Proceedings of CECNet 2022
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220539

Approach for Cryptography Digital Ecosystem Deployment

Inara OPMANE[1] and Rihards BALODIS
Institute of Mathematics and Computer Science of University of Latvia, Latvia

Abstract. The paper introduces the Cryptography Digital Ecosystem concept and describes the rationale for its implementation. A checklists approach is offered to ensure efficient and high-quality ecosystem deployment and helps to ensure consistency and completeness of necessary tasks. A collection of checklists are indicated, which have been analytically developed based on extensive analysis of public literature regarding the development of quantum encryption solutions and adequate compliance with the solution requirements.

Keywords. Checklist, methodology, cryptography, digital ecosystem deployment, quantum cryptography, quantum key distribution (QKD)

1. Introduction

An important research topic of the University of Latvia Centre for Quantum Computing Science is quantum computing: the theoretical aspects of quantum information including quantum algorithms, computational complexity, communications, and cryptography.

As solutions of the practical application of quantum computing are in the nearest future, the strategy of the Institute of Mathematics and Computer Science of the University of Latvia (IMCS UL) is to use quantum technologies that can be applied now and immediately.

The activity of IMCS UL was concentrated in quantum communications and encryption (quantum encryption) applications.

IMCS UL started the development of quantum cryptography research topics in 2019 with the purchase and operational testing of Clavis 3 from ID Quantique (https://www.idquantique.com). In order to develop the research of quantum cryptography at the institute, close research cooperation has been established with industry: the State Joint Stock Company "Latvijas Valsts radio un televīzijas centrs" LVRTC (www.lvrtc.lv), mobile operator LMT (www.lmt.lv), telecommunication company TET (www.tet.lv), and the Electronic Communications Office of Latvia (www.vases.lv). Currently, QKD technology has been tested in LVRTC and LMT fibre infrastructure. The necessity of research is related to development of strategy for introducing a new comprehensive technology that could influence very different aspects and players of our everyday lives. The chosen research method is conceptual analysis. It includes data exploration gathered through literature research, in. The research strategy includes comparison and assessment of a different interpretation in theoretical research and its reflection on real situations analysed in the implementation of the European

[1] Corresponding Author, Inara OPMANE; E-mail: inara.opmane@lumii.lv

Regional Development Fund project "Applications of quantum cryptography devices and software solutions in computational infrastructure framework in Latvia", Project ID number 1.1.1.1/20/A/106 (01.06.2021–30.11.2023).

In this paper authors describe in detail the topics and tasks for deploying a cryptography digital ecosystem strategy.

2. Digital Ecosystem Concept

The word 'ecosystem' was first used in print by A.G. Tansley in 1935 [1]. In literature, you can find different ecosystem establishing models: on the basis of business relations and services [2, 3], and ecosystem models in higher education [4].

Various Ecosystem Analogies are indicated in a summary report [3]:

- Biological Ecosystem
- Industrial Ecosystem
- Economy as an Ecosystem
- Digital Business Ecosystem
- Social Ecosystem.

The introduction of Digital Ecosystem concept started in 2000 at the World Economic Forum [5]. The concept was solidified in subsequent conferences and publications.

We follow the principles set forth by the World Economic Forum [5]:

- The digital renaissance and the global digital ecosystem
- Putting people at technology's heart
- Sustainability.

3. Cryptography Digital Ecosystem Concept

We deploy a Cryptography Digital Ecosystem model in connection with ICT cyber security and cryptography as a central technological solution for ICT security.

Cryptography Digital Ecosystem community cooperation partners are bound together by purposeful action, ensuring a higher level of cyber security in the environment, introduction of safer cryptography tools in the economy, and intensified replacement of classic cryptography solutions with post-quantum cryptography (PQC) secure tools.

We will distinguish three layers in the concept:

- Operational objectives layer: cybersecurity, cryptography
- Community and cooperation partners: research institutions, industry, cryptography use case, certification and accreditation standardization institutions (OSI, ETSI, NIST etc.), university education programs, technology producers (QKD, QRNG, chips, software)
- Ecosystem deployment orchestration and attracting an ecosystem partner layer: CERT, ENISA, legislation, PQC maturity assessment, best practice policy, survey, checklists collection

Cryptography Digital Ecosystem is characterized by the aspects required in [6]: Complexity, Self-organization, Emergence, Co-evolution, Adaptation. The model corresponds to the innovation ecosystem type.

4. Digital Cryptography Ecosystem Deployment Orchestrating

Cryptography digital ecosystem deployment orchestration requires several support activities to promote community partner collaboration. Analyzing the extensive literature and practice on cryptography, the authors identify the pillars of support activities: 1) follow CERT and ENISA recommendations, 2) follow standardization organizations ETSI, NIST requirements in cryptography, 3) follow and implement new innovative cryptography solutions, including technology mail stones as Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), Post-Quantum Cryptography (PQC) solutions etc. We recommend to provide a maturity test of system readiness to PQC.

4.1. CERT, ENISA Recommendations Deployment Pillar

A computer emergency response team CERT (CERT or CSIRT with small differences) is a trademarked term to monitor and track security incidents in the country, industry or corporate networks. CERT units are networked for mutual coordinated cooperation, for example, in networks and cooperation partnerships such as the CSIRTs Network (CNW) (https://csirtsnetwork.eu), the European Government CSIRTs Group (EGC) (https://egc-group.org), FIRST (https://www.first.org), Trusted Introducer (https://www.trusted-introducer.org), EU ENISA, the EU Agency for Cybersecurity (https://www.enisa.europa.eu) , and the NATO Computer Incident Response Capability (NCIRC) as a part of the NATO Communications and Information Agency (see: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf).

Practically every member state of the European Union has one or more CERT units. CERT units promote information technology (IT) security solutions, including cryptography technology applications. The activity of CERT is a big umbrella for the development of cryptographic tasks and solutions for the cryptography digital ecosystem deployment.

ENISA, the EU Agency for Cybersecurity analyses the situation with cyber security in EU countries, evaluates technological solutions, including cryptography, and provides innovative recommendations for EU member states. Since 2013, ENISA has published an annual document “ENISA THREAT LANDSCAPE” [7] with summary news about the cyber security situation. In a similar way, the authors of the manual want to establish an overview of the use of cryptography as the main solution for ensuring cyber security in Latvia. ENISA has accumulated rich experience in the preparation of relevant documents over many years and has formalised the document preparation process by preparing a methodology intended for similar action [8].

ENISA provides recommendations for policy makers, risk managers and information security professionals in the field of cyber security up-to-date, but we focus more on one of the components of the implementation of cyber capability – cryptography.

4.2. Maturity Assessment Model

The concept of digital maturity is often used in ICT management. It is the basis of a methodology that aims to help people assess the effectiveness in a digital transformation process. Collapse of classical cryptography in the quantum computing era prompts us to hastily switch to quantum secure cryptography, and therefore we recommend to perform a maturity test for the readiness of the system for PQC solutions, for example, [9,10].

4.3. Institutional Cryptography Strategy, Risk Management, Good Practice Crypto Policy Development Pillar

Support for cryptography digital ecosystem deployment orchestration can be provided by institutional cryptography strategy, risk management, and good practice crypto policy [11].

In order to write a high-quality policy and good practice document, it is necessary to be familiar with cryptography, the experience gained in other institutions and their recommendations, the results of numerous questionnaires and monitoring of the situation.

4.4. Pillar of Checklists Approach as a Proof of Quality of Ecosystem Maturity Assessment Model

The Wikipedia explains the typical use of the term Checklist, "A checklist is a form of job support used to reduce failure by compensating for potential limitations of human memory and attention. This helps ensure consistency and completeness in the task. A basic example is am 'to-do list'. The primary task of the checklist is to document the task and compare the documentation" [12].

The checklists approach is described in our manual for cryptography deployment as a tool to qualitatively implement necessary tasks.

Checklists help for Cryptography digital ecosystem deployment composition and decomposition, modelling organizational decision processes.

Checklists have been developed by analytically gathering the relevance (in the authors' point of view) of documents available in the public space appropriately to crypto solutions and their implementation, requirements methodology and other issues.

The Digital Ecosystem Framework is organized around three separate, overlapping pillars: Digital Society, Rights, and Governance. And it encompasses four cross-cutting topics: Inclusion, Cybersecurity, Emerging technologies, and Geopolitical Positioning.

Each checklist contains questions that cover cryptography application tasks and available WEB links to such specific checklists in detail. By thoroughly analyzing the public literature, the employee responsible for the cryptosystem implementation can adapt checklists to his needs and include the necessary tasks and executable topics.

Checklists cover tasks presented in the manual:

- Compliance of the cryptography solution with standards (ETSI, ISO, NIST)
- Cryptography solution accreditation tasks
- Migration of cryptographic solutions to post-quantum cryptography (PQC)
- Cryptographic solutions evaluation according to PQC Maturity Assessment Model
- Institutions crypto policy good practice evaluation
- Software security requirements checklist

- Checkpoint Microsoft Azure Security Best Practices checklist
- The University of Toronto checklists for cryptography and information classification and protection
- SANS, Amazon (AWS), Microsoft (Azure), Google (GCP) security checklists,
- Security checklists for system requirements
- Checklist for the cryptography designer at the institution
- Checklist when hiring a cryptography specialist.

Conceptually very close are a terms checklist, survey, and questionnaire. The questionnaire and the checklist applies to clarifying the situation on the subject under consideration, but the purpose of the checklist is to assess the current reality, while a questionnaire often gives clarity on the future [13], for example, discussion [14].

4.5. Digital Cryptography Ecosystem Deployment Manual

Cryptography covers an important and very broad spectrum of issues and tasks and cryptography digital ecosystem deployment must cover this wide range of tasks. To describe the existing situation in Latvia we developed the manual for Cryptography digital ecosystem deployment. www.lumii.lv uses a specific "Point of View" (POW) (users POW, industry POW, technology POW) according to the definition of Point of View terms in [15] and [16].

The content of the manual is described in the manner of "State of the Art" [17].

Ecosystem deployment and cryptography applications are expanding and improving the quality of practical ICT security. The manual contains recommended methodologies for Cryptography Digital Ecosystem deployment implementers.

In preparing the manual, we have widely used ENISA's recommendations and publications, however, the content presentation style is more general, based on the above-mentioned approaches – changing the content presentation style from "landscape" to "point of view" and "state of the art".

The considered manual does not follow the use of a checklist or questionnaire: it describes only a task/topic that can be transformed into either a questionnaire or a checklist.

5. Cryptography Digital Ecosystem Deployment Model Rationale

For justification, we will cite three arguments that indicate the practical possibility of Cryptography Digital Ecosystem deployment: geographic area (Latvia in EU), adequate level of knowledge in the cryptography field and available financing.

We define the digital ecosystem vertically (ecosystem status, in our case: EU level or national level) and horizontally – defining the boundaries that include technology (cryptography, in our case: ICT security and cryptography as practical instrument for security needs).

We will base the compliance model of the digital ecosystem of cryptography on the following features:

- Cryptography is widely used technology. With the growing importance of cyber security, the widespread use of cryptography in technological platforms and security solutions is predicted;

- There are several arguments to include cryptography in General Purpose Technology line [18]; Compliance of the cryptography solution with standards (ETSI, ISO, NIST) Migration of cryptographic solutions to post-quantum cryptography (PQC)
- Quantum cryptography as an EU development strategy has high priority, defined in the European Union (EU) Digital Europe Programme 2021–2027 (DEP) [19] and justification for sufficient knowledge and available financing source: QKD National Backbone Deployment and IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS) Secure Priority.

We deploy a Cryptography Digital Ecosystem model in connection with ICT cyber security and cryptography as a central technological solution for ICT security.

In order to intensify the practical implementation of quantum cryptography in the country, we propose to base the development strategy on the Cryptography Digital Ecosystem concept.

5.1. QKD National Backbone Deployment

The objective of the Digital Europe Program (DEP) [19] is to ensure the wide use of digital technologies across the economy and society. DEP provides funding for projects in supercomputing, artificial intelligence, cybersecurity and advanced digital skills and the aim of the program is to connect digital technology research and market deployment. In this paper we will focus on cryptography, quantum cryptography and quantum communications as one of the methods to insure cyber security.

In 2019, EU countries signed a declaration to explore together and deploy a quantum communication infrastructure (QCI) within the initiative EuroQCI.

In 2022, the EU announced three Calls as part of the initiative:

- The digital renaissance and the global digital ecosystem. DIGITAL-2021-QCI-01-DEPLOY-NATIONAL
- Create a European industrial ecosystem for secure QCI technologies and systems, DIGITAL-2021-QCI-01-INDUSTRIAL
- Coordinate the first deployment of national EuroQCI projects and prepare the large-scale QKD testing and certification infrastructure, DIGITAL-2021-QCI-01-EUROQCI-QKD.

In the EuroQCI initiative, partners from Latvia (LVRTC, IMCS UL, TET and VASES) have presented Project LATQN and received an EU grant for development of a national QKD (Quantum Key Distribution) network backbone as secure/restricted networking part and deployment of public QKD backbone part.

5.2. IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS) Secure Priority

The European Commission has set up a Strategic Forum for Important Projects of Common European Interest (IPCEI). IPCEI is an EU initiative of DEP and represents a very important contribution to economic growth, jobs and competitiveness for the Union’s industry and economy. IPCEI aims is to create a common cloud and edge infrastructure and its associated smart services for the future. IMCS UL's interest is

directed at secure Cloud solutions, based on cryptography/quantum cryptography solutions.

The digital ecosystem concept is strongly related to society's needs. Development of national level digital ecosystem frame limits are influenced by society, the political and economic system of the EU.

The development of a large digital ecosystem depends on decisions made and funding tenders announced. As a rule, the creation of a national digital system is based on several (many) participations in tenders, funding sources and several technological components. We believe that the national ecosystem is created iteratively and is actually based on the evaluation of the EU society in advance, taking into account political and economic decisions.

6. Conclusions

1. The authors move forward the Cryptography national digital ecosystem deployment concept. In the view of the authors, this corresponds to DEP on QKD national backbone and international connectivity of these backbones.
2. An example of a national ecosystem readiness concept has been developed.
3. Recommended Cryptography digital Ecosystem deployment concepts that must be analysed: networking protocols, QKD networking, QKD in OSI layer protocols, research priorities, crypto in universities education curricula, PQC maturity, ecosystem deployment strategy and risks, standardisation rolling plan, checklists [20].
4. The checklists approach is offered to ensure efficient and high-quality ecosystem deployment, helping to ensure consistency and completeness of necessary tasks.

Acknowledgements
Publication vas supported from European Regional Development Fund project "Applications of quantum cryptography devices and software solutions in computational infrastructure framework in Latvia", Project ID number 1.1.1.1/20/A/106 (01.06.2021–30.11.2023).

References

[1] Tansley, A. G. "The Use and Abuse of Vegetational Concepts and Terms." Ecology 16, No. 3 (1935): 284–307. https://doi.org/10.2307/1930070.
[2] Matthias Koch, Daniel Krohmer, Matthias Naab, Dominik Rost, Marcus Trapp, A matter of definition: Criteria for digital ecosystems, Digital Business, Volume 2, Issue 2, 2022, ISSN 2666-9544, https://www.sciencedirect.com/science/article/pii/S2666954422000072.
[3] Peltoniemi, M. & Vuori, E. (2005). Business ecosystem as the new approach to complex adaptive business environments. Seppä, M. Hannula, A.M. Järvelin, J. Kujala, M. Ruohonen & T. Tiainen (Eds.), Frontiers of e-Business Research 2004, Conference Proceedings, Tampere, Finland (pp. 267–281) http://www.ebrc.fi
[4] Ziye Wang, Qingying Zhang, Higher-Education Ecosystem Construction and Innovative Talents Cultivating, Open Journal of Social Sciences, Vol. 7 No. 3, 2019, https://www.scirp.org/journal/paperinformation.aspx?paperid=91072.
[5] Carly Fiorina, "The Digital Ecosystem", World Resources Institute Conference: Creating Digital Dividends Seattle, Washington, October 16, 2000, http://www.hp.com/hpinfo/execteam/speeches/fiorina/ceo_worldres_00.html, Accessed 29.09.2022
[6] Järvihaavisto, Ulriikka & Riitta, Smeds. (2018). From Technology Platform to Innovation Ecosystem. Academy of Management Proceedings. 2018.

[7] ENISA THREAT LANDSCAPE 2021. April 2020 to mid-July 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape- 2021, last accessed 29.08.2022
[8] ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY, JULY 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology/@@download/fullReport, last accessed 30.08.2022
[9] Post Quantum Crypto Survey, DigiCert, 2019, https://www.digicert.com/content/dam/digicert/pdfs/2019-digicert-post-quantum-crypto-survey-report-en.pdf
[10] Post-Quantum Cryptography (PQC) Maturity Model, DigiCert, 2020 https://www.digicert.com/content/dam/digicert/pdfs/post-quantum-cryptography-maturity-model-whitepaper-en.pdf, last accessed 29.08.2022
[11] OECD, Recommendation of the Council concerning Guidelines for Cryptography Policy, OECD/LEGAL/0289, 2022, https://legalinstruments.oecd.org/public/doc/115/115.en.pdf, last accessed 29.08.2022
[12] Checklist, Wikipedia, https://en.wikipedia.org/wiki/Checklist, last accessed 29.08.2022
[13] Anna Georgiadou, Spiros Mouzakitis, and Dimitris Askounis, Designing a Cyber-Security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis, International Journal of Network Security & Its Applications (IJNSA) Vol. 13, No. 1, January 2021
[14] Ali A. Naeem. What is the scientific difference between the checklist and the questionnaire? When and why is each tool used? https://www.researchgate.net/post/What-is-the-scientific-difference-between-the-checklist-and-the-questionnaire, last accessed 29.08.2022
[15] Complete Guide to Different Types of Point of View: Examples of Point of View in Writing, Written by MasterClass, Last updated: Sep 2, 2021 https://www.masterclass.com/articles/complete-guide-to-point-of-view-in-writing-definitions-and-examples, last accessed 29.08.2022
[16] Point of view Definition & Meaning – Merriam-Webster, https://www.merriam-webster.com/words-at-play/point-of-view-first-second-third-person-difference), last accessed 29.08.2022
[17] State of the art Definition & Meaning – Merriam-Webster), https://www.merriam-webster.com/dictionary/state%20of%20the%20art, last accessed 29.08.2022
[18] Richard Lipsey, Kenneth I. Carlaw, Clifford T. Bekhar (2005). Economic Transformations: General Purpose Technologies and Long-Term Economic Growth. Oxford University Press. pp. 131-218. ISBN 978-0-19-928564-8.
[19] The Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme, Accessed 29.08.2022
[20] Marco Lucamarini, Andrew Shields, Romain Alléaume, Christopher Chunnilall, Ivo Pietro Degiovanni, Marco Gramegna, Atilla Hasekioglu, Bruno Huttner, Rupesh Kumar, Andrew Lord, Norbert Lütkenhaus, Vadim Makarov, Vicente Martin, Alan Mink, Momtchil Peev, Masahide Sasaki, Alastair Sinclair, Tim Spiller, Martin Ward, Catherine White, Zhiliang Yuan, Implementation Security of Quantum Cryptography, Introduction, challenges, solutions, ETSI White Paper No. 27, First edition – July 2018, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf