EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CRYPTOGRAPHIC PRODUCTS AND SERVICES MARKET ANALYSIS

VERSION 1.0

AUGUST 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please send an email to market@enisa.europa.eu.
For media enquiries about this paper, please send an email to press@enisa.europa.eu.

AUTHORS

Sofia-Roxana Banica, Louis Marinos, Polyxeni Mitsaki, Greta Nasi, Corina Pascu, Aljosa Pasic, Bart Preneel, Silvia Portesi ([1])

ACKNOWLEDGEMENTS

ENISA would like to thank the following persons.

- The members and observers of the ENISA ad hoc working group on cybersecurity market analysis for their guidance and feedback during the various phases of this work and review of this document.
- The ENISA National Liaison Officers Network, the ENISA Advisory Group, the European Cybersecurity Certification Group and Stakeholder Cybersecurity Certification Group for their input during the scoping phase and for their feedback during the validation phase of this report.
- The Bocconi University team, in particular Professor Greta Nasi, Benedetta Julia Burston, Federica Stefanizzi, Martina Gianola and Leonardo Saveri for their support with the data analysis and data visualisation.
- All ENISA colleagues who provided input during various phases of this report and/or reviewed this report.

[1] The authors are listed in alphabetical order by surname.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources, including external websites, referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-670-5 doi: 10.2824/249233

TABLE OF CONTENTS

1. INTRODUCTION 8

1.1. AIM 8

1.2. TARGET AUDIENCE 9

1.3. CONTEXT IN LAW AND POLICY 10

1.4. RELATED WORK AT THE LEVEL OF EU MEMBER STATES 11

1.5. SCOPING AND KEY COMPONENTS OF THE ANALYSIS 14

1.6. DATA COLLECTION 17

1.6.1.MARKET INFORMATION OUTSIDE THE SCOPE OF THIS ANALYSIS 18

1.7. STRUCTURE OF THIS REPORT 19

1.8. USE OF THE RESULTS AND THE DATA 19

2. CHARACTERISTICS OF THE CRYPTOGRAPHIC PRODUCTS/SERVICE ECOSYSTEM 20

2.1. STRUCTURING CRYPTOGRAPHIC PRODUCT CHARACTERISTICS 21

2.2. STANDARDISATION 24

2.3. CRYPTOGRAPHY MARKET STAKEHOLDER TYPES 25

2.4. CRYPTOGRAPHIC PRODUCTS AND SERVICES 26

2.5. CRYPTOGRAPHIC REQUIREMENTS 29

2.6. CYBERTHREAT EXPOSURE OF CRYPTOGRAPHIC FUNCTIONS 30

3. DEMOGRAPHICS OF INVOLVED STAKEHOLDER TYPES 34

3.1. OVERVIEW OF DEMOGRAPHICS FOR DEMAND, SUPPLY, RESEARCH AND REGULATORS 34

3.1.1. Demand 34
3.1.2. Supply 36
3.1.3. Research 38
3.1.4. Regulators 39

3.2. FOCUS ON SMES 40

4. CRYPTOGRAPHIC PRODUCTS USAGE PATTERNS 42

4.1. USAGE PATTERNS ON THE DEMAND SIDE 42

4.2. PRODUCT PATTERNS ON THE SUPPLY SIDE 45

4.3. SUPPLIER PRODUCT/SERVICE DEVELOPMENT PRACTICES 49

5. THREATS, REQUIREMENTS AND CAPABILITIES 51

5.1. REQUIREMENTS FOR CRYPTOGRAPHIC PRODUCTS AND SERVICES 51

5.2. CYBERTHREAT EXPOSURE OF CRYPTOGRAPHIC PRODUCTS AND SERVICES 54

5.3. CAPABILITY LEVELS OF DEMAND AND SUPPLY SIDES 56

5.3.1. Demand-side capabilities 56
5.3.2. Supply-side capabilities 59

6. ROLE OF CERTIFICATION, REGULATION AND STANDARDISATION 61

6.1. ROLE OF REGULATORS 61

6.1.1. Findings focusing on EU regulation 61
6.1.2. Findings focusing on non-EU regulation 64

6.2. FINDINGS FOR CERTIFICATION 65

6.3. FINDINGS FOR STANDARDISATION 67

6.4. PROJECTIONS ON THE EU CRYPTOGRAPHY MARKET 69

7. CRYPTOGRAPHIC PRODUCTS MARKET AND RESEARCH TRENDS 71

7.1. CRYPTOGRAPHIC PRODUCTS MARKET EVOLUTION 71

7.2. CRYPTOGRAPHIC PRODUCTS DRIVERS AND BARRIERS 73

7.2.1. Market drivers 73
7.2.2. Market barriers 75

7.3. CRYPTOGRAPHY RESEARCH AND INNOVATION IDEAS 78

8. CONCLUDING REMARKS 80

8.1. MAIN MARKET CHARACTERISTICS AND TRENDS 80

8.2. MAIN GAPS 82

8.3. MAIN BARRIERS 82

8.4. MAIN POINTS WITH REGULATORY RELEVANCE 83

8.5. MAIN RESEARCH TRENDS 84

1. ANNEX A: LEGAL AND POLICY FRAMEWORK – EXAMPLES OF INSTRUMENTS 86

2. ANNEX B: CRYPTOGRAPHIC PRODUCTS MARKET ANALYSIS QUESTIONNAIRES 91

3. ANNEX C: LIST OF CRYPTOGRAPHY STANDARDS 97

4. ANNEX D: ABBREVIATIONS 100

EXECUTIVE SUMMARY

This report presents an analysis of the cryptography products and services market in the EU as it has evolved from the point of view of the cybersecurity market under the Cybersecurity Act. This analysis contributes to the implementation of the ENISA's *Single Programming Document 2023–2025* ([2]), in particular Activity 7, Output 7.1., "Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes".

The selection of cryptographic products and services as the focus of this cybersecurity market analysis, which was conducted in 2023, took into account stakeholders' feedback from a survey among ENISA external and internal stakeholders. The criteria used to select this area for analysis included the size, nature and importance of the market, the importance of the market segment for cybersecurity and its relevance to existing and upcoming EU regulatory activities and policy efforts, research and innovation.

For this analysis, ENISA has performed primary research, i.e., a survey involving the main stakeholder types of the cryptography product and service ecosystem by means of dedicated questionnaires. The quantitative information from the survey has been validated/integrated via qualitative information obtained through open-source information and, to further assure quality, internal and external experts, including the members of the ENISA ad hoc working group on cybersecurity market analysis, were involved in the validation of the results. In addition, desk analysis has been carried as well as expert input provided by area experts involved throughout the research and analysis phases.

The overall aim of this market analysis report is to:

- Contribute to understanding the structure of the cryptography market by assessing the size and profile of market players (demand, supply, regulators, research), geographies and sectors of activity, available skills and knowledge available;
- Contribute to understanding the current cryptography products and services landscape by assessing which products are offered and how are they used, what the plans for future product deployments are and how skills and capability are being developed within various stakeholders;
- Support assessing threat exposure and stakeholder cybersecurity requirements by analysing the threat exposure of various cryptographic products and services, understanding incident and vulnerability management methods and the requirements to be fulfilled by products in reducing the level of threat exposure and attack surface;
- Support the role of regulatory and standardisation efforts by assessing the compliance of cryptography products and services to regulation, standardisation and certification efforts;
- Identify cryptography market trends by assessing the directions in which the market is likely to evolve, the perceived market drivers and barriers, and emerging research and innovation themes.

Besides the core part of this report containing the performed analysis and conclusions drawn regarding to the cryptography products and services market, there are some finer aspects of this report that might be useful to a range of audiences, such as threat exposure, cybersecurity

[2] https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025, accessed November 2023.

requirements, questionnaires used, and a list of relevant standards and regulations related to cryptography. This material can feed into the various activities of stakeholders, such as: procurement of cryptography products and services, threat and risk assessment of deployed products and services, surveys in the field of cryptography, and guidelines for relevant observatories.

The main conclusions of this analysis include that:

- cryptography-as-a-service is expected to grow over the next 2–3 years in spite of the perceived complexity on the demand side;
- regulatory compliance was assessed as the top business driver for the supply side;
- the adoption of digital identities by EU Member States is driving the crypto market in that specific area;
- there is a need to set up a centralised EU open-source software (OSS) repository for lightweight crypto libraries;
- there is a need to develop guidance to vendors concerning the integration of OSS components into products, notably internet of things (IoT) ones;
- at research level, privacy-enhancing cryptography (PEC) emerges as the most significant cryptography research theme.

Additional conclusions drawn from the findings of this analysis can be found in Chapter 8.

1. INTRODUCTION

This report presents an analysis of the cryptography products and services market in the EU as it has evolved from the point of view of the cybersecurity market under the Cybersecurity Act. While ENISA has asserted a longstanding presence and a role in the analysis of cryptography concerning cybersecurity past reports can be instrumental to setting the stage and providing a background[3]. Building on ENISA assertions it can be inferred that:

"Cryptography is a vital part of cybersecurity. Security properties such as confidentiality, integrity, authentication and non-repudiation rely on strong cryptographic mechanisms, especially in an always connected, always online world.

In addition, cryptography applications open up new opportunities and markets; digital signatures or online transactions would not be possible without it. Given its importance, cryptography remains a heavily researched field and even finds its way into the headlines. It is also referenced in high level policy and regulatory streams of work."

This report aims to complement past ENISA work items by presenting the results of a cybersecurity market analysis carried out by ENISA in 2023 focusing on cryptographic products and services in the EU.

1.1. AIM

This report addresses the cybersecurity-related properties of cryptographic products and services market offerings, analyses the perceptions of the stakeholders of the cryptography ecosystem, their cybersecurity and business requirements, their needs, and the impact of service deployment towards reduced exposure to cyberthreats. The focal point of this analysis is the current cybersecurity market of cryptographic products and services in the EU. The aim of the report is to contribute to fostering the cybersecurity market in the EU in the meaning of the Cybersecurity Act and within the scope of the role of ENISA therein.

This report seeks to provide information on the cybersecurity market of cryptographic products and services in the EU. It is based on data collected via a survey conducted in 2023 and targeting demand, supply, regulators and research and development organisations; open-source (OS) information has also been used to amend and validate collected data, when necessary. This report has been drawn up with the aim of helping stakeholders better understand this segment of the market, and the opportunities it offers from a cybersecurity standpoint for the purpose of making better-informed decisions.

Stakeholders in this report broadly include entities on both the supply side and the demand side: consumers, consumer organisations and associations, industry, small and medium-size enterprises (SMEs), public authorities and research entities.

While preparing this report, notions such as user requirements, supply capabilities, threats, market trends, market drivers and market barriers were taken into account. The work was carried out following the steps and the activities described in the *ENISA Cybersecurity Market Analysis Framework V2.0* ([4]). This framework was drawn up, validated, and confirmed by ENISA, over the course of 2 years.

[3] https://www.enisa.europa.eu/topics/cryptography, accessed January 2024.
[4] https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0, accessed November 2023.

This current market analysis is the third report in the cybersecurity market series. It was performed by ENISA, leveraging the ENISA market analysis methodology, and has served as an additional thorough test of the framework.

It is of interest to highlight that on the outset the ENISA market analysis methodology is skewed towards market criteria and observations that are of particular interest to cybersecurity experts and reflect a cybersecurity point of view. The decision to rely on cybersecurity-centric criteria to carry out the market analysis was implicitly taken by ENISA when the ENISA market analysis methodology was adopted and was squarely based on the provisions of Article 8 of the Cybersecurity Act.

It follows, that criteria concerning the economic analysis, competition position and strategic analysis pose a lower degree of interest from a purely cybersecurity-oriented perspective and therefore they were not considered since they fall outside the scope of this report.

It is also worth mentioning that the current version of the ENISA cybersecurity market analysis methodology caters to collecting data in the interest of this market analysis report and with a view to providing data feeds to the benefits of the research, innovation and operational cooperation in cybersecurity, and the cybersecurity index work that ENISA carries out, maximising the effect of the investment in this data collection exercise.

Moreover, this analysis helped ENISA increase its maturity level in the performance of cybersecurity market analysis tasks, gain further experience in terms of scoping and structuring a cybersecurity market survey, and perform market stakeholder mobilisation, data sanity checks and validation, with the advantage of enhancing ENISA’s capabilities to transfer collected knowledge in the area to external and internal ENISA stakeholders alike.

1.2. TARGET AUDIENCE

The target audience of this report includes the following.

- **EU institutions, bodies and agencies, and national public authorities, in particular bodies involved in policymaking and regulation** that can use this analysis to better understand supply- and demand-related issues and trends in the cybersecurity market of cryptographic products and services.
- **ENISA stakeholder groups**, such as the European Cybersecurity Certification Group (ECCG), the Stakeholder Cybersecurity Certification Group (SCCG), and the ENISA Advisory Group (AG), for which market intelligence may support their decision-making in prioritising various cybersecurity efforts and spotting market gaps.
- **Industry and cross-sectoral associations** for which this report can be of support in their analysis of market opportunities, trends, challenges and vulnerabilities. Moreover, related standards and regulations listed in the report may be used during the design, implementation, deployment and operation of cryptographic products and services.
- **SMEs** that play an important role in the economy, for instance, by means of innovation potential, flexibility of adaptation to market needs, and deployment of research results, and that can use the analysis to better understand the market needs and trends.
- **Consumer organisations and associations** that can use this analysis to better comprehend the needs and requirements of consumers with regard to cybersecurity products, services and processes, and their prospects in the European cybersecurity market. The information in this report (e.g., on cryptography requirements and threat exposure) can be used in the procurement processes of cryptographic products and services.
- **Critical infrastructure providers** that can be from both the public and the private sectors (e.g., utilities, financial systems and transportation networks) and for which the report can

be of help in taking better decisions on EU v non-EU technologies for highly resilient cryptographic components in their networks.

- **Research and development (R & D) organisations** that can use this analysis to support their assessment of the maturity of existing products and markets and guide the development of new technologies and services.

It is worth noting that the value of the activities carried out to perform this analysis goes beyond the strict content of this report and lies mainly in the fact that an entire market analysis life cycle process was performed. Numerous other side products of this life cycle may also be useful to a variety of stakeholders: scoping information, generated questionnaires, threat assessments, raw data collected, etc. This material bears, among others, a high potential for reuse, re-scoping and adaptation to serve other purposes. Last but not least, by performing a complete market analysis life cycle, ENISA is in the position to transfer this knowledge to concerned and interested parties and/or elaborate on the integration and the analysis use cases with relevant cybersecurity disciplines, thereby creating a win-win situation with a broad policy scope.

1.3. CONTEXT IN LAW AND POLICY

The Cybersecurity Act (CSA) ([5]) states that “ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union” (Article 8(7), CSA) and that “ENISA should develop and maintain a “market observatory” by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides” (recital 42, CSA).

This current analysis has been conducted as an implementation of Output O.7.1 “Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes”, under Activity 7 “Supporting European cybersecurity market and industry” of the ENISA Work Programme 2023 ([6]). Elaborations on the market uptake of cybersecurity products, services and processes contribute toward ENISA’s strategic objectives of a “high level of trust in secure digital solutions” and “empowered and engaged communities across the cybersecurity ecosystem”.

Furthermore, the European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), aim at fostering the European cybersecurity market and building a European cybersecurity community. One of the ECCC’s tasks is to provide “support for the uptake by the market of cybersecurity products, services and processes” (Article 5(2), point (b)(i)(5) of the ECCC founding regulation ([7])). The ECCC will develop and implement, with Member States, industry and the cybersecurity technology community, a common agenda for technology development and its wide deployment in areas of public interest and businesses, particularly SMEs. It follows that ENISA is looking forward to synergising further, beyond the realm of its own stakeholders (i.e., ad hoc working group, ENISA AG, National Liaison Officers Network), to tap into numerous and more voluminous data sources for the purpose of providing more substantiated analyses in the future.

In order to provide the best possible analyses, interpretations and recommendations, ENISA has chosen to limit the collection of data to verified, proven and trustworthy sources. This approach was considered much more effective than accessing numerous sources whose quality cannot necessarily be guaranteed.

[5] https://eur-lex.europa.eu/eli/reg/2019/881/oj, accessed November 2023.

[6] https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025, accessed November 2023.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0887, accessed December 2023.

1.4. RELATED WORK AT THE LEVEL OF EU MEMBER STATES

Member States have performed work related to cryptographic products and services which can be divided into the following categories: regulatory work, certification schemes, provision of good practices, requirements and guidance and cryptographic market analysis.

The main subjects of material developed by Member States are approved cryptographic algorithms, cryptographic primitives and cryptographic mechanisms, along with cryptographic requirements. In some cases, requirements for the use of cryptography in various use cases / sectors with increased security needs are provided (e.g., smart metering, record keeping, networking and telecommunication). Moreover, Member States provide guidelines for the evaluation of cryptographic products and for the regulation of import/export of cryptographic equipment. Table 1 gives an overview of the related work identified for the purpose of this study.

Table 1. Main related outputs at Member States' level in the area of cryptography ([8])

Title	Content	Relevance	Comment
France			
Ordonnance no 2005-1516 Le référentiel général de sécurité (RGS)	Defines rules and recommendations regarding the selection of cryptographic mechanisms and key sizes, recommendations regarding cryptographic key management and recommendations regarding authentication mechanisms.	Guideline for the selection of cryptographic parameters used in various cryptographic functions.	The level of detail of this material is outside the scope of this work.
Law no. 2004-575 on confidence in the digital economy	The supply, import, intra-community transfer and export of cryptology equipment are subject, with certain exceptions, to various control mechanisms. Under the terms of these texts, a company wishing to import or supply a crypto-enabled item on French territory must first make a declaration to the French Cybersecurity Agency (ANSSI). If the item is transferred to another Member State or exported outside Europe, an export	Regulation.	Used within the ENISA survey (as a possible answer).

[8] The list in Table 1 is non-exhaustive. These are the main documents that have been identified and taken into account in this report, when relevant.

	authorisation must also be issued by the agency.		
Germany			
BSI – Crypto Library Botan	An OS cryptographic library provides a secure, clear, controllable and well-documented cryptographic library to increase resistance to side-channel attacks.	Good practice.	Used within the ENISA survey (as a possible answer).
Technical Guideline BSI TR-03153 Security mechanism for electronic record-keeping systems	Security mechanisms for record-keeping devices and infrastructure, aiming at the protection of tax records against manipulation.	Regulation.	Used within the ENISA survey (as a possible answer).
Technical Guideline TR-03116-TS TLS Test Specification	Requirements for conformity tests of transport layer security (TLS) protocol.	Guideline for the evaluation of cryptographic products.	Used within the ENISA survey (as a possible answer).
Technical Guideline TR-03181 for Cryptographic Service Provider	The Cryptographic Service Provider (CSP) is a hardware module that makes cryptographic primitives, algorithms and advanced protocols readily available for secure usage. The guideline describes requirements for the implementation of such modules.	Guideline for implementation of cryptographic primitives.	The level of detail of this material is outside the scope of this work.
BSI-CC-PP-0111-2019 Protection Profile Cryptographic Service Provider light	This protection profile describes the requirements for the development of a software component, i.e., a cryptographic library that is installed and runs on a dedicated	Certification scheme and guidance for the development of compliant software implementing cryptographic primitives.	Used within the ENISA survey (as a possible answer).

	hardware platform, i.e., an embedded system.		
BSI TR-03116 Cryptographic specifications for project of the federal government	Provides a series of documents for the proper use of cryptographic functions/primitives within governmental projects.	Guidance for the implementation of cryptography.	The level of detail of this material is outside the scope of this work.
The Netherlands			
TNO 2022 R10712 EZK Valorisation Chains	This report outlines the valorisation chain of crypto communication, which serves as the foundation for the crypto communication roadmap.	Market analysis report.	Used within ENISA's work as a source for the validation of the observations and conclusions drawn.
Spain			
CCN-STIC 102 Procedure for the evaluation of cryptological products	The cryptological evaluation is responsible for verifying the operation, implementation and analysis of the algorithms used, the security mechanisms and the correct operation of the equipment.	Guidelines for the evaluation of cryptographic products.	Used within the ENISA survey (as a possible answer).
CCN-STIC 221 Cryptographic Mechanisms approved by CCN	Defines the cryptographic algorithms approved by Spain's National Cryptologic Center (CCN) and provides guidance for their parameterisation.	Approved cryptographic algorithms and guidance for their parametrisation.	The level of detail of this material is outside the scope of this work.
CCN-STIC 103 Catalogue of products with cryptological certification, not publicly available	The products approved for the encryption of classified national information or that legally require protection are included in the catalogue of products with cryptological certification.	Approved cryptographic products.	The level of detail of this material is outside the scope of this work.

This material has been taken into account in this report, especially in the context of regulation, certification and standardisation (see Chapter 6). Additional related references with regulatory relevance are also provided in Annex A (see Annex 1).

1.5. SCOPING AND KEY COMPONENTS OF THE ANALYSIS

Performed in accordance with the updated ENISA Cybersecurity Market Analysis Framework (ECSMAF) ([9]), this analysis of the cryptography product market began with a scoping activity.

The objectives of scoping were manifold and included the following.

- To balance the depth and breadth of the analysis by focusing on the relevant cybersecurity market elements according to their importance (i.e., role for the supplier, role for the demand side, level of exposure to threats). The scope of the analysis was defined in consultation with the members of the ENISA ad hoc working group on cybersecurity market analysis, other ENISA stakeholders (ENISA AG and National Liaison Officers Network) and ENISA internal stakeholders.
- To contain the analysis within the available resource boundaries (human and financial) and within the available time, providing sound project stewardship.
- To identify and motivate the data collection method (primary, secondary).
- To identify the groups participating in the validation of the intermediate and final results of the analysis.

In line with the ECSMAF, the focus of the current cybersecurity market analysis has been set to cover the important concerns and perceptions of the various stakeholders of the cryptographic products and services market ecosystem, namely the demand side, the supply side, the regulators and R & D in cryptography.

Detailed descriptions and profiles of these stakeholders can be found in Section 2.3.

The focus of the present cryptographic products and services market analysis is summarised in Table 2. The detailed scoping of the analysis can be found in Annex B.

Table 2. Scoping overview of current market analysis

Scoping criteria group	Scoping criteria
Criteria on the demand side	• **Business impact of product use for demand side** focuses on the role of cryptographic product use in the value-chain. • **Required demand side capability/maturity** focuses on the demand side's level of capability in deploying/managing the purchased cryptographic product. • **Role in threat/risk mitigation** focuses on the role of the cryptographic product in reducing threat exposure and consequently in risk avoidance/mitigation/reduction. • **Demand-side geographies** focuses on the geography of activity of the demand-side, by means of physical presence in various areas through branches.

[9] https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0, accessed November 2023.

Scoping criteria group	Scoping criteria
	• **Demand-side requirements** focuses on demand-side requirements that the procured cryptographic product has to fulfil. • **Gap identification** focuses on the identification of gaps in available cryptographic products. • **Investment plan** focuses on the plan to finance the procurement of a cryptographic product. • **Demand-side company characteristics** focuses on the assessment of generic company data for the demand side. • **Market barriers** focuses on barriers encountered by the demand side in procuring a cryptographic product.
Criteria on the supply side	• **Business impact of product for supplier** focuses on the role of the cryptographic product in comparison to the total business volume (turnover). • **Covered profiles for product deployment** focuses on asserted capabilities on the demand side to deploy/manage the cryptographic product. • **Role in exposure reduction** focuses on the asserted role of the product in reducing threat exposure and consequently risk avoidance/mitigation/reduction. • **Supply-side geographies** focuses on the geography of the physical presence of the supplier through branches. • **Assessment of product requirements** focuses on the method followed by the supplier to identify requirements to be fulfilled by the cryptographic product. • **Known gaps / emerging requirements in the area of cryptography** focuses on any gaps encountered by the surveyed stakeholders in cryptography. • **Supply-side targets** focus on various targets set by the supplier to be achieved via the cryptographic product. • **Supplier company characteristics** focuses on the assessment of generic company data on the supply side. • **Market barriers** focuses on barriers encountered by the demand side in procuring the cryptographic product. • **Identification of “hidden champions” / “unicorns”** focuses on companies and start-ups with products with great innovation potential/value in the area of cryptography.

Scoping criteria group	Scoping criteria
Criteria for R & D organisations	• **Research organisation characteristics** focuses on various characteristics of the research organisation. • **Cryptography research** indicates the main areas of cryptographic research. • **Identification of "hidden champions" / "unicorns"** focuses on known start-ups / deployment actions regarding cryptography products with great innovation potential/value. • **Threats, challenges, incidents** focus on various events, threats and incidents that may impact the market. • **Research drivers and barriers** focuses on various factors facilitating and/or hindering cryptography research.
Criteria for regulatory bodies	• **Standardisation organisation characteristics** focuses on various characteristics of the organisation (including academia and industry). • **Triggers for development** focuses on triggers for the development of cryptographic standards. • **Threats, challenges, incidents** focus on various events, threats and incidents that have been taken into account for the development of new cryptographic standards.

It is logical that the scope of this market analysis determines the content of the survey. The consequences of this scoping decision for the collected and analysed information are discussed hereinafter.

The following elements have been taken into consideration in the market analysis.

- **Collection of stakeholder perspectives on equal or similar issues.** By asking questions about various cybersecurity-related matters of cryptographic products/services to a variety of stakeholder types, their viewpoints can be compared, and various interesting points can be identified (i.e., similarities and gaps in perception, differentiated requirements, various views of relevant threats, etc.). Most of the sections of this analysis present such views in a comparative manner.
- **Emphasis on the cybersecurity details of the offerings.** Instead of looking at generic market figures, the cybersecurity analysis conducted concentrates on the cybersecurity-related properties of cryptographic products and services. This creates a specific angle of analysis that is merely based on the conception and consumption of the cybersecurity characteristics of cryptographic products and services.
- **Emphasis on cybersecurity threats and challenges.** A basic element in the conducted analysis is the ability of cryptographic products and services to reduce exposure to cyberthreats and to help master cybersecurity challenges. By taking into account data on cyberthreat exposure and cybersecurity challenges for cryptographic products and services, we generate a multi-stakeholder perception of the central cybersecurity properties of the analysed cryptographic products and services.
- **Assessment of necessary capabilities, market drivers and barriers.** A number of important market success parameters are also taken into account. Adequate demand-

side capabilities to efficiently deploy the cryptographic product/service is an important adoption criterion. Similarly, market drivers (and its antipode, market barriers) are decisive factors towards achieving market vitalisation and the successful launch of a cryptographic product/service.

It is worth mentioning that the results of the analysis do not include classified information, for obvious reasons. Stakeholders from defence and other authorities with security tasks might be under-represented or not present with their demands and views.

Moreover, we consider consensus mechanisms for blockchain (proof of work, proof of stake, Byzantine fault tolerance) and cryptography to support blockchain applications outside the scope of this report.

The use of cryptographic products and services by criminals or rogue states and the challenges that this represents for law enforcement agencies are topics that also fall outside the scope of this report.

1.6. DATA COLLECTION

Through ENISA stakeholder consultations and past experience with market analysis, it has been decided to perform primary research for the cryptographic products and services market analysis. For this purpose, a survey has been generated, supported by the ENISA ad hoc working group on cybersecurity market analysis and external experts.

ENISA conducted the survey to collect data from the following main stakeholder types.

- **Demand**, which includes the end users of cryptographic products and services.
- **Supply**, which includes suppliers of cryptographic products/services and suppliers of services related to cryptography.
- **Bodies involved in regulation**, which includes those covering regulatory activities in the cryptography market.
- **R & D**, which includes organisations conducting research in cryptography.

The survey was divided into questions targeting the various stakeholders of the cryptographic products/services ecosystem. The survey consisted of around 100 questions in total, for all cryptographic products and services market stakeholder types (i.e. supply, demand, bodies involved in regulation, and R & D).

A survey tool, the EUSurvey ([10]) platform, was used. The survey was anonymous, so no data about the responders was collected, making it impossible to trace the respondents.

Through an ENISA announcement, ca 150 stakeholders interested in participating in the survey were identified (preregistered). While the preregistered individuals came from all over the world, the majority were located or active within the EU. Around 50 responses were submitted via the online survey.

[10] https://ec.europa.eu/eusurvey/home/welcome, accessed November 2023.

Table 3 provides an overview of the data collection process.

Table 3. Overview of survey phases and data collection

Survey phase	Responders	Comment
Announcement of survey		Via the ENISA website, social media and email messages to potential participants
Preregistration	ca 150	Worldwide coverage
Number of respondents to survey	ca 58 (38 %)	Worldwide coverage
Balance among targeted stakeholder types	Supply: (33) 57 % of total Demand: (10) 17 % of total Regulators: (5) 9 % of total R & D: (10) 17 % of total	

The dataset that went into the analysis is considered to be representative thanks to its:

- suitable mix of large and smaller organisations, on both the demand side and the supply side;
- comprehensive coverage of Member States;
- representative reporting on EU regulatory bodies engaging in regulation related to cryptography; and
- broad inclusion of R & D organisations conducting cryptography research.

It is worth mentioning that, for this analysis, ENISA provided assistance to the surveyed organisations. External experts were engaged to help organisations participating in the survey fill in the questionnaires by explaining the content and rationale of the questions. The assistance has been offered alongside over half of the submitted surveys. This support has led to a higher percentage of submissions and a higher quality of collected data. In addition, an analysis of the quality of the data collected via the survey was performed. This included mainly data sanity checks, such as plausibility and data consistency checks.

The quantitative data obtained through the survey have been validated and complemented by means of additional qualitative data obtained through desktop research and input from subject-matter experts from ENISA and externals: the analysed results and conclusions made were compared and integrated with findings from publicly available information and input from experts. As an additional validation step, the analysis and the final conclusion was reviewed by various subject-matter experts, such as contracted external experts and members of the ENISA Advisory Group and of the ENISA ad hoc working group on cybersecurity market analysis.

The number of demand and regulators respondents might be seen as limited. However, the data collected via the survey – which were in any case also complemented by OS information – were of good quality.

1.6.1. Market information outside the scope of this analysis

Given the selected scope of the cryptographic products and services market analysis, we have neither collected economic/financial figures regarding supply and demand in cryptographic products/service nor assessed any of the long-term financial figures and statistics of the relevant market. This is particularly the case for financial data on supplier and end-user market activities and market development statistics; such data include past, present and forthcoming market-value information on suppliers and end users. The collection of such economic figures is a long-term activity, requiring qualitative, long-term data collection. Such activities go beyond our scope, resource availability and planning horizon. There are certainly other activities/organisations that are better suited to perform such long-term tasks, both outside ([11]) and within ENISA ([12]).

1.7. STRUCTURE OF THIS REPORT

The report is structured in such a way that it contains the highlights of the performed market analysis. Its sections contain the most important findings from the performed survey and comprise a synthetic view based on the collected evidence.

The structure of this report is as follows.

- **Chapter 1 "**Introduction"
- **Chapter 2 "**Characteristics of the cryptographic products/services ecosystem"
- **Chapter 3** "Demographics of involved stakeholder types"
- **Chapter 4** "Cryptographic products usage patterns"
- **Chapter 5** "Threats, requirements and capabilities"
- **Chapter 6** "Role of regulation, certification and standardisation"
- **Chapter 7** "Cryptographic products market and research trends"
- **Chapter 8** "Concluding remarks"

It is worth mentioning that the structure of this report has been validated by ENISA stakeholders, such as the ENISA AG, the National Liaison Officers Network and ENISA internal groups working in areas related to the content addressed in this analysis.

1.8. USE OF THE RESULTS AND THE DATA

With the present material, we seek to cover the information needs of the main target group of the report, i.e., all stakeholder types of the cryptographic products and services market ecosystem (see also Section 2.3), thus covering the information needs of the demand and supply sides, regulatory bodies, and R & D organisations. It is assumed that with this information at hand, the needs of Member States and the EU institutions, bodies and agencies will also be covered, as they will be in the position to satisfy their information needs by taking into account the results in all kinds of oversight, guidance and regulatory activities. Should some of these external stakeholders wish to have access to the anonymous raw data collected, they can contact ENISA to submit their request (see contact information at the beginning of this report).

Moreover, the results will be of value to ENISA's internal stakeholders. For example, various ENISA activities in the areas of certification, the cybersecurity index, R & D, cybersecurity investments, cyberthreat analysis, vulnerability management, etc., may use these results, along with raw data from the performed survey, for their own purposes.

[11] https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=Cj0KCQjwmouZBhDSARIsALYcouoE5lzylvOuu6pgJA3ZcVr5TYESo_H1GEciWISu5uf4HnOeNJlW7F0aAhTvEALw_wcB, accessed November 2023.

[12] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-spending-an-analysis-of-investment-dynamics-within-the-eu and https://www.enisa.europa.eu/publications/nis-investments-2023, accessed November 2023.

2.CHARACTERISTICS OF THE CRYPTOGRAPHIC PRODUCTS/SERVICES ECOSYSTEM

When analysing the cryptographic products and services market, it is necessary to envisage/assess their building blocks. This activity aims at defining the main elements found in all the products in scope, thus establishing a basis for correspondences among product characteristics, but also building a common denominator for this highly diversified market segment.

Cryptographic products are key in implementing cybersecurity functions (e.g., cybersecurity controls). Given the scope of ENISA's market analysis – focusing on cybersecurity product properties – in this analysis, the entire spectrum of cryptographic product functionality can be considered as being relevant to cybersecurity. Thus, the present analysis focuses on the entire set of product characteristics of cryptographic products, as opposed to other sectors where the cybersecurity relevance concerns only specific product parts.

Another challenge that needs to be addressed in structuring this market segment relates to the broad variety of cryptographic functions, implementations, architectures/platforms/protocols and standards. The model chosen to structure this area needs to contain common properties of as many cryptographic product variations as possible. In order to achieve this, within this analysis we have concluded that a structuring should be based on:

- cryptographic techniques and controls; and
- a data-centric and application-centric approach.

We selected these cryptographic characteristics as being better suited for a generic structure that transcends cryptographic products. By providing a mapping among these structuring concepts, their interdependencies cover most of the functional characteristics of a vast majority of cryptographic products.

With these considerations in mind, survey questions have been formulated to cover both demand and supply perceptions on:

- the number of functions supported by cryptographic products;
- available services related to the development, production and operation of cryptographic products;
- the common threat exposure of cryptographic products;
- cybersecurity challenges linked to the development, deployment and operation of cryptographic products; and
- cybersecurity controls, technologies and solutions, deployed to deal with threats and challenges of cryptographic products.

The development and adoption of emerging technologies, such as IoT, 5G and AI, but also the pace of digital transformation, have contributed to an even faster evolution and adoption of cryptography and consequently of cryptographic products available on the market.

In this analysis, the ecosystem perspectives are targeted through a number of stakeholder views (see also Section 2.3).

As a **final note**, we would like to highlight that the cryptographic functionality today is a commodity: many devices are delivered with built-in cryptographic hardware support and/or cryptographic software libraries.

- All high-end Intel, Advanced Micro Devices, Inc. (AMD) and advanced reduced instruction set computer (RISC) machine (ARM) processors have built-in support for Advanced Encryption Standard (AES) and Galois/Counter Mode (GCM), while many low-end processors offer support for AES.
- Most hard drives have built-in hardware AES encryption functionality.
- Smart cards and some IoT processors offer a cryptographic coprocessor for a range of algorithms (triple data encryption algorithm (3-DES), AES, Rivest–Shamir–Adleman (RSA), elliptic-curve cryptography (ECC).

This implies that some cryptographic functions – and to the extent of this analysis, cryptographic products – are an integral part of the design and are not marked separately. An eventual added value of such cryptographic functions may be achieved through the management of the cryptographic functionality, specifically by means of key management services. As an example, most cloud services have built-in cryptographic functionality available, and it is possible for users to utilise hardware security modules (HSMs) in the cloud, when they wish to use it to encrypt their data.

2.1. STRUCTURING CRYPTOGRAPHIC PRODUCT CHARACTERISTICS

If we zoom in on the security functions that are implemented using specific cryptographic techniques/controls, we can distinguish among techniques and controls to protect data and applications.

Firstly, we consider cryptographic techniques/controls to protect valuable assets (data, applications). These techniques/controls are listed and briefly described below ([13]).

- **Data authentication**. This service combines the concept of data origin authentication (the entity that wrote the data is authenticated) and data integrity (the data have not been modified). This goal can be achieved with message authentication code (MAC) algorithms and digital signatures. The advantage of a digital signature is that the recipient can verify the authenticity based on authenticated public information (there is no need to share a prior secret with the sender).
- **Data confidentiality**. The main technique used for this is encryption; special variants include format-preserving encryption (FPE), masking and tokenisation.
- **Authenticated encryption**. In practice, data confidentiality needs to be combined with data authenticity. The cryptographic technique that supports this combination is authenticated encryption. It occurs frequently that one wants to leave part of the data (e.g., the packet header or the filename) unencrypted. The corresponding cryptographic service is called authenticated encryption with associated data.
- **Non-repudiation of origin and receipt**. Data authentication is a service between two mutually trusting parties. If one of the parties is not trustworthy, a third party is needed to settle disputes. The most efficient way to achieve this is through digital signatures: in this case, non-repudiation of origin can be achieved while neither the recipient nor the third party needs to share a previously established secret key with the originator of the message; similarly, non-repudiation of receipt can be achieved without sharing a previously established secret key with the recipient.

[13] The techniques/controls mentioned in this list are arranged according to their frequency of use (i.e., popularity). More frequently used controls precede controls that are more specialised in nature.

- **Fully homomorphic encryption (FHE)**. Allows a third party to perform computations on encrypted data, without having access to the data in clear. The result can be decrypted by the data owner or another party with access to the private key.
- **Partially homomorphic encryption (PHE)**. **"**[W]here only a single operation can be performed on cipher text, for example, addition or multiplication" ([14]).
- **Somewhat homomorphic encryption (SHE)**. "[S]imilar to partially homomorphic encryption but with a limitation on the number of operations instead of the types of operations" ([15]).
- **Functional encryption (FE)**. A public-key encryption scheme that allows decryption keys to be created that on their turn allow the recipient to compute only a function of the plaintext; examples include identity-based encryption (the secret key is derived from the name of the recipient) and attribute-based encryption (parts of the secret key are related to attributes of the recipient or the ciphertext). FE allows policy decisions to be enforced through key management.
- **Multi-party computation (MPC)**. Allows two or more parties to jointly compute a function of data by computing on shares of these data, without any party learning any information on the data except perhaps for the result of the computation. In the strongest model, this result can be achieved even if all but one of the computing parties are corrupt. In addition, one can have the property that one can prove that the result has been computed correctly (verifiable outsourcing of computation). For some specific problems, such as private set intersection (each party holds a list of people and the parties want to compute the intersection without leaking any information regarding the people not in the intersection), more efficient protocols can be conceived.
- **Other cryptographic tools**. There is a broad range of other tools, including zero-knowledge protocols (ZKPs), commitments, oblivious transfer, verifiable computation, and blind signatures. These tools can be used for more advanced applications.

Cryptographic services move the protection of data or transactions to the protection of cryptographic keys. This necessitates the use of **key management** techniques ([16]) for key generation and associated random number generator (RNG) purposes, and for controlling the distribution, use and update of cryptographic keys, which consists of the following functions:

- key **generation** and **associated RNG** services;
- key **registration** and **certification** services including digital certificate management and revocation;
- key **establishment** and **distribution** services;
- key **storage** and **recovery** services, including secret sharing; and
- key **deletion** services.

These services can be very complex because they cover a broad range of systems (cloud, on-premise, infrastructure, applications) and because they are typically integrated with the identity and access management system of the organisation.

Next, we consider an approach based on the **protection goals** of cryptography, by considering **data** and **applications** as the main asset to be protected. This results of a **data-centric and application-centric** view of cryptography.

The **data-centric** view of cryptography covers the following.

[14] https://www.enisa.europa.eu/publications/data-protection-engineering, p. 14, accessed January 2024.
[15] https://www.enisa.europa.eu/publications/data-protection-engineering, p. 14, accessed January 2024.
[16] See also NIST Special Publication 800-57 Part 2.
Revision 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf, accessed November 2023.

- **Securing data at rest**. This corresponds to securely storing data, which means that only authorised entities can access the data (confidentiality) and only authorised entities can write the data, while designated parties can verify the authenticity (data authentication).
- **Securing data in transit**. This corresponds to secure communications.
- **Secure data while computations are being performed on the data or while computing on encrypted data**. This includes a broad range of techniques, such as MPC, FHE, attribute-based encryption (ABE), private set intersection and verifiable computing.

In the **application-centric** view, we consider cryptographic protocols in which two or more parties try to achieve a specific goal beyond protecting abstract data.

- **Entity authentication**. In this setting, one party wants assurance that another party identity corresponds to the identity claimed. More generally, one party may want to verify one or more attributes of the other party – these attributes can be age range, country in which the person is born, vaccination status, membership of an organisation, etc.
- **Attestation**. One party wants assurance that another party is in possession of a device that has been produced by a manufacturer according to a certain specification. One example of such a protocol is the attestation for trusted platform modules (TPMs).
- **Electronic transactions**. A large number of online interactions make use of payment transaction protocols such as those by Maestro and EMV; proprietary systems exist on top of cards such as Mifare from NXP and for many mobile payment apps.
- **Electronic voting**. These are among the most complex and subtle protocols to design as there are two hard-to-reconcile requirements: integrity for the outcome of the vote (only legitimate voters should be able to vote and anyone should be able to verify that the vote is cast as intended, recorded as cast and counted as recorded) and the anonymity of the voters; in addition, some protection against coercion of voters or vote buying may be required. Last but not least, to ensure that people with disabilities can vote, with all the related guarantees.

The intersection of these structuring elements establishes their mutual relationships and visualises their interplay in covering the properties of products on the market segment of encryption. Although not exhaustive, Table 3 gives an overview of the main relationships between cryptography goals and cryptographic services (see Table 4).

Table 4. Main relationships between cryptography goals and cryptographic services – an overview

	Data authentication	Data confidentiality	Authenticated encryption (with associated data)	Non-repudiation of origin or receipt	FHE	MPC	Other building blocks (e.g., ZKP)	Key management services
Data at rest	√	√	√	√				√
Data in transit	√	√	√	√				√
Computing on encrypted data					√	√	√	√

Entity Authentication	√							√
Attestation	√						√	√
Electronic Transactions	√	√	√	√				√
Electronic voting	√	√	√	√		√	√	√

2.2. STANDARDISATION

Compliance to cryptography and encryption standards is a significant element of existing market offerings for all kinds of available products and services. Aiming at fulfilling security requirements for various uses, compliance to standards is key for the placement of cryptographic products on the market, for interoperability and builds the basis for the certification of offerings. The standardisation is based on standard protocols that have been specified for each protection goal.

In this section, an overview of relevant standards is provided, in particular regarding protocols that can be used to achieve the protection goals mentioned in Section 2.1. It is worth mentioning that standards for the application-centric areas of computing on encrypted data (techniques such as FHE or MPC) and electronic voting are not provided, as relevant standardisation is still underway.

The coverage of standardisation is as follows.

- **Securing data at rest** (secure storage). In this case there are few standards but there is cryptographic protection (e.g., encryption, data authentication) at the hard disk level (using xor–encrypt–xor (XEX) for example), file level, database level and data field level (FPE).
- **Securing data in transit** (secure communications). Today most modern standards offer authenticated encryption with the associated data service in combination with a key establishment service.
    - *Physical layer encryption*. This includes quantum key distribution (QKD) for QKD deployments ([17]) and physical layer security protocols. Standardisation is present at a very early stage. It is also clear that both will only be applicable to niche markets for the next decade, as they offer security services that are dependent on the physical channel, which is not compatible with open services on an open infrastructure.
    - *Link level encryption*. 2G/3G/4G, WiFi, Bluetooth, Zigbee. While 2G offers only encryption, the others offer authenticated encryption. The more recent version of these protocols offers solid protection. However, link-level encryption is a basic service that is typically limited to the wireless part of the channel: while this is the most vulnerable part, the cryptographic protection is terminated at the access point.
    - *Network-level encryption*. Internet Protocol Security (IPsec). This service is based on authenticated encryption with associated data. There are several variants, including gateway to gateway, user device to gateway and user device to user device.

[17] https://www.etsi.org/technologies/quantum-key-distribution, accessed November 2023.

  - *Transport layer encryption.* TLS, Secure Shell (SSH). The recent versions of these protocols offer authenticated encryption with associated data. While TLS (originally called secure sockets layer - SSL) was originally designed for web traffic, it quickly became the most widely used protocol for other applications as well (e.g., access to email, VPN). The free certification services offered by Let's Encrypt since 2016 have given TLS a further boost.
- **Email and messaging**.
  - *Email*. Pretty Good Privacy, GNU Privacy Guard (GPG), secure/multipurpose internet mail extensions (S/MIME). While there are several standards, the large-scale deployment of email protection between organisations has never happened due to interoperability issues, privacy concerns and usability issues. It should be noted that the TPM devices (cf. infra) are increasingly supporting the protection of application keys such as those for email.
  - *Messaging*. The Internet Engineering Task Force (IETF's) messaging layer security (MLS) protocol, the signal protocol. Unlike in email, end-to-end protection is built into most messaging apps. The Signal protocol offers advanced security features such as forward secrecy, post-compromise security and deniability. Several apps have made proprietary implementations. The IETF has developed the MLS specification that includes security for multi-recipient messages.
- **Entity authentication** (these services are typically integrated with access control and authorisation). RFC 6238 (time-based one-time password (TOTP), HMAC-based one-time password (HOTP)), Kerberos, FIDO, Radius. There is a broad range of standard protocols that support this core enterprise functionality. Another important set of standards is the International Civil Aviation Organization (ICAO)standards for e-passports.
- **Attestation**. The Trusted Computing Group TCGdefined the TPM specification that has been published as an international standard.
- **Electronic transactions**. EMV (credit card). The EMV specifications are used to secure payment transactions in billions of devices and tens of millions of terminals. Another important player in this area is the GlobalPlatform that delivers standards for digital services and devices, such as payment services and smart cards.

2.3. CRYPTOGRAPHY MARKET STAKEHOLDER TYPES

Table 5. Cryptography market stakeholder types assumed for the purpose of the present market analysis

Stakeholder type	Description (by sector)	Examples
Demand side: public and private sector end users / consumers	Cryptographic products and services are used by almost all types of organisations and users. Public organisations, for example, authenticate users of digitalised government services, support electronic signatures, encrypt sensitive data and communication channels, etc. Private organisations use cryptography to secure transactions, authenticate users, sign electronic documents, encrypt communication channels, secure sensitive data, secure end devices, etc. End users use cryptographic functions to secure authentication, communication and stored data.	Examples are: • government • financial services • telecommunications • media industry (digital rights management (DRM) / digital asset management (DAM)) • information technology (IT) companies • manufacturing • health care • critical infrastructure

		• transportation
Supply cryptographic product developers	Suppliers of cryptographic products provide hardware, software (including libraries) and services, whereas all delivered components implement various cryptographic functions. They are usually developed by implementing cryptographic standards and/or sectoral specifications. Suppliers may be private organisations or OS groups delivering cryptographic libraries and publicly available services.	Examples are: • companies offering digital signature services • key management solutions providers • issuers of digital certificates and other public key infrastructure (PKI) services • industry players developing products for encryption • OSS community
Supply of services related to cryptographic products	A number of organisations provide services to cryptographic product developers, mainly related to the specification, testing of components/functions and attestation of compliance to standards. Such organisations act in support of cryptographic product developers with the purpose of achieving the desired assurance level of their products.	Examples are: • testing laboratories • conformity assessment bodes (CABs) • cryptography specification and development • major cloud players offer extensive cryptographic services
Research	Public and private organisations – both national and international – performing research on various aspects of cryptography, including next-generation encryption, weaknesses of existing techniques and the maintenance of testing capabilities.	Examples are: • private organisations conducting research, including industry • universities, research institutions
Regulators, national competent bodies	National or international entities / public authorities / institutions that – directly or indirectly – exert regulatory influence on cryptography.	Examples are: • European Commission • Member State regulators • data protection authorities • standardisation organisations • sectoral associations

In this market analysis, the two groups related to these suppliers are covered with a single questionnaire (and thus a single collection of data points). Professional associations representing both supply and demand (e.g., the European Cyber Security Organisation (ECSO), Digital Europe) have been enrolled in this analysis by means of supply and demand questionnaires, depending on the activities of their member organisations.

2.4. CRYPTOGRAPHIC PRODUCTS AND SERVICES

This section provides a **non-exhaustive** list of products and services developed to cover the cybersecurity requirements and needs of both supply and demand sides. This information is presented in tabular form according to the composition of various services/functions/products, in a similar manner as the ECSMAF ([18]) (see Table 6).

Table 6. Various cybersecurity-related added-value services related to cryptography

Value-added service group	Types of products and services	Comments
Cryptographic hardware	Cryptographic co-processors	
	Smart cards	
	Secure login tokens	
	Secure elements	
	TPMs	
	Hardware-based secure execution environments	
	Hard disk encryption	
	Hardware VPNs	
	Hardware security module	
	Secure communication devices	
	Networking/routing	
Software-based cryptographic products	Cryptographic libraries (open-source)	https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries; https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html
	User authentication	
	Key management products: keys, certificates and tokens for various purposes	
	Digital signature	
	MAC algorithms	
	Digital assessment management	
	Network access control	https://www.spiceworks.com/it-security/network-security/articles/top-10-network-access-control-software-solutions/
	Software VPNs	

[18] https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf/@@download/fullReport, accessed November 2023.

Value-added service group	Types of products and services	Comments
	Database encryption	
	Embedded smart cards (eSIM, eUICC)	
	Software-based secure execution environments	
	Whitebox cryptography	
	Authenticated encryption	
Cryptography-as-a-service	Certification authority services	
	Digital signature services	
	Smart card personalisation services	
	Cloud cryptographic services	
	Procurement platforms services	
	User identification and authentication management services	
	Data masking, tokenisation services	
	FHE/SHE/FE services	
	Key-management-as-a-service (e.g., the generation, establishment, distribution, destruction, revocation and recovery of keys)	
Advanced cryptographic techniques and protocols	Verifiable computation	
	Privacy through FHE	
	ABE	
	ZKP	
	Electronic voting	
	Electronic transactions	
Cryptographic product/service specification, testing and certification	Product certification services	
	Specification of cryptographic functions	
	Testing of cryptographic functions, products and services	

2.5. CRYPTOGRAPHIC REQUIREMENTS

In this section, some generic requirements regarding cryptography are presented. These requirements are assumed to be subject to fulfilment for various cryptographic products and services and are of concern for both supply and demand sides. The purpose of these requirements is to assess the ability of cryptographic products and services to reduce the exposure to related cyberthreats (see also Section 2.6). Thought not completely overlap free, the fulfilment of these requirements will be checked for the number and strength of available security measures taken in all phases of the cryptographic products/services life cycle (i.e., from design to deployment and operation).

1. **Agility of cryptographic algorithm/protocol, including secure negotiation**. "A cryptosystem is considered crypto-agile if it can be replaced by another cryptosystem, for example in terms of cryptographic algorithms, key lengths, key generation schemes or technical implementation, without having to make significant changes to the rest of the overall system" ([19]).
2. **Correct binding with application (e.g., authentication of cryptographic function calls)**. Binding using cryptographic techniques allows for the creation of a secure connection between two communicating entities (i.e., applications), by using authentication function calls ([20]). In this case, applications must have access to an application programming interface that uses security functions.
3. **Correct implementation (functional correctness)**. Cryptographic algorithms usually undergo a functional correctness test, i.e., a mathematical proof of function of the calculations ([21]). When implemented via an IT component, the final product/process needs to undergo a verification of the implementation. The verification is a test that the implementation implements the functions in a correct manner, without introducing any unforeseen weaknesses ([22]).
4. **Effective and correct key management and backup**. Keys used by a cryptographic system are generated, managed, stored, recovered and destroyed in a secure manner.
5. **Protection of implementation against key extraction/modification**. Throughout their entire life cycle, keys need to be protected against extraction and modification threats (see also threats 18–21 in Section 2.6).
6. **Resistance of implementation against side-channel attacks**. The cryptographic product needs to provide countermeasures to defend against side-channel attacks (see also threat 19 in Section 2.6), for example ([23]).
7. **Resistance of implementation against active attacks such as faults and combined attacks**. The cryptographic product needs to provide countermeasures to defend against combined attacks (see also threats 9 and 13 in Section 2.6) ([24]).
8. **Secure key/randomness generation**. In order to have strong/secure keys, the cryptographic product/service uses key generation based on random numbers, hence the result of RNG being unpredictable ([25]).
9. **Security proof for algorithm or protocol**. The security of the cryptographic algorithm and cryptographic protocol being used are formally validated, by means of a mathematical reduction proof ([26]).

[19] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile, accessed January 2024.
[20] https://datatracker.ietf.org/doc/html/rfc5056#page-6, accessed November 2023.
[21] https://silo.tips/download/functional-correctness-proofs-of-encryption-algorithms, accessed November 2023.
[22] https://core.ac.uk/download/pdf/55615014.pdf, accessed November 2023.
[23] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Seitenkanalresistenz/seitenkanalresistenz_node.html, accessed November 2023.
[24] https://link.springer.com/chapter/10.1007/978-3-642-14712-8_19, accessed November 2023.
[25] https://cryptobook.nakov.com/secure-random-generators, accessed November 2023.
[26] https://theses.hal.science/tel-03150443/document, accessed November 2023.

10. **Adequacy of crypto mechanisms to cover emerging threats, including quantum attacks**. Although state-of-the-art cryptographic functions are mathematically well studied and validated, their resistance to quantum computing attacks (towards decrypting encrypted messages) is also important. New, quantum-safe techniques have been developed to resist such attacks ([27]) ([28])·, thus being quantum-safe.
11. **Update of algorithms and functions**. The cryptographic product/function provides means to securely perform updates, by confirming the integrity/authenticity of proposed changes and validating the performance of the update action.
12. **Use of standards**. The cryptographic product/service has been developed based on internationally recognised standards.

It should be noted that these requirements are generic, sector-independent requirements to be fulfilled by cryptographic products/functions.

This list can be used as a list of requirements for general purpose cryptographic functions, but it must be noted that specific requirements also exist.

Although in this analysis we cannot go into detail about the specific requirements, it must be noted that in addition to the generic requirements, there are also specific EU requirements (either from EU or national regulation) regarding specifications, standards, conditions of procurement, conditions of use, export control and conditions of validation/certification, be it for the general market or for the protection of sensitive information (considering classified where necessary). Moreover, specific, sectoral requirements may cover additional cryptographic characteristics and properties.

2.6. CYBERTHREAT EXPOSURE OF CRYPTOGRAPHIC FUNCTIONS

Cryptographic products and services are exposed to a number of cyberthreats. For the current analysis, we have collected a number of cyberthreats, as they are used within various security assessments and/or evaluation of products towards product and service certifications. Though these cyberthreats are known within expert groups working on the evaluation of cryptographic products and there is presently an incentive by the Senior Officials Group Information System Security (SOG-IS) community to publish elements of attention to avoid common pitfalls in the implementation of crypto ([29]), threat information platforms do not provide much information. This could be due to the scarcity of incidents in cryptographic products and services, the high effort required to exploit these threats or the fact that some of these attacks are theoretical. Moreover, it must be noted that, at least for potential cyberthreats uncovered during evaluation under a certification scheme, the evaluation results are subject to an NDA between manufacturer and evaluation body, are sometimes even classified, and reported to the certification body only.

Below we present a comprehensive collection of cyberthreat types assumed within the present market analysis.

1. **Abuse of weaknesses in key management tools and procedures**. Weaknesses of key management tools are often related to the age of keys, quality of keys, incorrect use of keys, and inappropriate storage and security controls. In such cases, key management tools may expose stored keys to attacks ([30]).

[27] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms, accessed November 2023.
[28] https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, accessed November 2023.
[29] https://www.sogis.eu/documents/cc/crypto/202203-hep-draft16.pdf, accessed on January 2024.
[30] https://www.cryptomathic.com/news-events/blog/cryptographic-key-management-the-risks-and-mitigations, accessed November 2023.

2. **Abuse of design weaknesses**. This is a threat inherent to design weaknesses of the design of cryptographic products and services (including all used components). Often, such attacks refer to one or more of the following cyberthreats ([31]).
3. **Abuse of an insecure RNG, pseudo-RNG or key generation algorithm**. This threat emerges when the RNG has weakness, the pseudo-random key generation algorithm is not cryptographically strong or the key generation algorithm has flaws. In this case, attackers may be able to recover cryptographic keys and gain access to privileged data or functionality ([32]).
4. **Abuse of weak or obsolete cryptography**. Weak or obsolete (outdated) cryptographic functions may be easily attacked, as their strength, used key material, design, etc. is outdated.
5. **Abuse of weak implementation/deployment practices**. Improper deployment and maintenance of cryptographic products and services may introduce weaknesses that can lead to successful attacks for a variety of reasons, such as: weak updates, weak integration into application environments, weak protection of protocols, weak key management.
6. **Downgrade attacks targeting algorithm, version**. Such attacks force the use of a low security mode of supported cryptographic algorithms/versions (also known as “version rollback attack” or a “bidding-down attack.”). Consequently, the product or service can be successfully attacked, exposing details that can lead to a successful attack on the full version of the algorithm ([33]).
7. **Exploit incorrect integration of cryptography with application (e.g., change data between user interface and cryptographic module)**. Improper integration of cryptography and applications may introduce weaknesses that may allow an attacker to compromise a system, gain access to sensitive data or manipulate data ([34]).
8. **Exploit key reuse**. If a key is used for a long period (referred to as cryptoperiod) then the risk emerges, that in case of a key compromise, the cryptographic protection is reduced. The National Institute of Standards and Technology (NIST) states “[a] suitably defined cryptoperiod limits the amount of exposure if a single key is compromised, limits the time available for attempts to penetrate physical, procedural, and logical access mechanisms that protect a key from unauthorised disclosure, limits the period within which information may be compromised by inadvertent disclosure of keying material to unauthorised entities, and limits the time available for computationally intensive cryptanalytic attacks” ([35]).
9. **Forging of authenticated data or plaintext/ciphertext forgery**. A forgery attack is based on sending a crafted cyphertext to be decrypted by a cryptographic module. “In particular, an attacker needs the decrypted version of their own ciphertext. If successful at that, the attacker can … decrypt other parties’ messages and forge new ones” ([36]). In addition to chosen-ciphertext attacks, there are other kinds of attacks, for example, chosen plaintext attacks, depending on the cryptographic scheme.
10. **Impersonation through bugs in implementation of protocol logic**. Despite the fact that cryptographic protocols are considered to maintain the security level of the entire cryptographic process, in some implementations, flaws at the level of protocol have led to successful attacks (e.g., heartbleed vulnerabilities in OpenSSL and seed leaking in the Juniper Network) ([37]).
11. **Impersonation, spoofing, modifying data, modifying keys, denial of service**. This threat consists of a combination of modification attacks based on spoofing and

[31] https://ieeexplore.ieee.org/abstract/document/708447, accessed November 2023.
[32] https://cwe.mitre.org/data/definitions/338.html, accessed November 2023.
[33] https://www.crowdstrike.com/cybersecurity-101/attack-types/downgrade-attacks/, accessed November 2023.
[34] https://dl.acm.org/doi/abs/10.1145/2814228.2814229, accessed November 2023.
[35] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, accessed November 2023.
[36] https://www.baeldung.com/cs/chosen-ciphertext-attack, accessed November 2023.
[37] https://yaogroup.cs.vt.edu/papers/Sazzadur_TDSC.pdf, accessed November 2023.

impersonation. Amending the content of messages in the network, modifying information stored in data files and changing programs in order to have them perform differently are some of the methods to implement such attacks ([38]). This threat assembles quite different types of attacks, some of them also mentioned under other cyberthreats, like key modification by attack on key storage or backup mechanism and key modification through fault attacks or memory overwrites.

12. **Key modification by attack on key storage or backup mechanism**. Improper key storage and key backup practices may lead to keys being exposed to unauthorised access, modification or loss ([39]).
13. **Key modification through fault attacks or memory overwrites**. "Memory fault attacks, inducing errors in computations, have been an ever-evolving threat to cryptographic schemes since their discovery for cryptography … the software-based rowhammer attack put forward by Kim et al. … (ISCA 2014) enabled fault attacks also through malicious software running on the same host machine" ([40]).
14. **Loss of cryptographic keys**. This threat is merely the impact from the exploitation of a variety of threats included in this list.
15. **Malicious software to modify or gain access to user management data and cryptographic functions/services**. Malware threatens stored or used key material, in particular during computations performed by software. Malware can lead to the modification or theft of secret keys during their usage by software ([41]).
16. **Abuse of cryptographic systems misconfiguration**. Just as in any software/hardware system, the abuse of misconfigurations is a common attack vector that targets cryptographic products and services ([42]).
17. **Misuse of the key generation function / weak key generation**. Weak ciphers are those encryption algorithms vulnerable to attack, often as a result of a key being of insufficient length ([43]).
18. **Physical manipulation in order to derive, disclose and misuse services**. Physical attacks to security (cryptographic) modules is a common attack vector that is materialised through access to the device performing the cryptographic computations, including management of secret keys. They may include "physically tampering with the hardware (HW); modifying it to remove security layers, adding additional unintended functionality, or physically replacing the device altogether with a backdoored copy" ([44]).
19. **Side-channel attacks**. Side-channel attacks in cryptography are based on additional/collateral information collection regarding the way of functioning of an algorithm or a protocol, as opposed to attacks seeking weaknesses in their design ([45]).
20. **Spoofing or phishing abusing user login with secure cryptographic mechanism and abuse of login for a different application or service (terrorist/mafia fraud)**. This threat is abused by relay-attacks to identification and authentication systems by making the verifier believe that the prover is in its close vicinity ([46]).
21. **Supply chain attack (lack of vigilance over the current encryption threat landscape and machine identity management strategy)**. Through the value-chain involved in the production of (HW) cryptography devices (e.g., HSMs), vulnerabilities

[38] https://security.stackexchange.com/questions/46704/is-there-an-attack-that-can-modify-ciphertext-while-still-allowing-it-to-be-decr, accessed November 2023.
[39] https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html#key-storage, accessed November 2023.
[40] https://eprint.iacr.org/2019/1053.pdf, accessed November 2023.
[41] https://apps.dtic.mil/sti/pdfs/ADA535981.pdf, accessed November 2023.
[42] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a, accessed November 2023.
[43] https://knowledge-base.secureflag.com/vulnerabilities/broken_cryptography/weak_cipher_vulnerability.html, accessed November 2023.
[44] https://www.ledger.com/blog/understanding_risk, access November 2023.
[45] https://www.sciencedirect.com/topics/computer-science/side-channel-attack, accessed November 2023.
[46] https://www.researchgate.net/publication/220833760_The_Swiss-knife_RFID_distance_bounding_protocol, accessed November 2023.

can be intentionally inserted into various components of the design. These can be then abused by the threat agent ([47]).

22. **Technical failure / malfunction**. Technical failures and malfunctions of cryptographic products may disclose used secrets (keys) and details of the algorithms used. This information can be used to subsequently attack similar components ([48]).

To conclude, it should be stated that these threats are not without overlap. This threat list might be useful as a checklist of potential threat exposure of cryptographic products and services and can be used in threat/risk assessments and evaluations of products/services towards available measures for the reduction of exposure to these threats and risk mitigation. It may be useful to make a reduced list by focusing on a specific application and/or implementation.

[47] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, accessed November 2023.
[48] https://crashtest-security.com/owasp-cryptographic-failures/, accessed November 2023.

3. DEMOGRAPHICS OF INVOLVED STAKEHOLDER TYPES

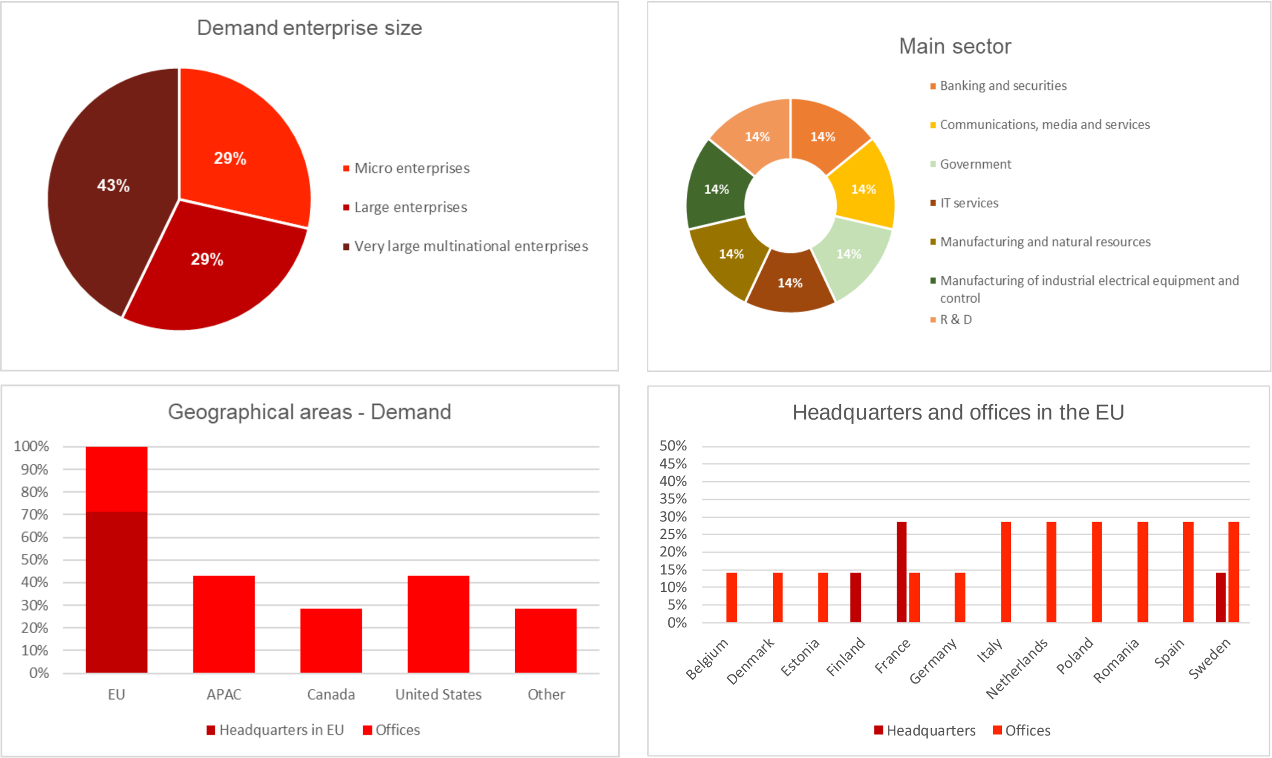
This chapter provides an overview of the demographics of the entities that participated in the survey. Besides a compound presentation of the demographics of participants (demand), suppliers, research organisations and regulatory entities, in this chapter we also provide an overview of relevant characteristics of small and medium-sized enterprises (SMEs) engaged in the supply of cryptographic products and services. The special focus on SMEs is motivated by the importance of the role of SMEs in the economy by means of innovation potential, flexibility of adaptation to market needs, deployment of research results, incubation and skill levels.

Nonetheless, large organisations play an important role in the cryptography market: due to the complexity of developing and deploying large scale cryptographic systems and the increased maintenance lifecycle (over 10 years), big companies have a significant influence on the national developments in the cryptographic domain.

3.1. OVERVIEW OF DEMOGRAPHICS FOR DEMAND, SUPPLY, RESEARCH AND REGULATORS

3.1.1. Demand

Figure 1. Main demographic information for demand-side organisations

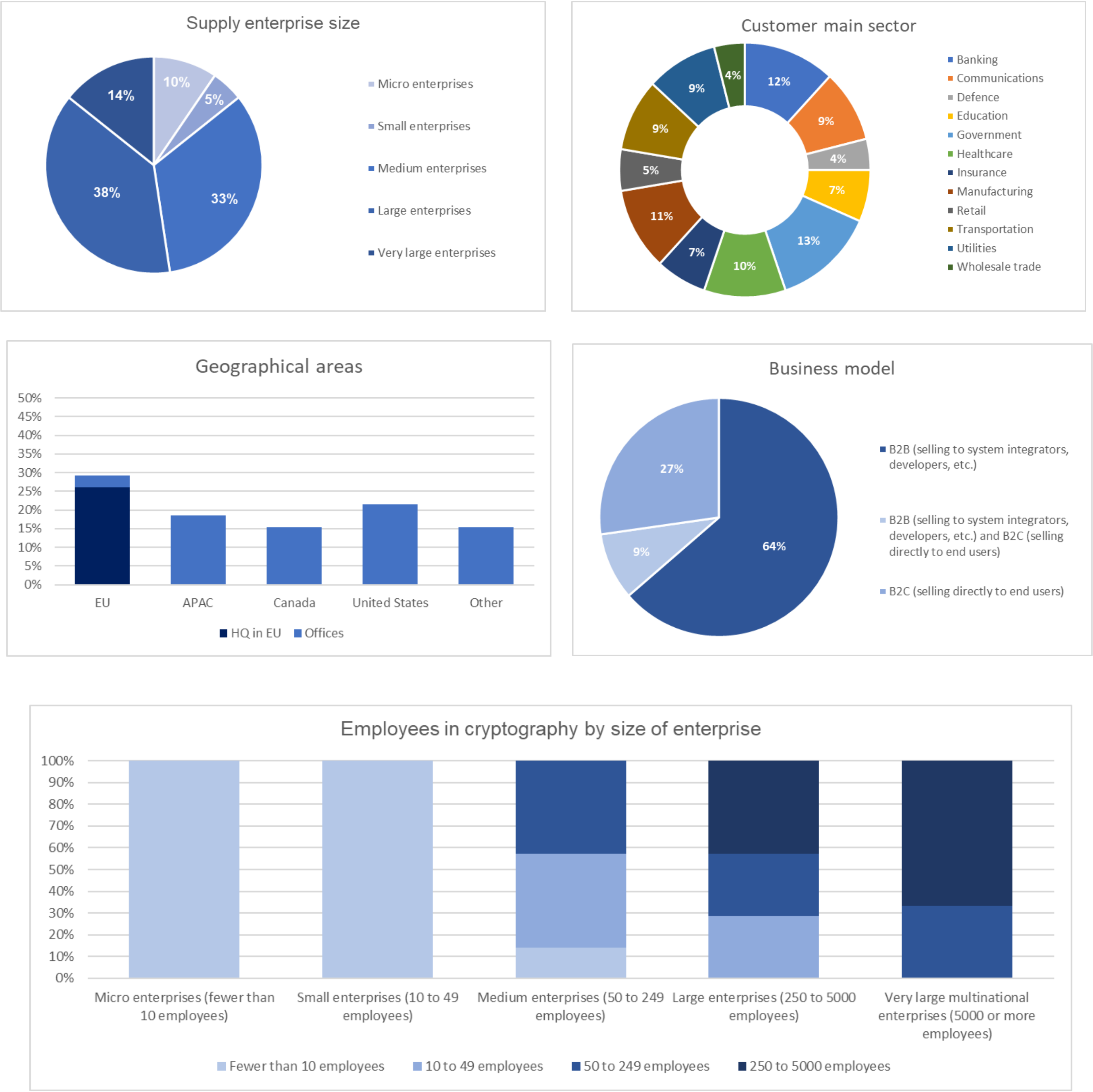


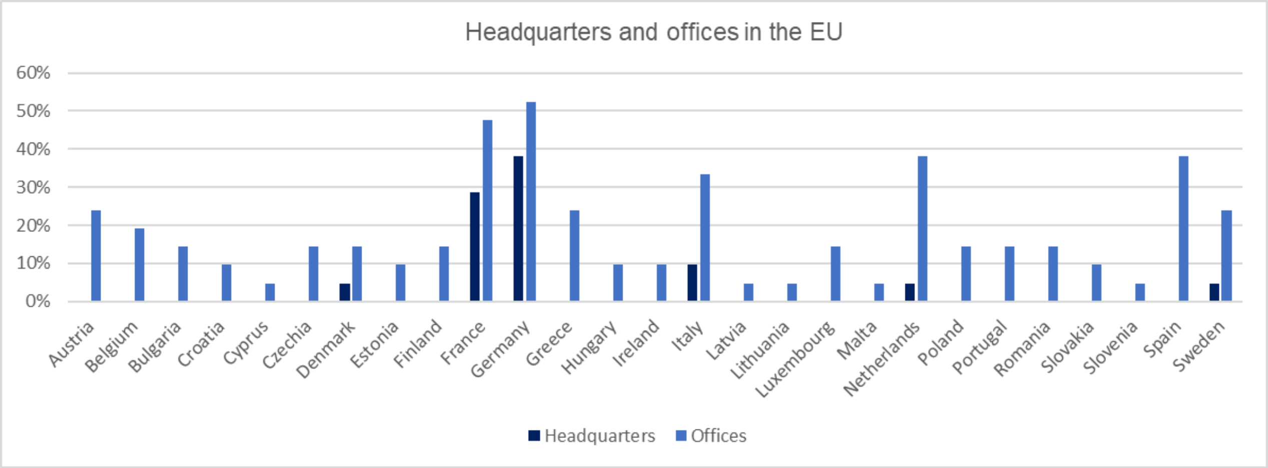
Observations drawn from demand demographics

- The respondents from the demand side belong to the critical infrastructure (banking, governments, IT services, telecommunication, manufacturing) and education/research sectors. Over half of them are multinational companies, located in Europe.
- The high response rate of large organisations is indicative for the concentration of economic capacity within established and sizable organisations. It is evident that such organisations have the critical mass, financial resources and valuable assets to protect, and hence an interest in investing in cryptographic products and services.
- Geographically, the demand-side respondents have headquarters and offices in Europe, with a concentration in: France, Germany, Italy, the Netherlands, Poland, Romania, Spain and Sweden. This concentration of offices in these Member States suggests a regional focal point for business operations.
- 40 % of respondents are located in the EU, but not all critical infrastructure sectors are represented. This might raise a need to create awareness and increase the interest in using cryptographic products and services within other sectors.

3.1.2. Supply

Figure 2. Main demographic information for supply-side organisations





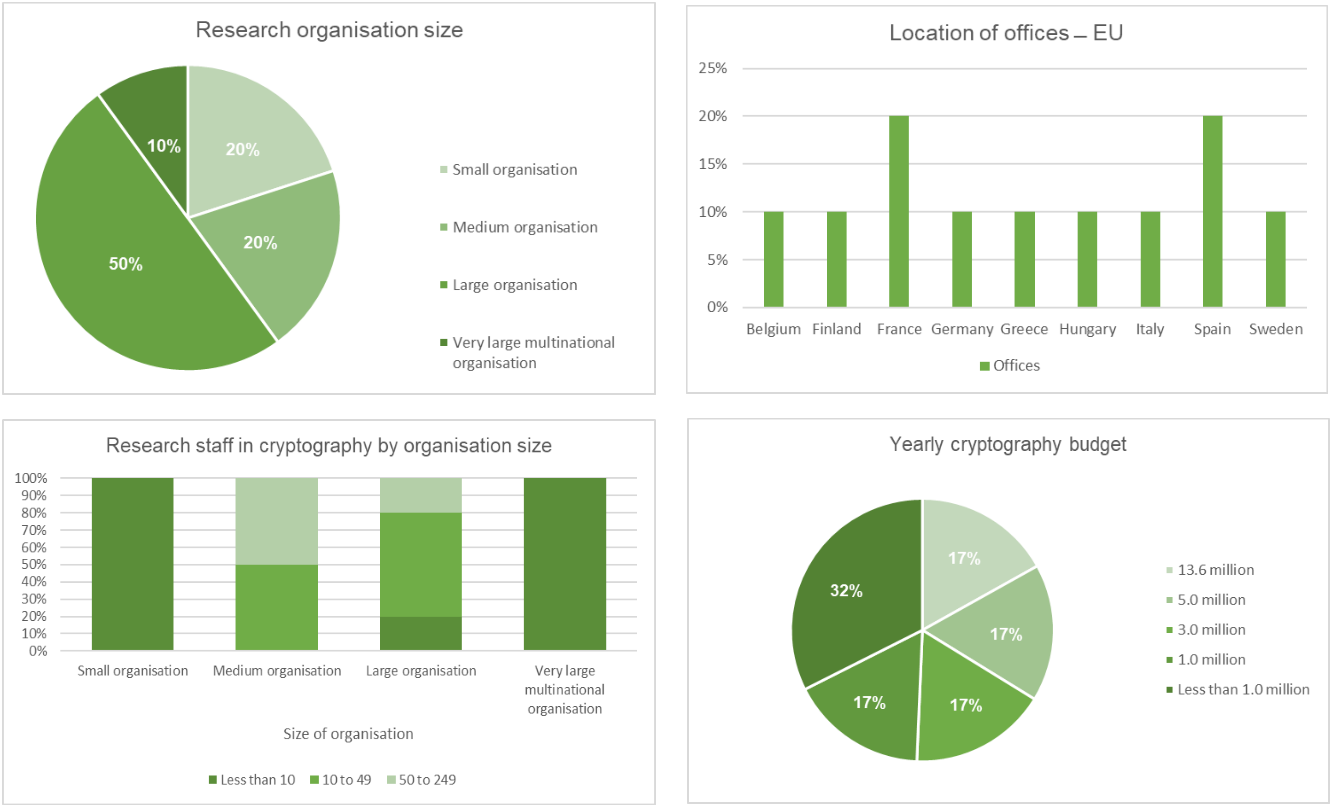
Observations drawn from supply demographics

- An overwhelming 86 % of businesses are found to operate in the B2B sector, underscoring the prevalence of inter-business transactions in the area of cryptographic products and services.
- The majority of enterprises identified in the survey fall within the medium and large categories, pointing towards a landscape dominated by established and sizable businesses. According to testimonies of cryptography experts, in cryptography there is a barrier for microenterprises to transition into SMEs. Moreover, companies of this size tend to be taken over by bigger market players, with the aim of acquiring innovation / additional cryptography skills.
- The EU emerges as a significant hub, hosting most of the surveyed offices, with a notable presence also observed in the United States.
- Within the EU, Germany stands out with the highest number of headquarters and offices, showcasing its pivotal role in the cryptography business supply chain. Moreover, it seems that Member States topping the gross domestic product per capita statistics ([49]), but also sovereignty index ([50]), host headquarters of companies engaging in cryptography. France, Italy and Spain are also preferred destination countries for several companies operating in the EU market.
- Very large multinational companies (over 5 000 employees) and large enterprises (over 250 employees) have established legal entities in some Member States, by increasing the development of cryptographic skills in the EU market.
- The benefits and risks for the EU single market arising from companies outside the EU, such as osmosis of skills, market penetration levels, technological dependencies and exposure to cyberthreats, require a continuous observation and assessment of the cryptographic market. This could help balance benefits and risks.
- It is remarkable that the ratio of cryptography experts to the total number of employees is rather high. This is indicative for the high level of specialisation of the suppliers in dedicated skills for the development of cryptographic products and services.

[49] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=GDP_per_capita,_consumption_per_capita_and_price_level_indices, accessed November 2023.
[50] https://ecfr.eu/special/sovereignty-index/, accessed November 2023.

3.1.3. Research

Figure 3. Main demographic information for research organisations

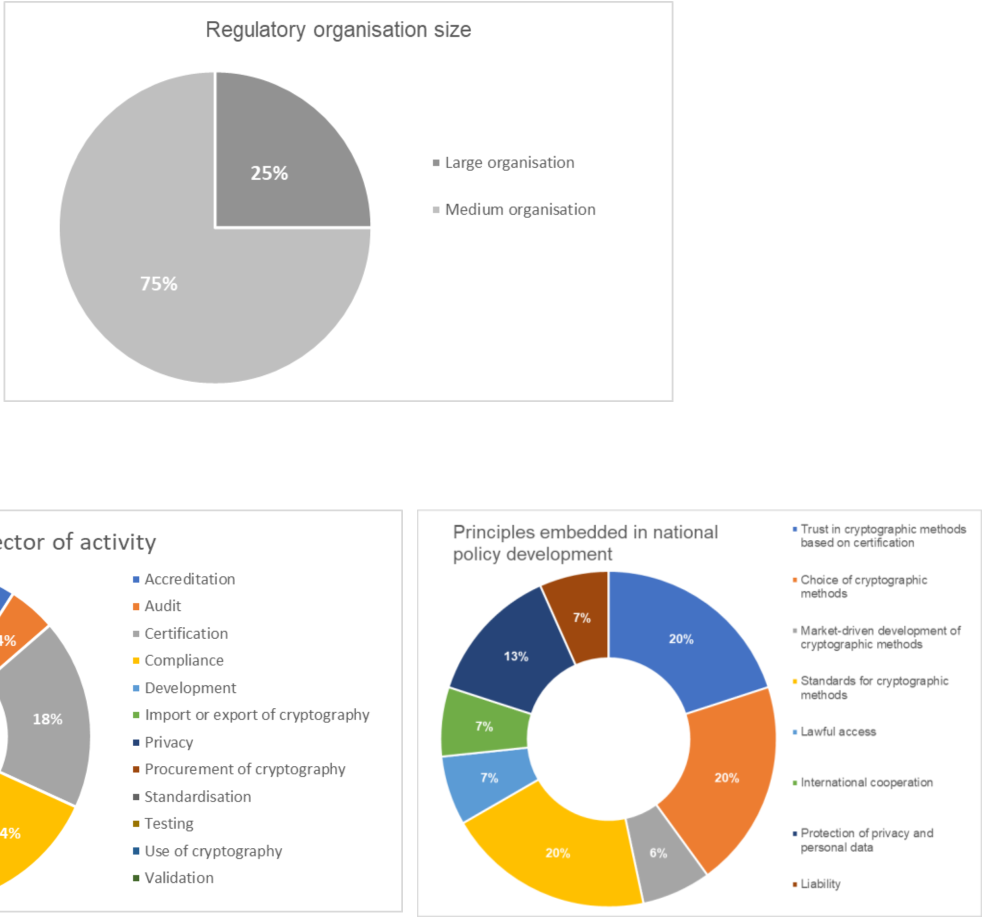


Observations drawn from research demographics

- Cryptography research is dominated by large and very large multinational organisations (ca 60 %), while SMEs make up ca 40 %. Interestingly, the latter produce a significantly higher number of scientific publications, which is indicative of their specialisation and efficiency.
- While some significant research players are outside the EU (Norway, United Kingdom), the trend observed on the supply side is reflected in cryptography research: some research organisations with a significant number of dedicated staff and publications are located in France, Germany and Italy, while Belgium seems to have the most active research organisation as regards the number of publications per year.
- Budget-wise, cryptography consumes on average ca 14 % of the research budget. Most of the cryptography staff (from 50 to over 250 employees) is found in medium to large research organisations, with a percentage ranging from ca 100 % in medium and 80 % in large research organisations that participated in the survey. This, on the other hand, can indicate that medium-sized organisations are specialised in cryptography research, whilst larger size firms are more diversified and cryptography may be just one of their product lines.

3.1.4. Regulators

Figure 4. Main demographic information for regulatory organisations



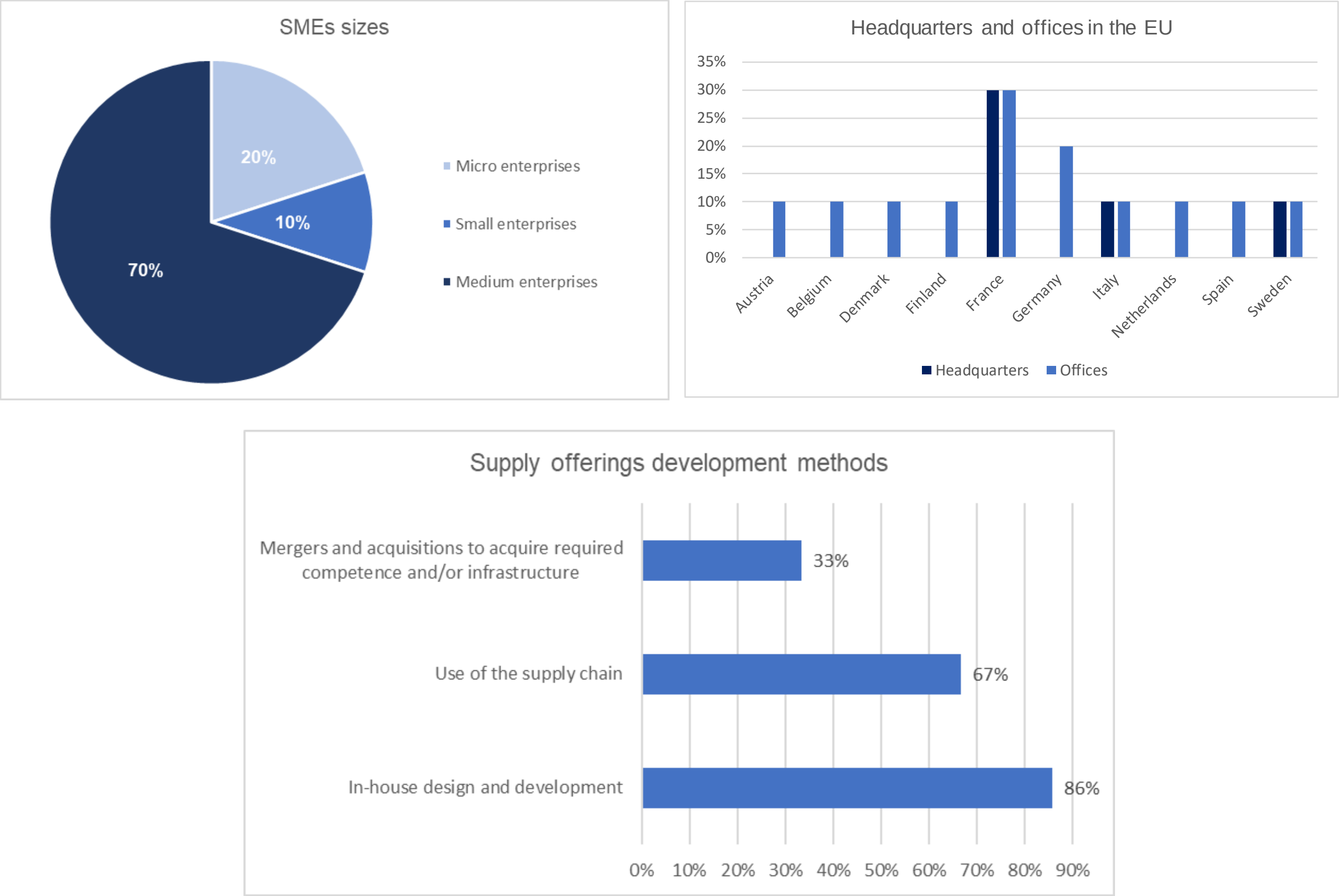
Observations drawn from regulator demographics

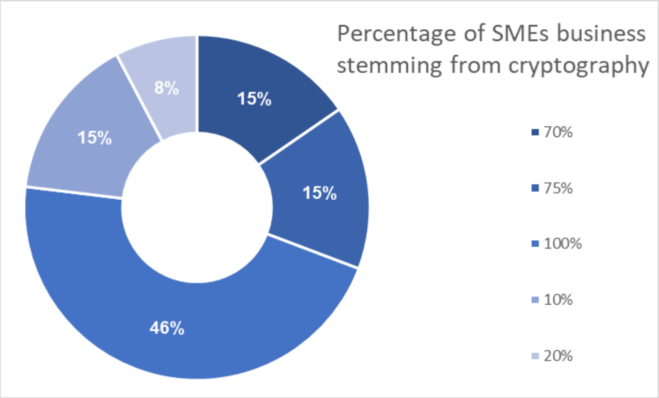
- Notably, the focal points of regulatory engagement revolve around the use of cryptography, certifications and compliance. This underscores the significance of ensuring secure and compliant practices in cryptographic operations.
- A secondary focus of regulatory organisations is the standardisation and accreditation of cryptographic products and services.
- The primary regulatory principles identified for cryptography include: reliance on algorithmic methods certified for trust, careful selection of cryptographic approaches and a commitment to adhering to standardised cryptographic methods. The implementation of these principles is in fact reflected in the findings related to certification (see Section 6.1).

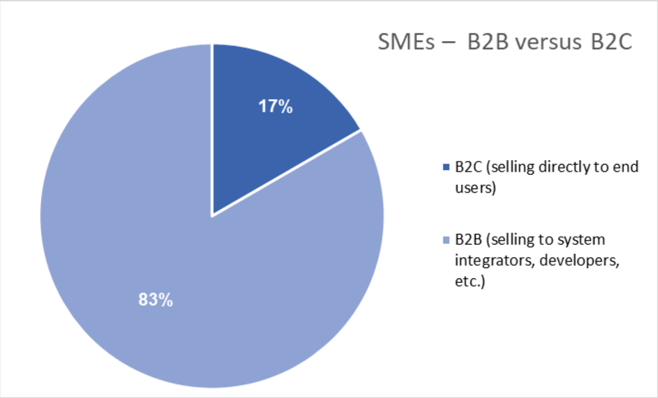
3.2. FOCUS ON SMES

This section presents some analysis regarding SMEs that took part in the survey. Given the important role of SMEs in innovation and incubation, the presented analysis aims at identifying interesting observations that explain their standing and role in the cryptographic products and services business. These observations provide a basis for actions to improve their role and viability in cryptography business.

Figure 5. SMEs in cryptography by enterprise size







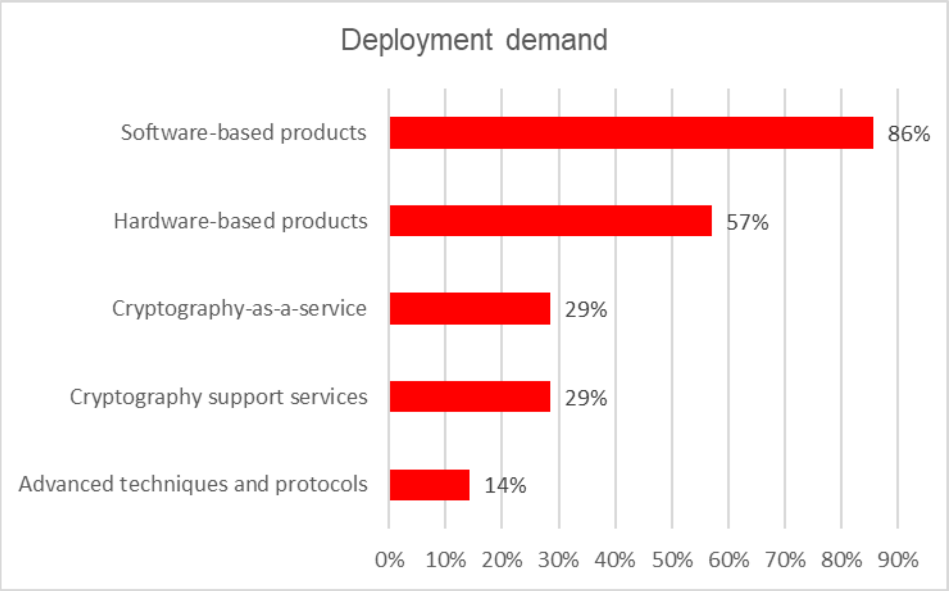
Observations drawn from data on SMEs

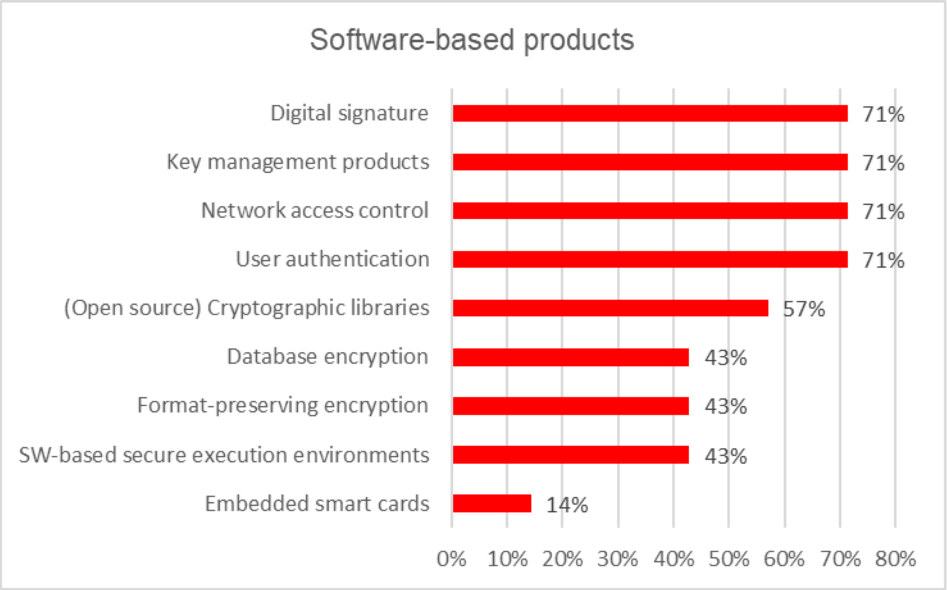
- The majority of SME participants were medium-sized. It is indicative that medium-sized enterprises have reached the critical mass to assume a position in the cryptography market. One possible reason for this is the relatively high cost of placing products on the market. These costs may be related to the high level of product assurance requirements (e.g., certifications, cost of security testing, acquisition and retention of staff, and cost of patents).
- SMEs have a better standing in countries with a higher level of industrialisation, R & D, digitisation and social wealth. These conditions seem to facilitate the emergence of organisations that contribute to the development of new technologies and manage to turn them into marketed products.
- As France seems to be the most favourable environment for SMEs in cryptography, it might be worth further analysing the factors that have led to better incubation in that market area (e.g., functioning B2B relationships, better skill development, better symbiosis between small and large organisations, better incentives, etc.).
- It is interesting that the majority of SMEs surveyed are specialised in cryptography: ca 80 % of them earn more than 70 % of their turnover in that market. The high degree of specialisation in cryptography is interconnected with numerous operational requirements (e.g., availability of specialised staff, acquisition of the necessary monetary resources, stable market standing and access to R & D).
- Micro and small enterprises are in the minority. It is assumed that this is due to difficulties in the transition of micro enterprises into SMEs (see also second observation in Section 3.1.2).
- The assessed methods to develop cryptographic offerings reveal that mergers and acquisitions are frequently adopted to expand product and capability portfolios. Obviously, SMEs are often subject to mergers with bigger players in the cryptographic product and service market. Moreover, they might also play a role in the supply chain of product development, given their high level of specialisation.
- The majority of SMEs are mostly active in business involving B2B transactions (ca 80 %). This indicates that SMEs show a higher engagement in providing services to business customers.

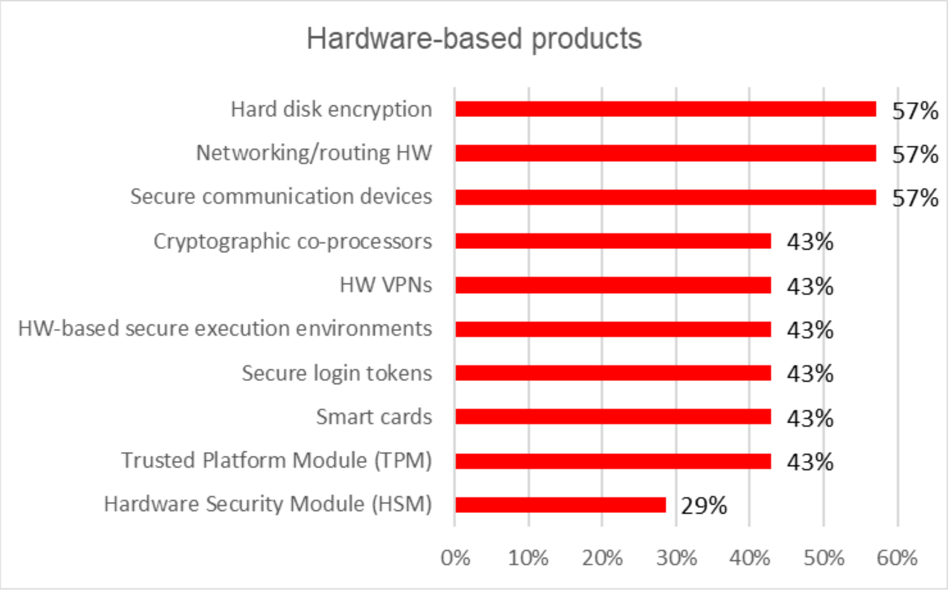
4. CRYPTOGRAPHIC PRODUCTS USAGE PATTERNS

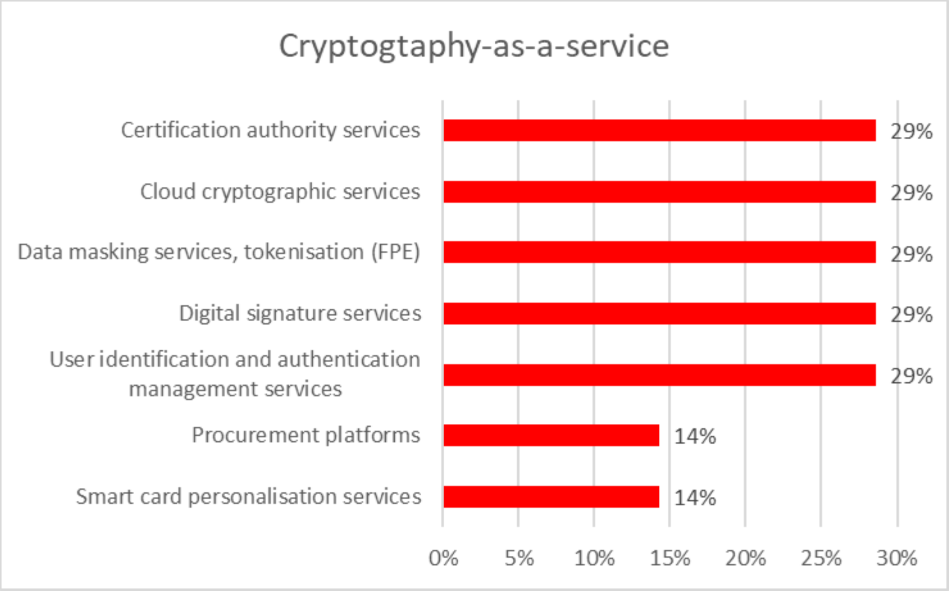
4.1. USAGE PATTERNS ON THE DEMAND SIDE

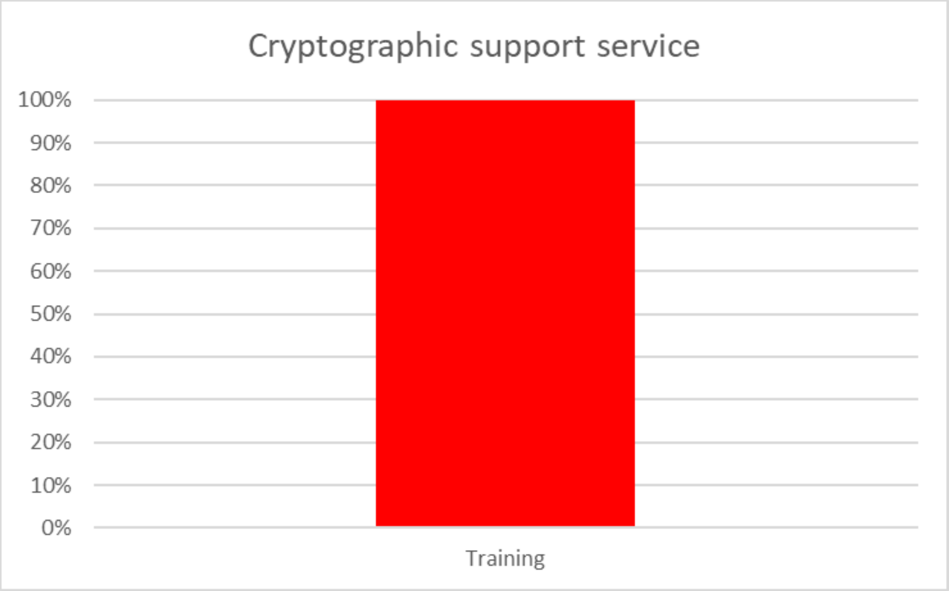
Figure 6. Usage of cryptographic products and services by demand






Hardware-based products
Hard disk encryption 57%
Networking/routing HW 57%
Secure communication devices 57%
Cryptographic co-processors 43%
HW VPNs 43%
HW-based secure execution environments 43%
Secure login tokens 43%
Smart cards 43%
Trusted Platform Module (TPM) 43%
Hardware Security Module (HSM) 29%
0%
10%
20%
30%
40%
50%
60%


Cryptogtaphy-as-a-service
Certification authority services 29%
Cloud cryptographic services 29%
Data masking services, tokenisation (FPE) 29%
Digital signature services 29%
User identification and authentication management services 29%
Procurement platforms 14%
Smart card personalisation services 14%
0%
5%
10%
15%
20%
25%
30%

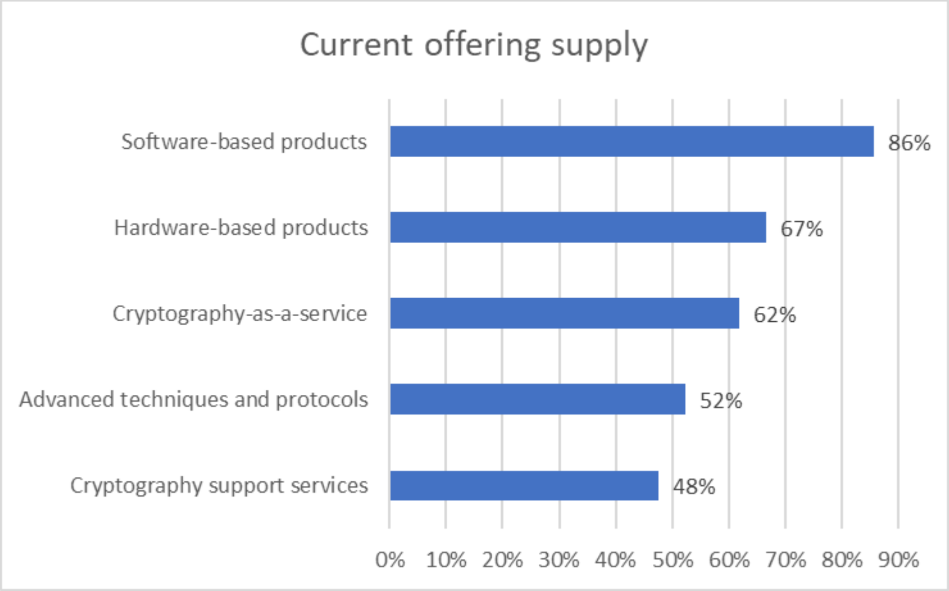

Cryptographic support service
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Training

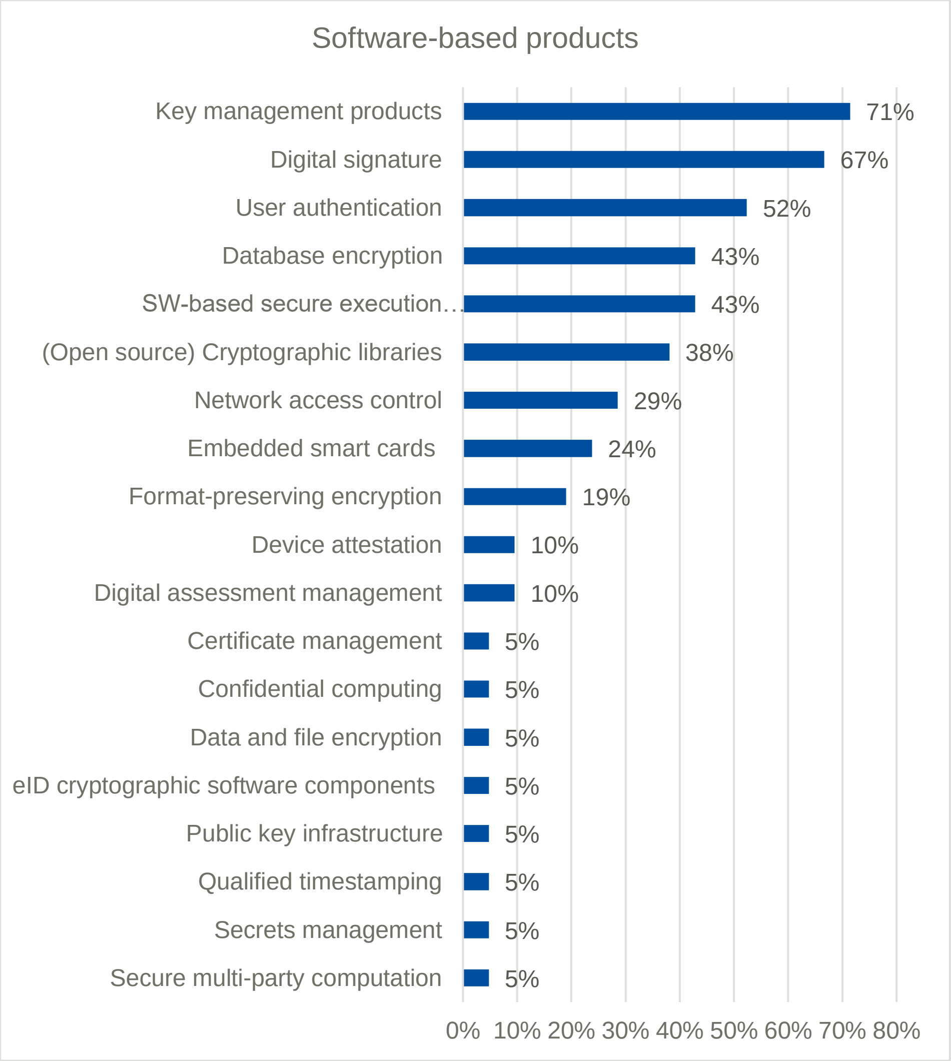
Observations drawn from demand-side usage

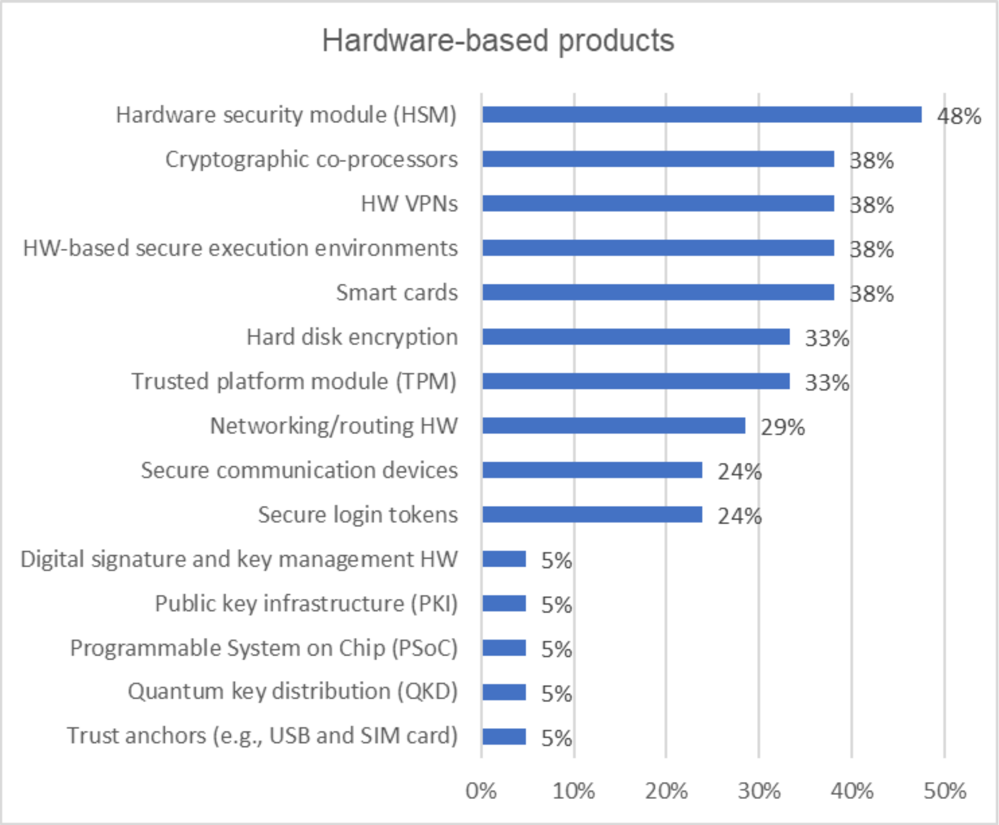
- As expected, demand-side organisations use primarily software-based products and services, with HW products being the second priority. The main priorities of software-based products are user identification, network access control, key management products and digital signatures, which shows that the predominant use cases of cryptographic software-based products focus on electronic identification (eID). Embedded smart cards and software-based secure execution environments, format preserving encryption and database encryption have the lowest priority.
- The moderate to significant adoption levels of OS cryptographic libraries on the demand side are indicative of the need to enhance their security maintenance and strive for a swift update process if vulnerabilities are discovered.
- HW-based products are topped by secure communication devices, hard-disk encryption and networking/routing devices. The use of hardware security modules (HSMs) holds the lowest priority.
- Cryptography-as-a-service and advanced techniques and protocols are used to a lesser extent by the demand-side organisations. The reason for this lower attention may be the low level of interest/understanding of the benefits of advanced cryptographic techniques, while demand is rather satisfied with available products and services, as long as they fulfil their requirements. These product/service categories, however, are technologically promising for the future of cryptographic businesses. Some examples are: ZKPs, post-quantum cryptography and cloud cryptographic services. With growing popularity of relevant products and services, it is expected that their use will increase in the short to middle term.
- As regards the use of cryptographic support services (i.e., certification services, specification of cryptographic functions, testing of cryptographic products/services and training) cryptography training is the single choice of the surveyed demand-side organisations.

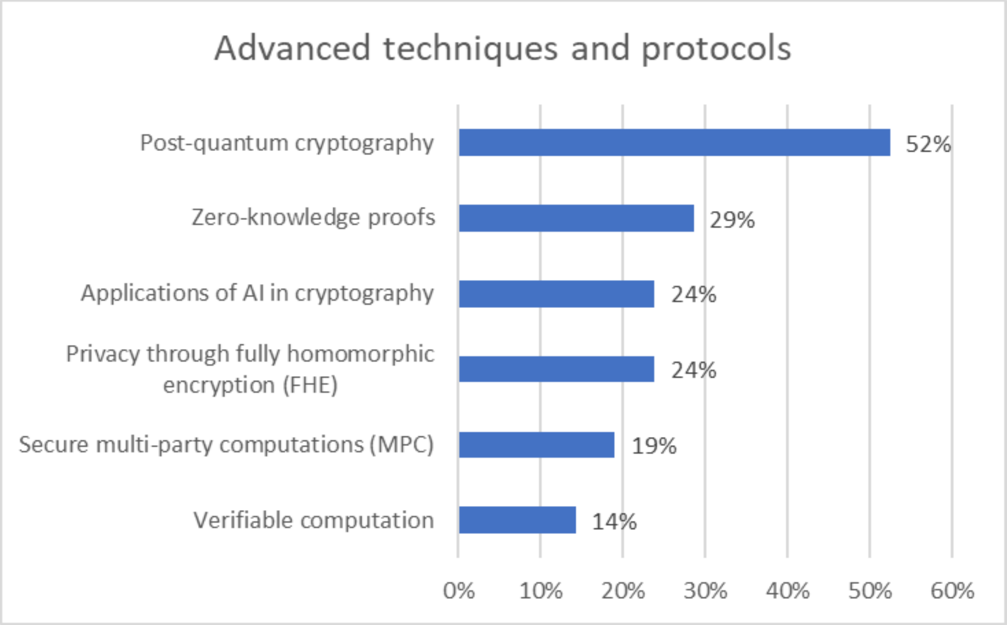
4.2. PRODUCT PATTERNS ON THE SUPPLY SIDE

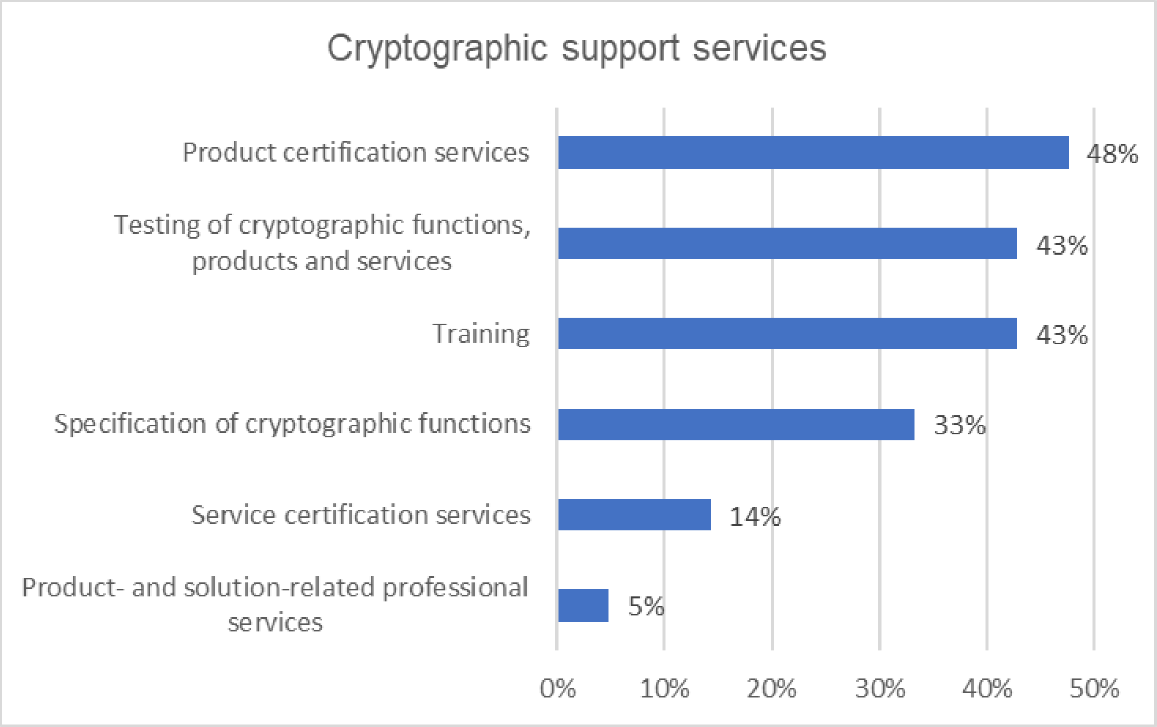
Figure 7. Offered cryptographic products and services by supplier

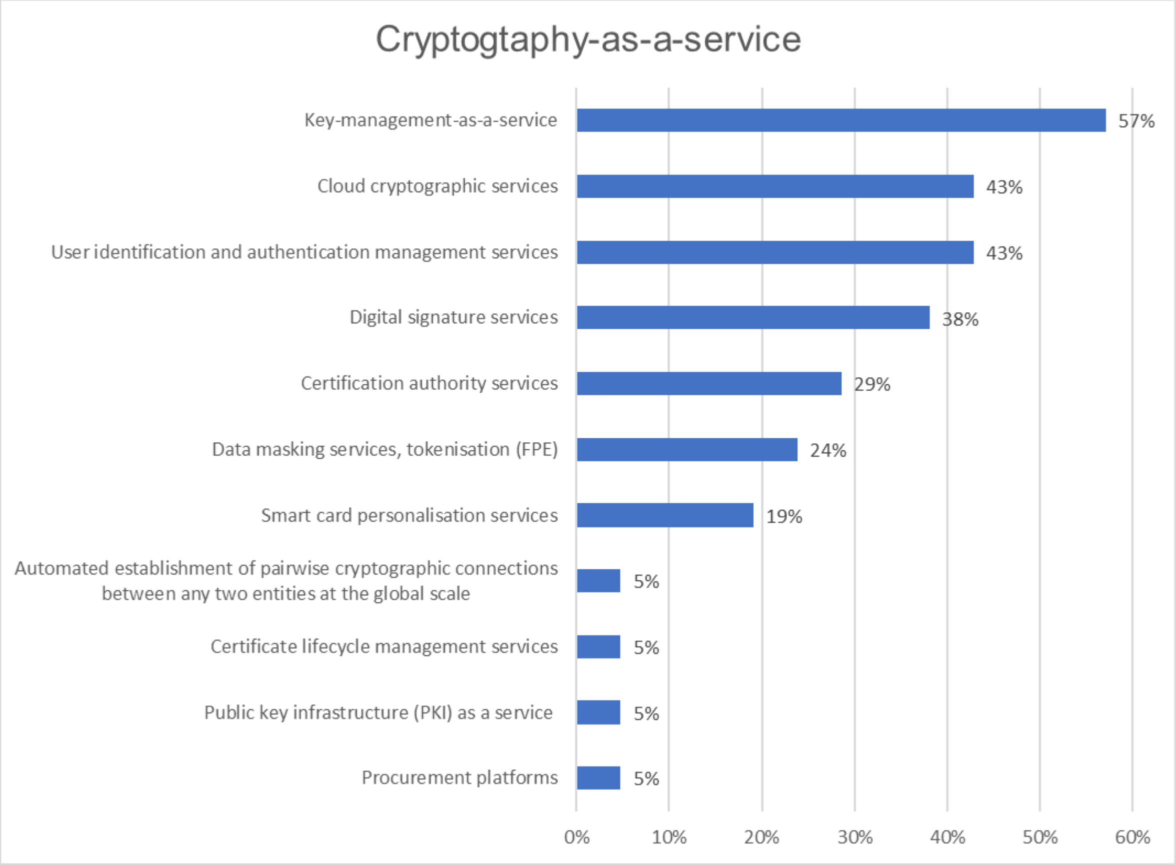





Hardware-based products
Hardware security module (HSM) 48%
Cryptographic co-processors 38%
HW VPNs 38%
HW-based secure execution environments 38%
Smart cards 38%
Hard disk encryption 33%
Trusted platform module (TPM) 33%
Networking/routing HW 29%
Secure communication devices 24%
Secure login tokens 24%
Digital signature and key management HW 5%
Public key infrastructure (PKI) 5%
Programmable System on Chip (PSoC) 5%
Quantum key distribution (QKD) 5%
Trust anchors (e.g., USB and SIM card) 5%
0% 10% 20% 30% 40% 50%


Advanced techniques and protocols
Post-quantum cryptography 52%
Zero-knowledge proofs 29%
Applications of AI in cryptography 24%
Privacy through fully homomorphic encryption (FHE) 24%
Secure multi-party computations (MPC) 19%
Verifiable computation 14%
0% 10% 20% 30% 40% 50% 60%


Cryptographic support services
Product certification services
48%
Testing of cryptographic functions, products and services
43%
Training
43%
Specification of cryptographic functions
33%
Service certification services
14%
Product- and solution-related professional services
5%
0%
10%
20%
30%
40%
50%

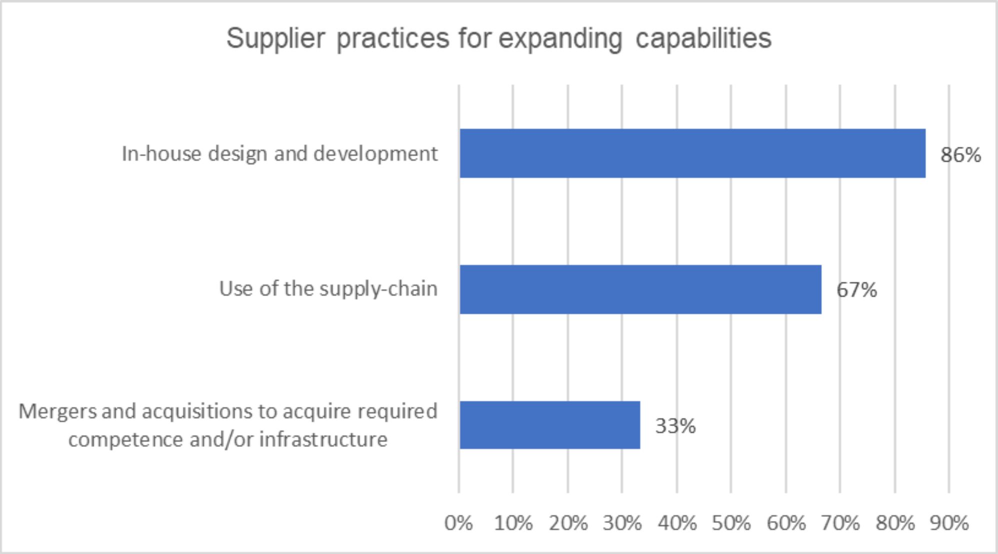

Cryptogtaphy-as-a-service
Key-management-as-a-service
57%
Cloud cryptographic services
43%
User identification and authentication management services
43%
Digital signature services
38%
Certification authority services
29%
Data masking services, tokenisation (FPE)
24%
Smart card personalisation services
19%
Automated establishment of pairwise cryptographic connections between any two entities at the global scale
5%
Certificate lifecycle management services
5%
Public key infrastructure (PKI) as a service
5%
Procurement platforms
5%
0%
10%
20%
30%
40%
50%
60%

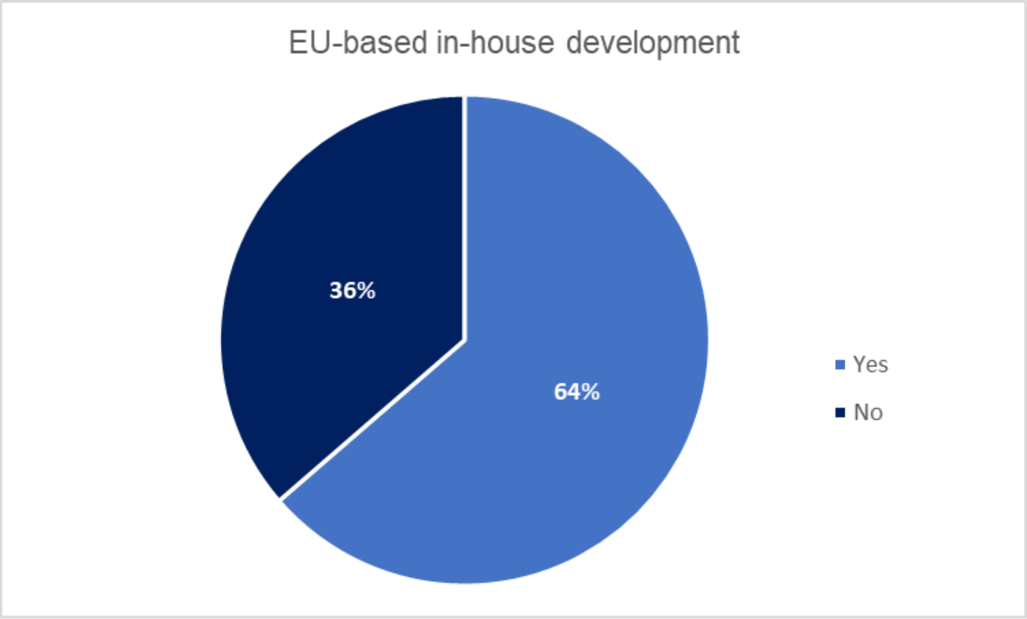
Observations drawn from cryptographic products/services offerings by suppliers

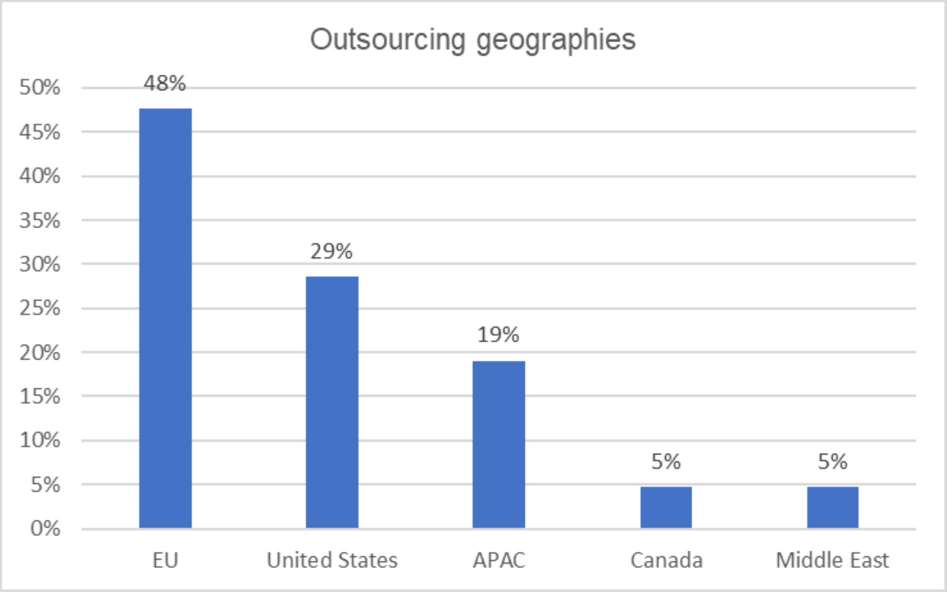
- The market seems to be balanced, i.e., products and services usage trends on the demand side match the offering trends in the main product categories (software and HW products and services). An inverse of priorities is visible in advanced techniques/protocols (lower by demand, higher by supply) and cryptography support services (higher by demand, lower by supply). Eventually, the higher rates of advanced techniques/protocols assessed reflect the plans by suppliers to invest in this product/service category, whereas users are not yet fully aware of, or ready to invest in this group of products. The fact that the supply side is investing in advanced techniques/protocols is a good sign of market dynamics: the supply side is investing in new products to gain first-mover competitive advantages by using time-to-market metrics.
- As regards the HW-based product categories, the highest priority is assigned to HSMs, followed by HW VPNs, smart cards, HW-based secure execution environments and cryptographic co-processors. This ranking, when compared with the demand side, indicates that these products are deployed B2B and have a larger share in the offerings than B2C products do. Some HW products with low share appearing in the list (e.g., QKD, trust anchors, dedicated digital signature HW), may be products addressing advances in cryptographic techniques and protocols and/or upcoming regulatory requirements.
- Cryptographic support services consist mostly of services related to certification: product certification services, specification and testing of cryptographic functions make up a significant part of this category. Training is the other important activity of this product/service category.
- Advanced techniques and protocols are dominated by activities related to emerging technologies and cryptography. This product/service category includes post-quantum cryptography, ZKPs and applications of AI in cryptography.
- Cryptography-as-a-service is a product/service category that facilitates the outsourcing of cryptographic infrastructure. The main offerings are key-management-as-a-service, user identification and user authentication services, and cloud cryptographic services. Of interest in this product/service category are emerging products and services such as procurement platforms, certificate lifecycle management services, data masking and tokenisation, and automated pairwise cryptographic connections between any two entities at the global level. Services such as these will provide solutions for securing user business processes and transactions and contribute towards emerging privacy requirements.
- Similar to all other cryptographic product/service categories, software-based products entail a number of mainstream products and some emerging ones covering upcoming cryptography trends and technologies. Key management, digital signatures and user authentication are the most frequently offered products, followed by software-based secure execution environments, database encryption and cryptographic libraries. Confidential computing, qualified timestamps, eID cryptographic software components and secure MPC are emerging cryptography products covering future market and regulatory requirements.

4.3. SUPPLIER PRODUCT/SERVICE DEVELOPMENT PRACTICES

Figure 8. Development practices followed by suppliers







Observations regarding supplier practices in development of offerings

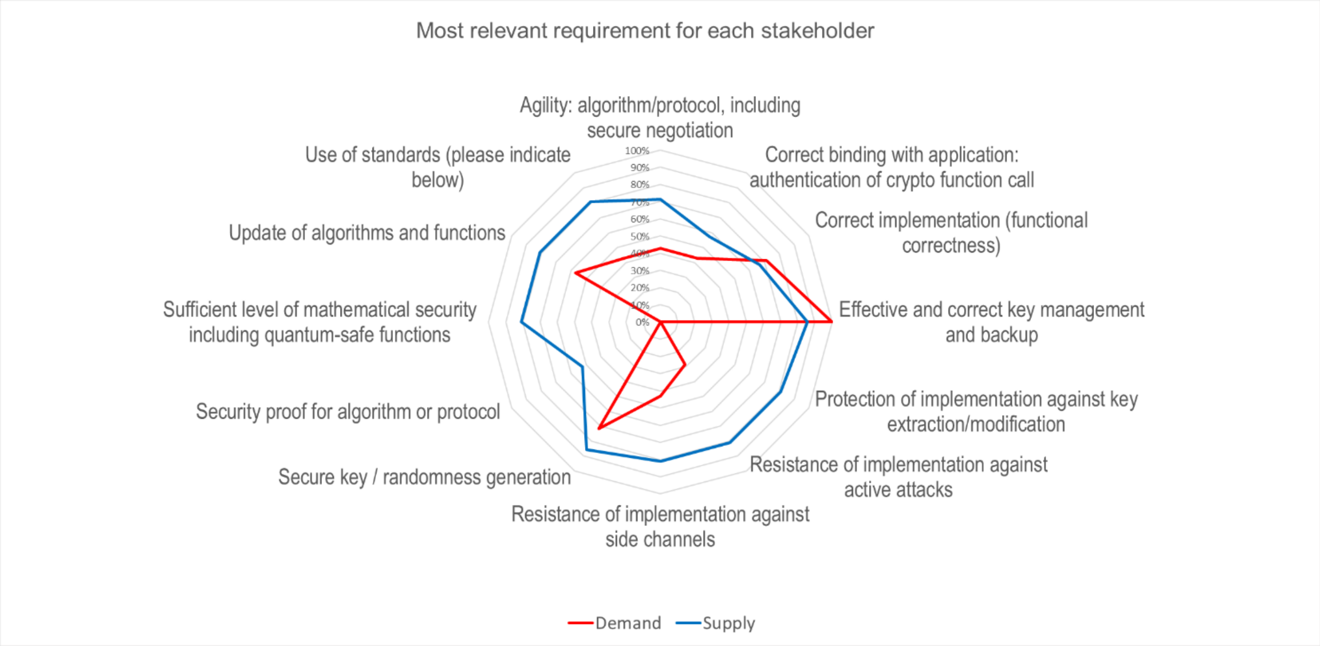
- Ranked by magnitude, the methods used by suppliers for the design and development of cryptographic products and services are in-house design and development, use of the supply chain, and mergers and acquisitions.
- While the in-house design and development is mostly performed within the EU (ca 64 %), the supply chain part covers a non-negligible part (ca 36 %), of which ca 50 % is outside the EU (ca 18 % Asia–Pacific (APAC), 28 % United States, 5 % Canada and 5 % Middle East). Of interest for the viability of SMEs is the ca 33 % of capabilities obtained through mergers and acquisitions, indicating that incubation of new cryptographic ideas/technologies is absorbed by organisations with critical mass.
- A significant part of product design and development is performed within the EU. Assuming the existence of compliance to EU regulation requirements, this is a positive fact as regards the quality of the developed cryptographic products and services.
- The part of cryptographic product design and development outsourced outside the EU is still significant, especially given the high sovereignty requirements in the area of cryptography (see Section 7.2.1). Nonetheless, the reliance on standards and the certification activities connected with cryptographic modules and validation of algorithmic correctness outbalance potential outsourcing risks to a certain degree. Residual risks remain when developed software uses HW from untrusted vendors.

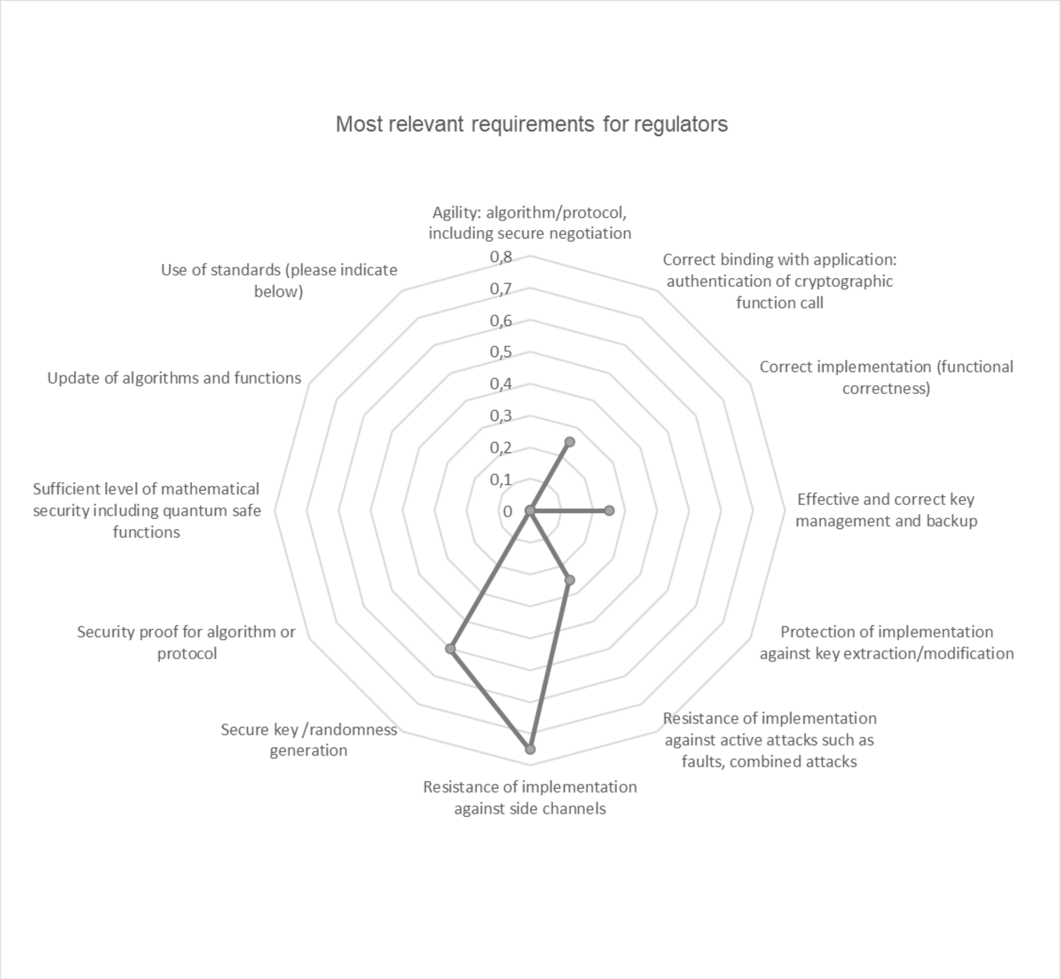
5. THREATS, REQUIREMENTS AND CAPABILITIES

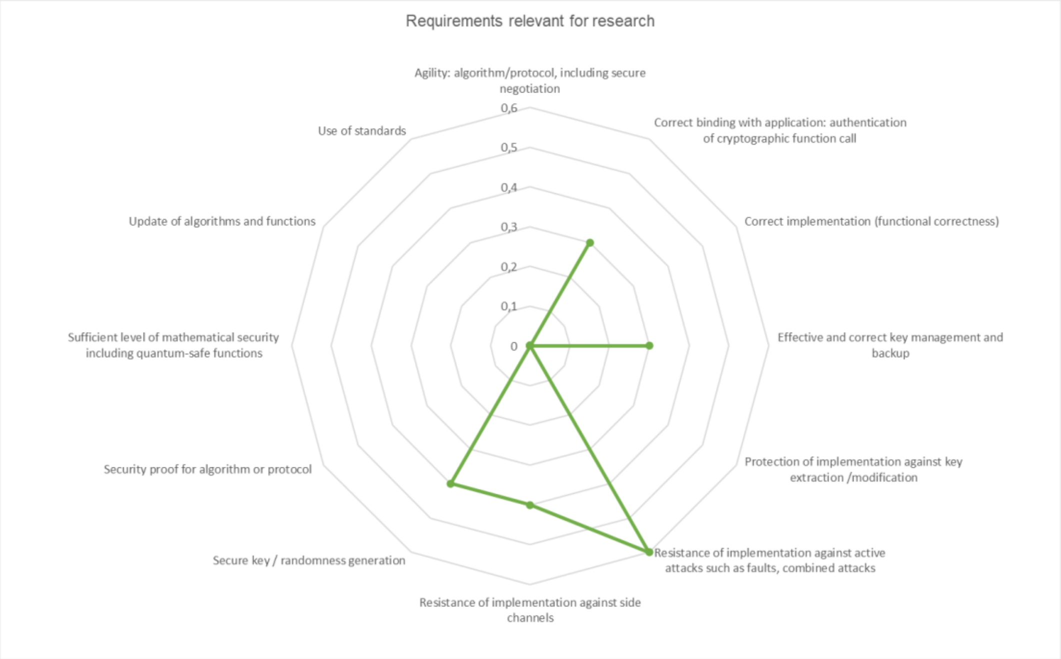
This chapter presents the findings regarding the threat perceptions of the demand, supply and research stakeholder groups. Similarly, it presents requirements for the cryptography products and services of these three stakeholder groups. Finally, the cryptographic capabilities of the groups are analysed. Given that threats and requirements are common in these groups, the analysis is based on changing perceptions. The analysis of capabilities is based on a self-assessment made by the demand side and on input about cryptography maturity, as assessed by suppliers from various sectors in their product portfolios.

5.1. REQUIREMENTS FOR CRYPTOGRAPHIC PRODUCTS AND SERVICES

Figure 9. The most relevant cryptographic requirements for each stakeholder




Most relevant requirements for regulators
Agility: algorithm/protocol, including secure negotiation
Correct binding with application: authentication of cryptographic function call
Correct implementation (functional correctness)
Effective and correct key management and backup
Protection of implementation against key extraction/modification
Resistance of implementation against active attacks such as faults, combined attacks
Resistance of implementation against side channels
Secure key /randomness generation
Security proof for algorithm or protocol
Sufficient level of mathematical security including quantum safe functions
Update of algorithms and functions
Use of standards (please indicate below)
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0

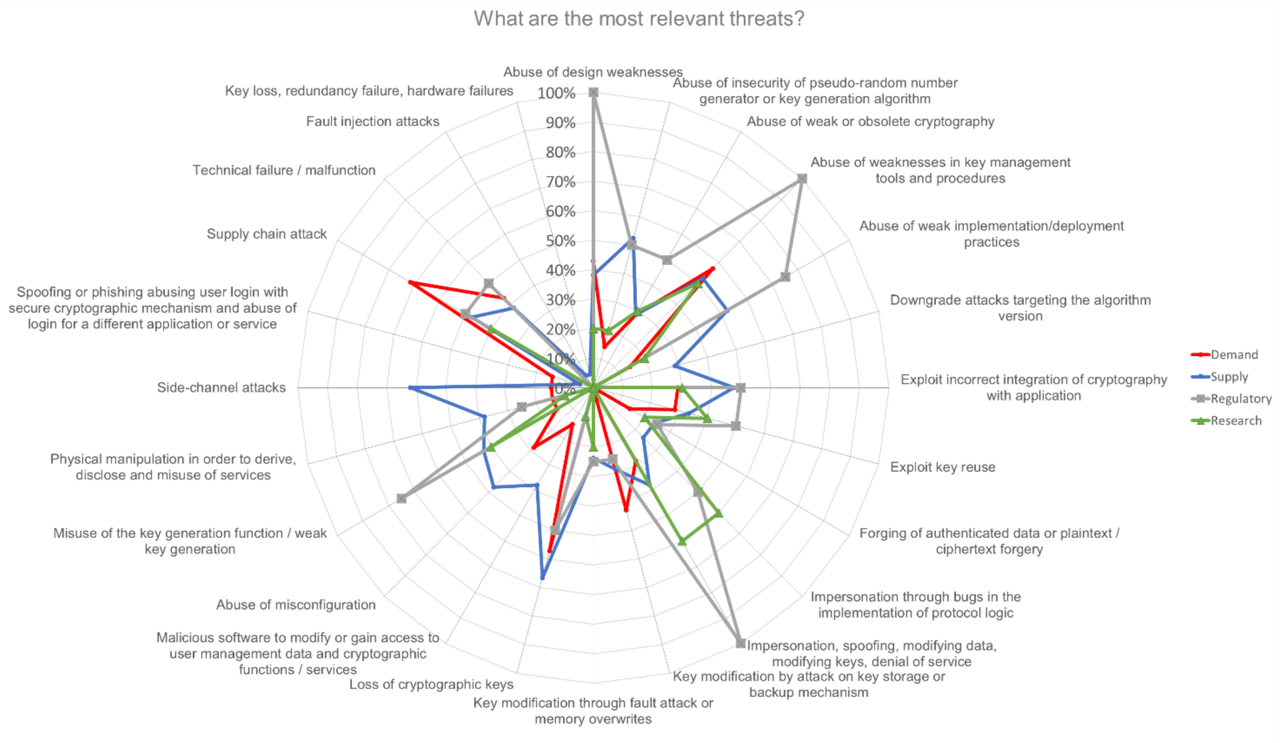

Requirements relevant for research
Agility: algorithm/protocol, including secure negotiation
Correct binding with application: authentication of cryptographic function call
Correct implementation (functional correctness)
Effective and correct key management and backup
Protection of implementation against key extraction /modification
Resistance of implementation against active attacks such as faults, combined attacks
Resistance of implementation against side channels
Secure key / randomness generation
Security proof for algorithm or protocol
Sufficient level of mathematical security including quantum-safe functions
Update of algorithms and functions
Use of standards
0,6
0,5
0,4
0,3
0,2
0,1
0

Observations regarding the cryptographic requirements of various stakeholders

- The supply side covers at a satisfactory level all cryptographic requirements assumed in the present market analysis. The lower levels of the requirement "Security proof for algorithm or protocol" can be explained with the reliance of cryptographic products and services on existing standards, hence assuming that this requirement is fulfilled by their use.
- Demand-side data reveal that users of cryptographic products and services have a clear focus on key-management security (key generation and effective key management/backup). A second focus of the demand side lies in requirements regarding the correct implementation of cryptographic functions and their correct binding within applications. Moreover, the agility of protocols and efficiency of update processes are also important. Requirements regarding the algorithmic/mathematical part of the cryptographic products are not the users' focus.
- Regulators and research both concentrate on similar cryptography requirements. They cover mainly security issues of key management. A secondary group of requirements is related to the correct binding of cryptographic functions within applications and the resistance of implementations against side-channel attacks.
- The similarity between the cryptographic requirements of regulators and research is a remarkable fact. It could be explained through a focus of research on content included in regulation. Nonetheless, research may help a great deal in the fulfilment of cryptographic requirements that are outside the assessed scope of research organisations (e.g., development of secure execution, protection of implementation against modification, security proof of algorithms and protocol, and agility).

5.2. CYBERTHREAT EXPOSURE OF CRYPTOGRAPHIC PRODUCTS AND SERVICES

Figure 10. The most relevant cyberthreat exposure in each stakeholder category ([51])



As regards the background supporting the perceptions of demand, supply, regulation and research stakeholder groups, the following assumptions can be made.

- Supply cyberthreat perceptions are driven by experiences gained during the development, testing, deployment and operation/maintenance of supported cryptographic products and services, including a deep understanding of the specification, code and interfaces of supported cryptographic functions, operation of the developed products and services, tracking and analysing incidents, bug fixes and updates.
- Demand cyberthreat perceptions are driven by experiences gained through their business operations, including interaction with business customers, operators of their cryptographic infrastructure (internal, external), maintenance of cryptographic products, own risk assessments, and own experience from the security management of their IT infrastructure.
- Regulator cyberthreat perceptions are driven by accumulated experiences from various cryptographic products and services, theoretical threat assessments (potentially emerging from certification schemes and functional specifications), sets of requirements dictated by various levels of assurance and various use cases, and national strategic considerations.

[51] For a detailed description of the various cyberthreat types, please see Section 2.6.

- Research cyberthreat perceptions are driven by experiences related to research activities, in particular by projecting existing cyberthreat exposures onto new ideas/technologies and/or trying to develop individual mitigation measures for particular types of cyberthreats.

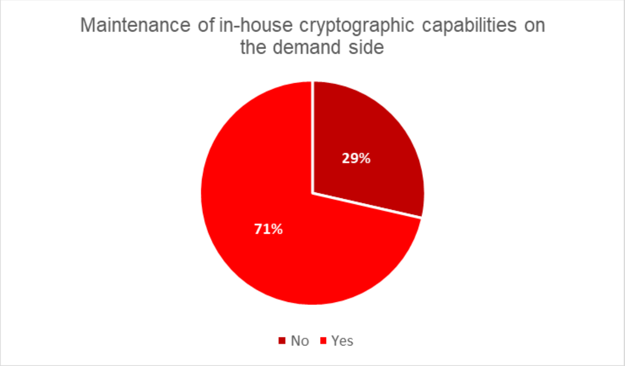
Observations from various cyberthreat perceptions of various stakeholders

- Regulators concentrate more on the targeting design of cyberthreats and the strength of supported cryptographic mechanisms. Special attention is given to rigid key generation and key-management functions and to correctness of design. Supply-chain attacks and failures/malfunctions are secondary concerns.
- The demand side mostly follows the lines of regulators and suppliers. Supply-chain attacks are the main concern and are assigned the highest relevance among all other stakeholder groups. Cyberthreats emerging from poor key-management practices (key reuse, key loss, key modification, abuse of weaknesses of key-management operation) are a second priority, followed by weaknesses arising from the integration of cryptographic functions within applications and the abuse of misconfigurations.
- It is remarkable that the demand side assigns very low priority to the cyberthreats: side-channel attacks, physical manipulation of devices, misuse of weak key generation, key modification through fault attacks or memory overwrites, downgrade attacks targeting the algorithm version, and spoofing or phishing abusing the user login. However, these cyberthreats are relevant for demand-side encryption. This leads to the conclusion that those on the demand side need to increase their awareness of attack methods on their cryptographic infrastructure, and eventually become better informed about incidents relating to cryptographic products and services in use.
- Regulators have a good overview of cyberthreats that are related to in par their regulatory role. They seem to (correctly) leave out of their scope cyberthreats related to the operation of cryptographic products and services, and cyberthreats inherent to the improper integration and use of products within applications. These are clearly the responsibility of application developers.
- Research stakeholders concentrate on a lower number of cyberthreats than the other groups. They concentrate on cyberthreats targeting key management, spoofing through run-time and implementation weaknesses, and supply-chain attacks. This focus is motivated by research interest in key management and secure development.
- A general observation from the cyberthreat perception of participating stakeholders is to keep track of the entire set of cyberthreats, as their work may collaterally affect threat exposure to cyberthreats that were not considered the primary focus. Feeding of threat intelligence platforms with cryptography related cyberthreats might be an initial step towards a better awareness of the cryptography threat landscape.

5.3. CAPABILITY LEVELS OF DEMAND AND SUPPLY SIDES

5.3.1. Demand-side capabilities

Figure 11. Overview of surveyed capabilities on the demand side



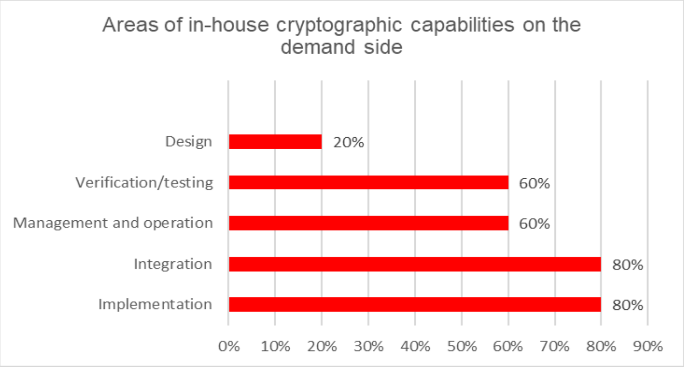
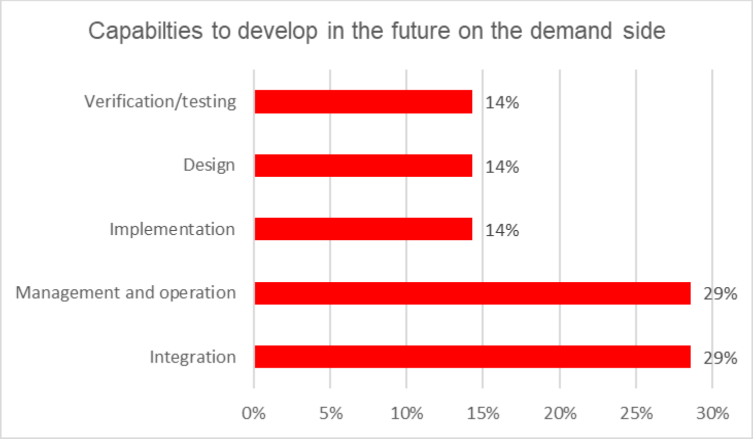
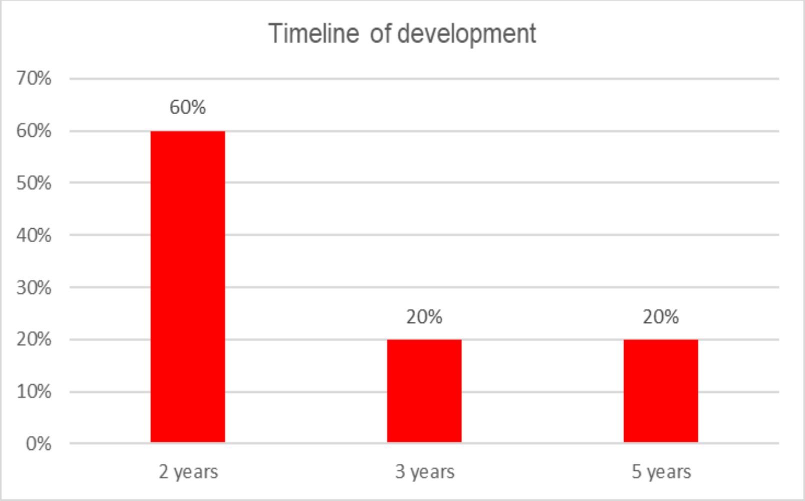
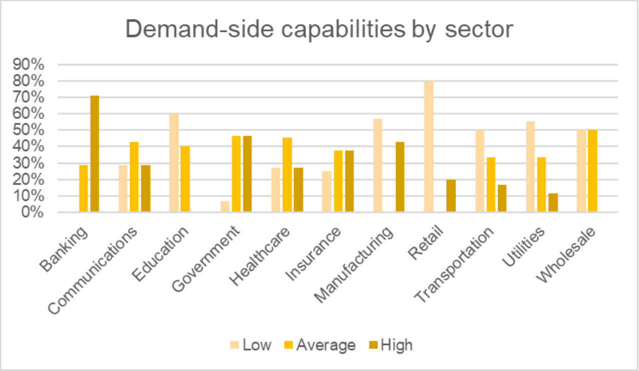
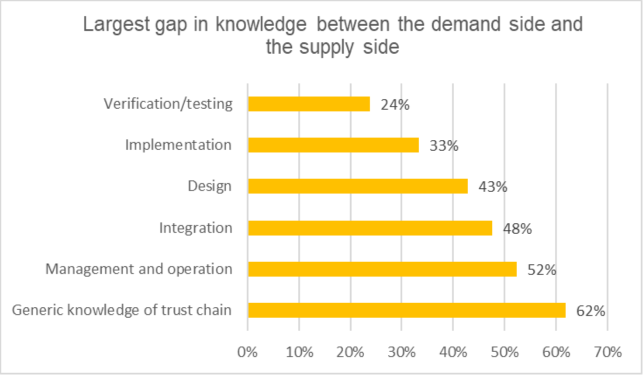


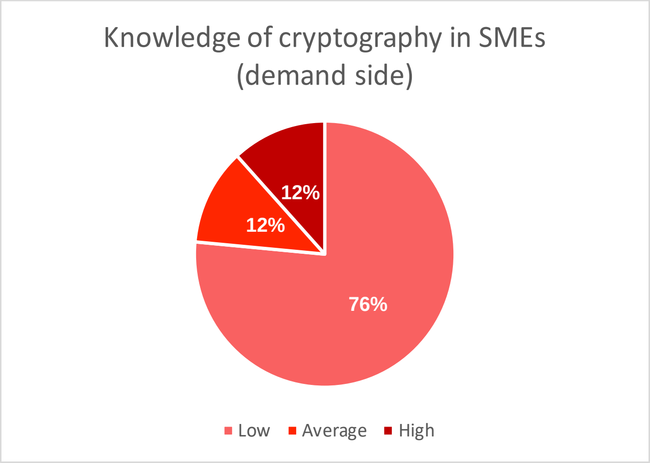
Figure 12. Demand capabilities per sector – assessed by suppliers

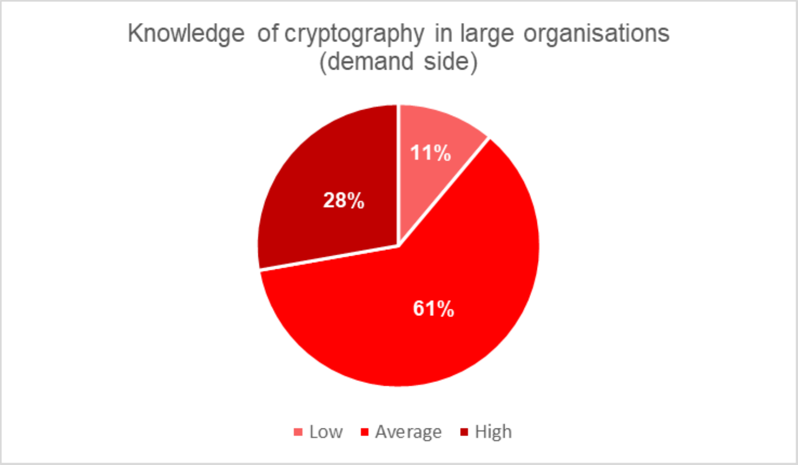





Demand-side capabilities by sector
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Banking
Communications
Education
Government
Healthcare
Insurance
Manufacturing
Retail
Transportation
Utilities
Wholesale
Low
Average
High


Largest gap in knowledge between the demand side and the supply side
Verification/testing
24%
Implementation
33%
Design
43%
Integration
48%
Management and operation
52%
Generic knowledge of trust chain
62%
0%
10%
20%
30%
40%
50%
60%
70%


Knowledge of cryptography in SMEs (demand side)
12%
12%
76%
Low
Average
High

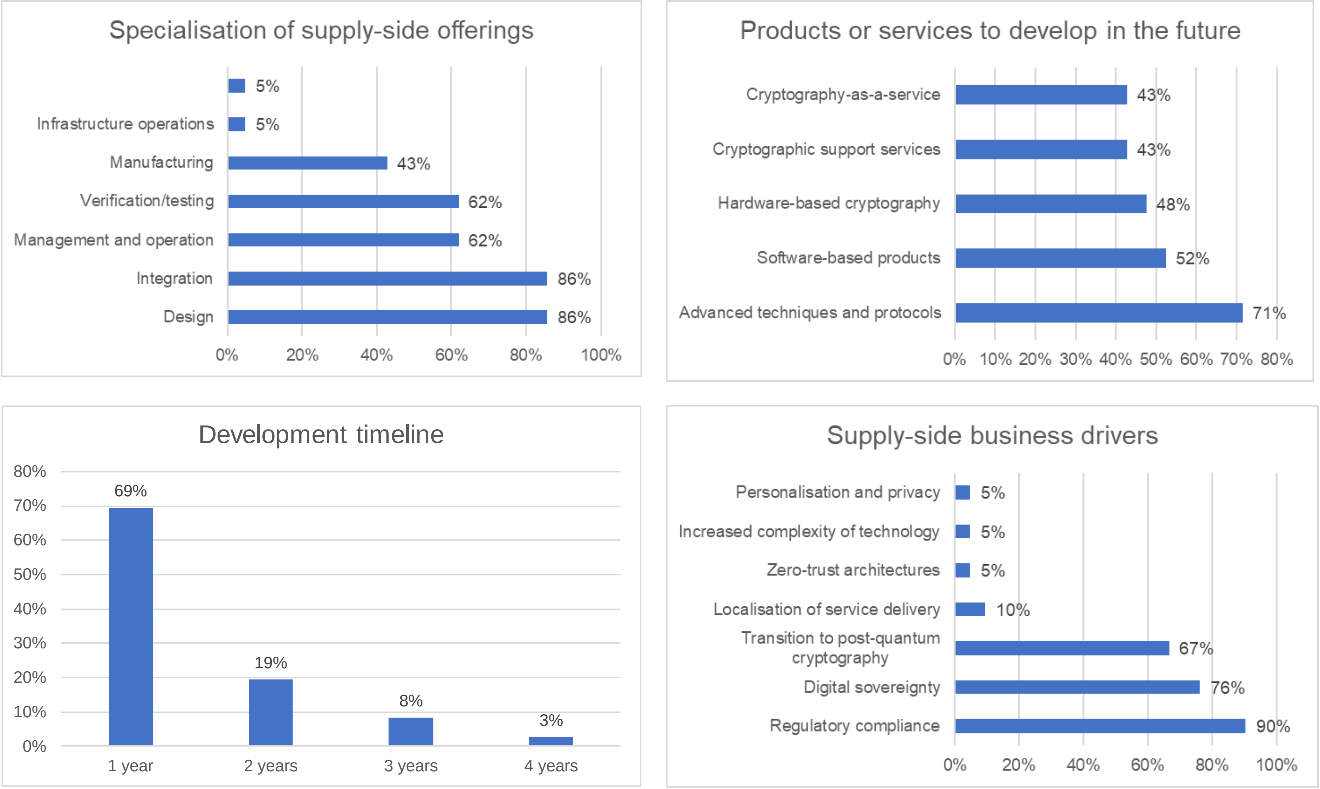

Knowledge of cryptography in large organisations (demand side)
11%
28%
61%
Low
Average
High

Observations regarding demand-side capabilities

- Demand-side capabilities in the area of cryptography are at a fairly good level. The surveyed demand-side organisations along with the sectoral assessment of cryptographic skills provided by suppliers show that the majority of demand-side organisations possess fairly good in-house cryptographic capabilities. Predictably, at the high end of capabilities are banking, government, insurance and manufacturing. At the low end are organisations from sectors with moderate cryptography needs, such as education, retail and wholesale.
- The demand side invests mainly in implementation and integration capabilities, followed by testing and operation/management capabilities. These findings indicate that the demand side builds up capabilities allowing for the implementation, integration, testing and operation of the deployed cryptographic products and services.
- As regards plans for the development of cryptographic capabilities, the trend goes towards enhancing operation and integration. This finding is indicative of a stronger focus on using off-the-self products/services and concentrating more on their integration into the business and their operation/management.
- The timeline for demand-side developments, seen in combination with the capability development plans, reveals the intention to move towards a reduction of own implementation efforts by adopting and operating available market solutions.
- Demand-side capabilities assessed by suppliers as per company size show a capability gap between small and large organisations. This gap might be counterproductive for the deployment of cryptographic products and services, in particular for SMEs that are involved in sectors with higher cryptography needs/requirements.
- The largest gap between demand and supply, as assessed by suppliers, lies in the generic knowledge of the trust chain and management/operation of cryptographic products and services. This gap may generate significant security issues in the usage of products and services and, in the medium term, needs to be closed. This will have positive effects in the proper use of the products and services, but also their more targeted selection and deployment.

5.3.2. Supply-side capabilities

Figure 13. Supply-side plans for expanding product portfolios and capabilities



Observations of supplier capabilities resulting from product/service development plans

- The current and future orientation of suppliers is in balance with the demand plans/expectations. Naturally, their capabilities focus on implementation and design, with integration and management/operation being the next most important capability.
- As regards future service development plans, as a first priority, suppliers plan to enhance their capabilities and their products portfolios in the area of advanced cryptographic techniques and protocols. This is clearly a decision that is intended to support the design, development and deployment of products/services to achieve their main business objectives: regulatory compliance, digital sovereignty and post-quantum cryptography.
- Secondary priorities for suppliers are software-based products, cryptography-as-a-service and HW-based cryptography. These plans resonate with demand-side plans to use off-the-shelf products and enhance the deployment of cryptography-as-a-service offerings.
- The development timeline corresponds fully to the demand-side plans. While the supply side sets 1 year as the time horizon for rolling out new products/services, demand-side development plans are for the coming 2–3 years.

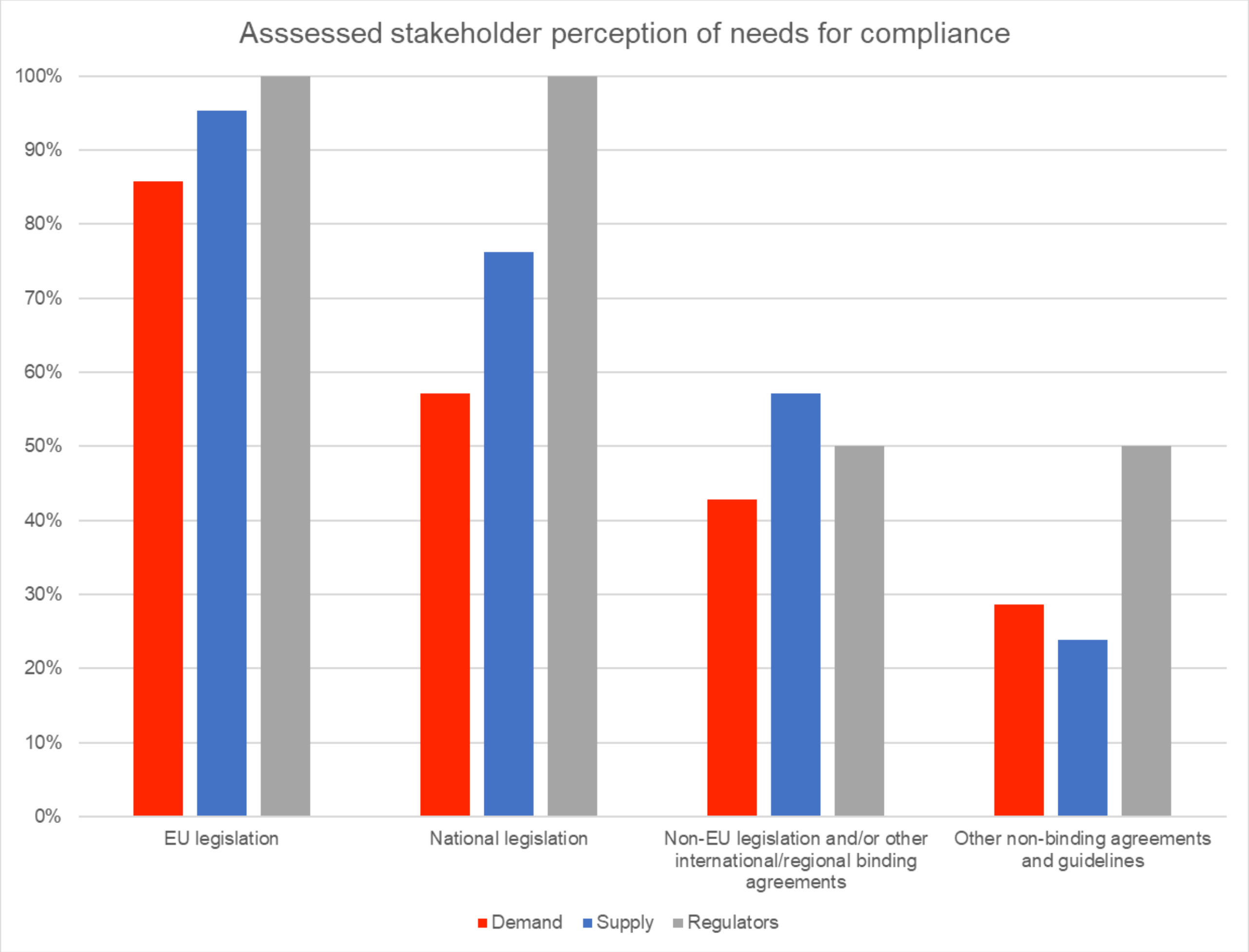
6. ROLE OF CERTIFICATION, REGULATION AND STANDARDISATION

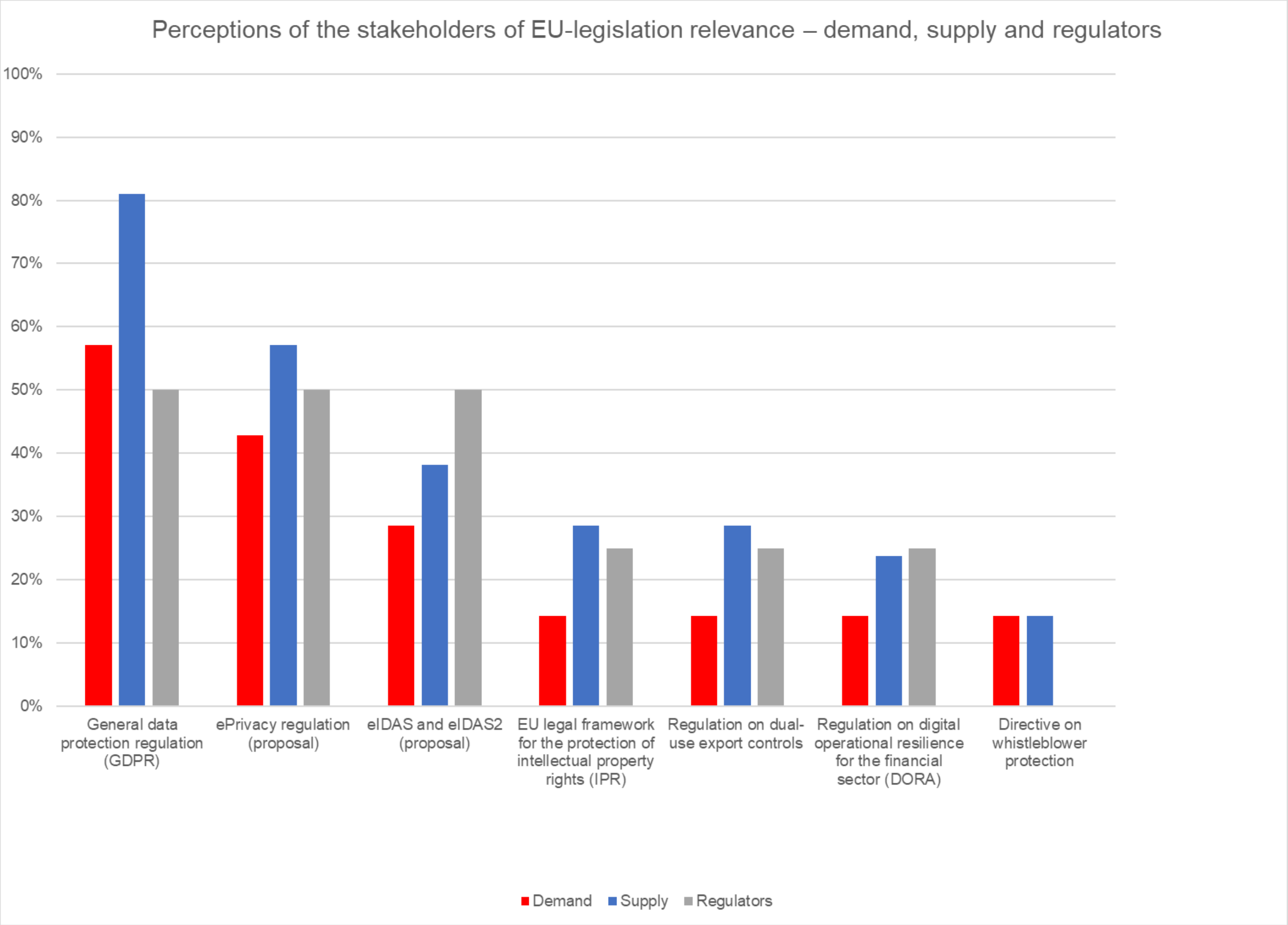
In this chapter, the findings regarding the roles of regulation, certification and standardisation in the development of cryptographic products and services are presented. The findings related to these roles are presented in the following sections, while Annex A presents some examples of relevant legal and policy instruments.

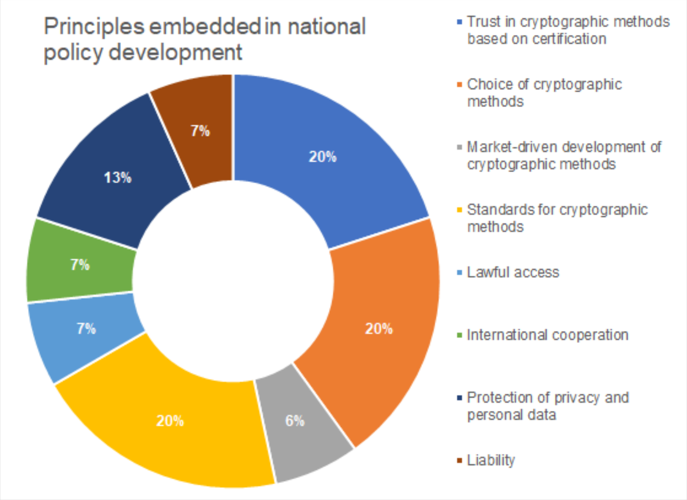
6.1. ROLE OF REGULATORS

6.1.1. Findings focusing on EU regulation

Figure 14. Stakeholder perceptions regarding compliance, relevance and policy principles of EU regulation







Observations drawn from perceptions regarding compliance, relevance and policy principles

- The vast majority of respondents from the demand, supply and regulators sides see a clear need for compliance with the EU and national legislation ([52]).

[52] Guidelines issued by national cybersecurity agencies, although not legislation, play an important role in facilitating compliance with legislation.

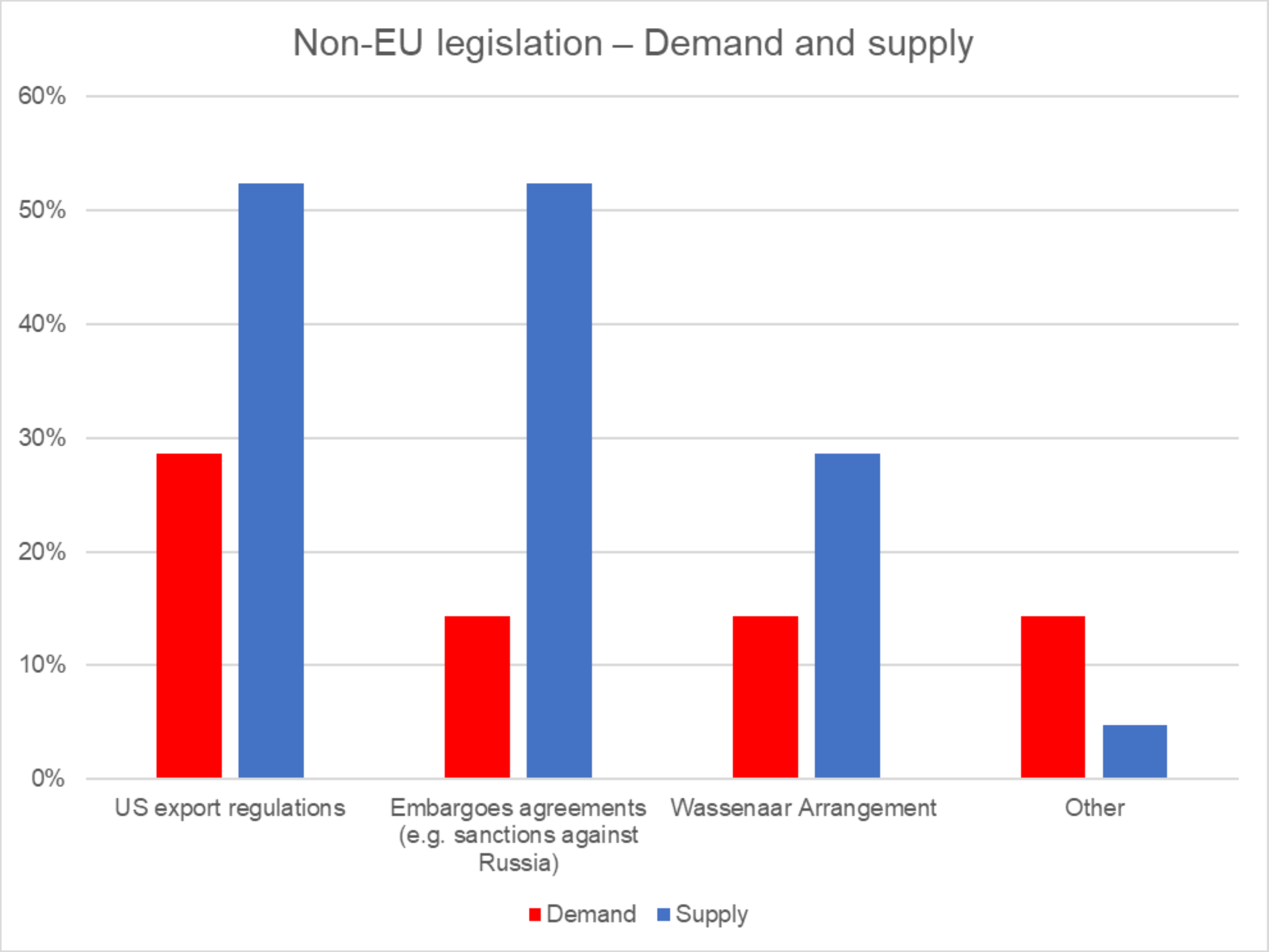
- The majority of respondents from the demand, supply and regulators sides consider, as required, the compliance with non-EU legislation and/or other international/regional binding agreements.
- Fewer respondents, especially from the supply side, see a need for compliance with other non-binding agreements and guidelines. The reason fewer respondents see the need for compliance with such instruments probably resides in the non-binding nature of the instruments.
- The EU general data protection regulation (GDPR), and the proposal for an ePrivacy regulation are the two EU legal instruments seen by the vast majority of respondents from the demand, supply and regulators sides as being the most relevant EU legislation with which suppliers and users of cryptographic products and/or services have to comply. Data protection regulations can therefore be considered as key drivers for the cryptographic product market: cryptographic products protect privacy and data protection regulations that suppliers need to comply with are the regulations that promote the use of such products.
- eIDAS[53] and the (proposal for) eIDAS2[54] are also seen by a certain number of respondents from the demand, supply and regulators sides as being relevant EU legislation with which suppliers and users of cryptographic products and/or services have to comply.
- Other legal instruments, existing or under development, that the respondents considered as relevant EU legislation with which suppliers and users of cryptographic products and/or services have to comply include DORA, intellectual property rights (IPR) and the EU dual use regulation.
- Only a few respondents consider also other instruments, such as the Cybersecurity Act and the NIS2 Directive, as relevant EU legislation with which suppliers and users of cryptographic products and/or services have to comply. This result could be explained by the fact that, although they are key instruments in cybersecurity, they are not addressing aspects directly relevant for the demand and supply of cryptographic products and/or services.
- The standards for cryptographic methods, the choice of cryptographic methods and the trust in the cryptographic methods based on certification are the main principles embedded in policy development.
- The principles of privacy and personal data protection, international cooperation, liability, lawful access and market-driven development methods are also embedded in policy development, but to a lesser extent.

[53] eIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[54] After completion of the drafting of this report, and during the proofreading stage, the eIDAS2 (Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework) was adopted and published at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183, accessed June 2024.

6.1.2. Findings focusing on non-EU regulation

Figure 15. Perceptions of the demand and supply sides regarding compliance with non-EU regulations

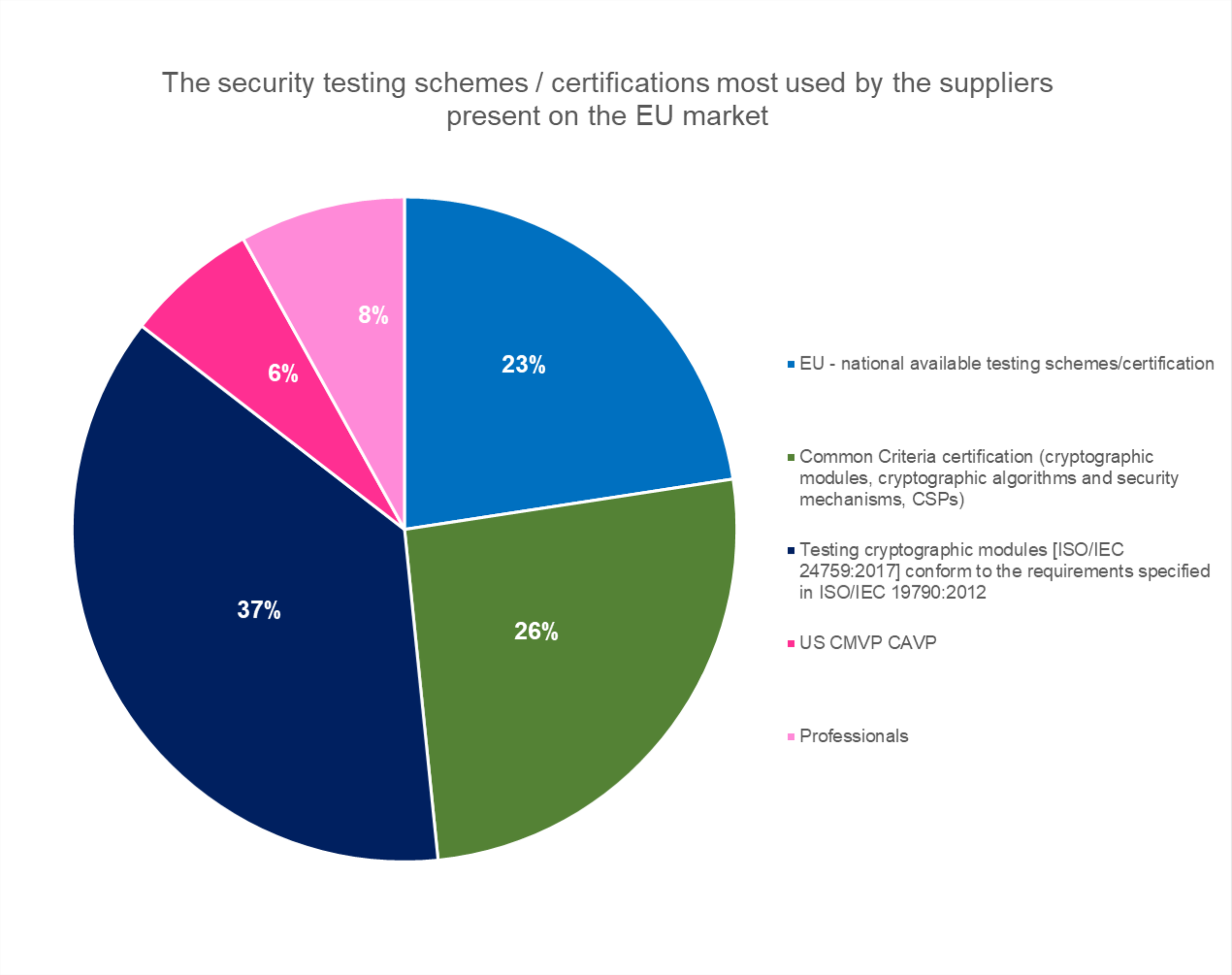


Observations drawn from data on relevant non-EU legislation

- According to respondents on the demand and supply sides, embargo agreements and United States export regulations are the most relevant pieces of non-EU legislation for the demand/supply of cryptographic products and/or services.
- The Wassenaar Arrangement, although not an international treaty and not binding, is also seen by the respondents as relevant, probably due to the fact that EU export controls also reflect commitments agreed upon this arrangement.
- In addition to US export regulations, other non-EU legislation – such as Singaporean and Swiss legislation – is also considered relevant.

6.2. FINDINGS FOR CERTIFICATION

Figure 16. Security testing / certification in the EU market



Observations drawn from certification

- Both EU and non-EU suppliers of cryptographic products (integrators, suppliers, cryptographic service providers) consider security testing / certification relevant for achieving compliance with market access legislation (import/export and other International/regional binding agreements). Specific to the EU market, the demand for standards and compliance through security testing methods/certifications is mainly generated by the implementation of the GDPR and eIDAS regulation.
- Common criteria (CC) certification (cryptographic modules, cryptographic algorithms and security mechanisms, CSPs) and nationally available security testing schemes/certifications dominate the certification market.
- The most important agreement that dominates the EU market is the SOG-IS *Agreed Cryptographic Mechanisms* ([55]), which is accepted by all SOG-IS participants in the SOG-IS crypto evaluation scheme. The *SOG-IS Agreed Cryptographic Mechanisms* will be onboarded into the EUCC scheme, to become the EU-wide reference for cryptographic algorithms and security mechanisms conformance testing.

[55] https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf, accessed November 2023.

- Member States have developed cryptographic specifications for government projects or as part of public procurement requirements for various technical fields. These security requirements are evaluated using the CC evaluation method or other evaluation methods tailor-made by that Member State, as in the following examples.

  Germany

  - BSI, Technical Guidelines for the technical security mechanisms of electronic record-keeping systems ([56]) and BSI, Technical Guideline with security requirements for the use of cryptographic methods in the infrastructure of smart metering systems ([57])
  - BSI TR-03181 Technical Guideline for Cryptographic Service Provider ([58]) – the CSP makes cryptographic primitives, algorithms and advanced protocols readily available for secure usage.
  - Protection profile: Cryptographic Service Provider Light ([59])
  - BSI – Crypto Library Botan ([60]) open-source cryptographic library: provides a secure, clear, controllable and well-documented cryptographic library to increase resistance to side-channel attacks.

  Spain

  - The CCN created a methodology for the evaluation of cryptographic mechanisms. This evaluation methodology is oriented towards products whose main functionality requires cryptography (VPN, encryptors, secure communications, etc.), defining the tasks to be performed by the evaluator in order to verify the requirements to be met by the products.
  - Cryptographic mechanisms approved by the CCN: cryptographic algorithms approved by the CCN in the CCN-STIC 221 guide ([61]) and the parameterisation associated with each one of them.

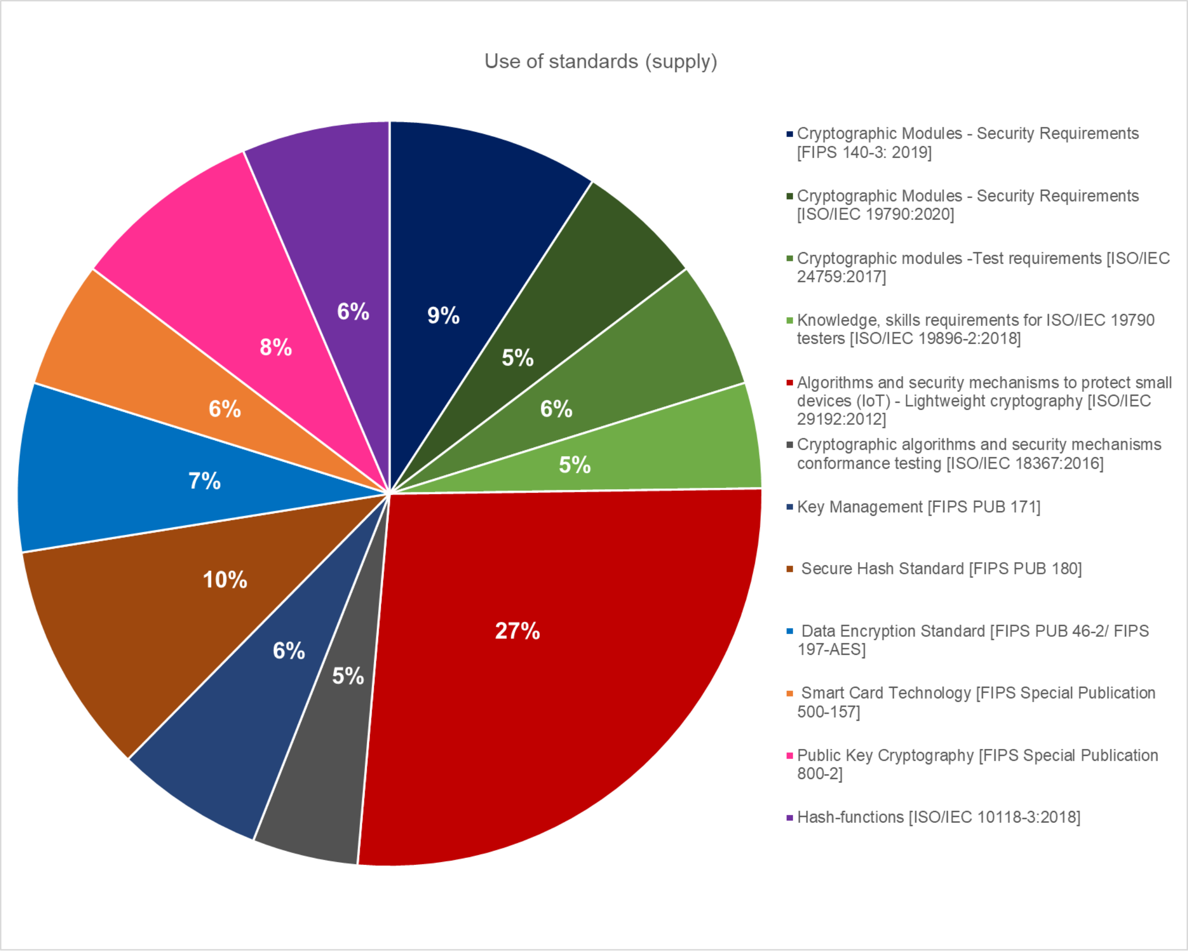
- For cryptographic modules, 36 % of suppliers in the EU market apply the security requirements for cryptographic modules specified by ISO/IEC 19790:2012 (FIPS 140-3) and tested for compliance by the test methods specified in the standard ISO/IEC 24759:2017 (test requirements for cryptographic modules).
- On the supply side, 6 % of the survey respondents are participating in the federal agencies procurement process of both the US and Canada, as they have validated their cryptographic modules and cryptographic algorithms under the US – Cryptographic Security Testing Program: Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) ([62]).
- The appearance of professional certifications (e.g., certified encryption specialist) is potentially indicative of organisations' appetite for certified professionals. One possible justification for suppliers' lack of interest in using professional certifications available in the industry is that the knowledge, skills and competence requirements are defined to

[56] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Schutz-vor-Manipulation-an-digitalen-Grundaufzeichnungen/schutz-vor-manipulation-an-digitalen-grundaufzeichnungen_node.html, accessed November 2023.
[57] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html, accessed November 2023.
[58] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03181/tr-03181.html, accessed November 2023.
[59] https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0111.html, accessed January 2024.
[60] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html, accessed November 2023.
[61] https://www.ccn-cert.cni.es/es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6954-ccn-stic-221-guia-de-mecanismos-criptograficos-autorizados-por-el-ccn-1/file?format=html, accessed November 2023.
[62] https://csrc.nist.gov/projects/cryptographic-module-validation-program/fips-140-3-standards , https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program, accessed November 2023.

test professionals associated with cryptographic module conformance testing programs. Part 2 of ISO/IEC 19896-2:2018 establishes a baseline for the knowledge, skills and effectiveness requirements of ISO/IEC 19790 testers.

6.3. FINDINGS FOR STANDARDISATION

Figure 17. Use of international standards



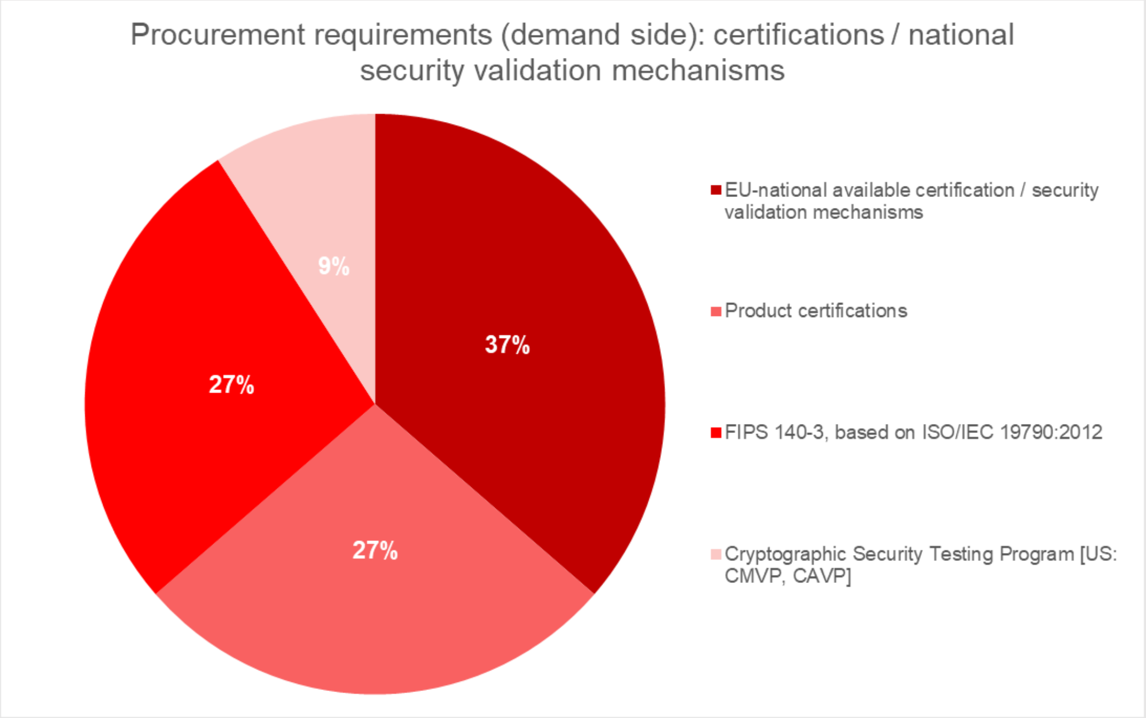
Observations drawn from the use of standards by suppliers

- Around 50 % of the suppliers on the EU market use ISO/IEC standards, while the other half uses NIST/FIPS standards. It is important to read this figure knowing that most of the interviewed suppliers are present in the EU, but at the same time they are also active in APAC, US and Canadian markets.
- Around 30 % of standards used are standards with requirements for cryptographic modules. Cryptographic modules are based on ISO 19790:2012 and ISO 24759:2017 or on FIPS 140-3. It is an understandable approach of cryptographic module vendors to comply with the security requirements defined by the ISO 19790 standard, as FIPS-3 is only an increment of the ISO standard.
- Around 30 % of suppliers rely on lightweight cryptography. Lightweight cryptography is an algorithm designed to protect information created and transmitted by IoT devices to protect all embedded components, such as sensors and actuators or implanted medical devices.

- Around 40 % of specifications are related to algorithms, functions and security mechanisms.
- The success of FIPS also lies in the fact that FIPS 140-3 validated encryption libraries are available (e.g., wolfSSL Crypt ([63])).

Note on the relevance of the findings: since suppliers accessing the EU market should simultaneously comply with national cryptographic specifications and/or go through an evaluation method specific to the Member State in which they sell their products and services, it is relevant to know the percentage of technical specifications requested at the national level.

Figure 18. Procurement requirements (demand side): certifications / national security validation mechanisms



Observations drawn from the use of international standards, national specifications and validation mechanisms on the demand side

- The procured products and services need to meet the following requirements:
  - 27 % of procurement requirements related to cryptographic modules are based on ISO 19790:2012 and ISO 24759:2017 or on FIPS 140-3.
  - 27 % of procurement requirements are related to product certifications – CC certification (cryptographic modules, cryptographic algorithms and security mechanisms, CSPs).
  - 37 % of procurement requirements are related to MSs national cryptographic specifications and national validation mechanisms.
- At the EU level, there is a margin of 37 % for the harmonisation of cryptographic security requirements and validation mechanisms (e.g., EU-approved algorithms).

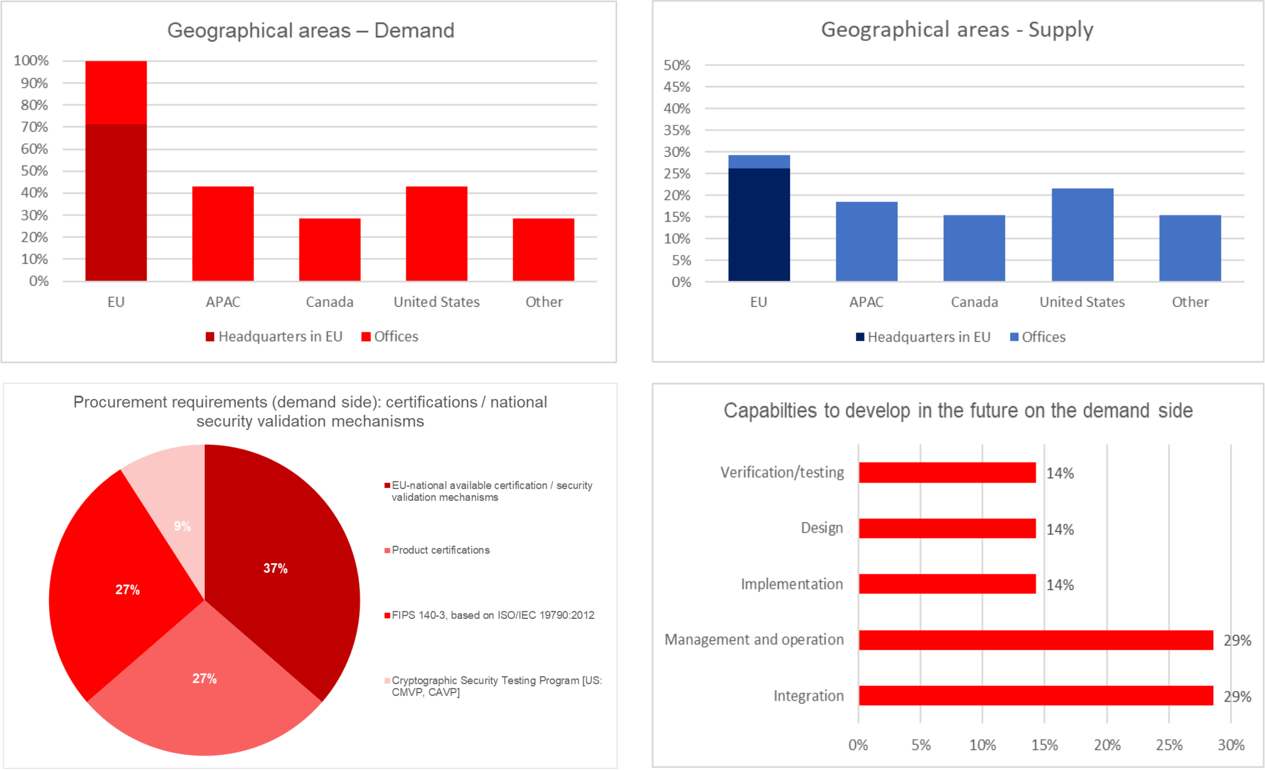
[63] https://www.wolfssl.com/license/fips/, accessed November 2023.

- This margin is indicative also of the need to develop an EU OSS repository for lightweight cryptographic libraries that would provide in a centralized way – a secure, clear, controllable and well-documented cryptographic library to increase resistance to side-channel attacks (also important for implementation of the Cyber Resilience Act (CRA).

6.4. PROJECTIONS ON THE EU CRYPTOGRAPHY MARKET

Based on the findings in this report, in particular the demand/supply demographics (see Sections 3.1.1 and 3.1.2) and the findings of the present chapter (see Sections 6.2 and 6.3), in this chapter we provide a reflection on the specificities of the EU cryptographic products and services market. Emphasis is given to the origin of supply and the nature of the required products and services on the demand side.

Figure 19. EU cryptography market dynamics (origin of supply and demand, procurement requirements, plan for developing capabilities by demand)



Observations drawn from demographics and procurement requirements

- The entire EU demand of cryptographic products and services (i.e., 100 %) is covered as follows:
  - ca 30 % through vendors located in the EU space, of which ca 25 % have headquarters in the EU, and
  - ca 70 % through vendors located outside the EU.
- Around 65 % of the EU demand indicates that cryptographic products and services of choice have to comply with national certifications and CC product certifications.

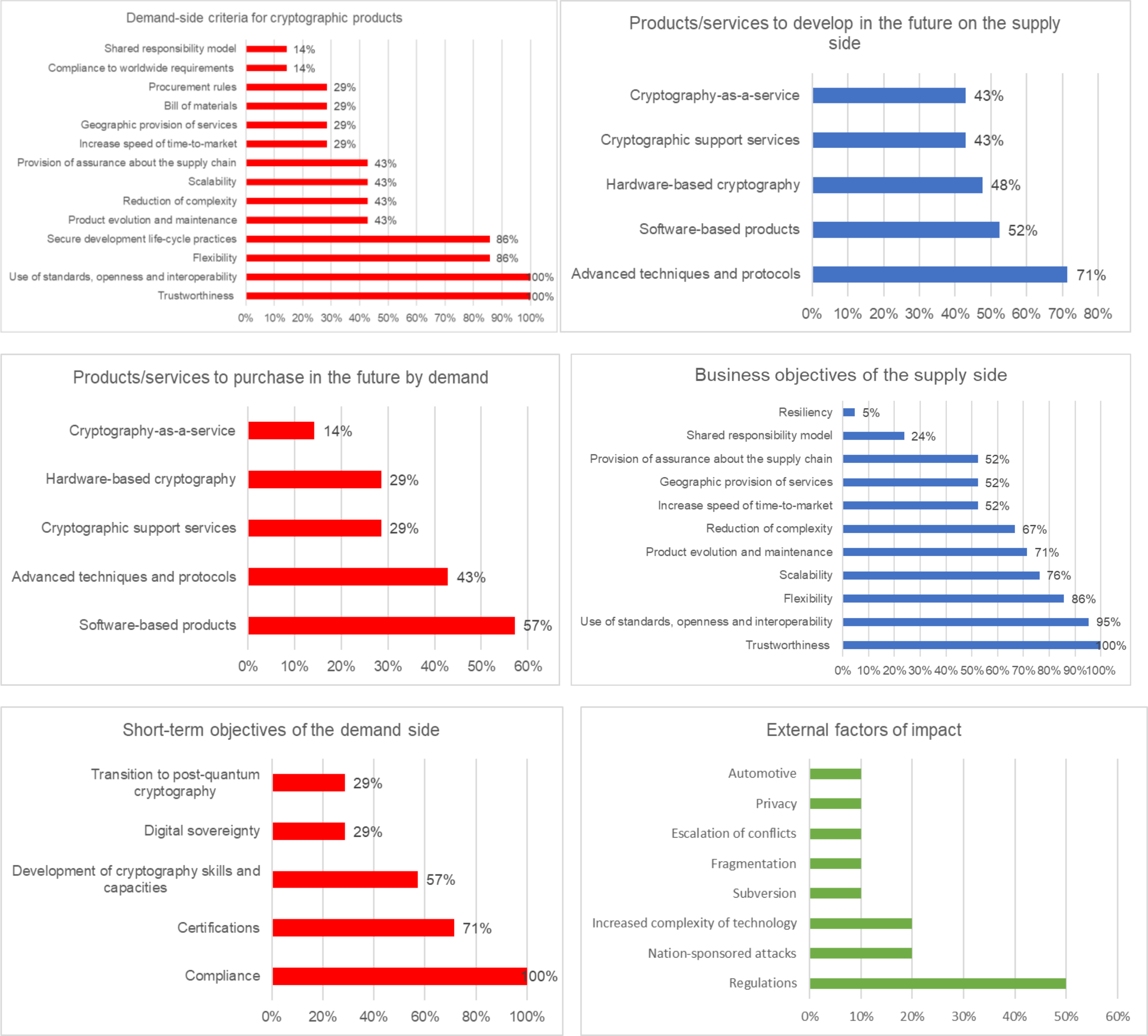
- Plans made by the demand side indicate that their cryptographic products and services needs will be covered by market products and services, while management and operation and integration will also increasingly be outsourced.
- While EU national certifications and CC product certifications currently have a significant market share (ca 65 %), it is expected that, in the medium to long term, they will dominate the EU cryptography market (i.e., going above 70 %).
- An EU-wide harmonisation of security requirements / validation of cryptographic algorithms will support the development of the secured products (e.g., reduction of costs, security of investments, etc.) and will facilitate the procurement of the cryptographic products with security metrics.
- Moreover, EU standards, specifications and guidelines on cryptography are required to enhance the assessment of secure implementation of cryptographic mechanisms at the EU level ([64]). EU vendors and service providers (e.g., CABs, test labs, integrators) may be in the position to increase their market shares within the EU.

[64] https://digital-strategy.ec.europa.eu/en/library/union-rolling-work-programme-european-cybersecurity-certification-0, accessed February 2024.

7. CRYPTOGRAPHIC PRODUCTS MARKET AND RESEARCH TRENDS

7.1. CRYPTOGRAPHIC PRODUCTS MARKET EVOLUTION

Figure 20. Findings on market evolution from all stakeholder types



Observations regarding market evolution by all types of stakeholders

- Use of standards, openness, interoperability and trustworthiness are very important for the demand-side stakeholders, when it comes to the choice of products. We expect that the market adoption of OS software will increase, especially in specific areas or in relation to crypto libraries; however, the CRA and compliance obligations related to the digital product lifecycle (updates, patching) might impact the adoption of OS solutions.
- There might be an opportunity for trustworthy providers of OS support and maintenance services. Flexibility and secure development practices are also important criteria choices.
- Through their objectives, suppliers show similar preferences and are investing in advanced techniques and protocols.
- Research underlines the role of regulation and the increased complexity of cryptographic products and services as the most influential factors for change in the cryptographic technology landscape. This is also reflected in demand objectives, with compliance being the highest prioritised objective.

Feedback on market evolution received from interactions with experts (external, ENISA) and open-source research

- The loss of encryption keys is a major concern, as is the correct configuration of encryption services. The greatest concern and largest gap in perception between supply and demand sides might be about who controls keys. Sometimes there is a problem of crypto inventory: what kind of crypto one organisation has and where the keys are.
- Debate around the bring your own encryption/key model (BYOE or BYOK), also known as hold your own key (HYOK), is moving attention from key control to key ownership, which is wrong. Real debate and the focus of the demand side should be on who controls keys. BYOK does not solve the problem since keys still can be in the cloud, not controlled by users. Strict governance rules are important in cases of key management outsourcing.
- There are some areas where OS cryptography is widely used, for example, OpenSSL, TLS, web services, client protocols and cryptographic libraries. As a matter of fact, the governance of OS cryptography has improved and there is no big gap in assurance/vulnerabilities between OS and proprietary cryptographic software. This may lead to a better market penetration of OS cryptography.
- It will not be easy for the supply side to monetise the use of OS libraries. Nonetheless, there might be some opportunities in services linked to OS, such as testing, consulting, integration, operation and management.
- Cryptographic policies and procedures are frequently not up to date, and have low priority on the demand side. Suppliers may fill this gap by providing up-to-date information on policies for the management and operation of their products and services.
- Through the emergence of AI, many privacy preserving techniques (FHE, homomorphic encryption, MPC, etc.) have also gained a lot of attention. It is expected that in the realm of AI market penetration, the role of privacy preserving techniques will be enhanced.
- FE, FHE and MPC are moving from research prototypes to the first emerging industrial applications. There is an opportunity for the EU’s supply side to enter this emerging

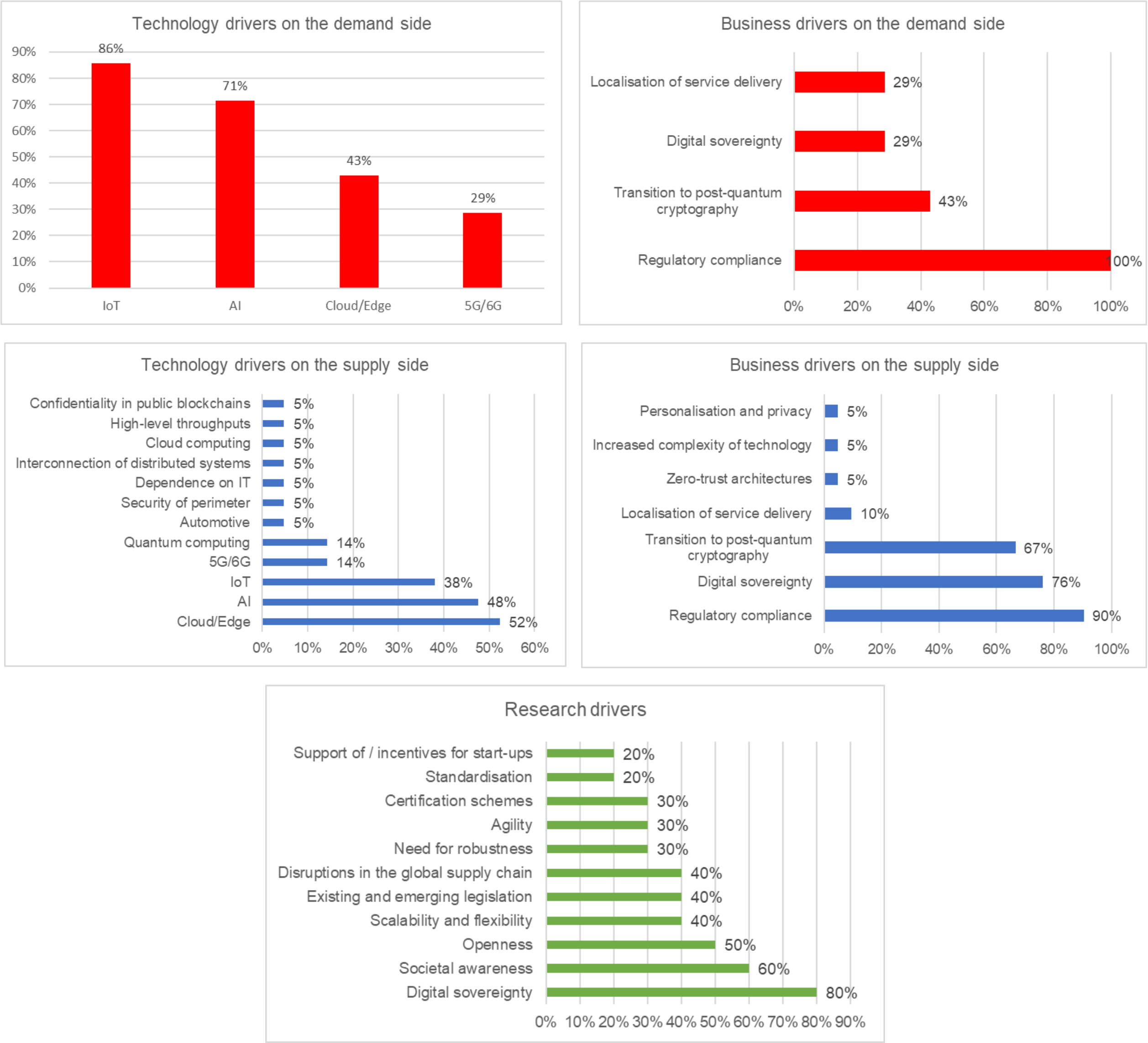
market segment. The EU is currently in the forefront, but if we look at HW support for this segment, the US is still more advanced.

- Training for software developers working on the development of cryptographic functions (e.g., the proper use of cryptographic libraries), but also integrators of cryptography in applications (e.g., using cryptographic keys, encrypting content, etc.), is in high demand as a means to enhance developers' cryptography skills.

7.2. CRYPTOGRAPHIC PRODUCTS DRIVERS AND BARRIERS

7.2.1. Market drivers

Figure 21. Findings on market drivers from all stakeholder types



Observations regarding market drivers from all types of stakeholders

- Just like in the business objectives, compliance is considered as a main market driver by the demand and supply sides, while emerging legislation is mentioned as a research driver.
- Digital sovereignty is considered by both the supply and research sides as an important driver for market and research, respectively.
- An interesting finding is the reference to societal awareness and certification schemes as research drivers.
- Technology drivers on the demand side, such as the adoption of IoT, are aligned with a growing supply of "lightweight" cryptography and research in advanced protocols (see findings in Section 7.3).

Feedback on market drivers received from interactions with experts (external, ENISA) and open-source research

Political, economic, societal, legal and environmental trends or developments that might impact the cryptographic market include the following.

- EU strategy on data sovereignty involves maintaining control over encryption and access to data, although encryption alone does not deal fully with sovereignty. The ability to control encryption keys separately from the cloud provider, for example, is very important.
- The demand side does not want to have too many suppliers, so convergence is likely to happen on the supply side. Many niche products will be absorbed.
- The detection and prosecution of criminal activity is also raising debate and regulation might need to be revisited in this respect. A proposal for client-side scanning is available, but EU parliament changed its position. There is no practical way to make cryptography safe where a single entity can have access, without creating vulnerability.
- Remote work and use of BYOD has increased the adoption of communication encryption solutions and data in transit encryption. The rapid growth of communication encryption solutions is likely to continue over the next few years.

Some additional business drivers for cryptography include the following.

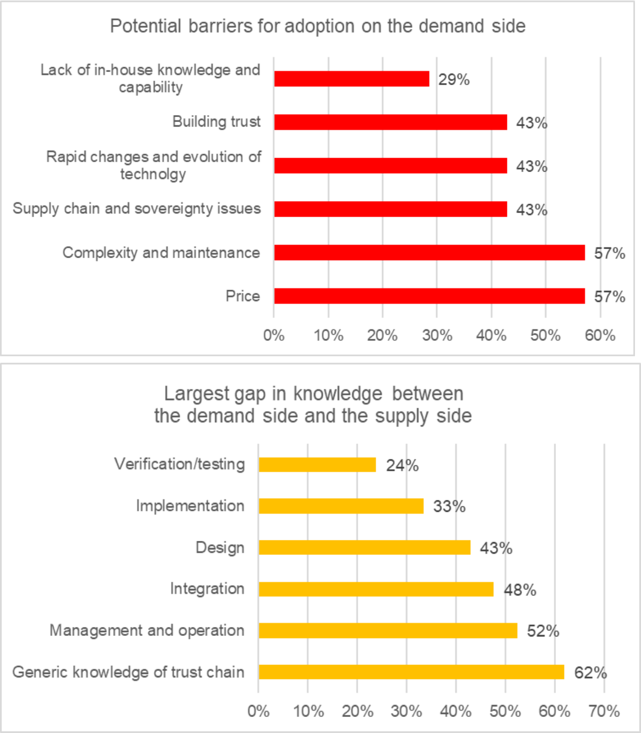
- Adoption of digital identities is also driving the encryption/cryptography market. Related technologies include cryptographic techniques and tools, deployed in an ecosystem with technology vendors, but also system integrators. Initiatives such as the eIDAS update (eIDAS2) are also driving this market segment. There will be short term demand from identity providers and cloud providers, for example for cryptographic key management services available on the EU Sovereign Cloud. Debate is open if cryptography to provide a unlikability is mature enough to meet eIDAS2 needs (in eIDAS unlikability is optional but recommended).
- Flexibility is driving many SMEs to shift to cloud-based solutions. Shift to cloud is typically not cheaper but offers more flexible support (on demand contracting of support), thus addressing the shortage of skills.
- Organisations also give priority to crypto agility, which is becoming one of the most important issues for demand-side stakeholders.
- Drivers resulting from technology and cryptography management issues include the following.

- Many DevOps teams have started to issue their own digital certificates, creating confusion since security teams do not fully know how many certificates have been issued, where they are managed and when they expire. There is an opportunity on the market for automated certificate lifecycle management and, as a result, many businesses are investing in PKI consolidation solutions.
- One of the drivers corresponds to the adaptation of cryptographic solutions to connected device (e.g., IoT), also referred as a “lightweight” cryptography. The speed of IoT adoption is creating new opportunities on supply side for cryptographic technique and tool providers. However, many IoT devices now have a larger capacity and the crypto that is running on them is not considered “lightweight” anymore. The message that AES was too expensive for many IoT devices is not true anymore, as there are cheap IoT devices with AES co-processors. Battery and communication HW might be more costly than crypto HW for IoT. In addition, OS HW (e.g., Open RISC-V) ([65]) is expected to have a positive impact on EU offerings.

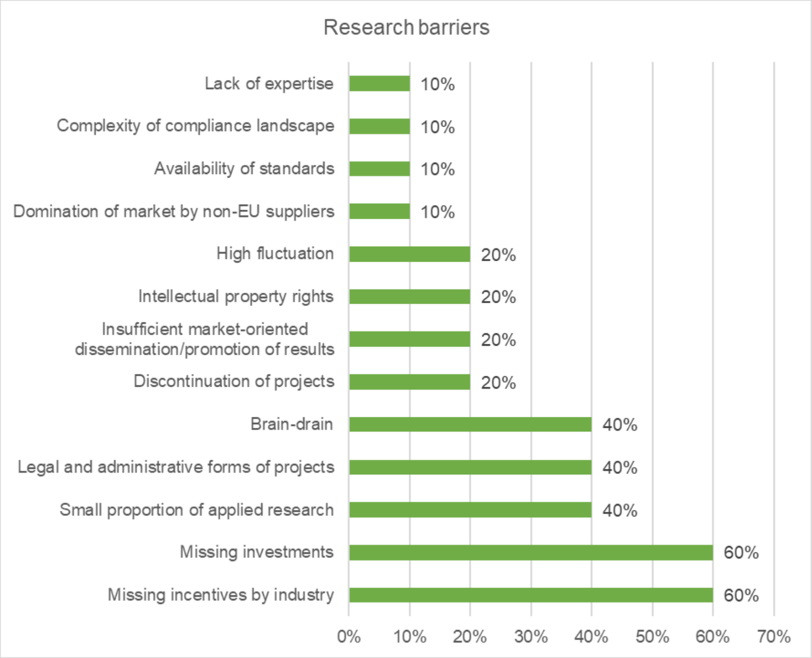
- Quantum-safe cryptography (QSC) or post-quantum cryptography (PQC) final standards are not expected until the end of 2024, but companies can start based on the draft standards. What is needed is also strategic agenda for migration. Although already envisaged in Germany and France and some sectors like the automotive industry, regulators should follow developments in the US with regard to migration roadmaps. It is advisable that migration and support plans are developed at the EU level.

7.2.2. Market barriers

Figure 22. Findings on market barriers from all stakeholder types



[65] https://riscv.org/, accessed November 2023.



Observations regarding market barriers by all types of stakeholders

- Price, complexity and maintenance, followed by trust, are the main barriers for adoption of cryptographic products and services from the demand side.
- The research indicates that there are insufficient incentives on the industry side and investment (public or private) for adoption of research on cryptographic products and services (and the necessary technology hereto).
- Sovereignty issues are perceived both as a barrier for adoption (in combination with supply chain threats) and as a business driver.
- Identified knowledge gaps between demand and supply sides may affect the evolution of the cryptography market, especially when it comes to knowledge of the trust chain which might be linked to transparency in cryptographic product supply chains.

Feedback on market barriers received from interactions with experts (external, ENISA) and open-source research

Identified barriers in the cryptography products/services market are as follows.

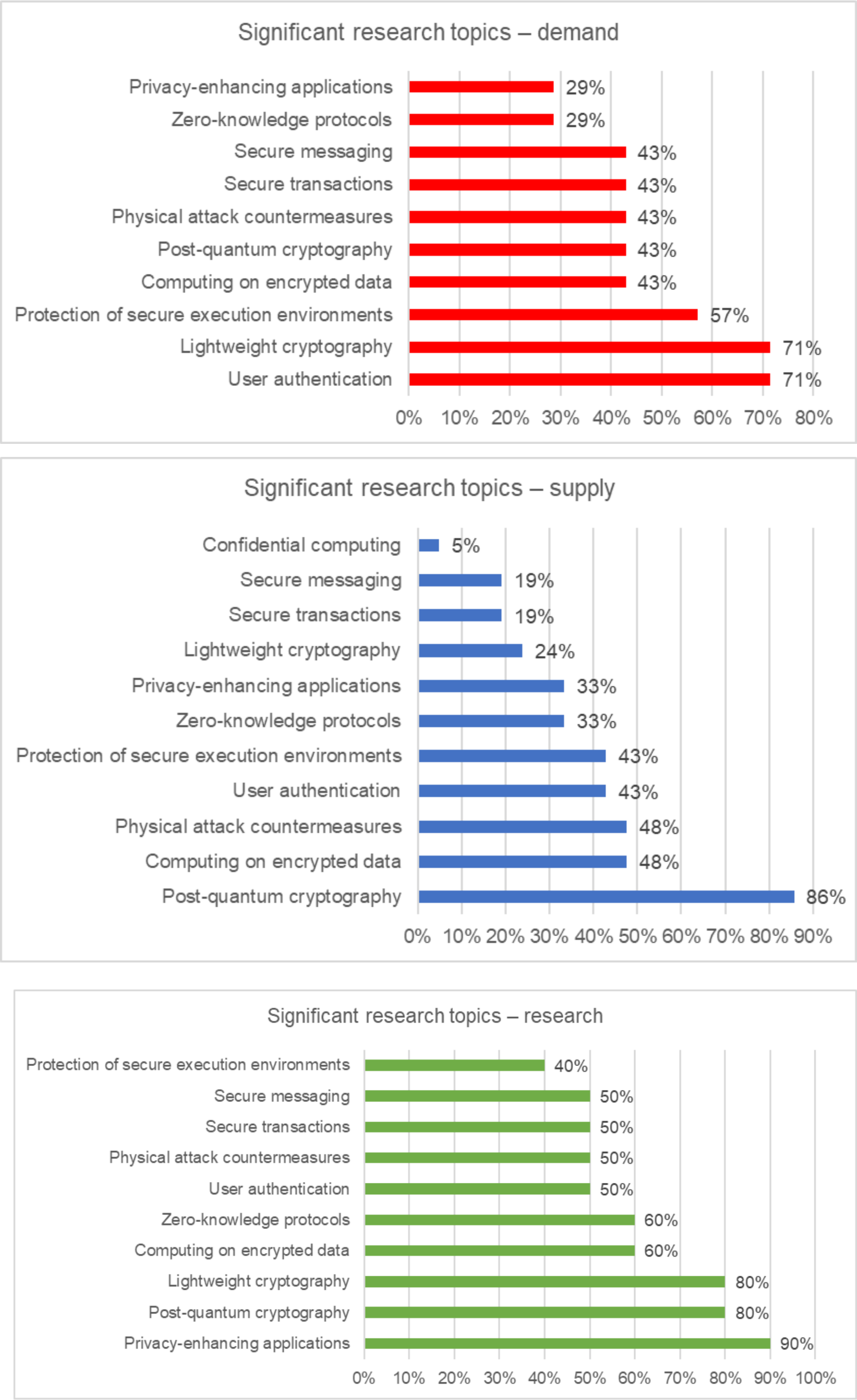
- The effect of cryptography on other security technologies and risk mitigation controls can be considered as a barrier: attackers, for example, might use encrypted content (i.e., data in transit or at rest) and orchestrate advanced malware attacks. Encrypted malware is usually not inspected and/or it is difficult to detect malicious signatures in encrypted content. The Zero Trust model assumes that encryption can create blind spots and hinder full visibility. This might be a downside of cryptography adoption, but there are solutions on the market that address this. In many organisations, for example, there is large scale TLS interception and ways to detect malicious traffic within the encrypted traffic.
- Threats are an important barrier to the use of cryptography. Physical attacks such as side-channel attacks have become one of the biggest threats to cryptosystems, especially in the IoT context. Fault attacks are an even bigger problem. Even if

adversary AI has had no big impact so far, it will very likely facilitate attacks on cryptography infrastructure, such as side-channel attacks.

- Cryptographic sustainability requirements lead to an increased interest in quantum communications (quantum key distribution) to respond to evolving technological approaches. This technology is limited to niche applications (data in transit over limited distance).
- The maturity of quantum communications (quantum key distribution) is still perceived as a barrier to the adoption of these types of solutions. It is still a topic that is mainly limited to research projects, without standards, and poor cost-effectiveness.
- Typical barriers in the cryptography market are the high costs for testing, certification and use of standards, all of those being mostly necessary for product development and deployment. The high costs of skills acquisition and maintenance is another barrier for small businesses. Seen in combination, these barriers are a serious threat to the viability of small businesses in the cryptography field.

7.3. CRYPTOGRAPHY RESEARCH AND INNOVATION IDEAS

Figure 23. Findings on research topics according to stakeholder types



Observations regarding research and innovation ideas by all types of stakeholders

- There is a different perception on significant research topics between demand, supply and research stakeholders. Lightweight encryption and user authentication are the two most important topics for the demand side, while the supply side is interested in post-quantum cryptography. Among researchers, the most important research topic is related to privacy enhancement, followed by lightweight and post-quantum cryptography.
- This was also expected, as we can find in OS literature many adaptations of cryptographic solutions to connected devices (e.g., IoT), also referred as a “lightweight” cryptography. In addition, advances in OS HW are expected to have an impact on cryptographic research.
- On the other hand, demand-side interest in user authentication topics is related to a wide area of cryptographic research, as well as policy (eIDAS2, PSD2) and societal trends (increased use of online service that need strong authentication). PEC, on the other hand, is an umbrella term for many different technologies, many of which originated or matured in the EU. Some are now being commercialised, but it is clear that researchers still expect many improvements and further evolution, also in relation to the use of AI for cryptography and the use of cryptography for AI. The high profile of this topic among researchers can also be explained by many projects funded in the area of dataspaces and the computing continuum, where PEC technologies play an important role.
- For the supply side, the most important research topic is post-quantum cryptography. As of 2023, quantum computers are not sufficiently mature for any large-scale computation, and definitely lack the processing power to break widely used cryptographic algorithms, but many providers are already considering the implementation of potentially quantum-safe algorithms into existing systems. The reason is that some applications require long-term confidentiality is that there are concerns about ciphertexts that are stored by adversaries today and that will be decrypted with the aid of quantum computers 15 to 20 years from now.

Feedback on research and innovation ideas received from interactions with experts (external, ENISA) and open-source research

- Several physical unclonable function (PUF) designs that exploit different physical parameters (e.g., volatile/non-volatile memory, circuit time delay characteristics) have been presented. PUF will likely be used as a key storage mechanism (weak PUF)[66].
- The first industrial applications of DNA cryptography and generative adversarial network (GAN) cryptography are expected to emerge in the next few years. DNA and GAN cryptography are among the topics to be investigated, but results will likely come in the long term.
- The cryptographic community is showing interest in new primitives based on mathematical problems that have not yet received sufficient attention. We can expect changes in the post-quantum context that involve different mathematical problems, but the impact will be long term, at least 5 to 10 years. In addition, we can assume that – as is typical in cryptography – researchers will identify some parameters or approaches that are weak and others that are more robust. There is also a strong need to develop advanced cryptographic primitives (such as anonymous credentials) based on post-quantum safe building blocks.
- There is research being done into indistinguishability obfuscation (iO), but it is far from adoption and being used in practice. It will not be ready until the next decade.

[66] Weak PUF mechanisms are not considered mature as challenge/response mechanism (strong PUF).

8. CONCLUDING REMARKS

This chapter summarises the findings of this market analysis. The aim of this summary is to highlight the most important issues identified in the cryptography products/services market and to deliver proposals that will facilitate its functioning. The following findings combine various interrelated cryptography topics covered in this analysis to express trends (T), gaps (G), barriers (B), regulatory related (R) and research (R & D) topics. For each of the findings, a practical proposal for addressing the identified issues is being made.

It should be noted that these points represent the main findings: in the analysis and observations made in the previous chapters, additional detailed cryptography market facts and issues can be found that may be of interest to readers with a special interest in the topics covered in each chapter.

8.1. MAIN MARKET CHARACTERISTICS AND TRENDS

T1 – Adoption of open-source cryptography
The usage patterns of cryptographic products revealed the notable importance of OS libraries for both the demand side and the supply side. It is expected that the market adoption of OS will increase, especially in specific areas or in relation to crypto libraries. As governance of OS cryptography has improved, there is no big gap in assurance/vulnerabilities between OS and proprietary cryptographic software. At the same time, CRA and compliance obligations related to digital product lifecycle (updates, patching) will introduce additional compliance requirements for software in general and in particular to OSS. There might be an opportunity for trustworthy providers to implement OS support and maintenance services but also intellectual property (IP) issues related to the use of OSS. At the same time, ongoing discussions with the OS community may enhance secure development and maintenance practices.

Practical proposal
Elaborate on state-of-the-art security practices of OS development. Allow the OS community and industry to engage in a dialogue to find solutions for viable secure life cycle practices, including IP matters.

T2 – Emergence of cryptographic technologies
There are some emerging cryptographic technologies that appear in the list of products. It might be of interest to observe these developments, as many of those might represent areas of new cryptographic products and services that respond to regulatory requirements (e.g., eIDAS). Examples include post-quantum cryptography, quantum key distribution, trust anchors, qualified digital signatures, confidential computing, qualified timestamps, eID cryptographic software components, secure login tokens and secure MPC. This trend becomes evident in plans made by the supply side (see Figure 13): advanced techniques and protocols are the highest priority for future product developments. Moreover, the high priority of the business objective of the transition to post-quantum cryptography is a clear indication of this trend.

Practical proposal
New cryptographic technology areas to be envisaged within upcoming regulation and standardisation, by engaging experts from companies developing such solutions. This will allow for a better level of preparation of EU-based companies in maintaining a good level of product design and development within the EU, while increasing maturity and early-to-market entry.

T3 – Uptake of cryptography-as-a-service

While currently cryptography-as-a-service is at a low level of use on the demand side, its use is expected to grow in the medium term (ca 2–3 years). This becomes evident from the trend on the demand side towards reducing implementation capabilities and increasing cryptography operation activities. Supply-side organisations, on the other hand, have increased their activities relating to cryptography-as-a-service, including key-management-as-a-service, user-authentication-as-a-service, cloud cryptographic services and HSMs. This becomes evident from plans made on the supply side to prioritise cryptography-as-a-service and HW-based cryptography (see Figure 13).

Practical proposal

Given the assessed high appetite on the demand side for cryptographic training, courses should be offered about the advantages gained from the use of cryptography-as-a-service in mastering the complexity of cryptography infrastructures and chains of trust.

T4 – Important role of medium/large organisations

The percentage of medium/large organisations participating in the survey, on both the demand side and the supply side, is indicative of the survivability of sizable market actors in the field of cryptography. Economic capacity and availability resources with a high degree of specialisation are vital existential characteristics in this market. Such organisations have increased the need to engage specialised resources.

Practical proposal

Incentivise the creation of branches close to educational institutes that are specialised in cryptography.

T5 – Adoption of digital identities

The adoption of digital identities by Member States is driving the cryptography market. The main compliance target in this market segment will be initiatives like the eIDAS update (eIDAS2). In the short to medium term, this trend may generate demand from identity providers and cloud providers, for example for cryptographic key management services available on the EU Sovereign Cloud.

Practical proposal

Observe eIDAS initiatives (e.g., through an observatory) to trace the state of product design, implementation, compliance with standards and compliance with certification schemes. Define support actions, based on observables. The state-of-play regarding eIDAS initiatives can be published on ENISA’s website, including, the cryptography for the eIDAS wallet package of technical specifications, standards and CSP PPs, etc.

T6 – The important role of SMEs in innovation

Smaller organisations seem to be a driving force for innovation in cryptography (on both the supply side and the research side). Through the incubation/take-up of research results and by generating a higher number of scientific results on cryptography, they demonstrate high degrees of specialisation and high turnover rates in cryptographic business. This seems to be the main reason why such companies are often taken over by larger organisations willing to buy-in innovation and cryptography skills. Together with the high costs associated with achieving the required assurance levels for their products, mergers and acquisitions are also factors that contribute to the lower survivability of such structures on the cryptography market.

Practical proposal

Through the generation of favourable conditions, spin-offs from active cryptography research institutes should be promoted, with the aim of increasing the uptake of ideas with high levels of technical readiness. Cooperation with larger organisations and investments (public, private) should be incentivised.

T7 – Importance of cryptography observatory
Due to its role in the implementation of protection in cyberspace, observing developments on the cryptography products and services market on a permanent basis is an important activity. Surveys like the one developed for this report could be kept online, with the aim of collecting and analysing market data at regular intervals.

Practical proposal
A European centre of excellence in cryptography or any national competence centre could be funded to implement an observatory/market surveillance in the area of cryptographic products and services. The feasibility of funding options from available EU instruments could be sought.

8.2. MAIN GAPS

G1 – Changing cyberthreat perceptions
The big differences in stakeholder perceptions regarding threat exposure of cryptographic products and services raise concerns about their awareness. Some of the most pertinent cyberthreats, for example, appear as relatively low priorities on the “radar” of relevant stakeholders, these include the abuse of misconfigurations, side-channel attacks, spoofing or phishing abusing user login, downgrade attacks targeting the algorithm version, and the physical manipulation of devices, just to mention the most important ones.

Practical proposal
Feed threat intelligence platforms with cryptography related cyberthreats, keep all sides informed about these threats and inform the demand-side about incidents and the vulnerabilities of cryptographic components.

G2 – Cryptographic capability gap
Demand-side capabilities, assessed by suppliers as per company size, show a capability gap between small and large organisations. This gap might be counterproductive for the deployment of cryptographic product and services, in particular for SMEs that are involved in sectors with higher cryptography needs/requirements. The largest gap between demand and supply – as assessed by suppliers – lies in the generic knowledge of the trust chain and management/operation of cryptographic products and services. This gap may generate significant security issues in the usage of products and services and, in the medium term, needs to be closed.

Practical proposal
Given the assessed high appetite on the demand side for cryptographic training, courses should be offered on methods for mastering the complexity of cryptography infrastructures, the management/operation of cryptographic products and services, in particular key management, and chains of trust.

8.3. MAIN BARRIERS

B1 – High complexity of cryptography
The complexity of cryptography is a main market barrier for the demand side. Complexity, the volatility of used technologies/approaches, operation, maintenance and knowledge gaps are the main barriers to the adoption of products and services. These barriers are particularly relevant for small demand-side organisations.

The supply side considers as barriers the high costs associated with testing, certification and the use of standards, all of which, however, are necessary for product development and deployment. The high cost of skills acquisition and maintenance is another barrier for small businesses. Combined, these barriers are a serious threat to the viability of small suppliers acting in the cryptography field.

Practical proposal
This barrier can be removed through proposals made under trends T3, T4 and T6 (see Section 8.1).

8.4. MAIN POINTS WITH REGULATORY RELEVANCE

R1 – Harmonisation of supply-chain issue
Regulators engage mainly in the areas of cryptography usage, certifications and compliance, while their policy principles include mainly the reliance on algorithmic methods certified for trust, the careful selection of cryptographic approaches and a commitment to adhering to standards. Supply-chain issues are a priority, and regulators foresee rules regulating the import and export of cryptographic products and services. There are also some approaches to capture the supply-chain information of available products (bills of materials (BOMs)). Nonetheless, the required, EU-harmonised practical guidelines for managing the security of the supply-chain for cryptography are not available.

Practical proposal
EU-wide, harmonised guidelines for managing the security of the supply-chain of cryptographic products and services need to be developed by capturing any available good practices, such as an inventory or catalogue of cryptographic products and services or a vulnerability reporting mechanism for cryptographic products and services.

R2 – Market mobilisation through regulation
Regulatory compliance, together with digital sovereignty, are the top business drivers on the supply side, indicating the major role of policy issues in the cryptographic products/services supply business. As encryption plays an increasingly important role in the EU's digital economy, becoming necessary in ensuring privacy and national security, some principles have been indicated as being embedded in the development of national policy, such as: trust in cryptographic methods based on certification; the market-driven development of cryptographic methods; standards for cryptographic methods and international cooperation.

Practical proposals

- Development of EU-harmonised technical specifications for a cryptographic service provider (CSP) adapted to improve the certification processes, such as 5G network components (EU5G), cloud solutions (EUCS) and the European digital identity (EUDI).
- Development of harmonised criteria at the EU level for the risk-based selection of recommended cryptographic mechanisms, together with harmonised evaluation procedures that are publicly available and, if possible, automated.
- The development of CSP-Light harmonised technical specifications with lower assurance levels could "provide cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication"[67], which might be used for small devices – IoT and other products in the scope of the CRA.

R3 – Protection of IPR, BOM
The GDPR, the proposal for an ePrivacy regulation and eIDAS and IPR– protection of intellectual property rights are the three EU legal instruments seen by the vast majority of respondents from the demand, supply and regulators sides as the most relevant EU legislation with which cryptographic products and/or services have to comply. Moreover, from the findings of this analysis it becomes clear that privacy has gained attention from various stakeholders on the cryptography market (demand, supply, research), but also within society. Through the emergence of AI, many privacy preserving techniques (e.g., FHE, HE, MPC) have also gained a

[67] https://commoncriteriaportal.org/files/epfiles/1139V2b_pdf.pdf, p.13, accessed November 2023.

lot of attention. It is expected that in the realm of AI market penetration, the role of privacy preserving techniques will be enhanced and new technologies and products will be developed.

Practical approach
In order to increase the security of the EU economy, one important aspect is to have visibility and transferability of the IPR via BOMs, but also to protect the IPR. The EU and its Member States will be better equipped to identify and assess risks to the EU's economic security, through a strategic tool dealing with inventory and the protection of IPR via cryptography.

R4 – Strategies for the migration to post-quantum cryptography
Post-quantum (quantum-safe) cryptography final standards are not expected until the end of 2023. Compliance efforts can start based on draft standards. Besides standardisation, a strategic agenda for migration is also needed. Although already envisaged in Germany and France and some sectors, for example, automotive, regulators should follow developments in the US with regard to migration roadmaps. It is advisable that migration and support plans are developed at the EU level.

Practical approach
Kick off EU-wide migration strategies for post-quantum (quantum-safe) cryptography by engaging all necessary actors.

R5 – Fostering lightweight cryptography
Technology drivers identified by both the demand and supply sides are related to the market potential of IoT adoption. As lightweight cryptography is the main control by which to secure such components, it becomes critical for the related market to provide widely accepted, harmonised cryptographic functions that are cost-effective and easy to implement/integrate. Combined with the existence of OS cryptographic libraries, the deployment of lightweight ready-to-use functions could be an important driver for market development. Furthermore, this will provide grounds for the implementation of the CRA, but also for the harmonisation of the validation process of OSS cryptographic libraries.

Practical approach
Develop an EU OSS repository for lightweight cryptographic libraries that would provide a secure, centralised, clear, controllable and well-documented cryptographic library, together with guidance to further help vendors for integrating OS components into IoT products.

8.5. MAIN RESEARCH TRENDS

The following main research trends have been assessed throughout this analysis.

R & D1 – PEC top research priority
PEC is an umbrella term for many different technologies, many of which originated or matured in the EU. Some are being commercialised now, but it is obvious that researchers still expect many improvements and further evolution, particularly in relation to the use of AI for cryptography. High score of this topic among researchers can also be explained by many projects funded in the area of dataspaces and computing continuum, where PEC technologies play an important role.

R & D2 – New cryptographic primitives
The cryptographic community is showing interest in new primitives based on mathematical problems that have not yet received sufficient attention. We can expect changes in the post-quantum context that involves different mathematical problems, but the impact will only be felt in the long term, at least 5 to 10 years in the future. In addition, we can assume that researchers will find new flaws in these new primitives as well.

R & D3 – Other emerging technologies

Several other findings from this analysis regarding emerging research trends are: DNA-based cryptography, indistinguishability obfuscation, the impact of advanced OS HW on cryptography research, lightweight cryptography, zero-trust protocols, secure execution environments, computing on encrypted data, and more (see also Section 7.3).

Practical proposal

Make cryptography research themes the focal point of funding and research deployment frameworks (e.g., launched by the Commission, European Cybersecurity Competence Center or national cybersecurity funds etc.).

1.ANNEX A: LEGAL AND POLICY FRAMEWORK – EXAMPLES OF INSTRUMENTS

This annex provides an overview of binding and non-binding (legal) instruments that, according to the data collected via the survey, play a role in shaping the demand and the supply of cryptographic products and services in the EU.

First, some relevant international instruments, export restriction measures and non-EU legislation are addressed; secondly, some relevant EU legislation is considered; thirdly, some examples of national legislation are given, mainly from Member States; finally, some relevant legislative initiatives and guidelines are mentioned.

The main components of this framework are listed and briefly described in the table below. Although this list of legal instruments is non-exhaustive and their descriptions do not go into much detail, this shows which instruments, according to the respondents to the survey, are relevant and set legal requirements that shape the demand and the supply of cryptographic products and services.

Table 7. Legal and policy framework - main instruments

Name of the instrument	Description of the instrument
International instruments and export restriction measures, non-EU-country legislation	
Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ([68])	"The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies" ([69]). Most Member States are participating in this arrangement and apply controls on the items included in the list of dual-use goods and technologies ([70]), which includes cryptography. Although the arrangement is not an international treaty and it is not binding, it is important because the "EU export controls reflect commitments agreed upon in key multilateral export control regimes such as … the Wassenaar Arrangement" ([71]). Private organisations use cryptography to secure transactions, authenticate users, sign electronic documents, encrypt communication channels, secure sensitive data, secure end devices, etc. End users use cryptographic functions to secure authentication, communication and stored data.
International and EU sanctions ([72])	There "are sanctions imposed by the UN which the EU transposes into EU law. Secondly, the EU may reinforce UN sanctions by applying stricter and additional measures … [f]inally, the EU may also decide to impose fully autonomous sanctions regimes" ([73]). For instance, the "EU has imposed … sanctions against Russia in response to the war of aggression against Ukraine" and the "list of sanctioned products includes among others … a number of dual-use

[68] https://www.wassenaar.org/, accessed November 2023.
[69] https://www.wassenaar.org/, accessed November 2023.
[70] https://www.wassenaar.org/app/uploads/2022/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-Dec-2022.pdf, accessed November 2023.
[71] https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en, accessed November 2023.
[72] https://www.eeas.europa.eu/eeas/european-union-sanctions_en, accessed November 2023.
[73] https://www.eeas.europa.eu/eeas/european-union-sanctions_en, accessed November 2023.

	goods (goods that could be used for both civil and military purposes), such as drones and software for drones or encryption devices" ([74]).
US encryption and export regulations ([75])	US for instance "regulate cryptography for export in international trade as a dual-use good" and export controls therefore apply.
EU legislation	
Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items ([76])	The 2021 export control regulation "upgrades and strengthens the EU's export control toolbox to respond effectively to evolving security risks and emerging technologies, and allows the EU to effectively protect its interests and values. […] The EU controls the export, transit, brokering and technical assistance of dual-use items so that it can contribute to international peace and security and prevent the proliferation of weapons of mass destruction" ([77]).
Directive (EU) 2019/1937 on the protection of whistleblowers ([78])	This directive setting out whistleblower protection in the EU guarantees "a high level of protection for whistleblowers who report breaches of EU law by setting new EU-wide standards". It establishes "safe channels for reporting both within an organisation and to public authorities". [It also protects] "whistleblowers against dismissal, demotion and other forms of retaliation" [and requires] "national authorities to inform citizens and provide training for public authorities on how to deal with whistleblowers" ([79]).
Regulation (EU) on digital operational resilience for the financial sector (DORA) ([80])	"DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies) -related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all member states. The core aim is to prevent and mitigate cyber threats" ([81]).
EU legal framework for the protection of intellectual property rights (IPR)	"The EU regulatory framework for IPR is based on EU regulations, directives and existing international intellectual property agreements. It provides protection in all EU Member States, thus creating a single EU system consisting of EU and national IPRs" ([82]). More specifically, the EU IPR regulatory framework consists of: (a) the Charter of Fundamental Rights of the European Union, Article 17(2); (b) the EU regulatory framework for trademarks (e.g., Regulation (EU) 2017/1001 on the European Union trade mark, Directive (EU) 2015/2436 to approximate the laws of the Member States relating to trade marks); (c) EU regulatory framework for designs; (d) EU regulatory framework for geographical indications; (e) EU IPR enforcement framework.
Regulation (EU) 2016/679 – general data protection regulation (GDPR) ([83])	"The general data protection regulation (GDPR) protects individuals when their data is being processed by the private sector and most of the public sector. The processing of data by the relevant authorities for law-enforcement purposes is subject to the data protection law enforcement directive (LED) instead […]. It allows individuals to better control their personal data. It also modernises and unifies rules, allowing businesses to reduce red tape and to benefit from greater consumer trust. It establishes a system of completely independent supervisory authorities in charge of monitoring and enforcing compliance. It is part of the European Union (EU) data protection reform, along with the data protection law enforcement

[74] https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russiaexplained/, accessed November 2023.

[75] https://www.bis.doc.gov/index.php/policy-guidance/encryption, accessed November 2023.

[76] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, OJ L 206, 11.6.2021, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32021R0821, accessed November 2023.

[77] https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en, accessed November 2023.

[78] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, 26.11.2019, p. 17, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937, accessed November 2023.

[79] https://commission.europa.eu/system/files/2018-04/placeholder_11.pdf, p.2, accessed November 2023.

[80] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333, 27.12.2022, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32022R2554, accessed February 2024.

[81] https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act, accessed February 2024.

[82] https://op.europa.eu/webpub/eca/special-reports/intellectual-property-rights-06-2022/en, accessed February 2024.

[83] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation), OJ L 119, 4.5.2016, pp. 1. Successive amendments to Regulation (EU) 2016/679 have been incorporated into the original text, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed February 2024.

	directive and Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies […]" ([84]).
Regulation on privacy and electronic communications ('ePrivacy regulation') (Proposal) ([85])	The Commission proposed a regulation on privacy and electronic communications to update current rules on technical developments and to adapt them to the GDPR, in order to reinforce trust and security in the digital single market ([86]). The proposed regulation will increase the protection of people's private life and open up new opportunities for business ([87]). "The proposal for a regulation for ePrivacy rules for all electronic communications includes: New players […]. Stronger rules […]. Communications content and metadata […]. New business opportunities […]. Simpler rules on cookies […]. Protection against spam […]. More effective enforcement […]" ([88]).
eIDAS ([89])	"The current rules on electronic identification and trust services for electronic transactions in the internal market (i.e., the eIDAS regulation) dating from 2014 aim at making national eID schemes interoperable across Europe in order to facilitate access to online services. In the EU digital strategy 'Shaping Europe's Digital Future', the Commission announced that it will review the eIDAS Regulation to improve its effectiveness, extend its application to the private sector and promote it" ([90]). For eIDAS2, see below.
eIDAS2 ([91])	On 3 June 2021 the Commission published its proposal amending the eIDAS regulation as regards establishing a framework for European Digital Identity (EUDI) Wallets. An EUDI wallet scheme will improve the eIDAS framework and extend its application to the private sector. Users will have the choice of a universally accepted EUDI wallet, which will allow for safer use of services online and enhance citizens' control over their personal data and privacy while respecting user anonymity. The proposed regulation was adopted and officially published on 30 April 2024.
eIDAS cryptographic requirements for the interoperability framework ([92])	These technical specifications were developed in line with the eIDAS regulation and with Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework, to help Member States to develop their own eIDAS-compliant implementation. "Within the eIDAS interoperability framework […], communication between eIDAS nodes […] is performed via the citizen's browser. […] [T]he content of the communication between eIDAS nodes is performed using cryptographically protected SAML [Security Assertion Markup Language] messages. To secure the transport layer of this communication between these components and the citizen's browser, TLS is used. This document specifies cryptographic requirements for the protection of the SAML communication as well as on the usage of TLS within this communication" ([93]).
NIS2 directive ([94])	The directive on measures for a high common level of cybersecurity across the Union (the NIS2 directive) is the EU-wide legislation on cybersecurity which provides legal measures to boost the overall level of cybersecurity in the EU ([95]).

[84] https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html#:~:text=Regulation %20(EU) %202016 %2F679 %20of %20the %20European %20Parliament %20and,1 %E2 %80 %938, accessed February 2024.

[85] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52017PC0010, accessed February 2024.

[86] https://digital-strategy.ec.europa.eu/en/library/stronger-privacy-rules-electronic-communications, accessed November 2023.

[87] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications, accessed November 2023.

[88] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, accessed November 2023.

[89] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv %3AOJ.L_.2014.257.01.0073.01.ENG, accessed November 2023.

[90] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid?sid=7201, accessed February 2024.

[91] After completion of the drafting of this report, and during the proofreading stage, the eIDAS2 (Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework) was adopted and published at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183, accessed June 2024.

[92] eIDAS eID Technical Subgroup, "eIDAS cryptographic requirements for the interoperability framework – TLS and SAML – v.1.4", eIDAS Technical Specifications – 31 October 2023, https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+eID+Profile?preview=/467109280/704841745/eIDAS%20Cryptographic%20Requirement%20v.1.4_final.pdf, accessed November 2023.

[93] Ibid, p.1, accessed November 2023.

[94] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 directive), PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80, https://eur-lex.europa.eu/eli/dir/2022/2555, accessed February 2024.

[95] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, accessed November 2023.

Cybersecurity Act (CSA) ([96])	The Cybersecurity Act strengthens ENISA and establishes a cybersecurity certification framework for products and services.
Cyber Resilience Act (CRA) ([97]) (Proposal)	“The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products” ([98]).
Radio equipment directive delegated act ([99])	“The delegated act to the Radio Equipment Directive […] aims to make sure that all wireless devices are safe before being sold on the EU market” ([100]).
National legislation (examples)	
National legislation from France	• Référentiel général de sécurité (RGS) ([101]) The RGS defines rules and guidelines to be enforced by information systems that are operated by government or public entities and that allow electronic exchanges or communications with other publicly operated systems or with French citizens. Annex B1 defines rules and recommendations regarding the selection of cryptographic mechanisms and key sizes. Annex B2 defines rules and recommendations regarding cryptographic key management. Annex B3 defines rules and recommendations regarding authentication mechanisms. • Law no. 2004-575 of 21 June 2004 on confidence in the digital economy (LCEN) ([102]), specified by its implementing decree no. 2007-663 of 2 May 2007 The supply, import, intra-community transfer and export of cryptology equipment are subject, with certain exceptions, to various control mechanisms. Under the terms of these texts, a company wishing to import or supply a crypto-enabled item on French territory must first make a declaration to ANSSI. If the item is transferred to another Member State or exported outside the EU, an export authorisation must also be issued by the agency.
National legislation from Germany	• The NIS2 Implementation Act ([103]). • Draft law to implement the critical entities resilience directive and strengthen the resilience of critical assets ([104]). • Act on the Federal Office for Information Security (BSI Act – BSIG) ([105]).
National legislation from Italy	• Decree-Law 82 – 14/06/2021 ([106]), which in Article 7, paragraph 1, point (m-bis) gives the Cybersecurity National Agency (ACN) the right to undertake adequate initiatives to promote cryptography as a tool to guarantee cybersecurity.
National legislation from Sweden	Protective Security Ordinance (2021:955) ([107]).

[96] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), PE/86/2018/REV/1, OJ L 151, 7.6.2019, p. 15, https://eur-lex.europa.eu/eli/reg/2019/881/oj, accessed February 2024.

[97] Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454, accessed February 2024.

[98] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act, accessed November 2023.

[99] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that directive, C/2021/7672, OJ L 7, 12.1.2022, p. 6, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32022R0030, accessed February 2024.

[100] https://single-market-economy.ec.europa.eu/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en, accessed November 2023.

[101] Référentiel général de sécurité (RGS), https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/, accessed February 2024.

[102] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’ économie numérique (telle que modifiée jusqu’ au 8 août 2015), https://www.wipo.int/wipolex/en/text/386032, accessed February 2024.

[103] Das NIS2 Umsetzungsgesetz,https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html, accessed February 2024.

[104] Referentenentwurf des Bundesministeriums des Innern und für Heimat Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz ‐ KRITIS-DachG).

[105] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz ‐ BSIG), https://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html, accessed February 2024.

[106] Decreto-Legge 14 Giugno 2021, n. 82, https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-08-04&atto.codiceRedazionale=21A04841, accessed February 2024.

[107] Säkerhetsskyddsförordning (2021:955), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-2021955_sfs-2021-955/, accessed February 2024.

Legislative proposals and guidelines	
Organisation for Economic Co-operation and Development (OECD), ‘Recommendation of the Council concerning guidelines on cryptography policy’ ([108])	Recommendations for basic issues that countries should consider in establishing cryptography policies at national and international levels.
Commission Recommendation on internal compliance programmes for controls of research involving dual-use items (EU) 2021/1700 ([109])	This recommendation provides guidance “to help research organisations … and their researchers, research managers and compliance staff to identify, manage and mitigate risks associated with dual-use export controls and to facilitate compliance with the relevant EU and national laws”.

[108] https://web-archive.oecd.org/2023-09-07/350059-cryptography.htm, accessed February 2024.

[109] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items C/2021/6636, OJ L 338, 23.9.2021, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32021H1700, accessed February 2024.

2. ANNEX B: CRYPTOGRAPHIC PRODUCTS MARKET ANALYSIS QUESTIONNAIRES

ENISA formulated the following questions for stakeholders for its cryptographic products cybersecurity market analysis. They may serve as a model or template for questions that are pertinent to other cybersecurity markets. Some questions may be more relevant than others, therefore the market analyst should feel free to adapt the questions as they see fit. The analyst may have other questions of particular relevance to their market segment. The answers to the questions provide data for the analysis.

Demand-side questionnaire

Stakeholder profile

- Indicate number of your employees in all areas of activity.
- Indicate approximate annual revenue (for NGO or public administration, please indicate operational budget).
- Indicate approximate budget spent for cybersecurity products and services (percentage of the total revenues).
- Indicate approximate budget spent for cryptography products and services (percentage of the total revenues).
- Indicate investments in cybersecurity research, development, and innovation, including cryptography (percentage of the total revenues).
- Indicate main sector of activity of your company.
- Does your company have headquarters established in the EU?
- In which geographical areas does your company have offices?
- What is the legal structure of your company?
- Is your company owned with a majority of EU capital?

Cryptography adoption and use

- In terms of use of cryptography for your business, would you describe your company as:
  - User of low-level cryptographic functions (algorithms, primitives, or methods)
  - User of cryptographic products (software, hardware)
  - User of cryptographic services (key management, systems, protocols, and technology)
  - User of cryptographic applications (that include previous two categories)
  - Use of other related services (please specify).
- Which cryptographic products and services have you already implemented, deployed or used?
- In terms of cryptographic policy and processes, do you have:
  - Data classification policy
  - Specific cryptographic processes and procedures
  - Dedicated cryptography use policy
  - Cryptography related policy is a part of cybersecurity policy
  - Cryptography as subject to risk assessments
  - Other related cryptographic processes and procedures.
- Indicate cases where you use encryption techniques.

Cryptographic needs and capabilities

- Which criteria/characteristics do you consider for the choice of cryptographic products and services?
- Do you maintain internal (in-house) cryptographic capabilities?
- Do you plan to develop these cryptography-related capabilities in the future, (indicate which one and when)?
  - Cryptography design

  - Cryptography implementation
  - Cryptography integration
  - Cryptography management and operation
  - Cryptography verification/testing
  - Other cryptography capability.
- Do you have providers of cryptographic products/services? If yes in which geographic areas are they located?
- Which of the following cryptographic products or services does your organisation plan to purchase or implement (please specify time horizon)?
  - Advanced techniques and protocols
  - Cryptographic support services
  - Cryptography as a service
  - Hardware based cryptography
  - Software based products
  - Other.
- Where does your organisation store encryption keys for the products it offers?
- What are the objectives you want to address with regard to cryptography in your organisation (short-medium term)?

Legislation and certification

- What legislation do you have to comply with, as a consumer of cryptographic products and/or services?
- Which cryptography-related certifications are the most relevant for your company?

Threats, incidents and challenges

- What are the most relevant threats your company considers as relevant for the cryptographic products/services used?
- Which requirements does your company consider as relevant for the use of cryptographic products /services?
- Are there any requirements that cannot be covered with commercially available cryptographic products and services?
- Are you aware of impactful incidents in your company related to the implementation, integration or use of your cryptographic products/services?
- What was impacted by these incidents?
- What was the overall impact of these incidents?
- Were any of these incidents subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- How many vulnerabilities of used cryptographic products/services have you handled in last 12 months?
- How many of those vulnerabilities were found in systems of your providers (including open-source libraries)?
- How many of them took more than 5 days to fix?
- Did you need to take manually any action by your side (like searching and deploying patches)?
- According to experience gained within your company, which are the main technological challenges related to the use of cryptographic technologies, products, and services?
- In your opinion, what measures could be taken to foster further adoption and improvements of cryptography?

Market evolution

- According to experience gained within your company, indicate potential barriers for adoption and/or upgrades of cryptographic technologies, products, and services.
- Indicate maximum 3 political, economic, societal, legal, environmental trends or developments that might impact overall cryptographic market.
- Indicate maximum 3 identified gaps between demand and supply, identified through activities of your organisation.
- What are main technology drivers for the cryptography? Name up to 3.
- What are the main business drivers for the cryptography for market evolution? Name up to 3.
- Indicate EU companies you know of with a high innovation potential in the area of cryptography.
- Indicate the most important cryptography research topics.

Supply-side questionnaire

Stakeholder profile

- Indicate number of your employees in all areas of activity.
- Indicate the number of employees working in cryptography.
- Indicate approximate annual revenue that your organisation has from cryptography related business.
- Indicate approximate percentage of the total business that your organisation has from cryptography related business.

- Indicate approximate percentage of revenues that your organisation spends for investments in research, development, and innovation.
- Indicate approximate number your organisation’s customers purchasing cryptography products or services.
- Indicate your organisation’s customer sectors of activity for B2C model.
- Does your organisation have headquarters established in the EU?
- In which geographical areas does your organisation have offices?
- In which geographical areas does your organisation have customers?
- What is the legal structure of your organisation?
- Is your organisation held by a majority of EU capital?

Cryptography offerings

- The offering of your organisation includes:
    - Cryptographic products (hardware or software)
    - Cryptographic services (key management, systems, protocols, and technology)
    - Cryptographic applications (that might include previous two categories)
    - Support services (evaluation and certification of cryptography)
    - Other (please specify).
- How do you build your cryptographic offerings?
- Is in-house design and development all based within EU?
- In which geographical areas are based the partners to which your organisation outsources?
- Which cryptographic products and services your organisation offer currently?
- Do the cryptographic products that your organisation offer also have a software download/update capability for importing updated cryptographic functions (primitives)?
- Which business model does your organisation support?
- Are there any registered cryptography patents owned by your organisation and used in your offerings?

Business objectives and capabilities

- Which business objectives does your organisation consider for its offerings?
- Is your company specialised in:
    - Design
    - Implementation
    - Integration
    - Management and operation
    - Verification/testing
    - Other (please specify)
- Where does your organisation store encryption keys for the products it offers?
- Which of the following offerings does your organisation plan to develop and integrate into its portfolio, in the context of cryptography (Please specify time horizon of implementation, when applicable)?
    - Advanced techniques and protocols
    - Cryptographic support services
    - Cryptography as a service
    - Hardware based cryptography
    - Software based cryptographic products
    - Other (Please specify).

Legislation and certification

- What legislation do you have to comply with, as a supplier of cryptographic products and/or services?
- Which are the most relevant certifications for your organisation as a supplier of cryptographic products and/or services?

Threats, incidents and challenges

- What is the most relevant threat exposure for the implementation, deployment and use of your product or service?
- Which requirements does your organisation consider in its offerings?
- Are you aware of potential incidents in the last 12 months that were prevented thanks to the use of your cryptography offerings (products or services)?
- Are you aware of impactful incident related to the implementation, integration or use of your cryptographic offerings?
- What was impacted by these incidents?
- What was the overall impact of these incidents?
- Were any of these incidents subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- Does your company use any suppliers of lower-level cryptographic components?

- If yes, do you have implemented templates for the bill of material (BOM)?
- How many vulnerabilities have you handled in last 12 months?
- How many of those vulnerabilities were found in systems of your providers (including open-source libraries)?
- How many of them took more than 5 days to fix?

Capabilities and awareness

- According to experience gained within your organisation, what is the level of knowledge in cryptography on the demand side in SMEs?
- According to experience gained within your organisation, what is the level of knowledge in cryptography on demand side in large organisations?
- Indicate the average level of knowledge and expertise in dealing with cryptography in the following customer sectors?
  - Banking and securities
  - Communications, media and services
  - Education
  - Government
  - Healthcare providers
  - Insurance
  - Manufacturing and natural resources
  - Retail
  - Transportation
  - Utilities
  - Wholesale trade
  - Other (please specify).
- Where do you think is the largest gap in the level of knowledge and expertise in dealing with cryptography between supply and demand side?

Market evolution

- Indicate maximum 3 events or incidents that might impact overall market.
- Indicate other important effects on market (e.g., deployment, regulation, network effect, bottleneck).
- Indicate maximum 3 identified gaps between demand and supply through activities of your organisation.
- What are the main technology drivers for the cryptography? Name up to 3.
- What are the main business drivers for the cryptography for market evolution? Name up to 3.
- Indicate EU companies you know of with a high innovation potential in the area of cryptography.
- Indicate the most important cryptography research topics.

Research-and-development-side questionnaire

Stakeholder profile

- Indicate your organisation's total yearly average budget for research projects.
- Indicate which percentage of your organisation's total research budget is dedicated to cryptography-related research projects.
- Indicate number of research staff in your organisation.
- Indicate number of employees in your organisation doing research in the area of cryptography.
- Indicate the number of your organisation's projects in the area of cryptography.
- Indicate the total number of scientific research papers published by your organisation in
- cryptography yearly.
- Indicate the total number of patents registered by your organisation in cryptography yearly.
- Indicate the legal structure of your organisation.
- Which technical readiness level (TRL) does your organisation target in its research & innovation in cryptography?
- Is your organisation owned with majority of EU capital?
- In which geographical areas does your organisation have offices?
- In which EU Member States does your organisation have offices?

Cryptography research

- Indicate the segments in cryptography that your organisation is working on.
- Indicate the most important research directions in cryptography.
- Indicate the developments that may be impactful on cryptography research (both negative and positive impact).

Drivers and barriers

- Indicate the main source of research budgets/grants for your organisation.
- Indicate how easy is for your organisation to find proper funding for cybersecurity research in cryptography.

- What does your organisation consider as the most important initiatives/actions benefiting from research funding?
- What are the political, economic, societal, legal and environmental drivers promoting research and /or innovations in the EU?
- What barriers does your organisation consider for research uptake?
- Which skills are lacking in general in cryptography research?
- Does your organisation have initiatives to attract more researchers to the field of cryptography?

Threats and requirements

- What are the most relevant cybersecurity threats to be addressed within cryptography research?
- What threats your organisation aim to reduce with its research?
- Does your organisation work towards discovery of vulnerabilities in cryptographic products and services (incl. open-source libraries)?
- Which requirements are considered in the research your organisation conducts?
- Specify which relevant standards your organisation uses.

Market evolution

- Indicate research projects and/or companies known to you with a great innovation potential in cryptography.
- Indicate external factors that might impact overall market (e.g., nation sponsored attacks, interceptions, large scale fraud etc.).
- Indicate other important internal market effects (e.g., deployment, regulation, network effect, bottleneck)?
- Do you think there are gaps and niche areas in the cryptographic market?
- Indicate the most important research topics with a potential to impact market in short to medium term (indicatively).

Questionnaire for bodies involved in regulation

Stakeholder profile

- Indicate total number of employees in your organisation in all areas of activities.
- Indicate geographical areas of influence w.r.t. cryptography.
- Indicate EU Member States of influence w.r.t. cryptography.
- Indicate the subject of cryptography-related regulatory activities in which your organisation is involved.
- Indicate how many attestations of cryptographic products and services your organisation has been granted in total.
- Indicate how many attestations of cryptographic products and services your organisation has been granted in 2021.
- Indicate how many attestations of cryptographic products and services your organisation has been granted in 2022.
- Indicate how many attestations of cryptographic products and services your organisation has been granted in 2023.

Regulatory practices in cryptography

- As a regulatory body, do you plan to add new regulatory requirements for cryptographic products or services?
- In case you do perform regulatory actions in the area of cryptography in your Member State, of what kind are those?
  - Regulation of supply (incl. architecture)
  - Regulation of usage
  - Regulation of export
  - Regulation of import
- Are there any restrictions or links to the other legislations (that result from patent law, trade secret law, trading, import/export restrictions, and national security concerns)?
- Which legislation do suppliers and users of cryptographic products and/or services have to comply in your country?
  - EU legislation
  - National legislation
  - Non-EU legislation and/or other International/regional binding agreements
  - Other non-binding agreements and guidelines
- Which principles are you embedding in your national policy development?
  - Trust in cryptographic methods based on certification
  - Choice of cryptographic methods
  - Market-driven development of cryptographic methods
  - Standards for cryptographic methods
  - Protection of privacy and personal data
  - Lawful access

  - Liability
  - International cooperation
- What additional awareness, support services and cryptography-related material do you have?
- Regarding certifications, which are the most relevant for you?
- Do you maintain inventory or catalogue of cryptographic products and services?
- Do you have any processes in place to exert regulatory control?

Threats and requirements

- What are the most relevant cybersecurity threats for cryptographic products/services?
- Which requirements do you consider relevant for regulation?
- Do you implement a vulnerability reporting mechanism for cryptographic products and services?
- Any additional information/comment you would like to provide about threats and challenges that you face?

3.ANNEX C: LIST OF CRYPTOGRAPHY STANDARDS

Security requirements for cryptographic modules

[ISO/IEC 19790:2020] – Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

[ISO/IEC 24759:2017] Test requirements for cryptographic modules – specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012

[FIPS 140-3: 2019], Security Requirements for Cryptographic Modules

[NIST Special Publications], Cryptographic Module Validation Program Security Requirements [CMVP] technical requirements: SP 800-140, SP 800-140A, SP 800-140B, SP 800-140C, SP 800-140D, SP 800-140E, SP 800-140F.

Security requirements for cryptographic algorithms: Block Ciphers; Block Cipher Modes; Digital Signatures; Key Derivation; Key Management; Key Establishment; Message Authentication; Random Number Generators; Secure Hashing

[ISO/IEC 9797:2011] Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[ISO/IEC 9797-2:2021] – Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function

[ISO/IEC 18033-2:2006] – Information technology – Security techniques – Encryption Algorithms – Part 2: Asymmetric ciphers

[ISO/IEC 18033-3:2010] – Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers

[ISO/IEC 10118-3:2018] IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions

[ISO/IEC 19772:2020] – Information technology – Security techniques – Authenticated encryption

[ISO/IEC 10116:2017] – Information technology – Security techniques – Modes of operation for an n-bit block cipher

[ISO/IEC 10118-3:2018] – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions

[ISO/IEC 11770-3:2021] – Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques

[ISO/IEC. ISO/IEC 14888-3:2018] – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm-based mechanisms

[ISO/IEC 18031:2011] – Information technology – Security techniques – Random bit generation

[FIPS Special Publication]:

- FIPS PUB 46-2, Data Encryption Standard.
- FIPS 197, Advanced Encryption Standard (AES).
- FIPS PUB 171, Key Management Using ANSI X9.17.
- FIPS PUB 180, Secure Hash Standard.
- FIPS Special Publication 500-157, Smart Card Technology: New Methods for Computer Access Control.
- FIPS Special Publication 800-2, Public Key Cryptography.
- FIPS 197, Advanced Encryption Standard (AES).

[NIST]: NIST SP 800-63-3, Digital Identity Guidelines

NIST SP 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications

NIST 800-57, Key Management

Lightweight cryptography: is designed to protect information created and transmitted by the Internet of Things – algorithms to Protect Small Devices including its sensors and actuators or implanted medical devices]

[ISO/IEC 29192-1:2012] Lightweight cryptography – Part 1: General – Security Architectures, Models and Frameworks; Baseline security requirements; Security mechanisms; Generic security mechanisms; Crypto utilities

[ISO/IEC 29192-2:2019] Lightweight cryptography Part 2: Block ciphers – Crypto utilities

[ISO/IEC 29192-2] Lightweight cryptography – Part 2: Block ciphers – Security mechanisms; Confidentiality mechanisms; Miscellaneous cryptographic mechanisms

[ISO/IEC 29192-3:2012] Lightweight cryptography Part 3: Stream ciphers – Security mechanisms; Generic security mechanisms; Crypto utilities

[ISO/IEC 29192-4:2013] Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques – Security mechanisms; Generic security mechanisms; Crypto utilities

[ISO/IEC 29192-5:2016] Lightweight cryptography – Part 5: Hash-functions

[ISO/IEC 29192-6:2019] Lightweight cryptography – Part 6: Message authentication codes (MACs) – Authorization

[ISO/IEC 29192-7:2019] Lightweight cryptography – Part 7: Broadcast authentication protocols – Authentication mechanisms; Security protocol standards

Test requirements for cryptographic modules [hardware, software, and/or firmware], including cryptographic algorithms and key generation

[ISO/IEC 24759:2017] Test requirements for cryptographic modules – specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012

[ISO/IEC 18367:2016] Cryptographic algorithms and security mechanisms conformance testing – Conformance testing assures that an implementation of a cryptographic algorithm or security mechanism is correct whether implemented in hardware, software or firmware. It also confirms that it runs correctly in a specific operating environment.

[SOG-IS, February 2023 2023] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, Version 1.3

[SOG-IS, 21/12/2020] SOG-IS Crypto Evaluation Scheme Harmonised Cryptographic Evaluation Procedures, Version 0.16

[EUCC, ENISA Cybersecurity Certification (europa.eu)] State-of-the-art documents related to the CC Technical Domain available on ENISA Cybersecurity Certification website, accessible at: https://certification.enisa.europa.eu/#documentation

[CC supporting documents] Hardware Devices with Security Boxes – Recommended PPs – available on SOG-IS website: SOG-IS – Protection Profiles (sogis.eu)

Cryptography competences

[ISO/IEC 19896-2:2018], Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

4. ANNEX D: ABBREVIATIONS

ABBREVIATION	DESCRIPTION
2G	second generation
3-DES	Triple Data Encryption Algorithm
3G	third generation
4G	fourth generation
5G	fifth generation
ABE	attribute-based encryption
ACN	National Cybersecurity Agency (Agenzia per la cybersicurezza nazionale)
AES	Advanced Encryption Standard
AI	artificial intelligence
AMD	Advanced Micro Devices
ANSSI	Agence nationale de la sécurité des systèmes d’information (French Cybersecurity Agency)
APAC	Asia–Pacific
B	barriers
B2B	business-to-business
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BSIG	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) Act
BYOE	Bring your own Encryption
BYOK	Bring your own Key
ca	circa
CAB	conformity assessment body
CCN	Centro Criptológico Nacional (National Cryptologic Center)
CCN-STIC	Centro Criptológico Nacional – Seguridad de las tecnologías de la información y las comunicaciones
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSP	Cryptographic Service Providers
DNA	Deoxyribonucleic acid
DORA	Regulation (EU) on digital operational resilience for the financial sector
DRM	Digital rights management
e-ID	electronic identification
e.g.	*exempli gratia* (for example)

ECCG	European Cybersecurity Certification Group
ECC	Elliptic-curve cryptography
ECSMAF	ENISA Cybersecurity Market Analysis Framework
ECSO	European Cyber Security Organisation
eIDAS	electronic identification, authentication and trust services (regulation)
eIDAS2	electronic identification, authentication and trust services version 2
eIDA	electronic identification and authentication
EMV	Europay, Mastercard, and Visa
ENISA	European Union Agency for Cybersecurity
ENISA Advisory Group	ENISA AG
eSIM	embedded SIM (subscriber identification module)
eUICC	Embedded UICC (universal integrated circuit card)
FE	functional encryption
FHE	fully homomorphic encryption
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standards
ICT	information and communications technology
iO	Indistinguishability Obfuscation
ISO	International Organization for Standardization
G	gaps
GDPR	general data protection regulation
GPG	GNU Privacy Guard
HMAC	hash-based message authentication code
HOTP	HMAC-based one-time password
HSM	hardware security module
HW	hardware
HYOK	Hold your own Key
i.e.	*id est* (that is)
IEC	International Electrotechnical Commission
IoT	internet of things
IPR	intellectual property rights
ISO	International Organization for Standardization
IT	information technology
LCEN	Loi pour la confiance dans l'économie numérique (Law on confidence in the digital economy)
MAC	message authentication code
MLS	messaging layer security
MPC	multi-party computation
NIS2	network and information security directive version 2

NIST	National Institute of Standards and Technology
OS	open-source
QKD	quantum key distribution
PEC	privacy-enhancing cryptography
PKI	public key infrastructure
PUF	physical unclonable function
QSC	Quantum-safe cryptography
R	regulatory
R & D	research and development
RGS	Référentiel général de sécurité (General Security Repository)
RFC	request for comments
Radius	remote authentication dial-in user service
SAML	Security Assertion Markup Language
RISC	Reduced Instruction Set Computer
RSA	Rivest–Shamir–Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SCCG	Stakeholder Cybersecurity Certification Group
SHE	somewhat homomorphic encryption
SME	small and medium-sized enterprise
SOG-IS	Senior Officials Group Information System Security
T	trends
TLS	transport layer security
TPM	trusted platform module
US	United States
VPN	virtual private network
w.r.t.	with regard to
ZKP	zero-knowledge protocol

TP-02-24-405-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN: 978-92-9204-670-5
doi: 10.2824/249233