DOI 10.20535/2411-1031.2023.11.2.293496
UDC 621.391.3

OLEKSANDR DULIA,
DMYTRO MINOCHKIN

AN EXPLORATION OF PUBLIC KEY INFRASTRUCTURE APPLICATIONS ACROSS DIVERSE DOMAINS: A COMPARATIVE ANALYSIS

This article delves into the vital role of Public Key Infrastructure (PKI) in securing and authenticating communications across a multitude of fields. PKI has evolved from a mere technical concept into a cornerstone of secure digital communications, playing a central role in various domains such as web security, healthcare, finance, the Internet of Things (IoT), and government services. PKI employs cryptographic techniques and digital certificates to establish trust, ensure data integrity, and enable secure communications, thus acting as the backbone of digital security.

In the wake of the digital revolution, the demand for reliable and robust security solutions has skyrocketed. The diversity and scale of modern digital platforms necessitate adaptable security solutions, a challenge which PKI tackles through its flexible implementation. Despite sharing core principles, the implementation of PKI demonstrates divergences influenced by factors such as scale, complexity, resource constraints, regulatory environments, and trust models.

This article offers an extensive comparison of PKI's utilization across various domains, highlighting the commonalities and divergences. It explores how PKI is tailored to meet the unique requirements and challenges of each sector and discusses the certificate lifecycle management in varying contexts. Moreover, it provides an analysis of the current state of PKI applications and challenges, offering insights into the evolving landscape of threats and technologies.

Not only does the article address the current state of PKI, but it also presents a forward-looking perspective on its potential future developments. As the digital landscape continues to evolve and expand, it is crucial to anticipate the emerging challenges and devise strategies for proactive adaptation. This article thus serves as a comprehensive resource for understanding the role and impact of PKI in the contemporary digital infrastructure.

Ultimately, the article seeks to underline the importance of PKI and highlight the need for continued research and development in this area. As our reliance on digital communications and transactions continues to grow, the role of PKI in safeguarding these interactions becomes increasingly significant. This comprehensive review serves as a valuable resource for researchers, practitioners, and policymakers in understanding the diverse applications of PKI and its critical role in securing the digital world.

Keywords: Public Key Infrastructure, Digital Certificates, Web Security, Internet of Things, Authentication, Encryption.

Introduction. In the rapidly evolving landscape of our interconnected world, the demand for secure communication and robust data protection reverberates across diverse sectors. Central to meeting this demand is Public Key Infrastructure (PKI), a sophisticated amalgamation of hardware, software, policies, and standards that plays a pivotal role in ensuring secure and authenticated communication between entities over digital networks [1]. As our digital environment continues to diversify, PKI has emerged as a linchpin, finding applications in fields ranging from web security and healthcare to finance, Internet of Things (IoT), and government services. Leveraging cryptographic techniques and the interaction between public and private keys, PKI ensures the security of communications, authenticates users and devices, and upholds non-repudiation and data integrity through digital signatures.

© O. Dulia, D. Minochkin, 2023

The implementation of PKI across these diverse domains gains prominence in the context of the global shift towards digitalization. For instance, the surge in the number of internet-connected devices through IoT technologies necessitates security solutions that are not only scalable but also robust. PKI, thus, stands out as a widely accepted solution addressing these evolving needs [2]. Similarly, the healthcare sector grapples with ensuring the confidentiality and integrity of Electronic Health Records (EHRs), making PKI a central component in safeguarding sensitive patient data [3].

Yet, while PKI operates on a standardized set of core principles, its application diverges significantly based on the unique requirements and constraints of different fields. Variables such as scale, complexity, regulatory environments, resource constraints, and trust models introduce variability in how PKI is implemented across domains.

This article, thus, seeks to offer a comprehensive exploration of the intricate applications of Public Key Infrastructure across diverse fields. By probing into both the commonalities and distinctions in its implementation, the objective is to provide insights into the challenges and future trajectories of PKI technology. As we navigate the complexities of secure digital communication, this nuanced understanding becomes instrumental in addressing the multifaceted demands of our interconnected and digitally driven era.

Formation of the problem. In the intricate landscape of our digitally interwoven world, the imperative to customize the application of Public Key Infrastructure (PKI) in response to varied security requirements across domains is undeniably complex. This crucial customization, while vital, has engendered a significant degree of fragmentation and intricacy within PKI implementations. As we traverse the dynamic arenas of web security, healthcare, finance, IoT, and government services, the multifaceted nature of securing these diverse environments necessitates a profound exploration. The challenges embedded within each domain, each presenting unique intricacies, beckon us to undertake a comprehensive inquiry into how PKI dynamically adapts to meet the evolving demands of security. Within this exploration, a cascade of questions unfolds, reaching beyond the surface to probe the practical ramifications of integrating diverse PKI implementations, the potential impediments to seamless interoperability, and the delicate equilibrium between customization and the nuanced shifts within the security landscape. This multifaceted perspective encourages an in-depth examination, urging us to understand the intricate dance between tailored applications of PKI and the evolving nuances of digital security.

Analysis of previous studies. Public Key Infrastructure (PKI) is a vital cornerstone for securing communications and verifying identities over networks. With an increasing emphasis on cybersecurity, PKI finds applications across diverse domains such as web security, healthcare, finance, the Internet of Things (IoT), and government services. This review collates and analyzes a wide range of scholarly works and industry reports to highlight the application, commonalities, divergences, and challenges associated with PKI in these fields.

*Web Security***.** Web security is one of the primary areas where PKI plays a central role. Rescorla examines the development of the TLS protocol and the importance of PKI in securing server-client communications [4]. Dierks & Rescorla explore the mechanics of the TLS protocol and how PKI ensures authentication, data integrity, and confidentiality [5]. Ray discusses modern developments in PKI for web security, highlighting certificate pinning and enhanced validation techniques [6].

Healthcare. In healthcare, PKI is crucial for protecting patient data and ensuring secure communications among healthcare systems. Gajanayake et al. offer an extensive analysis of the utilization of PKI for securing Electronic Health Records (EHR) [7]. Mense et al. discuss challenges such as scalability and interoperability in implementing PKI in healthcare systems [8]. Fernandez-Aleman et al. add to this by evaluating the security and privacy concerns related to EHR systems and emphasizing the importance of PKI [9].

Finance. Alkhateeb and Mahmood [10] discuss PKI's role in financial transactions and user authentication. They particularly highlight 3-D Secure technology. Stallings provides a comprehensive analysis of PKI in finance, emphasizing digital certificate management and integration with existing systems [10]. Kundi et al. evaluate the challenges and requirements of deploying PKI in mobile banking, providing insights into the complex security demands in modern financial systems [11].

Internet of Things (IoT). Sicari et al. provide an overview of PKI applications in IoT, focusing on device authentication and secure communications [12]. Lee & Lee present a business perspective on IoT, discussing investment trends and challenges in integrating PKI [13]. Heer et al. analyze the security challenges in IoT and how PKI can be adapted for resource-constrained environments [14].

Government Services. The United States Government report provides insights into how Federal PKI secures communications and verifies identities across government agencies [15]. Kapadia discusses the policies, costs, and complexities involved in large-scale PKI implementation in government services [16]. Adams & Lloyd delve into the foundational concepts and deployment considerations for PKI, which is especially relevant for government implementations [17]. Misra et al. [18] present a global perspective, evaluating PKI deployment in e-governance systems in different countries and the challenges therein.

PKI, with its paramount role in securing communications and authenticating entities, stands as an indispensable framework cutting across an array of domains. While the fundamental principles of PKI provide a solid foundation, its implementation nuances, and challenges exhibit domain-specific characteristics. For instance, in the realm of web security, a perpetual emphasis on the continual strengthening of protocols is crucial to keep pace with ever-evolving cyber threats. In healthcare, the focal point shifts towards the safeguarding of patient data, necessitating not only encryption but also meticulous access controls and privacy measures. In the financial domain, where secure transactions and user authentication are paramount, PKI plays a pivotal role in ensuring the integrity and confidentiality of sensitive financial data. In the IoT landscape, the adaptation of PKI to resource-constrained environments is central, requiring lightweight cryptographic solutions and efficient key management. Meanwhile, in government services, large-scale deployment and meticulous policy formation become significant aspects, demanding a careful orchestration of PKI to meet the diverse needs of a broad citizen base.

While the literature underscores the importance of continued innovation and adaptation in PKI systems to tackle evolving security challenges and complexities, future research holds the promise of further advancing this dynamic field. A pivotal avenue for exploration lies in the creation of adaptive and scalable PKI systems that can flexibly cater to the specific needs and challenges inherent in different domains. This adaptive quality becomes increasingly essential as digital landscapes continue to evolve, presenting unique security challenges that demand tailored solutions. Additionally, delving into the intricate interplay between PKI and emerging technologies, such as blockchain, could prove pivotal in the development of more robust and resilient security solutions. Understanding how these technologies complement and enhance each other could pave the way for innovative approaches to address the ever-expanding threat landscape. In essence, the future trajectory of PKI research and implementation hinges on its ability to not only adapt but also synergize with emerging technologies to fortify digital security across diverse domains.

Main part. The applications of Public Key Infrastructure (PKI) traverse a vast spectrum, showcasing versatile implementations across various domains. While the core principles of authentication, encryption, and digital signatures form the bedrock of PKI, the intricacies of its use-cases, scale, and deployment requirements diverge significantly among sectors.

Looking ahead, the evolution of PKI will likely continue along divergent paths as each domain grapples with its distinct challenges. Future developments may include more specialized PKI solutions, enhanced interoperability measures, and a deeper integration with emerging technologies to fortify digital security in an ever-evolving landscape. In essence, the exploration of PKI applications underscores its versatility and the imperative of adapting to the nuanced demands of diverse sectors in the digital era (Table 1).

Table 1 – Overview of PKI Applications in Different Fields

Field	Application of PKI	Key Features	Unique Considerations
Web Security	Secure communication through SSL/TLS; Code Signing	Authentication, Encryption	Reliance on public CAs; Wide range of end-users
Healthcare	Secure Electronic Health Records (EHRs); Medical devices communication	Data Integrity, Authentication, Encryption	Strict compliance with healthcare regulations; Patient data privacy
Finance	Secure online transactions; Digital signatures for contracts	Non-repudiation, Authentication, Encryption	Rigorous security standards for financial data; Legal compliance
IoT	Secure communication between devices; Device identity verification	Lightweight cryptography, Authentication	Scalability, resource constraints; Diverse types of devices
Government Services	Secure government digital services; Electronic IDs	Digital signatures, Authentication, Encryption	Use of private CAs; Legal compliance; Citizen data protection

Web Security. In the realm of web security, PKI is foundational for establishing secure communication channels. Protocols like HTTPS rely on PKI to encrypt data transmission, prevent man-in-the-middle attacks, and secure online transactions. Certificate management poses a challenge, and the impact of emerging technologies on PKI in web security is substantial. Despite challenges, PKI remains integral to fortifying web security, ensuring the confidentiality and integrity of data exchanged over the internet. Its role in user authentication and trust establishment is paramount in the evolving landscape of cybersecurity. In addition to securing communications with SSL/TLS, PKI is also used for code signing, where developers sign their code with a digital signature, ensuring that the software hasn’t been tampered with since its publication. This is particularly important for ensuring the integrity of software downloads and updates.

Healthcare. In healthcare, where the sensitivity and confidentiality of patient data are paramount, PKI serves as a linchpin for secure communication and data integrity. EHRs and medical information exchange between healthcare professionals necessitate a robust security framework. PKI not only encrypts communication channels, safeguarding against unauthorized access but also ensures the authenticity of users and devices within the healthcare ecosystem. The unique challenges within this domain, such as the constant need for real-time access, the growing number of connected medical devices, and compliance with stringent healthcare regulations, make the application of PKI particularly intricate. Nevertheless, its implementation in healthcare remains crucial to maintaining the trust and privacy of patient information in an increasingly interconnected digital healthcare landscape. Besides securing EHRs, PKI is also crucial for secure communications among medical devices, such as heart rate monitors or insulin pumps, and ensures the confidentiality and integrity of the data being transmitted.

Finance. In the fast-paced world of finance, where online transactions occur at lightning speed and vast amounts of sensitive data are exchanged, PKI plays a pivotal role in fortifying security measures. From online banking to payment gateways, PKI ensures the confidentiality and integrity of financial transactions. The authentication of users and the verification of digital signatures become critical components in thwarting fraudulent activities. Despite the finance sector's inclination towards innovation and rapid technology adoption, the challenges associated with PKI implementation are evident. Balancing the need for stringent security measures with the demand for seamless user experiences and scalability requires a delicate approach. PKI, nevertheless, remains indispensable in mitigating cyber threats and ensuring the resilience of financial systems in the digital era. PKI is also employed for securing contractual communications through digital signatures, which guarantees the integrity and non-repudiation of contracts in digital form.

Internet of Things (IoT). IoT has witnessed an explosive growth in interconnected devices, ranging from smart home gadgets to industrial sensors. PKI, in this context, becomes a cornerstone for establishing secure communication channels and safeguarding the integrity of data transmitted between devices. The dynamic nature of IoT networks, coupled with resource constraints in many IoT devices, presents unique challenges for PKI implementation. Scalability is a crucial consideration as the number of connected devices continues to surge. Furthermore, the heterogeneity of IoT ecosystems demands adaptable and lightweight security solutions. PKI, by providing a framework for device authentication and secure data exchange, addresses these challenges, ensuring the trustworthiness of IoT deployments across various industries. PKI is also involved in the secure onboarding of devices onto the network. This process involves authenticating and adding new devices in a secure manner to prevent unauthorized devices from joining the network.

Government Services. Governments worldwide leverage PKI to secure digital identities, authenticate users, and protect sensitive information in their online services. From e-Government initiatives to secure communication among government agencies, PKI ensures the confidentiality and integrity of digital transactions. The issuance of digital certificates plays a vital role in establishing the trustworthiness of individuals and entities engaging with government services. However, the government sector faces unique challenges, such as the need for interoperability among diverse systems, adherence to stringent regulatory standards, and the constant evolution of cybersecurity threats. Despite these challenges, PKI remains an indispensable tool in fortifying the security posture of government services and safeguarding citizen data in the digital age. Government services increasingly employ PKI for electronic IDs which allow citizens to securely access a range of governmental services online.

The implementation of PKI must be tailored to the needs and constraints of the specific field it is being employed in. Understanding these commonalities and divergences is crucial for effective PKI deployment and management. PKI continues to evolve in response to emerging challenges and the changing landscape of digital communications and security. Commonalities and divergences are summarized in table 2.

Table 2 – Commonalities and Divergences in PKI Application Across Fields

Commonalities	**Divergences**
Authentication and Trust Establishment	Scale and Complexity
Data Confidentiality and Integrity	Resource Constraints and Device Heterogeneity
Regulatory Compliance	Real-time Access and Criticality of Operations
Key Management and Certificate Lifecycle	Interoperability and Standardization
Securing Communication Channels	User Authentication Methods

PKI serves as a unifying force across these domains, addressing common challenges and ensuring robust security frameworks. The authentication and trust establishment, data confidentiality and integrity, regulatory compliance, key management, and securing communication channels stand as shared principles, emphasizing PKI's adaptability and effectiveness in safeguarding digital interactions.

Authentication and trust establishment stand as foundational pillars across all domains leveraging PKI. In web security, PKI ensures the verification of users and the establishment of trust between websites and visitors using digital certificates. Similarly, in healthcare, PKI authenticates healthcare professionals accessing electronic health records, fostering trust in the integrity of medical information. The finance sector relies on PKI for user authentication in online banking, enhancing trust in secure financial transactions. In IoT, PKI authenticates devices in interconnected networks, building trust in the communication between smart devices. Government services utilize PKI for the authentication of citizens and entities, establishing trust in digital interactions. In each domain, the commonality lies in PKI's role in robustly authenticating entities and fostering a foundation of trust in digital communications.

The universal imperative of maintaining data confidentiality and integrity is a shared principle addressed by PKI across diverse domains. In web security, PKI encrypts data transmission, safeguarding sensitive information from unauthorized access and ensuring its confidentiality. Similarly, in healthcare, PKI plays a crucial role in encrypting patient data, preserving confidentiality and maintaining the integrity of medical records. Finance relies on PKI to encrypt financial transactions, securing sensitive data and upholding its integrity. In the IoT landscape, PKI encrypts data exchanged between devices, ensuring confidentiality and integrity in the vast network of interconnected devices. Government services utilize PKI to secure digital information, preserving the confidentiality and integrity of citizen data. In essence, PKI's role in ensuring the confidentiality and integrity of data is a unifying factor across these domains, fortifying their digital security landscapes.

Adherence to regulatory standards is a commonality underscoring PKI's application across various domains. In web security, compliance with data protection regulations is paramount, and PKI aids in meeting these standards through secure communication protocols. Healthcare relies on PKI to adhere to stringent healthcare regulations, ensuring the secure handling of patient information. The finance sector navigates financial regulations with the support of PKI in securing transactions. In the IoT landscape, compliance with data privacy regulations is addressed by PKI, contributing to the ethical use of interconnected devices. Government services, subject to diverse regulatory frameworks, benefit from PKI in meeting compliance standards for secure digital interactions. In essence, PKI serves as a common tool in ensuring regulatory compliance across domains, providing a standardized approach to data protection and privacy.

Effective key management and the lifecycle management of digital certificates emerge as shared considerations in PKI implementation. In web security, PKI involves the generation, distribution, and management of cryptographic keys, ensuring the secure exchange of information. Healthcare relies on PKI for the systematic management of keys and certificates to maintain the integrity of medical data. The finance sector navigates the complexities of key management in PKI to secure financial transactions. In the IoT ecosystem, the scalability of key management is crucial for the secure operation of interconnected devices. Government services benefit from PKI's structured approach to key management, ensuring the integrity of digital identities. Across these domains, the common thread lies in PKI's role in effective key and certificate management, contributing to the robustness of digital security infrastructures.

PKI's role in securing communication channels is a unifying factor across diverse domains. In web security, PKI encrypts data transmission, securing communication between users and websites through protocols like HTTPS. Healthcare relies on PKI to secure communication channels between medical professionals, ensuring the confidentiality of patient information. Finance employs PKI to encrypt and secure communication channels in online transactions, safeguarding financial data. In the IoT landscape, PKI establishes secure communication between interconnected devices, mitigating the risk of data breaches. Government services utilize PKI to secure communication channels in various online interactions, enhancing the confidentiality and integrity of digital communications. The commonality lies in PKI's contribution to securing communication channels, fostering a trusted environment for digital interactions across these diverse domains.

The divergences in PKI application across diverse domains underscore the need for nuanced, context-specific approaches. Recognizing the distinct challenges posed by scale, resource constraints, operational criticality, interoperability, and user authentication methods allows for the effective tailoring of PKI solutions to meet the unique demands of each domain.

The scale and complexity of PKI implementation vary significantly across domains, shaping the contours of digital security landscapes. In web security and finance, where large-scale, global networks are prevalent, the demands on PKI scale exponentially. Robust key management, certificate issuance, and revocation processes become intricate endeavors. Conversely, in healthcare, localized networks may not necessitate the same scale, allowing for more focused PKI implementations tailored to specific operational needs. IoT introduces an entirely different dimension, demanding a balance between scalability and resource constraints in interconnected devices. Government services, dealing with diverse systems and services, encounter complexities of interoperability, adding another layer of intricacy. Recognizing and navigating these divergences is crucial for crafting PKI solutions that align with the unique scale and complexity challenges in each domain.

In the realm of IoT, resource constraints in devices and the heterogeneity of the IoT ecosystem introduce divergent challenges. PKI solutions in this domain must be lightweight, adaptable, and cognizant of resource limitations. Balancing the need for robust security with the constraints of IoT devices becomes a delicate act. Conversely, web security and finance sectors, often endowed with more robust computing resources, may implement sophisticated PKI solutions without the same resource constraints. This divergence necessitates tailored approaches in IoT to ensure the efficacy of PKI while accommodating the inherent limitations of interconnected devices.

Divergent operational demands emerge in healthcare, where real-time access to patient data is not just a convenience but a critical necessity. System downtime in healthcare can have life-threatening consequences, demanding a highly available PKI infrastructure. In contrast, web security and finance sectors may prioritize seamless user experiences, where downtime, while impactful, does not carry the same immediate health-related implications. Recognizing the divergent needs for real-time access and the criticality of operations is imperative in crafting PKI solutions that align with the specific demands of each domain.

Government services demand a high degree of interoperability and standardization due to the diverse range of systems and services involved. PKI in this domain must navigate complex ecosystems, ensuring seamless integration across various government functions. In contrast, other domains may have more flexibility in adopting PKI solutions tailored to their specific needs without the same level of interoperability constraints. Recognizing and addressing the divergences in interoperability requirements is vital for effective PKI implementation in the government sector.

Divergent requirements in user authentication methods further distinguish PKI implementation across domains. While the finance sector may employ multifactor authentication for heightened security, healthcare may prioritize methods that ensure convenient yet secure access for medical professionals. Government services might require authentication methods that align with the diverse range of citizens accessing public services. Understanding and accommodating these divergent needs in user authentication methods are essential for crafting PKI solutions that enhance security while aligning with the specific user access requirements in each domain.

Conclusions. Public Key Infrastructure (PKI) emerges as a linchpin in the realm of securing digital communications and upholding data integrity across an expansive array of fields. As this discourse has brought to light, the foundational principles of PKI – authentication, encryption, and digital signatures – stand as steadfast sentinels, consistently applied in diverse domains including web security, healthcare, finance, the Internet of Things (IoT), and government services. Yet, the nuanced implementation and deployment of PKI underscores the influence of domain-specific considerations such as scale, complexity, resource constraints, regulatory environments, and trust models.

The adaptability and robustness of PKI shine through in myriad applications, from securing communications through SSL/TLS in web security to the safeguarding of sensitive patient data in healthcare. In the financial domain, PKI's role in ensuring the authenticity of online transactions stands as a testament to its adaptability and reliability. In the unique landscape of the IoT, where scale and device diversity pose distinct challenges, PKI remains instrumental through the deployment of lightweight cryptography and tailored certificate management strategies. The use of PKI in government services for electronic IDs and secure digital services further underscores its significance, enhancing both security and operational efficiency.

It is crucial to underscore that PKI is far from a one-size-fits-all solution. The nuanced exploration of commonalities and divergences across fields, as delineated in this article, emphasizes the imperative of customizing PKI implementations to align with the specific needs and constraints inherent in each sector.

Looking ahead, the evolution of technologies and the emergence of new challenges necessitate continuous innovation and adaptation for PKI to sustain its efficacy in securing communications and safeguarding data. The intricate interplay between emerging threats, evolving compliance and regulatory requirements, and the increasing complexity of digital ecosystems demands vigilant attention. Through proactive adaptation and astute management, PKI is poised to endure as a cornerstone of secure digital communications across diverse domains, providing a robust and reliable foundation for the future of digital security.

Future research. As we draw conclusions from our exploration of PKI applications across diverse domains, several avenues for future research and development become apparent. They encapsulate the evolving landscape of secure digital communication and underscore the need for continuous innovation. One of the possible research directions might be a deeper exploration of the integration between PKI and emerging technologies, particularly blockchain. Investigating how these technologies can synergize will unlock novel approaches to fortify security solutions and effectively combat evolving threats. The future demands adaptive and scalable PKI systems. Therefore, it is necessary to research flexible PKI implementations that can cater to the specific needs of diverse domains, ensuring resilience in the face of evolving technological landscapes. Interoperability challenges persist in diverse PKI implementations. Future research should focus on understanding and addressing these challenges, with an emphasis on developing standardized solutions to facilitate seamless integration across different sectors. It is important to explore user-centric security measures within PKI systems. Research in this area should aim to enhance user authentication methods without compromising security, especially in sectors where user convenience is paramount. Given the rising concerns around privacy, future research should delve into privacy-preserving PKI solutions. Investigating techniques to bolster the privacy aspects of PKI, particularly in sensitive domains, will be critical for compliance with evolving privacy regulations. Dynamic PKI policies and governance structures need to be explored. Adaptive policies that can navigate changing regulatory environments, ensuring effective governance and compliance across diverse domains are promising. In the era of quantum computing, research should prioritize the development of quantum-resistant PKI solutions. Investigating cryptographic techniques resilient to potential quantum threats will safeguard the long-term security of PKI systems. Acknowledging the human factor in PKI security is essential. Future research could explore user education and awareness programs, studying the impact of user behavior on PKI effectiveness and devising strategies for enhanced system security through user engagement.

Lastly, fostering cross-disciplinary collaboration is crucial. We advocate for collaborative efforts between researchers, industry experts, and policymakers, ensuring that research outcomes align with operational needs and regulatory requirements in the ever-evolving landscape of PKI security.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 2017.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266-2279. doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[3] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2008.

[4] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", *IETF Trust*, 2018, 160 p. [Online]. Available at: https://datatracker.ietf.org/doc/html/rfc8446. Accessed on: Aug. 03, 2023.

[5] T. Dierks, and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", *RFC 5246*, IETF, 2008, 104 p. [Online]. Available at: https://www.rfc-editor.org/rfc/rfc5246.html. Accessed on: Aug. 03, 2023.

[6] C. Evans, C. Palmer, and R. Sleevi, "Public Key Pinning Extension for HTTP", *Internet Engineering Task Force (IETF)*, 2015, 27 p. [Online]. Available at: https://datatracker.ietf.org/doc/rfc7469/. Accessed on: Aug. 08, 2023.

[7] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy oriented access control for electronic health records", *Electronic Journal of Health Informatics*, vol. 8, no. 2, 2014, 9 p. [Online]. Available at: https://www.researchgate.net/publication/267805570_Privacy_Oriented_Access_Control_for_Electronic_Health_Records. Accessed on: Aug. 12, 2023.

[8] A. Mense, P. Urbauer, S. Sauermann, and M. Frohner, "Integration von Personal Health Records (PHR) in die österreichische elektronische Gesundheitsakte (ELGA)", in *Proc. eHealth2013*, May 23-24, Vienna, Austria, 2013, pp. 45-51. [Online]. Available at: https://www.dhealth.at/wp-content/uploads/scientific-papers/2013/mense.pdf. Accessed on: Sep. 08, 2023.

[9] J. L. Fernandez-Aleman, I. C. Senor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *Journal of Biomedical Informatics*, vol. 46, no. 3, 2013, pp. 268-286. [Online]. Available at: https://www.sciencedirect.com /science/article/pii/S1532046412001864?via%3Dihub. Accessed on: Sep. 08, 2023. doi: https://doi.org/10.1016/j.jbi.2012.12.003.

[10] M. Sayal, "Providing A Secure Environment For E-Commerce Sites Using SSL Technology", *Journal of Education and Science*, vol. 29 (1), pp. 174-191. [Online]. Available at: https://edusj.mosuljournals.com/article_164371.html. Accessed on: Aug. 17, 2023. doi: https://doi.org/10.33899/edusj.2020.164371.

[11] C. Narendiran, S. A. Rabara, and N. Rajendran, "Public key infrastructure for mobile banking security", in *Proc. 2009 Global Mobile Congress*, Shanghai, China, 2009, pp. 1-6. [Online]. Available at: https://ieeexplore.ieee.org/document/5295898. Accessed on: Sep. 17, 2023. doi: https://doi.org/10.1109/GMC.2009.5295898.

[12] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy, and trust in Internet of Things: The road ahead", *Computer Networks*, vol. 76, 2015, pp. 146-164. [Online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971?via%3Dihub. Accessed on: Aug. 15, 2023. doi: https://doi.org/10.1016/j.comnet.2014.11.008.

[13] I. Lee, and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises”, *Business Horizons*, vol. 58, no. 4, 2015, pp. 431-440. [Online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0007681315000373?via%3Dihub. Accessed on: Sep. 21, 2023. doi: https://doi.org/10.1016/j.bushor.2015.03.008.

[14] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, “Security Challenges in the IP-based Internet of Things”, *Wireless Personal Communications*, vol. 61, no. 3, 2011, pp. 61-76. Online]. Available at: https://link.springer.com/article/10.1007/s11277-011-0385-5. Accessed on: Sep. 23, 2023. doi: https://doi.org/10.1007/s11277-011-0385-5.

[15] United States Government, “Federal Public Key Infrastructure (PKI) Trust Infrastructure Overview”, Federal PKI Policy Authority. [Online]. Available at: https://www.idmanagement.gov/fpki. Accessed on: Aug. 23, 2023.

[16] Ministry of Government Administration, Reform and Church Affairs, “Requirements specification for PKI in the public sector”. [Online]. Available at: https://www.regjeringen.no/en/dokumenter/requirements-specification-for-pki-in-th/id611085. Accessed on: Aug. 23, 2023.

[17] C. Adams, and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, Addison-Wesley Professional, 2002.

[18] A. Alshehri, S. Alharbi, M. Khayyat, and O. Aboulola, “Global E-government Trends, Challenges and Opportunities”, *SAR Journal*, vol. 4(1), 2021, pp. 175-180. [Online]. Available at: https://www.sarjournal.com/content/44/SARJournalDecember2021_175_180.html. Accessed on: Aug. 23, 2023. doi: https://doi.org/10.18421/SAR44-04.

Стаття надійшла до редакції 05.11.2023.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 2017.

[2] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266-2279. doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[3] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2008.

[4] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3”, *IETF Trust*, 2018, 160 p. [Online]. Available at: https://datatracker.ietf.org/doc/html/rfc8446. Accessed on: Aug. 03, 2023.

[5] T. Dierks, and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, *RFC 5246*, IETF, 2008, 104 p. [Online]. Available at: https://www.rfc-editor.org/rfc/rfc5246.html. Accessed on: Aug. 03, 2023.

[6] C. Evans, C. Palmer, and R. Sleevi, “Public Key Pinning Extension for HTTP”, *Internet Engineering Task Force (IETF)*, 2015, 27 p. [Online]. Available at: https://datatracker.ietf.org/doc/rfc7469/. Accessed on: Aug. 08, 2023.

[7] R. Gajanayake, R. Iannella, and T. Sahama, “Privacy oriented access control for electronic health records”, *Electronic Journal of Health Informatics*, vol. 8, no. 2, 2014, 9 p. [Online]. Available at: https://www.researchgate.net/publication/267805570_Privacy_Oriented_Access_Control_for_Electronic_Health_Records. Accessed on: Aug. 12, 2023.

[8] A. Mense, P. Urbauer, S. Sauermann, and M. Frohner, "Integration von Personal Health Records (PHR) in die österreichische elektronische Gesundheitsakte (ELGA)", in *Proc. eHealth2013*, May 23-24, Vienna, Austria, 2013, pp. 45-51. [Online]. Available at: https://www.dhealth.at/wp-content/uploads/scientific-papers/2013/mense.pdf. Accessed on: Sep. 08, 2023.

[9] J. L. Fernandez-Aleman, I. C. Senor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *Journal of Biomedical Informatics*, vol. 46, no. 3, 2013, pp. 268-286. [Online]. Available at: https://www.sciencedirect.com /science/article/pii/S1532046412001864?via%3Dihub. Accessed on: Sep. 08, 2023. doi: https://doi.org/10.1016/j.jbi.2012.12.003.

[10] M. Sayal, "Providing A Secure Environment For E-Commerce Sites Using SSL Technology", *Journal of Education and Science*, vol. 29 (1), pp. 174-191. [Online]. Available at: https://edusj.mosuljournals.com/article_164371.html. Accessed on: Aug. 17, 2023. doi: https://doi.org/10.33899/edusj.2020.164371.

[11] C. Narendiran, S. A. Rabara, and N. Rajendran, "Public key infrastructure for mobile banking security", in *Proc. 2009 Global Mobile Congress*, Shanghai, China, 2009, pp. 1-6. [Online]. Available at: https://ieeexplore.ieee.org/document/5295898. Accessed on: Sep. 17, 2023. doi: https://doi.org/10.1109/GMC.2009.5295898.

[12] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy, and trust in Internet of Things: The road ahead", *Computer Networks*, vol. 76, 2015, pp. 146-164. [Online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971? via%3Dihub. Accessed on: Aug. 15, 2023. doi: https://doi.org/10.1016/j.comnet.2014. 11.008.

[13] I. Lee, and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", *Business Horizons*, vol. 58, no. 4, 2015, pp. 431-440. [Online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0007681315000373?via%3Dihub. Accessed on: Sep. 21, 2023. doi: https://doi.org/10.1016/j.bushor.2015.03.008.

[14] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things", *Wireless Personal Communications*, vol. 61, no. 3, 2011, pp. 61-76. Online]. Available at: https://link.springer.com/article/10.1007/ s11277-011-0385-5. Accessed on: Sep. 23, 2023. doi: https://doi.org/10.1007/s11277-011-0385-5.

[15] United States Government, "Federal Public Key Infrastructure (PKI) Trust Infrastructure Overview", Federal PKI Policy Authority. [Online]. Available at: https://www.idmanagement.gov/fpki. Accessed on: Aug. 23, 2023.

[16] Ministry of Government Administration, Reform and Church Affairs, "Requirements specification for PKI in the public sector". [Online]. Available at: https://www.regjeringen.no/en/dokumenter/requirements-specification-for-pki-in-th/id611085. Accessed on: Aug. 23, 2023.

[17] C. Adams, and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, Addison-Wesley Professional, 2002.

[18] A. Alshehri, S. Alharbi, M. Khayyat, and O. Aboulola, "Global E-government Trends, Challenges and Opportunities", *SAR Journal*, vol. 4(1), 2021, pp. 175-180. [Online]. Available at: https://www.sarjournal.com/content/44/SARJournalDecember2021_175_180.html. Accessed on: Aug. 23, 2023. doi: https://doi.org/10.18421/SAR44-04.

ОЛЕКСАНДР ДУЛЯ,
ДМИТРО МІНОЧКІН

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВИКОРИСТАННЯ ІНФРАСТРУКТУРИ ПУБЛІЧНИХ КЛЮЧІВ В РІЗНИХ СФЕРАХ

У статті розглянуто роль Інфраструктури Публічних Ключів (PKI) у забезпеченні безпеки та автентифікації комунікацій в різних галузях. PKI перетворилася з простого технічного концепту в основу безпечних цифрових комунікацій, відіграючи центральну роль у таких доменах, як веббезпека, охорона здоров'я, фінанси, Інтернет речей (IoT) та державні служби. PKI використовує криптографічні методи та цифрові сертифікати для встановлення довіри, забезпечення цілісності даних і забезпечення безпечних комунікацій, тим самим виступаючи основою цифрової безпеки.

Сьогодні попит на надійні та стійкі рішення з безпеки стрімко зріс. Різноманітність та масштаб сучасних цифрових платформ вимагають адаптивних рішень з безпеки, виклик, з яким PKI бореться через свою гнучкість впровадження. Незважаючи на спільні основні принципи, впровадження PKI демонструє розбіжності, що визначаються такими факторами, як масштаб, складність, обмеження ресурсів, регуляторні середовища та моделі довіри. Тому, в роботі проведено широке порівняння використання PKI в різних секторах, висвітлюючи спільні та відмінні характеристики та дослідити, як PKI адаптується для вирішення унікальних вимог та викликів кожного сектору.

Проаналізовано поточний стан застосувань та проблем PKI. З розвитком та розширенням цифрового ландшафту, критично важливо передбачати нові виклики та розробляти стратегії для проактивної адаптації. Підкреслено важливість PKI та висвітлено необхідність продовження наукових досліджень та розробок у цій області. З ростом нашої залежності від цифрових комунікацій та транзакцій, роль PKI у захисті цих взаємодій стає все більш значущою.

Ключові слова: інфраструктура публічних ключів, цифрові сертифікати, веббезпека, інтернет речей, аутентифікація, шифрування.

Dulia Oleksandr, Ph.D. student of the department of telecommunications, Institute of telecommunication systems of the National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine, ORCID 0000-0002-9769-3178, sasa97973@gmail.com.

Minochkin Dmytro, candidate of technical sciences, senior researcher, associate professor of the department of telecommunications of the National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine, ORCID 0000-0003-4988-7098, dmytro.minochkin@gmail.com.

Дуля Олександр Олександрович, аспірант кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

Міночкін Дмитро Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри телекомунікацій Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.