Recommendations on aligning research programme with policy

Recommendations in the specialised area of NIS

NOVEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Authors would like to thank Dr. George Leventakis for his input and feedback during the drafting of this report.

ISBN 978-92-9204-208-0, DOI 10.2824/323039

Table of Contents

Executive Summary 5

1. Introduction 6

1.1 Scope and Objectives 7

1.2 Overview of Research, Innovation and Policy Support Programmes 7

1.3 Evaluation Criteria 9

1.3.1 Effectiveness 9
1.3.2 Coherence 9
1.3.3 Relevance 9
1.3.4 EU added value 9
1.3.5 Impacts 9

2. Impact Assessment Pillars 10

2.1 Cryptography 10

2.1.1 European Network of Excellence in Cryptology (Phase II) – Ecrypt II 10
2.1.2 Computer Aided Cryptography Engineering – CACE 11
2.1.3 Secure, Embedded Platform with advanced Process Isolation & Anonymity Capabilities – SEPIA 12
2.1.4 Trusted Revocable Biometric Identities – TURBINE 12

2.2 Identity Management 13

2.2.1 Secure Identity Across Borders Linked – STORK 13
2.2.2 Authentication and Authorisation for Entrusted Unions – AU2EU 14
2.2.3 Shaping the Future of Electronic Identity – FutureID 15
2.2.4 Trusted Architecture for Securely Shared Services - TAS3 15
2.2.5 Secure Widespread Identities for Federated Telecommunications - SWIFT 16

2.3 Privacy Enhancing Technologies 17

2.3.1 Attribute-Based Credentials for Trust – ABC4Trust 17
2.3.2 Privacy and identity management for community services - PICOS 18
2.3.3 Privacy and Identity Management in Europe for Life – PrimeLife 18
2.3.4 Context-aware data-centric information sharing – CONSEQUENCE 19
2.3.5 Privacy-aware Secure Monitoring - PRISM 20

2.4 Threat Detection and Mitigation 21

2.4.1 Worldwide Observatory of Malicious Behaviors and Attack Threats – WOMBAT 21
2.4.2 Nippon-European Cyberdefense-Oriented Multilayer threat Analysis – NECOMA 22
2.4.3 Securing Websites through Malware Detection and Attack Prevention Technologies – SWEPT 23

2.5 Critical Infrastructure Protection 24

2.5.1 A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World – SysSec 24

2.5.2 Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures – MICIE 24
2.5.3 Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security – TREsPASS 25

2.6 Trustworthy Digital Services 26
2.6.1 Network of Excellence on Engineering Secure Future Internet Software Services and Systems – NESSoS 26
2.6.2 Secure Provision and Consumption in the Internet of Services – SPaCIoS 27
2.6.3 Policy and Security Configuration Management – PoSecCo 28
2.6.4 Holistic Approaches for Integrity of ICT-Systems – HINT 29

2.7 Cloud Computing Security 30
2.7.1 TRustworthy Embedded systems for Secure Cloud Computing Applications – TRESCCA 30
2.7.2 Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure – TCLOUDS 30
2.7.3 Privacy-Preserving Computation in the Cloud – PRACTICE 31
2.7.4 Confidential and Compliant Clouds – Coco Cloud 32
2.7.5 Secure Provisioning of Cloud Services based on SLA management – SPECS 33

3. Main achievements and Recommendations for the way ahead 34

3.1 Main Achievements 34

3.2 The way ahead 35

4. Future Work Programme Recommendations 40

Executive Summary

The EU Cybersecurity Strategy[1] includes a number of measures aimed to promote a Single Market for cybersecurity products together with fostering research and development investments and innovation. The development of a Digital Single Market is also the main objective of the Digital Agenda (currently Digital Single Market strategy[2]), one pillar being strengthening online trust and security, on which the growth of the European economy and the development of a strong digital business sector depend. The Digital Agenda sees internet trust and security as vital to a vibrant digital society and considers a high level of network and information security across the EU essential to ensure consumer confidence and to keep the online economy running. Although there is state-of-the-art research in Europe in the field of NIS, and this area is extensively supported by European funded programs, research is usually not focused on the aspects where NIS policies need available technologies to move forward on their implementation.

The scope of this report is to review existing analysis reports on EU funded Trust and Security Projects, summarize achievements that have significantly promoted specific pillars of NIS, identify and summarize specific outcomes that can promote and support emerging policy and legislative initiatives, namely eIDAS, GDPR, support industry policy in cybersecurity, and provide recommendations on the formulation of forthcoming work programmes. For the analysis of the selected projects, through their reports, six assessment pillars were identified, based on the ICT & Trust and Security interrelated thematic areas and emerging policy and legislative initiatives aspects. For each project, achievements that can significantly promote/favour specific pillars of NIS, are identified along with specific outcomes that can favour and support emerging policy and legislative initiatives - notably: eIDAS, GDPR, NIS and industry policy in cybersecurity, including the cybersecurity cPPP.

Even given the limited subset of projects reviewed within the scope of this report, notable achievements and innovative approaches are identified. Particular note should also be taken of the promotion of horizontal aspects such as usability, standardization, societal acceptance, economic viability and legal compliance of the research results. Furthermore, several projects have been particularly successful in shortening the gap from research to innovation and thus promoting the establishment of a vibrant market in secure and trustworthy ICT in Europe. The analysis however indicated that there is still a large number of unresolved cybersecurity, privacy and trust issues (areas of the main legislative initiatives that are not covered) which necessitate further research across all ICT technology, components, applications and services.

The recommendations for the forthcoming research and innovation work programmes of H2020 and cybersecurity cPPP can be summarized as follows:

- Sustain close collaboration with all relevant stakeholders on research and innovation topics while supporting key EU policy initiatives;
- Promote market-oriented innovation and direct transferability of outcomes to products or services;
- Introduce horizontal requirements for new information and transparency models and endorse the adoption of by design and by default paradigms.

[1] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[2] https://ec.europa.eu/digital-single-market/en/europe-2020-strategy

1. Introduction

The Europe 2020 strategy[3] for smart, sustainable and inclusive growth identifies research as a driver for innovation, economic growth and sustainability. Through different framework programmes, EU funded research projects promote and support state-of-the-art research in Europe. The specialized field of Network and Information Security (NIS) is extensively supported by European-funded programmes, but is not always focused on the aspects where emerging policy and legislative initiatives need available technologies to move forward on their implementation. Within the scope of this report, the following policy and legislative initiatives have been considered and are briefly presented below.

The EU Cybersecurity Strategy[4] includes a number of measures aimed to promote a Single Market for cybersecurity products together with fostering research and development investments and innovation. The development of a Digital Single Market is also the main objective of the Commission's Digital Agenda, one pillar being strengthening online trust and security, on which the growth of the European economy and the development of a strong digital business sector depend. The Digital Agenda and the Digital Single Market Strategy[5], perceive trust and security in digital services vital for a vibrant digital society and consider a high level of network and information security across the EU essential to ensure consumer confidence and to keep the online economy running.

The Network and Information Security (NIS) Directive, adopted by the EU Council on 17 May 2016[6], aims to put in place the necessary mechanisms at national and EU level to improve security levels and respond to cyber threats. The aim is to have a secure and trustworthy digital environment throughout the EU. This should include improving Member States' national cybersecurity capabilities, improving Member States cooperation and improving cooperation between public and private sectors.

The Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[7] adopted on 23 July 2014 is a milestone to provide a stable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It lays down the foundations for people, companies (in particular SMEs) and public administrations to access safely cross border electronic services and seamlesly perform electronic transactions.

The General Data Protection Regulation (GDPR), which entered into force on 24 May 2016 and shall apply from 25 May 2018.[8], aims to achieve a comprehensive reform of data protection rules in the EU. The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market.

---

[3] http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf
[4] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192
[6] http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and
[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
[8] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

1.1 Scope and Objectives

This work is undertaken under ENISA Work Programme 2016, as part of Work Package 1.3. - Research & Development, Innovation under the Strategic Objective 1 - To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS). The overall scope is to improve coordination and facilitate support in policy areas that rely on a technological base. The objectives of this report are to:

- Review findings from existing reports on the achievements of a subset of the ICT Trust & Security research projects, funded under the 7th Framework Programme, that have exceeded expectations and have been characterized as success stories;
- Summarize achievements from the aforementioned projects that have significantly promoted specific pillars of Network and Information Security (NIS);
- Identify and summarize specific outcomes that can promote emerging policy and legislative initiatives, such as the eIDAS Regulation and the General Data Protection Regulation, stimulate trust across different stakeholders and support industry policy in cybersecurity, including the cybersecurity contractual Public Private Partnership;
- Provide recommendations on promoting research approaches that can move forward Network and Information Security (NIS) at EU level;

It should be noted however that the overall aim of this report is not to supplement the role of reviewers of the projects, nor the relevant review meetings and procedures. ENISA did not analyse the deliverables of the projects but only information from publicly available reports.

1.2 Overview of Research, Innovation and Policy Support Programmes

The 7th Framework Programme for Research and Technological Development (FP7) was the EU's main instrument for funding research in Europe from 2007 to 2013. The total budget for this seven years period was € 50.5 billion which marked the priority of Europe in research, innovation and technological development. It consisted of 4 main blocks of activities forming 4 specific programmes, namely co-operation, ideas, people and capacities, plus a fifth specific programme on nuclear research. Information and Communication Technologies (ICTs) research activities were part of the co-operation programme and the total budget was € 9.1 billion. As mentioned in the 2014 Digital Agenda Scoreboard[9], ICT was the largest research area in the FP7 Cooperation programme. The FP7 ICT worked on the approach of implementing strategic roadmaps, but also kept an open part for emerging ideas. Under both approaches, the EU has co-funded over the period 2007-2013 2,261 projects for a total Union funding of about €7.6 billion. In parallel the CIP ICT Policy Support Programme has allocated € 593.2 million of EU funding over the period 2008 – 2013, distributed to 233 different projects. The ICT PSP (Policy Support Programme) was one of specific programmes within the CIP (Competitiveness and Innovation framework Programme). Projects that acted within this programme are funded to support the realization of the Digital agenda for Europe. More specifically, the programme addressed issues and challenges related to effective exploitation of innovative, IT products and services.

[9] https://ec.europa.eu/digital-single-market/en/news/scoreboard-2014-overview-participation-fp7-and-cip-programmes-ict-domain

In absolute terms Germany, United Kingdom, Italy, France and Spain accounted for 60% of total EU funding and 57% of participations. Cyprus, Greece, Slovenia, Austria and Belgium are the 5 Member States with the highest amounts of funding compared to the size of their ICT sector. According to the latest analysis of publications and patents of ICT research in FP7[10], funded projects were particularly effective in strengthening scientific excellence as well; they have generated over 170,000 publications, have led to more than 1,700 patents and 7,400 commercial exploitations of products or services.

In the specific ICT research area of Trust and Security the overall focus was towards "*developing knowledge and technologies for building an open, secure and trustworthy information society in Europe, where citizens and organisations can fully reap the benefits from the new technologies*". Towards this direction, a number of interrelated thematic areas[11] were promoted and are briefly depicted below.

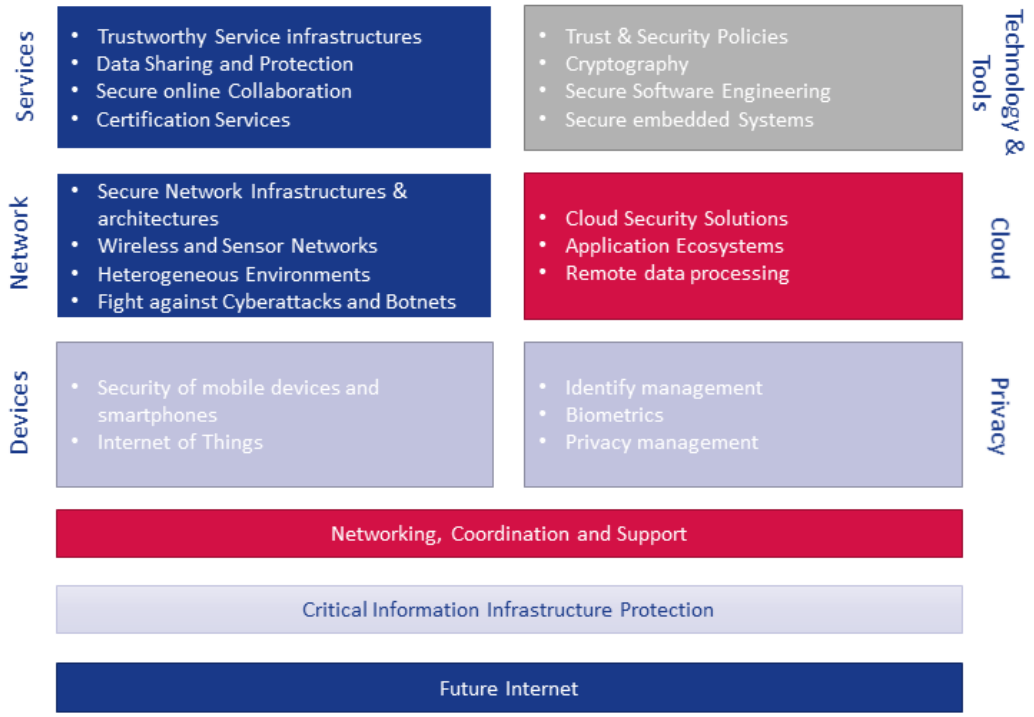

Figure 1: Main thematic areas of FP7 ICT Trust & Security[8]

A very high percentage of the EC funding in FP7 was received by organizations that have already participated in FP6. This holds especially true for universities and research organizations, where a comparably small number of organizations managed to build up the qualifications and capacities for

[10] http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14504
[11] http://cordis.europa.eu/fp7/ict/security/projects_en.html

continuing to be key players in European-funded research. FP7 can therefore be considered as having balanced the need for openness and concentration central to global competition.

1.3 Evaluation Criteria

The evaluation criteria used to review findings and summarize achievements of EU Funded research projects were inspired by the Better Regulation "Toolbox"[12], and in particular Tool # 42: Identifying the evaluation criteria and Questions. According to the Toolbox "*All evaluations must assess the evaluation criteria of effectiveness, efficiency, coherence, relevance and EU added value*" and "*Evaluations ... should also always assess the economic, social and environmental impacts* ...". Based on these indications, five (5) evaluation criteria were defined and are briefly described in the following subsections.

1.3.1 Effectiveness

Effectiveness analysis considers how successful the project has been in achieving or progressing towards its objectives. The evaluation aims at forming an opinion on the progress made. The analysis also tries to identify if any unexpected or unintended effects have occurred.

1.3.2 Coherence

The evaluation of coherence involves looking at a how well or not different actions work together. Checking "internal" coherence means looking at how the various internal components of the project operate together to achieve its objectives. Similar checks can be conducted in relation to other ("external") interventions at different levels, for example with respect to projects in related areas and EU interventions within the same policy field or in areas which may have to work together.

1.3.3 Relevance

Relevance looks at the relationship between the needs and problems in society and the objectives of the project. For example, incorrect assumptions may have been made about the cause and effect relationships or circumstances may have changed and the current needs/problems may not be the same as the ones looked at when the project was proposed.

1.3.4 EU added value

EU-added value looks for changes which it can reasonably be argued are due to EU scope, rather than any other factors. Under the principle of subsidiarity (Article 5 Treaty on European Union), the EU should only act when the objectives can be better achieved by Union action rather than by potentially varying action by Member States.

1.3.5 Impacts

Evaluations should also always assess the economic, social and environmental impacts of EU-funded projects, with – in this specific context - particular emphasis on those impacts that are relevant for the creation of a Digital Single Market[13].

[12] http://ec.europa.eu/smart-regulation/guidelines/toc_tool_en.htm
[13] http://ec.europa.eu/priorities/digital-single-market_en

2. Impact Assessment Pillars

Impact Assessment is also part of the Better Regulation "Toolbox" and provides support to the political decision-making process. It pertains gathering and analysing evidence to support policy making, verifying, identifying and assessing whether EU action is needed and analysing the advantages and disadvantages of available solutions. Within the scope of this report six assessment pillars were identified, based on the ICT & Trust and Security interrelated thematic areas and emerging policy and legislative initiatives aspects. Namely these pillars are i) Cryptography, ii) Identity Management, iii) Privacy Enhancing Technologies, iv) Threat Detection And Mitigation, v)Critical Infrastructure Protection and vi) Trustworthy Digital Services. For each project, achievements that can significantly promote/favour specific pillars of NIS, are identified along to specific outcomes that can favour and support emerging policy and legislative initiatives - notably: eIDAS, GDPR, NIS and industry policy in cybersecurity, including the cybersecurity cPPP. The assessment of each project is a result of an analysis from existing (and publicly available) reports. It is worth emphasizing that the project list is by no means exhaustive, i.e. many other projects funded within the context of the same calls, that have also exceeded expectations and could thus be characterized as success stories, have not been included in this deliverable, due to lack of room and of time (as well as of – possibly – public information).

2.1 Cryptography

2.1.1 European Network of Excellence in Cryptology (Phase II) – Ecrypt II

ECRYPT's objective was to promote the collaboration of European researchers in information security, and especially in cryptology and digital watermarking. ECRYPT listed five core research areas, termed "virtual laboratories": symmetric key algorithms (STVL), public key algorithms (AZTEC), protocol (PROVILAB), secure and efficient implementations (VAMPIRE) and watermarking (WAVILA). Its continuation, ECRYPT II, was a Network of Excellence in the area of cryptology aiming towards durable integration of European research in both academia and industry.

ECRYPT II	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2013
Effectiveness	The objectives of the project have been achieved through a wide range of dissemination, communication and awareness activities including a training program, a substantial contribution towards standardization bodies, and an active publication policy.	
Coherence	The ECRYPT II research roadmap was motivated by the changing environment and threat models in which cryptology is deployed, the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and the requirements of new applications and cryptographic implementations. The project was coherent with a number of other interventions which had similar objectives.	
Relevance	Research in Cryptology and digital watermarking is relevant, since these are fundamental enablers for secure, dependable, and trusted ICT infrastructures.	
EU added value	Ecrypt II engaged leading EU players to integrate their research capabilities within three virtual labs focusing on i) symmetric key algorithms, ii) public key algorithms and protocols, and iii) hardware and software implementation. Additionally, it had a critical mass and	

ECRYPT II	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2013
	breadth to address the key questions in these areas that could only be achieved at the European level.	
Impacts	Cryptology and digital watermarking are research areas with a high strategic impact for European industry and for the society as a whole. The intense networking activity done in Ecrypt II not only brought together industrial and public recourses but also helped stimulate cybersecurity industry by aligning the demand for advanced cryptology.	

2.1.2 Computer Aided Cryptography Engineering – CACE

CACE objective was to design, develop and deploy a toolbox that would support the specific domain of cryptographic software engineering. The main motivation was that development of hardware devices and software products is facilitated by a design flow, and a set of tools (e.g., compilers and debuggers), which automate tasks normally performed by experienced, highly skilled developers. However, in both hardware and software examples the tools are generic since they seldom provide specific support for a particular domain.

CACE	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2010
Effectiveness	Project objectives were achieved as final validated solutions enable (relatively) non-expert personnel to develop high-level cryptographic applications and business models by means of cryptography-aware high-level programming languages and compilers.	
Coherence	Cryptographic software is one of the key enabling technologies of a secure and trustworthy ICT infrastructure in Europe. Cryptographic software engineering can be a viable solution for the European software industry to cope with the ever increasing volume of requests for high-quality cryptographic software. Internally, project objectives were coherent, in that they were pursued via the development of an integrated set of tools. Externally, the overarching objective of improving the productivity of the cryptographic software industry in Europe was – and will be even more so in the years to come – entirely coherent with other actions aiming at gearing up the European ICT industry for the future challenges related to secure operation of ICT infrastructures.	
Relevance	The final solutions allow automatic analysis and transformation of cryptographic software to detect security critical implementation failures, e.g., software and hardware based side-channel attacks, when realizing low level cryptographic primitives and protocols. These objectives are still relevant, since mission critical and modern applications processing sensitive data are in need of sophisticated cryptographic techniques and cryptographic software.	
EU added value	The challenges that the project addressed affect the industry supplying cryptographic applications in all European Member States in the same manner. The tackled research challenges are not limited to regional or national boundaries. Thus, research in this area would be inefficient at a national level: limiting the scope to the academic or industrial research in a particular country would lead to a solution that is not sufficient to make the results usable and efficient for the European-wide use.	
Impacts	Development of better-quality and robust software at a much lower cost can provide a clear economic advantage to the European industry in the short term and positions it better in dealing with future roadblocks to ICT development in the longer term.	

2.1.3 Secure, Embedded Platform with advanced Process Isolation & Anonymity Capabilities – SEPIA

SEPIA focused on three topics: security enhancements of mobile platforms, cryptography and privacy protecting technologies, delta-evaluation and certification methodologies. The project researched privacy protecting mechanisms based on strong cryptography and time- and cost-efficient certification processes reducing the time from design to market. Within the scope of the project, establishing trustworthiness was seen as an asset that is to be considered right from the design phase rather than being addressed as an add-on feature.

SEPIA	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2013
Effectiveness	SEPIA through theoretical and practical research, as well as the development of proof-of-concept prototypes, managed to meet its objectives. The final SEPIA reference platform was disseminated via demonstrators and as an open platform for further research and product development.	
Coherence	Establishing trust is a multi-faceted problem, which requires assessments from independent organisations. Internally, the project was coherent, since significant progress was made with respect to objectives characterized by a common overarching goal. Externally, the SEPIA endeavour is perfectly aligned to other interventions, aiming at establishing a trustworthy ICT infrastructure in Europe.	
Relevance	The SEPIA project addressed challenges that are – and will be even more so in the future – central for the development of prominent digital markets, such as mobile devices and applications and the Internet of Things. The project tackled issues of trustworthiness, security and protection of mobile devices as key enablers for new businesses opportunities and the integration of mobile platforms.	
EU added value	The solutions that have been constructed during the project are an example where the SEPIA concerted efforts of Europe's leading researchers can be used to validate the project's results. By operating at the European level, the consortium has been able to participate in clusters of projects aiming at related or complementary goals, in order to disseminate, discuss and compare the results. The consortium was a mix of industrial and academic partners that brought together expertise and excellence from various disciplines.	
Impacts	SEPIA focused on topics that have a tremendous impact on the development of borderless and secure Digital Single Market in Europe. Mobile and embedded devices are rapidly evolving into powerful, ubiquitous personal assistants. As such, they will be involved in security-critical operations like authentication, payment, e-Banking and e-Government applications and transactions as regarded in the eIDAS regulation.	

2.1.4 Trusted Revocable Biometric Identities – TURBINE

TURBINE proposed a multi-disciplinary privacy enhancing authentication technology combining innovative developments in cryptography and fingerprint biometrics. Specific objectives of the project were to ensure that the crypto-protection deployed on the biometric data was non-invertible and had the lowest possible impact on biometric verification performance. Project results were assessed using very large fingerprint data bases held by two project partners to compare performance with and without crypto-protection.

TURBINE	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	TURBINE provided reliable biometric 1:1 verifications, multi-vendor interoperability, and system security, while addressing major issues related to privacy concerns associated to the use of biometrics for ID management. Its primary objective of rendering this innovation commercially viable was also achieved, by demonstrating that the technology is sufficiently mature for deployment as a solution to large scale eID requirements.	
Coherence	TURBINE addressed topics that were – and still are – coherent with other actions which have similar objectives. In particular, it explored: i) data protection and privacy issues and ii) requirements of key application sectors for eID management solutions. Expert groups were included in the project to advise the consortium.	
Relevance	TURBINE addressed privacy concerns regarding the use of fingerprint biometrics for ID management. Through a comprehensive verification test and demonstration environment, it evaluated how single fingerprint data of an individual may be used to generate several secure identities with different levels of trust without weakening the overall security.	
EU added value	The challenges that the project addressed affect the industry supplying cryptographic applications in all European Member States. The breadth of technical expertise necessary to undertake this project could not be assembled at the national level.	
Impacts	TURBINE addressed research issues that have a tremendous potential in terms of market opportunities as they can offer all the benefits of biometric security while mitigating or eliminating the associated risks. Additionally, the European Data Protection Supervisor (EDPS) issued a positive opinion[14] on TURBINE's approach which provides evidence that data protection concerns, as imposed by GDPR, related to the use of biometrics can be resolved.	

2.2 Identity Management

2.2.1 Secure Identity Across Borders Linked – STORK

The aim of the STORK project was to establish a European eID Interoperability Platform to enable citizens to establish new e-relations across borders, just by presenting their national eID. STORK 2.0 followed up on STORK and validated the STORK platform in additional pilots, promoting interoperability of different approaches at national and EU level.

STORK	CIP-ICT-PSP-2007.1.2 - TOWARDS PAN-EUROPEAN RECOGNITION OF ELECTRONIC IDS (EIDS)	2008 - 2011
Effectiveness	The STORK interoperable solution for electronic identity (eID) was based on a distributed architecture that paved the way towards full integration of EU e-services while taking into account specifications and infrastructures currently existing in EU Member States. The main technology outcome of STORK was the creation of a pan-European federation of electronic identities along to common rules and specifications to assist mutual recognition of eIDs.	
Coherence	The STORK project aimed to establish a European eID Interoperability Platform that allows citizens to authenticate themselves using their own national credentials in order to access	

[14] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

STORK	CIP-ICT-PSP-2007.1.2 - TOWARDS PAN-EUROPEAN RECOGNITION OF ELECTRONIC IDS (EIDS)	2008 - 2011
	cross-border services provided by national service provider. The project's main contributions and achievements are coherent with other EU interventions and objectives.	
Relevance	Interoperability across different countries has been, and is still a challenge as far as identity is concerned, because of the many issues involved (security, privacy, compliance). STORK's user centric and cross-border approaches, and its results, are valuable for the development of future projects.	
EU added value	STORK's goal was to ensure eID interoperability at European level including common specifications, a common code for an architecture and a framework for sustainable deployment across EU. STORK and STORK 2 paved the way towards the provision of a pan-European ID, since they has addressed main issues like enabling mutual recognition of eID and trust services among Member States and tangible evidence on the applicability of the eIDAS regulation.	
Impacts	STORK and STORK 2.0 had a direct impact on the adoption of the eID services across Europe through a federated and trustworthy framework for cross-border eID services and build the basis for a future widespread use of eID solutions across borders.	

2.2.2 Authentication and Authorisation for Entrusted Unions – AU2EU

AU2EU brought advanced privacy-enhancing attribute-based credentials towards the cloud to simplify deployments, e.g., by reducing or avoiding the requirement to install user-side software. The aim of the project was to implement and demonstrate in a real-life environment an integrated eAuthentication and eAuthorisation framework to enable trusted collaborations and delivery of services across different organisational/governmental jurisdictions.

AU2EU	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2015
Effectiveness	AU2EU built on existing schemes and research results, mainly ABC4Trust, and efficiently executed aligned activities defined in the Trust in Digital Life (TDL) strategic research agenda. It developed tools allowing unifying authorisation policies, attributes and claims of different security domains, and providing the advanced authorisation and platform working across organisational borders.	
Coherence	The project is coherent with basic EU interventions in the area of identity management, increasing trust, security and privacy and aims at fostering the adoption of security technologies at European level.	
Relevance	The projects advanced the technology in the fields of eAuthentication and eAuthorization providing a privacy-friendly authentication architecture and platform across organisational borders. It has developed tools allowing unifying authorisation policies, attributes and claims of different security domains, and providing the advanced authorisation platform working across organisational borders.	
EU added value	The project has successfully advanced four different domains: assurance of claims, trust indicators, policy enforcement mechanisms and processing under encryption techniques to address specific security and confidentiality requirements of large distributed infrastructures.	
Impacts	Achievements of AU2EU will have a direct impact on the promotion and deployment of the trust services as defined within the eIDAS regulation. Moreover, the eAuthentication and	

AU2EU	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2015
	eAuthorization framework support concepts as (un)Traceability, (un)Linkability from relying party to claims provider, (un)Linkability between relying parties and (non)Disclosure, which are directly related to GDPR specifically in the areas of privacy by design, privacy enhancing technologies and data subject rights.	

2.2.3 Shaping the Future of Electronic Identity – FutureID

FutureID integrated existing eID technologies and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims towards a privacy-aware and ubiquitous identity management infrastructure for Europe.

FUTUREID	ICT-2011.1.4 - TRUSTWORTHY ICT	2012 - 2015
Effectiveness	FutureID developed building blocks that can be used to provide interoperability between different identity management standards and organize an open marketplace for identity management where many service providers and identity providers can operate. End users can benefit from ubiquitously usable open source eID client, while application and service providers will be enabled to use trustworthy authentication services.	
Coherence	FutureID bridged the gap between the various existing electronic identities and promoted efforts towards the implementation of a trust infrastructure for authentication support and promoted reliable, accountable and coherent with EU initiatives deployment of electronic identity technologies.	
Relevance	FutureID can by exploited by different providers and operators, supporting the flexible development of new and possibly diverging business cases while the infrastructure is expected to provide benefits to all stakeholders involved in the eID value chain.	
EU added value	FutureID can support all stakeholders involved in the eID value chain. Users will benefit from the availability of ubiquitously usable open source eID client application and service providers will use trustworthy authentication services without the need of making large up-front investments in eID technologies or to meet legal obligations.	
Impacts	FutureID offers the technical components that together form the infrastructure necessary for online authentication and electronic signatures while considering the electronic identification and trust services requirements in the vision of providing of the infrastructure of eSignature services. Moreover, the architecture puts high emphasis on privacy protection and integrates state of the art privacy-enhancing attribute-based credentials addressing also GDPR requirements.	

2.2.4 Trusted Architecture for Securely Shared Services - TAS3

TAS3 aimed at developing and implementing an architecture with trusted services to manage and process distributed personal information. It contributed to the design of an architecture able to meet the requirements of complex and highly versatile business processes and to enabling the dynamic user-centric management of policies.

TAS3	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	TAS3 focused on the development of a Trust Policy Management architecture, where issues like trust and privacy, identity management, authentication and authorisation as well as legal and privacy issues were efficiently handled. It efficiently validated and demonstrated the applicability of the open, secure and trusted architecture that was developed for the exchange of personal information in the domains of e-Employability and e-Health.	
Coherence	TAS3 developed architecture supports dynamic user-centric management of policies, ensures end-to-end secure transmission of personal information and user-controlled attributes between heterogeneous, context dependent and continuously changing systems.	
Relevance	Empowering individuals to be in control of their personal data and supporting their lifelong re-use of personal data while preserving personal privacy and confidentiality in dynamic environments are fundamental issues for the provision of electronic services.	
EU added value	TAS3 promotes trust and confidence in electronic transactions, and indirectly addresses the requirements of the electronic identification and trust services as described in the eIDAS regulation. Moreover, the proposed notification mechanism can also be used by service providers and organizations to easily implement requirements imposed by GDPR concerning mainly on mechanisms for notification of citizens when breaches do occur. Moreover, the techniques proposed in TAS3 are directly relevant for EU cyber preparedness.	
Impacts	TAS3 participated in the development of European Trust Observatory (ETO), which aimed towards the development of trust compliance policies and procedures for Service Providers. Such “policy and procedure specifications" need to be observable and auditable and these will deliver the information to certify and build trustworthiness into the systems, services and their providers, paving the way towards GDPR implementation.	

2.2.5 Secure Widespread Identities for Federated Telecommunications - SWIFT

The SWIFT project leveraged identity technology as a key to integrate service and transport infrastructures for the benefit of users and the providers. It focused on extending identity functions and federation to the network while addressing usability and privacy concerns.

SWIFT	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2010
Effectiveness	SWIFT developed an identity framework that transforms identity as a key enabling technology for convergence between networks, services, applications and content on the technical side and between operators, service providers, micro-operators and even users as providers on the business side. It has efficiently achieved its objectives to solve identity fragmentation, by extending IdM systems for multiple services at different network layers using the same ID and bridging platforms and layers.	
Coherence	The SWIFT framework advanced traditional IdM solutions and provided an environment for an advanced management of end users identities through identity aggregation from different individual identities, anonymous services access and cross-layer authentication and authorization.	
Relevance	The SWIFT framework extended and progressed identity management solutions like identity aggregation, anonymity, cross-layer SSO, advanced access control and mobility at network level, and between devices. Regarding privacy, it supported prevention of unauthorized	

SWIFT	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2010
	parties linking different steps or actions due to identical identifiers, enforcement of privacy rules at different providers, and assurance of the user's autonomy in disclosing attributes.	
EU added value	The SWIFT project leveraged identity as a convergence layer between different players in the communication and services space, and aimed to make identity a communication end point through which service and network providers can discover the users and deliver their services. It covered a number of privacy issues and user concerns and tackled the relative regulatory issues of GDPR. Moreover, the SWIFT identity framework aimed to overcome the Identity fragmentation in EU, provide cross-layer IdM taking into account both application and network layers, support for multiple devices and provide independency from online components. These aspects consist requirements of the electronic identification and trust services architecture.	
Impacts	SWIFT leveraged digital Identities to solve mainly identity fragmentation and extended IdM systems for multiple services at different network layers. An effective IdM can have a significant impact on networks and network services providing new service delivery options and guaranteeing end users about the authenticity of the service provider.	

2.3 Privacy Enhancing Technologies

2.3.1 Attribute-Based Credentials for Trust – ABC4Trust

ABC4Trust's focus was to improve internet privacy by developing capabilities to introduce attribute-based credentials into identity management systems, allowing users to only reveal the minimum information required by the application, without giving away full identity information.

ABC4TRUST	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2015
Effectiveness	ABC4Trust successfully addressed the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABCs). The proposed architecture is able to decompose future (reference) implementations of Privacy-ABC technologies into sets of modules and specify the abstract functionality of these components in such a way that they are independent from algorithms or cryptographic components used underneath.	
Coherence	ABC4Trust is applicable to the architectures of existing widely deployed identity protocols and frameworks such as WS-*, SAML, OpenID, OAuth and X.509 and also alleviates some of their security, privacy, and scalability issues.	
Relevance	The project outcomes provide benefits in the concept of "partial identities" and the legal principle of data minimisation as included in GDPR, allowing people to control release of their data.	
EU added value	ABC4Trust facilitates the implementation of a trustworthy and at the same time privacy-protecting digital society which provides an added value in GDPR implementation. Privacy ABCs alone and together with other mature Privacy Enhancing Technologies (PETs) have a high potential to influence the ongoing development in the domain of data protection and privacy. This will influence the understanding and definition of what appropriate technical and organisational measures are adequate to ensure data protection.	

ABC4TRUST	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2015
Impacts	ABC4Trust promotes European privacy values in infrastructures and will empower individuals and communities by increasing accountability, trustworthiness of information, allowing more elaborate access control and user-centred Identity Management (IdM).	

2.3.2 Privacy and identity management for community services - PICOS

The objective of PICOS was to develop and build a state-of-the-art platform for providing the trust, privacy, and identity management aspects of social community services and applications on the Internet and in mobile communication networks.

PICOS	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	PICOS met its objective through the implementation of Sub-communities and Partial Identities concepts that allows users to reveal only selected personal information as an attribute and the Privacy Advisor tool to guide the users in aspects of their privacy and identity management. The notion of Private Rooms was also introduced enabling users to establish a personal area for managing their private information and content, enhancing their privacy by enabling them to store and selectively publish their private information to a certain set of other users.	
Coherence	The resulting platform provided a state-of-the-art community, supporting identity management system that can be used by the industrial members of PICOS creating benefits and insights in the European IT and telecommunications industry beyond the scope of the project. By involving all stakeholders on the community value chain, PICOS will strengthen integrated European privacy and trust products and Europe's competitive advantage for trust in on-line applications and services.	
Relevance	PICOS concepts and developments provide the basis for the enhancement of products and services with regards to privacy and data protection, confirming also their key role during the participation and engagement in online communities.	
EU added value	PICOS through insights on citizens' perception and understanding of privacy, achieved implementation of privacy-enhancing technologies for trustworthy, privacy-friendly community transactions addressing several areas of the GDPR.	
Impacts	The results of PICOS have an impact at different levels of community related services, by integrating privacy enhancing concepts as part of a holistic approach to improve privacy and trust in social communities.	

2.3.3 Privacy and Identity Management in Europe for Life – PrimeLife

PrimeLife's vision was to provide privacy, trust and ID management through tools such as browser plug-ins, social networks and encryption. It was built upon and extended the FP6 Project PRIME, which dealt with enabling citizens to exercise their legal rights to control personal information in online transactions. PrimeLife aimed to resolve core privacy and trust issues involving protection of privacy for web-based applications, making existing privacy enhancing technologies useable and foster the adoption of privacy enhancing technologies by providing open source components and educational materials.

PRIMELIFE	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	PrimeLife developed a number of mechanisms and open source tools for privacy and identity management that can be used as building blocks of future privacy-enabled technologies. Project results further advanced state-of-the-art in the sphere of interface usability, configurable policy languages, federation of web services, privacy-enhanced identity management enablers, and privacy-enhancing cryptography. PrimeLife has extended identity management towards transparency with a set of open source tools such as the W3C Privacy Dashboard for tracking data collection while protecting usage of personal data through encryption.	
Coherence	PrimeLife contributed to the development of a new generation of web-based applications and services, removing trust and security barriers and enabling end users to control personal information in on-line transactions.	
Relevance	The privacy-enhancing technique developed during the projects lifetime still corresponds to the needs and problems within the EU and can be used for virtual communities (social networks) and collaborative applications on the Internet.	
EU added value	In the fields of transparency in general data processing and information exchange, project tools can be re-used and extended, as the Privacy Dashboard, with the focus on emerging ICT systems and life-log of personal data within social communities.	
Impacts	By promoting aspects like user reputation, certification and granting users the ability to control their privacy, Primelife contributed to addressing EU societal challenges and obligations as imposed by GDPR.	

2.3.4 Context-aware data-centric information sharing – CONSEQUENCE

Consequence focused on the engineering of an interoperable architecture for data sharing, facilitating dynamic policy management enforcement and end-to-end data protection across multiple organizations and techniques for organisation of neutral data sharing agreements.

CONSEQUENCE	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	Consequence combined known technologies extending and combining them to achieve the required goal and delivered new research results (e.g. DSA and EPL languages). The use of the controlled natural language (CNL4DSA), the insertion of a help-on-line facility partly mitigating usability issues and a world-wide patent depict project's achieved objectives.	
Coherence	Consequence defined a generic, scalable, context-aware, secure and resilient architecture within a framework that enable dynamic management policies based on agreements that ensure end-to-end secure protection of data-centric information, addressing the increasing need for quick, dynamic and secure information sharing.	
Relevance	The proposed framework took into account not only technological, but also economic and social aspects of data exchange while promoting Data Sharing Agreements (DSA) for managing shared data among multiple participants in several specific domains and contexts and EPL languages.	

CONSEQUENCE	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
EU added value	Consequence advanced available technologies for quick, dynamic and secure information sharing in multi-organisational environments with independent IT Infrastructures addressing the emerging need for information sharing as expressed in all major EU policy interventions.	
Impacts	The integrated capability of the developed solution for converting a high level specification of security requirements into low-level enforceable policies can be exploited in several different domains, through respective customization and integration.	

2.3.5 Privacy-aware Secure Monitoring - PRISM

PRISM's aim was to devise a privacy-preserving network monitoring system with enforcement of the applicable data protection legal framework. It investigated the possibility to preserve the customers' privacy, by avoiding disclosure of raw captured data even inside the controller domain itself, while preserving the possibility of executing monitoring applications, including the possibility to detect and react to attacks and trace back abuses and having as result to improve public security.

PRISM	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2010
Effectiveness	PRISM developed a privacy-preserving network monitoring system where carefully designed data protection mechanisms can coexist with suitably adapted monitoring applications. Moreover, it addressed the challenge of out-sourcing monitoring applications without privacy concerns. A regulatory assessment was also performed based on the EuroPriSeCriteria[15] .	
Coherence	PRISM is coherent with EU interventions in the area of privacy. The interest in monitoring systems resides in their results and even if they do not introduce directly any privacy concern, their need to access a data trace does. The middleware policies ensure that the processing of data gathered through monitoring will be carried out in line with the set of rules and limitations provided by respective data protection obligation and requirements.	
Relevance	PRISM moved traffic analysis and data reduction to the edge of the measurement system where possible, and replaced general techniques with specific analysis targeted toward specific tasks. This approach allows aggressive data reduction and protection for scalability as well as privacy protection.	
EU added value	The approach undertaken managed to adapt to the regulatory requirements of functional separation between the entities accessing the gathered data and the entities controlling and managing access permissions while reducing the data that telecom operators needs to process and store.	
Impacts	PRISM can impact the way citizens perceive their network activities about being monitored and increase their trust in communication infrastructures since network monitoring applications are able to operate in a privacy-preserving manner and in accordance to the underlying legal obligations and restrictions.	

[15] https://www.european-privacy-seal.eu/EPS-en/Criteria

2.4 Threat Detection and Mitigation

2.4.1 Worldwide Observatory of Malicious Behaviors and Attack Threats – WOMBAT

WOMBAT aimed at the development of new means to address the current and future threats related to the Internet and IT services. It focused on real-time gathering of security-related raw data, with particular attention put on leveraging existing tools and exploring the development of tools dedicated to wireless (WiFi, RFID, Bluetooth) networks, threat analysis and techniques to enrich the raw secure-related data.

WOMBAT	ICT-2007.1.4 - SECURE, DEPENDABLE AND TRUSTED INFRASTRUCTURES	2008 - 2011
Effectiveness	The project reached its objectives, in particular as reported in the WOMBAT experimental reports. Root Cause Analysis framework and prototype of early warning system developed during the project have been successfully tested and applied to various WOMBAT datasets to perform intelligence analyses. Moreover, the WOMBAT Consortium provided end-users with the open-access to WOMBAT API (WAPI) - a set of API developed by the project partners to allow integrated access to different attack datasets.	
Coherence	Current EU and national initiatives prove that combating cybercrime is one of the major priorities in the security field in general. In addition, problem of the usability and accessibility of security-related information is still challenging. Therefore the goals, approach and outputs of the WOMBAT project are still coherent with the scope of the current cyber security efforts. WOMBAT scope and focus were also coherent with NIS Working Group 2 WG2 focused on information exchange and incident coordination.	
Relevance	The WOMBAT objectives were in line with expectations of potential end-users (i.e.: ISPs, CERTS, antivirus companies, security researchers, security-conscious organizations and home users) related to threat analysis. Objectives of the project were relevant to the end-user needs, and current obstacles related to sharing the security data, trade-off between safety and flexibility of access to the data, and also independency of the analyses of security threats. Moreover, the project addressed also issues related to the insufficient level of confidence of the European citizens related the cyber security and addressed the needs for raising security awareness in Europe.	
EU added value	Results of WOMBAT were a step towards obtaining more global and comprehensive view of the security-related data, thus they can contribute to supporting cyber-security experts in their decision making process for countermeasures selection. Also, the project results can foster cyber security investments in EU organisations.	
Impacts	The potential impact of WOMBAT activities can strengthen users (society, government, business) trust in the use of networks, software and e-services. Moreover, the outputs of the project have a potential to provide IT users with means to protect their digital identity and personal data, which is consistent with the current European efforts leading to adoption of the new GDPR regulation.	

2.4.2 Nippon-European Cyberdefense-Oriented Multilayer threat Analysis – NECOMA

NECOMA addressed aspects of data collection, aiming at expanding currently used data gathering mechanisms and adapting them to threat data analysis purposes. Moreover, the project aimed to analyse threat-related data including both the target and victim perspective, instead focusing only on attack mechanisms and system vulnerabilities. NECOMA aimed also at developing cyber security metrics to assess attack impact and novel cyber defence mechanisms that could be used with these metrics.

NECOMA	ICT-2013.10.1 - EU-JAPAN RESEARCH AND DEVELOPMENT COOPERATION	2013 - 2016
Effectiveness	One of the main outputs of the project was the implementation of the threat analysis platform with a set of unified interfaces for accessing heterogeneous security related information that can be used both for real as well as for non-real time analyses. The prototype of the platform allowed to monitor and analyse a number of security incidents and attack patterns across different layers (end-point layer and infrastructure layer).	
Coherence	Current EU and national initiatives prove that combating cybercrime is one of the major priorities in the security field in general. In addition, problem of the usability and accessibility of security-related information is still challenging, therefore the goals, approach and outputs of the WOMBAT project are still coherent with the scope of the current cyber security efforts. Moreover, NECOMA objectives and scope are coherent with other, previous EU initiatives funded under FP7 ICT schemes, e.g. with the WOMBAT project.	
Relevance	NECOMA contributed to the development of new approaches and instruments addressing the fight against cyber-attacks. The proposed scenarios are in line with the currently emerging threats, in particular combating botnets and malware, as well as cyber security of mobile/micro devices are the topics addressed in European and US roadmaps related to cyber security, e.g. “A Roadmap for cybersecurity research” and “The Red Book: A Roadmap for Systems Security Research”. Those threats and scope are also in line with recently published cyber threats landscape by ENISA. Moreover, the comprehensiveness of the proposed approach (including both victim and attacked infrastructure perspective analysis) is relevant to the current needs and trends.	
EU added value	As the project is funded within the EU-Japan collaboration scheme, NECOMA included project partners both from EU and Japan fostering international cooperation in the field of cyber security and promoting EU cybersecurity preparedness.	
Impacts	The NECOMA consortium intensively collaborated with the industry aiming at adoption of the project results and in order to augment the exploitation potential for consortium members. Moreover, NECOMA industrial partners are actively involved in development and providing DDoS mitigation solutions and are major European players in the area of cyber security.	

2.4.3 Securing Websites through Malware Detection and Attack Prevention Technologies – SWEPT

The SWEPT project focus was put on protection of websites against cyber-attacks, malware and on mitigation of web vulnerabilities. The main goal of the consortium was to develop a solution that will be able to minimize impact of malicious attacks on websites, maximizing their security posture with the assumption that website owners or administrators intervention is not necessary (or limited intervention is needed) to secure the website.

SWEPT	ICT CIP-PSP 2007-2013	2014 – 2017
Effectiveness	The proposed SWEPT security solution mixes two approaches, namely proactive security (website attacks prevention) and reactive security (including detection and mitigation). At the current stage of the project the consortium effectively progresses towards the defined objectives. Two business-oriented pilots are planned for year 2016: Pilot for ISP, website administrators and owners, and Pilot 2 for web designers and developers.	
Coherence	The SWEPT initiative is coherent with other initiatives in this research area. SWEPT consortium formally interacts with ACDC project (FP7) in order to maximize benefits coming from future implementation of both projects' outputs. Complementarities between SWEPT and ACDC projects have been reported in an official deliverable and enable future integration of projects results, namely SWEPT can use threat and vulnerability data from the ACDC Central Clearing House (CCH) and analogically threats and vulnerabilities detected using the SWEPT platform can feed the CCH.	
Relevance	The project approach reflects the needs for securing websites and targets the majority of actors from the Internet ecosystem, in particular website owner and administrators, web hosting providers and ISPs. Nowadays, one of the main challenging issues is the lack of resources in the majority of organisations to invest on websites security (both in terms of funding and time/human resources). In this sense, SWEPT introduces an approach that will be cost-effective, automated and easy to implement addressing this main challenge. Finally, the SWEPT outputs can be integrated and can complement 3rd party security products of web security companies.	
EU added value	The successful implementation of the SWEPT platform will bring benefits to individual website owners and administrators, and small/SME organizations with limited resources that must balance between security of their websites and cost of security investments. This could be achieved by the SWEPT approach promoting not only secure design of the websites (Security-by-Design) but also by fostering the automation of response (automated detection and threat mitigation) in case of malicious attack. The project outputs will contribute to increasing the European consumers trust in websites and web applications, including emerging markets of e-services.	
Impacts	The expected impact reaches a variety of stakeholders from the whole Internet value chain, impacting also common Internet users that can be ultimately affected by the malicious website infection. Additionally, the SWEPT project has the ambition to define and develop "de facto" standards and good practices in the context of websites protection and a model of certification that will assess the security of given website in accordance to the SWEPT security measures. Therefore, the project outputs will have potential to impact also certification/auditing standards and standardisation bodies.	

2.5 Critical Infrastructure Protection

2.5.1 A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World – SysSec

SysSec was a Network of Excellence project extending the FORWARD project and aimed at building strong synergies with industry and policy makers by advancing the field of Systems Security. Three areas were identified as the most important and crucial in securing ICT systems: malware, targeted attacks and social engineering/phishing. The project also identified the major technologies which require more investment in their security: social networks, on-line games, e-commerce, e-banking, sensors/drones, embedded systems, smart environments, legacy systems, Critical Infrastructures, mobile/wireless networks, implantable devices and cloud computing.

SYSSEC	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2014
Effectiveness	The main output of the project was the Roadmap for Systems Security Research. Moreover, SysSec consortium created and maintained a virtual centre of excellence with the goal to consolidate system security researchers across EU.	
Coherence	The project was coherent with the vision of Horizon H2020 programme, taking into account industrial and societal perspective of cyber security challenges. The SysSec threat identification and recommendations were also consistent with ENISA Threat Landscape reports published during the SysSec project. SysSec efforts was highly coherent with the activities of NIS PPP Working Groups dealing with risk management (WG1) by SysSec educational activities, with security information exchange (WG2) by identification of Future Internet vulnerabilities, and with secure ICT research and innovation through the SysSec Roadmap contribution.	
Relevance	The identified research outputs are relevant to the actual cyber security trends and the Future Internet challenges, addressing such topics as privacy preservation, big data challenges, security of smart cities and smart infrastructures (e.g. smart grids).	
EU added value	SysSec established a strong community of experts in the field of systems security with an ambition to play a noticeable role in the changing cyber security environment. Creation of a synergy between research/academia and policy makers - both through the Red Book content as well as by the SysSec community involvement –also adds value for the EU cyber security and CIP initiatives. It should be noted that Red Book includes clearly articulated research gaps, the main challenges and recommendations for future R&D actions that can be reflected in the EU interventions.	
Impacts	The main impact of the project can be expected on policy makers and research communities. In particular identification of the Grand Challenge Research Problems in the area of Systems Security is strong advice to the collaboration between RTO organisations and funding agencies in order to improve cyber security of ICT.	

2.5.2 Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures – MICIE

The MICIE project was focused on the Critical Infrastructure (CI) protection domain and resilience of CI against malicious activities and failures caused by natural phenomena. It developed and validated an alerting system, able to identify threats related to given CI component in real time and to identify dependencies of threaten CI with other critical facilities.

MICIE	ICT-SEC-2007.1.7 - INFORMATION AND COMMUNICATION TECHNOLOGIES: CRITICAL INFRASTRUCTURE PROTECTION	2008 - 2011
Effectiveness	The core of the alerting system prototype was the Prediction Tool – the central module of the early warning system. Other expected results were also achieved, namely the off-line design of CI models and the mediation gateways to collect CI-related security events with ability to describe them using common meta-data model.	
Coherence	Critical Infrastructures have to ensure the highest security levels to be able to fulfil their duty in any circumstances. Modelling and analysing them and their interdependencies are essential to discovering hidden vulnerabilities and threats.	
Relevance	The MICIE project was consistent with end-user needs related to daily operation of Critical Infrastructures and reflected in the Work Programme, namely better understanding and management of complex and interdependent interactions between different CI components, as well as systematic risk analysis and security configuration dedicated to CI. Risk analysis was also the main focus of the NIS PPP WG1 working group. The MICIE project objectives and results were consistent with and can contribute to the EU proposal of Critical Infrastructure Warning Information Network (CIWIN) that is a pillar of the European Programme for Critical Infrastructure Protection (EPCIP).	
EU added value	Based on the results of MICIE system validation, it can be concluded that MICIE solution have a potential to increase the quality of services provided with European Critical Infrastructures. Automated support for the operator that will be assisted in detecting failures, malicious attempts of attacks and appropriated countermeasures can contribute to the cost-savings and increased resilience of the EU CI networks. Contribution to the modelling of CIs and CI dependencies can also be perceived as an added value due to still immature and inadequate models currently in use.	
Impacts	Implementation of results of the MICIE can impact CI owners and operators leveraging CI resilience against disruptions. In result, this may have a positive impact of CI end-users (societal impact). Moreover, contributing to CIWIN can impact CI expert communities.	

2.5.3 Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security – TREsPASS

The TREsPASS project's main objectives are to develop tools supporting analysis and visualisation of information about security risks, and to propose possible countermeasures for them. The developed tool will identify various attack paths (their possibility and impact) and analyse which countermeasures are the most effective. The project combines technical approach (analysis of assets and protocols vulnerabilities) with social aspects.

TRESPASS	ICT-2011.1.4 - TRUSTWORTHY ICT	2012 - 2016
Effectiveness	The expected outputs of the TREsPASS project will be included in the developed framework allowing organisations to employ analytic, model-based methods in their risk management processes. This framework will allow for the iterative development of socio-technical security models and will also include tools for prediction of attacks and their prioritisation based on attack properties extracted from these models. Finally, the project will deliver a preventive tool able to calculate the effects of an attack and the most appropriate countermeasures and	

TRESPASS	ICT-2011.1.4 - TRUSTWORTHY ICT	2012 - 2016
	mitigation strategies taken into account the cost-effectiveness of those countermeasures. Up to date (close to the end of the project) it seems that objectives will be effectively achieved.	
Coherence	Since the project aims at identification and protection against security threats related to information and at improvements of existing risk management methods, it is coherent with a number of complementary EU funded R&D projects and address Risk Management Emerging Challenge (NIS PPP WG1).	
Relevance	The project addresses three case scenarios from different domains: a cloud infrastructure, a telecommunication infrastructure and remote payment system with a focus on security technologies, and the business models related to given domain.	
EU added value	By integrating European expertise on socio-technical security into a widely applicable and standardised framework, TREsPASS has the ambition to decrease the number of security incidents in Europe and support organisations and their customers to take more conscious decisions about security investments. In result, TREsPASS can contribute to the increased resilience of European businesses and to social and economic benefits.	
Impacts	The TREsPASS consortium partners include organisations from the entire value chain, both from the academia/RTO domain, as well as from SMEs and large institution, thus the consortium combines social and the technical expertise and integrates theoretical research with the cyber security practice. Therefore, TREsPASS impacts research communities and cyber security practitioners contributing to the development of cyber security and risk management tools development and their maturity.	

2.6 Trustworthy Digital Services

2.6.1 Network of Excellence on Engineering Secure Future Internet Software Services and Systems – NESSoS

NESSoS aimed at constituting and integrating a long lasting research community on engineering of secure software-based services and systems. The main assumption was to address security concerns from the beginning of design, thus incorporating security principles in the engineering processes.

NESSOS	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2014
Effectiveness	The NESSoS consortium has reached its objectives by performing community building activities and by setting up the joint virtual research lab (JVRL) for collaborative working. NESSoS project also integrated a number of security service-oriented tools into the NESSoS workbench called SDE (Service Development Environment). Moreover, NESSoS has developed an educational program for master degree related to security engineering for Future Internet services.	
Coherence	The NESSoS project was coherent with the NIS objectives, in particular with secure ICT innovation principles. Moreover, NESSoS project was consistent with other EU projects funded under the related topics, e.g. interoperability of the SPaCloS Tool with the NESSoS SDE platform was achieved. NESSoS researchers also actively contributed to the Network and Information Security Platform (NIS).	

NESSOS	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2014
Relevance	The NESSoS project and the community established and acting after the project address the need for support to networking and coordination of research aimed at improving trustworthy of the current ICT.	
EU added value	The main expected added value of NESSoS is improvement of competitiveness of EU industry in trustworthy ICT market. NESSoS contributes to the development of trustworthy European infrastructures and security of networked services and improved interoperability of these services. NESSoS provides also a support for standardisation efforts in the area of secure services development. Moreover, NESSoS network of excellence provides a necessary support in coordination and integration of research activities in Europe.	
Impacts	NESSoS aimed at re-addressing, integration, and fostering the research activities in the secure/trustworthy ICT area, and had a goal to increase and spread the expert knowledge among research communities. NESSoS and its after-project community collaborate and impact industrial stakeholders with the goal of contributing to the industrial best practices and supporting a growth of software-based service systems. Finally, NESSoS efforts supported the European competitiveness in the Future Internet area.	

2.6.2 Secure Provision and Consumption in the Internet of Services – SPaCIoS

SPaCIoS aimed to develop and combine currently used technologies for penetration testing, security testing, model validation and related automated reasoning techniques, model inference, model extraction and automatic learning and to integrate them into the SPaCIoS tool supporting secure design and development of Internet services.

SPACIOS	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2014
Effectiveness	The SPaCIoS project reached its objectives and the consortium has particularly developed: • techniques for security testing that allow security properties (e.g. confidentiality and authentication) to be testable, • vulnerability-based testing techniques that incorporate tests or test strategies deriving from vulnerabilities (e.g. XSS), • techniques for model inference/extraction from the behaviour or code of the implementation, including generation of test cases and related automated reasoning techniques, security goals and a model of the attacker. These techniques are implemented and integrated into the SPaCIoS Tool that is publicly available for cyber security experts and analysts.	
Coherence	The consortium performed integration activities for achieving interoperability of the SPaCIoS Tool with the NESSoS SDE platform. Therefore the project was coherent and was complementary to the EU research initiatives launched in parallel to SPaCIoS and also after its finalization. Moreover, the scope of the SPaCIoS is in line with the Commission efforts towards securing the Internet of Services and with Digital Agenda for Europe. The SPaCIoS project was a follow-up of the AVANTSSAR (funded under ICT-2007.1.4 call).	
Relevance	The project was relevant to the actual trends (i.e. growing Internet of Services) and addressed the main security testing challenges related to IoS, contributing to the assurance of security and trustworthiness in the entire lifecycle of services.	

SPACIOS	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2014
EU added value	The project was an added value to the security validation technologies and processes. Results of the project contributed to the development of innovative tools for analysis and validation of a service not only at the design stage, but also during the service consumption. Moreover, the SPaCIoS shared its results and experience gained during the course of the project within industry, research organisation as well as contributed to the number of working groups and standardization organizations.	
Impacts	The results of the project have a great potential for successful transferring into industrial practices and processes (by involvement such industrial partners as SAP or Siemens). This may strengthen efforts towards trustworthy services available over Internet. Lessons learned and best practices collected and published during the project may impact standardisation in security testing area and communities acting in this area. Other stakeholders that may be impacted with the project results are service developers and producers that will be provided with the novel security testing capabilities, and finally e-services consumers.	

2.6.3 Policy and Security Configuration Management – PoSecCo

The PoSecCo project addressed the challenges related to ISPs/ IT service providers and complexity of their systems. The project had a goal to support of resolving conflicts between interdependent high-level security requirements, low-level security configurations and corresponding security policies.

POSECCO	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2013
Effectiveness	PoSecCo developed a set of integrated tools to manage the security and policy requirements. The proposed framework included the central model repository (the MoVE tool), system for identification security and policy requirements (the CoSeRMaS system), tool for specification of policies and resolving conflicts with security requirements (the IT Policy tool), and decision support system for security (SDSS).	
Coherence	The PoSecCo was coherent with the EC research initiatives dealing with the problem of growing complexity of IT systems and compliance between security requirements at the different levels. Enabling traceability and mapping between requirements and security configuration of the system was also coherent with the NIS PPP WG1 group focused on risk management.	
Relevance	High (and still growing) complexity of the systems and evolving security and configuration requirements, as well as continuously changing policies and law regulations are undoubtedly one of the major obstacles that service providers must face to achieve demanded security compliance. Additional difficulties arise with the growth of “shared IT systems”, i.e. with the growing popularity of cloud-based services or infrastructures. In this light, cost-efficient system for managing security policies and configurations (often resulting from the 3rd party needs) is highly relevant to the actual needs, trends and challenges.	
EU added value	The economic and organizational benefits of an improved policy-making and configuration management for security purposes was studied by the consortium. Such initiatives can contribute to the increased effectiveness of IT security configuration processes by incorporating self-managed features and decision support systems. Also, more appropriate and security requirements-aware policy modelling as well as conflict detection and resolving in European IT services can contribute to greater competitiveness of the EU digital market.	
Impacts	The PoSecCo approach can impact on organizations that are facing conflicts between high-level requirements and low-level software system configuration. In general, the project	

POSECCO	ICT-2009.1.4 - TRUSTWORTHY ICT	2010 - 2013
	approach achieved a demanded compliance of developed/provided services with existing laws and regulations without reducing their security. Moreover, the project adopted some existing industry-standards for change management and for auditing.	

2.6.4 Holistic Approaches for Integrity of ICT-Systems – HINT

The HINT project was focused on trust in hardware devices, including two techniques namely Physically Unclonable Functions (PUFs) used for chip authentication, and side channel analysis-based Hardware Trojan (HT) detection for verification of chip integrity and counterfeit detection.

The major objective was to implement a common security framework for verification of a system integrity based on Trusted Computing technologies and to demonstrate the potential and capabilities of the developed solutions in real-life applications.

HINT	ICT-2011.1.4 - TRUSTWORTHY ICT	2012 - 2015
Effectiveness	HINT proposed a novel PUF technology for chip authentication. To increase effectiveness of Hardware Trojan (HT) detection, the project studied and assessed several measurement (such as power, EM, timing information) and detection alternatives. Each of them has been implemented and demonstrated.	
Coherence	HINT addressed several legislative actions taken by the European Commission with the goal of hardware integrity and trustworthiness assurance. The project was also coherent and complementary with other the EURO-MILS project funded under the same topic and dealing with security of embedded systems.	
Relevance	Nowadays ICT systems are combination of software and hardware components for which security must be equally assured. Such systems work in many critical applications such as avionics, Critical Infrastructures and their control systems, embedded systems in health and transport or smart cards (ID cards, financial sector). The security of such systems, where the authenticity and integrity of the hardware components can be the possible attack targets, is continuously challenged. On the other hand, currently existing approaches based on PUFs and HT detection schemes are not ready for the market adoption and wide use in the real conditions due to lack of stability. Taking into account the above facts, growing trends of counterfeiting of hardware ICT components and growing threat of "Trojans" in Integrated Circuits (IC), the project objectives, scope and results were relevant to the current needs and challenges.	
EU added value	The HINT project aimed to contribute for increased ICT trustworthiness by providing holistic, multi-level approach towards device integrity and authenticity. Since such technologies as e.g. smart cards or ICT in medical sector are future/emerging applications, the trustworthiness of these systems and protection of their hardware components can contribute to increase of the societal acceptance of such solutions and to foster their future market adoption.	
Impacts	The project results had possible impact on overall security of integrated circuits, resulting in higher security of end-user devices. HINT had a very wide potential impact, including the homeland security market, the embedded security market, the smart card market and the personal identity market as was identified by the HINT consortium. Moreover, the HINT results had impact on standardisation bodies, as the HINT created the foundations for a new ISO standard for the PUF technology.	

2.7 Cloud Computing Security

2.7.1 TRustworthy Embedded systems for Secure Cloud Computing Applications – TRESCCA

TRESCCA aimed to define the basis of a secure and trustable cloud platform by ensuring strong logical and physical security on the edge devices, using both hardware security and virtualization techniques. It proposed and demonstrated hardware/software solutions allowing stakeholders to delegate the processing of their sensitive data to a remote processing engine, thus ultimately enabling a new breed of cloud services and applications.

TRESCCA	ICT-2011.1.4 - TRUSTWORTHY ICT	2012 - 2015
Effectiveness	TRESCCA developed mechanisms that enable end users and cloud operators to delegate the processing of their sensitive data to the un-trusted other. Lack of these mechanisms limits the potential of the cloud computing market, since cloud operators and end users may not have established mutual trust relationships.	
Coherence	The objectives of the project, particularly the ones related to creating a dependable chain of trust, have substantial synergies potential with a number of actions related to effectively addressing security issues and supporting trust and security research.	
Relevance	TRESCCA objectives are considered relevant, since cloud computing is an inevitable trend, but lack of trust limits the potential of the cloud computing market. Through hardware security modules and virtualization with live migration to isolate individual processes, the basis for a secure and trusted cloud platform is created. Safety-critical applications can run in a secure environment on the user side and non-safety-critical ones can be outsourced to the cloud safely.	
EU added value	The collaboration, dialog at a European level and participation in clusters of projects facilitated the validation and merging of approaches and proposals for standardization that could be quite different if the work had been carried out at a national level. Openness was also an important characteristic as most of the project's outcomes have been made public and released under free software licenses.	
Impacts	TRESCCA project promoted the concept of secure and trustable cloud platforms by ensuring strong logical and physical security on the edge devices, using both hardware security and virtualization techniques, while considering the whole cloud architecture and key metrics, namely: cost, performance, and acceptability.	

2.7.2 Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure – TCLOUDS

TClouds goal was to provide a computing and network platform to enable resilient and privacy-enabled deployment of Internet-scale critical information and communication infrastructures. Projects' aim was to provide this while addressing the challenges of cross-border privacy, end-user usability and acceptance, which are essential for wide deployment of such an infrastructure.

TCLOUDS	ICT-2011.1.4 - TRUSTWORTHY ICT	2010 - 2013
Effectiveness	The project has achieved important results, and in particular: 1) A Trustworthy Infrastructure Cloud enables individual providers to offer more resilient and privacy-aware infrastructure clouds. 2) Privacy and Resilience for Commodity Clouds enables end users to put a security layer on top of existing commodity infrastructure clouds to enforce their security objectives. 3) Federated Cloud-of-cloud Middleware offers privacy-protection and resilience beyond any individual cloud.	
Coherence	Clouds may evolve into a single point of failure, threaten all dependent ICT, and put the Future Internet at risk. Thus, there are many synergies between the project and other actions.	
Relevance	Protecting critical infrastructures providing communications, energy, or healthcare is still very relevant, since it presents increasing ICT challenges as ICT itself has become vital to them. The project specifically targeted Internet-scale ICT infrastructures (the so called "infrastructure clouds"). These infrastructures promise scalable virtualised computing, network, and storage resources over the Internet. They provide scalability and cost-efficiency but pose significant new privacy and resilience challenges.	
EU added value	Establishing trust in cloud environments requires mechanisms for assessing the operational trust on the cloud which includes assessing the trustworthiness of self-managed services and is considered as a vital requirement for moving critical applications out of private cloud environments.	
Impacts	The project targeted application domains with high impacts on the society at large. One was smart power grids, connecting renewable energy sources and users. This is a premier example of an Internet of Things. The second was home healthcare, where prophylaxis was provided to citizens. Collaboration with complementary standardisation and FP7 projects resulted in increased impact and fostered a European trustworthy cloud ecosystem.	

2.7.3 Privacy-Preserving Computation in the Cloud – PRACTICE

The PRACTICE project aims to build a secure cloud framework that allows for the realization of advanced and practical cryptographic technologies providing sophisticated security and privacy guarantees for all parties in cloud computing scenarios.

PRACTICE	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2016
Effectiveness	PRACTICE goal is to create the conditions for users to have data confidentiality and integrity guarantees without having to trust their cloud providers. The progress so far seems to indicate that the project will achieve its objectives.	
Coherence	The traditional computing paradigm is experiencing a fundamental shift: organizations no longer completely control their own data, but instead hand it to external untrusted parties, cloud service providers, for processing and storage. There currently exist no satisfactory approach to protect data during computation from cloud providers and from other users of the cloud. Thus, project objectives are very timely and coherent with other actions aiming at improving cloud security.	
Relevance	PRACTICE is among the first projects addressing the issue of mitigating insider threats and data leakage for computations in the cloud while maintaining economies of scale. This goes beyond current approaches that can only protect data at rest within storage clouds once insiders may misbehave. Moreover, it will investigate economical and legal frameworks,	

PRACTICE	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2016
	quantify the economic aspects and return on security investment, as well as evaluate legal aspects regarding private data processing and outsourcing.	
EU added value	Secure computation and secure computation services for the cloud have a potential of being a disruptive technology that will change the economics of technology development and deployment. The ability to provide cryptographic and more general secure computation services in the cloud can bring forth new economic and technological opportunities for Europe, and new efficiencies from which multiple sectors of industry in Europe will benefit.	
Impacts	PRACTICE is strongly industry-driven and will demonstrate its results on two end-user defined use cases in statistics and collaborative supply chain management. PRACTICE is based on real-life use cases underpinning the business interest of the partners. The project focus is on near-term and large-scale commercial exploitation of cutting-edge technology where project results are quickly transferred into novel products. Since computation is done on encrypted data, even insiders can no longer disclose secrets or disrupt the service. This opens new markets, increases their market share, and may allow conquering foreign markets where reach has been limited due to confidentiality and privacy concerns. PRACTICE enables European customers to save money by globally outsourcing to the cheapest providers while still maintaining guaranteed security and legal compliance.	

2.7.4 Confidential and Compliant Clouds – Coco Cloud

Coco Cloud aims to empower cloud users to securely and privately share their data in the cloud. This is expected to increase the trust of users in cloud services, and thus favour widespread adoption of cloud technology, with substantial benefits for the users and for the digital economy in general.

COCO CLOUD	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2016
Effectiveness	The project has achieved its overarching goal of enabling control of the disseminated data based on mutually agreed data sharing agreements that are uniformly and end-to-end enforced. These agreements may reflect legal, contractual or user defined preferences, which may be conflicting and thus an appropriate balance and model for their enforcement must be found.	
Coherence	The project goal is creating an efficient and flexible framework for secure data management from the client to the cloud, and vice-versa. The research work is internally coherent, since it develops along three main dimensions that are technically sound: 1) facilitation of the writing, understanding, analysis, management, enforcement and dissolution of data sharing agreements; 2) appropriate selection of enforcing mechanisms, depending on the underlying infrastructure and context; 3) legal compliance in the data sharing process. Externally, the activity is coherent with major related initiatives in the field of protection of personal information.	
Relevance	The objectives of the project are relevant, since the outsourced nature of the cloud (and the inherent loss of control that goes along with that) means that sensitive data must be carefully controlled to ensure it is always protected. The most appropriate form/level of protection depends on the peculiar characteristics of the application, as well as on the situation, context, and environment. Coco Cloud solutions enable data protection (including personal information) by means of flexible mechanisms.	

COCO CLOUD	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2016
	This is essential to citizens, governments and organizations across all sectors, including healthcare and banking and it will be even more so in the future.	
EU added value	By taking a "compliance by design" approach, the project places an early emphasis on understanding and incorporating legal and regulatory requirements into the data sharing agreements. Coco Cloud contributes to fulfil the pervasive need for data protection in cloud services that arises from different stakeholders, including business organizations and citizens, and overcoming the limitations of currently available technology offerings. These are important achievements towards the creation of a Digital Single Market and the requirements imposed by GDPR.	
Impacts	Providing assurance on data protection and data usage control is a key prerequisite for facilitating data sharing among individuals and organisations (or among organisations) to create new ventures and novel means of leveraging the data value. Thus, the outputs of the project can indeed favour the creation of a cloud ecosystem, where data is securely shared.	

2.7.5 Secure Provisioning of Cloud Services based on SLA management – SPECS

SPECS focuses on the development and implementation of an open-source framework that will offer security-as-a-service relying on security parameters as specified in service level agreements (SLAs). SPECS also provides techniques to systematically manage their lifecycle.

SPECS	ICT-2013.1.5 - TRUSTWORTHY ICT	2013 - 2016
Effectiveness	SPECS's solution offers intuitive user centric interfaces to negotiate, enforce, monitor and real-time remediate to possible fluctuations in the Quality of Security (QoSec) by suggesting and/or applying proper actions/countermeasures.	
Coherence	SPECS is coherent with related actions such as participation in the Data Protection, Security and Privacy (DPSP) cluster initiative, contribution in standardization activities, definition of a Security Metric Catalogue and collaboration with relevant projects.	
Relevance	Providing comprehensible and enforceable security assurance by Cloud Service Providers (CSP) can be considered as a vital aspect of deploying trustworthy Cloud ecosystems. SPECS's proposed framework puts also emphasis on small/medium/federated CSP's and can be also integrated "as-a-Service" into existing ecosystems.	
EU added value	SPECS propose solutions for Continuous Security Monitoring, which implements SLA monitoring solutions dedicated to continuously control the security offered by CSP and to help ensuring the granted security service level objectives through agreed SLAs and eventually provide comprehensible and enforceable security assurance.	
Impacts	Providing comprehensible and enforceable security assurance by Cloud Service Providers (CSP) is a critical factor to deploy trustworthy Cloud ecosystems and relates directly to EU cybersecurity strategy and NIS objectives.	

3. Main achievements and Recommendations for the way ahead

3.1 Main Achievements

The overall aim of ICT research in the Seventh Framework Programme was to develop knowledge and technologies for building an open, secure and trustworthy information society in Europe. As already supported by ex post evaluation and impact assessment reports key innovative results have been produced as immediate results while indirect benefits have also been acknowledged regarding provision of a knowledge base to support key EU policy initiatives and alignment of research activities between Member States.

Even given the limited subset of projects, reviewed within the scope of this report, notable achievements and innovative approaches can be identified in the areas of trustworthy network and service infrastructures, user-centric identity and privacy management and technologies, trusted computing, cryptology and advanced biometrics. Particular note should also be made to the promotion of horizontal aspects such as usability, standardization, societal acceptance, economic viability and legal compliance of the research results. Many projects in ICT Security and Trust have been particularly successful in shortening the gap from research to innovation and thus promoting the establishment of a vibrant market in secure and trustworthy ICT in Europe.

However, such impact could not have been achieved without assembling key experts concentrating efforts of Europe's leading researchers. The backing of several European universities and companies provided a critical thrust behind each project that a national level research program might not be able to provide. Only with European partners from different European countries have the projects been able to deliver results that allow the European industry supplying security solutions to fully leverage the potential of the advancements proposed.

Apart from the technical results and their innovation potentials, several FP7 projects also managed to support EU's efforts to achieve policy promotion and coherence. The ICT Trust & Security Programme has been thought to "*implement the EU Cybersecurity Strategy and to address the technological and industrial issues that derive from the Network and Information Security (NIS) policy of DG CONNECT, including the implementation of research and innovation agenda related to cybersecurity, privacy and trustworthy ICT*". In addition to NIS, promotion and support of other emerging legislative initiatives at EU level, namely eIDAS and GDPR has been also achieved.

Similar to the reports prepared under the Security and Trust Coordination and Enhanced Collaboration (SecCord) project[16], Figure 2 below, attempts to summarize the promotion and support offered by each project to the three main legislative initiatives that have been identified above. It is however apparent that still a large number of unresolved cybersecurity, privacy and trust issues (areas of the main legislative initiatives that are not covered) necessitate further research across all ICT technology, components, applications and services.

[16] http://www.seccord.eu/

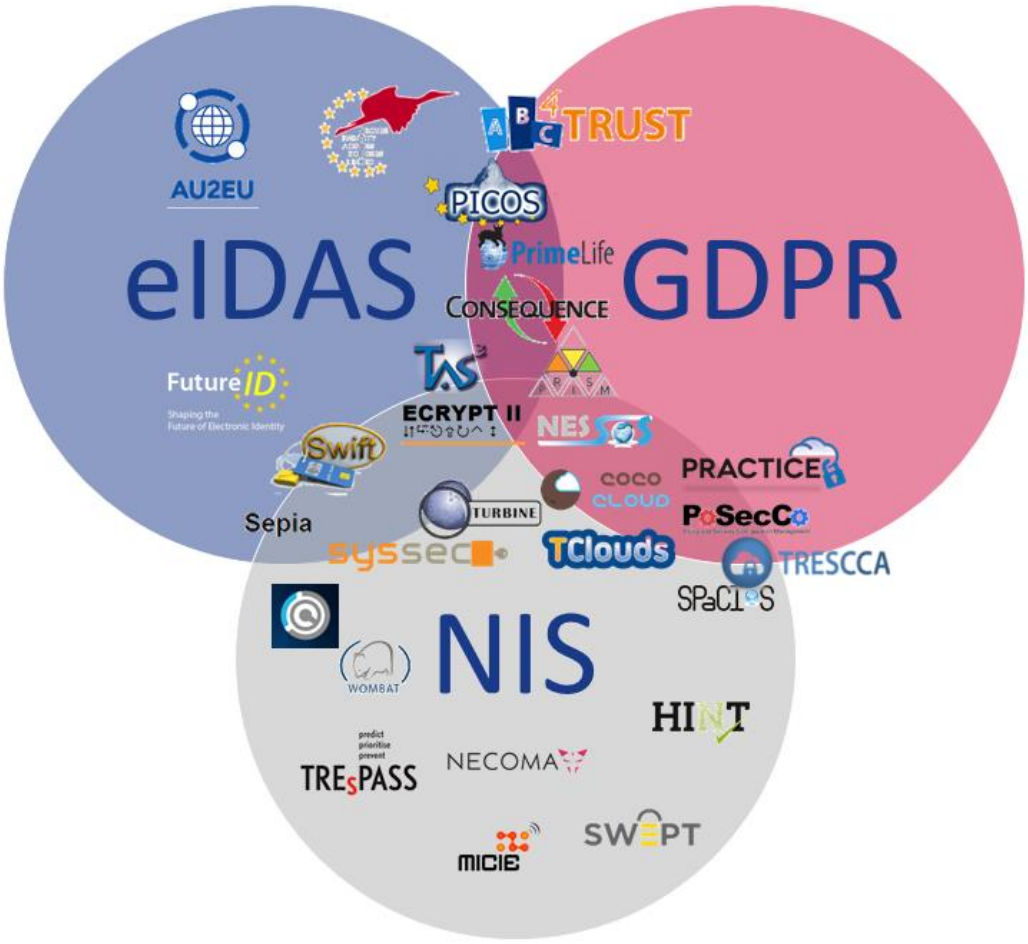

Figure 2: Overview of Projects contribution per main legislative initiatives

3.2 The way ahead

ICT is the backbone every modern society, thus the EU needs to become the single market of preference for governments and industry where trusted core NIS technologies and services for industry and citizens are concerned. The ENISA Threat Landscape 2015[17] provides an analysis of the state and the dynamics of the cyber-threat environment. Among other findings it acknowledges that cyber-threats have undergone significant evolution and just as in 2014, cyber-threat agents have had the tranquillity and resources to implement a series of advancements in malicious practices. An overview and comparison of cyber-threat landscapes for 2015 and 2014 is presented in Table 1 below.

[17] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015/at_download/fullReport

TOP THREATS 2014	ASSESSED TRENDS 2013	TOP THREATS 2015	ASSESSED TRENDS 2014	CHANGE IN RANKING
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	➲	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	➲	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	➲	11. Data breaches	➲	↓
12. Information leakage	↑	12. Identity theft	➲	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1: Overview of cyber-threat landscapes for 2015 and 2014

It is therefore apparent that due to the continuous evolvement of the landscape, identification and prioritising of forthcoming research and innovation topics should be performed in close collaboration with industrial stakeholders across Europe towards a more focused and coordinated approach. A lot of work has already been done with industrial stakeholders within the NIS Platform. WG3 identified key challenges and desired outcomes in terms of innovation-focused, basic and applied research in the fields of cyber security, privacy, and trust and proposed ways to promote multidisciplinary research that foster collaboration among researchers, industry, and policy makers through the Strategic Research Agenda (SRA)[18]. According to the SRA, the main the main research priorities to be further investigated in the future are summarized in the following key objectives:

- Fostering assurance
- Focussing on data
- Enabling secure execution
- Preserving privacy
- Increasing trust
- Managing cyber risks
- Protecting ICT infrastructures
- Achieving user-centricity

EU level public-private partnerships in research and innovation were first introduced in 7th research Framework Programme (FP7), mainly through Joint Technology Initiatives (JTIs) and they were implemented through dedicated legal entities - Joint Undertakings. Public-private partnerships is considered a powerful tool to deliver on innovation and growth in Europe, also supported by the respective Communication[19] from 2013. The new EU research framework programme – Horizon 2020 – may be implemented through public-private partnerships (PPPs) in the case of research and innovation activities of strategic importance to the Union's competitiveness and industrial leadership, or to address specific societal challenges. On 2015, the European Commission adopted the Digital Single Market (DSM)[20] Strategy, which establishes a Public-Private Partnership (PPP) on cybersecurity in the area of technologies and solutions for online network security in the course of 2016.

The contractual PPP (cPPP) objective is to allow the EU to retain a high degree of technological capacity in securing its digital economy and ensuring access to products and services reflecting European values such as privacy. The cPPP will focus on Research and Innovation but also go beyond and address measures that can help impose connection to end users, improve the reporting of validation activities with users of research results and promote participation of relevant EU Industry. As the technology progresses, new areas emerge and have to be explored addressed and secured. Therefore, the governance model should be flexible enough and well represented by all relevant public and private sector stakeholders to address this evolvement.

Based on the latest finding and reports from the research projects funded under the *SEC-2013.2.5-1 - Developing a Cybercrime and cyber terrorism research agenda – Coordination and Support Action* call, the proposed future research roadmap should pertain Technical, Human, Organizational and Regulatory

[18] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/at_download/file
[19] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0494&from=EN
[20] http://ec.europa.eu/priorities/digital-single-market/

dimensions. A provisional instantiation of this roadmap from Comprehensive Approach to cyber roadMap coordINation and develOpment (CAMINO) project[21] is presented below.

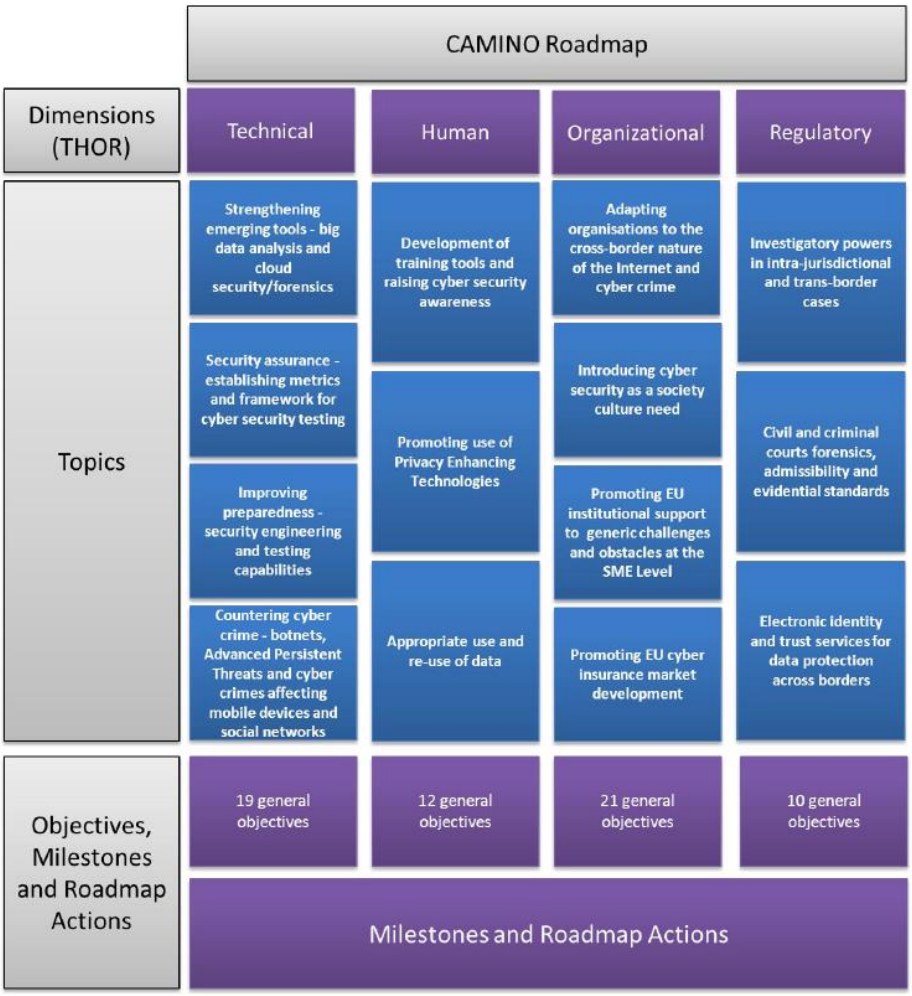

Figure 3: CAMINO project Roadmap[18]

The technical dimension relates to concrete technological approaches and solutions that will strengthen emerging tools and techniques and improve security assurance and preparedness. Human dimension relates to human factors and behavioural aspects, training tools, promotion of privacy enchanting technologies and appropriate use and re-use of data. The organisational dimension relates to processes, procedures and policies within organisations, adapting to the cross-border nature of the Internet and promoting cooperation and collaboration. Finally, the regulatory relates to law provisioning on information sharing and flow of information and standardization in the areas of electronic transactions. SRA has taken one step further and has also compiled a set of indicative examples of expected benefits and contributions per each identified objective.

[21] http://www.fp7-camino.eu/

TOPIC / BENEFITS	BUSINESS	CITIZENS	SOCIETY
Fostering Assurance	Business will be able to operate across Digital Single Market (DSM) thanks to more uniform assurance/protection requirements and achieved levels.	Citizens will be able to compare offerings and make informed decisions based on cybersecurity assurance/protection levels.	Trust in digital space will increase.
Focussing on Data	Business will be able to build innovative data-driven services while being compliant with the data protection and privacy legislation.	Citizens will have means to monitor and enforce policies on data usage, as well as to express their preferences.	Wealth of data will be exploited for various purposes, from healthcare research to fraud detection.
Enabling secure execution	Business will save costs on security management and post-incident activities.	Citizens will enjoy higher level of protection while having more simplicity.	Integration and seamless move between life domains (e.g. work and home) will be achieved.
Preserving privacy	Less privacy breaches will lead to the increase of trust and will become competitive feature.	Citizens will have more guarantees that their privacy is respected.	Societal values will be preserved, such as respect of minorities, dignity, etc.
Increasing trust	Proportion of trust based on demonstrable trustworthiness will be increased.	Citizens will be enabled to make more informed decisions.	Society will evolve to trust digital institutions in a similar way to their trust in the physical world.
Managing cyber risks	More frequent and accurate assessment will lead to more effective use of resources.	Citizens will be able to make instant decisions based on risk "traffic light".	Notion of cybersecurity risk will become an essential part of digital culture.
Protecting the ICT infrastructure	Reduction of "out-of-business" due to ICT infrastructure downtimes and reduction of industrial espionage.	Availability of services that rely on ICT infrastructures.	Less disruptions in critical services for society.
Achieving User-centricity	More users, therefore potential customers, will access digital services.	Simplification will increase the use of advanced protection mechanisms.	Wellbeing achieved by citizens that feel comfortable with new or complex technologies.

Table 2: SRA expected benefits/contributions per research commonality[15]

4. Future Work Programme Recommendations

Promote market-oriented innovation and direct transferability of outcomes to products or services.

The need to establish online trust has been identified early upon by the European Commission with a number of policy initiatives supporting this objective such as the NIS Directive, General Data Protection Regulation, the eIDAS Regulation and the ePrivacy Directive. However, with the progress in the field of information and communication technologies, and especially due to the decrease in calculation and storage costs, new challenges to privacy and data protection, and eventually online trust, have emerged. Forthcoming H2020 and Cyber Security contractual Public-Private Partnership (cPPP) work programmes are already oriented towards promoting synergies between different areas of research and innovation; yet additional effort should be made to ensure more market-oriented innovation and direct transferability of outcomes to products or services.

Introduce horizontal requirements for new information and transparency models and endorse the adoption of by design and by default paradigms.

At the end user's level, this concern has given rise to an increasing appearance of online tools, often open-source and/or freeware, affirming that they can offer certain privacy-preventive functionality for the average user, secure communication, protection against tracking, safeguarding of personal data, anonymous browsing, etc. However, in many cases the functionality of such tools can only be compared against the initial commitments and not the actual development and operation of the tool.

Proper information and transparency is a key issue in any data processing, so as to allow individuals to understand how their data are being processed and to make relevant informed choices. As indicated in ENISA 2015 report[22], transparency needs to expand beyond the original point of data collection and individuals should be adequately informed about the logic and the criteria applied in the context of analytics and automated decision-making processes. To this end, new information and transparency models need to be developed and could comprise a horizontal requirement in forthcoming work programme pillars Purely textual information or existing privacy policies do not seem to cope with the evolution of services and to comprehensively inform users on the processing of data occurring in the complex data value chain. Along with transparency (or as part of it), providing access to users on their data is an important privacy condition as well as an obligation of data controllers.

Sustain close collaboration with all relevant stakeholders on research and innovation topics while supporting key EU policy initiatives

Tools and models that put the data subject in charge of managing their data and promote transparency and user control online seems a promising and emerging research field. The forthcoming revision[23] of the ePrivacy Directive is one of the key policy initiatives aimed at reinforcing trust and security in electronic

[22] Privacy by Design in Big Data: https://www.enisa.europa.eu/publications/big-data-protection
[23] https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive

communications in the EU with a focus on ensuring a high level of protection for citizens and a level playing field for all market players. However, in order to bridge the gap between the legal framework and the available technological implementation approaches, research and innovation activities that will bring together all relevant stakeholders and will provide building blocks of various degrees of maturity should also be promoted.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias
Marousi 151 24, Athens, Greece

TP-05-16-089-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-208-0
DOI: 10.2824/323039