

Encryption Vulnerability Graph for Assessing IT System Compliance with Kerckhoffs' Principle in Healthcare

Rihards Balodis

*Institute of Mathematics and Computer
Science of Latvia University*
Riga, Latvia
rihards.balodis@lumii.lv

Inara Opmane

*Institute of Mathematics and Computer
Science of Latvia University*
Riga, Latvia
inara.opmane@lumii.lv

Kristaps Kulis

TET
Riga, Latvia
kristaps.kulis@tet.lv

Abstract—The authors propose a methodology to improve the use of cryptography in information systems and visualise the vulnerability level of encryption keys. The proposed methodology contains recommendations for developing a specially targeted encryption key usage document as special IT system documentation annex and encryption vulnerability graph when developing an information system project, thus bringing attention to the use of security requirements for the design of cryptography requirements recommended in the literature; the annex depicts the use of encryption keys statically at the initial and implementation stages of information system development, as well as the implementation of the TCP/IP SNMP protocol for the dynamic monitoring use of encryption keys in online mode during information system maintenance. The vulnerability visualisation scheme proposed by the authors is projected with information from the ITU standard X.1710. The methodology proposed in the article is implemented in an encryption key management system that is in the project development stage; the methodology is intended for individual adaptation to the views and needs of information system designers.

Keywords—*encryption key, key management system, quantum key distribution, quantum random number generation key, Kerckhoffs' principle*

I. INTRODUCTION

The need to ensure better data protection is growing, as the range of users that require protected data is expanding. The most widely used computer-based data protection solutions utilise data encryption. The encryption key is the basis of all cryptographic functionalities.

Many data protection solutions are available, and the most fundamental need for humans and computers is to keep encryption keys secret. Special crypto platforms implement data encryption solutions in information systems and use them to work with digital data. The use of encryption keys can be opaque, complex, and even difficult to control due to the malicious use of data encryption keys.

When implementing information systems, a policy for data protection and encryption keys implemented in a system must be written, following the recommendations for developing a secure system architecture. In accordance with the generally accepted requirements for information system development, the authors recommend developing a security policy as a separate, significant document as an annex to the system project. Adding

use case solutions to the encryption key policy (Encryption vulnerability graph, encryption primitives) and the methodology to supplement the requirement is also recommended, as well as designing a security architecture to ensure transparent adherence to Kerckhoffs' principle.

The need to ensure better data protection is growing, as the range of users that require protected data is expanding. The most widely used computer-based data protection solutions utilise data encryption.

Many data protection solutions are available, and the most fundamental need for humans and computers is to keep encryption keys secret. Special crypto platforms implement data encryption solutions in information systems and use them to work with digital data. The use of encryption keys can be opaque, complex, and even difficult to control due to the malicious use of data encryption keys.

Solutions for the use of data encryption are constantly being upgraded with innovative technologies and an increased level of data protection, but two areas of cryptography use stand out in particular: the protection of personal health privacy and the specially protected financial sector, and transactions with money.

II. SPECIFIC REGULATIONS FOR PERSONAL DATA PROTECTION IN HEALTHCARE

The European Health Data Space is a cornerstone of the European Health Union and the first common EU data space dedicated to a specific sector as part of the European Data Strategy [1]. The data protection rights of healthcare patients are regulated by the general human rights framework, GDPR (General Data Protection Regulation, in Europe) [2] and HIPAA (Health Insurance Portability and Accountability Act of 1996, in the USA). HIPAA has deep practical experience of use, including in the field of personal data protection in healthcare. [3, 4] The processing of personal data in healthcare systems (including the Encryption Key Management System) requires the consent of the person concerned (the patient) to data processing: consent must be freely given, unambiguous, and the system must provide the patient with the right to withdraw their consent.

HIPAA also requires the use of cryptography in healthcare [5–10].

HIPAA mandates the use of cryptography to protect healthcare data and communications (data at rest and data in transit).

HIPAA requires the encryption of protected health information (PHI) [11]. Encryption requirements under HIPAA are recommended, but not mandatory. To ensure data privacy, data encryption should be used during the exchange of sensitive data between a healthcare system patient and healthcare provider, as well as during storage to protect data in the event that storage devices are stolen.

III. SPECIFIC REGULATIONS FOR THE BANKING SECTOR

In the banking sector, information systems ensure punctuality and high data security. These information systems, used every day, also have deep historical practical experience in data protection. Currently, banks use adequate encryption methods, such as AES, RSA and ECC, and use the SSL/TLS protocol for data transmission over the internet, with software updates constantly being made to ensure the highest level of security.

If we evaluate banking operations from the point of view of encryption key exchange solutions, then it corresponds to traditional schemes; however, they have been supplemented with specific requirements due to the threat of quantum computers, and the requirements are still dynamically supplemented [12–14].

The mission of the Accredited Standards Committee (ASC) X9 and the International Organisation for Standardisation (ISO) is to develop and maintain U.S. and international standards that improve payment and securities transactions, protect data, and facilitate information exchange.

The payment card industry is made up of all organisations that store, process, and transmit cardholder data, particularly debit and credit card data. Security standards are developed by the Payment Card Industry Security Standards Council, which develops Payment Card Industry data security standards that are used across the industry.

The transition from traditional PKI with asymmetric certificate issuance algorithms to PQC algorithms also means a modification of PKI and certificate issuance. Similarly, the financial services industry has its own needs that are no longer met by existing certification mechanisms and browsers. Therefore, ASC X9 has adopted X9 Financial PKI as an alternative for PQC readiness and crypto flexibility for banks, merchants, and third-party financial service providers.

X9 Financial PKI is expected to have significant changes (additions) to the certification mechanism (2025):

- Addendum: X.509 certificates with PQC solution;
- Addendum: X.509 hybrid certificates with PQC solutions;
- Addendum: X.509 hybrid certificates with composite PQC Private key;
- Addendum: X.509 chameleon certificates with PQC solution.

PCI Data Security Standard for payment cards is being clarified [15, 16].

Not only are traditional payment schemes in banks and with cards at terminals being modified, but also in bank payments with cloud services [17–19].

IV. WHEN WILL KERCKHOFFS' PRINCIPLE BE RESPECTED IN A DEVELOPED SYSTEM?

The need to ensure better data protection is growing, as the range of users that require protected data is expanding. The most widely used computer-based data protection solutions utilise data encryption. The encryption key is the basis of all cryptographic functionalities.

Many data protection solutions are available, and the most fundamental requirement for humans and computers is to keep encryption keys secret.

Kerckhoffs' principle [20–22] is a postulate, the validity of which is assessed in the context of the practical sphere of activity, depending on the solutions one has at their disposal at the time – equipment, algorithms and programs (primitives).

The root of encryption key vulnerability depends on the quality of the encryption key at the time of its generation, based on truly random and highest entropy (randomness), known as quantum uncertainty (quantum computing threat), further providing an uncopied encryption key for precisely this (this quality) in the execution of encryption algorithms.

Below, in descending order, we will indicate the following quality levels of data encryption keys to be used in compliance with Kerckhoffs' principle, depending on whether the generated data encryption keys are derived from qualitative entropy sources and encryption key predictability is protected by the laws of physics:

- QRNGs are quantum-based/also Quantum Physical Unclonable Function (QPUF) (highest security and true randomness);
- TRNGs use quantum mechanics (unpredictable but can have lower entropy);
- PRNGs generate keys with algorithms (fast calculation but predictable, especially concerning the threats of quantum computers).

In this article, we will look at the compliance of data encryption key protection with the Kerckhoffs' principle in a wide range of applications, including KMS, QMS, and cloud key storage.

The encryption keys generated (key at generation status) in the manner described above must be transferred to other servers in the information system (key at transit status), used in communication protocols, and finally, the encryption keys must be obtained for the data encryption algorithms (key in use status).

The transfer of the encryption key (key in transit) can be performed in different ways, and as a result, the level of vulnerability of the encryption key differs.

When creating encryption documentation, the following encryption key usage schemes can be distinguished:

- **In Use**, the key is utilised in the data encryption process, in an encryption algorithm or encryption primitive.
- **In Transit**, the key is transferred from one server to another; the vulnerability is adequate for the data encryption protocol.
- **At Rest**, the key is placed on the server for storage; the vulnerability is adequate for the data protection of server storage.
- **In Transformation**, the encryption key is algorithmically transformed into another encryption key and the vulnerability changes upon being evaluated by the system administrator. At this key processing point, physical protection is recommended.

The quantum communications field usually uses a Quantum Key Distribution QKD platform, in which encryption keys are generated by QRNG chips; QKD manufacturers add a quantum key exchange layer QMS to the platform, and system owners add a consumer layer, which provides data encryption. Typically, consumers use symmetric keys for data encryption (provided by the QMS layer), while PKI is generally used for the authorisation/authentication of operations.

For a simplified understanding, Fig. 1 demonstrates this concept.

In [23], the term – System Level of Compliance with Auguste Kerckhoffs' Cryptography Principle is defined.

The categorisation of adherence to Auguste Kerckhoffs' cryptography principle regarding access to cryptographic keys should be introduced in cryptography-based information systems:

- The encryption key value is securely protected from access: QKD level – the maximum level of compliance with Kerckhoffs' principle; this includes protection against tampering and physical key protection in transit,
- Compliance with Kerckhoffs' principle: QMS level – null level – is based on the physical protection of the devices located nearby (for example, in the same room) that use quantum mechanics or other laws of physics,
- Software-based solutions at the consumer level: TCP/IP protocols and the use of Post-Quantum Cryptography (PQC) solutions and PQC – the soft level.

To the question – what does Kerckhoffs' principle mean? One could answer that Kerckhoffs' principle is respected if the encryption key has remained unchanged, without being compromised, and has not been read (copied from the moment of generation) until its use in the encryption algorithm.

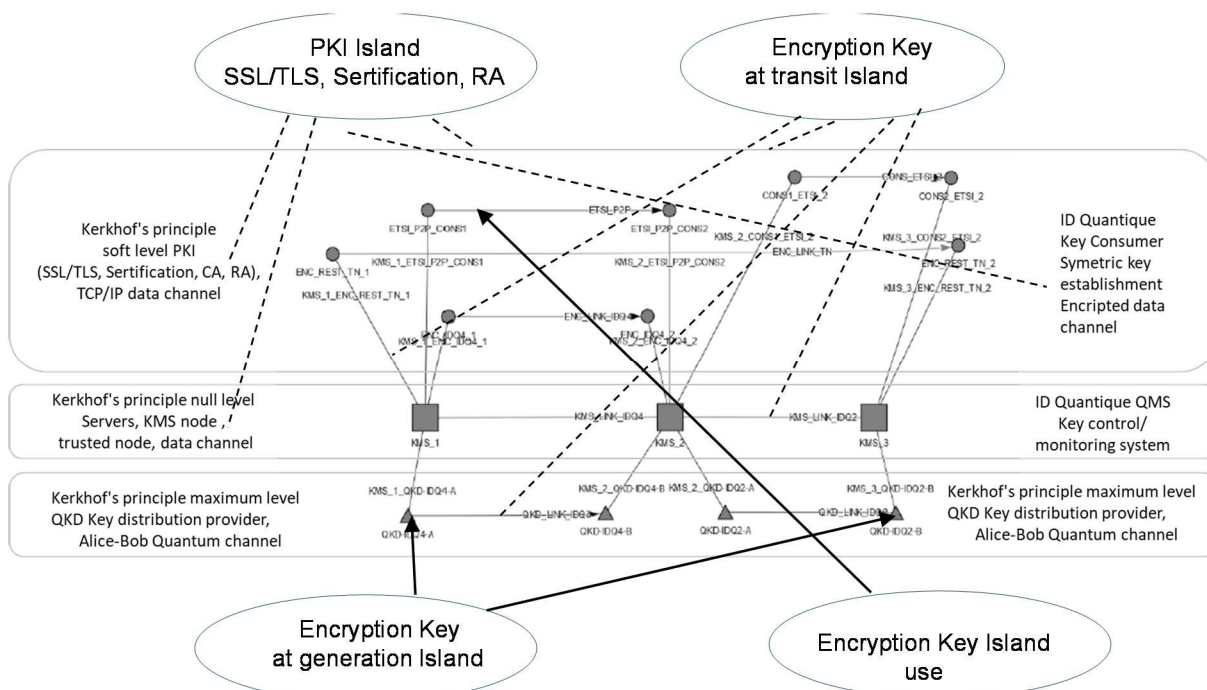


Fig. 1. Auguste Kerckhoffs' principles in the ID Quantique QKD solution.

V. SECURITY FRAMEWORK FOR QUANTUM KEY DISTRIBUTION NETWORKS

The document [24] describes the detailed sequence of encryption key usage in a QKD network fragment. It also includes an assessment of the vulnerability of encryption keys. The authors of the article propose to simplify and visualise the scheme of encryption key usage implemented in the encryption system, making vulnerability assessment easier (the estimate is more approximate) and, therefore, simpler to understand for the customer. With the use of the SNMP protocol, the actual use of encryption keys can be tracked.

We draw your attention to two images included in the ITU standard X.1710 (Typical structure of a QKDN and user network, Security threats to QKDN). They depict potential cryptographic threats in identified areas of the QKD network, while the table provides threat assessments at three possible threat levels:

- High level of Vulnerability. This level is fatal if a threat occurs;
- Medium level. If such threats occur, secure and reliable operations of a QKDN cannot be achieved;
- Low level.

When designing a QKD network according to the methodology recommended in this article – creating a coloured vulnerability graph, determining the cryptographic islands to be analysed in the network fragment, determining the encryption primitives and their vulnerability level according to Kerckhoff's principle, it is advisable to add the above-mentioned information from the ITU standard X.1710 to the analysis, as well as the relevant information available in the documentation of the IDQ product CLAVIS3.

VI. RECOMMENDATION FOR THE DEVELOPMENT OF AN ENCRYPTION INFORMATION SYSTEM PROJECT ANNEX AND ENCRYPTION DECOMPOSITION

Today, the practical use of data encryption is complex, characterised by the diversity of possible technical solutions; thus, selecting the required level of security is complex. The authors of the article recommend a methodology of actions, taking the path of simplifying solutions and achieving logical transparency for the practical solution of the task. The first step in such a case is usually to develop an action plan; a separate encryption technical project Annex is needed, similar to, for example, a construction project in the field of housing development.

The authors believe, contrary to the globalisation thesis and the development of broad, comprehensive universal cryptography use platforms, that it is currently more expedient to follow the path of decomposition, creating limited segments of different encryption key usage – islands, in which the encryption key is used to perform a certain goal intended for a predefined functional task.

Typical encryption islands are public key infrastructure (PKI) and the symmetric key establishing key infrastructure (SII) segment; the basic encryption key bar in the authors'

vulnerability analysis model is the highest-quality key in the whole encryption system application. PKI and SII only provide service functionality for the necessary actions in the key bar segment – mainstream use of quantum keys from the QKD platform.

From the viewpoint of the actual purpose of using encryption keys, encryption islands can overlap. When assessing the vulnerability level of information system segments, overlapping encryption islands inherit the highest vulnerability level. Therefore, when designing the information systems annex, it is important to ensure that encryption islands do not overlap.

It is recommended to design a system architecture in which one encryption key is used per segment. If necessary, a dedicated key exchange segment with its own encryption key is used for key exchange between segments, thus creating multiple segments using a common key as an exception. At this level of key processing, it is recommended to plan physical encryption key protection methods; for example, placing servers in a closed room.

The decomposition principle is also used to solve complex mathematical and management problems. Decomposition is also proposed for encryption key management KMS systems.

The theoretical basis for the convergence and divergence hypotheses is actively discussed in sociology, politics and economics, as well as modern technology. This is also seen in the development of Encryption Key Management systems [23].

Just as cryptographic algorithms are described in terms of cryptographic primitives, it is also recommended that each functional cryptographic island is described using certain primitives. In this way, with conceptual primitives, one can more accurately define the use of encryption keys in the segment. Conceptual primitives make it easier to assign a level of vulnerability (colour shown in the vulnerability graph) to keys, with the colour in the graph determining the risk level of the information system's cryptographic vulnerability.

The following possible island segments and primitives have a functional, dedicated task of using an encryption key:

- Island for exploring digital identity and Public Key Infrastructure (PKI), including digital certification authority functionality, with an indivisible key bar service island with its own risk level.
- The Management of Symmetric Keys (SK), establishing an island.
- Island of Key aspects of Hashing, which may be added to the PKI and SK.
- Hardware security module HSM infrastructure, which may be added to the PKI and SK or KE Island.
- Island of Key Management Service, usually the QKD platform manufacturer's QMS Island, with its own risk level.
- Other segments as required.

A catalogue of usable primitives should be developed when implementing one's own key usage proposal.

As previously mentioned, the existing practice of incorporating encryption solutions is very diverse and, therefore, logically difficult to understand. In the authors' opinion, a specific solution and a specific project, with its decomposition into islands of encryption key usage, makes the logic of the solution more transparent.

Project design principles to be followed when creating a vulnerability project and its primitives [23, 25]:

1. Security by design principle: decomposition of the encryption system into islands.
2. Security by design principle: evaluation of the role of Physical Security in implementation.
3. Security by design principle: hardware-based security. Many literature sources indicate that the risks of security threats are reduced if implementation is based on physical devices and not software solutions; for example, encryption key storage implementation is recommended in a special device for this purpose – HSM.
4. Security by design principle: use of OSI layer 2, 3 and/or 4 communication protocols as a priority, thus ensuring a higher level of communication security.

It is recommended to establish an Ethernet interface in the communication channel between Alice (also Bob) and the QMS node of the encryption key management system, as well as to combine all of Kerckhoffs' null and maximum level ICT infrastructure into one LAN, which uses MACsec and IPsec protocols and QKD (also QRNG) generated encryption keys, even in one physically protected room.

5. Security by design principle: communication perimeter protection system and localisation functionalities as needed.

Communication perimeter protection usually includes a combination of physical and technological barriers. The perimeter, which incorporates both the physical location of the equipment in one room or in nearby rooms, is provided, where entry can be controlled according to a defined entry policy, but also access control to information with virtual firewall settings, as well as external user connections to the ICT infrastructure along the perimeter. Several perimeters can be created, as well as inclusive ones; for example, for the maximum and zero layers of Kerckhoffs' principle, a single protection dome is created for all infrastructure units, the role of which is to ensure the distribution of QKD encryption keys. Enclosing the necessary PKI infrastructure in such a domain is possible with limited functionality; for example, by creating one's own enterprise-type PKI.

6. Kerckhoffs' principle must be complied with to the extent possible [23].

We recommend using the QKD platform to ensure customer data protection in information systems.

VII. RECOMMENDATIONS FOR INTRODUCING A CRYPTOGRAPHIC VULNERABILITY GRAPH

It is recommended to display the level of encryption system vulnerability with a vulnerability graph. Regardless of whether one is creating a project annex for using encryption in a new

information system or utilising an existing information system that uses encryption, the authors recommend creating a graph that reflects the use of encryption keys.

Stealing a key, copying a key in any status, or protecting access (reading) to the key in the mailbox is always a risk, but how high is it?

This is why the graph is known as a vulnerability graph; it allows us to understand and analyse the level of vulnerability, create an information system architecture, and determine information system usage requirements with the aim of reducing vulnerability.

Graphs are used for encryption vulnerability analysis. In cryptography, graphs are also used in the development of new encryption algorithms. The authors' intention is to use graphs to simplify the understanding of the use of encryption keys, in particular, in the information system, and thus assess the vulnerability level of an encryption key and determine the level of compliance with the iconic postulate put forward by Kerckhoffs' Principle – focus on the inaccessibility of the key to a third party.

The graph shows vertices (typically, virtual servers of the system) with encryption keys, identifying the purpose of using the encryption key, while the edges indicate the functional link between key storage locations; for example, an edge showing that an encryption key is being transferred from one server to another, and which data transfer protocol or technology pack is used for such encryption key transfer.

Vertices, essential points in the use of encryption keys, are located on one of the islands and perform a certain functional task of data protection.

A structured decomposition of the cryptographic system islands is recommended, aimed at providing a simplified understanding of how and why an encryption key or a whole island is protected from vulnerability.

The vulnerability level for encryption keys on an island is one, and the graph assigns the island the colour corresponding to the weakest security (higher vulnerability) level. The edges represent the type of connection for the necessary information and the key exchange between islands/vertices (physical protection provided, and the specific data exchange protocols used, such as UDP, LAN Ethernet connection, Quantum channel or other). Edges and vertices, depending on the purpose of the used functionality of the encryption key placed there, provide a publicly available assessment of the vulnerability level (assigned a colour that may change over time, depending on the acquisition of new, improved solutions).

VIII. RECOMMENDATIONS FOR THE DE FACTO VISUALISATION ENCRYPTION KEY PROTECTION LEVEL

It is recommended to monitor the use of encryption keys with Simple Network Management Protocol v3 (SNMP) and an SNMP MIB (Management Information Base) [26–28]. This protocol also ensures the use of quantum encryption keys, quantum communication dedicated equipment, and relevant network software in online mode. The SNMP MIB is a hierarchical database (dictionary, registry) used to manage

network devices and software, including cryptography protocols. In the MIB, the objects to be monitored are defined, with the variables (configured data descriptions) and OIDs (object identifiers) named, which allows the data of interest to be obtained online.

The MIB registry, SNMP Agents, and alerts known as “traps” can be used to provide online visual mapping of the intensity of encryption use. By using a special application that integrates MIB data with a vulnerability graph introduced at the early stage of information system design, de facto security mapping can be provided for the planned cryptographic project.

The graph shows the most vulnerable areas in the use of encryption keys.

IX. CONCLUSIONS

The method proposed by the authors will provide information system developers and system maintainers with a deep understanding of the use of encryption keys and thus greater adherence to Auguste Kerckhoffs’ principle in everyday life.

Information systems process, transfer, and store customer data in data storage for a long time using a variety of telecommunications environments. Nowadays, it is becoming essential to protect customer data from third-party access and illegal (unintended in the system) data distortion. Typically, data encryption employing cryptographic solutions is used to protect data in a digital environment. The primary task of an information system is to process data as required for the functionality of the information system, with the task of protecting data becoming secondary.

The methodology proposed by the authors of the article emphasises the need to understand cryptographic solutions in an information system, using a well-thought-out and third-party transparent encryption solution scheme in the information system, creating vulnerability graphs, using recognised encryption design methods, as well as ensuring encryption monitoring in linking solutions with vulnerability graphs, using the TCP/IP protocol SNMP v3 (in the case of quantum-safe encryption keys and quantum mechanics applications).

The method can be used when developing an information system architecture (by developing a special annex to the information system project on the use of cryptography), or a document of similar content for an existing information system (in this case, by developing a data security policy). These documents provide third parties with higher transparency regarding the use of encryption solutions by providing visual information system vulnerability mapping.

ACKNOWLEDGMENT

The research leading to these results has received funding from the project Competence Centre of Information and Communication Technologies for Digitalisation of the Recovery and Resilience Facility, contract No. 2.2.1.3.i.0/1/24/A/CFLA/006 signed between the IT Competence Centre and the Central Finance and Contracts Agency, Research No. 1.7 Full-cycle data encryption key management platform solution for data protection during

transmission and storage in data centres and cloud environments.

REFERENCES

- [1] European Health Data Space Regulation (EHDS), https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en
- [2] General Data Protection Regulation GDPR, <https://gdpr-info.eu/>
- [3] HIPAA Security Rule NPRM, <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html>
- [4] HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information Fact Sheet, <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>
- [5] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, <https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information>
- [6] HIPAA Encryption Requirements, <https://www.hipaajournal.com/hipaa-encryption-requirements/>
- [7] HIPAA Encryption Requirements, <https://www.mimecast.com/content/hipaa-encryption-requirements/>
- [8] HIPAA Encryption Requirements: An Updated Guide, <https://drata.com/blog/hipaa-encryption-requirements>
- [9] HIPAA Encryption Requirements: The Key to Protecting Patient Privacy, <https://sprinto.com/blog/hipaa-encryption-requirements/>
- [10] How Encryption Protects Vendor Data in Healthcare, <https://www.censinet.com/perspectives/how-encryption-protects-vendor-data-in-healthcare>
- [11] What is Considered PHI Under HIPAA?, <https://www.hipaajournal.com/considered-phi-hipaa/>
- [12] ASC X9 PKI Policy Group, Certificate Policy (CP) for the X9 Financial Public Key Infrastructure (PKI), Accredited Standards Committee X9 Inc., Publication Date: 3 April 2025, Release: 1.0
- [13] Accredited Standards Committee X9, Quantum Computing Risks to the Financial Services Industry, ASC X9 INFORMATIVE REPORT, ASC X9 IR-F01-2022, 29 November 2022
- [14] Jeff Stapleton, X9 Financial PKI: PQC Readiness and Crypto-Agility for Financial Services, Post-Quantum Cryptography Conference, January 2025, https://www.youtube.com/watch?v=GUHynaGq_Fs
- [15] Payment Card Industry Data Security Standard: Requirements and Testing Procedures, PCI Security Standards Council, v4.0, March 2022
- [16] PCI Data Security Standard, PCI Security Standards Council, <https://www.pcisecuritystandards.org/standards/pci-dss/>
- [17] AWS Payment Cryptography, AWS User Guide, Amazon Web Services, 2025, <https://docs.aws.amazon.com/pdfs/payment-cryptography/latest/userguide/payment-cryptography-userguide.pdf#security-iam>
- [18] Identity and access management for AWS Payment Cryptography, <https://docs.aws.amazon.com/pdfs/payment-cryptography/latest/DataAPIReference/payment-cryptography-data-api.pdf#Welcome>
- [19] What Is AWS CloudTrail?, Amazon Web Services, Inc., 2025, <https://docs.aws.amazon.com/pdfs/awsccloudtrail/latest/userguide/awsccloudtrail-ug.pdf#cloudtrail-user-guide>
- [20] Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5-38, Jan. 1883, pp. 161-191, Feb. 1883, <https://www.arcsi.fr/doc/cryptomilitaire.pdf>
- [21] Fabien Petitcolas, Kerckhoffs' principles from "La cryptographie militaire", <https://www.petitcolas.net/kerckhoffs/index.html>
- [22] Jean-Claude Caraco, Rémi Géraud-Stewart, David Naccache, Kerckhoffs' Legacy, International Association for Cryptologic Research Cryptology ePrint Archive, Paper 2020/556, <https://eprint.iacr.org/2020/556>
- [23] Rihards Balodis, Inara Opmane, Guna Soloveja, The Role of Physical Security in the Implementation of Kerckhoffs' Principle in the Quantum

- Era, Proceedings of ICAMP 16th International Conference on Applied Physics and Mathematics (ICAPM 2026), Osaka, Japan, 10-12 April 2026, in press
- [24] Recommendation ITU-T X.1710 - Security framework for quantum key distribution networks, ITU-T Telecommunication standardisation sector of ITU, x.1710. Series x: data networks, Open system communications and security, 2020
- [25] Sergey E. Yunakovsky, Maxim Kot, Nikolay Pozhar, Denis Nabokov, Mikhail Kudinov, Anton Guglya, Evgeniy O. Kiktenko, Ekaterina Kolycheva, Alexander Borisov, Aleksey K. Fedorov, and Yunakovsky et al., Towards security recommendations for public-key infrastructures for production environments in the post-quantum era, EPJ Quantum Technology (2021), <https://doi.org/10.1140/epjqt/s40507-021-00104-z>
- [26] Simple Network Management Protocol (SNMP), DXi-Series SNMP Reference Guide, 6-68449-04, August 2017, Last Updated : 3 Oct. 2025, <https://www.geeksforgeeks.org/computer-networks/simple-network-management-protocol-snmp/>
- [27] NIST, Key Management Guidelines, NIST 800-57, Recommendation for Key Management, 5 December 2025, <https://csrc.nist.gov/projects/key-management/key-management-guidelines>, <https://zeronetworks.com/blog/nist-cybersecurity-framework-best-practices>
- [28] NIST, Cybersecurity Framework Best Practices: Deploying Microsegmentation for Built-In Resilience, Secure Network Architecture Design: Segmentation, VPNs, and Key Measures, <https://www.youtube.com/watch?v=EzQFt6FNReY>