|  |  |
| --- | --- |
| Proposal No. 830929 | Project start: 1 February 2019 |
| Call H2020-SU-ICT-03-2018 | Project duration: 47 months |



D4.6

Evaluation of the Research and Innovation Roadmap

|  |  |
| --- | --- |
| **Document Identification** | |
| Due date | 31 July 2022 |
| Submission date | 22 July 2022 |
| Revision | 3.0 |

|  |  |  |  |
| --- | --- | --- | --- |
| Related WP | WP4 | Dissemination  Level | PU |
| Lead Participant | FORTH | Lead Author | Evangelos Markatos |
| Contributing Beneficiaries | All | Related Deliverables | D4.5 |

Abstract**:** This deliverable presents an evaluation of the research roadmap of CyberSec4Europe. The evaluation is done along three dimensions: (i) completeness (i.e. whether the research challenges identified cover the research needed for each vertical), (ii) usefulness (i.e. whether other projects and organisations have used the roadmap in their own work), and (iii) progress made (i.e. whether there has been any progress on the research challenges identified) by the partners and the rest of the community. To evaluate the completeness, we constructed a questionnaire that was distributed to the community. More than 90% of the responses suggest that the identified research challenges adequately cover the research that needs to be done. The rest of the responses provided useful feedback about other challenges that need to be covered. To evaluate the usefulness, we present other projects and organisations that have used (portions of) our roadmap. Finally, to report on progress made we present the work that has been done towards addressing the identified research challenges both from within the project partners and from without.

|  |  |
| --- | --- |
| This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.  The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. |  |

Executive Summary

The CyberSec4Europe project has created a roadmap for research and development in the area of cybersecurity. The roadmap focuses on research directions relevant to the several vertical areas of the project: (1) Open Banking, (2) Supply Chain Security Assurance, (3) Privacy-Preserving Identity Management, (4) Incident Reporting, (5) Maritime Transport, (6) Medical Data Exchange, and (7) Smart Cities.

This deliverable focuses on evaluating the roadmap. The evaluation is being done along three dimensions:

* **Completeness**. That is, are the research challenges proposed enough to address the work needed to be done in each vertical? Do we need to propose more research challenges?
* **Usefulness**. That is, have other projects and organisations used some of this work? Have these organisations used parts of the CyberSec4Europe roadmap in their own work?
* **Progress Made**. That is, has the community made any progress towards addressing the challenges of the roadmap? The community involves (i) the partners of the project and (ii) organisations outside the project who work to address the same challenges.

To evaluate the completeness of the research challenges identified we created a questionnaire which was distributed to the community and received more than 80 responses.

Our main findings include:

* More than 90% of the responders believed that the research challenges identified adequately cover the work that needs to be done in order to address the cybersecurity issues of the verticals. The percentage is even higher (reaches almost 95%) for the responders who work in industry.
* Around 5% of the responders had interesting suggestions for research challenges that could be added to the proposed ones.
* Parts of the project’s roadmap have been used in the roadmaps (or similar documents) of other organisations as well including Cyberwatching.eu: the European observatory of research and innovation in the field of cybersecurity and privacy.

Document information

**Contributors**

|  |  |
| --- | --- |
| **Name** | **Partner** |
| Cristina Alcaraz | UMA |
| Marco Angelini | ENG |
| Laura Colombini | INTESASANPAOLO |
| Said Daoudagh | CNR |
| Jérémy Decis | DAWEX |
| Christos Douligeris | UPRC |
| Davide Ferraris | UMA |
| David Goodman | TDL |
| Elma Kalogeraki | UPRC |
| Marco Kompara | UM |
| Panagiotis Kotzanikolaou | UPRC |
| Stephan Krenn | AIT |
| Antonis Krithinakis | FORTH |
| Eda Marchetti | CNR |
| Evangelos Markatos | FORTH |
| Juan Carlos Pérez Baún | ATOS |
| Aljosa Pasic | ATOS |
| Jesús García Rodríguez | UMU |
| Rodrigo Roman | UMA |
| Michael Salmony | TDL |
| Antonio Skarmeta | UMU |
| Rafael Torres Moreno | UMU |
| Silvia Vidor | UNITN |
| Susana González Zarzosa | ATOS |

**Reviewers**

|  |  |
| --- | --- |
| **Name** | **Partner** |
| Elias Athanasopoulos | UCY |
| Javier Lopez | UMA |

**History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Authors** | **Comment** |
| 0.01 | 2022-04-18 | Evangelos Markatos | 1st Draft |
| 1 | 2022-06-25 | All | Draft sent for 1st review |
| 2 | 2022-07-15 | All | Draft sent for 2nd review |
| 3 | 2022-07-21 | All | Draft sent to the PC |
| 4 | 2022-07-22 | Ahad Niknia | Final check, preparation and submission process |

Table of Contents

[1 Introduction 1](#_Toc109406342)

[2 Completeness 2](#_Toc109406343)

[2.1 Process 2](#_Toc109406344)

[2.2 Results 5](#_Toc109406345)

[2.2.1 Open Banking 5](#_Toc109406346)

[2.2.2 Supply chain security assurance 7](#_Toc109406347)

[2.2.3 Privacy-preserving identity management 8](#_Toc109406348)

[2.2.4 Incident Reporting 9](#_Toc109406349)

[2.2.5 Maritime Transport 11](#_Toc109406350)

[2.2.6 Medical Data Exchange 12](#_Toc109406351)

[2.2.7 Smart Cities 14](#_Toc109406352)

[2.2.8 Evaluation per sector 15](#_Toc109406353)

[3 Usefulness 16](#_Toc109406354)

[3.1 Cyberwatching.eu 16](#_Toc109406355)

[3.2 ECSO 17](#_Toc109406356)

[3.3 Roadmapping Focus Group 19](#_Toc109406357)

[3.4 ENISA 19](#_Toc109406358)

[4 Progress Made 21](#_Toc109406359)

[4.1 Progress Made in Open Banking 21](#_Toc109406360)

[4.1.1 Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing 22](#_Toc109406361)

[4.1.2 Challenge 2: Setting up and discontinuing business relationships 22](#_Toc109406362)

[4.1.3 Challenge 3: Cross-border cooperation under differing legislation and security controls 23](#_Toc109406363)

[4.1.4 Challenge 4: Convenient and compliant authentication 23](#_Toc109406364)

[4.1.5 Challenge 5: Real time revocation of right of access 24](#_Toc109406365)

[4.1.6 Challenge 6: Corporate Open Banking security 24](#_Toc109406366)

[4.2 Progress Made in Supply Chain Security Assurance 25](#_Toc109406367)

[4.2.1 Challenge 1: Detection and management of supply chain security risks 26](#_Toc109406368)

[4.2.2 Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems 27](#_Toc109406369)

[4.2.3 Challenge 3: Security and privacy of supply chain information assets and goods 28](#_Toc109406370)

[4.2.4 Challenge 4: Management of the certification of supply partners 29](#_Toc109406371)

[4.3 Progress Made in Privacy-Preserving Identity Management 29](#_Toc109406372)

[4.3.1 Challenge 1: System-based credential hardening 31](#_Toc109406373)

[4.3.2 Challenge 2: Unlikability and minimal disclosure 31](#_Toc109406374)

[4.3.3 Challenge 3: Distributed Oblivious Identity Management 32](#_Toc109406375)

[4.3.4 Challenge 4: Privacy Preservation in Blockchain 33](#_Toc109406376)

[4.3.5 Challenge 5: Passwordless Authentication 34](#_Toc109406377)

[4.3.6 Challenge 6: GDPR and eIDAS impact on Identity Management 35](#_Toc109406378)

[4.3.7 Challenge 7: Identity Management Solutions for the IoT 35](#_Toc109406379)

[4.4 Progress Made in Incident Reporting 36](#_Toc109406380)

[4.4.1 Challenge 1: Lack of harmonization of procedures 37](#_Toc109406381)

[4.4.2 Challenge 2: Facilitate the collection and reporting of incident and/or data leaks 38](#_Toc109406382)

[4.4.3 Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience 39](#_Toc109406383)

[4.5 Progress Made in Maritime Transport 39](#_Toc109406384)

[4.5.1 Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems 40](#_Toc109406385)

[4.5.2 Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems 41](#_Toc109406386)

[4.5.3 Challenge 3: Resilience of critical maritime systems 42](#_Toc109406387)

[4.5.4 Challenge 4: Maritime system communication security 42](#_Toc109406388)

[4.5.5 Challenge 5: Securing autonomous ships 43](#_Toc109406389)

[4.6 Progress Made in Medical Data Exchange 44](#_Toc109406390)

[4.6.1 Challenge 1: Mechanisms for preserving user data privacy 45](#_Toc109406391)

[4.6.2 Challenge 2: Trustworthiness on the data exchange platform 46](#_Toc109406392)

[4.6.3 Challenge 3: Accomplish regulation during the data sharing process 47](#_Toc109406393)

[4.6.4 Challenge 4: Data exchange platform user experience 48](#_Toc109406394)

[4.7 Progress Made in Smart Cities 49](#_Toc109406395)

[4.7.1 Challenge 1: Trusted Digital Platform 51](#_Toc109406396)

[4.7.2 Challenge 2: Cyber threat intelligence and analysis platform: 52](#_Toc109406397)

[4.7.3 Challenge 3: Cyber competence and awareness program 53](#_Toc109406398)

[4.7.4 Challenge 4: Privacy by design 53](#_Toc109406399)

[4.7.5 Challenge 5: Cyber response and resilience 54](#_Toc109406400)

[4.7.6 Challenge 6: End user trusted data management 54](#_Toc109406401)

[4.7.7 Challenge 7: Interoperability between legacy and new systems 55](#_Toc109406402)

[4.7.8 Challenge 8: Cyber fault/failure detection and prevention 55](#_Toc109406403)

[4.7.9 Challenge 9: Logging and monitoring 56](#_Toc109406404)

[4.7.10 Challenge 10: Information security and operational security 56](#_Toc109406405)

[5 Summary Conclusions 58](#_Toc109406406)

[6 References 59](#_Toc109406407)

[Annex A: Questionnaire 60](#_Toc109406408)

List of Figures

[Figure 1: Distribution of the responders based on the sector of their work. We see that about one third of the responders work in industry and about two thirds work in “Research/Academia”. 4](#_Toc109332629)

[Figure 2: Areas of expertise of the responders. We see that close to 70% declare that they are experts in “Smart Cities”, around 60% declare that they are experts in “Medical Data Exchange”, etc. 4](#_Toc109332630)

[Figure 3: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Open Banking”. 5](#_Toc109332631)

[Figure 4: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Supply chain security assurance”. 7](#_Toc109332632)

[Figure 5: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Privacy-preserving identity management”. 8](#_Toc109332633)

[Figure 6: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Incident Reporting”. 9](#_Toc109332634)

[Figure 7: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Maritime Transport”. 11](#_Toc109332635)

[Figure 8: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Medical Data Exchange”. 12](#_Toc109332636)

[Figure 9: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Smart Cities”. 14](#_Toc109332637)

[Figure 10: We see that people from industry agree that the identified research challenges cover the work that needs to be done in more than 90%. The related percentage for academia is slightly lower with a bit more than 80% of the people. 15](#_Toc109332638)

[Figure 11: The final roadmap of the “cyberwatching.eu” project 16](#_Toc109332639)

[Figure 12: Cyberwatching.eu Roadmap listing our research challenges and our SWOT analysis. 17](#_Toc109332640)

[Figure 13: ECSO Contribution to the Horizon Europe Program and to the Digital Europe Program 18](#_Toc109332641)

[Figure 14: The four pilot project composed the above table of research priorities and delivered it to EU JRC. 19](#_Toc109332642)

[Figure 15: Members of the CyberSec4Europe project have contributed to this document of ENISA on the Research Directions for EU’s Digital Strategic Autonomy. 20](#_Toc109332643)

List of Acronyms

|  |  |  |
| --- | --- | --- |
| *A* | **ABC** | Attribute-based credential |
|  | **ASPSP** | Account Servicing Payment Service Provider |
| *C* | **CTI** | Cyber Threat Intelligence |
|  | **CISO** | Chief Information Security Officer |
|  | **CYTILIS** | Cyber Threat Intelligence and Information Sharing |
|  | **CPS** | Cyber-Physical Systems |
| *E* | **EPC** | European Payments Council |
|  | **ERPB** | Euro Retail Payments Board |
| *D* | **DANS** | Data Anonymization Service |
|  | **DEP** | Data Exchange Platform |
|  | **DFIR** | Digital Forensics Incident Response |
|  | **DLT** | Distributed Ledger Technology |
|  | **DPIA** | Data Protection Impact Assessment |
| *E* | **eIDAS** | electronic IDentification, Authentication and trust Services |
| *F* | **FE** | Functional Encryption |
|  | **FE2MED** | Functional Encryption to Medical Data |
|  | **FIDO** | Fast Identity Online |
|  | **FIDO2** | Fast Identity Online (FIDO Alliance) |
| *G* | **GDPR** | General Data Protection Regulation |
| *I* | **IBAN** | International Bank Account Number |
|  | **IoT** | Internet of Things |
| *M* | **MFA** | Multi Factor Authentication |
|  | **MISP** | Malware Information Sharing Platform |
|  | **MIM** | Minimal Interoperability Mechanisms |
|  | **MPC** | Multi-Party Computation |
| *N* | **NFC** | Near-field communication |
| *O* | **OBSIDIAN** | Open Banking Sensitive Data Sharing Network for Europe |
| *P* | **p-ABC** | Privacy attributed-based credential |
|  | **PE-BPMN** | Privacy-Enhanced Business Process Model and Notation |
|  | **PET** | Privacy Enhancing Technology |
|  | **PIN** | Personal Identification Number |
|  | **PSD2** | Payment Services Directive 2 |
|  | **PSD3** | Payment Services Directive 3 |
| *S* | **SDO** | Standards Development Organization |
|  | **SEPA** | Single Euro Payments Area |
|  | **SPAA** | SEPA Payment Account Access |
|  | **SS-PP-IdM** | Self-Sovereign Identity Privacy-Preserving Identiy Management |
| *T* | **TATIS** | Trustworthy APIs for enhanced Threat Intelligence Sharing |
|  | **TLS** | Transport Layer Security |
|  | **TPP** | Third Party Provider |
| *U* | **URL** | Universal Resource Locator |
| *V* | **VCUCIM** | Verifiable Credential User Centric Identity Management |
| *W* | **W3C** | World Wide Web Consortium |
| *X* | **XACML** | eXtensible Access Control Markup Language |

# Introduction

This is the evaluation of the project’s roadmap as described in deliverable D4.5 [D4.5]. We evaluate the roadmap along three dimensions:

* Completeness
* Usefulness
* Progress made

**Completeness**: We evaluate whether the roadmap is complete. That is, whether the research challenges proposed cover the vertical they address. To evaluate the completeness of the roadmap we reached out to the community via a questionnaire in which we asked for their opinion. The community was given the opportunity to comment on (1) whether the research challenges identified clearly addressed the research that is needed for each vertical and (2) whether there are any research challenges that need to be added. Section 2 describes the results of this exercise.

**Usefulness**: In this dimension we evaluate whether the roadmap has been useful to other entities and organisations. For example, has the roadmap been used by other projects? Has it been included in their work? Has it been cited in their deliverables? Section 3 describes the results of this process.

**Progress Made**: In this dimension we evaluate what progress has been made with respect to the research challenges identified. The progress does not have to originate from CyberSec4Europe partners only. Progress can also be made by the broader community who may be working to address these challenges. Section 4 summarises these results.

Our main findings include:

* More than 90% of the responders believed that the research challenges identified adequately cover the work that needs to be done in order to address the cybersecurity issues of the verticals. The percentage is even higher (reaches almost 95%) for the responders who work in industry.
* Around 5% of the responders had interesting suggestions for research challenges that could be added to the proposed ones.
* Parts of the project’s roadmap have been used in the roadmaps (or similar documents) of other organisations as well including Cyberwatching.eu: the European observatory of research and innovation in the field of cybersecurity and privacy.

# Completeness

## Process

In this section we evaluate whether the roadmap is complete. The roadmap was structured around the seven verticals of the project:

* **Open Banking**
* **Supply chain security assurance**
* **Privacy-Preserving Identity Management**
* **Incident Reporting**
* **Maritime Transport**
* **Medical Data Exchange**
* **Smart Cities**

For each vertical, the Roadmap identified several research challenges as documented in [D4.5]:

* **Vertical: Open Banking. Research challenges identified:** 
  + Mapping of stakeholder interaction in end-to-end Open Banking processing
  + Setting up and discontinuing business relationships
  + Cross-border cooperation under differing legislation and security controls
  + Convenient and compliant authentication
  + Real time revocation of right of access
  + Corporate Open Banking security
* **Vertical: Supply chain security assurance. Research challenges identified:**
  + Detection and management of supply chain security risks
  + Security hardening of supply chain infrastructures, including cyber and physical systems
  + Security and privacy of supply chain information assets and goods
  + Management of the certification of supply partners
* **Vertical: Privacy-Preserving Identity Management. Research challenges identified:** 
  + System-based credential hardening
  + Unlinkability and minimal disclosure
  + Distributed oblivious identity management
  + Privacy preservation in blockchain
  + Password-less authentication
  + GDPR and eIDAS impact on identity management
  + Identity management solutions for the IoT
* **Vertical: Incident Reporting. Research challenges identified:** 
  + Lack of harmonisation of procedures
  + Facilitate the collection and reporting of incident and/or data leaks
  + Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience
* **Vertical: Maritime Transport. Research challenges identified:**
  + Early identification and assessment of risks, threats and attack paths for critical maritime systems
  + Security hardening of maritime infrastructures, including cyber and physical systems
  + Resilience of critical maritime systems
  + Maritime system communication security
  + Securing autonomous ships
* **Vertical: Medical Data Exchange. Research challenges identified:** 
  + Mechanisms for preserving user data privacy
  + Trustworthiness on the data exchange platform
  + Accomplish regulation during the data sharing process
  + Data exchange platform user experience
* **Vertical: Smart Cities. Research challenges identified:** 
  + Trusted digital platform
  + Cyber threat intelligence and analysis platform
  + Cyber competence and awareness program
  + Privacy by design
  + Cyber response and resilience
  + End user trusted data management
  + Interoperability between legacy and new systems
  + Cyber fault/failure detection and prevention
  + Logging and monitoring
  + Information security and operational security

In order to evaluate the roadmap for completeness, we wanted to know whether or not the challenges identified cover the research in the vertical. To do so, we created a questionnaire[[1]](#footnote-2) which we distributed to the community and asked them exactly that i.e. whether they think that the research challenges cover the research work that needs to be done in the vertical.

We distributed the questionnaire to our constituency which consists of:

* The four pilot projects
* ECSO
* Our community in each vertical
* Our associated partners
* The cybersecurity community of the cyberwatching.eu project

The questionnaire was hosted by EUSurvey at **https://ec.europa.eu/eusurvey/runner/CS4E-Roadmap**

We collected more than 80 responses in total: both from research/academia as well as from industry. About two thirds of the responses came from research/academia and one third came from industry as can be shown in Figure 1. The responses were collected from late March to mid-April 2022.

Figure 1: Distribution of the responders based on the sector of their work. We see that about one third of the responders work in industry and about two thirds work in “Research/Academia”.

Figure 2: Areas of expertise of the responders. We see that close to 70% declare that they are experts in “Smart Cities”, around 60% declare that they are experts in “Medical Data Exchange”, etc.

Figure 2 shows the distribution of the expertise of responders. For example, just over 40% expressed their opinion in the cybersecurity challenges for Open Banking, around 60% expressed their opinion on the cybersecurity challenges of supply chain security assurance, etc. Note that the percentages add up to more than 100% because several responders declared that they are experts in more than one vertical.

## Results

### Open Banking

Figure 3: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Open Banking”.

Figure 3 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of Open Banking. We see that the largest percentage of the responders (around 89%) believes that the research challenges identified in the project’s roadmap accurately reflect the research that needs to be done in the area of Open Banking. However, some of the responders have some more specific recommendations to make including[[2]](#footnote-3):

* *Financial & insurance aspects*
* *Development of algorithms for fast(er) and safe cryptocurrency transactions with cards.*
* *Perhaps research on defense techniques against human-centric attacks such as phising attacks is also a priority.*
* *Governance Aspects for Open Banking*

The first suggestion (i.e. *Financial & insurance aspects*) is a very broad one and it’s not clear how it should be applied to Open Banking rather than banking in general.

In the EU, all Fintechs need to have insurance as a prerequisite for getting a licence. Therefore, it’s not clear what the security aspect/concern is. “Financial aspects” is rather too broad to give a meaningful comment – apart from, yes, a FinTech can go bankrupt – as indeed can a bank.

The second suggestion (i.e. *Development of algorithms for fast(er) and safe cryptocurrency transactions with cards.*), while undoubtedly an interesting topic, does not appear to bear any direct relevance to Open Banking. We have seen the risks of crypto in the recent collapse of everything in that space: even some of the biggest Stablecoins[[3]](#footnote-4), which are supposed to be pegged to the dollar or gold, collapsed. It’s not apparent what algorithms for transaction with cards the commentator is thinking of. The world’s central banks are developing central bank digital currencies (CBDCs)[[4]](#footnote-5) and will likely use that to ban private crypto after all the misuses. Several countries have already done this.

With respect to the third suggestion (i.e. *Perhaps research on defense techniques against human-centric attacks such as phising attacks is also a priority.),* preventing phishing attacks is a general concern associated with all vulnerable attack surfaces and, for many reasons, all financial and banking services are particularly sensitive. An example of phishing fraud in the context of Open Banking is documented in D4.5 Research and Development Roadmap 2, section 3.5.1., which observes that ‘*That incident prompted the OBIE steering group to discuss the possibility that open banking payments were more exploitable because of the varying methods used for fraud prevention and detection along the payment journey.*’ If the commentator is referring to social engineering (“human-centric”), then it is a strong point. A huge security issue in the UK, referred to as APP[[5]](#footnote-6) fraud/Instant fraud, is caused by social engineering. The UK has tried a few counter-measures, such as confirmation of payee, but it’s not really helping. Research on how to combat this effectively would be very welcome. An example of the difficulties associated with APP fraud is extensively discussed in D4.5 Research and Development Roadmap 2, section 3.5.3., highlighting the devastating impact of the fraud and the responses taken by the UK authorities in particular. In addition, one of the demonstrator use cases in T5.1 Open Banking associated with the Open Banking Application Architecture includes stress testing against social engineering attacks.

Finally, the last suggestion (i.e. *Governance Aspects for Open Banking*), although both a good and important point, it’s not apparent quite how relevant it is for cybersecurity. However, for the overall working of a complex ecosystem with many actors, good governance is essential and different models are being tried in different geographies. One will see which ones are delivering the best results. Again, more an operational, commercial issue rather than addressing security but it is surely part of the wider topic. Broadly speaking, governance is the umbrella concept underpinning all six of the research challenges identified in the Open Banking roadmap activity.

### Supply chain security assurance

Figure 4: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Supply chain security assurance”.

Figure 4 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of supply chain security assurance. We see that the largest percentage of the responders (close to 90%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of supply chain security assurance. However, some of the responders have some more specific recommendations to make including:

* *Perhaps the identified challenges already cover this, but I would also add: Security of distributed (blockchain based) supply chain tracking systems.*
* *Research related to secure integration and/or certification of integration of components originating from the Supply Chain.*
* *Missing is Interoperability of information architectures for exchange of information amongst business and government stakeholders.*
* *An unresolved challenge is to be able to really incentivize the publication of cyber incidents of suppliers. Often the entire supply chain suffers damage from communication delays due to hesitation. A win-win strategy must be devised between those who suffer and report the attack and those who are informed.*

These are really good suggestions which, to the best of our understanding, have been implicitly considered in the challenges identified. For example, the first recommendation, is implicitly considered in the current roadmap, as blockchain-based distributed supply chain tracking systems can be considered as data sharing infrastructures – whose security and privacy needs are highlighted in “*Challenge 3: Security and privacy of supply chain information assets and goods*”. Nevertheless, it is important to point out that in the near future, due to the current adoption of blockchain-based solutions, it will be necessary to analyze the specific needs of such solutions in this context. As for the second recommendation, it is also implicitly considered in “*Challenge 4: Management of the certification of supply partners*”, since this challenge takes into consideration the existence of multiple suppliers – and their outputs – during the certification process. Still, due to its importance, it should be introduced and explained in an explicit way. Finally, the third recommendation is also implicitly considered in “*Challenge 3: Security and privacy of supply chain information assets and goods*”, as it is mentioned that secure and privacy-aware data sharing infrastructure should manage “common interfaces and data types for the exchange of information”. Again, for the sake of clarity and completion, this particular challenge should be made explicit.

As for the fourth recommendation, although it is a challenge – the coordinated and responsible publication of cyber incidents – that is not unique to supply chain ecosystems, we have to consider that its impact on this particular ecosystem is quite high, and as a result it should have been described in the roadmap. Still, we also can consider that there are various research challenges that have been already detailed in the roadmap (continuous certification and monitoring, shared data spaces) and that can serve as a foundation for this particular purpose.

### Privacy-preserving identity management

Figure 5: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Privacy-preserving identity management”.

Figure 5 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of privacy-preserving identity management. We see that the largest percentage of the responders (more than 95%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of privacy-preserving identity management. However, some of the responders have some more recommendations to make including:

* *Governance of identity management*
* *Ease of integration into, and backwards-compatibility with, legacy systems (to the extent possible) would also be important.*
* *“Unlinkability and minimal disclosure” could be broadened to “controlled linkability”*
* *User perception and usability are missing.*

These are indeed nice areas, but for the most part have been considered as sub-problems intrinsic to the consecution of the identified research challenges. In the following, we discuss the particulars for each suggestion.

The topic of “identity management governance” is a research area that has been missed (although it can be argued that is very dependent on the approaches for identity management, e.g. whether distributed, SSI… approaches are used), but partially addressed within the project’s efforts, in particular in regulatory matters (*GDPR and eIDAS impact on Identity Management* challenge, with work on easing and improving compliance) and in an indirect way with de exploration of different identity management paradigms (e.g., *password-less authentication, distributed/decentralized identity management*). Regarding “controlled linkability”, this research challenge has been implicitly included in the roadmap under the name *unlinkability and minimal disclosure*, as most discussion regarding unlinkability also must tackle controlled linkability, though indeed it may have been more appropriate to broaden the challenge’s name. As for “user perception and usability”, this has again been considered as an intrinsic goal of the research challenges for identity management (and, in fact, the whole project). A complete task (T3.6, with multiple associated deliverables like D3.16 and D3.17) has been dedicated to this topic, including work necessary for the consecution of key results in challenges like *distributed oblivious identity management* (i.e., ensuring user-friendliness of such system) or *GDPR and eIDAS impact on identity management* (both from the perspective of user friendliness as a key element for enabling compliance, and improving the usability of tools that help with compliance planification and assessment).

### Incident Reporting

Figure 6: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Incident Reporting”.

Figure 6 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of incident reporting. We see that the largest percentage of the responders (around 90%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of incident reporting. However, some of the responders have some more specific recommendations to make including:

* *Quantification of risks is part of cybersecurity governance, incident reporting can be used to support it*
* *Missing efforts to map incentives and/or regulations for information sharing*
* *Anonymized reporting support*
* *Secure intelligence sharing between non trusted organisations*
* *Digital forensics procedures and tools*

These are interesting suggestions.

The first one (Information sharing in general, as well as incident reporting in particular) can be of support in achieving as much as possible a precise quantification of cyber risks. Information sharing, for example, allows companies to do benchmarking and compare each other’s experience concerning cyber risk management. Incident reporting can provide one (or more) previous case(s) of example in relation to the probable location of the most relevant cyber vulnerabilities, which kind of damage an attack can cause, and how much was required to repair it in terms of financial, but also human, resources. The primary objective of cyber risks quantification remains the prevention of cyber incidents through accurate modelling and the gathering of meaningful measurements, two elements which information sharing and incident reporting can help achieving. However, information sharing in the cybersecurity environment also remains complex, especially due to the persistent fear of reputation damage and the difficulties involved in sharing confidential business data. For this reason, although this research area is indeed included as part of the research challenge 3, during the CyberSec4Europe roadmap we have focused more on threat intelligence data sharing.

The second is an interesting area, but we consider this is not really in the scope of the main problems and challenges identified by the vertical stakeholders at the beginning of the project and out of the scope of the cyber-security assets developed by the partners during the project.

With respect to the third suggestion, the first aim of the project is to provide a first prototype of an incident reporting platform that helps the financial institutions in the mandatory reporting tasks; secondly, to offer mechanisms to improve trustworthiness and reliability for threat intelligence data sharing using MISP. However, including support for anonymised reporting would be a nice working line for the future to improve the current prototype. The theme of anonymized data is of prime importance when it comes to sharing information on incidents that have occurred between stakeholders.

The fourth challenge is already included as part of the research challenge 3 of this vertical, since we have also considered that the generic and not sensitive information available about a security incident could be shared with anyone (including non-trusted organisations). Through the assets TATIS and Privacy-CTI, it has been enhanced and extended the security features provided by MISP platform so the users can establish the trust policies and determine which type of information can be shared only with trusted organisations or with any organisation.

With respect to the fifth suggestion although this is a nice research area that has not been the priority for this Incident Reporting vertical, one of the assets integrated with the incident reporting platform for data enrichment, JUDAS,[[6]](#footnote-7) is a tool developed to provide support in the context of digital forensic investigation with the identification of all data relevant to users and devices.

### Maritime Transport

Figure 7: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Maritime Transport”.

Figure 7 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of maritime transport. We see that the largest percentage of the responders (around 90%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of maritime transport. However, some of the responders have some more specific recommendations to make including:

* *Connection of cyber-physical assets and threats and development of a method for a holistic risk measurement and mitigation.*
* *Best practices for disaster recovery of data and services in ports.*
* *Joint cybersecurity/safety approaches so that both are promoted*

All these suggestions are interesting and useful food for thought topics for the maritime transport sector.

Concerning the first recommendation, it can be an enhanced approach of the first research challenge identified by CyberSec4Europe for the maritime transport sector “Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems”. Within this research challenge, we have considered cyber-physical systems of the maritime transport sector in respect of the impact that may be caused from a cyber attack on IT systems to physical interdependent systems. In particular, we demonstrate the importance of capturing infrastructure interdependencies between cyber and physical systems. In addition, we indicate cyber attack paths generation and threat propagation calculation among systems to identify how sophisticated adversaries may infiltrate into maritime transport systems and compromise a variety of cyber assets which are interdependent with physical assets and may have a devastating impact on them. For instance, a cyber attack on a SCADA-type oil monitoring system of a petroleum tanker may damage oil pump pressure relief valves and cause malfunctions leading to oil spills while bunkering which can harm the environment. Another aspect which is considered through this challenge is how cyber threats may be utilized to implement physical threats. For instance, attacks, such as eavesdropping (i.e. video recording, shoulder surfing, keylogging, etc.) intend to gain information on maritime transport services and assets (i.e. planned deliveries, content of cargos, etc.) may facilitate and motivate adversaries to perform physical attacks. Moreover, we have included in this challenge investigations on software vulnerabilities deriving from human errors. We may enhance the current challenge with indicative state-of-the-art hybrid solutions to illustrate cyber and physical relations of assets and methods for measuring combined (cyber and physical) threats.

As regards the second recommendation “disaster recovery of data and services in ports”, these are sub-topics of incident handling and privacy concerns which have been addressed within the identified research challenges, mainly in the third research challenge 3 “Resilience of critical maritime systems” and fourth research challenge “Maritime system communication security”. Infrastructure resilience as presented in the third research challenge is “the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions”. Within this context, the third research challenge stresses the need to focus on deployment methodologies for the critical maritime systems that follow the “resilience-by-design principle”, to inherently design systems that may resist and quickly recover from unwanted events. Moreover, it suggests distributed and resilient trust management system solutions to reinforce the security of communications in Maritime Transport and ensure data storage and data integrity. Besides, the research goal of this challenge addresses techniques for quick adaptation to security threats, namely, suggests the development and implementation of AI monitoring techniques that are capable of analysing threat events enabling systems to quickly adapt to attacks and apply proper mitigation controls. In addition, we stress the need to focus on novel methodologies and tools needed for fast recovery of critical maritime systems, such as those used in autonomous ships (Research challenge 5: Securing autonomous ships). Regarding data recovery, in maritime transport systems, we have illustrated in challenge 4 appropriate means and measures to address data integrity in maritime communications. Furthermore, encryption and tokenization techniques are proposed for data loss prevention.

Regarding the recommendation for joint cybersecurity and safety approaches, this is really a good suggestion but it should be investigated at first whether it is applicable in the maritime transport sector as it relies on a variety of regulations and standards due to the fact that embraces multiple industries. In a sense, combined cybersecurity and safety approaches have been addressed in the fifth research challenge “Securing autonomous ships” where considerations for unified security and safety risk management of heterogeneous components for autonomous ships are set as long-term research goals.

### Medical Data Exchange

Figure 8: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Medical Data Exchange”.

Figure 8 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of medical data exchange. We see that the largest percentage of the responders (more than 90%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of medical data exchange. However, some of the responders have some more specific recommendations to make including:

* *Regulation (responsibility, etc.) after the data sharing process is over*
* *Creation of material for cybersecurity training of medical personnel (awareness and right use of the technology in practice).*
* *Unified data model for every EU Member States.*
* *Missing aspect is the governance of the system for medical data exchange and the challenge 'accomplish regulation during the data sharing process' can be more specific as it is not clear what is meant by it. Neither is it clear who the platform user is in the aspect 'data exchange platform user experience' (the data subject or the organisation that used the data that is exchanged on/via the platform).*

Among the points mentioned, the “*Creation of material for cybersecurity training of medical personnel*” is a nice area, but is not really a research challenge, even though the medical data exchange demonstrator has delivered some guidelines documents for the technologies provided in order to cover this aspect. Medical data exchange demonstrator considers that the following challenges need to be addressed and are currently under study and are already included in the roadmap:

* “*Regulation (responsibility, etc.) after the data sharing process is over*” this aspect is being cover by this demonstrator by studying the benefits of the adoption of self-sovereign identity (SSI) solution and the use of verifiable credentials (VCs). Through this approach the data owner has the control over their data, including the subsequent use of the data, who can use the data and the purpose for using the data.
* “*Unified data model for every EU Member States*”. This challenge is included in the roadmap, and during the project period some study has been made on how to include standards such as HL7/FHIR on the anonymisation tool.

Regarding the “*Missing aspect is the governance of the system for medical data exchange and the challenge 'accomplish regulation during the data sharing process' can be more specific as it is not clear what is meant by it*”, this demonstrator is already checking the GDPR compliance of the system, by following the provided GDPR guidelines generated by this project, namely in WP3.

Finally the point “*Neither is it clear who the platform user is in the aspect 'data exchange platform user experience' (the data subject or the organisation that used the data that is exchanged on/via the platform)*”, it is necessary to clarify that the user of the platform provided in this demonstrator for sharing data (the COVID-19 data exchange platform) would be organisations, but in the future need to be considered that the data subject could play the role of platform’s user, selling his/her own data.

### Smart Cities

Figure 9: Percentage of people who believe that the research challenges identified in the project’s roadmap reflect the research that needs to be done in area “Smart Cities”.

Figure 9 plots the percentage of people who believe (or not) that the research challenges identified in the project’s roadmap reflect the work that needs to be done in the area of smart cities. We see that the largest percentage of the responders (around 85%) believes that the research challenges identified in the project’s roadmap reflect the research that needs to be done in the area of smart cities. However, some of the responders have some more specific recommendations to make including:

* *Effort to identify (and address) legal challenges*
* *Hardening of IOT devices.*
* *Radiation fields measurements and values demarcation for the safety of human health.*
* *Topics are quite generic (e.g., logging and monitoring) - is it possible to condense it/focus on specifics of smart cities*
* *Same as for others where there's a physical component to the system: Joint cybersecurity/safety approaches so that both are promoted*
* *Privacy by design can be extended by 'privacy by default'.*
* *How can citizens be made aware of data being collected about themselves and how can they revoke or modify usage of their data? It would be necessary to define good, easy and transparent procedures to make citizens able to access their data, control them and update usage permissions*
* *new, suitable governance models*
* *Ensuring security resilience is not included as a challenge. This can be achieved by implementing adaptive security mechanisms.*

Most of the recommendations are quite interesting. A few of them are related to new technologies or approaches well addressed by the already identified challenges, like IoT, privacy by default, and citizens’ data collection and management. Maybe the users did not catch the work behind each challenge from the title reading. Others are quite general, like the one about governance models, and they are subject of others WPs of the project (WP2 Governance Design and Pilot).

Some others instead are new and more interesting because of their specificity, the one about the radiation for instance.

Those about the cybersecurity/safety approach and adaptive security should be investigated, in order to find out whether it is applicable in smart cities environment and with which benefits.

### Evaluation per sector

In this section we would like to explore whether people from academia or people from industry believe that the identified research challenges cover the work that needs to be done. Figure 10 shows the percentages of people per sector (industry vs. academia) who believe that the challenges address the verticals. We see that in both cases the percentages are rather high. Indeed, in both cases around 90% of the people believe that the research challenges identified reflect the work that needs to be done. Interestingly, the percentage is slightly higher in industry (close to 95%) and slightly lower in academia (close to 90%).

Figure 10: We see that people from industry agree that the identified research challenges cover the work that needs to be done in more than 90%. The related percentage for academia is slightly lower with a bit more than 80% of the people.

# Usefulness

In this dimension we explore whether this roadmap has been useful in other settings. For example, we would like to see whether other organisations have adopted parts of the roadmap, or whether other entities have included our priorities in their roadmap. In the rest of the section we describe the most important of such cases.

## Cyberwatching.eu



Figure 11: The final roadmap of the “cyberwatching.eu” project

The cyberwatching.eu project published its final roadmap as D4.7 on 31/7/2021. Their roadmap invested almost 25 pages to describe the CyberSec4Europe roadmap. D4.7 included not only the research priorities identified by our project, but also the SWOT analysis.

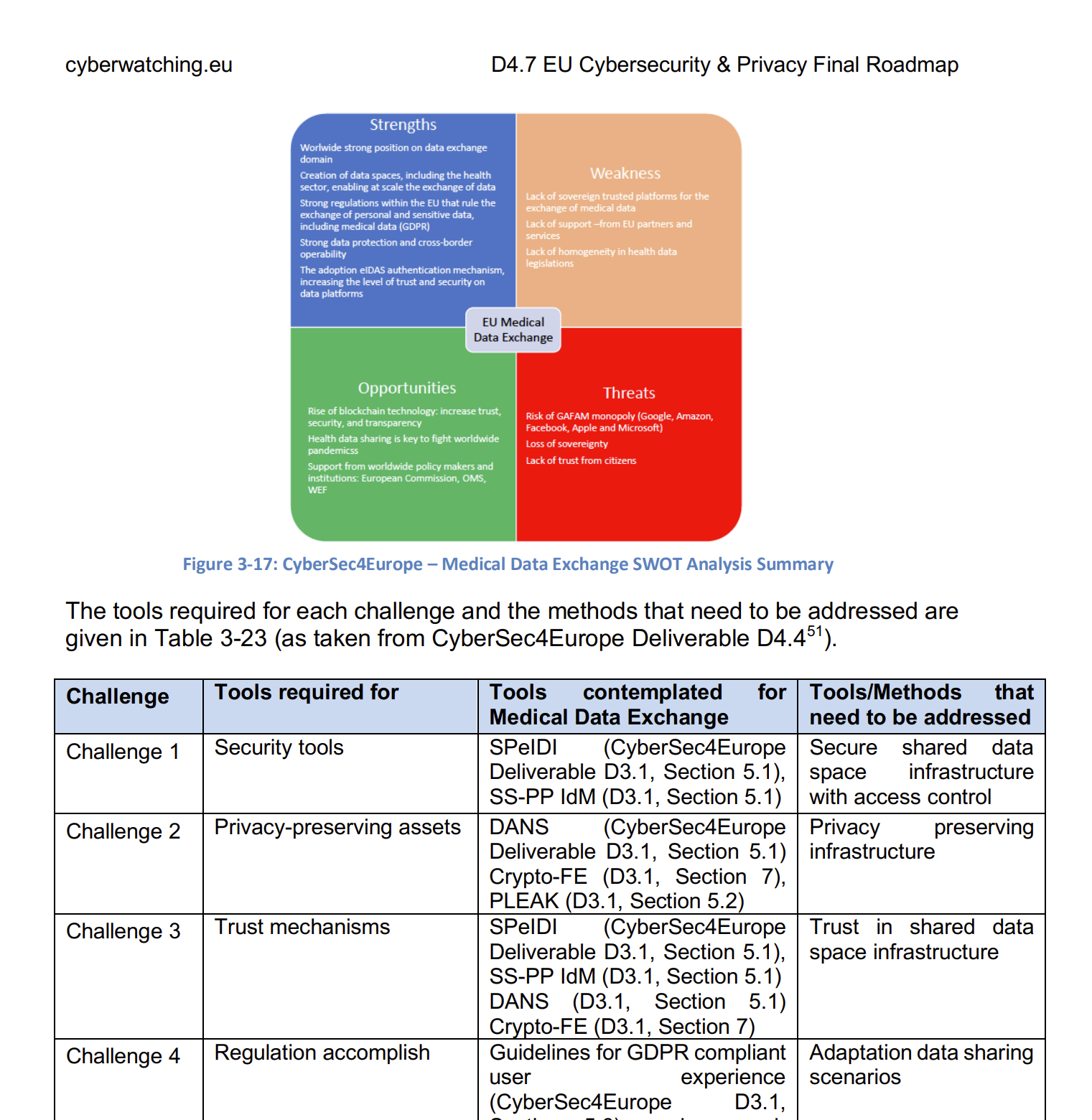


Figure 12: Cyberwatching.eu Roadmap listing our research challenges and our SWOT analysis.

## ECSO

The European Cyber Security Organization (ECSO) recently published its research priorities both for Horizon Europe and for the Digital Europe Programme. We see that there is some cross-fertilisation between the CyberSec4Europe roadmap and the ECSO research priorities, especially in the areas of privacy-preserving technologies and software hardening. This implies that the research challenges identified by CyberSec4Europe are indeed useful and are included in the priorities of other organisations as well.

|  |
| --- |
|  |
|  |

Figure 13: ECSO Contribution to the Horizon Europe Program and to the Digital Europe Program

## Roadmapping Focus Group

The four pilot projects along with ECSO have formed a working group (WG) on roadmapping. This WG has created a set of important research directions in the area of cybersecurity. These directions have been communicated to the JRC (Joint Research Centre) of the European Commission that is developping Atlas (“a knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts in support of the EU Digital Strategy.”) CyberSec4Europe has been a leading contributor to this WG and the research priorities.

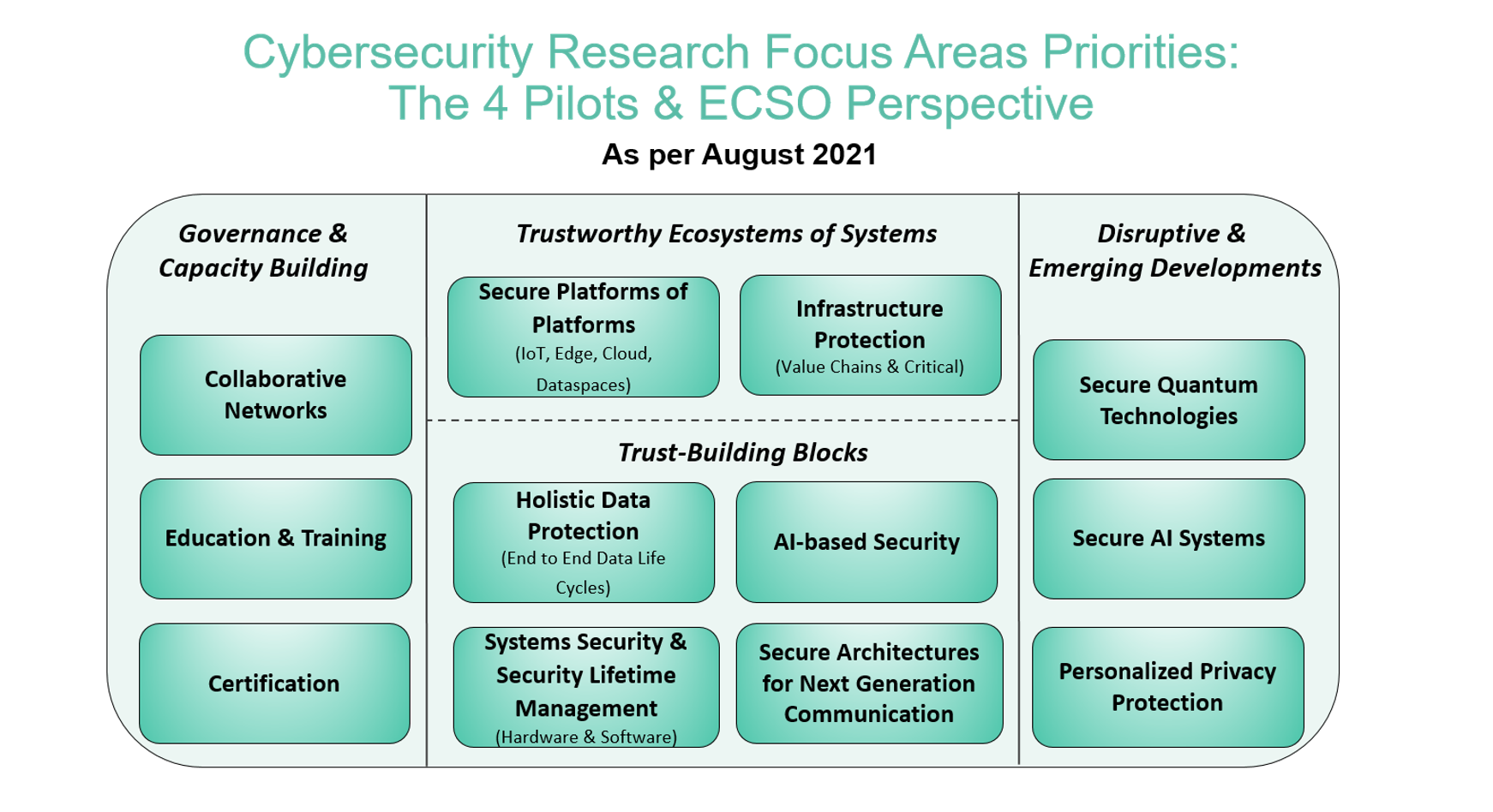


Figure 14: The four pilot project composed the above table of research priorities and delivered it to EU JRC.

## ENISA

In April 2021 ENISA published a deliverable outlining some of the important research directions that contribute to EU’s Digital Strategic Autonomy[[7]](#footnote-8). Evangelos Markatos (leader of CyberSec4Europe WP4) was a co-author of this document. Markatos, along with other CyberSec4Europe members (including Kai Rannenberg, Afonso Ferreira and Elias Athanasopoulos) contributed to this document based on their experience with the WP4 roadmapping activities.

|  |  |
| --- | --- |
|  |  |
|  |

Figure 15: Members of the CyberSec4Europe project have contributed to this document of ENISA on the Research Directions for EU’s Digital Strategic Autonomy.

The report identified several important research areas:

1. Data security
2. Trustworthy software platforms
3. Cyber threat management and response
4. Trustworthy hardware platforms
5. Cryptography
6. User-centric security practices and tools, and
7. Digital communication security

# Progress Made

In this section we evaluate the roadmap along the dimension of progress made towards addressing the research challenges identified. The progress may have been made by us or by other entities. One may ponder for quite some time on how to judge the progress made. To simplify the process, we chose to report the publications that we (or others) have made towards the research challenges identified. Thus, for each vertical we list the (most important publications) that have been published in the last two years (2020 and 2021) that address the challenges identified in the CyberSec4Europe roadmap.

## Progress Made in Open Banking

Among the distinguishing differences between the work carried out in WP4 and WP5 is that the several demonstrator use cases have been seeking to improve specific cybersecurity-related instances whereas the roadmapping activities have been focussed on the ‘bigger picture’ issues associated with Open Banking (and payments). Hence, there is less of a direct correlation between the two workpackages.

A number of assets developed in WP3 and WP5 and evaluated in CyberSec4Europe are used by the demonstrators and consequently addressing the cybersecurity challenges identified for the use cases, if not directly to the WP4 research challenges. These are:

* CYTILIS (Cyber Threat Intelligence and Information Sharing):

This use case is described in deliverable “D5.5 Specification and set up demonstration case Phase 2” [D5.5] and the assets associated with it are listed in deliverable “D3.13 Updated version of enablers and components” (TATIS and Blockchain Platform) [D3.13] and deliverable “Deliverable D3.14: Cooperation With Threat Intelligence Services For Deploying Adaptive Honeypots” (PP-CTI) [D3.14].

* + TATIS (Trustworthy APIs for enhanced Threat Intelligence Sharing): this asset is used as a proxy to the MISP (Malware Information Sharing Platform) instance in CYTILIS. TATIS enhances the CTI (Cyber Threat Intelligence) sharing platform to share indicators of compromise in a trustworthy manner.
  + PP-CTI (Privacy-Preserving Cyber Threat Intelligence): this asset is used to apply PETs (Privacy Enhancing Technologies) to the shared information in CYTILIS and will investigate, integrate and adapt privacy-preserving solutions, anonymity techniques within CTI systems.
  + Blockchain Platform: the CYTILIS demonstrator leverages this blockchain architecture (i) to allow private transaction exchanges by ensuring that only the relevant stakeholders receive the information; (ii) to tolerate byzantine faults and scale to a much larger network size by using a novel consensus protocol.
* OBSIDIAN (Open Banking Sensitive Data Sharing Network for Europe)

This use case is described in deliverable “D5.5 Specification and set up demonstration case Phase 2” [D5.5] and the asset, which is not yet integrated into the demonstrator, is listed in “D3.13 Updated version of enablers and components” [D3.13].

* + Sharemind MPC (Multi-Party Computation): this asset is being used to implement a privacy-preserving financial fraud detection application in collaboration with the OBSIDIAN demonstrator
* Privacy-Preserving Verifiable Credentials
* This use case described in “D5.5 Specification and set up demonstration case Phase 2” [D5.5] and the asset is listed in deliverable “D3.1: Common Framework Handbook #1” [D3.1].
  + VCUCIM: the asset is used as the basis for this demonstrator as the FIDO2 (Fast Identity Online 2) authenticator application

Numerous publications covering different aspects of Open Banking as well as the associated formal directives have been published during the lifetime of the project that address aspects of the identified research challenges in the Open Banking roadmap. The list includes publications from both CyberSec4Europe partners and others.

### Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing

During the course of its meeting on 24 November 2021, the European Payments Council (EPC) Board accepted an invitation from the Euro Retail Payments Board (ERPB) to act as Scheme Manager for a new single euro payments area (SEPA) payment account access (SPAA) scheme. To develop the scheme, the EPC Board established a SPAA multi-stakeholder group (SPAA MSG). The initial goal was a 90-day public consultation which was launched on 13 June 2022 to give the wider market an opportunity to share their views on the first draft version. The final version of the SPAA scheme rulebook’s first release is still anticipated to be published on the EPC website by 30 November 2022, subject to EPC Board approval.

The SPAA scheme covers the set of rules, practices and standards that will allow the exchange of payment accounts related data and facilitates the initiation of payment transactions in the context of ‘value-added’ (‘premium’) services provided by asset holders (i.e. account servicing payment service providers (ASPSPs)) to asset brokers (e.g. third party providers (TPPs)).

The aim of the SPAA scheme is to drive ‘open payments’ in the EU in a way that unlocks and creates value whilst allowing for a fair distribution of value and risk between scheme participants.

While it is good to see the progress of this initiative, in terms of Challenge 1, the proposed scheme only addresses payments rather than the full cycle of banking processes. By contrast, the giropay API developed in Germany and supported by 1500 German banks has a wider remit but is limited to Germany. When selecting giropay, customers are prompted to select their bank and then to sign into their online banking account. After reviewing the pre-filled payment details, they can agree to the payment, before being redirected back to the bank’s website. Once completed, the bank receives confirmation via a URL notification.

Ideally, we would like to see one comprehensive approach rather than a plethora of independent schemes. Fortunately, there is still time that to address this concern through the PSD3 (Payment Services Directive 3) consultation as well as the SPAA consultation, both of which are open at the time of writing.

References:

* Deloitte. 2017. "Achieving robust cyber-security in a connected banking environment." Accessed July, 2022. <https://www2.deloitte.com/uk/en/pages/financial-services/articles/achieving-robust-cyber-security-in-connected-banking-environment.html>

### Challenge 2: Setting up and discontinuing business relationships

There a suggestion that the introduction of schemes as described above would make the process of setting up and discontinuing business relationships easier. Again, as above, there is an opportunity the revision of PSD2 (Payment Services Directive 2) and the final SPAA may go some way to addressing the identified challenge.

References:

* Sidley. 2022. "European Commission Launches PSD3 Consultations." May 2022. Accessed July, 2022. <https://www.sidley.com/en/insights/newsupdates/2022/05/european-commission-launches-psd3-consultations>
* Toppr. n.d. "Major Security Issues and Challenges." Accessed July, 2022. <https://www.toppr.com/guides/general-awareness/banks/major-security-issues-and-challenges>

### Challenge 3: Cross-border cooperation under differing legislation and security controls

Some progress was made in addressing this research challenge in WP5 with the collaboration between a French bank, a Spanish bank and the Italian Banking Association lab. It is hoped that the revision of PSD3 may addressing some of the wider issues, particularly in relation to payments.

References:

* Duncan, Elie. 2022. "The journey from PSD2 to PSD3." March 2022. Accessed July, 2022. <https://www.openbankingexpo.com/features/feature-the-journey-from-psd2-to-psd3>
* HID Global. 2019. "Opportunities and Challenges of Open Banking Around the World." Accessed July, 2022. <https://www.hidglobal.com/doclib/files/resource_files/hid-iam-open-banking-opps-challenges-wp-en.pdf>

### Challenge 4: Convenient and compliant authentication

Three of the WP5 demonstrator use cases touched on the issues arising from this research challenge from two different perspectives: one that of preventing bad actors from presenting fraudulent IBANs (International Bank Account Numbers) and other information with the objective of defrauding individuals and financial institutions whilst maintaining GDPR (General Data Protection Regulation) compliance. And the other ensuring the option of secure eKYC (electronic know-your-customer) using FIDO2 for authentication. In truth there are too many ways of addressing authentication and it is to be hoped that the publication of PSD3 may bring further improvements.

References:

* Fortech. 2022. "How PSD3 could close the gap between implementation and actual adoption." January 2022. Accessed July, 2022. <https://www.fortech.ro/whitepaper-how-psd3-regulations-could-close-the-gap-between-implementation-and-actual-adoption>
* Jendruszak, Bence. 2021. "The Risks of Open Banking Fraud and How to Prevent Them." Seon. April 2021. Accessed July, 2022. <https://seon.io/resources/open-banking-risk-and-fraud>
* Accenture. 2016. "PSD2 & Open Banking Security and Fraud Impacts on Banks." Accessed July, 2022. <https://www.accenture.com/_acnmedia/pdf-40/accenture-psd2-open-banking-security-fraud-impacts.pdf>
* OBSIDIAN. 2020. "Le projet européen OBSIDIAN de partage d’information sur les IBAN comme moyen de lutte contre la fraude." Observatoire de la sécurité des moyens de paiement, Rapport Annuel 2019. September 2020. Accessed July, 2022. <https://www.vie-publique.fr/rapport/276365-observatoire-de-la-securite-des-moyens-de-paiement-rapport-annuel-2019>
* Collas, Médéric. "OBSIDIAN: Projet de partage d’informations entre banques pour mieux lutter contre la fraude externe." Cyber & Conformité. June 2021.

### Challenge 5: Real time revocation of right of access

As with Challenge 4, one of the issues is that there are too many approaches to authentication that stymie efforts to comprehensively remove this loophole, which ideally will be addressed in PSD3.

References:

* PYMNTS. 2022. "EU Regulator Launches PSD3, Open Finance Consultations." May 2022. Accessed July, 2022. <https://www.pymnts.com/news/regulation/2022/eu-regulator-launches-psd3-open-finance-consultations>
* PwC. 2019. "Putting security and privacy at the heart of open banking." Accessed July, 2022. <https://www.pwc.com/ca/en/industries/banking-capital-markets/canadian-banks-2019/putting-security-and-privacy-at-the-heart-of-open-banking.html>

### Challenge 6: Corporate Open Banking security

Evidence from industry indicates that progress has been made in raising awareness of the gaps identified in this research challenge. In addition, it appears that many of the issues are being addressed in PSD3 which is encouraging, although it is questionable whether it is a good idea for the regulator to cover them rather than leaving it to the corporate world.

References:

* Balharrie, Joanne. 2021. "How Safe and Secure Is Open Banking?" Bidataintel, July 2021. Accessed July, 2022. <https://bidataintel.com/2021/07/how-safe-is-open-banking>
* MoneyHelper. 2021. "Open Banking and sharing your information online." Accessed July, 2022. <https://www.moneyhelper.org.uk/en/everyday-money/banking/open-banking-and-sharing-your-online-banking-information>
* Shliakhouski, Alexey. 2021. "Security in Open Banking: Concerns And Solutions." Forbes. August, 2021. Accessed July, 2022. <https://www.forbes.com/sites/forbestechcouncil/2021/08/19/security-in-open-banking-concerns-and-solutions>
* Tumaián, Rodrigo. 2021. "Why cybersecurity frameworks are crucial for the future of open banking." Securitymagazine, July 2021. Accessed July, 2022. <https://www.securitymagazine.com/articles/95570-why-cybersecurity-frameworks-are-crucial-for-the-future-of-open-banking>
* Tumaián, Rodrigo. 2021. "Open Banking Isn’t Without Its Cybersecurity Risks. Here’s How to Overcome Them." Spiceworks. May 2021. Accessed July, 2022. <https://www.toolbox.com/it-security/vulnerability-management/guest-article/open-banking-isnt-without-its-cybersecurity-risks-heres-how-to-overcome-them>
* Dragas, Danijella. 2021. "The security risks of Open Banking." LinkedIn. September 2021. Accessed July, 2022. <https://www.linkedin.com/pulse/security-risks-open-banking-danijella-dragas>
* OPENBANKING. 2019. "Open Banking Operational Guidelines: Security." December 2019. Accessed July, 2022. <https://standards.openbanking.org.uk/tpp-operational-guidelines/security/v3-1-4>
* SOLDO. 2022. "How secure is open banking?" Accessed July, 2022. <https://www.soldo.com/en-eu/business-banking/how-secure-is-open-banking>
* Kundariya, Harikrishna. 2021. "Everything You Need to Know About Open Banking Security." October 2021. Accessed July, 2022. <https://www.appknox.com/blog/open-banking-security>
* Trend Micro. 2019. "Trend Micro Highlights Security Risks of New Open Banking Regulation." September 2019. Accessed July, 2022. <https://www.trendmicro.com/en_fi/about/newsroom/press-releases/2019/trend-micro-highlights-security-risks-new-open-banking-regulation.html>
* Wilson, Mike. 2022. "Open Banking Opens Up New Security Vulnerabilities." February 2022. Accessed July, 2022. <https://www.cutimes.com/2022/02/22/open-banking-opens-up-new-security-vulnerabilities>

## Progress Made in Supply Chain Security Assurance

Regarding Cybersec4Europe’s assets that contribute to securing supply chains, there have been various assets, developed in WP3 and WP5 and evaluated by CyberSec4Europe, that support setting up and operating supply chains across collaborating organisations in a controlled and secure way, taking into consideration aspects of all the research challenges identified for this vertical. The main three assets are:

* **Blockchain Platform** is an asset developed in WP3 that represents a blockchain-as-a-service solution introducing the concept of “satellite chains” which are kind of blockchains on a blockchain. Satellite chains allow to address privacy and governance for federating partners in a blockchain network. Such a feature is highly relevant for supply chains where organisations might be partners and competitors at the same time and must keep control over corporate proprietary information when being shared in a distributed ledger. Via satellite chains, data can be shared and handled securely between selected partners, only, and access to the whole community (default when storing data in a blockchain) would be prevented. By offering byzantine fault tolerant (BFT) consensus approaches, this blockchain based infrastructure for supply chains also offers the required robustness without the need (or possibility) to establish trust to a trusted third party. A description of the asset and details of its implementation can be found in section 4.13 Blockchain Platform of D3.13. The Blockchain Platform also got evaluated by task T5.2, Supply Chain Security, and details on the corresponding use case demonstrator can be found in section 3 Supply Chain Security Assurance of D5.5.
* **Workflow Compliance Assurance** focuses on the definition, implementation, and controlled execution of distributed workflows that span multiple organisations. The asset covers both, the approach for modelling cross-organisational business processes as well as a framework for the technical implementation and enforcement of those business processes. Petri Nets are used for workflow specifications. This formal approach provides a basis for the validation of the workflow and its implementation. The framework is based on a distributed ledger architecture that is used to establish and mange trust amongst potentially untrusted partners such as competitors. The Petri Nets layer in combination with smart contracts executed on the blockchain is used to enforce workflow compliance. The asset was further developed in task T5.2 of WP5 and evaluated by use case SCH-UC2 (Compliance and Accountability in distributed Manufacturing). Details on the status of the implementation and usage of the demonstrator can be found in section 3 Supply Chain Security Assurance of D5.5.
* **Workflow Compliance Accountability** was developed in T5.2 of WP2 and evaluated by the demonstrator for use case SCH-UC2 (cf. section 3 Supply Chain Security Assurance of D5.5). It addresses measures to determine violations of the code of conduct and to react accordingly. It provides the basis for "secure blaming" in the context of workflow enforcement. This starts with determining the actor responsible for non-compliance. To achieve this, a framework is provided that allows to identify actors and trace their activities within a distributed workflow – such as a supply chain. The audit data for these activities are stored in an immutable way in a distributed ledger, i.e., blockchain. Such audit log entries are clearly assigned to a participant via digital signatures and cannot be modified or deleted afterwards. Audit log information is shared among all collaborating organisations. This way, identification of any non-compliance is made easy and can also be supported or even automated via smart contracts.

Additionally, several publications have been published during recent years that address the research challenges identified for this vertical. This list includes both publications by CyberSec4Europe partners and other researchers.

### Challenge 1: Detection and management of supply chain security risks

The Blockchain Platform and Workflow Compliance Accountability assets, applied in SCH-UC1 (cf. CyberSec4Europe deliverable D5.5) address this requirement. More specifically, it addresses the specific research goal of “tracing and visualizing attack paths and the flow of possible attacks in optimal times” for user interactions. Other works not focused on blockchain-based solutions include graph-based frameworks for inferring challenges, information flow-based frameworks for dynamic analysis of software dependencies, enhanced risk classification schemes, and optimization mechanisms for selection of security controls.

References:

* Resende, João. 2021. "D3.13 Updated version of enablers and components." Cybersec4Europe. October, 2021. Accessed July, 2022. <https://cybersec4europe.eu/wp-content/uploads/2022/02/D3.13-Updated-version-of-enablers-and-components-v3.0-submitted.pdf>
* Sforzin, Alessandro. 2021. "D5.5 Specification and set-up demonstration case Phase 2." Cybersec4Europe. December, 2021. Accessed July, 2022. <https://cybersec4europe.eu/wp-content/uploads/2022/01/D5.5-Specification-and-set-up-demonstration-case-Phase-2-v1.0_submitted.pdf>
* Li, Wenting, Alessandro Sforzin, Sergey Fedorov, and Ghassan O. Karame. "Towards scalable and private industrial blockchains." In Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts, pp. 9-14. 2017. DOI: 10.1145/3055518.3055531
* Liu, Jian, Wenting Li, Ghassan O. Karame, and N. Asokan. "Scalable byzantine consensus via hardware-assisted secret sharing." IEEE Transactions on Computers 68, no. 1 (2018): 139-151. DOI: 10.1109/TC.2018.2860009
* Wang, Wan, Fengjiao Xu, Chao Zhang, and Tingxin Qin. "Analysis on security management for supply chain under Emergencies." In 2021 International Conference on Public Management and Intelligent Society (PMIS), pp. 208-211. IEEE, 2021. DOI: 10.1109/PMIS52742.2021.00052
* Kieras, Timothy, Muhammad Junaid Farooq, and Quanyan Zhu. "Modeling and assessment of iot supply chain security risks: the role of structural and parametric uncertainties." In 2020 IEEE Security and Privacy Workshops (SPW), pp. 163-170. IEEE, 2020. DOI: 10.1109/SPW50608.2020.00043
* Ohm, Marc, Arnold Sykosch, and Michael Meier. "Towards detection of software supply chain attacks by forensic artifacts." In Proceedings of the 15th international conference on availability, reliability and security, pp. 1-6. 2020. DOI: 10.1145/3407023.3409183
* Vasilakis, Nikos, Achilles Benetopoulos, Shivam Handa, Alizee Schoen, Jiasi Shen, and Martin C. Rinard. "Supply-chain vulnerability elimination via active learning and regeneration." In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 1755-1770. 2021. DOI: 10.1145/3460120.3484736
* Topping, Colin, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid. "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks." Computers & Security 108 (2021): 102324. DOI: 10.1016/j.cose.2021.102324
* Gupta, Nikhil, Akash Tiwari, Satish TS Bukkapatnam, and Ramesh Karri. "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks." IEEE Access 8 (2020): 47322-47333. DOI: 10.1109/ACCESS.2020.2978815
* Sawik, Tadeusz. "Balancing cybersecurity in a supply chain under direct and indirect cyber risks." International Journal of Production Research 60, no. 2 (2022): 766-782. DOI: 10.1080/00207543.2021.1914356
* Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. No. NIST Internal or Interagency Report (NISTIR) 8276. National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.IR.8276
* Etemadi, Niloofar, Yari Borbon-Galvez, Fernanda Strozzi, and Tahereh Etemadi. "Supply chain disruption risk management with blockchain: a dynamic literature review." Information 12, no. 2 (2021): 70. DOI: 10.3390/info12020070
* Wang, Xinyuan. "On the Feasibility of Detecting Software Supply Chain Attacks." In MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM), pp. 458-463. IEEE, 2021. DOI: 10.1109/MILCOM52596.2021.9652901

### Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems

All existing CyberSec4Europe assets developed in this vertical implicitly improve the resilience of cyber-physical systems, due to their decentralized nature. IT/OT convergence is also supported by initiatives like Zero Trust, applied by CyberSec4Europe partners and other entities. Other approaches in this area include specific security frameworks for cyber-physical risks in digital supply chains, cost-benefit analyses for infrastructure hardening, and security mechanisms that take advantage of cyber and physical systems specific features (e.g. sensor capabilities of dynamic IoT networks).

References:

* Kasinathan, Prabhakaran, and Jorge Cuellar. "Securing emergent IoT applications." In International Summer School on Engineering Trustworthy Software Systems, pp. 99-147. Springer, Cham, 2018. DOI: 10.1007/978-3-030-17601-3\_3
* Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero trust architecture. No. NIST Special Publication (SP) 800-207. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207
* Jayaprasanna, M. C., V. A. Soundharya, M. Suhana, and S. Sujatha. "A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain." In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 253-257. IEEE, 2021. DOI: 10.1109/ICICV50876.2021.9388568
* ASangeetha, A. S., S. Shunmugan, and G. Murugan. "Blockchain for IoT enabled supply chain management-A systematic review." In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 48-52. IEEE, 2020. DOI: 10.1109/I-SMAC49090.2020.9243371
* Ofori-Yeboah, Abel, Ronald Addo-Quaye, Waheed Oseni, Prince Amorin, and Conrad Agangmikre. "Cyber supply chain security: a cost benefit analysis using net present value." In 2021 International Conference on Cyber Security and Internet of Things (ICSIoT), pp. 49-54. IEEE, 2021. DOI: 10.1109/ICSIoT55070.2021.00018
* Bhutta, Muhammad Nasir Mumtaz, and Muneer Ahmad. "Secure identification, traceability and real-time tracking of agricultural food supply during transportation using internet of things." IEEE Access 9 (2021): 65660-65675. DOI: 10.1109/ACCESS.2021.3076373
* Skrodelis, Heinrihs Kristians, and Andrejs Romanovs. "Cyber-physical Risk Security Framework Development in Digital Supply Chains." In 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), pp. 1-5. IEEE, 2021. DOI: 10.1109/ITMS52826.2021.9615305
* Melnyk, Steven A., Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F. Chang, and Derek Friday. "New challenges in supply chain management: cybersecurity across the supply chain." International Journal of Production Research 60, no. 1 (2022): 162-183. DOI: 10.1080/00207543.2021.1984606
* Sawik, Tadeusz. "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains." International Journal of Production Research 60, no. 4 (2022): 1368-1385. DOI: 10.1080/00207543.2020.1856442
* Kyranoud, Pinelopi, Eleni-Maria Kalogeraki, Alexandra Michota, and Nineta Polemi. "Cybersecurity Certification Requirements for Supply Chain Services." In 2021 IEEE Symposium on Computers and Communications (ISCC), pp. 1-7. IEEE, 2021. DOI: 10.1109/ISCC53001.2021.9631467

### Challenge 3: Security and privacy of supply chain information assets and goods

Both use case demonstrators (cf. CyberSec4Europe deliverable D5.5) developed in this vertical illustrate how corporate proprietary information or sensitive data can be shared and stored reliably in a blockchain-based environment. In fact, most of the solutions developed in the last years have focused in the integration of blockchain solutions, aiming to capture supply chain stakeholder interactions that enhance trust among participating entities. In addition, novel technologies such as decentralised identifiers (DIDs) and verifiable credentials (VCs) allow individuals to decide on their own how to manage and share information.

References:

* Zupan, Nejc, Prabhakaran Kasinathan, Jorge Cuellar, and Markus Sauer. "Secure smart contract generation based on petri nets." In Blockchain Technology for Industry 4.0, pp. 73-98. Springer, Singapore, 2020. DOI: 10.1007/978-981-15-1137-0\_4
* Kasinathan, Prabhakaran, Davide Martintoni, Benedikt Hofmann, Valerio Senni, and Martin Wimmer. "Secure Remote Maintenance via Workflow-Driven Security Framework." In 2021 IEEE International Conference on Blockchain (Blockchain), pp. 29-37. IEEE, 2021. DOI: 10.1109/Blockchain53845.2021.00016
* Omar, Ilhaam A., Raja Jayaraman, Mazin S. Debe, Haya R. Hasan, Khaled Salah, and Mohammed Omar. "Supply Chain Inventory Sharing using Ethereum Blockchain and Smart Contracts." IEEE Access 10 (2021): 2345-2356. DOI: 10.1109/ACCESS.2021.3139829
* Syed, Naeem Firdous, Syed W. Shah, Rolando Trujillo-Rasua, and Robin Doss. "Traceability in supply chains: A Cyber security analysis." Computers & Security 112 (2022): 102536. DOI: 10.1016/j.cose.2021.102536
* Sezer, Bora Buğra, Selçuk Topal, and Urfat Nuriyev. "TPPSUPPLY: A traceable and privacy-preserving blockchain system architecture for the supply chain." Journal of Information Security and Applications 66 (2022): 103116. DOI: 10.1016/j.jisa.2022.103116
* Ravi, Deebthik, Sashank Ramachandran, Raahul Vignesh, Vinod Ramesh Falmari, and M. Brindha. "Privacy preserving transparent supply chain management through Hyperledger Fabric." Blockchain: Research and Applications 3, no. 2 (2022): 100072. DOI: 10.1016/j.bcra.2022.100072
* Bader, Lennart, Jan Pennekamp, Roman Matzutt, David Hedderich, Markus Kowalski, Volker Lücken, and Klaus Wehrle. "Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability." Information Processing & Management 58, no. 3 (2021): 102529. DOI: 10.1016/j.ipm.2021.102529
* El Azzaoui, Abir, Haotian Chen, So Hyeon Kim, Yi Pan, and Jong Hyuk Park. "Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems." Sensors 22, no. 4 (2022): 1371. DOI: 10.3390/s22041371
* Demertzis, Konstantinos, Lazaros Iliadis, Elias Pimenidis, Nikolaos Tziritas, Maria Koziri, Panagiotis Kikiras, and Michael Tonkin. "Federated Blockchained Supply Chain Management: A CyberSecurity and Privacy Framework." In IFIP International Conference on Artificial Intelligence Applications and Innovations, pp. 769-779. Springer, Cham, 2021. DOI: 10.1007/978-3-030-79150-6\_60

### Challenge 4: Management of the certification of supply partners

All three assets listed in the beginning of this section strongly contribute to the specific research goal to “continuously monitor for compliance with standards and recommendations”, as illustrated, for example, in the demonstrator setup and usage of SCH-UC2 (cf. CyberSec4Europe deliverable D5.5). In addition, these assets can also be used to fulfil use cases like carbon footprint tracking for general compliance, which is being considered by non-profit associations and corporate initiatives such as ESTAINIUM and SiGREEN. As for other solutions not based on blockchains, this area has advanced less compared to other challenges, although there have been approaches such as metrics and models for continuous safety assessment and retail-driven sustainability certification schemes.

* ESTAINIUM. Accessed July, 2022. <https://profiles.eco/estainium>
* SiGREEN. Accessed July, 2022. <https://www.siemens.com/sigreen>
* Stahnke, Susanne. 2020. "Workflow enforcement for certification of the construction of industrial plants." Passau: University of Passau (2020)
* Santos, Henrique, André Oliveira, Lúcia Soares, Alan Satis, and Alexandre Santos. "Information Security Assessment and Certification within Supply Chains." In The 16th International Conference on Availability, Reliability and Security, pp. 1-6. 2021. DOI: 10.1145/3465481.3470078
* Tong, Xun, Kee-hung Lai, Chris KY Lo, and T. C. E. Cheng. "Supply chain security certification and operational performance: The role of upstream complexity." International Journal of Production Economics 247 (2022): 108433. DOI: 10.1016/j.ijpe.2022.108433
* Chkanikova, Olga, and Robert Sroufe. "Third-party sustainability certifications in food retailing: Certification design from a sustainable supply chain management perspective." Journal of Cleaner Production 282 (2021): 124344. DOI: 10.1016/j.jclepro.2020.124344

## Progress Made in Privacy-Preserving Identity Management

Regarding Cybersec4Europe’s assets that contribute to improving the privacy-preserving identity management landscape, there have been various assets, developed in WP3 and WP5 and evaluated by Cybersec4Europe, that support this goal through either technical advances that enable privacy-preserving mechanisms, or supporting systems. The main assets related to this vertical are:

* **SS-PP-IdM:** This asset leverages the OLYMPUS virtual identity provider, which is comprised of multiple individual IdPs, to manage user identities and authentication. It relies on distributed p-ABCs (i.e., privacy -preserving attribute-based credentials) to offer privacy-preserving (minimal disclosure and unlinkability) and authentication (presentation of attributes) linked to eIDAS. Moreover, the asset proposes a trust framework based on Blockchain to complement the usage of credentials.
* **P-ABC scheme**: P-ABC allow users to control which information is revealed when interacting with the capability-based access control and avoiding the IdP as a single point of failure. What is more, it tackles the lack of homogeneity in representing p-ABCs, one of the issues that jeopardized adoption of previous p-ABC systems, by integrating with the emerging W3C Verifiable Credential standard for serialization.
* **Issuer-hiding attribute-based credentials**: Issuer-hiding anonymous credential systems provide a mechanism for privacy-friendly identity management. They enhance over the state of the art by not only offering means for selective disclosure and data minimization (cf. also asset SS-PP-IdM and cloud-based credentials), but also allow for hiding the issuer of a certain credential (allowing, e.g., to prove that one is eligible for a student discount without having to reveal the university one is studying at).
* **eIDAS browser:** The eIDAS regulation aims at increasing the effectiveness of public and private online services, electronic business, and electronic commerce in the Union. To this end, it includes provisions for electronic identification and trust services. In that sense, eIDAS browser is an application that allows interacting with eIDAS nodes to obtain certified attributes in compliance with the regulation.
* **Password-less AuthN:** The password-less authentication asset is based on the FIDO standards. It provides a device-centric authentication that implements a) a challenge-response scheme in which the user is authenticated locally (i.e., on the device that it is deployed to access the service) using alternative authentication methods, such as PIN, USB keys, and biometrics and b) public key cryptography to authenticate the device in the service. During the FIDO authentication, when a user (in our case a student) is authenticated in its device (for instance, using a USB key), it unlocks its private key, which subsequently is deployed to sign the challenge and the service deploys the user’s public key, to decode the challenge.
* **GDPR compliant user experience**: It is a document with guidelines on the regulation's requirements and how to achieve them. It is structured around the GDPR principles. The asset also includes a template for Data Protection Impact Assessments (DPIA). The template guides users through the process of doing a DPIA and also serves as documentation for the performed analysis. The asset was introduced in deliverable D3.6 Guidelines for GDPR compliant user experience and later partially updated in deliverable D3.16 Security requirements and risks conceptualisation. It was demonstrated on a small scale in deliverables D3.13 Updated version of enablers and components and D3.17 Integration to demonstration cases.
* **Interoperability and cross-border compliance**: It is an asset that addresses issues related to different electronic Identification, Authentication and trust Services (eIDAS) and GDPR implementations and legislation differences in EU member states, ultimately hampering the idea of a Single European Market. This asset mainly focuses on some shortcomings of the eIDAS network (in its interoperability between nodes and across member states' borders) as it is currently and also some questionable technologies used in user authentication. In the second part, the asset identifies and documents the differences between Member states from the perspective of the GDPR. The asset was introduced in deliverable D3.18 Analysis of interoperability and cross-border compliance issues and was later demonstrated in deliverables D3.13 Updated version of enablers and components and D3.20 Final cybersecurity enablers and underlying technologies components.
* **Cloud-based privacy-preserving authentication mechanism:** This type of ABC systems have been designed with constraint devices in mind, by allowing to outsource the computationally heavy parts of the authentication flow to a cloud-service without disclosing sensitive information to this service.

### Challenge 1: System-based credential hardening

One of the assets most related to this challenge is the SS-PP-IdM. While the development of the asset within the project has not been focused on this, the SS-PP-IdM includes password hardening by using distributed oblivious pseudorandom functions, so identities cannot be compromised unless all servers are. Other approaches in this area have also focused on cryptographic mechanisms (secret-sharing…) or on system-based solutions, using supporting tools like MFA or TLS.

References:

* Baum, Carsten, Tore Frederiksen, Julia Hesse, Anja Lehmann, and Avishay Yanai. "PESTO: proactively secure distributed single sign-on, or how to trust a hacked server." In 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 587-606. IEEE, 2020
* Karie, Nickson M., Victor R. Kebande, Richard A. Ikuesan, Mehdi Sookhak, and Hein S. Venter. "Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud." In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, pp. 1-6. 2020
* Diomedous, Constantinos, and Elias Athanasopoulos. "Practical password hardening based on TLS." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 441-460. Springer, Cham, 2019

### Challenge 2: Unlikability and minimal disclosure

While various assets of the project are related to this challenge, two are the most relevant in this context. We have achieved a distributed p-ABC based on efficient Pointcheval-Sanders multi-signatures. Within the project, its maturity has been improved, resulted in the full inclusion of range proofs for integers and dates, as well as some general implementation improvements and its integration with the W3C’s Verifiable Credential’s specification. Additionally, we have introduced the notion of issuer-hiding ABC systems, where even the issuer of a credential may be hidden within a dynamic set of issuers, thereby improving the level of privacy in many practical scenarios with multiple eligible yet independent issuers. The relevance of such an approach is underpinned by the independent and parallel work of Connolly et al.

Most recent works regarding unlinkability and minimal disclosure have been focused on cryptographic tools and, more specifically, on advances on the practicality (including different hierarchical scenarios such as delegatable credentials), expressiveness and functionality (e.g., including advanced features like revocation), and efficiency of attribute-based-credentials.

Finally, the progress of the solutions to this challenge is underpinned by multiple ongoing standardization activities within major SDOs.

References:

* Bernabe, Jorge Bernal, Jesús García-Rodríguez, Stephan Krenn, Vasia Liagkou, Antonio Skarmeta, and Rafael Torres. "Privacy-Preserving Identity Management and Applications to Academic Degree Verification." In IFIP International Summer School on Privacy and Identity Management, pp. 33-46. Springer, Cham, 2022 (explains concepts about p-ABCs and recounts how the p-ABC scheme can be applied to improve a use case over using Idemix.)
* Bobolz, Jan, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, and Kai Samelin. "Issuer-Hiding Attribute-Based Credentials." In International Conference on Cryptology and Network Security, pp. 158-178. Springer, Cham, 2021
* Connolly, Aisling, Pascal Lafourcade, and Octavio Perez Kempner. "Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes." In IACR International Conference on Public-Key Cryptography, pp. 409-438. Springer, Cham, 2022.
* Camenisch, Jan, Manu Drijvers, Anja Lehmann, Gregory Neven, and Patrick Towa. "Short threshold dynamic group signatures." In International Conference on Security and Cryptography for Networks, pp. 401-423. Springer, Cham, 2020
* Hébant, Chloé, and David Pointcheval. "Traceable constant-size multi-authority credentials." Cryptology ePrint Archive (2020)
* Sanders, Olivier. "Efficient redactable signature and application to anonymous credentials." In IACR International Conference on Public-Key Cryptography, pp. 628-656. Springer, Cham, 2020.
* Zhang, Zhiyi, Michal Król, Alberto Sonnino, Lixia Zhang, and Etienne Rivière. "EL PASSO: Efficient and lightweight privacy-preserving single sign on." Proceedings on Privacy Enhancing Technologies 2021, no. 2 (2021): 70-87
* Sarier, Neyire Deniz. "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management." Computers & Security 105 (2021): 102243
* Frederiksen, Tore. "A Holistic Approach to Enhanced Security and Privacy in Digital Health Passports." In The 16th International Conference on Availability, Reliability and Security, pp. 1-10. 2021
* Begum, Nasima, and Toru Nakanishi. "An Accumulator-Based Revocation in Delegatable Anonymous Credentials." In 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), pp. 314-320. IEEE, 2020
* Andersen, Mads Schaarup. "Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark–Usefulness, Barriers, and Recommendations." In The 16th International Conference on Availability, Reliability and Security, pp. 1-8. 2021
* [ISO/IEC 27551], published in 2021, provides a framework for attribute-based unlinkable entity authentication.
* [ISO/IEC 23264-1], published in 2021 and co-edited by CyberSec4Europe experts, provides the framework for redactable signatures, which in turn are a core building block for many entity authentication schemes; Part 2 with specific schemes is currently under development.
* [ISO/IEC 20009-3], published in 2022 and co-edited by CyberSec4Europe experts, specifies a specific anonymous entity authentication scheme from blind signatures.

### Challenge 3: Distributed Oblivious Identity Management

In relation to the challenge of achieving Distributed Oblivious Identity Management there are two particularly important assets. First, **eIDAS browser**. The browser is an Android application that transparently integrates eIDAS authentication via NFC using Spanish ID card (DNIe). This asset has been integrated with the project’s pilots and as a source of trusted data for registration in the SS-PP-IdM.

Secondly, the **SS-PP-IdM** asset introduces oblivious distributed issuers of privacy-preserving attribute-based credentials for a user-controlled approach. We have worked on the improvement of the system, and its integration with blockchain acting as a verifiable data registry for a holistic IdM environment. Additional work has been done in improving the usability and user experience of the system, as well as its integration in ecosystems like smart cities, XACML-based authorization frameworks and with other project assets like GDPR-based tools CaPe and GENERAL\_D. Other works have usually been focused on improving specific aspects (like allowing practical SSO with cryptographic materials), but are usually lacking some desirable properties (e.g., non-distributed issuance).

References:

* Bernabe, Jorge Bernal, Jesús García-Rodríguez, Stephan Krenn, Vasia Liagkou, Antonio Skarmeta, and Rafael Torres. "Privacy-Preserving Identity Management and Applications to Academic Degree Verification." In *IFIP International Summer School on Privacy and Identity Management*, pp. 33-46. Springer, Cham, 2022 (explains the ideas behind the SS-PP-IdM asset implementation and its use for improved pp-IdM)
* Daoudagh, Said, Eda Marchetti, Vincenzo Savarino, Jorge Bernal Bernabe, Jesús García-Rodríguez, Rafael Torres Moreno, Juan Antonio Martinez, and Antonio F. Skarmeta. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal." *Sensors* 21, no. 21 (2021): 7154 (proposes GDPR-aware and private-by-design consent and access control in a smart city scenario using project’s tools
* Bernabe, Jorge Bernal, Martin David, Rafael Torres Moreno, Javier Presa Cordero, Sébastien Bahloul, and Antonio Skarmeta. "ARIES: Evaluation of a reliable and privacy-preserving European identity management framework." *Future Generation Computer Systems* 102 (2020): 409-425
* Moreno, Rafael Torres, Jesús García-Rodríguez, Jorge Bernal Bernabé, and Antonio Skarmeta. "A Trusted Approach for Decentralised and Privacy-Preserving Identity Management." *IEEE Access* 9 (2021): 105788-105804
* Torres Moreno, Rafael, Jorge Bernal Bernabe, Jesus Garcia Rodriguez, Tore Kasper Frederiksen, Michael Stausholm, Noelia Martínez, Evangelos Sakkopoulos, Nuno Ponte, and Antonio Skarmeta. "The OLYMPUS architecture—Oblivious identity management for private user-friendly services." *Sensors* 20, no. 3 (2020): 945
* Zhang, Zhiyi, Michal Król, Alberto Sonnino, Lixia Zhang, and Etienne Rivière. "EL PASSO: Efficient and lightweight privacy-preserving single sign on." *Proceedings on Privacy Enhancing Technologies* 2021, no. 2 (2021): 70-87

### Challenge 4: Privacy Preservation in Blockchain

Within the project, we have worked on the blockchain integration for the SS-PP-IdM asset, achieving a mature deployment based on Hyperledger Ledger Fabric with Smart Contract support. This deployment enabled the integration and improvement of the distributed oblivious system and the adoption of the W3C Verifiable Credential, acting as a verifiable data registry and regulating the publication of critical data (public keys, schemas and even services and policies offered by dependent parties) through smart contracts. The integration with blockchain and smart contracts has demonstrated the feasibility and performance of the SS-PP-IdM solution, enabling transparent management of public cryptographic material and demonstrating flexibility in the scenario deployment. Additionally, attribute-based credentials are one of the main building blocks for privacy-preserving blockchain solutions, so the ABC assets within the project also contribute to the general advancement of this field. Other works have been also mostly focused on attribute-based credentials, or general infrastructures for enabling identity management (e.g. Sovrin).

References:

* Shin, Ji Sun, Shincheol Lee, Seoyun Choi, Minjae Jo, and Sung-Hoon Lee. "A New Distributed, Decentralized Privacy-Preserving ID Registration System." IEEE Communications Magazine 59, no. 6 (2021): 138-144
* Sarier, Neyire Deniz. "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management." Computers & Security 105 (2021): 102243
* Torres Moreno, Rafael, Jorge Bernal Bernabe, Jesus Garcia Rodriguez, Tore Kasper Frederiksen, Michael Stausholm, Noelia Martínez, Evangelos Sakkopoulos, Nuno Ponte, and Antonio Skarmeta. "The OLYMPUS architecture—Oblivious identity management for private user-friendly services." Sensors 20, no. 3 (2020): 945
* Abraham, Andreas, Karl Koch, Stefan More, Sebastian Ramacher, and Miha Stopar. "Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation." In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 506-513. IEEE, 2021.
* Helminger, Lukas, Daniel Kales, Sebastian Ramacher, and Roman Walch. "Multi-party revocation in sovrin: Performance through distributed trust." In Cryptographers’ Track at the RSA Conference, pp. 527-551. Springer, Cham, 2021

### Challenge 5: Passwordless Authentication

The Password-less AuthN asset introduces an authentication method that is based on FIDO standards[[8]](#footnote-9) to perform a secure password-less authentication based on challenge-response scheme. Particularly, the authentication is performed via something that user has (e.g., smartphone) and/or something that user is (e.g., biometrics). More information about this asset can be found in [D3.13]. Other works have also been based on the important FIDO standard, or attribute-based authentication.

References:

* Angelogianni, Anna, Ilias Politis, and Christos Xenakis. "How many FIDO protocols are needed? Surveying the design, security and market perspectives." arXiv preprint arXiv:2107.00577 (2021)
* Vasileios Grammatopoulos, Athanasios, Ilias Politis, and Christos Xenakis. "A web tool for analyzing FIDO2/WebAuthn Requests and Responses." In The 16th International Conference on Availability, Reliability and Security, pp. 1-10. 2021
* Papadamou, Kostantinos, Savvas Zannettou, Bogdan Chifor, Sorin Teican, George Gugulea, Alberto Caponi, Annamaria Recupero et al. "Killing the Password and Preserving Privacy with Device-Centric and Attribute-Based Authentication." IEEE Transactions on Information Forensics and Security 15 (2019): 2183-2193
* Lyastani, Sanam Ghorbani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication." In IEEE Symposium on Security and Privacy, pp. 268-285. 2020.

### Challenge 6: GDPR and eIDAS impact on Identity Management

The GDPR compliant user experience is a document with guidelines on regulation's requirements and how to achieve them. It is structured around the GDPR principles. While the asset provides general guidelines, they are very relevant for the field of authentication, and privacy-preserving authentication is especially beneficial to the data minimization principle. The asset also includes a template for Data Protection Impact Assessments (DPIA). The template guides users through the process of doing a DPIA and also serve as documentation for the performed analysis. Additionally, the Interoperability and cross-border compliance asset addresses issues related to different eIDAS implementations and legislation differences in EU member states, ultimately hampering the idea of a Single European Market. This asset mainly focuses on some shortcomings of the eIDAS network (in its interoperability between nodes and across member states' borders) as it is currently and also some questionable technologies used in user authentication. In the second part, the asset identifies and documents the differences between Member states from the perspective of the GDPR.

References:

* Kutyłowski, Mirosław, and Przemysław Błaśkiewicz. "Advanced Electronic Signatures and eIDAS–Analysis of the Concept." Computer Standards & Interfaces (2022): 103644
* McDowell, Brett. "Three ways in which GDPR impacts authentication." Computer Fraud & Security 2019, no. 2 (2019): 9-12
* Naik, Nitin, and Paul Jenkins. "Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity." In 2020 7th International Conference on Behavioural and Social Computing (BESC), pp. 1-6. IEEE, 2020
* Hölbl, Marko, Boštjan Kežmah, and Marko Kompara. "Data Protection Heterogeneity in the European Union." Applied Sciences 11, no. 22 (2021): 10912

### Challenge 7: Identity Management Solutions for the IoT

While applicability of project’s solutions in general (regarding their efficiency, decentralization level, and other parameters relevant to the IoT landscape) to IoT scenarios is taken into account, there is an asset most specifically linked to these scenarios: the cloud-based credential mechanism co-developed within the project, with feasibility results[[9]](#footnote-10) for its applicability for privacy-preserving identity management in constrained scenarios through delegation. Many of the proposals in this field have focused on the safe delegation of expensive procedures, while some have been centred on achieving efficient solutions or establishing system-wide infrastructures for identity management.

References:

* Haböck, Ulrich, and Stephan Krenn. "Breaking and fixing anonymous credentials for the cloud." In International Conference on Cryptology and Network Security, pp. 249-269. Springer, Cham, 2019
* Hanzlik, Lucjan, and Daniel Slamanig. "With a little help from my friends: constructing practical anonymous credentials." In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 2004-2023. 2021.
* Camenisch, Jan, Manu Drijvers, Petr Dzurenda, and Jan Hajny. "Fast keyed-verification anonymous credentials on standard smart cards." In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 286-298. Springer, Cham, 2019.
* Pinjala, Sandeep Kiran, S. Sree Vivek, and Krishna M. Sivalingam. "Delegated Anonymous Credentials with Revocation Capability for IoT Service Chains (DANCIS)." IEEE Internet of Things Journal 9, no. 5 (2021): 3729-3742.
* Boneh, Dan, Saba Eskandarian, and Ben Fisch. "Post-quantum EPID signatures from symmetric primitives." In Cryptographers’ Track at the RSA Conference, pp. 251-271. Springer, Cham, 2019
* Bouras, Mohammed Amine, Qinghua Lu, Sahraoui Dhelim, and Huansheng Ning. "A lightweight blockchain-based IoT identity management approach." Future Internet 13, no. 2 (2021): 24
* Vallois, Valentin, Ahmed Mehaoua, and Mourad Amziani. "Blockchain-based Identity and Access Management in Industrial IoT Systems." In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 623-627. IEEE, 2021
* Barbareschi, Mario, Valentina Casola, Alessandra De Benedictis, Erasmo La Montagna, and Nicola Mazzocca. "On the adoption of physically unclonable functions to secure iiot devices." IEEE Transactions on Industrial Informatics 17, no. 11 (2021): 7781-7790
* Prabhakar, Anjana, and Tricha Anjali. "Towards flexible hardware authentication for IoT." In 2021 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6. IEEE

## Progress Made in Incident Reporting

The following assets, developed in WP3 and evaluated by Cybersec4Europe, provide support in the mandatory incident reporting process that need to be followed by the financial sector, taking into consideration aspects of all the research challenges identified for this vertical in section 6.6 of roadmap deliverable D4.5 [D4.5] and that will be described below in different subsections. The main assets are:

* **Atos Incident Reporting Engine (AIRE)** is an asset developed in T3.5 in the context of adaptive security, focused on the adaptation of the mandatory incident reports that need to be produced and sent to different Competent Authorities according to different procedures and templates which depend on the different regulatory frameworks affecting the financial sector and on providing, through its integration with an incident management tool (such as the open source tool TheHive[[10]](#footnote-11) used in the demonstrator of T5.4) capabilities to enforce the suitable workflow to be used in the incident reporting process with managerial judgement. This is an asset that was developed from scratch in Cybersec4Europe to cover those missing main functionalities included in the demonstrator of T5.4 of WP5 as described in D5.4 [D5.4] (IR-F08, IR-F09 and IR-F13). The description and details about this asset are available in section 6.1 of D3.21 [1] and its integration in the Incident Reporting Platform demonstrator is described in section 5.2 of D5.5 [D5.5].
* **Trustworthy APIs for enhanced threat intelligence sharing (TATIS)** is an asset developed in T3.4 to provide threat intelligence data sharing trustworthiness in MISP through the application of encryption mechanisms depending on enhanced privacy policies defined (the description of this assets and details about it are available in section 2.3.1.1 of D3.14 [D3.14]). This asset has been included in the IR-UC4 use case of the Incident Reporting Platform demonstrator of T5.4 to provide the capability to the financial institutions to share information about the security incident reported with different granularity depending on the confidentiality they have defined in the data sharing policy in order more sensitive information will be not shared with everybody but only with trusted organisations or entities. More details about the integration of this asset with the demonstrator can be found in D5.5 [D5.5].
* **Threat Intelligence Integrator** **(TIE)** is an asset that provide context awareness for shared threat intelligence data. It has been integrated to the Incident Reporting Platform demonstrator of T5.4 to offer the users a score with the actionability of the security events shared through MISP considering its accuracy, completeness, relevant, timeliness and variety based on previous threat intelligence information received as well as an inventory with information about the specific infrastructure of the financial institution where the platform is running. More details about this asset can be found in section 2.3.1.3 of D3.14 [D3.14])

Other assets that also contribute in some way to the progress in this vertical are:

* **Reliable Cyber-Threat intelligence sharing (Reliable-CTIs)** is an asset developed in T3.4 to generate a score that assess the trustworthiness and reliability of the exchanged data (as described available in section 2.3.1.6 of D3.14 [D3.14]). This asset was foreseen to be included in the last phase of the demonstrator of T5.4 to analyse and enrich with information about the trustworthiness of its source the security event about an incident shared by a financial entity through the Threat Intelligence Platform MISP. However, finally it has not been included since the partner involved in the implementation of this prototype has focused on other asset, Privacy-Preserving CTI that could be also included in this demonstrator to complement the capabilities provided by TATIS asset described above.
* **Automatic analysis of malware samples (HADES)** is an asset developed in T3.4 to orchestrate sandboxes for malware execution (details about the asset available in section 2.3.1.9 of D3.14 [D3.14]). This asset has been integrated with the demonstrator of this vertical as an analyser that can be used by the users of the Incident Management Team to obtain more information about a security incident to be reported during the data enrichment phase. More details about the integration of this asset with the demonstrator can be found in section 5.2 of D5.5 [D5.5].
* **JSON Users and Device analysis (JUDAS)** is an asset also developed in T3.4 that can be used for digital forensic analysis to extract information about the context of an incident providing the relationships between users and devices. This asset has been integrated in the same way than HADES with the Incident Reporting Platform demonstrator for data enrichment in the process of collection of information about a security incident to be reported. More details about the asset available in section 5.1.8 of D3.3 [D3.3].

### Challenge 1: Lack of harmonization of procedures

This challenge is mainly addressed by the asset AIRE and integrated in the use cases IR-UC1 (Incident Data Collection, Enrichment and Classification), IR-UC2 (Managerial Judgement) and IR-UC3 (Data Conversion and Reporting Preparation) which go throughout the different phases included in any mandatory incident reporting process, as described in D5.5 [D5.5].

References:

* “EBF Position Paper on the European Commission’s Proposal for a Regulation on Digital Operational Resilience for the Financial Sector (DORA).” European Banking Federation, April 2021. https://www.ebf.eu/wp-content/uploads/2021/05/EBF-Position-Paper\_DORA.pdf.
* “European Commission Proposal for a Regulation on Digital Operational Resilience of the Financial Sector (DORA).” Association for Financial Markets in Europe (AFME). February 2021. https://service.betterregulation.com/document/487540
* “Cyber Incident Notification and Reporting Requirements for Financial Institutions”. Bank Policy Institute. April 2022. <https://bpi.com/wp-content/uploads/2022/04/Cyber-Incident-Notification-and-Reporting-Requirements-for-Financial-Institutions-04-21-2022.pdf>
* “Revision proposal on Directive on security of network and information systems (NIS2 Directive)”. Council of the European Union. November 2021. https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf
* “Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence”. Financial Stability Board. October 2021. <https://www.fsb.org/wp-content/uploads/P191021.pdf>
* “EBF Position on Cyber incident reporting”. European Banking Federation. June 2020. <https://www.ebf.eu/wp-content/uploads/2020/06/EBF-position-paper-on-cyber-incident-reporting_annex-on-FLIIS.pdf>
* “EU CyberSecurity Initiatives in the Finance Sector”. ENISA. March 2021. <https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector>
* “Financial Sector’s Cybersecurity: A Regulatory Digest”. World Bank Group. May 2019. <https://thedocs.worldbank.org/en/doc/208271558450284768-0130022019/original/CybersecDigest3rdEditionMay2019.pdf>

### Challenge 2: Facilitate the collection and reporting of incident and/or data leaks

All the assets involved in the demonstrator of this vertical described in the introduction of this section participate in some way to address this challenge. Through the integration with the open-source tool TheHive to collect information about the security incidents, AIRE is responsible for ensuring the reporting process is followed and the reports generated in the suitable format. Additional, AIRE integrates a dashboard to collect additional and specific information required for mandatory incident reporting. HADES and JUDAS, also integrated with the open-source tool TheHive facilitate investigation and additional information about the security incidents. Finally, TATIS, Reliable-CTIs and TIE provide support for the collection and data sharing of threat intelligence information related to the incidents.

References:

* ENISA. 2022. "Compendium of Risk Management Frameworks with Potential Interoperability." January 2022. Accessed July, 2022. <https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>
* ENISA. 2021. "Technical guideline on incident reporting under the EECC." March 2021. Accessed July, 2022. <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc>
* Nieto, Ana. "Becoming JUDAS: correlating users and devices during a digital investigation." IEEE Transactions on Information Forensics and Security 15 (2020): 3325-3334
* Silverajan, Bilhanan, and Petteri Vistiaho. "Enabling cybersecurity incident reporting and coordinated handling for maritime sector." In 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), pp. 88-95. IEEE, 2019.

### Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience

The three assets deployed in the demonstrator of this vertical related to threat intelligence data sharing (TATIS, Reliable-CTIs and TIE) are aimed at addressing this challenge of collaboration. Although it is widely extended the use of Cyber Threat Intelligence Platforms and they are considered as fundamental to be up to date about security incidents and there is an agreement on the advantages they can provide to the organisations, there are not too much work done on using it for risk assessment and mitigation, as it was described with details in D3.14 [D3.14].

References:

* Preuveneers, Davy, and Wouter Joosen. "TATIS: trustworthy APIs for threat intelligence sharing with UMA and CP-ABE." In International Symposium on Foundations and Practice of Security, pp. 172-188. Springer, Cham, 2019.
* Preuveneers, Davy, Wouter Joosen, Jorge Bernal Bernabe, and Antonio Skarmeta. "Distributed security framework for reliable threat intelligence sharing." Security and Communication Networks 2020 (2020).
* Gonzalez-Granadillo, Gustavo, Mario Faiella, Ibéria Medeiros, Rui Azevedo, and Susana Gonzalez-Zarzosa. "Enhancing Information Sharing and Visualization Capabilities in Security Data Analytic Platforms." In 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 1-8. IEEE, 2019.
* Albakri, Adham, Eerke Boiten, and Richard Smith. "Risk Assessment of Sharing Cyber Threat Intelligence." In European Symposium on Research in Computer Security, pp. 92-113. Springer, Cham, 2020.
* Orlando, Albina. "Cyber risk quantification: Investigating the role of cyber value at risk." Risks 9, no. 10 (2021): 184. DOI: 10.3390/risks9100184
* Böhme, Rainer, Stefan Laube, and Markus Riek. "A fundamental approach to cyber risk analysis." Variance 12, no. 2 (2019): 161-185.
* PwC. 2021. "Cyber risk quantified. Cyber risk managed." Accessed July, 2022. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-risk-quantification-management.html>

## Progress Made in Maritime Transport

The following assets have been developed in the project addressing the research challenges identified for this vertical:

* The **Maritime Transport demonstrator** has been developed, including:
* the deployment of maritime risk assessment (*MITIGATE)* provided by UPRC [D3.1]
* enhancement with security hardening controls provided by UCY [D3.1]
* secure maritime communication *(Secure AIS ASM endpoint)* provided by CYBER [D3.1]
* enhancement with maritime-specific PKI service *(PKI Service)*provided by SINTEF [D3.1]
* enhancement with additional human threat identification (using HAMSTERS) provided by UPS-IRIT [D3.1].

The Maritime Transport demonstrator development was carried out in the context of WP5.

* An **adaptive situation-based risk assessment and security enforcement framework** for the maritime transport sector has been delivered, including methodology development and proof-of-concept implementation, contributed by UPRC and UPS-IRI as part of the activities of tasks T3.5 of WP3 and T5.5 of WP5 (description available in deliverable D3.21 [D3.21])
* A **methodology** has been developed **for the addition of human-related threats to the maritime risk assessment methodology**, contributed by UPS-IRIT *(HAMSTERS)* and UPRC *(MITIGATE)*as part of the activities of tasks T3.6 of WP3 and T5.5 of WP5 (description available in deliverable D3.17 [D3.17])

During the project’s lifespan, a group of security research challenges have been explored and acknowledged as critical for the Maritime Transport vertical. Within the following sections, the mayor advances provided by CYBERSEC4EUROPE partners towards the identified challenges are presented together with a list of publications related to these challenges. Furthermore, the publications list contains research work conducted by consortium partners and other researchers as well which is associated with the current vertical challenges.

### Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems

The CYBERSEC4EUROPE Maritime Transport demonstrator supports methodologies and tools that procure stable datasets. In particular, the CYBERSEC4EUROPE Maritime Transport demonstrator supports an integrated intra and inter-organisation dynamic risk assessment process coupled with an adaptive, event driven security enforcement mechanism which estimates the evolving risks in cost-efficient manner. It allows the early identification and calculation of risks, threats vulnerabilities and attack paths. Moreover, the utilization of machine learning techniques, enables capturing and integrating vulnerability related information from different vulnerability open frameworks and corresponding versions (e.g. CVSS 3.1). In addition, it promotes an evidence-based and scenario-based risk analysis, relying on recent cybersecurity incidents that encapsulate sophisticated attacks, and provides supporting threat scenarios that can be used for active learning processes (i.e. problem-based and case-based learning).

References:

* Grigoriadis, Christos, Romain Laborde, Antonin Verdier, and Panayiotis Kotzanikolaou. "An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector." Sensors 22, no. 1 (2021): 238.
* Martinie, Célia, Christos Grigoriadis, Eleni-Maria Kalogeraki, and Panayiotis Kotzanikolaou. "Modelling Human Tasks to Enhance Threat Identification in Critical Maritime Systems." In 25th Pan-Hellenic Conference on Informatics, pp. 375-380. 2021.
* Grigoriadis, Christos, Adamantios Marios Berzovitis, Ioannis Stellios, and Panayiotis Kotzanikolaou. "A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems." In European Symposium on Research in Computer Security, pp. 23-39. Springer, Cham, 2021.
* Broders, Nicolas, Célia Martinie, Philippe Palanque, Marco Winckler, and Kimmo Halunen. "A Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms." In International Conference on Human-Centred Software Engineering, pp. 61-83. Springer, Cham, 2020.
* Dionysiou, Antreas, and Elias Athanasopoulos. "SoK: Machine vs. machine–A systematic classification of automated machine learning-based CAPTCHA solvers." Computers & Security 97 (2020): 101947.
* Kalogeraki, Eleni-Maria, Spyridon Papastergiou, and Themis Panayiotopoulos. "An Attack Simulation and Evidence Chains Generation Model for Critical Information Infrastructures." Electronics 11, no. 3 (2022): 404.
* Schauer, Stefan, Nineta Polemi, and Haralambos Mouratidis. "MITIGATE: a dynamic supply chain cyber risk assessment methodology." Journal of Transportation Security 12, no. 1 (2019): 1-35.
* Kavallieratos, Georgios, and Sokratis Katsikas. "Attack path analysis for cyber physical systems." In Computer Security, pp. 19-33. Springer, Cham, 2020.
* Polatidis, Nikolaos, Elias Pimenidis, Michalis Pavlidis, Spyridon Papastergiou, and Haralambos Mouratidis. "From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks." Evolving Systems 11, no. 3 (2020): 479-490.
* Gyamfi, Eric, James Adu Ansere, Mohsin Kamal, Muhammad Tariq, and Anca Jurcut. "An Adaptive Network Security System for IoT-Enabled Maritime Transportation." IEEE Transactions on Intelligent Transportation Systems (2022).
* Enoch, Simon Yusuf, Jang Se Lee, and Dong Seong Kim. "Novel security models, metrics and security assessment for maritime vessel networks." Computer Networks 189 (2021): 107934.

### Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems

The CYBERSEC4EUROPE Maritime Transport demonstrator produced in this vertical integrates security controls related to software hardening which can be used to protect critical maritime systems towards malicious activity. In this context, applied controllers have been instantiated to specific threat classes and binary-level analysis techniques and methodologies for program hardening with no recompilation have been utilized.

References:

* Papaevripides, Michalis, and Elias Athanasopoulos. "Exploiting mixed binaries." ACM Transactions on Privacy and Security (TOPS) 24, no. 2 (2021): 1-29.
* Diomedous, Constantinos, and Elias Athanasopoulos. "Practical password hardening based on TLS." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 441-460. Springer, Cham, 2019.
* Lin, Yan, Debin Gao, and David Lo. "ReSIL: Revivifying Function Signature Inference using Deep Learning with Domain-Specific Knowledge." In Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy, pp. 107-118. 2022.
* Duck, Gregory J., Yuntong Zhang, and Roland HC Yap. "Hardening binaries against more memory errors." In Proceedings of the Seventeenth European Conference on Computer Systems, pp. 117-131. 2022.
* Priyanga, S., Roopak Suresh, Sandeep Romana, and V. S. Shankar Sriram. "The Good, The Bad, and The Missing: A Comprehensive Study on the Rise of Machine Learning for Binary Code Analysis." In Computational Intelligence in Data Mining, pp. 397-406. Springer, Singapore, 2022.
* Steudel, Zachary Michael, and Cynthia C. Fry. "Code Hardening: Development of a Reverse Software Engineering Project." In 2020 ASEE Virtual Annual Conference Content Access. 2020.

### Challenge 3: Resilience of critical maritime systems

The maritime transport security demonstrator has been developed and validation has been performed and reported. All CYBERSEC4EUROPE assets of this vertical can be used to improve the resilience of critical maritime systems. The SC4E Maritime Transport demonstrator supports automation of the security policy enforcement promoting the implementation of automated security policies per situation. It provides an adaptive, event-driven security enforcement mechanism which can be utilized to adaptively implement security controls on critical interdependent maritime systems. In addition, Machine Learning based techniques provide efficient indexing of vulnerability related information that facilitates the data analysis during the assessment process. All these features may contribute to advance the level of security of critical maritime systems and thereby improve their resilience.

References:

* Grigoriadis, Christos, Spyridon Papastergiou, Panayiotis Kotzanikolaou, Christos Douligeris, Antreas Dionysiou, Athanasopoulos Elias, Karin Bernsmed, Per Håkon Meland, and Liina Kamm. "Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator." In 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), pp. 371-377. 2021.
* Meland, Per Håkon, Shukun Tokas, Gencer Erdogan, Karin Bernsmed, and Aida Omerovic. "A Systematic Mapping Study on Cyber Security Indicator Data." Electronics 10, no. 9 (2021): 1092.
* Erdogan, Gencer, Enrique Garcia-Ceja, Åsmund Hugo, Phu H. Nguyen, and Sagar Sen. "A Systematic Mapping Study on Approaches for Al-Supported Security Risk Assessment." In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 755-760. IEEE, 2021.
* Papastergiou, Spyridon, Haralambos Mouratidis, and Eleni-Maria Kalogeraki. "Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures." Evolving Systems 12, no. 1 (2021): 91-108.
* Potamos, Georgios, Savvas Theodoulou, Eliana Stavrou, and Stavros Stavrou. "Maritime Cyber Threats Detection Framework: Building Capabilities." In IFIP World Conference on Information Security Education, pp. 107-129. Springer, Cham, 2022.
* Onishchenko, O., K. Shumilova, S. Volyanskyy, Y. Volyanskaya, and Y. Volianskyi. "Ensuring Cyber Resilience of Ship Information Systems." TransNav, International Journal on Marine Navigation and Safety od Sea Transportation 16, no. 1 (2022).
* Akpan, Frank, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, and Michalis Michaloliakos. "Cybersecurity Challenges in the Maritime Sector." Network 2, no. 1 (2022): 123-138.
* Hutschenreuter, Helmar, Salva Daneshgadeh Çakmakçi, Christian Maeder, and Thomas Kemmerich. "Ontology-based Cybersecurity and Resilience Framework." In ICISSP, pp. 458-466. 2021.

### Challenge 4: Maritime system communication security

A demonstrator of a maritime trust infrastructure based on a PKI specifically configured for the environmental limitations of the maritime transport sector, such as network availability and communication costs, has been implemented and validated. The developed trust infrastructure could support encryption requirements to safeguard data during maritime systems communication. In addition, integration of the VDES-ready secure communications application with actual VDES devices is expected to be available in the next few years which will be able to support both satellite and radio communication means.

References:

* Nesheim, Dag Atle, Karin Bernsmed, Bjørn Marius von Zernichow, Ørnulf Jan Rødseth, and Per Håkon Meland. "Secure, Trustworthy and Efficient Information Exchange–Enabling Added Value through The Maritime Data Space and Public Key Infrastructure."
* Konoth, Radhesh Krishnan, Björn Fischer, Wan Fokkink, Elias Athanasopoulos, Kaveh Razavi, and Herbert Bos. "SecurePay: Strengthening Two-Factor Authentication for Arbitrary Transactions." In 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 569-586. IEEE, 2020
* Patsakis, Constantinos, Fran Casino, and Vasilios Katos. "Encrypted and covert DNS queries for botnets: Challenges and countermeasures." Computers & Security 88 (2020): 101614
* Hurley-Smith, Darren, Constantinos Patsakis, and Julio Hernandez-Castro. "On the unbearable lightness of FIPS 140-2 randomness tests." IEEE Transactions on Information Forensics and Security (2020)
* Wimpenny, Gareth, Jan Šafář, Alan Grant, and Martin Bransby. "Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility." The Journal of Navigation 75, no. 2 (2022): 333-345
* Papathanasaki, Maria, Panagiotis Fountas, Leandros Maglaras, Christos Douligeris, and Mohamed Amine Ferrag. "Quantum Cryptography in Maritime Telecommunications." In 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 530-535. IEEE, 2021
* Gupta, Brij Bhooshan, Akshat Gaurav, Ching-Hsien Hsu, and Bo Jiao. "Identity-based authentication mechanism for secure information sharing in the maritime transport system." IEEE Transactions on Intelligent Transportation Systems (2021)

### Challenge 5: Securing autonomous ships

The developed CYBERSEC4EUROPE Maritime Transport demonstrator supports an adaptive risk assessment mechanism that can be adjusted to detect and model threats of autonomous surface ships and thereby increase their preparedness towards malicious activity by performing a more targeted risk assessment and thus increase their level of security. In addition, the future implementation of VDES-ready secure communications application may partially address the need for achieving network availability in unmanned and autonomous ship communications.

References:

* Jo, Yonghyun, Oongjae Choi, Jiwoon You, Youngkyun Cha, and Dong Hoon Lee. "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework." Sensors 22, no. 5 (2022): 1860
* Chang, Chia-Hsun, Christos Kontovas, Qing Yu, and Zaili Yang. "Risk assessment of the operations of maritime autonomous surface ships." Reliability Engineering & System Safety 207 (2021): 107324
* Dittmann, Kjeld, and Mogens Blanke. "Risk mitigation by design of autonomous maritime automation systems." at-Automatisierungstechnik 70, no. 5 (2022): 469-481
* Tusher, Hasan Mahbub, Ziaul Haque Munim, Theo E. Notteboom, Tae-Eun Kim, and Salman Nazir. "Cyber security risk assessment in autonomous shipping." Maritime Economics & Logistics (2022): 1-20
* Askari, Humayun Rashid, and Mohammad Nazir Hossain. "Towards utilizing autonomous ships: A viable advance in industry 4.0." Journal of International Maritime Safety, Environmental Affairs, and Shipping 6, no. 1 (2022): 39-49
* Yoo, Ji-Woon, Yong-Hyun Jo, and Young-Kyun Cha. "Artificial Intelligence for Autonomous Ship: Potential Cyber Threats and Security." Journal of the Korea Institute of Information Security & Cryptology 32, no. 2 (2022): 447-463

## Progress Made in Medical Data Exchange

During the life span of the project the following assets have been developed and evaluated in WP5, for a direct integration in the Medical Data Exchange demonstrator. Aspects identified for this vertical in the roadmap deliverable D4.5 [D4.5] have been considered.

* **Data Anonymisation Service (DANS)** is an anonymisation tool for preserving user data privacy when sensitive data are shared. DANS provides different privacy models such as k-anonymity or l-diversity. These privacy models protect against data disclosure and guarantee data privacy-preserving. DANS is provided as an Anonymisation-as-a-service solution, and as a java library to be integrated directly by the systems of the data provider[D3.2]. DANS asset has been developed in the context of WP3 and WP5 and a more detailed description can be found in section 5.1 Data Anonymisation Service of D3.2 [D3.2]. DANS has been integrated and validated by task T5.6 Medical Data Exchange demonstrator. Details of this demonstrator can be found in section 7 Medical Data Exchange of D5.5 [D5.5];
* **Functional Encryption to Medical Data (FE2MED),** isa functional encryption (FE) tool for protecting medical data when sharing with a third party. FE2MED provides an end-to-end encryption, securing personal and sensitive data. Also, ensures data confidentiality and integrity, and provides a fine-grained control of the decryption capacities of the data recipients [D3.12]. FE2MED is provided as a Functional-as-a-service solution and developed in the context of WP5. More detailed description can be found in section 5 Additional Enablers and Assets Identified in D3.12 [D3.12]. FE2MED has been integrated and validated by task T5.6 Medical Data Exchange demonstrator. Details of this demonstrator can be found in section 7 Medical Data Exchange of D5.5 [D5.5].
* **Visualization tool** is an instrument developed in the context of T5.6 for improving the user experience of the users when browsing the catalogue through the data exchange platform (DEP). This asset includes data sampling and data assessment tools showing a graphical overview of the data included in the data platform [D5.5].
* **eIDAS connector,** is a module created for integrating the eIDAS network with the DEP for authentication purposes when the users acceding the DEP. This tool provides a strong authentication mechanism by using eID issued by the European countries, allowing cross-border access to the DEP [D5.5].
* **Self-Sovereign Privacy-Preserving Identity Management (SS-PP-IdM)** is a component based on the Self-Sovereign Identity paradigm providing a privacy-preserving solution which allows the user to keep the control of their personal identity information through a decentralized solution [D3.11]. The T5.6 demonstrator will study how this enabler could be beneficial for accessing the DEP.

Additionally, the following assets has been developed in the context of WP3 and are being used for checking the privacy risks and regulatory compliance of Medical Data Exchange use:

* **PLEAK**[[11]](#footnote-12), a privacy risk assessment web-based tool allowing “*to model and analyse business processes specified in privacy-enhanced Business Process Model and Notation (PE-BPMN)*” [D3.15]. PLEAK helps to design and analyse processes involving data sharing, for avoiding data privacy leaks. PLEAK has been validated by task T5.6 Medical Data Exchange demonstrator. Details of this demonstrator can be found in section 7 Medical Data Exchange of D5.5 [D5.5];
* **GDPR** **guidelines** **tool**, provides GDPR guidelines to be adopted by data sharing systems. [D3. 6]. These guidelines are the outcomes of research activities developed in T3.7 Regulatory Sources for citizen-friendly Goals providing guidelines for GDPR compliance [D3.6]. GDPR guidelines has been followed by task T5.6 Medical Data Exchange demonstrator. Details of this demonstrator can be found in section 7 Medical Data Exchange of D5.5 [D5.5].

Additionally, several publications have been published during the recent years that address the research challenges identified for this vertical. This list includes both publications by CYBERSEC4EUROPE partners and by other researchers.

Some research challenges have been identified in this demonstrator as follows:

1. Mechanisms for preserving user data privacy
2. Trustworthiness on the data exchange platform
3. Accomplish regulation during the data sharing process
4. Data exchange platform user experience

Several publications have been published during the recent years for addressing these challenges. Some of them are provided next considering the current state of the art and the trends and challenges to cover. This list includes both publications by CYBERSEC4EUROPE partners and by other researchers.

### Challenge 1: Mechanisms for preserving user data privacy

The DANS, FE2MED and PLEAK applied in the MD-UC1 or MD-UC2 [D5.5] address this challenge. In particular DANS and FE2MED enablers are focused on preserve user privacy and PLEAK shows the privacy leaks during the data exchange process. Other works are proposing methods, schemes and technologies such as blockchain or SMPC for increasing the efficiency, security and preserving privacy on medical data sharing.

References:

* Zhuang, Yan, Lincoln R. Sheets, Yin-Wu Chen, Zon-Yin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. "A patient-centric health information exchange framework using blockchain technology." IEEE journal of biomedical and health informatics 24, no. 8 (2020): 2169-2176. DOI: 10.1109/JBHI.2020.2993072.
* Abdellatif, Alaa Awad, Lutfi Samara, Amr Mohamed, Aiman Erbad, Carla Fabiana Chiasserini, Mohsen Guizani, Mark Dennis O’Connor, and James Laughton. "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange." IEEE Internet of Things Journal 8, no. 21 (2021): 15762-15775. DOI: 10.1109/JIOT.2021.3052910.
* Akkaoui, Raifa, Xiaojun Hei, and Wenqing Cheng. "EdgeMediChain: a hybrid edge blockchain-based framework for health data exchange." IEEE access 8 (2020): 113467-113486. DOI: 10.1109/ACCESS.2020.3003575.
* Fadheel, Wesam, Raed Salih, and Leszek Lilien. "PHeDHA: Protecting healthcare data in health information exchanges with active data bundles." In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1187-1195. IEEE, 2018. DOI: 10.1109/TrustCom/BigDataSE.2018.00164.
* Jin, Hao, Yan Luo, Peilong Li, and Jomol Mathew. "A review of secure and privacy-preserving medical data sharing." IEEE Access 7 (2019): 61656-61669. DOI: 10.1109/ACCESS.2019.2916503.
* Gilad-Bachrach, Ran, Kim Laine, Kristin Lauter, Peter Rindal, and Mike Rosulek. "Secure data exchange: A marketplace in the cloud." In Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, pp. 117-128. 2019. DOI: 10.1145/3338466.3358924
* Peng, Cong, Debiao He, Jianhua Chen, Neeraj Kumar, and Muhammad Khurram Khan. "EPRT: an efficient privacy-preserving medical service recommendation and trust discovery scheme for eHealth system." ACM Transactions on Internet Technology (TOIT) 21, no. 3 (2021): 1-24. DOI: 10.1145/3397678
* Shen, Nelson, Therese Bernier, Lydia Sequeira, John Strauss, Michelle Pannor Silver, Abigail Carter-Langford, and David Wiljer. "Understanding the patient privacy perspective on health information exchange: a systematic review." International journal of medical informatics 125 (2019): 1-12. DOI: 10.1016/j.ijmedinf.2019.01.014.
* Li, Tiantian, Wei Ren, Yuexin Xiang, Xianghan Zheng, Tianqing Zhu, Kim-Kwang Raymond Choo, and Gautam Srivastava. "FAPS: A fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, Ether cheque and smart contracts." Information Sciences 544 (2021): 469-484. DOI: 10.1016/j.ins.2020.08.116.
* Soni, Mukesh, and Dileep Kumar Singh. "Blockchain-based security & privacy for biomedical and healthcare information exchange systems." Materials Today: Proceedings (2021). DOI: 10.1016/j.matpr.2021.02.094.
* Esmaeilzadeh, Pouyan. "The effect of the privacy policy of Health Information Exchange (HIE) on patients’ information disclosure intention." Computers & Security 95 (2020): 101819. DOI: 10.1016/j.cose.2020.101819.
* Lawrenz, Sebastian, Priyanka Sharma, and Andreas Rausch. "Blockchain technology as an approach for data marketplaces." In Proceedings of the 2019 International Conference on Blockchain Technology, pp. 55-59. 2019. DOI: 10.1145/3320154.3320165
* Munoz-Arcentales, Andres, Sonsoles López-Pernas, Alejandro Pozo, Álvaro Alonso, Joaquín Salvachúa, and Gabriel Huecas. "An architecture for providing data usage and access control in data sharing ecosystems." Procedia Computer Science 160 (2019): 590-597.
* Agahari, Wirawan, Riccardo Dolci, and G. A. de Reuver. "Business model implications of privacy-preserving technologies in data marketplaces: The case of multi-party computation." In 29th European Conference on Information Systems (ECIS 2021) A Virtual AIS Conference: Human Values Crisis in a Digitizing World, pp. 1-16. Association of the Information Systems (AIS), 2021.
* Cunha, Mariana, Ricardo Mendes, and João P. Vilela. "A survey of privacy-preserving mechanisms for heterogeneous data types." Computer science review 41 (2021): 100403. DOI: 10.1016/j.cosrev.2021.100403
* Zalonis, Jasmin, Frederik Armknecht, Björn Grohmann, and Manuel Koch. "Report: State of the Art Solutions for Privacy Preserving Machine Learning in the Medical Context." arXiv preprint arXiv:2201.11406 (2022). DOI: 10.48550/arXiv.2201.11406

### Challenge 2: Trustworthiness on the data exchange platform

All the assets involved in this vertical contribute to the trustworthiness of DEP by the users, in terms of improving the user data privacy, the regulatory compliance and usability experience. The following works propose architecture design, models and technologies increasing the trustworthiness of health data exchange platforms, by using analytic tools, blockchain or smart contracts.

References:

* Malamas, Vangelis, Panayiotis Kotzanikolaou, Thomas K. Dasaklis, and Mike Burmester. "A hierarchical multi blockchain for fine grained access to medical data." Ieee Access 8 (2020): 134393-134412. DOI: 10.1109/ACCESS.2020.3011201.
* Khan, Azam, and Ashiq Anjum. "Blockchain-based distributed platform for accountable medical data sharing." In Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion, pp. 1-8. 2021. DOI: 10.1145/3492323.3503506
* Celik, Z. Berkay, Abbas Acar, Hidayet Aksu, Ryan Sheatsley, Patrick McDaniel, and A. Selcuk Uluagac. "Curie: Policy-based secure data exchange." In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, pp. 121-132. 2019. DOI: 10.1145/3292006.3300042
* Koscina, Mirko, David Manset, Claudia Negri-Ribalta, and Octavio Perez. "Enabling trust in healthcare data exchange with a federated blockchain-based architecture." In IEEE/WIC/ACM International Conference on Web Intelligence-Companion Volume, pp. 231-237. 2019. DOI: 10.1145/3358695.3360897
* Hernandez, Julio, Lucy McKenna, and Rob Brennan. "TIKD: A trusted integrated knowledge dataspace for sensitive healthcare data sharing." In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1855-1860. IEEE, 2021. DOI: 10.1109/COMPSAC51774.2021.00280.
* Alarcon, Mauro Lemus, Minh Nguyen, Saptarshi Debroy, Naga Ramya Bhamidipati, Prasad Calyam, and Abu Mosa. "Trust Model for Efficient Honest Broker based Healthcare Data Access and Processing." In 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 201-206. IEEE, 2021. DOI: 10.1109/PerComWorkshops51409.2021.9430954.
* Esmaeilzadeh, Pouyan. "The impacts of the privacy policy on individual trust in health information exchanges (HIEs)." Internet Research (2020). Vol. 30 No. 3, pp. 811-843. DOI: 10.1108/INTR-01-2019-0003
* Moutselos, Konstantinos, Dimosthenis Kyriazis, Vasiliki Diamantopoulou, and Ilias Maglogiannis. "Trustworthy data processing for health analytics tasks." In 2018 IEEE International Conference on Big Data (Big Data), pp. 3774-3779. IEEE, 2018. DOI: 10.1109/BigData.2018.8622449.
* Sheehan, Mark, Phoebe Friesen, Adrian Balmer, Corina Cheeks, Sara Davidson, James Devereux, Douglas Findlay, Katharine Keats-Rohan, Rob Lawrence, and Kamran Shafiq. "Trust, trustworthiness and sharing patient data for research." Journal of medical ethics 47, no. 12 (2021): e26-e26. DOI: 10.1136/medethics-2019-106048.
* Graham, Mackenzie. "Data for sale: trust, confidence and sharing health data with commercial companies." Journal of Medical Ethics (2021). DOI: 10.1136/medethics-2021-107464

### Challenge 3: Accomplish regulation during the data sharing process

The GDPR guidelines tool is addressing this challenge providing methods and practices for fulfilling current European regulation. The use of assets such as DANS, FE2MED, SS-PP-IdM and PLEAK facilitates the compliance of the regulation. The next works presents how to address issues related to regulatory frameworks when health information is shared.

References:

* Kim, Dae-young, Lavanya Elluri, and Karuna P. Joshi. "Trusted Compliance Enforcement Framework for Sharing Health Big Data." In 2021 IEEE International Conference on Big Data (Big Data), pp. 4715-4724. IEEE, 2021. DOI: 10.1109/BigData52589.2021.9671834.
* Molnar-Gabor, Fruzsina, Julian Sellner, Sophia Pagil, Santa Slokenberga, Olga Tzortzatou, and Katarina Nyström. "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: insights from Germany, Greece, Latvia and Sweden." In Seminars in Cancer Biology. Academic Press, 2021. DOI: 10.1016/j.semcancer.2021.12.001.
* Vlahou, Antonia, Dara Hallinan, Rolf Apweiler, Angel Argiles, Joachim Beige, Ariela Benigni, Rainer Bischoff et al. "Data sharing under the general data protection regulation: time to harmonize law and research ethics?" Hypertension 77, no. 4 (2021): 1029-1035. DOI: 10.1161/HYPERTENSIONAHA.120.16340
* Graef, Inge, and Jens Prüfer. "Governance of data sharing: A law & economics proposal." Research Policy 50, no. 9 (2021): 104330. DOI: 10.1016/j.respol.2021.104330;
* Martens, Bertin, Alexandre De Streel, Inge Graef, Thomas Tombal, and Néstor Duch-Brown. "Business-to-Business data sharing: An economic and legal analysis." EU Science Hub (2020).

### Challenge 4: Data exchange platform user experience

The visualization tool specifically addresses this challenge. It allows the data provider and data consumer to visualize the data and metadata included in the data catalogue and the quality of these data. Other works exploring the use of techniques for presenting data (data visualization) improving the UX and the usability, boosting the willingness of users to exchange health data.

References:

* Wang, Pengwen, and Jiangru Wang. "Research on the Application of Data Visualization in the UI interface Design of Health Apps." In 2021 International Wireless Communications and Mobile Computing (IWCMC), pp. 2013-2019. IEEE, 2021. DOI: 10.1109/IWCMC51323.2021.9498648.
* Bitkina, Olga Vl, Hyun K. Kim, and Jaehyun Park. "Usability and user experience of medical devices: An overview of the current state, analysis methodologies, and future challenges." International Journal of Industrial Ergonomics 76 (2020): 102932. DOI: 10.1016/j.ergon.2020.102932.
* Esmaeilzadeh, Pouyan, and Tala Mirzaei. "Comparison of consumers’ perspectives on different health information exchange (HIE) mechanisms: an experimental study." International Journal of Medical Informatics 119 (2018): 1-7. DOI: 10.1016/j.ijmedinf.2018.08.007.
* Abbas, Antragama Ewa, Wirawan Agahari, Montijn van de Ven, Anneke Zuiderwijk, and Mark de Reuver. "Business data sharing through data marketplaces: a systematic literature review." Journal of Theoretical and Applied Electronic Commerce Research 16, no. 7 (2021): 3321-3339. DOI: 10.3390/jtaer16070180
* Distler, Verena, Carine Lallemand, and Vincent Koenig. "How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs." Computers in Human Behavior 106 (2020): 106227. DOI: 10.1016/j.chb.2019.106227
* Sibenik, Goran, and Iva Kovacic. "Assessment of model-based data exchange between architectural design and structural analysis." Journal of Building Engineering 32 (2020): 101589. DOI: 10.1016/j.jobe.2020.101589

Recently, the Medical Data Exchange demonstrator presented on Privacy Symposium[[12]](#footnote-13), held in Venice, the main results of the demonstrator focused on the work on anonymisation (DANS) and functional encryption (FE2MED) tools for preserving health data privacy and securing data.

As a summary of the health community progress, the progress made in the health and medical information exchange during the last years has been focused on the creation of a trusted, secure and privacy-preserving environment for sharing sensitive data between different stakeholders. Efforts for promoting the preservation of user data privacy, developing data privacy-preserving techniques, implementation of current regulations and improving the user experience, has been made to this end. Also, the creation of a European health data space[[13]](#footnote-14) in the context of the European data strategy.

## Progress Made in Smart Cities

There are several Cybersec4Europe’s assets/frameworks that contribute to tackling challenges related to the Smart Cities vertical. The identified assets are mainly developed within the WP3 and WP5 work packages and demonstrated by Cybersec4Europe, that support securing the Smart Cities considering several aspects.

More precisely, 11 (eleven) assets have been developed within WP3 and described in both deliverable D3.1 [D3.1] and D3.11 [D3.11], and they are listed below. Note that the description of the assets has been taken from both the above deliverables and from WP3 corresponding GitHub entry[[14]](#footnote-15) that contains details of online proof-of-concept demonstrators, repositories, videos and other dissemination material related to the assets..

1. ARGUS is a broker (ARGUS) that acts as a proxy to the existing public cloud infrastructures by performing all the necessary authentication, cryptography, and erasure coding. ARGUS uses erasure code to provide efficient redundancy (opposite to standard replication) while adding an extra layer to data protection in which data is broken into fragments, expanded, and encoded with redundant data pieces that are stored across a set of different storage providers (public or private). The key characteristics of ARGUS are confidentiality, integrity and availability of data stored in public cloud systems. (D3.11, Section 5.9)
2. Briareos Modular Framework for Elastic Intrusion Detection and Prevention and it has been extended with integration of the honeypot feature. (D3.1, Section 5.3)
3. DANS: The main aim of the Data Anonymization Service (DANS) tool is data protection, namely preserving personal data privacy. Considering regulatory aspects anonymized data are excluded from GDPR regulation because anonymized data is no longer “personal data”. In this way, the DANS asset is an anonymization tool that avoids user tracking and user re-identification by the use of privacy and risk models which prevents privacy threats when data are managed. As perfect anonymization is not possible it is necessary to balance between privacy and data accuracy for analytics. (D3.1, Section 5.1)
4. eiDASBrowser is an Android application implementing a browser that transparently integrates eIDAS authentication via NFC using Spanish ID card (DNIe). (D3.1, Section 5.1)
5. GENERAL\_D (Gdpr ENforcEment of peRsonAL Data) is an asset for supporting the integrated GDPR-based process development life cycle for the specification, deployment, and testing of adequate fine-grained authorization mechanisms able to consider legal requirements.

GENERAL\_D has the following objectives:   OBJ 1: defining a GDPR-based Life Cycle for authorization systems. That means defining a specific and integrated process development life cycle for the specification, deployment, and testing of adequate fine-grained authorization mechanisms, by considering legal requirements. OBJ 2: providing an integrated environment for automatically enforcing the data protection or privacy regulations. Indeed, we define an integrated environment where we combine some of the available solutions for specifying the privacy requirements, controlling personal data, processing them, and demonstrating compliance with the GDPR in collecting, using, storing, disclosing, and disposing of the personal data GENERAL\_D Life cycle. For more information, please refer to GENERAL\_D repository: https://generald-dataprotection.github.io/(D3.1, Section 5.1)

1. Mobile p-ABC is an open-source privacy-preserving Attribute Based Credential (p-ABC) system for Android, based on the Idemix Anonymous Credential System and the ABC4Trust implementation. It supports minimal disclosure of personal information through zero knowledge crypto proofs, allowing users holding their smartphone to present those proofs against Identity Providers. (D3.1, Section 5.1)
2. PLEAK is an analysis tool for the privacy audit of an existing system and the design of new privacy-aware systems. PLEAK allows modelling business processes using the Business Process Model Notation (BPMN) and privacy-preserving algorithms using the SecreC privacy-preserving programming language. PLEAK can then analyse the data flows using cryptographic privacy and differential privacy. PLEAK also supports the inclusion of Privacy Enhancing Technologies (PETs) in the business process models to reduce the leakage of private information. (D3.1, Section 5.2)
3. SS-PP-IdM uses OLYMPUS virtual identity provider, which is comprised of multiple individual IdPs, to manage user identities and authentication. It relies on distributed p-ABCs to offer privacy- preserving (minimal disclosure and unlinkability) and authentication (presentation of attributes) linked to eIDAS. Moreover, the asset proposes a trust framework based on Blockchain to complement the usage of credentials. (D3.1, Section 5.1)
4. PTASC PTASC presents a decentralized, secure device-to-device communications solution in which device provisioning is focused on improving usability while providing security by default. The solution focuses on using a PKI where the CA is represented by a manager device that can be switched on/off to reduce single point of failure (SPOF) problems. The solution combines public-key cryptography and symmetric keys with the One Time Password (OTP) concept using a secure token. Device identity is guaranteed by physical access to this physical token. (D3.11, Section 5.8)
5. SPeIDI aims at integrating online services with eIDAS infrastructure to European eID use. This connectivity eIDAS-based solution is intended to provide a hub or proxy service between the private SP domain and the European country eIDAS nodes. for secure accessing to the e-services using the eID issued by any European country. Based on the building blocks provided by CEF following the eIDAS technical specifications, including signing, encryption and the SAML 2.0 standard. SP connection is based on a simple API based on JWT. SPeIDI is under EUPL license (D3.1, Section 5.1)
6. Threat Intelligence Integrator is an asset able to correlate static and real-time information (e.g.,  
   Indicators of Compromise), associated to the monitored infrastructure, with cybersecurity related  
   data coming from external OSINT sources, through a heuristic analysis process, enriching it with an indicator of relevance, accuracy and actionability, called threat score. Furthermore, the component can also share the enriched information with external trusted entities, in an automated way, relying on the open-source Malware Information Sharing Platform (MISP) (D3.1, Section 5.3)

The additional 3 (three) assets/frameworks have been developed within WP5 and described in deliverable D5.2:

1. CaPe is a “consent based” and open-source platform with the goal to manage and control “personal data” during the interaction among data subjects and public and private services as Data Controller and processors (PA, Social, IoT, B2C). It provides tools for lawful data sharing processes, with the ability to grant and withdraw consent to third parties for accessing own personal data. It follows the MyData principles to exploit the potential of personal data, facilitates its control and new business opportunities in compliance with the GDPR. (D5.2, Section 8.2.3.2 [D5.2])
2. RATING aims to support organisations to assess evidence-based cyber-risk profiles. Following ISO31000, RATING supports Organisations to identify major cybersecurity risks for their business and main assets. Using this asset, Service Providers can conduct an entire cyber risk assessment, based on holistic approaches, involving both Financial and Cybersecurity boards to understand the relationships between cyber-attacks and intangible capital at risk; (D5.2, Section 8.2.3.2)
3. TO4SEE aims at measuring the susceptibility of the employees against Social Engineering attacks based on simulating a phishing campaign. Such tool can perform a real phishing attack regulated by several security and privacy by design principles. According to privacy regulations policies, the results of the assessment are aggregated and anonymized, so that it is possible for CISO to get informed of the most critical “target-groups” prone to human-based vulnerabilities. (D5.2, Section 8.2.3.2)

In the following sub-sections, for each challenge the progress made by the project are described in terms of enhancement of the assets and a list of references are provided when available.

### Challenge 1: Trusted Digital Platform

During the project we worked on the integration of eIDAS authentication, privacy-preserving Attribute-Based Credentials and Distributed ledger technologies (DLTs) for a trustworthy and privacy-respecting authentication and authorization framework.

A good example of successful study on digital platform is the one of Indonesia, where the research investigated the factors that affect the seeking and sharing of information on the smart city digital platforms.

More generally, the academic world has been discussing deeply on this topic and a useful research agenda was issued on 2018 by de Reuver, Sørensen and Basole where the authors suggest to researcher to “*seek to*

1. *advance conceptual clarity by providing clear definitions that specify the unit of analysis, degree of digitality and the sociotechnical nature of digital platforms;*
2. *define the proper scoping of digital platform concepts by studying platforms on different architectural levels and in different industry settings; and*
3. *advance methodological rigour by employing embedded case studies, longitudinal studies, design research, data-driven modelling and visualisation techniques*”

Another interesting paper (Cooper and Martin) describes an open architecture for digital rights management (DRM) enforcement on trusted computing platforms that empowers the consumer to select their operating-system and applications, including open-source options, without weakening the strength of the security functions.

Speaking of the SC’s Cyber-Physical Systems (CPS), an interesting study suggests adding intelligent agents in CPS in order to have new social characteristics, morals, and ethics to enhance the smart city’s performance and produce less biased decisions in a more trusted environment. Thus, the paper describes how smart city problems could be solved by considering both technical aspects and social features to potentiate the smart city’s performance.

References:

* De Reuver, Mark, Carsten Sørensen, and Rahul C. Basole. "The digital platform: a research agenda." Journal of information technology 33, no. 2 (2018): 124-135. DOI: 10.1057/s41265-016-0033-3
* Cooper, Andrew, and Andrew Martin. "Towards an open, trusted digital rights management platform." In Proceedings of the ACM workshop on Digital rights management, pp. 79-88. 2006. DOI: 10.1145/1179509.1179525
* Kusumastuti, Ratih Dyah, N. Nurmala, Juliana Rouli, and Herdis Herdiansyah. "Analyzing the factors that influence the seeking and sharing of information on the smart city digital platform: Empirical evidence from Indonesia." Technology in Society 68 (2022): 101876. DOI: 10.1016/j.techsoc.2022.101876.
* Ponce, Pedro, Juana Isabel Méndez, Adán Medina, Omar Mata, Alan Meier, Therese Peffer, and Arturo Molina. "Smart Cities Using Social Cyber-Physical Systems Driven by Education." In 2021 IEEE European Technology and Engineering Management Summit (E-TEMS), pp. 155-160. IEEE, 2021. DOI: 10.1109/E-TEMS51171.2021.9524889

### Challenge 2: Cyber threat intelligence and analysis platform:

About Challenge 2, the asset have been improved with integration of Malware Information Sharing Platform (MISP) accessed through an implemented reverse proxy and controlled by the SC infrastructure. The MISP retrieves cyber-threat information from compromised situations, and a privacy-preserving module applies anonymization techniques to protect sensitive data, following the guidelines of a privacy policy. Finally, the processed Cyber Threat Intelligence (CTI) events will be shared with further MISP instances participating in the CYBERSEC4EUROPE project. Furthermore, a Federated Learning infrastructure will be deployed and the resulting machine learning models will be also shared as CTI events.

References:

* Fernández, P., Martínez, J. F., Marín, A., Bernal, J., Skarmeta, A. (2022, April 5-7). Privacy-preserving Cyber Threat Intelligence Sharing for enhanced intrusion detection in the Financial Sector [Conference Presentation]. Privacy Symposium, Venice, Italy[[15]](#footnote-16).
* Campos, Enrique Mármol, Pablo Fernández Saura, Aurora González-Vidal, José L. Hernández-Ramos, Jorge Bernal Bernabe, Gianmarco Baldini, and Antonio Skarmeta. "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges." Computer Networks (2021): 108661.
* Zibak, Adam, Clemens Sauerwein, and Andrew Simpson. "A success model for cyber threat intelligence management platforms." Computers & Security 111 (2021): 102466.
* Al-Taleb, Najla, Nazar Abbas Saqib, and Sujata Dash. "Cyber threat intelligence for secure smart city." arXiv preprint arXiv:2007.13233 (2020).

### Challenge 3: Cyber competence and awareness program

For addressing Challenge 3, we made a double-round assessment of SC employees’ awareness of social engineering threats through the SDVA tool, and an organisational cyber risk assessment with an evaluation of risk affecting tangible and intangible assets. This for giving to GEN a clear view of its cyber posture.

In the specific context of SC, an interesting paper describes a digital smart citizenship competence development with a cyber-physical learning approach supported by internet of things technologies. The proposed approach exploits the potential of Internet of Things technologies to create authentic blended and augmented learning experiences.

References:

* Atif, Yacine, Stylianos Sergis, and Demetrios Sampson. "Digital smart citizenship competence development with a cyber-physical learning approach Supported by Internet of Things technologies." In Digital Technologies: Sustainable Innovations for Improving Teaching and Learning, pp. 277-300. Springer, Cham, 2018. DOI: 10.1007/978-3-319-73417-0\_16
* Langner, Gregor, Florian Skopik, Steven Furnell, and Gerald Quirchmayr. "A Tailored Model for Cyber Security Education Utilizing a Cyber Range." In ICISSP, pp. 365-377. 2022.
* Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. "Cyber security awareness, knowledge and behavior: a comparative study." Journal of Computer Information Systems 62, no. 1 (2022): 82-97.

### Challenge 4: Privacy by design

The work for addressing Challenge 4 was multiple and described by the following points:

* integration of PP-IdM for the achievement of privacy by design in the authentication and authorization modules of SCs.
* CaPe solution’ evaluation taking into account the privacy improvement after its integration in SC’s service. Multiple deployment and integration approaches have been developed to support the different legacy systems from SC's systems. Evolution on aspects related to UX and interaction with national ID schemes.
* GENERAL\_D is being enhancing with GDPR-based testing tools for assessing the GDPR compliance of systems managing personal data. More precisely, GENERAL\_D integrates the following testing tools:
  + - GROOT (GdpR-based cOmbinatOrial Testing) is a generic combinatorial testing methodology, supported by a tool, specifically conceived for assessing the GDPR compliance and its contextualization in the context of access control domain.
    - GRADUATION (GdpR-bAseD mUtATION) is a GDPR-Based Mutation Methodology supported by a tool for:
      1. analyzing and managing model-based specifications of legal text (such as the GDPR), so as to extract main concepts and useful data;
      2. selecting and applying a set of mutation operators to a specific GDPR-based model instance, so as to derive its mutated versions.

References:

* Daoudagh, Said, and Eda Marchetti. "The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities." In ICISSP, pp. 571-578. 2022. DOI: 10.5220/0010912300003120
* Daoudagh, Said, and Eda Marchetti. "GROOT: A GDPR-Based Combinatorial Testing Approach." In IFIP International Conference on Testing Software and Systems, pp. 210-217. Springer, Cham, 2022. DOI: 10.1007/978-3-031-04673-5\_17
* Daoudagh, Said, and Eda Marchetti. "GRADUATION: a GDPR-based mutation methodology." In International Conference on the Quality of Information and Communications Technology, pp. 311-324. Springer, Cham, 2021. DOI: 10.1007/978-3-030-85347-1\_23
* Daoudagh, Said. "The GDPR Compliance through Access Control Systems." (2021).
* Daoudagh, Said, Eda Marchetti, Vincenzo Savarino, Jorge Bernal Bernabe, Jesús García-Rodríguez, Rafael Torres Moreno, Juan Antonio Martinez, and Antonio F. Skarmeta. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal." Sensors 21, no. 21 (2021): 7154. DOI: 10.3390/s21217154

### Challenge 5: Cyber response and resilience

Here the two asset to respond to the Challenge 5 are listed and described with their evolution and benefits:

* Briareos solution was extended with integration of the honeypot feature.
* RATING tool gave to the SC’s CISO a detailed view about the cyber-risk posture of Genoa municipality.

A complete literature review on this field is available in references. It identifies peer-reviewed literature and investigates empirical primary studies that address cyber resilience and digital forensic incident response (DFIR) aspects of cyber–physical systems (CPSs) in smart cities. It also provides scientific evidence of the gaps in the literature for possible future directions for research within the CPS cybersecurity realm, paving the way for the research community for future and unaddressed research topics.

References:

* Ahmadi-Assalemi, Gabriela, Haider Al-Khateeb, Gregory Epiphaniou, and Carsten Maple. "Cyber resilience and incident response in smart cities: A systematic literature review." Smart Cities 3, no. 3 (2020): 894-927. DOI: 10.3390/smartcities3030046
* Benedik, Robert, and Haider Al-Khateeb. "Digital Citizens in a Smart City: The Impact and Security Challenges of IoT on citizen’s Data Privacy." In Challenges in the IoT and Smart Environments, pp. 93-122. Springer, Cham, 2021
* Hammad, Eman, and Abdallah Farraj. "Risk‐Aware Cyber‐Physical Control for Resilient Smart Cities." Cyberphysical Smart Cities Infrastructures: Optimal Operation and Intelligent Decision Making (2022): 95-122

### Challenge 6: End user trusted data management

Here the three assets to respond to the Challenge 6 are listed and described with their evolution and benefits:

* CaPe evaluation and related evolution will contribute on future version of Minimal Interoperability Mechanisms (MIM) plus[[16]](#footnote-17) specifications.
* PTASC and ARGUS evaluation including new modules from the assets. In the PTASC, now users can block specific domains using a middleware implementation on a router. In the context of ARGUS, users can use searchable encryption techniques to store metadata locally.
* GENERAL\_D will be integrated with facilities that make the conceived GDPR-based access control system auditable by the end users. Therefore, that feature will enhance the trust of the systems using GENERAL\_D for managing, protecting and ruling access to personal data.

Outside CYBERSEC4EUROPE project, it is worth to be mentioned the SMARTIE project, where it has been developed a framework to enable end-to-end security and trust in information delivery for decision-making purposes, following the data owner's privacy requirements, allowing highly scalable and secure information for smart city applications.

References:

* Bohli, Jens-Matthias, Antonio Skarmeta, M. Victoria Moreno, Dan García, and Peter Langendörfer. "SMARTIE project: Secure IoT data management for smart cities." In 2015 International Conference on Recent Advances in Internet of Things (RIoT), pp. 1-6. IEEE, 2015. DOI: 10.1109/RIOT.2015.7104906
* Daoudagh, Said. "The GDPR Compliance through Access Control Systems." (2021)
* Daoudagh, Said, and Eda Marchetti. "The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities." In *ICISSP*, pp. 571-578. 2022. DOI: 10.5220/0010912300003120

### Challenge 7: Interoperability between legacy and new systems

For CaPe tool, multiple deployment and integration approaches have been developed to support the different legacy systems from SC's systems.

Concerning GENERAL\_D asset, it has been conceived for integrating and enhancing existing systems with functionalities that enable the GDPR compliance through authorization systems (i.e., access control). Decoupling the business logic and authorization, and using standardized access control systems and model, enable both interoperability and integrability between legacy and emerging systems. Indeed, thanks to its modularity, GENERAL\_D can be customized for offering specific and suitable functionalities such as specification, design and testing and assessment of the GDPR compliance.

References:

* Hernandez-Ramos, Jose L., Juan A. Martinez, Vincenzo Savarino, Marco Angelini, Vincenzo Napolitano, Antonio F. Skarmeta, and Gianmarco Baldini. "Security and privacy in Internet of Things-enabled smart cities: Challenges and future directions." IEEE Security & Privacy 19, no. 1 (2020): 12-23. DOI: 10.1109/MSEC.2020.3012353
* Daoudagh, Said, Eda Marchetti, Vincenzo Savarino, Roberto Di Bernardo, and Marco Alessi. "How to Improve the GDPR Compliance through Consent Management and Access Control." In ICISSP, pp. 534-541. 2021. DOI: 10.5220/0010260205340541
* Daoudagh, Said. "The GDPR Compliance through Access Control Systems." (2021)

### Challenge 8: Cyber fault/failure detection and prevention

For Challenge 8, RATING, among other recommendations, provides CISO with prevention countermeasures for attack strategies that exploit cyber failure as well.

From the outside, the IoT field is the one riskier for SCs at the moment. They are designed and constructed by using advanced techniques which consist of sensors, electronics, and networks. It is crucial to understand (1) vulnerabilities in wireless sensors and techniques to avoid them, (2) emerging wireless standards for sensors, and (3) what role these standards will play in the future.

References:

* Alshambri, Hind, Mohammed A. AlZain, Ben Soh, Mehedi Masud, and Jehad Al-Amri. "Cybersecurity attacks on wireless sensor networks in smart cities: an exposition." INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH 8, no. 1 (2020).
* Ali, Nazakat, and Jang-Eui Hong. "Failure detection and prevention for cyber-physical systems using ontology-based knowledge base." Computers 7, no. 4 (2018): 68.
* Cioroaica, Emilia, Said Daoudagh, and Eda Marchetti. "Predictive Simulation for Building Trust Within Service-Based Ecosystems." In 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 34-37. IEEE, 2022. DOI: 10.1109/PerComWorkshops53856.2022.9767457.

### Challenge 9: Logging and monitoring

About Challenge 9, project has no asset to address it. Outside, there were many studies on this field. One is about cloud infrastructure, often used for offering SC services. It says that current cloud infrastructures do not offer customers, and in the case of Smart Cities to citizens, the monitoring of the underlying physical infrastructure; with the monitoring information, the service provider could create the necessary audit logs for compliance monitoring. The article proposes a collaboration between the cloud infrastructure provider and the service provider: the first one monitors virtual machines on behalf of the second and makes infrastructure-level monitoring information available to it. Very interesting approach.

A CyberSec4Europe’s partner, namely CNR, involved in an ongoing European project[[17]](#footnote-18), is developing and conceiving solutions for monitoring and auditing to build trust within System of Systems (SoS) and Ecosystems by considering both security and privacy concerns.

References:

* Massonet, Philippe, Syed Naqvi, Christophe Ponsard, Joseph Latanicki, Benny Rochwerger, and Massimo Villari. "A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures." In 2011 IEEE international symposium on parallel and distributed processing workshops and PhD forum, pp. 1510-1517. IEEE, 2011. DOI: 10.1109/IPDPS.2011.304.
* Calabrò, Antonello, Said Daoudagh, and Eda Marchetti. "MENTORS: Monitoring Environment for System of Systems." In WEBIST, pp. 291-298. 2021. DOI: 10.5220/0010658900003058
* Calabrò, Antonello, Emilia Cioroaica, Said Daoudagh, and Eda Marchetti. "BIECO Runtime Auditing Framework." In Computational Intelligence in Security for Information Systems Conference, pp. 181-191. Springer, Cham, 2021. DOI: 10.1007/978-3-030-87872-6\_18

### Challenge 10: Information security and operational security

Neither about Challenge 10 the project has specifics assets. Nevertheless, the main studies on this field for SC regard the blockchain. This is one of the most promising technologies for securely manage information. Despite this, the literature is still divided among pros and cons.

References:

* Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." Symmetry 12, no. 8 (2020): 1328. DOI: 10.3390/sym12081328
* Khanna, Abhirup, Anushree Sah, Vadim Bolshev, Michal Jasinski, Alexander Vinogradov, Zbigniew Leonowicz, and Marek Jasiński. "Blockchain: Future of e-governance in smart cities." Sustainability 13, no. 21 (2021): 11840.
* Al-Taleb, Najla, Nazar Abbas Saqib, and Sujata Dash. "Cyber threat intelligence for secure smart city." arXiv preprint arXiv:2007.13233 (2020).

# Summary Conclusions

The CyberSec4Europe project has created a Roadmap for Research and Development in the area of cyber security. The Roadmap focuses on research directions relevant to the several vertical areas of the project: (1) Open Banking, (2) Supply chain security assurance, (3) Privacy-Preserving Identity Management, (4) Incident Reporting, (5) Maritime Transport, (6) Medical Data Exchange, and (7) Smart Cities.

This deliverable focuses on evaluating the Roadmap. The evaluation is being done along three dimensions:

* **Completeness**. That is, are the research challenges proposed enough to address the work needed to be done in each vertical? Do we need to propose more research challenges?
* **Usefulness**. That is, have other projects and organisations used some of this work? Have these organisations used parts of the CyberSec4Europe Roadmap in their own work?
* **Progress Made**. That is, has the community made any progress towards addressing the challenges of the Roadmap? The community involves (i) the partners of the project and (ii) organisations outside the project who work to address the same challenges.

To evaluate the completeness of the research challenges identified we created a questionnaire which was distributed to the community and received more than 80 responses.

Our main findings include:

* More than 90% of the responders believed that the research challenges identified adequately cover the work that needs to be done in order to address the cybersecurity issues of the verticals. The percentage is even higher (reaches almost 95%) for the responders who work in industry.
* Around 5% of the responders had interesting suggestions for research challenges that could be added to the proposed ones.
* Parts of the project’s roadmap have been used in the roadmaps (or similar documents) of other organisations as well including Cyberwatching.eu: the European observatory of research and innovation in the field of cybersecurity and privacy.

Based on the above we can safely conclude that the roadmapping work has been useful and effective. However, roadmapping is not an one-time thing: it is a continuous process. We hope that we (the CyberSec4Europe partners along with its broader constituency) will be able to continue this roadmapping work in the near future and help the research community build a more resilient digital Europe.

# References

[D3.1] Antonio Skarmeta, “CyberSec4Europe D3.1: Common Framework Handbook 1”, 2019

[D3.2] S. Krenn, “CyberSec4Europe D3.2: Cross Sectoral Cybersecurity Building Blocks”, 2020.

[D3.3] Davy Preuveneers, “CyberSec4Europe D3.3: Research challenges and requirements to manage digital evidence”, 2020.

[D3.6] Boštjan Kežmah, “CyberSec4Europe D3.6: Guidelines for GDPR Compliant User Experience”, 2020.

[D3.11] Alessandro Sforzin, “CyberSec4Europe D3.11: Definition of Privacy by Design and Privacy Preserving Enablers”, 2020.

[D3.12] A. Hita and A. Skarmeta, “CyberSec4Europe D3.12: Common Framework Handbook 2”, 2021.

[D3.13] João Resende (Editor) “CyberSec4Euope D3.13: Updated version of enablers and components”, 2022.

[D3.14] Massimo Guarascio and Giuseppe Manco, “CyberSec4Europe D3.14: Cooperation with Threat Intelligence Services for deploying adaptive honeypots”, 2021

[D3.15] J. Resende, “CyberSec4Europe D3.15: Proactive approaches for secure software development”, 2021.

[D3.17] Célia Martinie, “CyberSec4Europe D3.17: Integration To Demonstration Cases”, 2021.

[D3.21] Liliana Pasquale and Alzubair Hassan, “CyberSec4Europe D3.21: Framework To Design And Implement Adaptive Security Systems”, 2022.

[D3. 6] B. Kežmah “CyberSec4Europe D3.6: Guidelines for GDPR Compliant User Experience”, 2020.

[D4.5] E. Markatos “CyberSec4Europe D4.5: Research and Development Roadmap III”, 2022.

[D5.2] A. Sforzin “CyberSec4Europe D5.2: Specification and Set-up Demonstration case Phase 1”, 2020.

[D5.4] A. Sforzin “CyberSec4Europe D5.4: Requirements Analysis of Demonstration Cases Phase 2”, 2021.

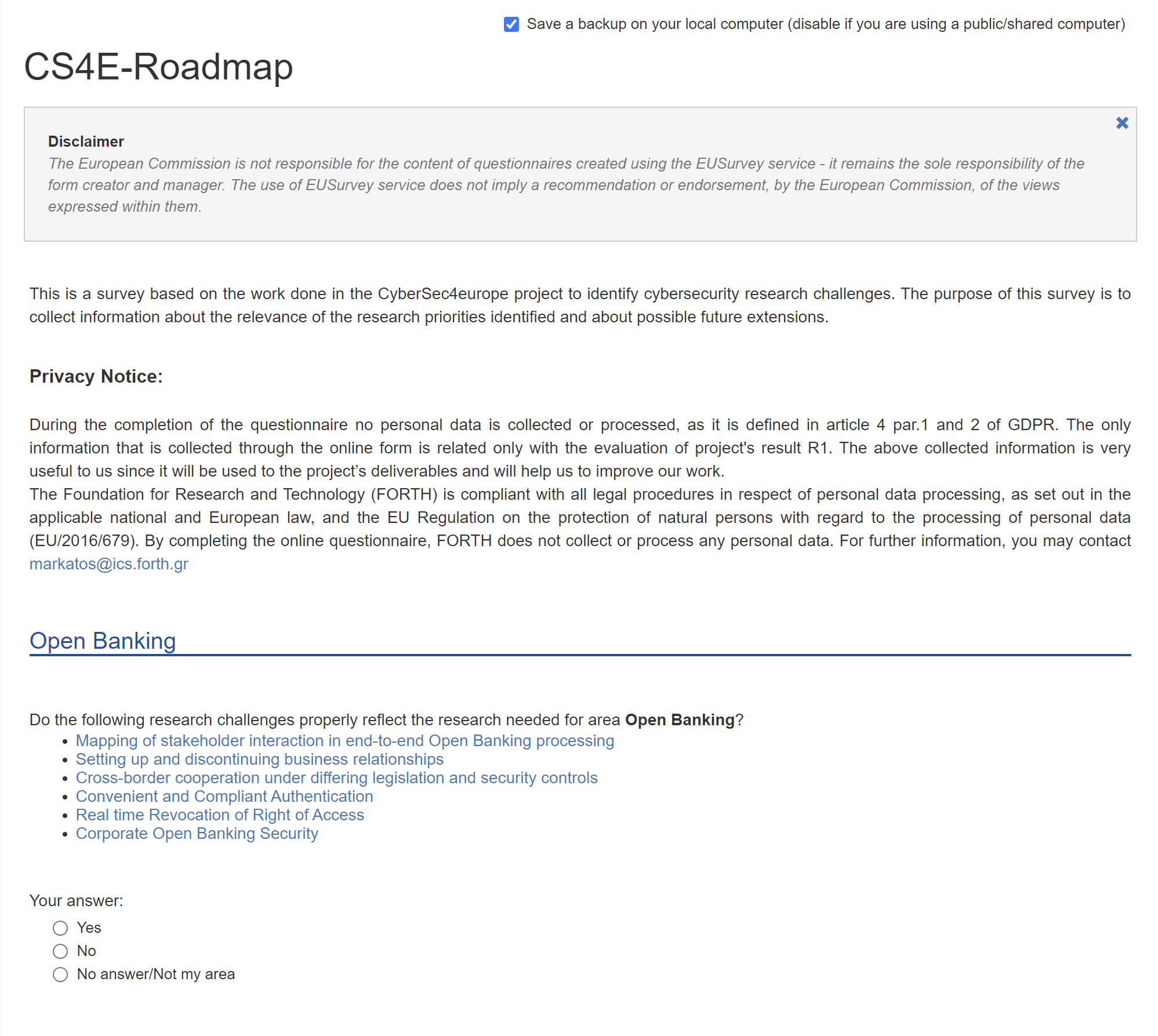
[D5.5] A. Sforzin, “CyberSec4Europe D5.5: Specification and set-up Demonstration case Phase 2” 2021.

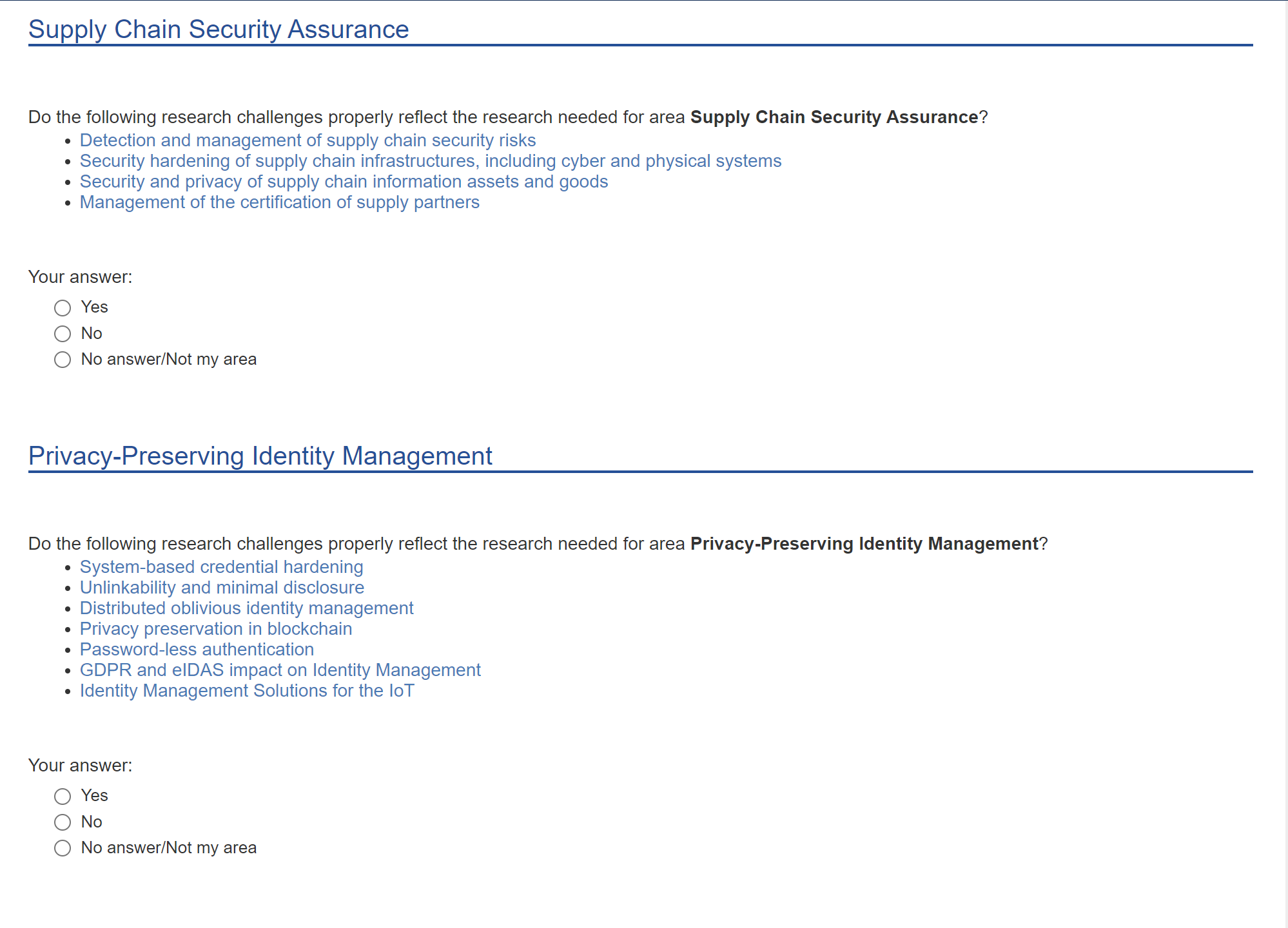
[ISO/IEC 27551] ISO/IEC 27551:2021 Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication

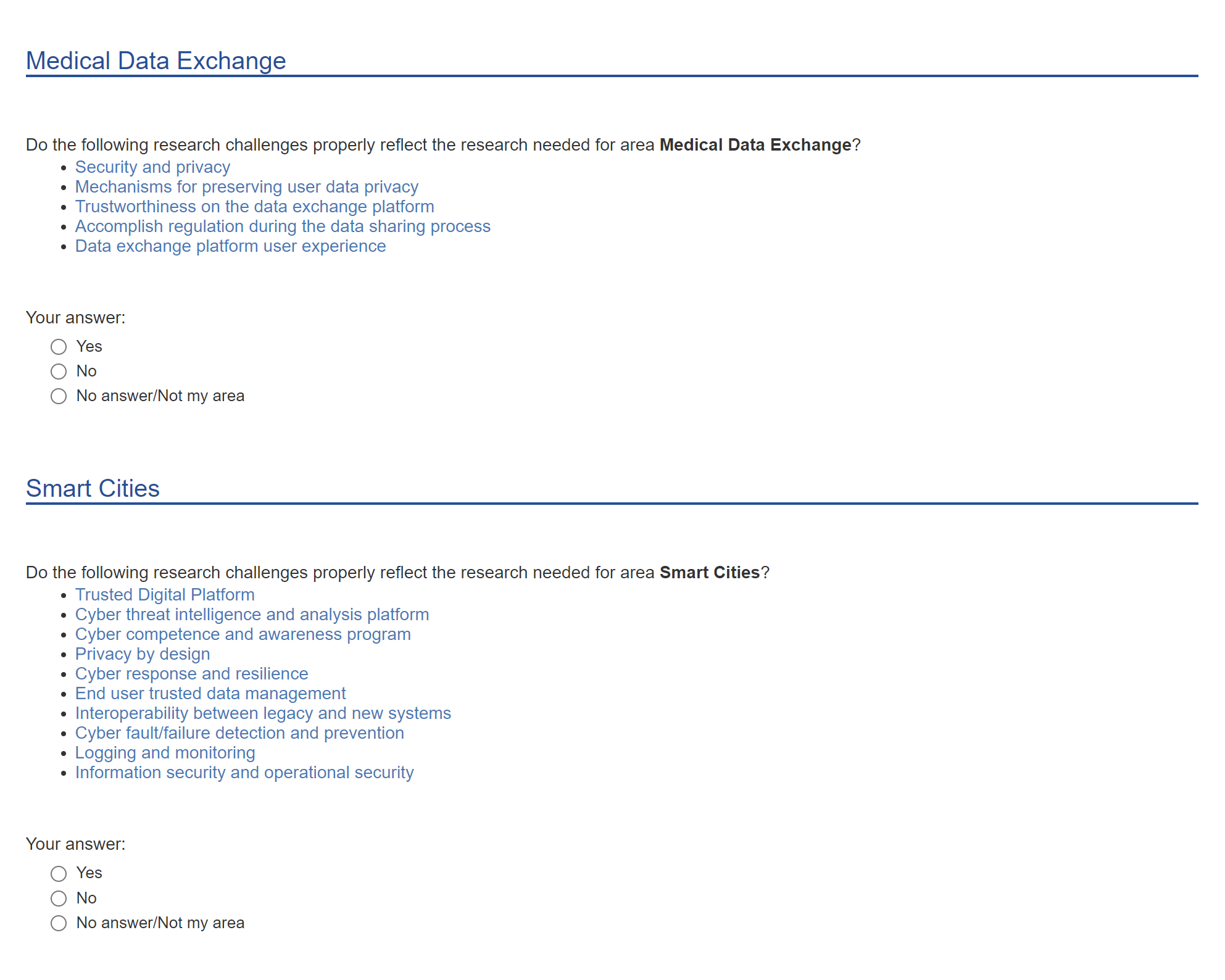
[ISO/IEC 23264-1] ISO/IEC 23264-1:2021 Information security — Redaction of authentic data — Part 1: General

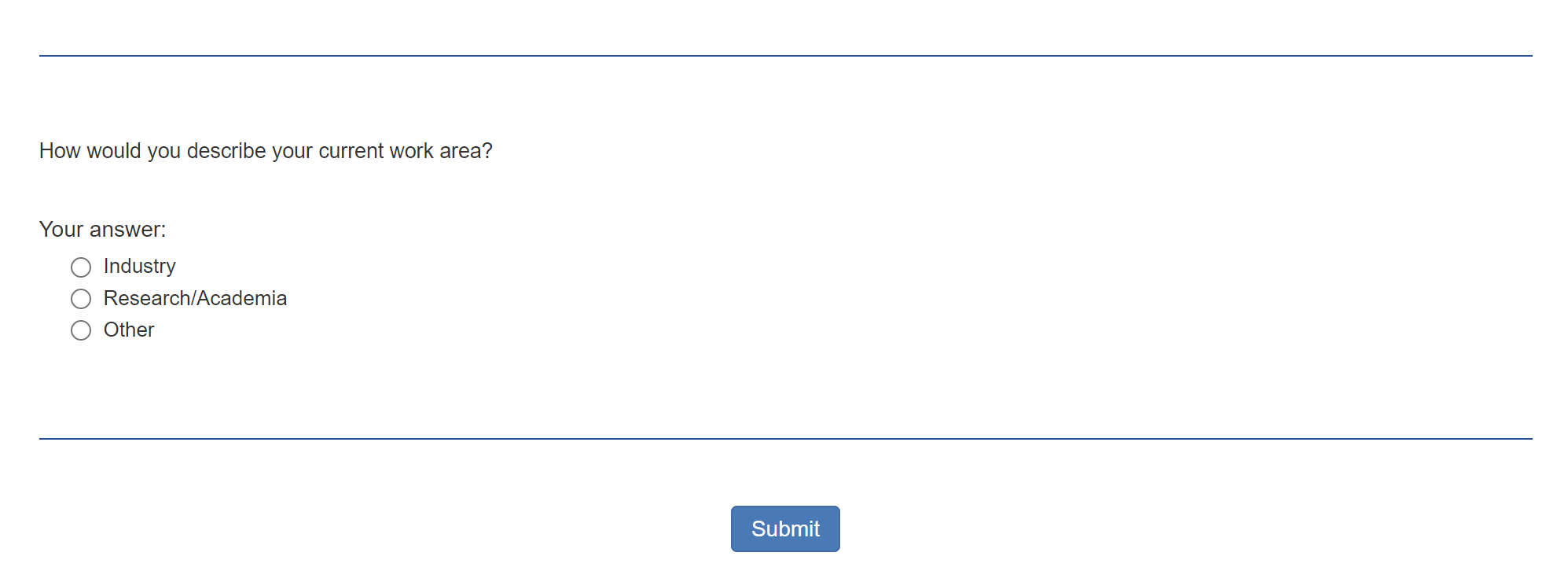
[ISO/IEC 20009-3] ISO/IEC 20009-3:2022 Information security — Anonymous entity authentication — Part 3: Mechanisms based on blind signatures

# Annex A: Questionnaire

In the following pages we list the questionnaire that we circulated: 







1. The full text of the questionnaire can be found at the end of this document in Annex A. [↑](#footnote-ref-2)
2. The text in the recommendations of the responders is taken “verbatim” from their responses. It was not changed or rephrased in any way. [↑](#footnote-ref-3)
3. https://www.investopedia.com/terms/s/stablecoin.asp [↑](#footnote-ref-4)
4. https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp [↑](#footnote-ref-5)
5. Authorised push payment  [↑](#footnote-ref-6)
6. https://github.com/cadirneca/judas [↑](#footnote-ref-7)
7. <https://www.enisa.europa.eu/news/enisa-news/exploring-research-directions-in-cybersecurity> [↑](#footnote-ref-8)
8. Srinivas, Sampath, John Kemp, and F. I. D. O. Alliance. "FIDO UAF architectural overview." (2013).

   Srinivas, Sampath, Dirk Balfanz, Eric Tiffany, Alexi Czeskis, and Fido Alliance. "Universal 2nd factor (U2F) overview." FIDO Alliance Proposed Standard 15 (2015). [↑](#footnote-ref-9)
9. Haböck, Ulrich, and Stephan Krenn. "Breaking and fixing anonymous credentials for the cloud." In *International Conference on Cryptology and Network Security*, pp. 249-269. Springer, Cham, 2019 [↑](#footnote-ref-10)
10. https://thehive-project.org/ [↑](#footnote-ref-11)
11. https://pleak.io/wiki/pleak [↑](#footnote-ref-12)
12. https://privacysymposium.org/programme/ [↑](#footnote-ref-13)
13. <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en> [↑](#footnote-ref-14)
14. The WP3, task T3.2 GitHub entry is available at: https://github.com/cs4ewp3/wp3/tree/main/3.2 [↑](#footnote-ref-15)
15. <https://privacysymposium.org/> [↑](#footnote-ref-16)
16. <https://living-in.eu/group/7/commitments/mims-plus-version-4-final> [↑](#footnote-ref-17)
17. CNR is leading work package WP5 of the EU H2020 BIECO project GA No. 952702. The CNR is developing an auditing solution that combines Monitoring and Digital Twins. More information of the BIECO can be found at: https://www.bieco.org/ [↑](#footnote-ref-18)