D5.1

Dynamic Security and Privacy Seal Model Analysis

This deliverable presents the results of ANASTACIA Task 5.1. The aim of the task is to analyse and design the Dynamic Security and Privacy Seal (DSPS) Model. This deliverable includes the initial design of the DSPS, including the design of the architectural elements that will support it.

Distribution level	PU
Contractual date	31.12.2017 [M12]
Delivery date	28.12.2017 [M12]
WP / Task	WP5 / T5.1
WP Leader	MAND
Authors	Adrian Quesada Rodriguez (MAND) Bojana Bajic (AS) Mythili Menon (MAND) Sébastien Ziegler (MAND) Ana Maria Pacheco Huamani (AS) Eunah Kim (DG)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's
Horizon 2020 research and innovation programme under Grant Agreement N° 731558
and from the Swiss State Secretariat for Education, Research and Innovation

INDEX OF TABLES

TABLE OF FIGURES

PUBLIC SUMMARY

Several projects have tried to address the need to enable trustable ICT deployments, however, the normative framework for security and personal data protection is evolving. New obligations are emerging from the recently adopted European General Data Protection Regulation (GDPR), with higher requirements and obligations for data controllers, as well as for data processors.

In parallel, ISO standards on IT security, privacy and Information management systems are increasingly becoming market requirements. Existing seals are generally focused either on security or on privacy, but not both. Moreover, they are usually based on two separate models:

- Either ISO standard based certification of products and information management systems, such as ISO 17065 and ISO 27021, relaying on human audit and assessment;
- Or purely system based monitoring of security, such as anti-virus applications, which are often designed independently from any standard.

Given the importance of the GDPR and ISO standards, ANASTACIA intends to combine them with real time monitoring of deployed systems, including a quantitative and qualitative run-time evaluation of the quality of security and privacy risks, which can be easily understood and controlled by the final users.

The Dynamic Security and Privacy Seal (DSPS) aims to generate a novel approach to IT security and privacy certification which combines the certainty and trustworthiness of conventional certification schemes with constant surveillance through real time dynamic monitoring (ANASTACIA) of the certified system. The DSPS will seek to be an accessible and informative resource. It will introduce encryption and verification mechanisms as additional trust-enhancing measures which will guarantee end-to-end security of the information that is presented as part of the Seal. Finally, it will seek to empower the end-user by enabling independent validation of the (current and) historic track record of the sealed system, which will be made available through an innovative blockchain solution to provide the highest possible level confidence on the genuine and authenticated nature of the seal.

"Certification and labelling processes are usually based on system evaluation by human experts at a given period of time. The seal or label is then generated at a given period of time to certify a certain level of trust and reliability attached to the targeted solution or system deployment. The rapid evolution of security landscape and threat may turn supposedly reliable certified systems into vulnerable ones. ANASTACIA aims to combine such conventional certification model, with dynamic monitoring in order to inform the end-user of any change in the trust level."(European Commission, 2016, p. 154).

The DSPS aims to provide a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a two-step process by which: 1) an initial certification examines both the privacy and security elements of both the product or system and the organizational policies and mechanisms that surround its implementation to ensure compliance with the most relevant ISO standards and regulations; and 2) ANASTACIA provides constant monitoring and reaction capabilities which are then used to update the DSPS, which will not only provide advanced trust-enhancing and information functionalities to its users, but will also serve as a surveillance solution, to inform both the client and the certification authority of variations and potential threats to the sealed system.

The current deliverable performs the initial research, design and analysis of the DSPS Model, aiming to:

1) Combine conventional certification schemes with real time dynamic monitoring
2) Addressing the new European General Data Protection Regulation
3) Modelling a secured and authenticated dynamic seal system as a service.

Furthermore, it sets the roadmap to be followed by future ANASTACIA WP5 activities and provides necessary recommendations, requirements and complementary considerations to facilitate their research efforts.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document is prepared in the context of ANASTACIA Work Package 5 – Dynamic Security and Privacy Seal, which is focused on the research and development of the dynamic security and privacy seal, combining security and privacy standards and real-time monitoring. Its work is structured in three complementary tasks.

This deliverable will focus on the first of these tasks, particularly as relates to researching, analysing and designing an innovative model of Dynamic Security and Privacy Seal. It will attempt to combine the most relevant obligations from the new European General Data Protection Regulation, the relevant ISO norms (such as ISO/IEC 27001, ISO/IEC 27018:2014, ISO/IEC 15408, ISO/IEC 29100, etc.), together with real time monitoring of deployed systems, including a quantitative and qualitative run-time evaluation of the quality of security and privacy risks, which can be easily understood and controlled by the final users.

A clearly specified Dynamic Security and Privacy Seal Model is the expected outcome of this document.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- Grant Agreement – Number 731558 - ANASTACIA
- ANASTACIA Deliverable 1.2 User centred requirements initial analysis
- ANASTACIA Deliverable 1.3 Initial Architecture Design

1.3 REVISION HISTORY

Version	Date	Author	Description
1.0	12/22/2017	Adrian Quesada Rodriguez	Final version of the deliverable
0.99	12/12/2017	Adrian Quesada Rodriguez	Final draft for peer review
0.95	11/12/2017	Sébastien Ziegler, Eunah Kim, Ana Maria Pacheco Huamani	Final internal review
0.94	10/12/2017	Adrian Quesada Rodriguez	Final document proofreading and styling
0.92	9/12/2017	Mythili Menon	Updated and reviewed Chapter 4
0.9	8/12/2017	Adrian Quesada Rodriguez	Updated Initial Sealing Process, expanded definitions and cross-references
0.87	4/12/2017	Matteo Filipponi	Technical comments / clarifications

0.86	1/12/2017	Cédric Crettaz	Review of draft and completion of requirements
0.85	27/11/2017	Adrian Quesada Rodriguez	First draft for internal review
0.8	22/11/2017	Adrian Quesada Rodriguez	First draft compiled for presentation in Anastacia General Meeting (Athens)
0.7	16/11/2017	Adrian Quesada Rodriguez	Graphics and figures added
0.6	1/11/2017	Sebastien Ziegler	Architectural framework defined
0.5	18/10/2017	Mythili Menon, Bojana Bajic	First draft of Synthetic model
0.4	30/9/2017	Adrian Quesada Rodriguez, Cédric Crettaz	Formal requirements identified
0.2	15/9/2017	Adrian Quesada Rodriguez	Identification of legal/technical environment
0.1	4/8/2017	Adrian Quesada Rodriguez, Sébastien Ziegler, Ana Maria Pacheco Huamani, Eunah Kim	Initial document outline and structure

1.4 Terms and Definitions

1. **Audit**: This refers to a systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria (including policies, procedures or other requirements) are fulfilled. (International Organization for Standardization, 2011b)
2. **Certification**: This Refers to the provision by an independent body of written assurance (a seal or certificate) that the product, service or system in question meets specific requirements.
3. **Cybersecurity**: This refers to the preservation of confidentiality, integrity and availability of information in the Cyberspace (wherein cyberspace refers to a complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it.
4. **End-User**: Any user of the DSPS or the DSPS GUI who accesses the platform or makes use of any of its services without being assigned any special privilege by the system.
5. Information security management systems: This refers to a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. (International Organization for Standardization, 2013).
6. **Internet of Things**: IoT has been defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. (International Telecommunications Union, 2012a).
7. **IT security**: Information Technology Security, also known as IT Security, is the process of implementing measures and systems designed to securely protect and safeguard information (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions. (www.sans.org)
8. **Personal data**: Personal data shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (EU Data Protection Directive (95/46/EC))
9. **Privacy impact assessment**: A privacy impact assessment is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. (ISO)
10. **Privileged End-User**: Any user of the DSPS or the DSPS GUI who accesses the platform or makes use of any of its services and is granted special privileges by the system due to being: a) properly identified / authenticated by the DSPS system; and b) having been granted special operational or administrative privileges by the DSPS administrator due to his/her functional relationship with ANASTACIA, the DSPS and/or any one of the IoT/CPS deployments being monitored.

1.5 List of Acronyms

Acronym	Meaning
API	Application Programming Interface
CPS	Cyber-Physical System
DDoS	Distributed Denial of Service
DoS / DDoS	Denial of Service / Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GUI	Graphical User Interphase
HSPL	High-level Security Policy Language
ICT	Information and Communication Technologies
IoT	Internet of Things
ITU	International Telecommunications Union
MSPL	Medium-level Security Policy Language
NIST	National Institute of Standards and Technology
PDP	Personal Data Protection
PII	Personally Identifiable Information
SMMI	Seal Manager Metadata Interface

2 Methodology and Approach

An exhaustive and comprehensive analysis process was carried out towards designing the synthetic DSPS model presented in this deliverable. This was supported by continuous feedback received from the partners involved in upcoming ANASTACIA WP5 tasks (5.2 and 5.3). The analysis methodology implemented for the design of the DSPS model was focused on the successive completion of the five main goals:

1) Performing an initial identification of the legal framework and technical environment which will surround and determine the DSPS:

   Initial research efforts pursued a broad-ranging examination of regional and national legislation which could be of relevance to the DSPS[1]. These efforts led to the identification of specific dispositions in the GDPR, eIDAS regulation, e-privacy directive and swiss regulations[2] which should shape the DSPS's approach to personal data protection and security certification and to the design of the seal itself.

   A similar process was followed in the case of technical standards: Following a sweeping examination of standards and recommendations by ISO, ITU, ENISA, NIST and other bodies related to the IoT/CPS ecosystem[3]; several standards were identified as having the

---

[1] The following normative sources were considered by this initial research effort:

- European Law
  - EU Charter of Fundamental Rights (2000/C 364/01)
  - Treaty on European Union
  - Treaty on the Functioning of the European Union 2012/C 326/01
  - General Data Protection Regulation (GDPR)
  - Directive 2002/58/EC (ePrivacy Directive)
  - Directive 2016/1148 (NIS Directive)
  - Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)
- Swiss Law
  - Federal Act on Data Protection (FADP)
  - Ordinance to the Federal Act on Data Protection (OFADP)
  - Ordinance on Data Protection Certification

[2] This deliverable examines Swiss regulations along European regulations in consideration of the location of the partners involved in ANASTACIA tasks 5.2 and 5.3. By doing so, it aims to address any possible additional requirements that might be of relevance if an eventual implementation of the DSPS architecture were to take place in Switzerland.

[3] As part of the research process for the development of this deliverable, the following technical sources were examined:

- ISO Standards
  - ISO/IEC 15408:2009 Security techniques -- Evaluation criteria for IT security
  - ISO/IEC 17030:2003 Conformity assessment – General requirements for third-party marks of conformity
  - ISO/IEC 18045:2005 Security techniques -- Methodology for IT security evaluation
  - ISO/IEC 24760:2016 Security techniques -- A framework for identity management
  - ISO/IEC 27000:2016 Security techniques -- Information security management systems -- Overview and vocabulary
  - ISO/IEC 27001:2013 Security techniques -- Information security management systems -- Requirements
  - ISO/IEC 27002:2013 Security techniques -- Code of practice for information security controls
  - ISO/IEC 29100:2011 Security techniques -- Privacy framework
  - ISO/IEC 29101:2013 Security techniques -- Privacy architecture framework
  - ISO/IEC 29134:2017 Security techniques – Guidelines for privacy impact assessment
  - ISO/IEC 29190:2015 Security techniques -- Privacy capability assessment model
- ITU Recommendations
  - ITU-T X.805 (10/2003) Security Architecture for Systems providing end-to-end communications

potential to support the synthetic DSPS model or to further define the DSPS architecture that should be developed and implemented.

2) Generating a comparative analysis of the two models that are traditionally used for monitoring and certification of an IT system:

   This goal aimed, in first place, to examine both the ISO standard based certification models (and the human audit and assessment processes they require) and the live monitoring systems utilized in IT for monitoring of diverse security threats (antivirus, antimalware, etc.). Upon the observations gathered from this process, a comparative analysis aimed at defining the most desirable traits from each model took place. This to shape the theoretical basis for the development of a DSPS model which synthesized these desirable elements into a holistic solution.

3) Modelling a synthetic model for the DSPS:

- ITU-T X.810 (11/1995) Security frameworks for open systems: Overview
- ITU-T X.816 (11/1995) Security frameworks for open systems: Security audit and alarms framework
- ITU-T X.1056 (01/2009) Security incident management guidelines for telecommunications organizations
- ITU-T X.1171 (02/2009) Threats and requirements for protection of personally identifiable information in applications using tag-based identification
- ITU-T X.1205 (04/2008) Overview of cybersecurity
- ITU-T X.1206 (04/2008) A vendor-neutral framework for automatic notification of security related information and dissemination of updates
- ITU-T X.1208 (01/2014) A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies
- ITU-T X.1209 (12/2010) Capabilities and their context scenarios for cybersecurity information sharing and exchange
- ITU-T X.1311 (02/2011) Security framework for ubiquitous sensor networks
- ITU-T X.1312 (02/2011) Ubiquitous sensor network middleware security guidelines
- ITU-T X.1313 (10/2012) Security requirements for wireless sensor network routing
- ITU-T X.1314 (11/2014) Security requirements and framework of ubiquitous networking
- ITU-T Y.2060 (06/2012) Overview of the Internet of things
- ITU-T Y.2201 (09/2009) Requirements and capabilities for ITU-T NGN
- ITU-T Y.3051 (03/2017) The basic principles of trusted environment in information and communication technology infrastructure
- ITU-T Y.3052 (03/2017) Overview of trust provisioning for information and communication technology infrastructures and services
- ITU-T Y.4050 (07/2012) Terms and definitions for the Internet of things
- ITU-T Y.4100 (06/2014) Common requirements of the Internet of Things
- ITU-T Y.4101 (04/2014) Common requirements and capabilities of a gateway for Internet of things applications
- ITU-T Y.4401 (03/2015) Functional framework and capabilities of the Internet of Things

• ETSI Standards
  - ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
  - ETSI TR 103 305 - CYBER; Critical Security Controls for Effective Cyber Defence
• NIST Standards and Frameworks
  - Framework for Improving Critical Infrastructure Cybersecurity
  - NIST IR 7628 R1 - Cybersecurity for Smart Grid Systems
  - NIST IR 8062 - An introduction to privacy engineering and risk management in federal systems
  - NIST IR 8114 - Lightweight Encryption
  - NIST SP 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
  - NIST SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  - NIST SP 800-147 - Hardware Roots of Trust
  - NIST SP 800-150 - Cyber Threat Information Sharing
  - NIST SP 800-161 - Supply Chain Risk Management

Having structured the theoretical requirements of the DSPS, research focused on developing the baseline functionalities, requirements and processes that should be introduced to the Seal. The minimum functionalities expanded the elements previewed by ANASTACIAs Grant Agreement; guiding principles were identified to help implement the Seal; and an example of potential application and use of the DSPS was developed to further explain the potential implementation of a hybrid model in a business practice. Finally, the goal focused on the specification of the foreseen interactions between ANASTACIA, the DSPS and the end-user.

4) Identifying the architectural requirements and associated considerations for the DSPS:

   Next, research focused on identifying requirements and considerations for the foreseen architecture of the DSPS. Based upon the sources identified throughout the first goal, a set of requirements and associated considerations (aimed at clarifying and facilitating the design and implementation work of ANASTACIA Tasks 5.2 and 5.3) were generated for the DSPS API/Agent, the secure connections, the DSPS Servers and Core Blockchain Network, and the GUI. Lastly the Personal Data Protection requirements developed by ANASTACIA deliverable 1.3 were further specified and the most relevant architectural elements for each requirement were noted.

5) Detailing the architectural elements that will support the DSPS upon implementation

   The last goal that was addressed by this research focused on clearly characterizing how each architectural element should work in relation to the rest of the DSPS System. This task involved divergent research on specific topics which will be relevant for further designing a functional DSPS (Such as research on viable API models, data formatting standards and potentially viable blockchain enablers currently on the market).

Upon completion of these goals, the deliverable underwent several internal review phases aimed at determining the technical feasibility of the proposed model which generated various iterations of the synthetic model and foreseen architecture. The results of this process led to the expected outcome of Task 5.1: a clearly specified Dynamic Security and Privacy Seal Model.

3 DYNAMIC SECURITY AND PRIVACY SEAL CONTEXT AND CONCEPT

The following section will present the fundamental concept and challenges of a Dynamic Security and Privacy Seal, which will be then complemented by a study of the applicable normative and technical frameworks which will define and determine the conditions for its future implementation. Finally, some conclusions will be drafted in order to identify the relevance of each source to the diverse elements of the seal and its foreseen architecture.

3.1 FUNDAMENTAL SEAL CONCEPT AND CHALLENGES

The Dynamic Security and Privacy Seal[4] aims to generate a novel approach to IT security and privacy certification which combines the certainty and trustworthiness of conventional certification schemes with constant surveillance through real time dynamic monitoring (ANASTACIA) of the certified system. The DSPS will seek to be an accessible and informative resource. It will introduce encryption and verification mechanisms as additional trust-enhancing measures which will guarantee end-to-end security of the information that is presented as part of the Seal. Finally, it will seek to empower the end-user by enabling independent validation of the (current and) historic track record of the sealed system, which will be made available through an innovative blockchain solution to provide the highest possible level confidence on the genuine and authenticated nature of the seal.

"Certification and labelling processes are usually based on system evaluation by human experts at a given period of time. The seal or label is then generated at a given period of time to certify a certain level of trust and reliability attached to the targeted solution or system deployment. The rapid evolution of security landscape and threat may turn supposedly reliable certified systems into vulnerable ones. ANASTACIA aims to combine such conventional certification model, with dynamic monitoring in order to inform the end-user of any change in the trust level."(European Commission, 2016, p. 154).

The DSPS aims to provide a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a two-step process by which: 1) an initial certification examines both the privacy and security elements of both the product or system and the organizational policies and mechanisms that surround its implementation to ensure compliance with the most relevant ISO standards and regulations; and 2) ANASTACIA provides constant monitoring and reaction capabilities which are then used to generate the DSPS, which will not only provide advanced trust-enhancing and information functionalities to its users, but will also serve as a surveillance solution, to inform both the client and the certification authority (DSPS Sealing Committee) of variations and potential threats to the sealed system[5].

In the greater context of the ANASTACIA framework, the Dynamic Security and Privacy Seal (DSPS) is fundamentally a trust-enhancing tool. It is aimed to ease end-user (both public and private) interaction with ANASTACIA while contributing to expand their awareness of the effectiveness of the technical measures implemented within the system to ensure compliance with the relevant security and personal data protection requirements.

The DSPS will leverage the information provided by ANASTACIA to certify the status and trustworthiness of a deployed system in real-time. It will interact with ANASTACIA's Security Monitoring and Reaction layers to retrieve information on attacks and countermeasures, and then describe the quality of the security and privacy to the end-user through a dedicated, adaptive web interface and a dynamic/real time graphical

[4] "The outcome of a successful certification (process) is a certificate (thus a document, and/or a seal, that attests that the applicant organisation meets the requirements (substantive and procedural) specified in the certification scheme, and provided in technical standards or legislation"(ENISA, 2017, p. 10).

[5] Enabling immediate reactions from both the client and the Sealing Committee in order to ensure that all organizational requirements and controls (e.g.: Privacy Impact Assessments and the implementation of risk management policies) have been carried out as required by the seriousness of the threat.

representation of the status of the monitored system (as for its compliancy with defined security and privacy policies) along with an explanatory legend for the different possible scenarios (e.g. green, yellow, orange, red).

In addition to these functionalities the DSPS will reflect not only the instantaneous state of the deployed system, but will also include a repository in which the system's status history and reliability changes over time will be stored, along with 1) causes (e.g. detected threats and related device/topology information and 2) actions (e.g. mitigation plans and modification in device/topology configurations). Finally, it will provide a reporting functionality capable of generating reports on 1) detected attacks, 2) affected items, 3) defined mitigation plans, 4) implemented mitigation actions and 5) potential privacy breaches.[6]

As noted in Figure 1, the DSPS aims to position itself as a tool that generates trust in the deployed system by: a) integrating privacy and security information and requirements; and b) introducing a novel, hybrid certification model that overcomes the challenges found in traditional, human-based audit and certification models (such as the one depicted in the standards of the International Standardization Organization) through the introduction of permanent, machine-based real time monitoring (as implemented by system security and anti-virus software) and reporting.

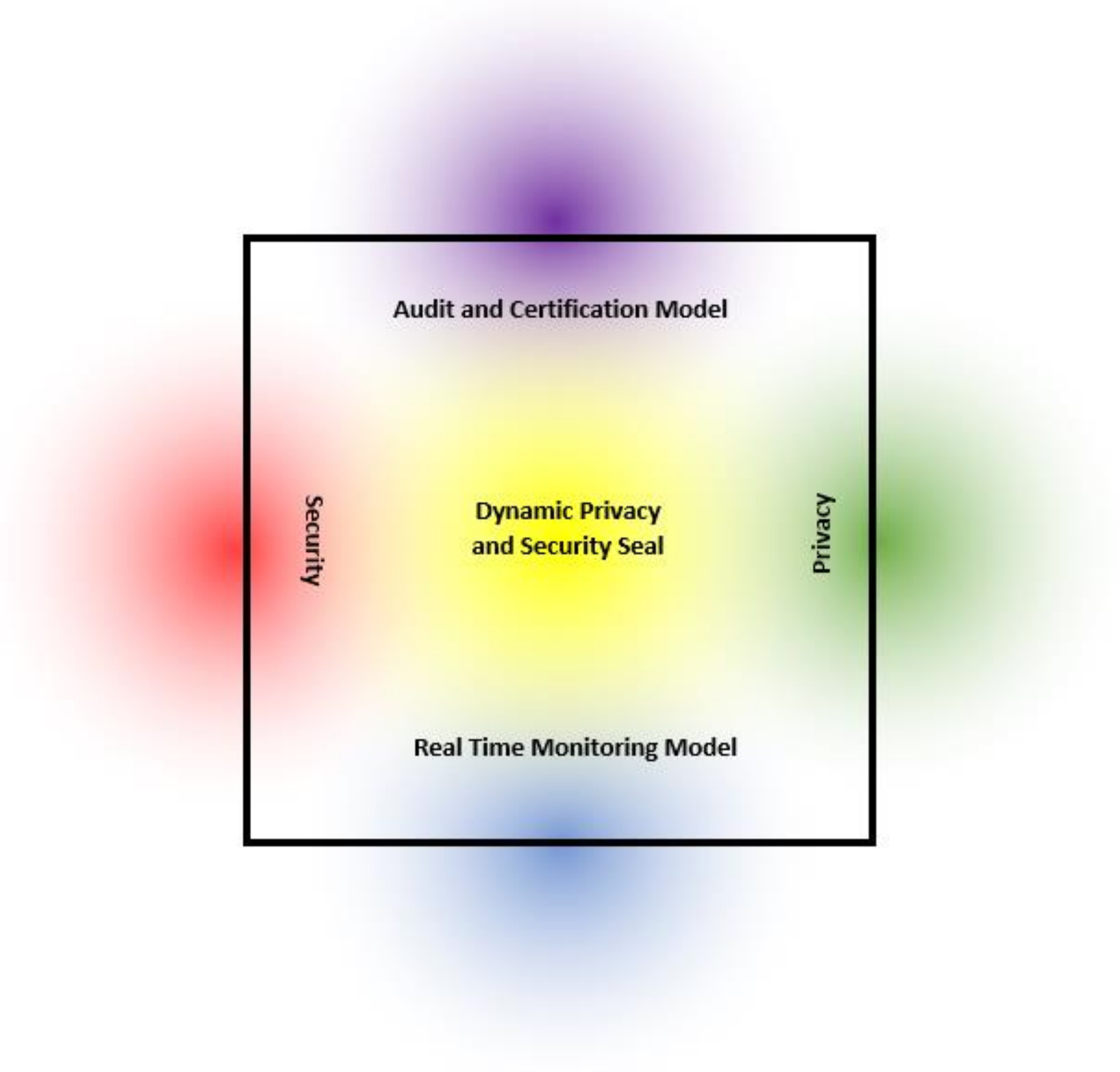

Figure 1 DSPS perspective in its context

[6] See WP1 T1.2 User centred requirements initial analysis page 60.

Effectively, the DSPS aims to introduce a synthetic model (see infra section 5.1) to address the problems and limitations found in both traditional security audit/certification models and real-time monitoring models that examine a system's protection of user privacy and system security; including:

- Traditional audit schemes are resource intensive; human-based audits are expensive and time-consuming as they usually require an auditor to manually perform all the checks to determine the stability and security of a system. In contrast, real time monitoring models do not depend on human verification.
- Traditional certification models are unable to provide real-time assessment and verification of a system's compliance with the audit requirements; they are based on the scheduled performance of audits, which leaves great voids in between every re-certification, thus opening the possibility of unsupervised events affecting end-user privacy/security, thus decreasing trust in the deployed systems. Real time monitoring provides a continuous stream of information on the system, however is unable to analyse all the potential variables and organizational/human context that conditions the system.
- Traditional certification models are reactive, not proactive; they incentivize limited transparency and openness as audit and stability data is only analysed every so often. Furthermore, given the potential impact of security and data breaches, organizations are less willing to immediately disclose the current state of an affected system, which could lead to continued usage of a vulnerable platform by unsuspecting users.
- The goals of privacy measures can be different from those adopted by security measures and no automated system is able to perfectly monitor either set of requirements. Personal data protection regulations introduce privacy-enhancing measures which not only have a different aim (the protection of data subject's rights) but are also heavily focused on the organizational context of the processing activities rather than the technical controls that are often the focus of security measures. The measurement and control of privacy-related organizational activities is highly problematic an automated system, for this reason traditional certification is the go-to solution for determining compliance with PDP regulations. On the other hand, examination of compliance with security norms could be more easily implemented by an automated system (as they are usually aimed to ensure system stability and availability), however organizational, environmental and human considerations require more traditional approaches to audit/certification.

The main challenges found by the DSPS lie in finding the correct balance between these approaches, particularly as relates to:

1) Developing a synthetic model capable of certifying both privacy and security while accounting for the measurement and reaction capabilities of ANASTACIA.
2) Ideating an innovative logging mechanism capable of securing the historic records of the seal while providing real time counterfeit protection.
3) Maximizing end-user integration into this process, enabling independent data verification and validation

To clearly specify a model that is capable of addressing these challenges, a clear understanding of the normative and technical environment that surrounds it must be obtained. The following sections will introduce a series of norms, standards, recommendations and publications which will be considered throughout this deliverable and that will shape both the synthetic DSPS model and the requirements and specifications of the architecture that will support its implementation.

3.2 Normative Environment

Given the DSPS aims to examine and certify the status of Personal Data and Security protections implemented in a system, its design and infrastructure must be tailored to meet the specific normative dispositions that are defined by the European Legal framework, where these topics have been touched upon by diverse instruments, namely:

3.2.1 European General Data Protection Regulation (GDPR)

One of the most important normative element to be considered by the DSPS is the General Data Protection Regulation (European Parliament & European Council, 2016), which was signed in 2016 as a successor to Directive 95/46/EC aimed to prevent disparities between Member States in terms of procedures and sanctions and to generally harmonize personal data protection in the European Union.

Among its key features, the GDPR enshrines a number of guiding principles and dispositions that are to be implemented whenever Personal Data is compiled, stored, processed, disclosed or otherwise handled. Namely the principles of Lawfulness; Fairness; Transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity; and Accountability. Additionally the GDPR explores the requirements for consent; details the requirements for processing personal data regarding underage persons and for processing special categories of data; sets out obligations towards the facilitation of exercise of the data subject's rights of information, access to personal data, rectification and erasure; enables the data subject to restrict processing of his data under certain circumstances, detailing processes for objection and seeks to protect the individual vis-à-vis automated decision-making mechanisms; creates the requirement of data portability; adopts the Data Protection by design and by default approach; sets specific requirements for Data Controllers and Processors; calls for the collection of records of processing activities and for auditing to be implemented; establishes general requirements regarding security of processing; calls upon the generation and implementation of Data Protection Impact Assessments; and sets out the rules to be implemented when dealing with transfers of personal data to countries outside the Union and those which do not ensure equivalent levels of protection to personal information.

A number of requirements that are particularly relevant to the DSPS have been identified in section 6.7 and should be carefully examined throughout the development and implementation of ANASTACIA tasks 5.2 and 5.3. Furthermore, it is important to remember that the GDRP includes specific dispositions (Art. 25 and Recital 78) to include the principles of privacy by design and by default (hereinafter *"PbD"*) to the European Normative Framework for Personal Data Protection. This concept[7] should be permanently considered by the implementation teams as they further develop the DSPS, as it requires the adoption of measures aimed to minimise the processing of personal data, pseudonymising personal data as soon as possible, enabling the data subject to monitor the data processing, ensuring that by default only the necessary personal data are processed, and preventing the disclosure of PII to an indefinite number of natural persons.

Finally, article 42 of the GDPR makes express dispositions on data protection seals, where it states that:

---

[7] Originally postulated by Dr. Ann Cavoukian (Cavoukian, 2011) as being comprised of the following foundational principles:

1) Proactive not reactive; preventative not remedial: the PbD approach aims to anticipate and prevent privacy invasive events (and possible affectations to the rights of data subjects) instead of reacting (and trying to remediate) them.

2) Privacy as the default setting: Privacy enhancing settings and technologies are enabled by default, not requiring further intervention by the end-user, thus ensuring their automatic protection from privacy invasive events.

3) Privacy embedded into design: Privacy considerations come as a fundamental pillar to be considered and supported throughout the design of any process or system and not as an afterthought.

4) Full Functionality – positive-sum, not zero-sum: The perspective considers that it's possible to find a balance between all legitimate interests and objectives, and to enhance the functionality of the system without introducing any drawbacks.

5) End-to-end security – full lifecycle protection: Personal data is protected by the approach even before collection, and continues doing so through the collection, processing and deletion processes through the adoption of strong technical and organisational security measures.

6) Visibility and transparency – keep it open: The approach aims to generate and enhance user trust in the system/business/process through enhanced transparency mechanism and openness to all interested parties.

7) Respect for user privacy: the interests of data subjects are of paramount importance to this approach, as is enabling the participation and empowerment of end-users in the determination and control over the processing of their data.

" 1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the Certification Body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means."(European Parliament & European Council, 2016)

At the moment of preparation of the current deliverable, the specific characteristics of the certification mechanism defined by the GDPR is still unclear[8], however it is recommended that the DSPS is aligned with the European Data Protection Seal and that the certification body exemplified in section 5.2.3 complies

[8] On this topic consider the Recommendations on European Data Protection Certification developed by ENISA, which recognize that "GDPR provisions on certification also introduce a number of challenges that relate to the interpretation of provisions and the terminology, the disposal of different accreditation models, the consistency of benchmarks and approval procedures by competent authorities and connected questions of mutual recognition and harmonization at a national and European level." (ENISA, 2017, p. 06).

with the specific requirements to be met by accredited certification bodies under GDPR Article 43, particularly:

> *"(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;*
> *(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;*
> *(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;*
> *(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and*
> *(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests."(European Parliament & European Council, 2016, pp. 59, 60)*

The criteria and methodology to be developed by Task 5.2 for the initial sealing process detailed in infra section 5.2.3 should be aligned (particularly as pertains to the initial verification of the data protection measures of the system that is to be sealed) with whichever specific dispositions, methodologies and criteria developed in the future by relevant authorities in addition or compliance with articles 42 and 43 of the GDPR. Finally, the implementation teams of Task 5.2 and 5.3 should examine the convenience of pursuing the European Data Protection Seal for the DSPS architecture[9] towards generating trust in the way the platform handles personal data.

3.2.2 Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)

This regulation serves as a basis for an European internal market for electronic trust services *"namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication"(Kirova, 2016).* It defines the concept of electronic seal as "data in electronic form, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal"(European Council, 2014), and according to Article 35, the legal effects of electronic seals relate to their legal effect and admissibility as evidence in judicial proceedings; the generation of a presumption of integrity of the data and correctness of the origin of the linked data; and recognition across the Union. Along this definition, it is noteworthy that the regulation considers a trust service as *"the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps (…) or the preservation of electronic signatures, seals or certificates related to those services" (European Council, 2014)*.

The requirements for advanced electronic seals are set by article 36, which states:

"An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;
(b) it is capable of identifying the creator of the seal;
(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable."(European Council, 2014)

[9] And consider the need to recommending the same certification is obtained for other ANASTACIA elements.

Finally, Attachment III introduces the elements that must be contained by qualified certificates for electronic seals, namely:

(a) *"an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;*
(b) *a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:*
    - *for a legal person: the name and, where applicable, registration number as stated in the official records,*
    - *for a natural person: the person's name;*
(c) *at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;*
(d) *electronic seal validation data, which corresponds to the electronic seal creation data;*
(e) *details of the beginning and end of the certificate's period of validity;*
(f) *the certificate identity code, which must be unique for the qualified trust service provider;*
(g) *the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;*
(h) *the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;*
(i) *the location of the services that can be used to enquire as to the validity status of the qualified certificate;*
(j) *where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing."*(European Council, 2014, Annex III).

These requirements, along with the relevant dispositions of Articles 29-34 of this regulation (pertaining the qualified electronic seal creation devices and the validation and preservation of qualified electronic seals as defined by Articles 39 and 40) shall be introduced to the DSPS requirements found in Section 5.2.1 of this deliverable. Additionally, efforts shall be made by the implementation team to ensure the tools and mechanisms developed throughout ANASTACIA tasks 5.2 and 5.3 comply with any remaining dispositions of the eIDAS Regulation that might be of application (such as Articles 10, 15 and 19), and that before the services are provided to the public, all necessary steps are taken to ensure the recognition of the DSPS as a qualified trust service and to obtain the necessary EU trust mark.

3.2.3 Directive on privacy and electronic communications (e-privacy directive)

Aimed at maximizing the protection of privacy in the electronic communications sector, the Directive is relevant as relates to the possible implementation of a verification and validation mechanism through the GUI. Particularly as recital 24 states that *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users" (European Parliament & European Council, 2009)*, and requires that any program installed on such equipment to be based on legitimate purposes. This is further expanded by Recital 25, which states that these legitimate purposes include the provision of information society services, and as such *"their use should be allowed on condition that users are provided with clear and precise information (…) so as to ensure that users are made aware of information being placed on the terminal equipment they are using" (European Parliament & European Council, 2009)*. Additionally, the recital requires that the user is given the right to refuse, and that any information is provided in a user-friendly manner.
The contents of these recitals are reinstated in Article 5.3, which reads:

> *"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a*

subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." (European Parliament & European Council, 2009).

The requirements set by this directive will be particularly relevant to the design and implementation of the GUI-based blockchain verification/validation web-app defined in sections 5.3.3; 6.4; and 7.4 of this deliverable, and for this reason they should be carefully examined and addressed throughout the development of ANASTACIA task 5.3.

3.2.4 Swiss Federal Act on Data Protection (FADP)

Aiming to provide a general framework for Personal Data Protection for Switzerland[10] (Federal Assembly of the Swiss Confederation, 1992), the Federal Act on Data Protection extends the protection of private persons provided by the Swiss Civil Code and aims to *"maintain good data file practice, and the facilitation of international data exchange by providing a comparable level of protection"(Federal Data Protection and Information Commissioner, 2017)*. It is further enriched by the Ordinance to the Federal Act on Data Protection (Swiss Federal Council, 1993) which aims to complement its dispositions by introducing specific considerations and administrative clarifications to its various sections.

The dispositions found in this regulation shall directly inform the Personal Data Protection Requirements found in Section 6.7 of this deliverable, and shall inform the work of the implementation teams of ANASTACIA tasks 5.2 and 5.3 towards ensuring that any architectural element installed in (or provided from) Switzerland complies with local legal requirements on personal data protection.

3.2.5 Swiss Ordinance on Data Protection Certification

The Ordinance on Data Protection Certification (Swiss Federal Council, 2007) aims to regulate the accredited organizations which provide certification services to systems, procedures and organizations on privacy and data protection in Switzerland[11]. It introduces the requirement of accreditation for certification organizations; enables certification of data processing procedures for which an organization is responsible; products; and individual, separately definable data processing procedures. Additionally, it recognizes the possibility of certifying the policy, documentation and organizational and technical measures involved in these procedures; and introduces sanctions to be imposed in case of detection of irregularities in the supervisory activities.

In the context of the DSPS, the ordinance might be of relevance in support of the synthetic model, particularly as relates to the initial certification process developed in section 5.2.3, which might benefit from an eventual certification under Swiss law. For this reason, it is recommended that the implementation teams of ANASTACIA Task 5.2 and 5.3 analyse the potential benefits of such a certification in the context of the actual measurements that can be provided by WP4 and the extent to which the initial human-based certification is developed in the future.

[10] On the relevance of Switzerland for this deliverable, see supra note 2.

[11] Idem.

3.3 Technical Environment

In conjunction with the normative framework, a number of Technical Standards, Recommendations and Publications have been identified as potentially relevant for the design and technical specification of the DSPS, including but not limited to:

3.3.1 ISO/IEC Standards

3.3.1.1 ISO/IEC 15408:2009 Security techniques -- Evaluation criteria for IT security

The standard details a general methodology for IT evaluation, by which assets and threats that constitute a Security Target are identified and then the IT countermeasures implemented to ensure the protection of the assets are evaluated (Target of Evaluation). The evaluation model is presented in a way by which an evaluator will be able to identify and assess many Security Assurance Requirements. The standard has 3 parts, which establish *"the general concepts and principles of IT security evaluation and provides a description of the organization of components throughout the model."(International Organization for Standardization, 2014)*; *"define the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408"(International Organization for Standardization, 2011a)*; and examine *"the assurance requirements of the evaluation criteria."(International Organization for Standardization, 2008)*.

The requirements detailed in this standard should inform ANASTACIA Task 5.2 in the creation of the specific criteria to be introduced to the initial sealing process and should also be used to benchmark the security of the DSPS architecture developed throughout ANASTACIA Tasks 5.2 and 5.3.

3.3.1.2 ISO/IEC 17030:2003 Conformity assessment – General requirements for third-party marks of conformity

Of prime relevance for the design of the Seal, ISO/IEC 17030:2003 introduces the general requirements for designing, issuing and using third-party marks of conformity. Section 4 and 5 of this standard state a number of actions that must be undertaken towards ensuring the protection of the mark of conformity, maintenance of the trust to be provided by the mark and the prevention of counterfeit.

The relevant parts of these sections read as follows:

> *"4.1 The owner of a third-party mark of conformity shall be responsible for protecting the mark legally against unauthorized use.*
> *4.2 The owner and/or issuer of the third-party mark of conformity shall*
> *a) have rules governing the use of the third-party mark of conformity,*
> *b) take measures to minimize misunderstandings and lack of clarity regarding the third-party mark of conformity that could lead to a reduction in its effectiveness,*
> *c) have rules to ensure that the third-party mark of conformity and any accompanying information are not misleading and take action against their use in a misleading way,*
> *d) have measures to protect and monitor the use of the third-party mark of conformity,*
> *e) take actions to resolve misuses of the third-party mark of conformity, including withdrawal of the mark or appropriate legal action, and*
> *f) take action on and keep a record of all complaints relating to the use of the third-party mark of conformity." (International Organization for Standardization, 2003, p. 2)*

And

> *"5.1 The design of the third-party mark of conformity, or accompanying or publicly available information, shall identify the issuer and the aspects covered by the mark (e.g. safety, environmental, performance, ethics) in a way that avoids any potential misunderstanding. A third-party mark of conformity should be so designed as to minimize the risk of counterfeiting or other forms of misuse.*

5.2 A third-party mark of conformity may be accompanied by additional information to make the meaning of the mark more clearly understood. Such information shall not be misleading and should be in a language understood by the intended recipients.
NOTE It is preferable to use symbols that are universally understandable rather than descriptive words.
5.3 A third-party mark of conformity shall be traceable back to the specified requirements to which the object of conformity assessment conforms."(International Organization for Standardization, 2003, p. 2)

The requirements introduced by this standard must be carefully considered in parallel with the principles identified by section 5.2.2 of this deliverable, as they will be fundamental for the final design and protection of the Seal by ANASTACIA tasks 5.2 and 5.3.

3.3.1.3 ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services

Which *"contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies"(International Organization for Standardization, 2012b)* As such, its contents have been considered in the design of the sealing process detailed in infra section 5.2.3 and should continue to be considered by ANASTACIA task 5.2 as it further defines the model.

3.3.1.4 ISO/IEC 18045:2005 Security techniques -- Methodology for IT security evaluation

A clear methodology for IT Security evaluation is fundamental for the initial certification involved in the development of any IT security seal. This standard *"specifies the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408." (International Organization for Standardization, 2008b)*. In this context, ISO/IEC 18045 should inform ANASTACIA Task 5.2's efforts towards the determination of the methodology for the human-based security evaluation that is to be carried out as part of the initial sealing process (detailed in infra section 5.2.3) of the synthetic model defined by this deliverable.

3.3.1.5 ISO/IEC 27000:2016 Security techniques -- Information security management systems -- Overview and vocabulary

This fundamental standard provides the *"foundation for understanding relevant dispositions of the ISO/IEC 27000 family of standards, as well as a guide to identify other potentially relevant standards"(International Organization for Standardization, 2016)* as it includes relevant terminology and an overview of the Information Security Management Systems. No requirements are found in this Standard given its introductory and general nature, however it should inform future ANASTACIA WP5 tasks, particularly as a contextual support to other standards in its family.

3.3.1.6 ISO/IEC 27001:2013 Security techniques -- Information security management systems -- Requirements

This international standard enables the integration of information security management within organizational management. It *"specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization." (International Organization for Standardization, 2013a).*

As such, this standard requires performance of information security risks assessments at planned intervals or when significant changes to the system take place, along with the requirement of retaining relevant information on such changes and the results of the assessments; calls for the evaluation of information security performance though the implementation of internal audits, managerial decisions on the range of elements to be monitored, and timely reviews of policies; and seeks the improvement of the systems through the implementation of corrective actions based upon the vulnerabilities found through the risk assessments.

The contents of ISO/IEC 27001 should be considered by ANASTACIA Tasks 5.2 and 5.3 in order to ensure that the organizational and managerial elements related to the DSPS (including but not limited to those pictured in supra section 3.2) are designed and implemented in a secure manner, which does not compromise the technical and architectural mechanisms that have been designed in this deliverable and will continue to be defined/implemented by their respective teams.

3.3.1.7 ISO/IEC 29100:2011 Security techniques -- Privacy framework

This standard *"provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology." (International Organization for Standardization, 2011b)*. As such, it complements the requirements introduced by the relevant legal framework and provides a set of principles to be considered by the ISO/IEC 27000 family of standards. The contents of this standard shall inform the personal data protection criteria to be generated in support of the initial sealing process (see infra section 3) and should continue to be considered by ANASTACIA Tasks 5.2 and 5.3 when implementing infra section 6.7 thorough the DSPS architecture.

3.3.1.8 ISO/IEC 29190:2015 Security techniques -- Privacy capability assessment model

Of high relevance due to its focus on assessment efficiency and effectiveness of privacy-related processes in organizations, this international standard *"specifies steps in assessing processes to determine privacy capability, specifies a set of levels for privacy capability assessment, provides guidance on the key process areas against which privacy capability can be assessed, provides guidance for those implementing process assessment, and provides guidance on how to integrate the privacy capability assessment into organizations operations." (International Organization for Standardization, 2015)*. Its contents should be considered by ANASTACIA tasks 5.2 in its efforts towards further specification of the initial sealing process exemplified by infra section 5.2.3.

3.3.1.9 ISO/IEC 40500:2012 (W3C) Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0

Originally developed by the Accessibility Guidelines Working Group of the World Wide Web Consortium (W3) to guide efforts towards the generation of accessible web contents, this standard *"covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photo-sensitivity and combinations of these."(International Organization for Standardization, 2012a)*.

The specific considerations introduced by this standard shall guide future Anastacia WP5 activities related to the front end of the DSPS platform and are relevant to this document as guiding elements to the definition of formal requirements to be implemented by the GUI and other end-user accessible elements.

3.3.2 ITU-T Standards

3.3.2.1 ITU-T X.1208 (01/2014) A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

"Recommendation ITU-T X.1208 describes a methodology for organizations to use cybersecurity indicators when computing a risk measure and it provides a list of potential cybersecurity indicators."(International Telecommunications Union, 2014a). It's relevance for this deliverable is mainly contextual, as at this point it is yet unclear how many of the proposed indicators could be implemented with the data provided by ANASTACIA. For this reason, it is recommended that ANASTACIA Task 5.2 explores the possibility of gathering the required measurements from the information provided by WP4 and that Task 5.3 considers all or some of these indicators in any future efforts aimed at expanding the functionalities available to privileged end-users through the DSPS GUI.

3.3.2.2 ITU-T Y.2060 (06/2012) Overview of the Internet of things

This recommendation is of very high relevance to ANASTACIA due to its relation to the subject and the provision of both high-level requirements and of reference models, it *"provides an overview of the Internet of things (IoT). It clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model. The ecosystem and business models are also provided in an informative appendix."(International Telecommunications Union, 2012a).* Additionally, it is especially well known for providing a definition of Internet of Things as *"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"(International Telecommunications Union, 2012a, p. 1).* In the context of the DSPS, this recommendation should be a fundamental contextual piece of information to be considered by all future WP5 tasks.

3.3.2.3 ITU-T Y.3051 (03/2017) The basic principles of trusted environment in information and communication technology infrastructure

"This Recommendation is devoted to the issue of creating trusted environment in ICT infrastructure providing information and communication services. The Recommendation provides the definition, common requirements, and the basic principles of creating trusted environment."(International Telecommunications Union, 2017a) It is of relevance to our project as it provides the fundamental elements to develop a trusted environment that will enable IoT applications and the project's services, which have been considered multiple times thorough this deliverable and should continue to guide the work of ANASTACIA Tasks 5.2 and 5.3.

3.3.2.4 ITU-T Y.3052 (03/2017) Overview of trust provisioning for information and communication technology infrastructures and services

Trust is fundamental to ICT; this recommendation addresses this issue and grants an overview of the evaluation process required to ensure users of the trustworthiness of the services. This recommendation *"introduces necessity of trust to cope with potential risks due to lack of trust. (…) From the general concept of trust, the key characteristics of trust are described. In addition, the trust relationship model and trust evaluation based on the conceptual model of trust provisioning are introduced. Finally, it describes trust* *provisioning processes in ICT infrastructures and services."(International Telecommunications Union, 2017b).*

The recommendation recognizes that *"Trust is a concept that can cover security and privacy. Security is considered to be the technological aspects, while privacy is considered to be the user aspects. By utilizing security and privacy mechanisms, trust can be realized in ICT infrastructures and services"(International Telecommunications Union, 2017b, p. 12)*. This relates directly to the goals of the DSPS to address both security and privacy while expanding on the basic trust-provisioning model found in the recommendation. As such, its contents are of special relevance to section 5 of this deliverable and should be considered by future WP5 tasks aimed towards further specifying the synthetic model that has been drafted therein.

3.3.2.5 ITU-T Y.4050 (07/2012) Terms and definitions for the Internet of things

Recommendation ITU-T Y.4050/Y.2069 *"specifies the terms and definitions relevant to the Internet of things (IoT) from an ITU-T perspective, in order to clarify the Internet of things and IoT-related activities."(International Telecommunications Union, 2012b)*, as such it presents an important set of contextual information that must be considered by this and future WP5 deliverables.

3.3.2.6 ITU-T Y.4100 (06/2014) Common requirements of the Internet of Things

Recommendation ITU-T Y.4100 *"builds on the overview of IoT (Recommendation ITU-T Y.2060), developing the common requirements based on general use cases of the IoT and the IoT actors and taking into account important areas of consideration from a requirement perspective." (International Telecommunications Union, 2014c)* and generally calls for the implementation of secure, trusted and privacy protected communication, data management and service provision capabilities; the integration of security policies and techniques as required in order to ensure a consistent security control over the variety of devices and user networks in IoT(International Telecommunications Union, 2014b, p. 13); and the support of security audits in IoT applications are to be transparent, transparent and reproducible) for data transmission, storage, processing and application access. (International Telecommunications Union, 2014b, p. 13). These requirements have been considered in the design of the DSPS Architectural Requirements and Considerations found in infra section 6.

3.3.3 ETSI Standards

3.3.3.1 ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services

This document *"proposes a number of scenarios focusing on today's ICT and develops an analysis of possible threats related to PII in mobile and cloud based services (…) to consolidate a general framework, in line with regulation, and international standards, on top of which technical solutions for PII protection can be developed"(European Telecommunications Standards Institute, 2016)*. As such, its contents (particularly those related to threats to PII) should be further considered by ANASTACIA Task 5.2 when developing the personal data protection criteria and methodology to be implemented as part of the Initial Sealing Process.

3.3.3.2 ETSI TR 103 305 - CYBER; Critical Security Controls for Effective Cyber Defence

This fundamental reference document presents a collection of twenty fundamental security controls which are *"an effective and specific set of technical measures available to detect, prevent, respond and mitigate damage from the most common to the most advanced"(European Telecommunications Standards Institute,* *2015, p. 4)* attacks. As such, this collection will also serve to identify the security safeguards to be implemented by the DSPS infrastructure.

3.3.4 NIST Standards

3.3.4.1 NIST SP 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations

This publication introduces a catalogue of both technical and organizational security requirements which address *"security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability)."(Joint Task Force Transformation Initiative, 2013)*. The control elements available in this catalogue possess a high level of detail which should provide additional supporting information to ANASTACIA Task 5.2's efforts towards the identification of security and privacy criteria to be examined through the Initial Sealing Process.

3.3.4.2 NIST SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

This publication adopts a risk-based approach to present the methods for determining PII confidentiality impact levels of potential breaches, the available safeguards and the methods for responding to incidents involving PII. (McCallister, Grance, & Scarfone, 2010). It recommends the minimization of the use, collection and retention of PII; the conduction of privacy impact assessments; the introduction of de-identification and anonymization techniques for personal information; and the implementation of specific set of NIST SP 800-53 R4 security controls, which it recharacterizes under the PII perspective. In this context, the value of this publication is similar to that given to NIST SP 800-53 R4 in its possible application for further clarifying the criteria to be developed by Task 5.2.

3.4 Overview of Potential Applicability of These Sources in the DSPS

As noted in the previous section, the normative and technical environment that surrounds the DSPS is wide and varied. Despite sharing a same origin, the sources detailed above might have widely different objectives. Conversely, legal and technical sources might have similar focuses regardless of their varying approaches. Despite their broad range, in the specific context of the DSPS (and the wider schedule of ANASTACIA WP5), the contents of sections 3.2 and 3.3 should be considered in great detail due to their potential impact on two main objects: a) the synthetic model and those elements that relate to the implementation of the seal itself (graphical elements, potential hybrid methodologies, requirements for certification, etc.); and b) the architectural elements that will support the DSPS.

As manner of conclusion to the review performed throughout section 3, a table aimed to further clarify the object of potential impact of each of these sources has been prepared and can be found below. In doing so, it is expected that upcoming tasks 5.2 and 5.3 will consider their guidance and, when necessary, will adapt their tasks to meet their requirements.

Sources relevant to the synthetic model (tasks related to Seal design and implementation methodology)	Reason or impact	Sources relevant to the DSPS Architecture	Reason or impact
European General Data Protection Regulation (GDPR)	The GDPR includes specific dispositions on certification and seals which should be considered by any task that aims to further specify the hybrid model	**European General Data Protection Regulation (GDPR)**	The GDPR should be consider in its entirety by the DSPS Architecture to ensure that end-user rights are respected and that appropriate safeguards are included in the systems to be developed
Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)	The regulation includes detailed specifications that should be considered when designing the Seal and to be implemented towards ensuring that the seal is capable of meeting its trust provisioning goals.	**Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)**	The regulation should be considered by the architecture as regards to potential integration of certificate and digital signature recognition (either as part of the authentication / identification mechanisms or as methods of validating supporting information uploaded to the system)
Swiss Federal Act on Data Protection (FADP)	In much the same way as the GDPR, the act should be considered by the model and seal as it includes dispositions on certification	**Directive on privacy and electronic communications (e-privacy directive)**	As mentioned above, the main impact of the directive will relate to the DSPS GUI and the DSPS blockchain validation/verification web-app detailed in infra sections 6.4 and 7.4.
Swiss Ordinance on Data Protection Certification	The extent of the Ordinance's requirements for registration of certification providers should be considered by the implementation teams	**Swiss Federal Act on Data Protection (FADP)**	The Act should be considered in parallel with the GDPR when developing those architectural elements to be based in Switzerland, to ensure the protection of data subject rights and legal compliance with local dispositions.
ISO/IEC 17030:2003 Conformity assessment – General requirements for third-party marks of conformity	This standard should be carefully examined by the implementation team of task 5.2 and 5.3 as it details the obligations of the providers of marks of conformity which should be accounted for.	**ISO/IEC 15408:2009 Security techniques -- Evaluation criteria for IT security**	The evaluation criteria should be carefully considered when designing and benchmarking the architectural elements that will support the DSPS.
ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying	This standard should guide any efforts to further develop and implement the human elements of the DSPS initial sealing process as exemplified in section	**ISO/IEC 27000:2016 Security techniques -- Information security**	The concepts and references found in this standard should inform further efforts towards the specification of the DSPS architecture, particularly as relates to the organizational

products, processes and services	5.2.3.	**management systems -- Overview and vocabulary**	structure that should support it and ensure its security.
ISO/IEC 18045:2005 Security techniques -- Methodology for IT security evaluation	The methodological elements of ISO/IEC 18045 are to be considered by any effort to further develop and implement the DSPS initial sealing process as exemplified in section 5.2.3.	**ISO/IEC 27001:2013 Security techniques -- Information security management systems -- Requirements**	The requirements and techniques depicted by this standard should directly impact and be respected by any DSPS architectural elements (and associated organizational structure) that are yet to be specified.
ISO/IEC 27000:2016 Security techniques -- Information security management systems -- Overview and vocabulary	The concepts and references found in this standard should inform further efforts towards the specification of the Seal and the DSPS initial sealing process.	**ISO/IEC 29100:2011 Security techniques -- Privacy framework**	The privacy framework developed by ISO should inform the implementation of the Personal Data Protection Requirements depicted in this text.
ISO/IEC 29190:2015 Security techniques -- Privacy capability assessment model	The privacy capability assessment model detailed by ISO should directly inform future specifications or modalities of the DSPS initial sealing process in direct complement of relevant GDPR dispositions.	**ISO/IEC 29190:2015 Security techniques -- Privacy capability assessment model**	The privacy capability assessment model detailed by ISO should be implemented to benchmark the DSPS architecture in direct complement of relevant GDPR dispositions.
ITU-T X.1208 (01/2014) A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies	The indicators specified by this recommendation should be considered by ANASTACIA Task 5.2 in its efforts to further develop the Seal's functionalities.	**ISO/IEC 40500:2012 (W3C) Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0**	These guidelines should be directly considered by task 5.3 when developing the Seal and the graphical user interface to the DSPS.

	ITU-T X.1208 (01/2014) A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies	The security indicators identified by this recommendation should be considered for implementation within the DSPS architectural elements in order to ensure transparency and user trust in the system.
	ITU-T Y.2060 (06/2012) Overview of the Internet of things	The concepts and references found in this recommendation should inform further efforts towards the specification of the the DSPS architecture, particularly as relates to its integration with ANASTACIA and the IoT systems it monitors.
	ITU-T Y.3051 (03/2017) The basic principles of trusted environment in information and communication technology infrastructure	The contents of this recommendation should be considered when developing the DSPS architecture, so as to ensure all the requirements for proper trust provisioning system are met.
	ITU-T Y.3052 (03/2017) Overview of trust provisioning for information and communication technology infrastructures and services	The contents of this recommendation should be considered when developing the DSPS architecture, so as to ensure all the requirements for proper trust provisioning system are met.
	ITU-T Y.4050 (07/2012) Terms and definitions for the Internet of things	The concepts and references found in this recommendation should inform further efforts towards the specification of the the DSPS architecture, particularly as relates to its integration with ANASTACIA and the IoT systems it monitors.

	ITU-T Y.4100 (06/2014) Common requirements of the Internet of Things	The concepts and references found in this recommendation should inform further efforts towards the specification of the the DSPS architecture, particularly as relates to its integration with ANASTACIA and the IoT systems it monitors.
	ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services	Contents of this guide should be considered to ensure proper protection of personal information by the DSPS architecture.
	ETSI TR 103 305 - CYBER; Critical Security Controls for Effective Cyber Defence	The controls depicted in this section have been considered when specifying the requirements and associated considerations depicted by section 6 of this deliverable and should directly inform implementation of these requirements carried out by ANASTACIA Tasks 5.2 and 5.3.
	NIST SP 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations	The controls depicted by this publication should be considered by tasks 5.2 and 5.3 if necessary to further specify the architectural requirements and associated privacy and security considerations found in section 6 of this deliverable.
	NIST SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	Contents of this guide should be considered in addition to abovementioned sources by any efforts directed towards ensuring personal data protection by the DSPS architecture.

Table 1 Classification by relevance of normative and technical instruments

4 Comparative Analysis of ISO and Real Time Monitoring Models

Following our consideration of the normative and technical environments that will surround the DSPS, our focus should turn towards the development of an innovative Dynamic Security and Privacy Seal which combines security and privacy standards and real-time monitoring.

As specified in ANASTACIA's Grant Agreement, *"Existing seals are generally focused either on security or on privacy, but not both. Moreover, they are usually based on two separate models:*

- *Either ISO standard based certification of products and information management systems, such as ISO 17065 and ISO 27021, relaying on human audit and assessment;*
- *Or purely system based monitoring of security, such as anti-virus applications, which are often designed independently from any standard.*

Given the importance of the GDPR and ISO standards, ANASTACIA will combine them with real time monitoring of deployed systems, including a quantitative and qualitative run-time evaluation of the quality of security and privacy risks, which can be easily understood and controlled by the final users"(European Commission, 2016, p. 154). The following sections of this deliverable shall contribute to the accomplishment of this goal by introducing both of these models, identifying their strengths and weaknesses (as well as the relevant opportunities and threats in each), and finally identifying a set of desirable traits which could guide a synthetic model, such as the one that is to be implemented by the DSPS.

4.1 ISO Methodology Analysis

Privacy and data protection are core concerns. While there exist technical and management mechanisms aimed at ensuring privacy and data protection, these are often only loosely interlinked to existing data governance strategies, which in turn need improved implementation. In this scenario, it is evident that compliance with the existing regulatory privacy and data protection frameworks needs to become more effective. The existing compliance gaps need to be bridged by building successful privacy-friendly design for products, processes and services. Such a design can be effectively promoted by using suitable international standards[12] that incorporate privacy and data protection features.(Perez.G.C, et al, 2016) (Barafort.B, et al., 2017)

In line with the above, the ISO model (derived from the existing international standards in this domain) is focussed on the following:

- Facilitating the formulation of incentive mechanisms for privacy-friendly services and products;
- Providing integrated management and quality management tools that enable the implementation of privacy properties;
- Providing independent guidance and assessing modules and tools for privacy and data management;
- Preparing standards[13] for interoperability of privacy features or characteristics.(Su, et al, 2015)

Within the ISO, the development of a standard is a complex process:

- Before initiating the creation of a standard, a clear objective and the selected target group have to be adequately defined and identified. This is usually encompassed in the first step wherein a ISO

[12] Standard that is adopted by an international standardizing/standards organization and made available to the public (ISO/IEC. Standardization and related activities-General vocabulary.2004)

[1313] Documents, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of optimum degree of order in a given context (ISO/IEC. Standardization and related activities-General Vocabulary. 2004) member (usually the national standardization bodies) are urged by sector members to highlight the need for a certain standard.[14]

- The request is then transmitted to ISO by the national standards organization.
- There are three main steps:
  - "new work item" step: This involves defining the technical scope of the standard
  - "consensus-building" step: This involves negotiating the requirements for the draft standard
  - "formal approval" step: This involves the approval of the draft standard as an international standard. ("Developing standards," 2017.)

For a standard to be formally acknowledged as an international standard, it needs to be approved by at least two-thirds of the participating ISO members (who were involved its development). It also needs to be approved by 75 % of all voting members. In the scenario where sufficient number of votes are received, the text is considered to be officially agreed upon and officially published as an ISO standard.(Su et al., 2015)

For the standards development process, ISO adheres to the following core principles ("Developing standards," 2017.)[15]:

Core Principle(s)
Principle 1: Responding to market needs: ISO does not decide on the creation of a new standard itself. It relies solely on requests received from industry or consumer groups
Principle 2: Standards are prepared by designated global experts: The scope and content of the ISO standards are prepared by experts, who form a part of ISO Technical Committees
Principle 3: Incorporates a multi-stakeholder process: Such a model ensure that a holistic approach is taken for the creation of each standard
Principle 4: Standards based on consensus[16]

Table 2 ISO Core Principles

Following the creation and approval of an international standard, it is prudent for interested parties to be able to adequately implement it and state beyond reasonable doubt that a certain, product, service of process adheres to the requirements, guidelines or characteristics underscored in the standard. In this regard, certification is the procedure which is able to verify adherence to specified requirements. These certifications serve as a credibility booster in the market, thereby assuring that partner companies or entities that the required procedures have indeed been carried out based on international standards. Although, the ISO standards are voluntary, often certain certifications are made mandatory to meet contractual needs or internal sector regulations.

Certifications delivered based on ISO standards are usually time-bound and need to be periodically recertified for the interested party to retain their respective certifications. These certifications are provided by independent certification bodies. It is important to note that ISO only maintains its role as an international standards developing organization and does not, on its own certify any product, process, service or company based on its. However, to assist bodies involved in delivering the certification, ISO has developed several standards which prescribe certification processes ("ISO Certification," 2017.) To better

[14] This step ensure that ISO standards cater directly to industry needs

[15] ISO. How we develop standards. Retrieved from https://www.iso.org/developing-standards.html

[16] General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments. Consensus does not imply unanimity (ISO/IEC. Standardization and related activities-General vocabulary.2004)

understand the ISO standardization model, the strengths and weaknesses have been detailed in the SWOT Analysis.

With reference to privacy and data protection, ISO has developed a list of standards including: ISO/IEC 15408 (Information technology-Security techniques-Evaluation criteria for IT security), ISO/IEC 18045 (Information technology-Security techniques-Methodology for IT security evaluation), ISO/IEC 24760 (Information technology-Security techniques- A framework for identity management), ISO/IEC 27000 (Information technology-Security techniques-Information security management systems-Overview and vocabulary), ISO/IEC 27001 (Information technology-Security techniques-Information security management systems-Requirements), ISO/IEC 27002 (Information technology-Security techniques-Information security management systems-Code of practice for information security controls), ISO/IEC 27006 (Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management system), ISO 27007 (Information technology — Security techniques — Guidelines for information security management systems auditing), ISO/IEC 29100 (Information technology-Security techniques-Privacy framework), ISO/IEC (Information technology — Security techniques — Privacy architecture framework), ISO/IEC 29180 (Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor network), ISO/IEC 29190 (Information technology — Security techniques — Privacy capability assessment model). These standards have been developed through the process described in this chapter. In order to verify conformance to these standards, interested parties will be required to approach accredited certification bodies which can initiate and conduct the certification process

An overall analysis of this model will enable us to characterize it as follows:

Strengths	***Weaknesses***
▪ Assures improved quality/reliability of IT services, processes and products ▪ Independent audit and verification ensure that security and quality of IT-based services is maintained ▪ Boosts customer satisfaction ▪ Competitive edge: access to new markets/trade ▪ Management control of information and related processes ▪ Better internal communication ▪ Limiting waste production ▪ Protects from duplication of IT product, service or process ▪ Provides a risk management framework through ISO 31000[17] ▪ Promotes social responsibility (ISO 26000) ▪ Structured allocation of responsibilities ▪ Prepared by consensus	▪ Lengthy (bureaucratic) implementation processes for IT-based services ▪ Needs to be maintained throughout the life-cycle of the IT product, services or process ▪ In general, there is limited knowledge on the implementation of ISO certifications ▪ Certification process and maintenance especially for IT products that are rapidly changing could entail high costs ▪ Valid for only specific periods[18].

[17] ISO 31000. Risk management – Principles and guidelines

[18] Certifications linked to ISO standards need to be reviewed at regular intervals.

Opportunities	*Threats*
▪ Adequate training could be provided to utilize ISO standards for the IT sector as appropriate ▪ Accreditation of certification bodies ensures that they operate according to a given international standard, thereby raising the credibility of certifications issued by these bodies ▪ Existing ISO standards can be adopted by different sectors and can be amended (within the ISO Technical Committees) in keeping with current industry needs (associated with technologies)	▪ As the audit/verification processes are heavily dependent on human interventions, there is scope for human error and leak of confidential information which can be catastrophic for personal data protection ▪ Likely to incur additional (unforeseen) expenses[19] ▪ Slow evolution of standards may pose a hindrance as technology constantly changes along with the associated cyber-threats

Table 3 SWOT Analysis of ISO Model

Our attempt to generate a synthetic model should consider[20] this brief characterization of the ISO model. Particularly, it shall be carefully aimed at developing those tools that are necessary to address the weaknesses and threats identified (mainly cost and dependence on human intervention); while introducing its strengths (especially as relates to its high-level of detail on the necessary organizational and operational perspectives); and dully considering the model's opportunities (towards trust-generation and extension of its eventual implementation).

4.2 Analysis of Live Monitoring Systems

The effective collection of data, specifically in the urban domain, has become an important factor in driving businesses and overall public administration. While the need for monitoring urbanization and businesses is well acknowledged, there is no universal or agreed mechanism for this purpose. This calls for an approach which includes data acquisition and analytics that specifically addresses real-time data management for effective monitoring. One important factor that influences any domain's information management is its dynamic competitiveness, which can be boosted using an appropriate operations data system. Another relevant factor is the individualistic and unpredictable nature of threats relating to information collection, processing and management, which also renders it essential to have a human-centric data system. (Christodoulou et al., 2016)

In line with the above, real-time monitoring mechanisms enable detection of interruptions in functioning. At a relatively low cost, they are also able to assist in detection and blocking threats and/or removing them from the information system through human intervention, thereby allowing the system to be restored to its original condition.

The main aspects to be considered when employing a real-time monitoring system are:

- What is the operational database volume limits of the system?
- What are the performance limitations (in terms of detection and warnings)(Nguyen et al., 2017)

While database volume limits may vary between real-time monitoring systems, incorporating a low-cost "feedback feature" remains a challenge in real-time monitoring technologies as this would require high-speed interconnection and multi-processors.

[19] Given the lengthy process associated with ISO standard implementation, there maybe be expenses associated with investigation, additional testing and validation of results.

[20] The gap analysis performed as part of this research and found in infra section 4.3 will expand on these elements as necessary to identify desirable traits to be introduced to our model.

As such while, real-time monitoring is expected to ensure the trustworthiness of physical data and identify outliers, there is a lack of effective physical parameters (other than human interventions) which can cross-check the information in the network traffic and characterize it as normal or abnormal, with respect to the real physical values generated by the field devices. By conducting simultaneous cross-validation, it would be more difficult to tamper with the data such that no anomaly would be detected by the system. (Townsend et al., 2017)

Real-time monitoring systems can gather "threat intelligence" from various sources including:

1. Devices: This is provided through notifications that the (compromised) device is accessing a site which is involved in unsavoury activities which can threaten the security of the device and other devices and networks connected to it. This includes botnet-like activities.
2. Malware Indicators: Studies are ongoing to understand exactly what malicious code can do to exposed devices. These studies enable to identification of technical and behavioural indicators, which allow for file blacklisting, such that the malware is no longer effective. As malwares evolve, new indicators are needed to detect them. Thus, research in this area should continue to ensure that real-time monitoring systems are up to date with malware detection.
3. Reputation: reputation data can be correlated with IP addresses to provide a dynamic list of known suspicious IP addresses. The implementation of this assessment method will usually involve tracking spam and phishing attacks to deduce when a trusted IP address has been compromised (Securosis, 2014.)

If effectively leveraged, threat intelligence can assist live monitoring systems to recognize patterns. Given the inherent dynamic nature of the concept of threat intelligence, there still maybe some associated challenges:

1. Integration: Threat intelligence prism needs to be incorporated into the monitoring system. Hence, it is essential to ensure that threat feeds can be integrated easily.

2. Alerting/Reporting: Following the gathering of the data, specified patterns and indicators need to be underscored. This needs to be an automated process as attacks may often occur rapidly and manual updates may not be able to keep up with the frequency of threats.

3. Validation: Before the required action is taken against the threat, it is essential for a skilled human to validate an action before it is executed. If the validation is not provided in a timely manner, restorative action could get significantly delayed thereby further exposing the system to other threats.(Kaspersky, 2015.)

One example of real-time monitoring is antivirus protection utilized by all computer users. The main advantage of this system is that it's implementation is not conditioned on the end-user having a high-level technical knowledge. Antivirus software is crucial for all devices as they are used continuously for downloading files or programs and can have different specifications and features:

- Detecting cyber-attacks in real time[21] to mitigate active threats entering networks. By halting an attack in progress, the risk of the threat spreading, or loss of data is reduced. This function predominantly includes: virus detection, file quarantine, online security and data protection

[21] Attack and threat identification is carried out by antivirus and malware detection software by means of:

- Scanning: The software predominantly runs in the background on computer, testing every file that is open working in real-time protection mood.
- Performing full-system scans: implemented after the installation of the antivirus program and most antivirus programs have scheduled full system scans set up to be implemented once a week. Full system scans are used to check the existence of dormant viruses and can be helpful before the IT system is repaired.
- Virus definitions: Antivirus software relies on existing virus definitions to detect the viruses. This is the reason why the definition files of the program are automatically updated with everyday download. Antivirus programs also follow a process for keeping up-to-date with the latest viruses.

- Automated threat responses ensures that after detecting the threat, adequate response is provided in terms of threat pattern analysis and malware removal, thereby closing the cybersecurity gap and providing post infection clean-up of the system.(Sahay & Sharma, 2016)

As mentioned previously, typically, real-time monitoring systems supervise the values of the physical data system in order to identify potential issues which can lead to failures or disturbances. Based on the observations of the real-time monitoring systems, necessary actions are taken for restoring the normal state of the physical system. However, there may be some discrepancies in the time taken for the restorative actions. This calls for the merging of cyber and physical security areas by which it will be possible to receive information on network traffic and identify possible attacks, while subsequently launching countermeasures based on the evaluation of cyber and physical events. While this seems to be an excellent solution to counter the gaps in real-time monitoring, testing the efficiency of security of such mechanisms in new environments, to detect intrusions is challenging and can often be inconclusive given the evolutionary nature of threats. These problems are exacerbated by the fact that the analysis of computer security algorithms is linked to the physical effects of network-connected systems in a standardized manner (see supra table 4). To facilitate a comparison and synthesis of both these models, the following characterization (SWOT analysis) of the real-time monitoring should be considered:

Strengths	***Weaknesses***
▪ Detects worms, privacy breaches and virus presence ▪ Extracts useful and relevant information for action against threats ▪ Low cost implementation	▪ Does not usually incorporate and effective follow-up mechanism (which is free of human interventions) ▪ May not provide timely automated responses to threats ▪ Needs to be upgraded in keeping with the varying cyber-threats ▪ Real-time monitoring systems often do not have effective memory management systems
Opportunities	***Threats***
▪ Building on traditional monitoring mechanisms, real-time monitoring can gather historical data linked to cyber-attack, which is useful for virus and malware profiling ▪ Training can be provided to foster and facilitate the use of real-time monitoring for cyber-threats worldwide.	▪ Real-time monitoring is not error free ▪ Real-time monitoring may not be able to detect multiple simultaneous attacks or threats. ▪ There is no feedback mechanism linked to the implementation and functioning of most real-time monitoring systems ▪ No evident alerts are usually available for real-time monitoring

Table 4 SWOT Analysis of Live Monitoring Systems

- Heuristics: which allow the antivirus program to identify the new or modified types of malwares, even without virus definition files.

These elements permit a high detection rate of threats and attacks by these automatic monitoring systems than any human-based examination, and for this reason they are considered to be a fundamental tool in preventing malicious activities in any IT system. Finally, it is noteworthy that these processes are not fool proof: while rare, false positives (erroneous identification of a safe file as a threat) do occur. This element should be considered as it has the potential of reducing the credibility of any threat detection mechanism (Hoffman, 2016).

.

4.3 Gap Analysis

Cyber security incidents are not just detrimental to data protection, they also pose a threat to the performance and reputation of many different organisations. The most common way to deal with cyber-threats is to record cyber security-related events, monitor them on a continuous basis, and subsequently investigate suspected breaches while remediating any issues. While the ISO model and real-time monitoring model together provide for a universal approach for logging, archiving, correlating and simulating capabilities along with responding to threats and providing practical guidance, individually, these models cannot be considered sufficient to deal with the growing number of security issues, especially in the data realm.

In recent years, there have been significant innovations in data science, machine learning and behavioural analysis, which, when combined aim to create a standardized approach to automating real-time threat detection, alerting, validation of responses and the final restorative action (Koutsandria. G et al., 2015.). In this context, any model that aims to bridge the existing gap between traditional certification approaches and live monitoring systems should also consider including the following desirable features:

- Security analytics: This should involve analysing, correlating, and alerting on external threat and internal security data
- Automated threat intelligence integration: As threat intelligence information is changing at a rapid rate, instead of manually trying to deduce patterns, it is essential to facilitate automated ingestion of data into the security monitoring platform and promote the use of artificial intelligence techniques which can recognize new patterns to safeguard against emerging threats. Integrated threat intelligence can help by providing additional context allowing responders to prioritize the threats so that analysts can investigate the highest risk cases first.
- Baseline environment: Even though cyber-threats are evolving, it is essential to identify a baseline of normal activity within a given environment, which will allow for the detection of anomalies. Such anomalies may indicate compromise and warrant further investigation.
- Alerts: When one or more anomalies have been detected, alerts should be triggered, and appropriate actions taken.
- Prioritize alerts: Given the volume of cyber-attacks devices and networks are subjected to, it is essential to prioritize alerts based on the frequency and anomalies associated with them. This should allow the system to ascertain which devices to inspect and in what order (Sahay & Sharma, 2016).

Having considered both the ISO and real-time monitoring models, it is evident that any effort towards developing a holistic solution should recognize both the weaknesses and strengths of each model. Furthermore, an effort should be made to determine the most relevant traits that the proposed solution should aim to integrate within itself. To this end, the following table proposes a gap analysis of both models towards the identification of desirable traits from the perspective of both ANASTACIA and the DSPS.

	ISO model	Real time monitoring tools	Desired traits to be included in a synthetic model (DSPS)
Duration for monitoring	Punctual	Ongoing	Ongoing
Standardized approach	Yes	No	Yes
Measures to prevent counterfeiting	Yes (legal)	No	Yes (legal and blockchain)
Medium for monitoring	Human	ICT	Mixed (ICT and/or Human)
Flexible?	No	Yes	Yes
Easily replicated	Yes	Yes	Yes

Easily implemented?	No	Yes	Yes
Cost effective?	No	Yes	Yes
Feedback	Yes (based on audit frequency)	No	Yes
Human Intervention required?	Yes	No	Optional
Based on International Standards?	Yes	No	Yes
Certification Available	Yes	No	Yes
Validity of the model	Valid (for a certain time period)	Valid (throughout)	Valid (throughout)
Easily upgraded?	No	Yes	Yes
Additional Resources required?	Yes	No	Yes (Periodic audits)
Surveillance (After Certification)	Periodically	Not Applicable	Yes
Preventive or Remedial	Preventive	Remedial	Preventive and Remedial
Pro-active Model?	No	No	Yes
Access Control	Not Applicable	Yes	Yes
Information security	No	No	Yes
Visible Warning Signs	No	Yes	Yes
Risk Management	Yes (ISO 31000)	Yes	Yes
Voluntary?	Yes	Yes	Yes
Type of access to the model	Paid	Depends (on type of software)	Paid
Incorporates fair trade practices and human rights	Yes (ISO 26000[22])	No	Yes
Document and data control	Yes	No	Yes
Process Control	Yes	No	Yes
Direct Control (by creators)	ISO does not issue certifications	No	Yes
Training provided by manufacturers	No	No	Yes

Table 5 Gap Analysis

[22] ISO 26000 - Guidance on social responsibility.

5 DSPS Synthetic Model

The following section will detail the DSPS Synthetic Model. It will aim to examine the expected functionalities to be provided by the Seal and the principles that will guide the model. An example of potential seal use will be provided before presenting some of the seal's salient features: the seal creation process; its interactions with Anastacia and the end-user; and the GUI-based blockchain validation and verification system.

5.1 Overview

As detailed in supra Section 3.1, the DSPS seeks to develop a synthetic model which combines the best elements of the traditional certification mechanisms and real-time monitoring processes. Such a synthesis will be accomplished through the performance of an initial human-based certification process which will be complemented by ANASTACIA's monitoring and reaction capabilities (for preventative actions and threat identification) and the continuous surveillance of the alerts and warnings it generates by both the owner of the certified system and the DSPS Sealing Committee through the DSPS GUI. By adopting this approach, the synthetic model aims to integrate both the certainty and transparency found in a traditional certification with the capabilities for historic and real-time analytics found in live monitoring models examined in supra section 4.

The first part of the synthetic model will rely on a traditional, human-based certification[23] (Initial Sealing Process as detailed in infra section 5.2.3) of the platform that is to be monitored through ANASTACIA and the DSPS. The synthetic model will be supported by a dedicated and independent body of experts (Sealing Committee), which will assess the technical and organizational elements that surround the monitored platform's compliance with relevant security and privacy requirements (particularly as defined by ISO standards (27001, 29100 and 29190) and the General Data Protection Regulation).

Once this initial stage has taken place, both ANASTACIA and the DSPS will be fully deployed within the IoT/CPS system that is to be monitored and the system will be integrated to the DSPS Servers. From this moment onwards, ANASTACIA's monitoring and reaction planes will generate a continuous stream of data which will be compiled and pre-processed by a local DSPS Agent, which will securely submit the data to the DSPS Servers for Seal generation. The DSPS Servers will perform a quantitative and qualitative run-time evaluation of the data and will record the seal status in a blockchain-based logging solution, which will maintain the historic records of the seal status and will enable advanced reporting and independent verification/validation through the DSPS GUI.

The DSPS aims to generate a process for constantly informing end-users, the client (system owners and/or administrators) and the DSPS Sealing Committee of potential threats to privacy and security that might have an impact in the certified system. By generating a permanent, unmodifiable log of the privacy/security status of the monitored systems that also functions as a surveillance mechanism for the certification body, the DSPS fills the vacuum left by traditional certification models and gives way for immediate reaction

[23] Designed to be compliant with ISO/IEC 17030 requirements for issuing third-party marks of conformity, particularly as relates to the need for *"a) determination of characteristics of the object of conformity assessment, consisting of, as appropriate, testing, examination of persons, assessment of bodies, auditing of management systems, etc.; b) review, i.e. examination of the extent to which an object of conformity assessment fulfils specified requirements; c) a decision following review that an object of conformity assessment fulfils specified requirements; d) licensing, or other methods, giving authorization to others to use the third-party mark of conformity (…); e)surveillance, evaluating the continued conformity of the object of conformity assessment to specified requirements sufficient to assure continued confidence in the third-party mark of conformity (…)"(International Organization for Standardization, 2003, p. 3).*

(particularly as relates to organizational processes) by all relevant parties in accordance with their capacities/interests.

As such, this synthetic model seeks to fulfil different roles towards its various kinds of users, namely:

- Towards generic end-users: The DSPS is to become a graphical and user-friendly tool which conveys the overall status of the certified system based on its track record of historic security/privacy events. For these kinds of users, the DSPS's main advantage lies on both the possibility to grant an overview of the system's reliability in time and to react immediately to attacks/threats by dynamically changing the information displayed in response to an attack that breaks the seal / makes the system insecure. As an additional trust-enhancing mechanism, end-users will be able to partake in the verification and validation activities of the DSPS Blockchain Log through the DSPS GUI.
- Towards system owners/administrators: The DSPS will grant not only the generic functionalities available to generic end-users but will also provide advanced reporting, visualization and analysis tools, which will build upon ANASTACIA's monitoring and reaction systems to grant insights to privileged users on the way their system is functioning and the alerts, warnings and threats that their systems might be facing. In addition to this element, the system will incorporate an enhanced blockchain verification/validation tool through which privileged end-users will be able to allocate local processing resources towards the expedited validation of their system's transactions in the DSPS blockchain.
- Towards the ANASTACIA Sealing Committee: The DSPS will serve as a surveillance mechanism aimed to continuously monitor the status of the certified system and to dynamically update the Seal and its associated information. This continuous monitoring process will enable expanded coordination activities between the client and the Sealing Committee, and will be particularly useful for maintaining the Committee's overview of those aspects of the system or process that are difficult to measure or analyse through automated tools (such as the organizational elements related to compliance with Personal Data Protection regulation for example).

5.2 DSPS: Functionalities, Principles and Process

This section will detail the minimum expected functionalities and principles that are expected from the DSPS implementation by ANASTACIA tasks 5.2 and 5.3. These elements will then be complemented with an example of the Seal's application in a potential business practice, which will aim to bring more clarity to the processes and organizational elements to be involved in final stages of its development.

5.2.1 Minimum functionalities

The DSPS will aim to provide two minimum functionalities at all times[24], namely:

- Qualitative run-time evaluation
- Historic reliability evaluation

[24] Current functionalities defined by this section respond directly on the defined elements found in the description of WP5 available in the ANASTACIA Grant Agreement(European Commission, 2016, p. 154). Additional functionalities might be developed as WP5 and WP4 become more integrated throughout the development of ANASTACIA Tasks 5.2 and 5.3. Among possible functionalities, it is recommended that Task 5.2 examines the viability of developing a mechanism to interpret and convey the information obtained throughout the Initial Sealing Process through the DSPS.

5.2.1.1 Qualitative run-time evaluation

The measurements provided by the monitoring and reaction module shall be compared against those ANASTACIA policies[25] currently in place to perform an initial determination of the system's immediate status, which will determine the colour of the Seal[26] to be displayed to the user.

Considering the dispositions of the policies as the system's desired baseline values, DSPS Servers will analyse the severity of the breach (as measured by the extent of the affectation to the system) to assign three possible values to the seal:

- Green seal: System is in full conformity with the policies currently in place, no breaches detected at the current time
- Yellow seal: The system is suffering from an attack which has engaged ANASTACIA's reaction capabilities.
- Orange seal: the system is suffering from an attack that has overpassed ANASTACIA's reaction capabilities, leading to the disablement of over 30% of the system's total functionalities
- Red seal: DSPS Seal broken: the system is suffering from an attack which has overpassed ANASTACIA's reaction capabilities, leading to the disablement of over 70% of the system's total functionalities. Currently, the system may not be considered reliable.

5.2.1.2 Historic reliability evaluation

As defined in the ANASTACIA Grant Agreement, "The dynamic seal will take into account the history and reliability over time of the system reliability. It will reflect not only the instantaneous state, but the reliability over time of the system. The Seal is expected to provide various levels of trusts"(European Commission, 2016, p. 154) these levels will be communicated to the user through the number of stars pictured in the Seal[27], as follows:

- Three stars: for systems whose monitoring indicates a secured state for 12 months without any breach;
- Two stars: for systems whose monitoring indicates a secured state for 3 months without any breach;
- One star: for systems whose monitoring indicates a secured state for less than 3 months, with security update in less than 3 hours;
- No star: Recent breach of more than 3 hours in the last three months;
- Red seal: DSPS Seal Broken; system not fully reliable."(European Commission, 2016, p. 155)

5.2.2 Guiding principles

Beyond the technical and organizational requirements that will support the design and implementation of the DSPS architecture, the core functionality of the Seal should be guided by the following principles:

Principles	Description	Basis
Accessibility	Seal-related information should be easily accessible and	ISO/IEC

[25] As developed by ANASTACIA WP2 and reported to the DSPS by WP4.

[26] The specific implementation of this indication by the GUI and the graphical design of the Seal might be further developed by ANASTACIA Task 5.3 if a better or more user-friendly way of conveying the relevant information is found.

[27] The specific implementation of this indication by the GUI and the graphical design of the Seal might be further developed by ANASTACIA Task 5.3 if a better or more user-friendly way of conveying the relevant information is found.

Principles	Description	Basis
	understandable by end-users, regardless of their language. Special considerations should be taken when designing the technical and graphical elements of the seal to ensure that the information it conveys remains accessible to impaired users. (International Organization for Standardization, 2012a) Privacy and security information should be correctly and easily conveyed. Users should be provided with all the necessary data to understand the meaning of each state shown by the DSPS and the implications it has with regards to their usage of the IoT/CPS platform. As required by ISO/IEC 17030:2003, the Seal will clearly show it has been generated by ANASTACIA and will introduce all necessary information (either in the seal itself or in the GUI) to enable contact between the end-users and the DSPS administrators. Feedback received should be considered to develop and enhance future iterations of the Seal, so as to maximize trust, accessibility and usability of the system.	17030, 40500
Accuracy	The Seal value to be displayed to end users and to be recorded in the DSPS Log shall be correct or exact. Errors in the calculation of the Seal status shall be avoided to the highest possible extent. (International Telecommunications Union, 2017b, p. 18)	ISO/IEC 17030, ITU Y.3052
Consistency	The values displayed by the Seal shall be consistent with the measurements obtained by ANASTACIA and with the algorithms that have led to their creation. *"Data consistency refers to the usability of data. Data must be consistent within the confines of many different transaction streams from one or more applications." (International Telecommunications Union, 2017b, p. 18)*	ISO/IEC 17030, ITU Y.3052
Real time update	*"Trust is dynamic, so the measurement of data needs to be conducted as soon as possible for the accuracy of the data" (International Telecommunications Union, 2017b, p. 18).* The graphic design of the Seal should immediately reflect changes in the status of the IoT/CPS deployment in accordance with the information provided by ANASTACIA WP4. The Seal should be updated in real time to alert end-users of potential affectations to their security / privacy in their usage of the IoT/CPS deployment. This requirement for shall also be considered when developing the GUI tools. As such, it will directly inspire the way the DSPS presents information and the tools that ensure the information is comprehendible (visualizations and reports on the system's historic status, the specific	ISO/IEC 17030, ITU Y.3052

Principles	Description	Basis
	indicators for the policies that have been set in the systems and the alerts that have been raised, etc.). The DSPS GUI will be designed in a way that incentivises end-user interaction and enables personalized/tailored solutions that address their needs.	
Counterfeit protection	Sufficient technical, organizational and legal mechanisms should be put in place to ensure the Seal is not counterfeited and/or its trustworthiness is not diluted by rogue implementations of confusingly similar seals by third parties. This principle extends to the need to ensure that a monitored party cannot misrepresent the status of a sealed system (e.g.: by changing the seal's colour or other graphical elements or by embedding a static image of the seal in its website instead of using the dynamic seal).	ISO/IEC 17030
Reliability and availability	The DSPS should be reliable and capable of providing the necessary information/associated services under any condition. As such, the Seal should be designed in a way that enables end-users to easily access the DSPS GUI (by redirecting the users that try to click on an embedded instance of the Seal for example). This requirement connects directly to the need to ensure that the architecture that supports the DSPS will be reliable, fault-resistant and capable of assuring the provision of (at least) minimum level of service at all times.	ISO/IEC 17030, ITU Y.3052
Security, auditability and validation	The Seal should be designed in a way that is consistent with the requirements of ISO/IEC 17030, the GDPR and the eIDAS Regulation[28] and should contain pieces of evidence that are sufficient to properly identify the seal's purpose; the time of creation (timestamp); the sealing policy by which the seal has been created; references to the certificate authority that has generated the seal; and all necessary information to enquire about the validity of the certificates used at the time of seal-creation. The Seal, the processes that lead to its generation and its related architecture should generate and securely store enough supporting information as to ensure their auditability. Furthermore, the human-based elements of the seal creation process should be respectful of the audit methodologies defined by ISO. This requirement includes the need to introduce technological tools to ensure that the data shared by the companies to the audit team is not compromised, introduction of security controls detailed by	GDPR, eIDAS, ISO/IEC 17030, 17065,15408, 18045, 29190, 27001.

[28] The implementation teams of ANASTACIA tasks 5.2 and 5.3 should consider, among other elements, ENISA's security guidelines on the appropriate use of qualified electronic seals (ENISA, 2016) when developing the Seal.

Principles	Description	Basis
	ITU/ENISA/NIST for audit performance, etc.	
Stability	Once generated the DSPS shall record the exact moment at which it was generated. The Seal value and any associated information should remain unchanged for that particular iteration of the seal even after being recorded in the DSPS Log. Future iterations of the seal generation process should not affect the stability of the data saved in the DSPS Log, so as to ensure the quality of any measurements based on historic data. (International Telecommunications Union, 2017b, p. 18)	ISO/IEC 17030, ITU Y.3052.

Table 6 Seal-specific requirements

5.2.3 Application and Use Example

The DSPS will be designed to be used as a self-standing tool and enabler for the end-user. In this context, a synthetic view on the system's interactions within the ANASTACIA framework will be provided in infra section 5.3.2. On the other hand, the DSPS could also be used in conjunction with an ISO certification. The following section presents a potential integration of the DSPS in a hybrid model combining ISO audits, such as ISO/IEC 27001, with real time monitoring of systems under control. While the focus of WP5 will be on the development of the seal itself, contextualization of the DSPS application and use in an example of potential business practice was deemed as relevant in the course of this research effort.

5.2.3.1 Administrative organization

To be recognized by ISO practitioners, the DSPS should align as much as possible with ISO model used for certification schemes. This would require establishing a certain number of roles and functions, including organizational measures. The initial sealing process could be organized through trained audit service providers. A pool of potential audit service providers (auditors, lead auditors, technical experts and reviewers) could be maintained by a DSPS sealing committee. The Seal would be formally authorized and validated by the DSPS Sealing Committee, which would also be tasked with controlling the auditors in order to maintain the quality of the sealing process.

While the assessment process would be led by the Audit Team, the primary resource for the creation and deployment of the Audit team could be a Sealing Process Manager, who would be in charge of selecting the auditors and experts from the DSPS Auditor Pool in order to create the Audit Team.

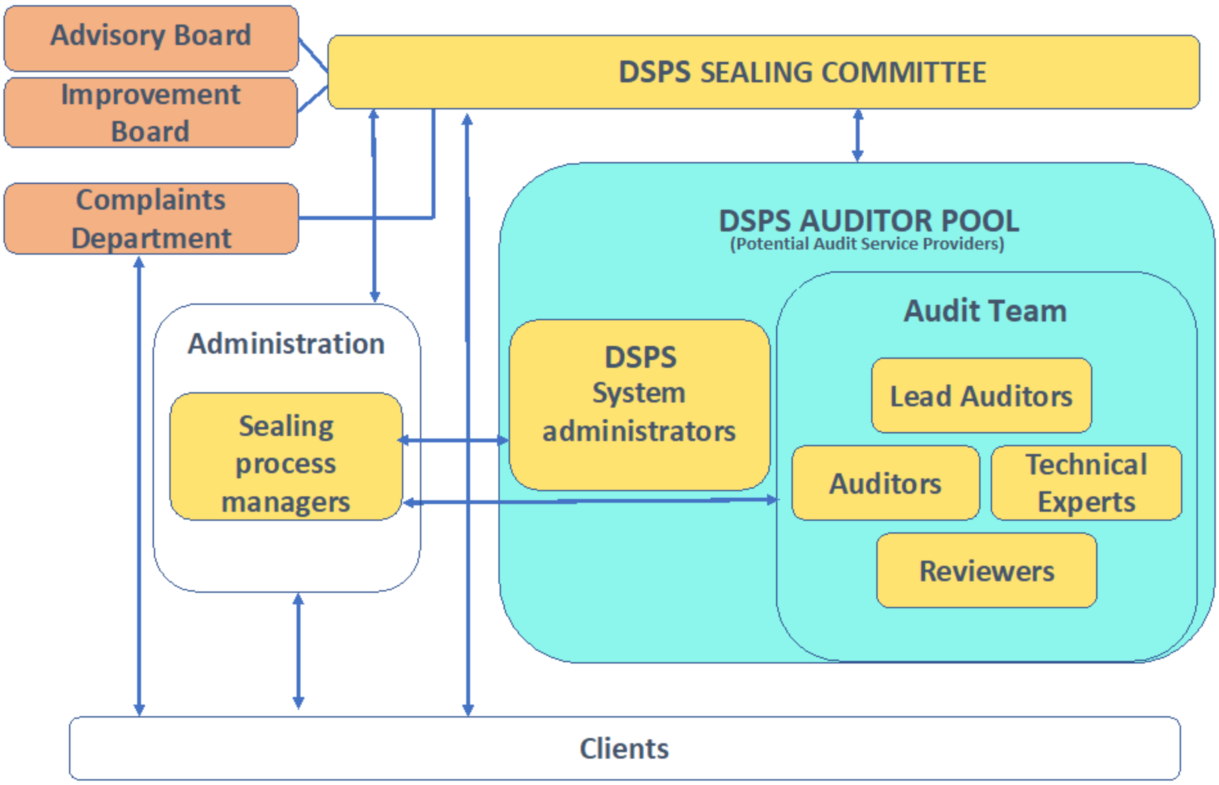

Figure 2 Sealing Process - Overview of potential administrative organization

The specific requirements for the DSPS Auditors, Technical Experts and Reviewers should be aligned with ISO 27001 requirements, the competence criteria for the selection of the Audit Team involved in the initial sealing process should ensure an adequate level of expertise in ICT security and data protection regulations.

Personal behaviour can affect an individual's ability to perform specific functions. The Sealing Process Manager would consider personal behaviour during the selection and training process and should additionally consider the personal strengths (while minimizing the impact of any personal weaknesses) when generating the Audit Team.

5.2.3.2 Stages of the Initial Sealing Process:

In general, the sealing process could be comprised of the following stages[29]:

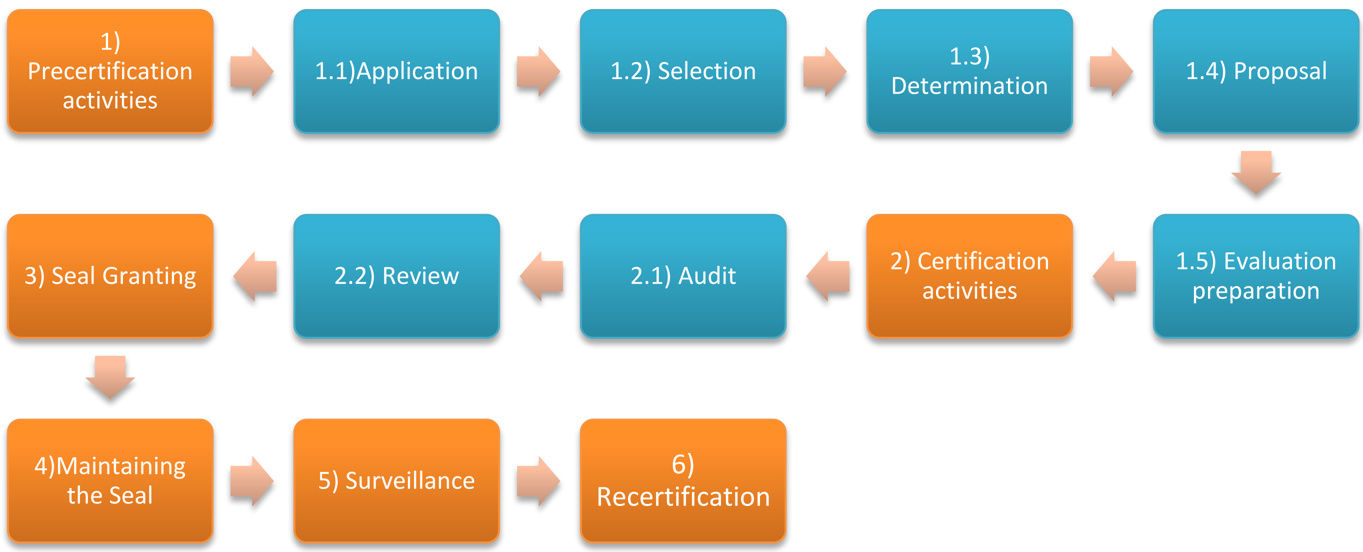

Figure 3 Stages of the Sealing Process

[29] This general outline should be followed unless so decided by ANASTACIA Task 5.2 as part of the further specification of the DSPS model and associated development of the administrative elements / audit criteria.

5.2.3.2.1 1) Precertification activities

1.1) Application

To initiate the certification process and obtain the DSPS, the client would be required to fill in a registration form and a questionnaire. This would allow the collection of relevant information and necessary documents for the precertification activities to take place.

As part of this initial input, all relevant information aimed at demonstrating that the IoT/CPS deployment is qualified/compatible for the sealing process would be provided by the client. Once an application has been accepted, the following steps will take place to ensure the correct review of the application:

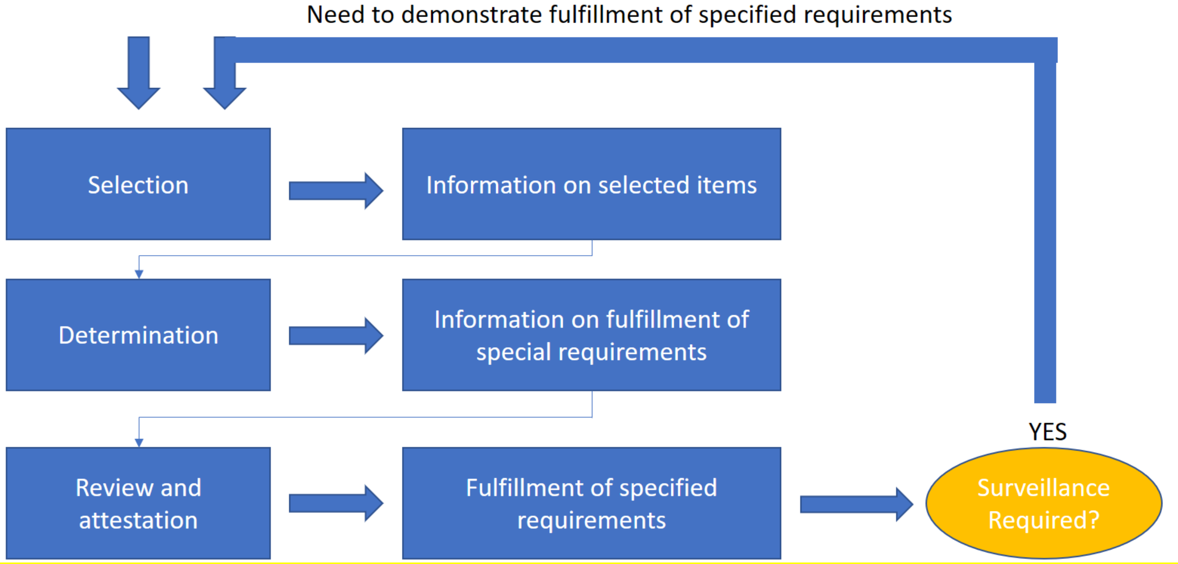

Figure 4 Functional Approach to Conformity Assessment (ISO & UNIDO, 2010, p. 30)

1.2) Selection

This step involves the analysis of the application to define whether the system is a viable candidate for implementation of ANASTACIA and the DSPS or not. During this part of the process the Sealing Process Manager should analyse the data delivered by the candidate in order to verify whether or not the system meets the minimum technical requirements for the implementation of ANASTACIA and the DSPS in his system.

If the applicant meets all the criteria, the manager will continue preparations for the Initial Sealing Process. If the conditions are not met the manager will contact the applicant with sufficient documentation to dully account for the refusal.

1.3) Determination

Once a client's system has been accepted, the scope of the certification should be defined through the identification of the specific characteristics of the products or systems to be certified. As part of this point, the Sealing Process Manager will ensure that any elements influencing the certification activities are considered (language, safety conditions, threats to impartiality, etc.). Additionally, the DSPS system administrators would examine the DSPS Auditor Pool for candidates fit to examining the client's system and would create an Audit Team (comprised of at least a lead auditor, and potentially additional auditors, and technical experts) that will implement the Initial Sealing Process.

1.4) Proposal

The Sealing Process Manager will submit a proposal to the client which will properly convey the details involved in the Sealing Process, including its complexity, breadth of the efforts involved, potential risks and estimated cost of the process. This information will be derived based on the data compiled throughout the pre-certification activities. The client will be invited to review the information provided and formally sign a contract agreeing to the implementation of the proposal and payment of the associated expenses. The contract will also elaborate on the rights and obligations of clients, including the technical, organizational and legal requirements[30] associated to the use of the DSPS.

1.5) Evaluation preparation

Following the signing of the proposal, the Client will receive detailed instructions for the Initial Sealing Process. The Client will have to provide all relevant information required from the Audit Team. The Lead Auditor assigned will analyse relevant documentation to:

- draw a critical vision of its comprehensiveness;
- detect eventual shortcomings; and
- request complementary information when necessary.

This assessment process will then be formalized together with the Client. This would include finalizing the Audit Programme and the Audit Plan with the list of documents, resources and records that shall be made available during the audit. The Audit Plan can be jointly defined or adjusted between the client and the audit team (based on mutual consent), to meet the specific characteristics (including trust, security, confidentiality, etc.) of the object of the certification and availabilities or requirements of the Client.

5.2.3.2.2 2) Certification activities

Acquiring the Dynamic Privacy and Security Seal is the final outcome of a certification process which indicates that the deployed IoT / CPS system being analysed by ANASTACIA conforms with a specified set of requirements. This process should be completed the based on two types of privacy and security assessments[31]:

1) An assessment of the organizational mechanisms and policies that define and/or surround the system/product to be certified;
2) A technical assessment of the software and hardware associated to the system/product to be certified (including an examination of the implementation of ANASTACIA by the system aimed at ensuring the DSPS's compatibility).

2.1) Audit

The Audit Team will cautiously examine the object of certification to obtain all necessary information to support their initial assessments[32]. Implementing predefined personal data protection/privacy and security

---

[30] The associated documentation, including contracts and terms/conditions for the use of the DSPS shall be generated as part of ANASTACIA Tasks 5.2 and 5.3.

[31] These assessments shall be carried out in accordance to the personal data protection and security criteria and methodology to be developed by Task 5.2 in light of relevant norms and ISO standards identified in supra sections 3.2 and 3.3.

[32] Furthermore, during the Audit the Audit Team may compile additional information, as voluntarily provided by the client which serves to demonstrate the system's privacy/security beyond the audit criteria, including but not limited to:

assessment methodologies, the Audit Team will review the mechanisms and policies currently in place in the client's organization (for compliance with relevant norms and organizational policies) and will test selected samples of the client's IoT/CPS deployments and/or its associated products.

The personal data protection/ privacy and security assessment methodologies, as well as the specific criteria against which the technical, normative and organizational elements are to be assessed shall be developed as part of ANASTACIA Task 5.2. This process should be based on the norms, standards and recommendations identified in supra Sections 3.2 and 3.3 (particularly ISO/IEC 15408:2009, ISO/IEC 18045:2005, ISO/IEC 29190:2015, ISO/IEC 27001:2013 and the General Data Protection Regulation).

Upon completion, an assessment report must be prepared by the Audit Team in which a detailed depiction of the findings of the assessments shall be dully presented.

2.2) Review

A reviewer, assigned by the Sealing process manager, will evaluate the assessment report made by the Audit Team, determining the current status of the system to be certified in light of the privacy and security criteria and the information compiled throughout the assessment. The reviewer will also verify the quality and the coherence of the information provided by the Audit Team and will finally draft a Proposal for the Certification Decision, which will be submitted to the DSPS Sealing Committee upon formal review by the Sealing Process Manager.

5.2.3.2.3 3) Seal Granting

The DSPS Sealing Committee will examine the assessment report and the Proposal for the Certification decision. Based on the information contained therein, the Committee will make the final decision about the certification of the client's system and the assignation of the DSPS seal to the certified product/IoT/CPS deployment.

When the decision is positive, and the assessment process has proved that the object of certification conforms with the DSPS criteria, the Committee will order the system's integration with the DSPS Servers (including the assignation of privileged user accounts to the client, the generation of an initial seal for the system, and any other technical activity required to ensure the client is able to fully implement the DSPS and to embed the dynamic Seal in the GUI of the certified product) and the transmission of all supporting documentation (including physical records of the certification activities carried out, their results and the Sealing Committee's decision) to the client.

5.2.3.2.4 4) Maintaining the seal

By obtaining the DSPS, the client will be able to make use of ANASTACIA's monitoring and reaction tools while benefitting from the tools available on the DSPS GUI. As part of the constant conformity surveillance associated with the Seal, both the client and the DSPS System Administrators will continuously receive

---

1) Security or privacy certifications or seals that have been obtained by the client;
2) Security or privacy policies implemented by the client in the context of the IoT/CPS deployment;
3) Data Protection Impact Assessments carried out in compliance with the GDPR;
4) Risk evaluations and/or Risk Treatment Action Plan regarding the privacy and security;
5) Information that prove the compliance with GDPR.

All additional information compiled will not, in principle, be considered as part of the elements that will determine the Status of the Seal, but may be made available to the end-user through the DSPS GUI as a value-added service aimed to introduce contextual information to further enhance end-user trust in the IoT/CPS deployment. Optionally, all or some of these elements may become part of the elements to be considered by the Seal if it is so deemed possible after further specification of the DSPS Model by ANASTACIA Tasks 5.2 and 5.3.

notifications on potential breaches to the system's privacy and security. Upon alerts of potential breaches to the system's privacy and/or security, it is the client's responsibility to perform a full assessment of the extent of the breach and ensure that the actions carried out by ANASTACIA's monitoring and reaction tools have correctly addressed the problem. In case of grave breaches or extended affectations to the system's privacy and security, the client shall comply with applicable legal dispositions (e.g.: by carrying out a Privacy Impact Assessment in accordance to the GDPR) and inform the Sealing Process Manager of the results of these activities, who may request an early recertification in case of a grave breach (or a breach that directly affects or disrupts the functions carried out by ANASTACIA and/or the DSPS in the certified system).

Finally, the client shall inform the Sealing Process Manager of any actions carried out during the time of operation of the DSPS which might further support the Sealed system's claims of compliance with privacy / security legislation (such as Privacy Impact Assessments carried out in the course of operation of the product, or further certifications obtained by the system) and might be required of submitting digitally signed copies of supporting documentation to the Sealing Process Manager (or uploading the information directly to the DSPS GUI).

5.2.3.2.5 5) Surveillance

The Sealing Process Manager will remain in charge of surveillance of the alerts and notifications submitted by the DSPS. When a grave breach is detected, the Sealing Process Manager may appoint a Lead Auditor to support his work in reviewing the outcomes of the client's implemented measures, as well as in the initiation of remedial and preventive actions in case of non-conformance.

5.2.3.2.6 6) Recertification

The certification period for DSPS is three years. Following the certification period, a new Sealing Process shall take place to re-examine the client's IoT/CPS deployments and to verify that they continue being compatible with ANASTACIA and the DSPS. This process shall be planned and conducted in due time to enable for timely renewal before the expiry date of the DSPS.

The DSPS Sealing Committee shall make decisions on renewing the certification and the continued provision of the DSPS services based on:

a) *"The results of the re-certification audit*
b) *The results of the review of the system over the period of certification*
c) *Complaints received from customers of certified clients" (International Organization for Standardization, 2015)*

Furthermore, the DSPS Sealing Committee may take into consideration the historic DSPS status records available in the DSPS Blockchain Log and the metadata compiled as part of the Seal creation process in order to make the best decision on whether the IoT/CPS deployment / product continues to meet the requirements for ANASTACIA/DSPS implementation.

5.2.3.2.7 Perspectives related to DSPS application and use in ISO certifications

As previously mentioned, the above described model presents an example of DSPS potential use in the context for instance of an ISO 27001 certification. The WP5 will take into account the requirements that can be extracted from this potential use case in order to design, develop and provide a DSPS seal that can be easily used by auditors as a complement to their existing tools. The upcoming WP5 work will continue analysing relevant and applicable ISO standards that may improve potential integration and adoption of the DSPS in ISO activities.

5.3 Reference Technical Use Cases

The following section aims to present the reference technical use cases that shall be considered for the salient elements of both the proposed Dynamic Security and Privacy Seal and its supporting architecture. The first of these sub-sections details the process that is to be pursued on a technical level for the creation of the Seal upon completion of the initial sealing process. Following this characterization, sub-section 5.3.2 will position the Seal manager in the architecture[33] and will identify its associated flows. Finally, the last sub-section will focus on the creation of the blockchain log and processes involved in the associated gui-based validation and verification tool.

5.3.1 Dynamic Security and Privacy Seal Creation Process

The DSPS creation process can be summarized as follows:

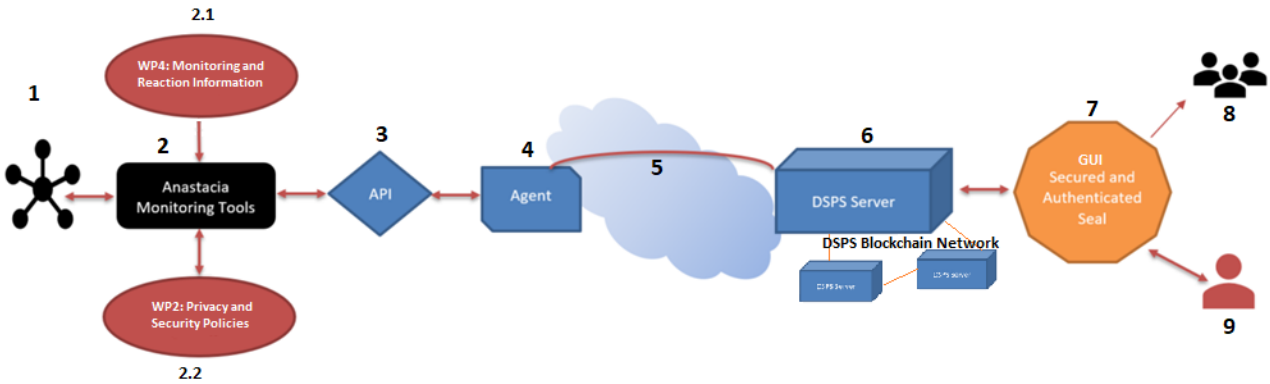

Figure 5 Outline of DSPS creation process

a) Upon completion of the Initial Sealing Process (as exemplified in section 5.2.3), the DSPS is considered to be enabled for the monitored system.
b) Based on the measurements from the deployed IoT system (point 1 in Figure 5), the Security alert service of the ANASTACIA Monitoring tools (point 2 in Figure 5) will identify alerts, warnings and vulnerabilities (point 2.1 in Figure 5) as well as the relevant privacy and security policies (point 2.2 in Figure 5).
c) The information is made available[34] to the DSPS through the SMMI API (point 3 in Figure 5).
d) A DSPS agent (point 4 in Figure 5) running on the ANASTACIA servers compiles this information (and does initial processing of low-level data into the necessary alerts, warnings and vulnerabilities if necessary), translates it (if necessary) into DSPS-ready formats, prepares encrypted data packets, and submit it over a secure communications connection (point 5 in Figure 5) to the DSPS Servers (point 6 in Figure 5). Additional packages containing security self-assessments and transactional verification information will also be submitted separately.
e) The DSPS Servers will compile the packages received from the agent, unencrypt and verify the information contained therein, and perform an evaluation of the current and historic status[35] of the

[33] On this point, it is necessary to clarify that while the contents of supra Figure 2 focuses on the organizational elements of the seal management and the initial sealing process that is to be pursued before assignation of the seal to a IoT/CPS system; supra section 5.3.2 and figures 5-8 aims to position the Seal Manager (as envisioned by ANASTACIA deliverable 1.3), in the context of the proposed architecture.
[34] See supra section 7.1.1 for further clarification on this point. Development of the SMMI API will be one of the tasks to be addressed by ANASTACIA Task 5.2 in direct coordination with WP4 partners.
[35] Available on the DSPS Blockchain Log.

deployed IoT system in function of the policies in place, the relevant alerts, warnings and vulnerabilities, in accordance with the functionalities specified by section 5.2.1. This evaluation will be used by the DSPS Servers to generate an updated Seal status[36], which will be securely communicated to the rest of the servers part of the Core DSPS Blockchain Network.

f) The updated Seal Status is verified/validated by the servers in the Core DSPS Blockchain network and added to the DSPS Blockchain Log, where it becomes permanently and unalterably registered.

g) The DSPS Servers make available the results of this process to both end-users (point 8 in Figure 5) and privileged end-users (point 9 in Figure 5) through a secure graphical user interface (point 7 in Figure 5) which will not only contain a graphical representation of the seal (aimed to easily convey relevant information), but also the necessary links or information channels to obtain further/more detailed data on the system's security and privacy.

h) End users connecting to the DSPS GUI will be asked to voluntarily (opt-in) provide some of their device's local processing power to the verification and validation of the data in the DSPS blockchain log for as long as they continue using the DSPS GUI. Once they have made a decision they will be able to access the Seal GUI and obtain general information on the status (Graphical representation of the Dynamic Security and Privacy Seal) of the deployed IoT system of their interest and additional (clarificatory) information on the status of the system's privacy/security.

i) Privileged end users connecting to the DSPS GUI will be asked to voluntarily (opt-in) provide some of their device's local processing power to the verification and validation of the data in the DSPS blockchain log regarding their own IoT system for as long as they continue using the DSPS GUI. Once they have made a decision they will be able to access the Seal GUI and obtain both the general information on the status of the deployed IoT system (Graphical representation of the Dynamic Security and Privacy Seal) as well as detailed information of the status of the system's privacy/security. Finally, it will provide privileged users with a reporting functionality that generates reports on 1) detected attacks, 2) affected items, 3) defined mitigation plans, 4) implemented mitigation actions and 5) potential privacy breaches.

The elements noted in this list constitute an initial iteration of the DSPS creation process. As such, further iterative modifications or specifications of this process shall be allowed as deemed necessary by ANASTACIA WP5 tasks 5.2 and 5.3. Regardless of this possibility, any such efforts should be aimed solely towards the expansion of the trust, security, ease of use and/or effectiveness of the DSPS.

5.3.2 Seal Manager: ANASTACIA and End User Interactions

As envisioned by ANASTACIA WP1 (Trapero et al., 2017), the Dynamic Security and Privacy Seal is aimed towards monitoring the security and privacy of the deployed system and providing a graphical representation of its status to the end user. As noted by Figure 6,the DSPS has been envisioned to interact only with the Monitoring and Reaction Plane (ANASTACIA WP4) and the End-User or System administrator.

[36] A copy of the data that served to generate the DSPS Seal may be securely stored in the DSPS Servers for its use by the DSPS GUI for provision of its services to Privileged end-users. This information will not be made available to non-privileged end-users and will be bound by confidentiality agreements and any other contractual dispositions that might apply

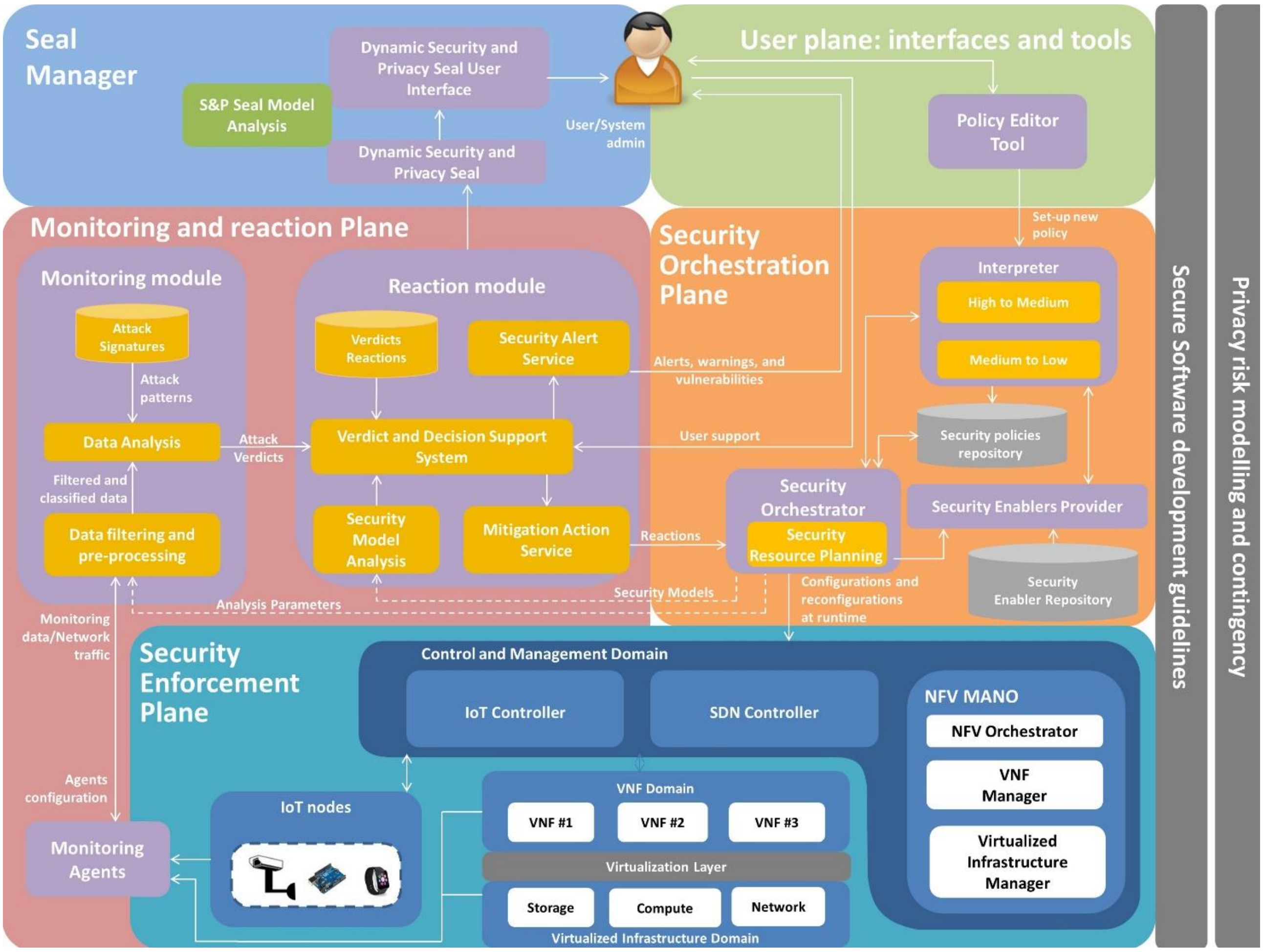

Figure 6 ANASTACIA Plane Overview

The DSPS will depend on two main interfaces for the performance of these interactions, namely: an API to connect with the monitoring and reaction plane (Seal Manager Metadata Interface or SMMI) and the graphical user interface which will enable interaction with the end-users and privileged end-users. As such, the DSPS will depend on the following preconditions to correctly perform as defined:

Preconditions:

1) ANASTACIA platform is connected to an IT System to be analysed in real time.
2) A security policy has been set up in ANASTACIA.
3) A privacy policy has been set up in ANASTACIA.
4) The Monitoring and Reporting plane has prepared the necessary data and metadata (regarding current policies, vulnerabilities, alerts, etc.) on the analysis and reactions undertaken in the normal course of its operations.
5) The data and metadata are saved to a central repository in the Monitoring and Reaction plane which is accessible through the SMMI.

Activity flow:

1) The DSPS servers verify the persistent connection with the DSPS Agent and submit any necessary configuration information[37] to ensure the Agent compiles the relevant data adequately, in the correct format and securely submits it to the DSPS servers.

[37] This configuration element accounts for the possibility of future updates in the functional parameters of the Agent, particularly with respect to the need to adapt to new policies introduced, changes in the language used by the

2) The DSPS Agent compiles the data[38] in a timely manner and securely submits it to the DSPS Servers.
3) The DSPS Servers constantly evaluate the status of the monitored systems using the policies, alerts and warnings identified by the Monitoring and Reaction Plane and the DSPS Agent
4) The DSPS Servers compare the system's latest evaluated status with the historic record available on the Blockchain DSPS log; and generate an updated seal status, which is then added to the Blockchain DSPS Log.
5) The GUI grants secure and differentiated access to end-users and privileged end-users. Additionally, it generates the graphical representation of the Seal, the visualizations of the data and metadata available on the DSPS Log[39], and enables the users to execute the DSPS Blockchain validation and verification web-app.

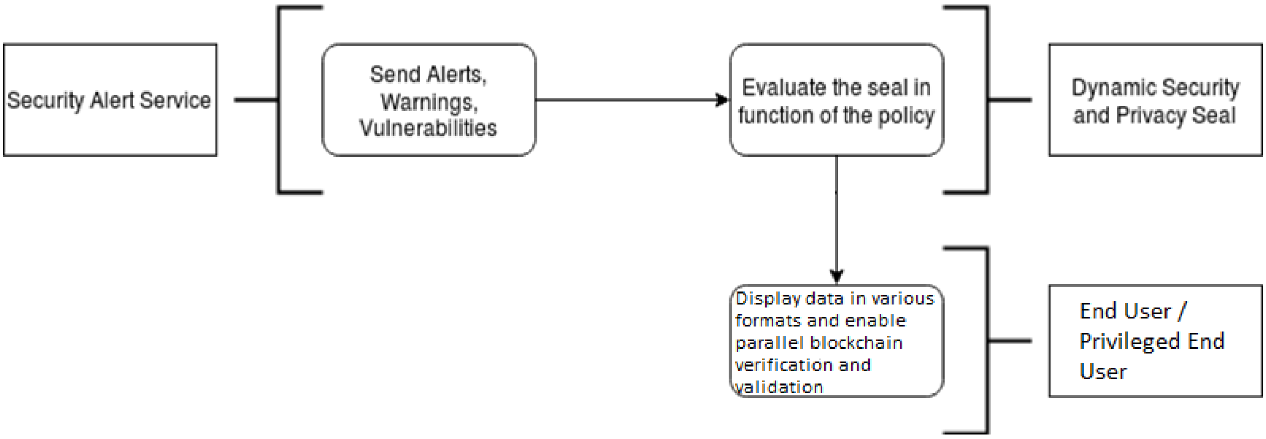

Figure 7 DSPS Activity Flow

Postconditions:

1) The end-user is connected to the DSPS GUI.
2) The Seal is updated in accordance to the latest reported status available in the DSPS Blockchain Log.
3) The DSPS GUI should react to the user inputs and take action in response to its defined capabilities (generate reports, visualizations, etc.).
4) The DSPS should react to any alerts received from the DSPS Blockchain validation and verification web-apps running on an end-user's machine, and perform a thorough re-examination of the identified problems (through a re-verification-validation of the DSPS Log on the Core DSPS Blockchain network, raising the problem to the DSPS System administrators, etc.).

Monitoring and Reaction plane, or increased security requirements (either in its internal function or in its communication with the DSPS Servers)

[38] Among other possible tasks, the agent might be charged with the examination of low-level data obtained directly from the Reaction Module and its characterization under the various possible threats/events that correspond to the measured events for the seal creation. The definition of this functionality will be further examined by ANASTACIA Task 5.2 in close communication and coordination with ANASTACIA WP4 partners.

[39] Visualization of policies, alerts, threats and vulnerabilities, as well as visualization of the data compiled by the Agent in real time will also be made available to privileged end-users. Development and further specification of the exact reach for this functionality will be addressed by ANASTACIA Task 5.3 along with all GUI-related elements.

Sequence Diagram:

The following sequence diagram represents the overall interactions between ANASTACIA, the Dynamic Security and Privacy Seal and the end-user:

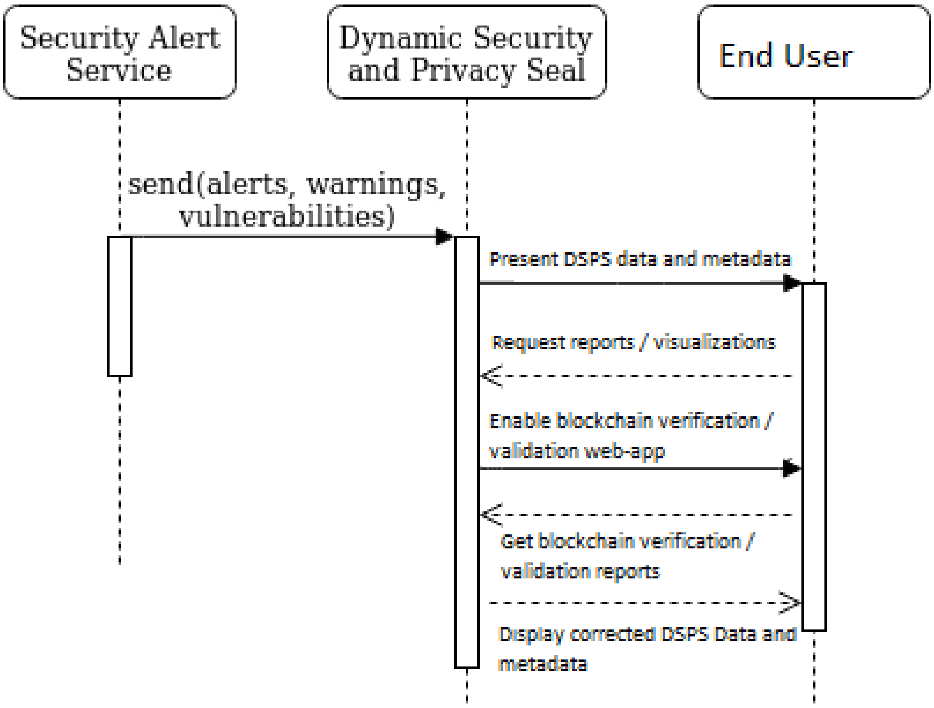

Figure 8 DSPS Sequence Diagram

5.3.3 Blockchain DSPS log creation and verification/validation process

Constituting a fundamental pillar of the DSPS's trust and security, the blockchain DSPS log and the parallel verification and validation process are two of the biggest differentiators of the synthetic model proposed by this deliverable. They permit a transparent, irrefutable, distributed, secure, open and collaborative approach to the task of certifying and logging ANASTACIA's monitoring activities. They introduce the end-user into the equation in a role that goes beyond that of the mere consumer: they not only grant him/her the capacity of independently verifying the validity of the data he is receiving in real time; but also grant the end-user with a new position in the privacy and security ecosystem: an enabler of trust and an impartial privacy and security referee of the systems and services he is interested in using.

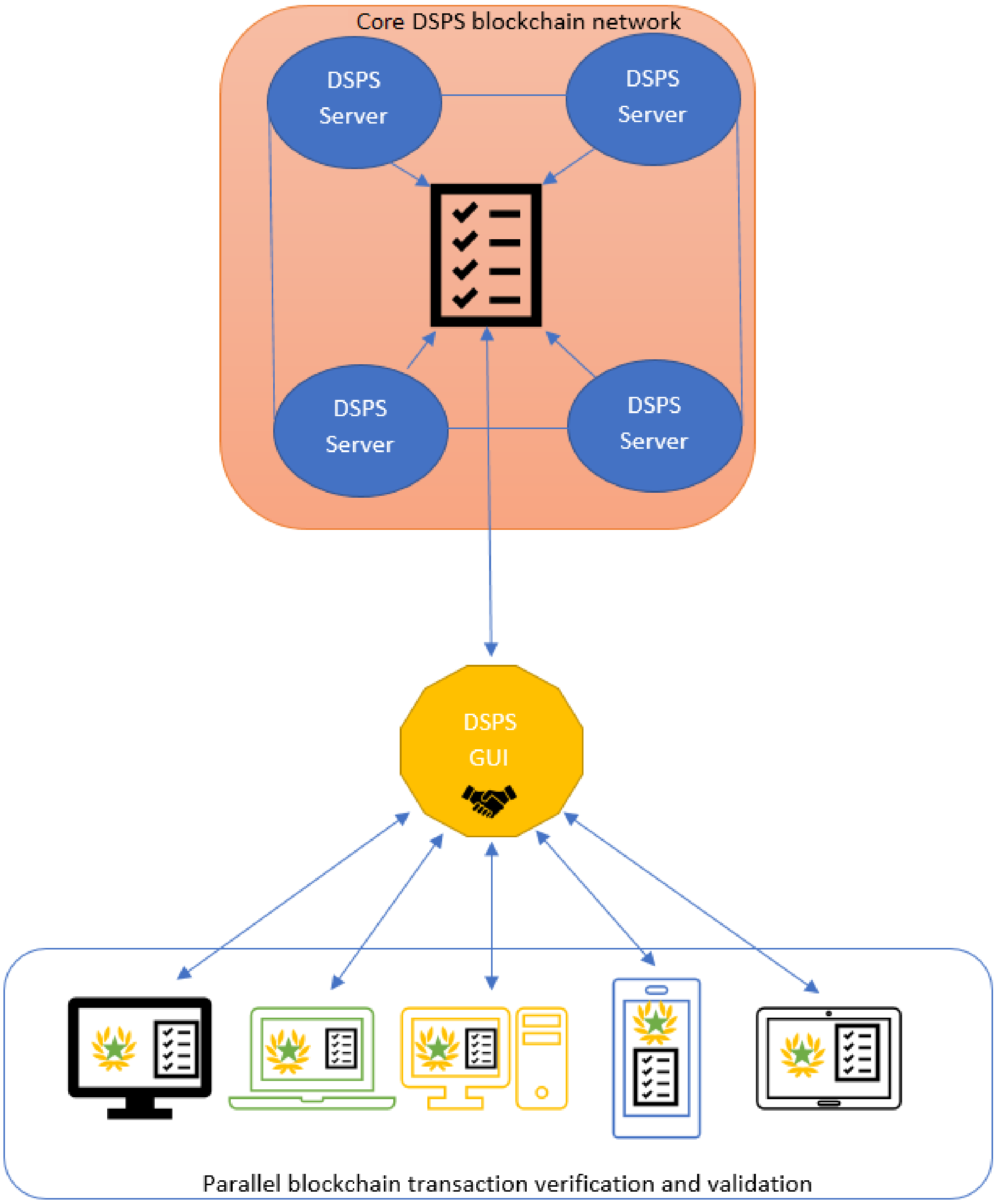

Figure 9 DSPS blockchain log creation and validation process

As detailed by Figure 9, this process involves two main activities:

A) Log creation by the Core DSPS Blockchain Network:

1. Upon receipt of the data from ANASTACIA by a DSPS Server (and the required verification of the authenticity of the data packet / decryption activities), the Server calculates the status of the Dynamic Security and Privacy seal for the monitored system based on the reported information.
2. Once calculated, the updated DSPS status is verified against the monitored system's historic status data available in the DSPS Blockchain Log[40].
3. All relevant information (the status calculations that led to the DSPS update[41] and the latest seal update) is compiled into a block[42].

[40] Recalculation of the seal in function of the system's historic data might be necessary at this point to comply with the Minimum Functionality defined in Section 5.2.1.

4. The block is then broadcasted to the rest of the DSPS Servers of the core blockchain network, which will validate its authenticity.
5. Once validated, the block is then re-distributed through the core DSPS network and to be added to the DSPS blockchain log which contains a consensus-driven, immutable and auditable blockchain of DSPS Status updates[43].
6. The DSPS Blockchain log is made available for end-users and privileged end-users through the DSPS GUI.

B) Parallel verification and validation process through the DSPS GUI

Based on the information available on the DSPS Blockchain log, the DSPS GUI will provide a graphical representation of the DSPS and enable end-users and privileged end-users to access the information generated by ANASTACIA, generating reports and visualizations as necessary. While the requirements for secure communications will be thoroughly implemented by the GUI, an optional parallel verification and validation mechanism will be provided to end-users through which they will be able to voluntarily dedicate their device's unused processing power to the verification of the information received from the DSPS Blockchain log (and secondarily contribute with the validation of DSPS blocks[44]). This process involves the following steps:

1. Once the user or privileged end-user has been properly authenticated and his account has been verified/authorized, he or she will be granted access to the main DSPS GUI, where information and visualization tools will be available in accordance to his/her access level.
2. Both end-users and privileged end-users will be presented by the GUI with a mechanism[45] which will optionally enable a web-app or other similar tool to perform extensive data verification tasks[46] for all the information received from the DSPS Blockchain log and to use any unused processing power or local resources (within reason and only to the extent agreed upon by the user) towards the validation of DSPS blocks and any necessary DSPS data.
    a. For end-users: this mechanism will enable the verification of all data received from the GUI and will contribute to all validation activities in an impartial and non-preferential manner.
    b. For privileged end-users: this mechanism will enable the verification of all data received from the GUI and will enable the privileged user to select whether local resources should be used impartially or if preference should be given to those blocks containing status updates for a DSPS-certified system of their choice.

[41] Supporting data and metadata used for the creation of the seal may be securely stored by the DSPS Servers as defined by supra note 36.
[42] A secure data container identified by a 256-bit hash generated by an algorithm agreed-upon by the network. Blocks are structured in a way that references the previous block's hash to create a sequence of linked hashes, thus enabling the creation of permanent and unalterable links to the blockchain.
[43] *"If a malicious miner [Compromised DSPS Server] tries to submit an altered block to the chain, the hash function of that block, and all following blocks would change. The other nodes [DSPS Servers or DSPS GUI web-apps] would detect these changes and reject the block from the majority chain [DSPS Blockchain log], preventing corruption."(Piscini, Guastella, Rozman, & Nassim, 2016)*
[44] DSPS Servers should be the only elements of the network capable of calculating DSPS status updates. End-user devices which take place in the process through the Dynamic Security and Privacy Seal GUI may only take the role of block validators as their main concern is to verify the validity of the status that is being received from the DSPS (and this task ultimately benefits the DSPS as a whole).
[45] Which might take the form of a popup, card, button, etc. as decided by ANASTACIA tasks 5.2 and 5.3 and in accordance to the requirements for obtaining informed consent.
[46] In case the verification or validation activities lead to the identification of anomalous or malicious behaviour, a report should be immediately submitted to the DSPS Servers for correction/examination by system administrators.

6 ARCHITECTURAL REQUIREMENTS AND CONSIDERATIONS

This section aims to generate a non-comprehensive set of requirements to be addressed by the architectural elements of the DSPS as initial guidance to future research carried out by ANASTACIA tasks 5.2 and 5.3. It includes information gathered from the regulations, recommendations, standards and publications identified thorough supra section 3. Regardless of the initial selection found herein, the implementation team is invited to consider the full range of recommendations and standards identified in section 3.3[47] to ensure the architecture meets all the necessary requirements for ensuring the trustworthy, secure and resilient provision of the DSPS services.

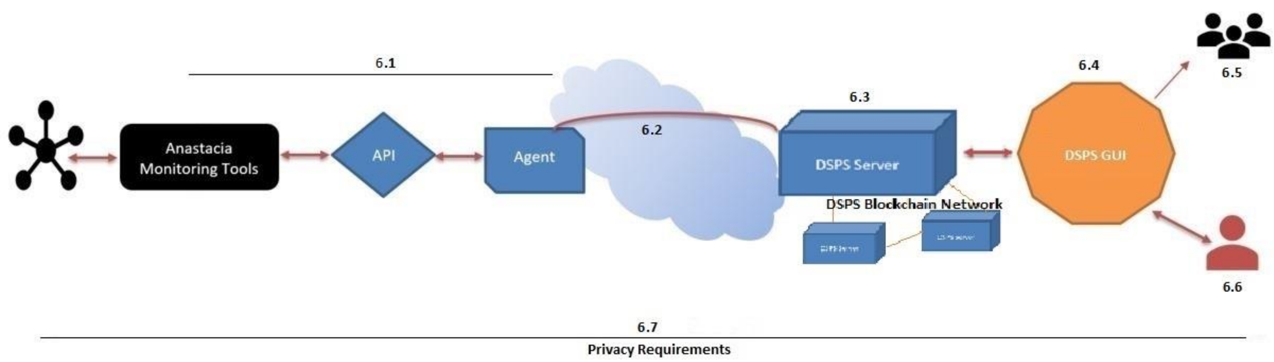

Figure 10 DSPS Architecture Overview for Formal Requirements

6.1 ANASTACIA MONITORING TOOLS API / AGENT

The following requirements have been generated from an examination of the International Telecommunications Union's work on trust provisioning and trusted environments and the eIDAS Regulation (European Council, 2014; International Telecommunications Union, 2017a, 2017b).

Requirement	Considerations for implementation:
Predictability	Every interaction facilitated by the API/Agent shall have a predictable outcome
Systematization	Every interaction facilitated by the API/Agent shall be correctly integrated in the frame of the wider ANASTACIA platform.
Information Security	All transactions taking place through the API shall be secure and transactional logs kept for posterior audit/verification. Access

[47] Particularly the implementation team should consider the requirements found in ISO/IEC 15408 (International Organization for Standardization, 2011a); ISO/IEC 27001 (International Organization for Standardization, 2013a); ISO/IEC 27002 (International Organization for Standardization, 2013b); and ISO/IEC 29100 (International Organization for Standardization, 2011b), the
The set of controls found in (Joint Task Force Transformation Initiative, 2013) can be considered for further clarification of the organizational processes that are to be associated with the development and implementation of the DSPS Servers.

Requirement	Considerations for implementation:
	controls shall be implemented to ensure that only validated programs/agents are able to make use of the API and obtain information from the ANASTACIA Monitoring tools.
Equal reliability	Equal security requirements are to be applied to all programs that attempt to interact with the API/Agent.
Interoperability	The standards (both for data format and transport mechanisms) to be introduced as part of the API/Agent shall enable the exchange of information with a broad range of verified programs while also ensuring the unified nature of the relevant interaction capabilities
Openness:	The standards (both for data format and transport mechanisms) to be introduced as part of the API/Agent shall be open
Data consistency	Requests performed through the API/Agent shall be addressed by the ANASTACIA platform in a consistent manner
Consistency of response delivery	Appropriate responses (either with the successful transfer of the requested data, or a notification of failure/reason of such failure) to such requests shall be guaranteed.
Quality of service	All requests submitted through the API/Agent shall be considered and classified by priority (considering time, nature of the request, etc.) and adequate response shall be provided in accordance to such priority.
System stability:	Special situations notwithstanding, the design of the API/Agent shall be aimed to ensure the stability and reliability of the data flow towards the DSPS agent, as necessary to ensure the accomplishment of the goals of the DSPS.
Unification	Unified forms of information shall be adopted to maximize trust while maintaining the uniqueness of the content that is to be transmitted. An effort shall be made by WP2, WP4 and WP5 implementation teams to adopt unified interfaces of information interaction (by adopting top-of-the-line standards, for example) throughout the Monitoring/Reaction-DSPS process or ensure the easy translation and completeness of the data as needed to meet the requirements of each platform.

Table 7 Formal requirements for the SMMI API / Agent

6.2 SECURE COMMUNICATIONS

Requirement	Considerations for implementation:
Encryption	All communications between the DSPS Servers and the DSPS Agent shall be encrypted to maximize security. The following technical recommendations shall be considered when designing the system: *"• Key management based on Internet key exchange (IKE).* *• Certificate management based on public key infrastructure [b-ITU-T X.509] (PKIX).* *• Certificate management protocol (CMP) (see [b-IETF RFC 2510]) and online certificate status protocol (OCSP) (see [b-IETF RFC 4557]).* *• In the application layer, through the use of TLS (see [b-IETF RFC 4366]) with strong keys.* *It is important to use standards based encryption algorithms and hashes such as DES, 3DES; AES, RSA and DSA (see [b-IETF RFC 2828]). MD5 (see [b-IETF RFC 1321]) and SHA-1 (see [b-IETF RFC 3174]) could be used for message integrity, and Diffie-Hellman (see [b-IETF RFC 2631]) and RSA (see [b-IETF RFC 2828]) for key exchange." (International Telecommunications Union, 2008, pp. 14–15)*
Secure communication channels	• *"VPN techniques using IPSec, with authentication header (AH) and encapsulating security payload (ESP) or tunnelling through the use of layer 2 tunnelling protocol (L2TP)". (International Telecommunications Union, 2008, pp. 14–15)* • SDNS should be implemented

Table 8 Formal requirements for secure communications

6.3 DSPS SERVERS AND CORE DSPS BLOCKCHAIN NETWORK

The following requirements have been generated out of a comparison of the functionalities expected from the DSPS Architecture, the Critical Security Controls for Effective Cyber Defence identified by ETSI (European Telecommunications Standards Institute, 2015) and the IoT Framework Assessment prepared by OWASP (Miessler, Smith, Keane, & Yunsoul, 2017). This list does not aim to be exhaustive, as additional requirements (and/or further specification of the current requirements) might be necessary as the architectural elements found in infra section 7.3 are developed by ANASTACIA Task 5.2.

Requirement	Considerations for implementation:
Application software security	Security design and coding principles shall be implemented by the network in order to ensure end-to-end security and to ensure the integrity of any applications developed or introduced in the system. This element includes such requirements as:

Requirement	Considerations for implementation:
	• Application authentication (to ensure the security of their sources) • Consistency checking • Internal logging and monitoring of applications/processes • Interoperability • Message authentication • Reset mechanisms and safety mechanisms to enable fall back to a secure software version in case of error • Secure operating system • Software and app isolation • Software protection and maintenance (software life-cycle management) • Vulnerability handling
Authentication	The DSPS Server shall implement access enforcement and account management tools including those required to: • Enable or terminate remote sessions • Ensure non-repudiation of administrative events • Grant and revocate access authorizations • Lock and terminate sessions • Prevent privileged access by non-organizational or non-privileged users to restricted areas • Terminate connections following a predetermined number of login attempts Additionally, strong authentication mechanisms shall be implemented including: • Username/password authentication with configurable levels of complexity. The highest possible levels should be introduced and vulnerable passwords prohibited by the system. • Salted / hashed storage of passwords • Two-factor authentication should preferably be used (Further information on this requirement can be found in section A.9 Access control of (International Organization for Standardization, 2013) and in the relevant sections of (Joint Task Force Transformation Initiative, 2013)).
Authorization	The DSPS Servers shall be capable of generating an inventory of authorized and unauthorized devices, software/processes and users to take preventative/responsive measures to ensure the inventory is respected. This requirement extends to the need to ensure that the DSPS Servers are capable of meeting all the necessary Authorization requirements of the DSPS GUI, so as to ensure the secure and accurate identification of end-users and privileged end-users, and to account for the privileges/functionalities available to each.

Requirement	Considerations for implementation:
Availability	Physical and logical measures should be implemented to ensure the DSPS Servers are to be available and capable of providing their service on a permanent basis. This requirement includes such elements as: • Autonomic service provisioning • Backup power, fire suppression, and other physical measures. • Updatability and service life-cycle management, so as to ensure these elements do not conflict or affect with service availability
Verification and Validation (Blockchain)	• Consensus model: to be defined and implemented in the DSPS Servers for registering of new events and/or transactions to the log. Care should be given to ensure that all nodes (Servers + nodes running on DSPS GUI) are able to carry out verification and validation activities. • Cryptographic (hash) functions: Properly implemented to ensure they are irrefutably linked to the transaction that is being recorded on the DSPS Log • Digital signatures (on the DSPS Servers-side) to enable end-users and privileged user verification of the validity of the transactions (status received from the servers)
Boundary defence / continuous vulnerability assessment and remediation	Control of internal and external network traffic should be implemented by the DSPS Servers so as to minimize possible attack vectors. In addition to this element, network traffic should be carefully observed by automated mechanisms capable of identifying possible attacks/vulnerabilities and of addressing these vulnerabilities automatically.
Configurability	The DSPS Servers shall be configurable to comply with the constraints or the requirements not mentioned or defined in this document. A high configurability avoids developing specific versions of the DSPS Servers to meet specific needs.
Data protection	The DSPS Server shall introduce constant data protection mechanisms to ensure all data (including personal data) remains under its control. This element includes, among other elements: • Confidentiality checks • Data assessments and classification • Data integrity checks • Encryption checks
Redundancy and Data recovery capability	Servers in the Core DSPS blockchain network shall introduce extensive data recovery capabilities based on redundant hardware and data recovery solutions/processes.
Effectiveness	The DSPS Servers shall be designed and programmed in such a

Requirement	Considerations for implementation:
	manner as to enable the effective processing of information that is necessary to meet the goals and minimum functionalities required of the DSPS.
Encryption	*"• Certificate management based on public key infrastructure [b-ITU-T X.509] (PKIX). (…) It is important to use standards based encryption algorithms and hashes such as DES, 3DES; AES, RSA and DSA (see [b-IETF RFC 2828]). MD5 (see [b-IETF RFC 1321]) and SHA-1 (see [b-IETF RFC 3174]) could be used for message integrity, and Diffie-Hellman (see [b-IETF RFC 2631]) and RSA (see [b-IETF RFC 2828]) for key exchange." (International Telecommunications Union, 2008, pp. 14–15)* Additional information and recommendations for implementation of this requirement can be found in the following sources: • GDPR: Art. 32 • ISO/IEC 27001:2013: Related indications in 8.2; 8.3; Annex A • ITU-T X.1171: Related indications in 10.6 • ITU-T X.805: Related indications in 6.8 • ITU-T Y.2060: Related indications in 7.2 • ITU-T Y.2066: Related indications in 7.5 / 7.7 / 8.8 • NIST IR 7628 R1: D-3.7 • NIST SP 800-122: 4.2.1 • NIST SP 800-53 R4: Related indications in Appendix J: AR-7 • Ordinance to the Federal Act on Data Protection (OFADP): Arts. 21, 32, 34
Extensibility	The DSPS Server shall be sufficiently modular and include a certain number of configuration tools that allow adding features and fine-tuning the current configuration of the server.
Incident response and management	Each detected incident shall be reported and the DSPS Server shall answer automatically to each identified incident. Each incident shall be reported and managed by the DSPS Server.
Malware defences	The DSPS Server shall put in place all the measures to avoid the installation of malware on the system.
Minimum service	The DSPS Server shall be designed in a way that ensures the constant provision of the minimum functionalities described in Section 5.2.1, and to achieve the objectives of both ANASTACIA and the DSPS.
Secure baseline configurations	By default, the basic configuration takes care of the security. For example, HTTPS is enabled by default.
Secure network engineering	The Core DSPS blockchain network shall be designed in a way that respects the security design and coding principles and provides end-to-end security. Particularly, the following elements shall be considered when designing the network:

Requirement	Considerations for implementation:
	• Device integrity and identification • Life cycle management of all elements in the network (including inventory management) • Minimum functionality (only documented and necessary functionality should be provided by the network) • Secure communication channels: Implementation of network isolation and restrictive communications (only enable documented and necessary communications through a secure channel)
System logs and auditability	The each DSPS Server shall, at minimum, generate internal logs for: • Record access/flow control rules related to an event • Record administrators tied to any change in the system • Record event descriptions • Record event-associated filenames • Record event-specific results • Record source and destination addresses • Record success / fail indicators • Record time stamps • Record user / process identifiers There should be no possibility of deletion or modification of the content of the log files and any access to these files should be logged/monitored. Automated reports/alerts on the status of the system should be generated through the processing of these files.

Table 9 Formal requirements for DSPS Servers

6.4 GUI and Blockchain Verification / Validation Web App

The following requirements have been identified through initial discussions with the leaders of ANASTACIA Tasks 5.2 and 5.3. Further specification of these requirements throughout Task 5.3 is highly recommended.

Requirement	Considerations for implementation:
Accessibility	Implement the accessibility guidelines of ISO/IEC 40500:2012, including but not limited to: • Alternative display methods for content • Alternatives for time-based media • Implementation of keyboard-based operation • Text alternatives for any non-text content
Consent revocation	A consent-revocation mechanism should be prominently displayed in the GUI and exercise of this right by the user should not only immediately suspend the local process, but also purge any information remainders from the host machine.

Requirement	Considerations for implementation:
Data and process visualization	Both the DSPS real time data and the data related to the verification and validation processes running on the end-user side shall be presented to the user in a way that enhances his understanding of the information and maximizes transparency
Ease-of-use	The GUI and blockchain verification/validation web app shall be designed in a way that maximizes ease-of-use and minimizes the steps necessary for a user to access the relevant information. Additionally, multimedia guides shall be generated and prominently displayed by the system in order to minimize the learning curve.
Language/internationalization	An effort shall be made to present all GUI and blockchain verification/validation web-app contents to the user in his/her local language.
Minimal input (particularly relevant for the verification/validation web app)	The verification/validation web app shall be designed in a way that minimizes the necessary input for the user. Simply put, once the user has granted consent for the local execution of the process, integration of the app in the GUI should be seamless and present all relevant information by default.
Platform neutrality	The GUI should be designed in a way that is flexible enough to present the content accurately in diverse platforms. Web standards for mobile content should be implemented and device limitations considered in order to optimize navigation. Known hazards and excessive network usage requirements should be avoided, so as to facilitate access to the content by users with low-bandwidth connections or using mobile platforms. See (World Wide Web Consortium, 2016)

Table 10 Formal GUI requirements

6.5 END-USER ACCESS MECHANISMS AND FUNCTIONALITIES

The following requirements have been identified through initial discussions with the leaders of ANASTACIA Tasks 5.2 and 5.3. Further specification of these requirements throughout Task 5.3 is highly recommended.

Requirement	Considerations for implementation:
Accessibility	For UI (e.g. web dashboards), accessibility guidelines will be taken into consideration (e.g. https://www.w3.org/WAI/intro/wcag)
Security	All transactions taking place through the GUI shall be secure and transactional logs kept for posterior audit/verification.
Blockchain verification and validation	A temporary node of the DSPS Blockchain network should be generated through a web-app designed as part of the GUI aimed at performing verification tasks of the information

Requirement	Considerations for implementation:
	received from the DSPS log and validation of the DSPS blocks, through the use of the user's local resources.

Table 11 Formal requirements for secure end-user access

6.6 Privileged User Access Mechanisms and Functionalities

The following requirements have been identified through initial discussions with the leaders of ANASTACIA Tasks 5.2 and 5.3. Further specification of these requirements throughout Task 5.3 is highly recommended.

Requirement	Considerations for implementation:
Accessibility	For UI (e.g. web dashboards), accessibility guidelines will be taken into consideration (e.g. https://www.w3.org/WAI/intro/wcag)
Security	All transactions taking place through the GUI shall be secure and transactional logs kept for posterior audit/verification. Access controls shall be implemented to ensure that only validated privileged users are able to make use of privileged functionalities and gain access to the specific logs obtained from ANASTACIA.
Blockchain verification and validation	A temporary node of the DSPS Blockchain network through a web-app in the GUI aimed at performing verification tasks of the information received from the DSPS log and validation of the DSPS blocks, through the use of the user's local resources. In accordance with the specific privileges granted to the user and any relevant contractual terms, the Web-App should enable the prioritization of processing of data relating to any system defined by the end-user.
Reporting	Reporting functionalities shall be implemented to enable privileged users to obtain reports on 1) detected attacks, 2) affected items, 3) defined mitigation plans, 4) implemented mitigation actions and 5) potential privacy breaches based on the contents of the DSPS log.

Table 12 Formal requirements for secure privileged user access

6.7 Personal Data Protection Requirements

The following requirements are based on the original table of Personal Data Protection Requirements specified in ANASTACIA deliverable 1.3 (Trapero et al., 2017, p. 12), and have been further specified to better meet the context and functionalities available in the DSPS.

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
Anonymization and pseudonymisation of personal data	DSPS Servers / End-user GUI / Privileged User GUI	Non-privileged end-users may use the DSPS GUI and any tools available to them in a completely anonymous manner and/or to create pseudonymized accounts.
Appropriate retention period	DSPS Servers	The default personal data retention period is set at one (1) month, without prejudice to other conflicting legal

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
		obligations, which will be appraised on a case by case basis on motivated request by the data controller (e.g. in case of different retention period for internet traffic data mandated by specific law on detection and prevention of crime). The exceptions to the one-month retention policy set above may derive from the implementation of Article 15(1) of the ePrivacy Directive (Directive 2002/58/EC) at national level. Such Directive provides that: "Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period" when it is necessary to safeguard "national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".
Authentication of identities	DSPS Servers / Privileged User GUI	Pursuant to GDPR Articles 28 and 29, persons acting under the authority of the controller or the processor shall process personal data on instructions from the controller. This requires, first of all, that they must have individual authentication credentials composed by a personal ID code and a secret password with at least eight characters; if this is not allowed, the password shall consist of the maximum permitted number of characters and it shall not contain any item that can be easily related to the person in charge of processing. It shall be also modified when it is first used as well as at least every six months, thereafter. Alternatively, these credentials shall consist in an authentication device that shall be used and held exclusively by the person acting under the authority of the controller or the processor or in a biometric feature (possibly, in both cases, associated with either an ID code or a password). The whole system will collect different types of data and it will be designed to ensure the privacy and trust of the users. In order to do this, each identity accessing the system will be authenticated and appropriately authorised to be able to use it. Where necessary (e.g. when the system is used to process health data), strong authentication (e.g. two-factor authentication, double opt-in, biometric recognition, etc.) methods must be supported.
Authorization	DSPS Servers / Privileged user GUI	Before the start of the processing, it is necessary to enable access to the data that are needed to perform processing operations, setting out an authorization

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
		profile for each person/homogeneous set of persons acting under the authority of the controller or the processor. Authorization profiles will be set out and configured prior to start of the processing so as to enable data controllers' access only to the data that are necessary to perform processing operations. It will be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorization profiles still apply. The DSPS Servers will work on the basis of a list of persons acting under the authority of the controller or the processor to identify categories of tasks and corresponding authorization profiles.
Data accuracy and updating	DSPS Servers / Privileged user GUI	Personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified. The normative base of data accuracy and updating is Article 5 (1) point (d) of the GDPR which states: "[…] personal data shall be: […] d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate, having regard to the purposes for which they are further processed, are erased or rectified without delay […]".
Data back-ups	DSPS Servers	Back-up operations will be carried out periodically, so as to ensure the continuity of the system and prevent the loss of data. Back-ups for each DSPS element will be maintained, in order to ensure the maintenance and the continuity of information and complete traceability of each activity.
Data breach information	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects. The legal source of this requirement is found in Articles 33 and 34 of the GDPR. Information about the breach can also be provided through the GUI of the DSPS.
Data management	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS Servers must automatically record all internally generated data, securely storing these data, while minimizing the collection of personal data. It shall be designed so as to support interfaces, at application level,

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
		that allow users to control the data processing taking place within the platform.
Data Portability	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS system must be able to support the data controller in responding to requests for data portability lodged by the data subjects. This entails that the data subject shall receive the data in a structured, commonly used and machine-readable format. This obligation stems from Article 20 of the GDPR. The capacity of a system to make data portable to another system needs interoperability as a prerequisite.
De-activation of authentication credentials	DSPS Servers	Personal authentication credentials shall be de-activated if they have not been used for at least six months (except in case of technical authorization). The DSPS Servers will periodically check if more than six months elapsed since the last log in of each person acting under the authority of the controller or the processor and disable its credentials if usage requirements are not met. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data. The objective is to guarantee that persons acting under the authority of the controller or the processor can only access and process personal data if they are provided with authentication credentials. The credentials are necessary for the appointed person to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.
Encryption by default	API / DSPS Agent / Secure Communications / DSPS Servers / End-user GUI / Privileged user GUI	Encryption will be applied to all stages of handling data, including in communication, storage of data at rest, storage of keys, identification, access, as well as for secure boot process.
Protection of traffic information and data		Traffic information and data compiled as part of the validation and verification activities of the DSPS (particularly as generated by the DSPS Blockchain Log) shall be minimized and pseudonymized/anonymized and shall not be kept for longer periods than as required to ensure the correct functioning of the DSPS.
Purpose limitation	DSPS Servers	The DSPS will process personal data only for security purposes, unless the data controller configures the system to pursue other legitimate, specific and explicit

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
		purposes, determined at the time of collection of the data. This requirement implements the purpose limitation principle set forth by Article 5 (1) point (b) of the GDPR. Moreover, the Art. 29 WP has provided an in-depth analysis of this principle in its Opinion 03/2013 on purpose limitation.
Regular Monitoring of Security	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS architecture will regularly monitor the system's status in terms of security for personal data. The system will be able to provide real time information on the level of security, also through the Dynamic Privacy and Security Seal. This obligation stems from Article 32 of the GDPR, which requires controllers and processors to implement measures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
Right of access	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS system shall support the data controllers in providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. The legal source of this requirement is Article 15 of the GDPR.
Right of erasure	DSPS Servers / End-user GUI / Privileged User GUI	The DSPS system must ensure that the right of erasure exercised by data subjects towards the data controller is enforced, when the conditions set out by law are met. The assessment must be performed by the data controller; personal data shall be erased if one of the criteria listed below is applicable: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject has withdrawn the consent on which the processing is based, and where there is no other legal ground for the processing; (c) the data subject objects to the processing on grounds relating to his or her particular situation, and there are no overriding legitimate grounds for the processing; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. This obligation stems from Article 17 of the GDPR, which in

Requirement	Particularly concerned element of the DSPS Architecture	Considerations for implementation:
		turn builds upon Article 12 of Directive 95/46/EC.
Security of processing	DSPS Servers	Personal data will be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. As defined by Article 32 of the GDPR, as part of the security of the processing, both controller and processor must "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudo-anonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."
User data management	DSPS Servers / Privileged User GUI	In case of personal data collection, the system enables users to control their personal data, to access, rectify, delete or block them. It is always possible, for the users, to change the sets of data that they have shared. The idea is to allow users to control their interaction with the project by revealing only the information they want to disclose and changing at any time the set of shared data. It is a user-centric approach that means that users have the power to play an active role in the management of their personal data. This may include the realization of a dashboard whereby the user may always keep control on the overall processing of his/her personal data.

Table 13 Formal requirements for Personal Data Protection (Trapero et al., 2017)

7 DETAILED SEAL ARCHITECTURE

The trust-enhancing activities intrinsic to the DSPS will be provided through its integration with the broader ANASTACIA tools and a separate and dedicated architecture/infrastructure which will secure and support the authentication and verification activities that are fundamental to the Seal itself. This architecture will implement privacy and security enhancing technical safeguards at its various levels, adopting the privacy (and security) by design and by default approach in accordance with the normative and technical frameworks noted in Section 3.

Synthetically speaking, the DSPS Architecture consists of: the ANASTACIA monitoring tools (including its Application Programming Interfaces (API) and the DSPS Agent); a secured communications channel; the DSPS Servers that conform the Core DSPS blockchain network, the DSPS Graphical User Interface (GUI), and two secured access mechanisms for end-users and privileged users. These elements can be identified in Figure 6 and their interactions and particularities will be detailed in the following subsections.

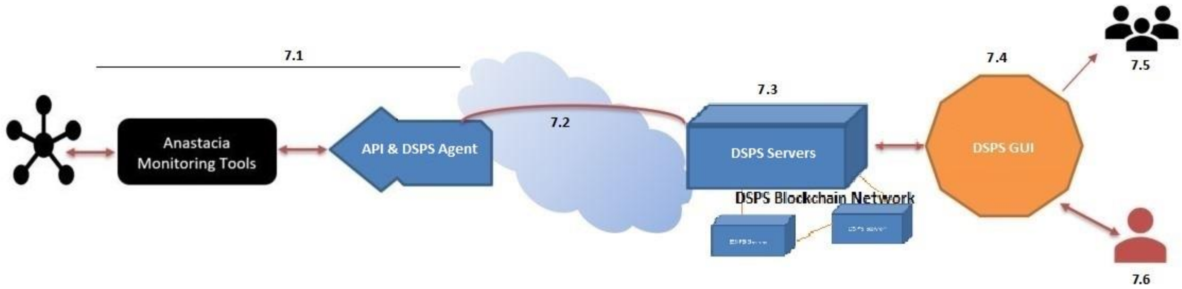

Figure 11 DSPS Architecture Overview

7.1 ANASTACIA MONITORING TOOLS, API AND DSPS AGENT

The Seal Management Plane of ANASTACIA will be in charge of computing the value of the Privacy and Security Seal. This process will make use of information provided by the Monitoring and Reaction Plane[48]: a set of data generated by the same Reaction Module (the set of suggested countermeasures and the alerts and warnings generated), and the Security Orchestrator (the capabilities – security enablers – the orchestrator can use and the set of applied countermeasures in the network, which might include an historical log of the applied mitigation actions against the encountered attacks).

In this context, ensuring the correct integration between the broader set of Monitoring and Reaction tools that are part of ANASTACIA and the DSPS is a fundamental objective of this section. This integration must take place on two fronts: The API to be facilitated by the ANASTACIA Monitoring Tools (the Seal Manager Metadata Interface) and the DSPS Agent that will interact with this API to ensure the data is dully formatted and communicated correctly, timely and securely to the DSPS Servers.

[48] Initial discussions with WP4 have led to fruitful possibilities for future integration, which should be explored further by ANASTACIA Task 5.2 Among other activities, Task 5.2 will be required to further specify the SMMI API, the possible level of implementation of STIX by both WPs and a method to process low level data into usable information for the Seal Creation Process. For more information see supra note 51.

7.1.1 Seal Manager Metadata Interface (SMMI)

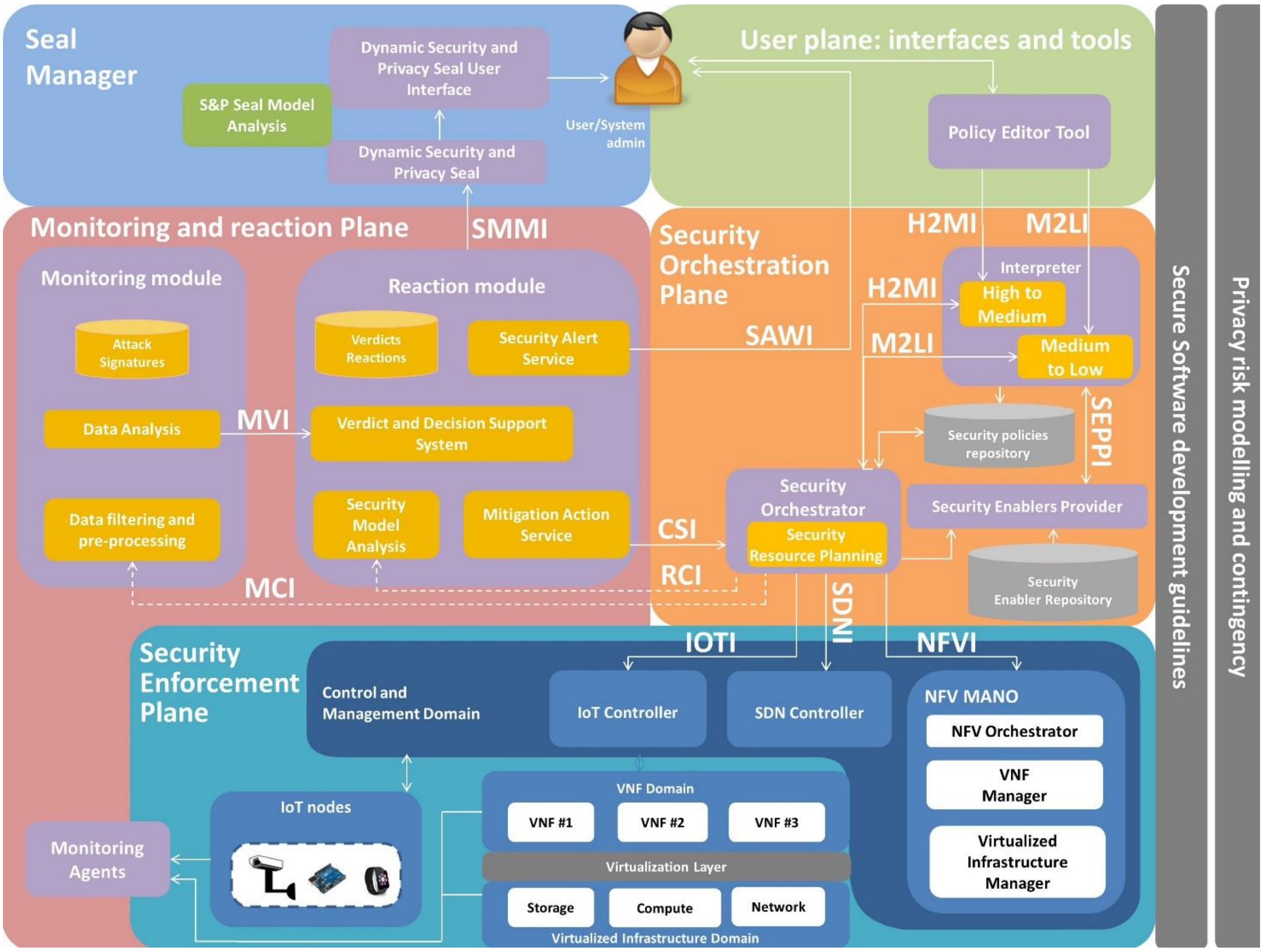

Figure 12 ANASTACIA Interface Overview as detailed in deliverable 1.3 (Trapero et al., 2017)

As detailed by ANASTACIA deliverable 1.3, interfaces for seal creation, a Seal Manager Metadata interface (SMMI) will be used for the exchange of the relevant data that the seal manager needs to create the Dynamic Security and Privacy Seal. The general characteristics of this interface have been continuously updated throughout discussions between WP5-WP4 and the resulting elements can be found in Table 14:

Seal Manager Metadata Interface (SMMI)	
Description	The interface provides the requested information to evaluate the security and the privacy in a real-time fashion. The security and privacy policies defined by the user are stored inside the policies repository and an interface is available to retrieve and set them from the seal manager.
Component providing the interface	Dynamic Security and Privacy Seal
Consumer components	Security Alert Service, Security Model Analysis
Type of Interface	RPC// JSON
State	Asynchronous

Input data: Alerts, warnings, vulnerabilities, MSPL-based capabilities	**Methods or endpoints** of the interface	**Parameters of the** method	**Return Values of the** method
	computeSecuritySeal	To be defined by Task 5.2 with WP4	none
Output Data	none		
Constraints	To be specified through task 5.2		
Pre-conditions	A security policy must have been set-up in the monitoring and reaction modules and enforced in the IoT platform		
Post-conditions	(Not applicable)		
Responsibilities	○ ATOS ○ AS ○ MONT		

Table 14 ANASTACIA Seal Manager Metadata Interface (SMMI) initial definition

In accordance with the data currently available from other ANASTACIA WPs the SMMI API will provide: a) information provided by the ANASTACIA monitoring and reaction plane, which will convey the security alerts and reactions (particularly as pertaining to any security and data protection breaches that have been identified); and b) information on currently applicable policies as compiled by ANASTACIA WP4 from ANASTACIA WP2. While the specific implementation characteristics of this API are still to be defined by the relevant WPs, at this point it is possible a list of general criteria for the design and implementation of any such interfaces. Such criteria have been listed as a set of formal requirements in section 6.1 and their implementation by ANASTACIA Task 5.2 should be aimed towards the creation of an interoperable and trusted[49] environment (particularly among WP5 and WP4).

In consideration of these formal requirements, the selection of an appropriate threat information sharing standard will have a high relevance for the successful development of the APIs and the DSPS Agent. And while it is acknowledged that the selection of the most viable standard will ultimately lie on the conditions found by the implementation team (both for WP4 and WP5 tasks), several threat information sharing standards (aimed at both data formatting and data transmission) have been identified as potentially relevant to the ends and purposes of the DSPS. In this context, the following standards have been found to be especially promising, and as such their pros and cons should be considered with care by the implementation teams before making a final decision:

a) **Incident Object Description Exchange Format (IODEF) and Real time Inter-network Defence (RID)**
These two standards developed by the Internet Engineering Task force are aimed towards enabling the exchange of intrusion detection and response data among the various IT systems responsible for the prevention of such events. While IODEF defines *"a data representation for security incident reports and indicators commonly exchanged by operational security teams for mitigation and watch and warning"(Internet Engineering Task Force (IETF), 2016)* and is capable of providing a XML representation for conveying *"indicators to characterize a threat; security incident reports to document attacks against an organization; response activity taken or that could be taken in response to an incident; and metadata so that these various classes of information can be exchanged among parties."(Internet Engineering Task Force (IETF), 2016, p. 5)*; RID *outlines "a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution." (Internet Engineering Task Force (IETF), 2012, p. 4)*.
Both of these standards are completely interoperable, as *"RID provides a secure method to communicate incident information, enabling the exchange of Incident Object Description and*

[49] "Trust is the level of confidence in the reliability and integrity of an entity to fulfil specific responsibilities. The identification of involved entities or at least the verification of their attributes is a prerequisite to achieve trust." (European Telecommunications Standards Institute, 2016, p. 15)

Exchange Format (IODEF) [RFC5070] Extensible Markup Language (XML) documents [which] considers security, policy, and privacy issues related to the exchange of potentially sensitive information [while including] provisions for confidentiality, integrity, and authentication" (Internet Engineering Task Force (IETF), 2012, p. 4).

b) **Structured threat Information Expression (STIX) v.2.0 and Trusted Automated eXchange of Indicator Information (TAXII) v.2.0**

Developed originally by the MITRE Corporation and currently in its second version under the OASIS consortium, STIX is a standardized XML programming language and serialization format which provides a mechanism for addressing structured cyber-threat information while supporting *"four cyber threat use cases: analysing cyber threats, specifying indicator patterns, managing response activities and sharing threat information"(Farnham & Leune, 2013)*. "*In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information including: cyber observables, indicators, incidents, adversary tactics, techniques and procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, targeting, etc.), exploit targets (…), courses of action, cyber attack campaigns, (and) cyber threat actors"(The Mitre Corporation, 2012, p. 5)*.

In order to facilitate transport of STIX data, MITRE also developed TAXII, an *"application layer protocol for the communication of cyber threat information in a simple and scalable manner"(OASIS, 2017b)*. *"TAXII defines two primary services, Collections and Channels, to support a variety of commonly-used sharing models. Collections allow a producer to host a set of CTI data that can be requested by consumers. Channels allow producers to push data to many consumers; and allow consumers to receive data from many producers"(OASIS, 2017a)*.

In order to advance the consideration of these potential standards, two comparison charts containing summary information are presented below:

	IODEF	STIX 2.0
Latest version:	December 2007	June 2017
Content	XML Large number of classes and sub classes to define incident data	JSON (XML in v.1.0) Defines twelve STIX Domain Objects (SDOs): Attack pattern, campaign, course of action, identity, indicator, intrusion set, malware, observed data, report, threat actor, tool and vulnerability
Adoption	Non-region-specific, CSIRT adoption recommended by IETF publications	US-Centric, Industry driven
Additional features	Extensions have been developed to expand its capabilities and convey enriched cybersecurity information (Internet Engineering Task Force (IETF), 2014)	Iterative development, open-source and free
Pros	Has been previously considered by ANASTACIA partners (Particularly WP3). Adopted by CSIRTs.	Currently used by ANASTACIA WP4 Wider industry adoption and possibility for future integration/exploitation Human-friendly structure and format, can be used manually or programmatically
Cons	Complicated XML syntax – not human friendly	Might require development of extensions to convey ANASTACIA-specific information

Table 15 IODEF / STIX Comparison chart

	RID	TAXII 2.0
Latest version:	April 2012	June 2017
Message content and transport:	HTTP/TLS	XML and HTTP/HTTPS Allows for custom formats and protocols, however it is designed with specific aim to support STIX 2.0
Services:	Five message types: request, acknowledgement, result, report and query	Four core services with distinct functionalities: Discovery, feed management (subscribe, unsubscribe, pause, delivery, resume delivery, modify subscription, status query), Inbox, Poll.
Additional features:	Includes policy class based on relationship with sharing partners	Includes mechanisms for confidentiality, integrity and attribution Supports multiple sharing models and push/pull transfer of data Implemented by major industry players (Microsoft, Symantec, NIST, DTCC, NATO, World Bank, etc.)
Pros	High security level provided	Large number of features
Cons	Limited scalability (appropriate for point-to-point systems	Complexity might increase interoperability challenges Backers are mainly US-centric

Table 16 RID/TAXII Comparison chart

Upon initial discussions with WP4, a proposal to adopt STIX as the format standard to be used by the DSPS has been approved. Further work on API Specification remains to be pursued throughout Task 5.2, which shall also consider the possibility of developing a STIX extension if necessary to convey ANASTACIA-specific information.

7.1.2 DSPS Agent

Acting as the first line of direct integration of the DSPS to the SMMI facilitated by ANATACIA's Monitoring Tools, the DSPS Agent will be directed towards:

a) Performing automated requests for data to the ANASTACIA Monitoring/Reaction and Policy APIs on behalf of the DSPS Servers in a timely manner, so as to ensure minimum possible latency between status/alert/policy changes and the modification of the DSPS[50].
b) Integrating the asynchronous data packages provided by the APIs into a unified and coordinated (timestamped) dataset for further processing.
c) Initial processing of the data obtained from WP4 to generate the information necessary for Seal Creation[51].

[50] This item has also been recognized as a fundamental objective of the ANASTACIA architecture by D. 1.3, which stated *"NFR-11 Performance (response time/ throughput) – the ANASTACIA system will monitor ICT infrastructure in real time and will immediately notify detected threats and potential privacy breaks, independently from the number of monitored devices"*

[51] Currently it has been determined that WP4 can provide WP5 with access to low-level data regarding the measurements and actions undertaken by ANASTACIA. Task 5.2 will include further coordination activities aimed at designing a process to be carried out by the Agent, which will aim to convert the provided measurement data to the required information for the Seal Creation Process, including:

- Security breach / intrusion alerts
- Description of the breach
- Timestamp

d) Translating any unformatted (or not format-compliant) event/threat data into a DSPS-ready language and serialization format for cyber threat intelligence.
e) Compiling the data into a verified and encrypted container for transmission to the DSPS Servers and ensure the parallel transmission of verification information (HASH function, etc.).
f) Receiving data packages (containing requests for additional data, privileged user requests for policy updates, etc.) from the DSPS Servers, verifying their authenticity, translating the information (if necessary), and relaying the requests contained therein to the APIs of the ANASTACIA Monitoring Tools.
g) Performing self-assessments and submit periodical reports to the DSPS Servers on its own stability and security (heartbeat), along with assessments of the communication channels (measure data loss, encryption/decryption errors, measure connection time, etc.) in order to maximize trust and protect the DSPS Architecture from potential vulnerabilities/attacks.

As a whole, the DSPS Agent shall contribute to the overall security of the DSPS architecture (by performing local verification of the encrypted data, ensuring its response only to secure connections from authenticated DSPS Servers queries, preventing unknown and/or unauthorized data streams to/from the DSPS Servers, etc.) while contributing to the extension of the potential impacts and outreach potential for ANASTACIA by serving as a translator of the cyber threat information into a language / communication standard that is widely adopted by the broader IT Security Industry. For these reasons, development and implementation of the DSPS Agent shall comply with the formal requirements identified in section 6.1, and just as with every other element in the DSPS architecture, its development shall follow the privacy and security by design principles.

7.2 Secure Communications

In the broader frame of implementation of the DSPS, maintaining the security of communications is highly relevant to ensure trust in the Seal. *"The objective of securing network traffic is to ensure the confidentiality, integrity and accuracy of network communications."(International Telecommunications Union, 2008, p. 14)*. All communication between the DSPS Agent and the DSPS Servers shall meet two main requirements (beyond those specified by the transport standard to be implemented) to ensure that top of the line security is provided to the transmitted data.

The first of these requirements relates to the need to implement end-to-end encryption, which makes use of secure cryptographic principles and key management practices, standardized and proven encryption protocols, a trusted root authority and correct implementation of the encryption mechanisms throughout the communications architecture (both through the transport and application layers and at both ends of the communication channels). The second of these requirements fundamentally requires the use of trusted and secure communication channels which are fail-safe and/or redundant to ensure service continuity. As such, communications between the DSPS Agent and the DSPS Servers shall take place only through a dedicated virtual private network connection (to further protect the data packages from potential interception/replication) and (whenever possible) verification data (encryption keys, HASH functions, security parameters, etc.) should be submitted through the redundant/secondary secure connection to maximize system and data security.

These two fundamental security measures shall be implemented to protect all communications vis-à-vis known attacks and vulnerabilities. Implementation of additional measures to maximize communications

---

- Attacked/affected system
- Impact of breach (major/minor)
- End of breach notification
- Current policies
- Etc.

security (including but not limited to: DDoS protection, man-in-the middle protection, introduction of secure name/address resolution services, use of transport layer security, coordinated and secure transmission of security parameters, resilience against compromised nodes, etc.) is also recommended in both sides of the communication network in a way that is correctly integrated with existing systems and does not affect the normal use of the ANASTACIA Monitoring Tools.

Finally, all communications that take place throughout the DSPS Architecture are to be designed with the goal of maximizing their potential scalability, availability, quality of service, efficiency, interoperability and interoperability while minimizing risk and response time. All of these objectives are to be implemented and communicated to the user as necessary to maximize trust in the system.

7.3 DSPS Servers And Core DSPS Blockchain Network

Due to its key role in the DSPS Architecture, the DSPS Servers shall be developed as an especially secured and robust IT system. As such, it shall consider and implement the full range of requirements (NFRs) identified by the ANASTACIA Initial Architecture Design (Trapero et al., 2017) along with the requirements identified in supra section 6.3, particularly those regarding availability, backup, configurability, effectiveness, extensibility, interoperability, performance, reporting, scalability and security.

ID	Name/Description (Trapero et al., 2017)	Priority*
NFR-1	**Accessibility** – as for UI (e.g. web dashboards), accessibility guidelines will be taken into consideration (e.g. https://www.w3.org/WAI/intro/wcag)	LOW
NFR-2	**Availability** – the ANASTACIA system will be available 24/7	MEDIUM
NFR-3	**Backup** – the ANASTACIA system will include automatic configurable back-up procedures and associated storage facilities for all relevant data (e.g. security and privacy configurations, mitigation plans, SDN configurations, VNF deployments, etc.)	MEDIUM
NFR-4	**Capacity** – the ANASTACIA system will have to manage a minimal set of <*N*> devices (to be defined at pilot level)	MEDIUM
NFR-5	**Certification/Compliance (PRIVACY)** – as for the internal processing of information, the ANASTACIA system will be compliant with the GDPR as for the identified Privacy Requirements	HIGH
NFR-6	**Certification/Compliance (SECURITY)** – the ANASTACIA system will adopt the *de facto/de iure* standards as for security protocols to use as for internal communication/interfaces	HIGH
NFR-7	**Configurability** - the ANASTACIA system will include tools for the configuration of security policies, privacy policies, network topologies, device features, VNF features	HIGH
NFR-8	**Effectiveness** – the ANASTACIA system will be able (at least) to notify attacks and potential privacy threats and (possibly) to identify a suitable mitigation plan and (possibly) to enforce mitigation actions, returning the monitored system in a safer status	HIGH
NFR-9	**Extensibility** – the ANASTACIA system will adopt a modular architecture and include configuration tools that allow adding features and defining customizations	MEDIUM
NFR-10	**Interoperability** – the ANASTACIA system will adopt *de facto/de iure* standards for interfacing with third parties' systems (e.g. exposed API) exposing e.g. main reporting functionalities	MEDIUM
NFR-11	**Performance** (response time/ throughput) – the ANASTACIA system will monitor ICT infrastructure in real time and will immediately notify detected threats and potential privacy breaks, independently from the number of monitored devices	MEDIUM
NFR-12	**Recoverability** (mean time to recovery - MTTR) – the ANASTACIA system will be able to detect and notify threats within <ΔT>, to define a mitigation plan within <ΔT>, to orchestrate a mitigation plan within <ΔT>, to enforce mitigation plan actions within <ΔT> (ΔT to be defined at pilot level)	LOW

ID	Name/Description (Trapero et al., 2017)	Priority*
NFR-13	**Reporting** – the ANASTACIA system will include functionality for real time notification of cyber-attacks and of potential privacy breaches (summarized by the DSPS) and will provide end users with the possibility to download reports on all managed events and actions undertaken	**HIGH**
NFR-14	**Scalability** – the ANASTACIA system will be able to transparently add/deploy new monitored IoT devices and VNFs	**HIGH**
NFR-15	**Security** – the ANASTACIA system will provide functionalities for Authentication, Authorization, and Accounting to guarantee proper access for registered users	**MEDIUM**

Table 17 Anastacia D. 1.3 Non-Functional Requirements 1.3(Trapero et al., 2017)

Special care shall be taken to comply with NFR-5 and NFR-6 on certification and compliance[52], for which the DSPS Server shall be designed to meet the full range[53] of Critical Security Controls for Effective Cyber-Defence detailed by ETSI (European Telecommunications Standards Institute, 2015)[54] while also complying with the dispositions of the most relevant ISO/IEC standards[55].

Among these controls/capabilities, the DSPS Servers shall introduce: anomaly detection; pre-emptive/automatic reaction capabilities (particularly towards potentially hazardous security events and data breaches); application level firewalls and defensive capabilities (IP blocking, throttling, account management, etc.); strong system-wide authentication mechanisms; automatic updates and update-verification mechanisms; capability to utilize encrypted communications to storage layer (if required); Data classification and segregation capabilities; denial of service and replay attack mitigation; encrypted communications, encrypted storage, interface segregation and isolation based on utility (device, management interface, user interface, etc.); strong (verbose) event logging, reporting and alerting capabilities; plugin or extension verification; strong component authentication; and secure and up-to-date third party components.

As mentioned in section 5.3.3, the DSPS Servers shall be developed in a way which enables the creation of a Core DSPS blockchain network (See Figure 13 Core DSPS blockchain network) aimed towards verifying and validating the transactional logging mechanisms which shall support (and prevent the counterfeiting of) the Dynamic Security and Privacy Seal. The architecture of this network shall be based on the principles of redundancy[56], security[57] and expandability and shall take into consideration the secure communication requirements identified in section 7.2 for its internal networking and communication processes.

[52] For which an external certification process shall be carried out once the DSPS Architecture has been implemented.

[53] Given the constant evolution of technology and the never-ending rise of potential security threats; it is not possible to perform a future-proof determination of security measures to be implemented by the DSPS Servers in the current deliverable. For this reason, additional measures to those established by this deliverable shall be considered and introduced to the system throughout its life cycle; in order to meet the highest possible security standards and address threats/minimize risk to the system at all times.

[54] Secondarily the implementation team should consider the security controls detailed by NIST (Joint Task Force Transformation Initiative, 2013) for further clarification of the organizational processes and particularly regarding technical mechanisms that are to be associated with the development and implementation of the DSPS Servers.

[55] Particularly: ISO/IEC 15408 (International Organization for Standardization, 2011a); ISO/IEC 27001 (International Organization for Standardization, 2013a); ISO/IEC 27002 (International Organization for Standardization, 2013b); and ISO/IEC 29100 (International Organization for Standardization, 2011b).

[56] Redundancy shall be a key characteristic of the DSPS Servers. It will not only ensure service continuity, but also enable the implementation of blockchain for authentication of all transactions (including ANASTACIA monitoring tools - DSPS transactions, as well as those transactions pertaining to the DSPS internal architecture and Seal creation/user verification processes).

[57] Physical, organizational, environmental, and logical security shall be considered when developing and implementing the DSPS blockchain network in accordance to the security controls, standards and recommendations identified in supra note 54. In direct relation to the requirement for redundancy, the core network will not necessarily be located in a single physical space, but might be geographically distributed to maximize security and ensure service continuity.

The design and implementation of the Core DSPS blockchain network shall be performed in strict consideration of the recommendations and controls related to data protection (CSC 17 as defined by ETSI (European Telecommunications Standards Institute, 2015, p. 58)); Physical and environmental security (PE family of controls as defined by (Joint Task Force Transformation Initiative, 2013, p. F-127)) and integrity and management requirements (Class FPT as defined by (International Organization for Standardization, 2011a, p. 76).

Starting from a minimum of two DSPS Servers to generate the core blockchain network, gradual introduction of additional Servers is highly recommended to maximize overall efficiency, processing capacity and trust. Regardless of the manner in which this is implemented, each DSPS Server must be capable of fulfilling all the roles (consensus management, management of the distributed logs, log storage and processing, etc.) necessary to ensure the accomplishment of the objectives of the DSPS. Furthermore, the Core DSPS blockchain network must be able to tolerate faults and to adapt itself to compromised/failing nodes/servers as necessary to ensure service continuity and data protection.

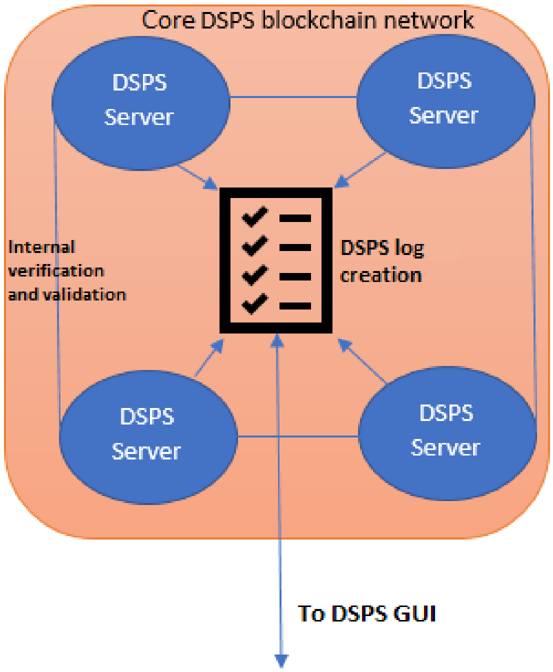

Figure 13 Core DSPS blockchain network

While the exact characteristics of the blockchain solution[58] to be developed or implemented in the DSPS Server is to be identified through the upcoming stages of WP5, the final decision on this element must

[58] Several companies provide blockchain solutions which might relate to the characteristics and purposes of the DSPS blockchain model. As such, further examination of their solutions, reference models are considered as potential enablers. Among these, the most relevant are:

- Ethereum (https://www.ethereum.org/): *"Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property."(Ethereum Foundation, 2017)*
- Factom (https://www.factom.com/): *"Factom Harmony provides a single, comprehensive, secure and unalterable document catalogue that eliminates the costs of document assembly and saves lenders time by consolidating document storage. With this streamlined platform, lenders can quickly and easily provide the auditors with credentials to the associated files. Using the Factom Harmony platform will remove the risk of lost or missing documents. Providing lenders with a blockchain based document audit solution that supports*

address the need for a shared, permissioned log, a consensus protocol and strong cryptographic means to support the system to be implemented. In addition to these requirements, the blockchain process that is to be deployed should be trustworthy, secure and based on technologies that have been recognized as viable by the industry.
On a wider perspective, transactional verification in the Core DSPS blockchain network shall meet four fundamental requirements:

1) Permanent, unbreakable relationship between the transaction (event and/or status certified by the DSPS) and the mathematic authentication.
2) Strong mechanisms (digital signatures and other identity management tools) to ensure the status of the seal and related information has been generated by the Core DSPS blockchain network and are not replicated or counterfeited.
3) Complex transaction management, capable of coordinating, standardizing, distributing and ensuring the transparency of all the transactions (particularly as relates to the distributed, parallel blockchain transaction verification that is to take place on user devices).
4) A clearly defined consensus based trust model among the Core DSPS blockchain network which also accounts for the verification/validation activities to be carried out through GUI nodes.

The integration of these four transactional verification requirements will generate a DSPS log in which DSPS Status updates and all related data will be indelibly and transparently recorded, while the implementation

---

review and assembly of the necessary loan documents for all audit types. Loan reviews for compliance all require accurate and complete loan files for a successful audit. Using the Factom Harmony collaborative blockchain platform supports storage of the audit results, findings, exceptions ratings, comments and defect reporting on each document."(Factom, 2017).

- Gladius (https://gladius.io/): *"the decentralized solution to protect against DDoS attacks by allowing you to connect to protection pools near you to provide better protection and accelerate your content. With an easy to use interface as well as powerful insight tools, Gladius enables anyone to protect and accelerate their website."(Gladius Network, LLC, 2011).*
- Golem (https://golem.network/): *"a global, open sourced, decentralized supercomputer that anyone can access. It's made up of the combined power of user's machines, from personal laptops to entire datacenters. Anyone will be able to use Golem to compute (almost) any program you can think of, from rendering to research to running websites, in a completely decentralized & inexpensive way."(The Golem Project, 2017).*
- NuCypher (http://www.nucypher.com/): *"The distributed nature of modern platforms translates into large attack surfaces while legacy encryption technologies cause performance bottlenecks and impair functionality. NuCypher protects data at-rest, in-transit, and in-use without impacting performance or functionality"(NuCypher, 2011).*
- Rivetz (https://rivetz.com/): *"The Rivetz ecosystem offers a simplified, intuitive approach to cybersecurity, built around hardware-based identity (…) [it] combines a hardware-based identity model with the immutable attestation offered by the blockchain."(Rivetz Intl, SEZC, 2017).*
- Rockchain (https://rockchain.org/): which *"enables distributed applications on the public blockchain to perform calculations, collaboration orchestration and machine learning on local private data through two core features: An access rights orchestrator managing rights on peer to peer node connections and a script engine that can perform computation on private data without compromising the data privacy. The Rockchain infrastructure is also creating an incentivisation scheme for miners (CPU or GPU) to help running the distributed datascripts."(Lambda Vision SAS, 2017).*
- Smartcontract (https://link.smartcontract.com/): *"ChainLink is blockchain middleware that allows smart contracts to access key off-chain resources like data feeds, various web APIs, and traditional bank account payments. By providing smart contracts secure access to these key resources, ChainLink allows them to mimic real-world agreements that require external proof of performance and need to make payment in widely available payment methods e.g. bank payments."(SmartContract, 2017).*
- Tierion (https://tierion.com/): *"The blockchain is becoming the new standard for trust and verification of data. Tierion turns the blockchain into a global platform for verifying any data, file, or process. Use Tierion's API and tools to anchor a permanent, timestamp proof of your data in the blockchain."(Tierion, 2017).*
- Zeppelin (https://zeppelin.solutions/): a *"leading technology firm in the blockchain industry, providing consulting, security audits and development services for organizations. Zeppelin has developed industry security standards for designing and deploying smart contract systems."(Zeppelin, 2017).*

of both the internal verification and validation procedures and the external GUI-based verification and validation will raise trust in the system.

7.4 GUI AND BLOCKCHAIN VERIFICATION / VALIDATION WEB APP

As previously mentioned, the DSPS Graphical User Interface aims to fulfil the double goal of enabling end user's access to the DSPS information in an easy to understand and trustworthy manner. Additionally, the GUI will introduce a decentralized tool for verification of the information received from the DSPS blockchain log and the distributed validation of DSPS blocks. Through these two goals, the end-user will adopt an active role in the verification of the privacy and security of the deployed systems and this will ultimately strengthen the DSPS's position as a trust-enhancing tool.

As explained in section 5.3.3 above, the overall processes involved in the GUI and blockchain verification and validation web app can be identified in the following figure:

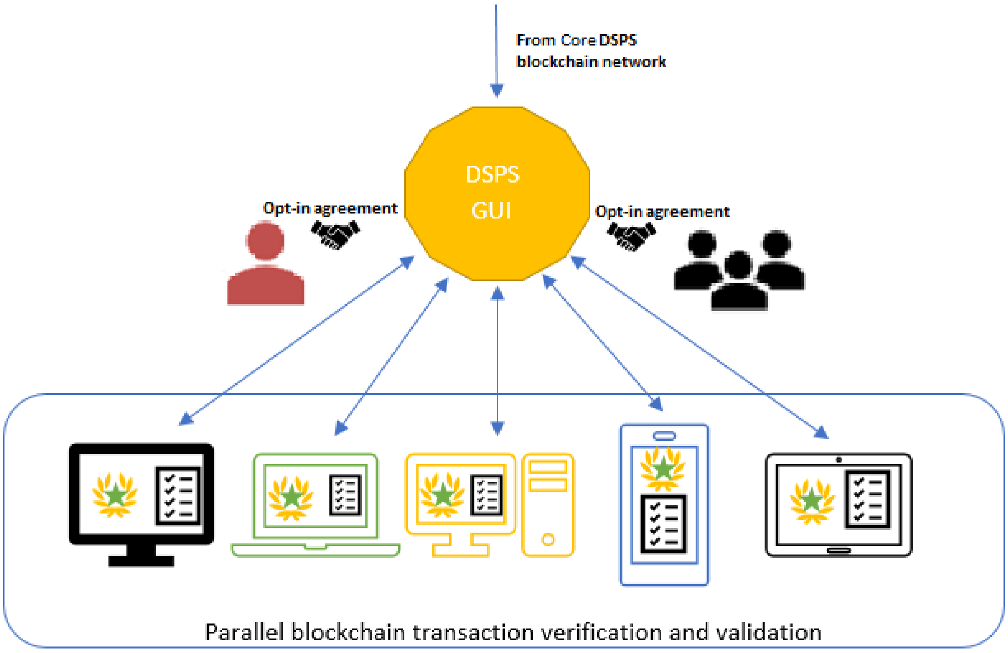

Figure 14 GUI-based blockchain verification and validation process

In order to perform these tasks, a series of technical and legal requirements should be considered, namely:

a) For the Seal Design:
   - Seal design should be focused on being as user-friendly and universal as possible. The desired information should be conveyed to the broadest possible public in a way that is easily understandable by most users at a glance. Accessibility enhancing technologies and design principles[59] should be considered.
   - The seal should additionally be capable of being integrated and seamlessly embedded into websites outside of the DSPS GUI while continuously conveying concise, real-time information on privacy, security and the stability of the DSPS itself. This embedded seal should be dynamic in its design and implementation, thus being capable of interacting with the end-user's inputs (for example by providing more information on the specific elements whenever the user attempts to interact with it or redirecting the user upon interaction to the DSPS GUI).

[59] Among other resources, see (International Organization for Standardization, 2012a) and (NCDAE, 2007).

- The Seal should be designed in a manner that does not compromises the security and privacy of the systems in which it is to be embedded, the end-user (or the devices in which the web-app will run) and the DSPS itself.
- The Seal should be designed to enhance trust and to prevent counterfeit.[60]

b) For the GUI design:

The general GUI design[61], as well as the design of the elements contained within each of its sections (Dynamic Security and Privacy Seal, data visualization tools, system analytics, etc.) shall consider design best practices[62] to ensure the GUI is user-friendly and the data is presented to the user in a meaningful and accessible manner.

This item includes the following elements:

- The general DSPS website / GUI homepage Must be easily accessible (platform neutral, internationalized/multi-language enabled and mobile-ready) and capable of adapting itself to a wide range of technologies and devices.
- Compatible with a wide range of access-enhancing technologies tailored to the accessibility needs of users with physical or mental disabilities.
- Dynamic visualization and reporting capabilities of a broad range of data sources: The DSPS GUI shall enable end-users and privileged end-users to customize the data that is presented to them (either in real time through the GUI or through any of the reporting systems) according to their interests.
- Include visible alerts for high-relevance events (such as a breach in the DSPS; particularly threatening situations; or user-programmed alerts).
- The services and elements available through the GUI must be tailored to the needs of two main kinds of users, namely:
    - End-users: general users that access the platform with the sole intention of receiving information on the overall status of the DSPS or any of the DSPS certified systems.
    - Privileged users: DSPS System administrators or representatives/system administrators of the DSPS certified systems which access the platform to obtain detailed information in accordance to their obligations and/or contractual agreements.

    Specific dispositions on the tailoring measures adopted to address the needs of these audiences will be found in Sections 7.5 and 7.6.

c) The blockchain verification and validation web-app:

- Must be a secure implementation of the blockchain processes into a solution that can be integrated and executed by the broadest possible range of web browsers and platforms.
- Must include an opt-in agreement: As the eventual implementation of this tool should comply with the dispositions of the e-privacy directive (article 5) and the GDPR (article 7). For this reason, the informed consent should be pursued through the presentation of all relevant information in a manner that is easy and clear to understand. The use of multimedia or accessibility-enhancing tools is greatly recommended to ensure the end user is correctly informed of all relevant aspects of this tool and the processing that will take place in his device.
- Must be open and transparent in its implementation and use of the user resources by the web app. It is highly recommended that the solution includes real-time visualizations[63] of

[60] As defined in section 5.2.1.

[61] Including but not limited to page structure; control elements; images; links; edit, email, and search boxes; charts and graphs; forms; filets and legends; tables; overlays; and error messages.

[62] See (World Wide Web Consortium, 2016).

[63] Inspiration on this item could be taken from projects like Seti@home (https://setiathome.berkeley.edu/) which have developed their visualization tools into an appealing and informative medium which the users can even set as their device's screensaver.

the transactional verification and validation process. If possible, the visualization tools should be aimed not only at informing the end-user, but also to pique his/her curiosity on the mechanisms and to encourage participation in the project[64].

7.5 End-User Access and Functionalities

The GUI shall provide secure access mechanisms to all-end users, regardless of their status as a privileged or non-privileged user. For this reason, all communications between a non-authenticated end-user (or one who has not been provided with sufficient privileges to access any functionality not available to common end-users) should still meet the secure communications requirements detailed in sections 6.2 and 7.2. Additionally, all measures aimed towards ensuring the protection of personal data of the end-user shall be applied in full for end-users regardless of any additional privileges granted by the DSPS system or it's administrators.

As previously defined, any end-user that accesses the DSPS GUI shall be granted a minimum set of functionalities as necessary to:

- Obtain information on the DSPS, its core functions, services, goals and impact. As the normal range of end-users will most probably have no or little information on ANASTACIA and its objectives, it is highly recommended that information is presented to the end-users in an easy to understand manner which entices them to explore further on the diverse elements that relate to the DSPS.
- Obtain basic information on the deployed system that most relates to his/her interests. End-users will most likely arrive at the DSPS GUI by clicking or interacting with the Seal embedded in any of the deployed system's sites. In this context, the information regarding the system's capacities, current and historic status, and any other relevant information should be presented in a way that does not detract from the user's experience. Reporting/data visualization functionality should be limited to those datasets that are most relevant to the end user without compromising any of the proprietary information of the systems that are overseen by ANASTACIA and the DSPS. Furthermore, the end-user should be made aware of the reasons for the imposition of these limitations in order to maximize transparency and user trust in the system.
- Opt-in to the execution of the DSPS verification/validation web-app, which will generate a temporary node of the DSPS blockchain network in the device of the user. As the non-privileged user might or might not be required to authenticate itself in the GUI to access this functionality, and considering the generic nature of his/her interest in the DSPS, the functions of the web-app will work in a completely neutral manner: verification of the information received from the DSPS log will be performed as required by the user's interactions and the remaining processing power will be dedicated towards validating DSPS blocks as defined by the DSPS system.

7.6 Privileged User Access Mechanisms

Special considerations will be granted to privileged users due to their positions as system administrators, owners of the system being certified by the DSPS or the requirements of any contractual dispositions that might require so. In this context, additional security measures will be adopted to ensure any activities they perform in the DSPS platform and any information they received is completely secure. According to their tasks and privileges, these users will be required to log-in to the system (using enhanced user identification mechanisms, two-factor authentication, etc.) and to register their devices in the system in order to ensure any privileged data submitted to them is correctly accounted for. This requirement will not affect in any

[64] Gamification techniques could also be used if deemed appropriate and possible by the implementation team.

way the DSPS efforts to ensure end-user privacy and the protection of any personal data that might be provided by the end-user.

Privileged end-users will be granted all the functions available to non-privileged end-users while additionally gaining access to:

- Expanded information on the DSPS, including access to any training resources necessary to ensure they can make full use of the advanced reporting and data visualization mechanisms that are to be made available to them through the DSPS GUI.
- Advanced or extended information on the status of those systems towards which their accounts have been linked. This to ensure complete transparency on the nature of the ANASTACIA/DSPS processes that are running on top of a certified system and to comply with any contractual dispositions on this topic.
- Privileged access to the opt-in verification/validation web-app, which will enable the users to dedicate additional processing power towards the validation of those DSPS blocks that correspond to those systems that are linked to their accounts. This measure will be aimed towards maximizing the participation of DSPS contractual partners in the generation of a strong blockchain while providing them with additional incentives for volunteering additional processing power and local resources.

8 CONCLUSIONS

This document analysed and specified the synthetic model for the Dynamic Security and Privacy Seal and the architectural elements that will support its implementation by ANASTACIA WP5 Tasks 5.2. and 5.3.

To accomplish this, the normative and technical frameworks that surround and determine the DSPS were analysed. This deliverable also examined the two models traditionally used for IT security and privacy monitoring and certification and generated a comparative analysis which enabled the identification of desirable traits to be introduced to the synthetic approach to be adopted by the DSPS. Once the contextual and theoretical elements were dully recognized, research focused on modelling the DSPS, the definition of both seal-specific requirements and the interactions between the DSPS and both ANASTACIA and the end-user. To further expand on the context, explorative research also delved the possible application of the hybrid model in a potential business practice.

Finally, research focused on identifying a set of requirements and supporting considerations for the design and implementation of the DSPS architecture. Specifications were drafted for the API and Agent that would enable interactions between ANASTACIA and the DSPS through secure communications. A redundant and secure server network was envisioned to provide the Seal creation services and a blockchain based logging solution for permanent and trust-generating storage of the historic seal records. Finally, a graphical user interphase was ideated to provide both data visualization and reporting tools and enhanced data verification and validation functionalities. This element constitutes the final element of the DSPS and ensures end-to-end security while fully respecting end-user privacy.

As part of the first deliverable to be provided by ANASTACIA WP5, the model that has been detailed in this document is foreseen to be further specified by ANASTACIA Tasks 5.2 and 5.3. As technical integration between WP5 and WP4 is strengthened, additional functionalities might be introduced to enhance the Seal's value to the end-user and to ANASTACIA as a whole. Future WP5 tasks should consider this deliverable in its context and carefully examine the sources identified throughout it to ensure that the final version of the DSPS reaches its full potential.

9 References

- A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid. (n.d.). Retrieved from http://web.cs.ucdavis.edu/~peisert/research/2015-CPS-SPC-Testbed.pdf
- Advanced Threat Defense and Targeted Attack Risk Mitigation. (n.d.). Retrieved from https://media.kaspersky.com/en/business-security/enterprise/kl_kata_whitepaper_og.pdf
- Barafort.B, Mesquida.A, Mas.A. (2017, November). Integrating risk management in IT settings from ISO standards and management systems perspectives - ScienceDirect. Retrieved December 9, 2017, from https://www.sciencedirect.com/science/article/pii/S0920548916301866
- Cavoukian, A. (2011, March). Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices. Retrieved from https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
- Christodoulou, S. E., Fragiadakis, M., Agathokleous, A., & Xanthos, S. (2018). Chapter 7 - Real-Time Monitoring. In *Urban Water Distribution Networks* (pp. 227–246). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-813652-2.00007-4
- ENISA. (2016, December). Security guidelines on the appropriate use of qualified electronic seals Guidance for users. Retrieved from https://publications.europa.eu/en/publication-detail/-/publication/90d99ddb-d3de-11e6-ad7c-01aa75ed71a1
- ENISA. (2017, November). Recommendations on European Data Protection Certification. European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification
- Ethereum Foundation. (2017, November). Ethereum homepage. Retrieved from https://www.ethereum.org/
- European Commission. (2016, October 28). Grant Agreement number 7315558 - ANASTACIA.
- European Council. (2014, July 23). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
- European Parliament, & European Council. Directive 2002/58/EC (as ammended by Directive 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009).
- European Parliament, & European Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- European Telecommunications Standards Institute. (2015, May). ETSI TR 103 305 - CYBER; Critical Security Controls for Effective Cyber Defence. Retrieved from http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf
- European Telecommunications Standards Institute. (2016, July). ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services. Retrieved from http://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf
- Factom. (2017, November). Factom Homepage. Retrieved from https://www.factom.com/
- Farnham, G., & Leune, K. (2013, October). Tools and Standards for Cyber Threat Intelligence Projects. SANS Institute. Retrieved from https://uk.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375
- Federal Assembly of the Swiss Confederation. (1992, June 19). Federal Act on Data Protection (FADP).

- Federal Data Protection and Information Commissioner. (2017). A Few Facts about the Federal Act on Data Protection. Retrieved from https://www.edoeb.admin.ch/org/00129/00131/index.html?lang=en
- Gladius Network, LLC. (2011, November). Gladius homepage. Retrieved from https://gladius.io/
- International Organization for Standardization. (2003, October). ISO/IEC 17030:2003 Conformity assessment -- General requirements for third-party marks of conformity. Retrieved from https://www.iso.org/standard/29353.html
- International Organization for Standardization. (2008, August). ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components. Retrieved from https://www.iso.org/standard/46413.html
- International Organization for Standardization. (2011a, May). ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components. Retrieved from https://www.iso.org/standard/46414.html
- International Organization for Standardization. (2011b, November). ISO 19011:2011 Guidelines for auditing management systems. Retrieved from https://www.iso.org/standard/50675.html
- International Organization for Standardization. (2012a). ISO/IEC 40500:2012 (W3C) Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0. Retrieved from https://www.iso.org/standard/58625.html
- International Organization for Standardization. (2012b, September). ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services. Retrieved from https://www.iso.org/standard/46568.html
- International Organization for Standardization. (2013, October). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. Retrieved from https://www.iso.org/standard/54534.html
- International Organization for Standardization. (2014, January). ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. Retrieved from https://www.iso.org/standard/50341.html
- International Organization for Standardization. (2015, June). ISO/IEC 17021-1:2015 Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements. Retrieved from https://www.iso.org/standard/61651.html
- International Organization for Standardization. (2016, February). ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. Retrieved from https://www.iso.org/standard/66435.html
- International Telecommunications Union. (2008, April 18). Recommendation X.1205: Overview of cybersecurity. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I
- International Telecommunications Union. (2012a, June 15). Recommendation Y.2060: Overview of the Internet of things. Retrieved from https://www.itu.int/rec/T-REC-Y.2060-201206-I
- International Telecommunications Union. (2012b, July 29). Recommendation Y.4050: Terms and definitions for the Internet of things. Retrieved from https://www.itu.int/rec/T-REC-Y.2069-201207-I/en
- International Telecommunications Union. (2014a, January 24). Recommendation X.1208: A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies. Retrieved from https://www.itu.int/rec/T-REC-X.1208-201401-I/en
- International Telecommunications Union. (2014b, June 22). Recommendation Y.4100: Common requirements of the Internet of things. Retrieved from https://www.itu.int/rec/T-REC-Y.2066-201406-I
- International Telecommunications Union. (2017a, March 29). Recommendation Y.3051: The basic principles of trusted environment in information and communication technology infrastructure. Retrieved from https://www.itu.int/rec/T-REC-Y.3051-201703-I/en

- International Telecommunications Union. (2017b, March 29). Recommendation Y.3052: Overview of trust provisioning for information and communication technology infrastructures and services. Retrieved from https://www.itu.int/rec/T-REC-Y.3052-201703-I/en
- Internet Engineering Task Force (IETF). (2012, April). Real-time Inter-network Defense (RID). Retrieved from https://tools.ietf.org/html/rfc6545
- Internet Engineering Task Force (IETF). (2014, April). An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information. Retrieved from https://tools.ietf.org/html/rfc7203
- Internet Engineering Task Force (IETF). (2016, November). The Incident Object Description Exchange Format Version 2. Retrieved from https://tools.ietf.org/html/rfc7970
- ISO. (2017a). Certification. Retrieved December 9, 2017, from https://www.iso.org/certification.html
- ISO. (2017b). Developing standards. Retrieved December 9, 2017, from https://www.iso.org/developing-standards.html
- ISO, & UNIDO. (2010, February). Building trust, The conformity assessment toolbox. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco_building-trust.pdf
- Joint Task Force Transformation Initiative. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (No. NIST SP 800-53r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4
- Kirova, M. (2016, June). eIDAS Regulation (Regulation (EU) N°910/2014). European Commission / Futurium. Retrieved from https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
- Lambda Vision SAS. (2017, November). Rockchain Homepage. Retrieved from https://rockchain.org/
- Leveraging Threat Intelligence in Security Monitoring. (n.d.). Retrieved from https://securosis.com/assets/library/reports/Securosis_ThreatIntelSecurityMonitoring_FINAL.pdf
- McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* (No. NIST SP 800-122). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122
- Miessler, D., Smith, C., Keane, J. K., & Yunsoul. (2017, August 17). OWASP Internet of Things (IoT) Project. Open Web Application Security Project. Retrieved from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main
- NCDAE. (2007, March). Principles of Accessible Design. Retrieved November 22, 2017, from http://ncdae.org/resources/factsheets/principles.php
- Nguyen, T. K., Dekneuvel, E., Jacquemod, G., Nicolle, B., Zammit, O., & Nguyen, V. C. (2017). Development of a real-time non-intrusive appliance load monitoring system: An application level model. *International Journal of Electrical Power & Energy Systems*, *90*(Supplement C), 168–180. https://doi.org/10.1016/j.ijepes.2017.01.012
- NuCypher. (2011, November). NuCypher Homepage. Retrieved from http://www.nucypher.com/
- OASIS. (2017a, June). TAXII Version 2.0. Retrieved from https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/pub#h.dwru50atx72x
- OASIS. (2017b, October). CTI Documentation. Retrieved from https://oasis-open.github.io/cti-documentation/
- Perez.G.C, Sellers.H.B, McBride.T, Low.G.C, Larrucea.X. (2016, November). An Ontology for ISO software engineering standards. Retrieved December 9, 2017, from https://www.sciencedirect.com/science/article/pii/S0920548916300344
- Piscini, E., Guastella, J., Rozman, A., & Nassim, T. (2016, February 24). Blockchain: Democratized trust - Distributed ledgers and the future of value. Deloitte. Retrieved from https://dupress.deloitte.com/dup-us-en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html

- Rivetz Intl, SEZC. (2017, November). Rivetz Homepage. Retrieved from https://rivetz.com/
- Sahay, S. K., & Sharma, A. (2016). Grouping the Executables to Detect Malwares with High Accuracy. *Procedia Computer Science*, *78*(Supplement C), 667–674. https://doi.org/10.1016/j.procs.2016.02.115
- SmartContract. (2017, November). SmartContract Homepage. SmartContract. Retrieved from https://www.smartcontract.com/
- Su, H.-C., Dhanorkar, S., & Linderman, K. (2015). A competitive advantage from the implementation timing of ISO management standards. *Journal of Operations Management*, *37*(Supplement C), 31–44. https://doi.org/10.1016/j.jom.2015.03.004
- Swiss Federal Council. (1993, June 14). Ordinance to the Federal Act on Data Protection. Retrieved from https://www.admin.ch/opc/en/classified-compilation/19930159/index.html
- Swiss Federal Council. (2007, September 28). Ordinance on Data Protection Certification (DPCO). Retrieved from https://www.admin.ch/opc/en/classified-compilation/20071826/index.html
- The Golem Project. (2017, November). Golem homepage. Retrieved from https://golem.network/
- The Mitre Corporation. (2012). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX). Retrieved from https://www.mitre.org/sites/default/files/publications/stix.pdf
- Tierion. (2017, November). Tierion Homepage. Retrieved from https://tierion.com/
- Townsend, M., Le Quoc, T., Kapoor, G., Hu, H., Zhou, W., & Piramuthu, S. (2017). Real-Time business data acquisition: How frequent is frequent enough? *Information & Management*. https://doi.org/10.1016/j.im.2017.10.002
- Trapero, R., Rivera, D., Taleb, T., Farris, I., Belabed, D., Crettaz, C., … Bianchi, S. (2017, September 31). ANASTACIA D 1.3 Initial architectural design. Retrieved from www.anastacia-h2020.eu
- World Wide Web Consortium. (2016). Web Design and Applications. Retrieved November 22, 2017, from https://www.w3.org/standards/webdesign/
- Zeppelin. (2017, November). Zeppelin Homepage. Retrieved from https://zeppelin.solutions/