate certificate is missing or misconfigured, validation can fail. This often occurs even in commercial solutions, especially during automatic certificate renewals.

Challenges also arise in managing revoked certificates. Although mechanisms such as Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP) exist, they have limitations. For example, large CRLs can slow down validation, and OCSP servers may be unavailable, preventing real-time verification. This creates opportunities for man-in-the-middle attacks [7].

A significant problem is the security of private key storage. In formats such as PKCS#12, the private key and certificate are stored together, and if user or server files are not adequately protected, unauthorized key usage is possible. This is particularly relevant for mobile devices or poorly secured workstations.

Certificate formats often do not take into account the needs of emerging technologies, such as the Internet of Things (IoT). IoT devices have limited resources, and standard X.509 certificates may be too large for efficient use. This creates a demand for lighter, optimized formats, which have not yet become widely adopted, delaying the deployment of certificate-based security in such environments.

Another critical aspect is the human factor. In many cases, users do not understand the importance of certificates and may, for instance, ignore browser

warnings about invalid certificates. This makes even the most robust certification systems vulnerable to simple social engineering attacks. The need for education and improved digital literacy is becoming increasingly urgent.

Compatibility issues between different systems also remain pressing. For example, certificates generated in one system may not be supported in another due to differences in supported algorithms or formats. This is particularly relevant to interoperability between Windows and Linux, or between different implementations such as OpenSSL, GnuTLS, and others.

Legal aspects also complicate the use of certificates. Different countries have varying requirements for electronic signatures, trust in certification authorities, and the storage of cryptographic materials. For instance, some government services only recognize certificates issued by nationally accredited authorities, limiting the use of international solutions [8].

The introduction of certificate management automation, such as Let's Encrypt, mitigates some problems but introduces new risks. For example, malicious actors can automatically obtain certificates for phishing websites, reducing the effectiveness of a trust model based solely on certificate presence.

Another issue is the limited flexibility when changing encryption algorithms. For example, transitioning from SHA-1 to SHA-256 or from RSA to ECC requires updating certificates, verifying compatibility, and reconfiguring systems. In large-scale infrastructures, this can be a costly and risky process that takes significant time.

Finally, the emergence of quantum computing poses a threat to the integrity of current cryptographic algorithms. Most existing certificate formats are not designed to withstand quantum attacks. Therefore, preparations for a transition period and the development of new, quantum-resistant certificate formats are already necessary to face future threats.

RECOMMENDATIONS FOR IMPROVING THE USE OF CERTIFICATE DATA FORMATS IN CYBERSECURITY SYSTEMS

Centralized certificate management is a crucial aspect of ensuring security within organizations, especially in the face of modern cyber threats. The implementation of a Public Key Infrastructure (PKI) allows for the control of certificate issuance, renewal, and revocation processes, which, in turn, reduces the risk of certificate compromise and enhances overall security. It is essential for organizations to have a clear understanding of how certificates are used within their infrastructure and to ensure proper oversight of these processes. This includes not only technical aspects but also management practices that help maintain the integrity of the system.

1. Automating certificate-related management processes can significantly reduce the likelihood of human errors. Using specialized tools to automate certificate issuance, renewal, and revocation not only simplifies these tasks but also enhances the efficiency of the security team. This allows them to focus on more critical aspects of security, rather than routine operations. For instance, automated systems can provide timely reminders about certificate expiration dates, helping to avoid situations where certificates expire without proper renewal.

2. Regular auditing and monitoring of certificate status are critical for detecting potential threats. Implementing monitoring systems allows for timely responses to changes in certificate status, which can prevent possible attacks. This process also contributes to the creation of a transparent certificate management system, where all changes are documented and analyzed. For example, maintaining a change log can help detect anomalies in certificate usage and take prompt action to address them.

3. Training employees on certificate management increases awareness of security importance. Organizing regular training helps employees understand how to properly use certificates and avoid mistakes. This promotes the development of a security culture within the organization, where each employee is aware of their role in protecting information. Additionally, training can include incident response scenarios, enabling employees to act quickly in the event of a threat.

4. Ensuring integration between different certificate formats enhances system flexibility. This allows organizations to use various technologies without the need to redesign all processes. For example, organizations can integrate new solutions without disrupting existing systems, simplifying the implementation of new technologies.

5. It is also important to adapt certificate formats to the specific needs of various sectors. This will help use these technologies more effectively in different industries, such as finance, healthcare, or the public sector, where security requirements may significantly differ. Developing action plans for certificate compromise scenarios is an essential part of the cybersecurity strategy. Incident response mechanisms must be clearly defined and regularly tested to ensure their effectiveness in the event of a threat.

6. Collaboration with cybersecurity experts and solution providers enables the exchange of experience and the implementation of best practices. This can significantly enhance the level of protection within the organization. For instance, engaging third-party consultants can help conduct an independent audit of the certificate management system and identify weaknesses.

CONCLUSIONS

Certificate data formats are critical elements of modern cybersecurity, ensuring authentication, confidentiality, and data integrity in various information systems. An overview of the main formats, such as X.509, PGP, OpenPGP, PKCS, and others, reveals their diversity and specific uses across different fields. Each format has its own advantages and disadvantages, determining the choice based on specific needs and requirements.

However, several issues and challenges arise when organizations use certificates. These include the complexity of certificate management, compatibility issues between different systems, the security of private key storage, and the need to adapt certificates to new technologies like IoT or quantum computing. Addressing these aspects is crucial for maintaining a stable and secure infrastructure.

Recommendations for improving certificate usage, including centralized management, process automation, regular auditing and monitoring, employee

training, and ensuring integration between different formats, can significantly enhance security within organizations. Additionally, adapting certificates to the specific needs of different industries and collaborating with cybersecurity experts to refine certificate management practices is essential.

Thus, proper implementation and management of certificates are key to ensuring a high level of protection in information systems, minimizing risks, and guaranteeing reliable communications in the digital environment.

REFERENCES

[1] Soiko, O. (2009). Protective features of passport documents and possible methods of their forgery (Textbook). International Center for Migration Policy Development.

[2] Milánkovich, Á., & Tuma, K. (2023). Delta security certification for software supply chains. IEEE Security & Privacy, 21(6), 24-33.

[3] Nikolskaia, K. Y. (2021). Analysis of the system of legal means of licensing and certification in the field of cybersecurity. In 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 90-93).

[4] Elmasri, R., & Navathe, S. (2021). Fundamentals of database systems. Pearson.

[5] Hernandez-Ramos, J. L., Matheu, S. N., & Skarmeta, A. (2021). The challenges of software cybersecurity certification [Building security in]. IEEE Security & Privacy, 19(1), 99-102. https://doi.org/10.1109/MSEC.2020.3037845.

[6] Hulshof, M., & Daneva, M. (2021). Benefits and challenges in information security certification – A systematic literature review. In B. Shishkov (Ed.), Business Modeling and Software Design (pp. 107-121). Lecture Notes in Business Information Processing, vol 422. Springer. https://doi.org/10.1007/978-3-030-79976-2_9.

[7] Pocheptsov, H. H., & Chukut, S. A. (2018). Information policy. Knowledge Publishing House.

[8] Kukarin, O. B. (2019). Electronic document management and information protection: A textbook. National Academy of Public Administration under the President of Ukraine. Retrieved from http://academy.gov.ua/infpol/pages/dop/2/files/dcc74a43-a939-4314-8f50-f6b1e80cf498.pdf (Accessed: April 6, 2025).

ПРОБЛЕМИ ТА ВИКЛИКИ ВИКОРИСТАННЯ ФОРМАТІВ СЕРТИФІКАТІВ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: ШЛЯХИ ДО ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ

[1]Крестьянполь Л. Ю. *Канд. тех. наук, доцент*
[1]Чеб Д.О. *Здобувач освіти*
[2]Кайдик О. Л. *Канд. тех. наук, доцент*
[1]Волинський національний університет імені Лесі Українки / Україна
[2]Луцький національний технічний університет / Україна

Анотація: у цій статті наведено огляд основних форматів даних цифрових сертифікатів (X.509, PGP, OpenPGP, PKCS тощо), які використовуються для забезпечення інформаційної безпеки та автентифікації в комп'ютерних мережах. Зокрема, розглядаються їх структура, сфери застосування, переваги та недоліки. У дослідженні аналізуються ключові виклики та проблеми, пов'язані з використанням сертифікатів у сучасних інформаційних системах. Серед них: складність керування життєвим циклом сертифікатів, питання сумісності між різними системами та форматами кодування (PEM, DER), безпека зберігання приватних ключів, а також необхідність адаптації форматів до потреб Інтернету речей (IoT) та постквантової криптографії. На підставі цього, в статті надано практичні рекомендації для вдосконалення процесів використання сертифікатів у системах кібербезпеки (централізоване керування, автоматизація процесів, регулярний аудит та навчання персоналу). Матеріал може бути корисним для фахівців з кібербезпеки, системних адміністраторів та розробників програмного забезпечення, які працюють із сертифікатами та прагнуть мінімізувати ризики, пов'язані з їхнім неправильним впровадженням та експлуатацією..

Ключові слова: цифровий сертифікат, формати даних, інформаційна безпека, автентифікація, криптографія.

Дата першого надходження статті до видання	Дата прийняття статті до друку статті після рецензування	Дата оприлюднення
27.10.2025 р.	18.11.2025 р.	23.12.2025 р.