ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

# D5.2

## Dynamic Security and Privacy Seal Monitoring Service

This deliverable presents the results of ANASTACIA Task 5.2. The aim of the task is to develop and implement the Dynamic Security and Privacy Seal (DSPS) Monitoring Service. This deliverable is primarily focused on the demonstrator of the DSPS as defined in D5.1 and includes some enhancements over the initial design.

| | |
|---|---|
| Distribution level | PU |
| Contractual date | 31.12.2018 [M24] |
| Delivery date | 08.01.2019 [M25] |
| WP / Task | WP5 / T5.2 |
| WP Leader | MAND |
| Authors | Adrian Quesada Rodriguez (MAND), Adriano Perlini (DG), Ana Maria Pacheco Huamani (AS), Bojana Bajic (AS), Cédric Crettaz (MAND), Eunah Kim (DG), Matteo Filipponi (DG), Sébastien Ziegler (MAND), Vincent Loup (MAND) |
| EC Project Officer | Carmen Ifrim<br>carmen.ifrim@ec.europa.eu |
| Project Coordinator | Softeco Sismat SpA<br>Stefano Bianchi<br>Via De Marini 1, 16149 Genova – Italy<br>+39 0106026368<br>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

# Table of Contents


PUBLIC SUMMARY ..... 4

1 Introduction ..... 5

1.1 Aims of the document ..... 5

1.2 Applicable and reference documents ..... 5

1.3 Revision History ..... 5

1.4 Terms and Definitions ..... 6

1.5 List of Acronyms ..... 7

2 DSPS Objectives and Requirements ..... 8

2.1 Guiding principles ..... 8

2.2 Implementation requirements ..... 10

2.2.1 ANASTACIA Monitoring Tools API / Agent ..... 10

2.2.2 Secure Communications ..... 11

2.2.3 DSPS Servers and Core DSPS Network ..... 11

3 DSPS Service Overview ..... 14

3.1 Expected DSPS Services ..... 14

3.1.1 Privacy Assessment ..... 16

3.1.2 The role of Privacy Assessments and DPO's feedback in the DSPS ..... 18

4 DSPS Architecture and Functional components ..... 21

4.1 Functional building blocks and processes ..... 21

4.2 DSPS Agent ..... 21

4.2.1 Functionalities ..... 21

4.2.2 Composition ..... 22

4.3 DSPS Creation Service ..... 23

4.3.1 Functionalities ..... 23

4.3.2 Composition ..... 24

4.4 DSPS Storage ..... 27

4.4.1 DSPS Distributed Ledger Solution ..... 27

4.4.2 DSPS Distributed Storage Solution (OFF-CHAIN STORAGE) ..... 31

4.4.3 DSPS Distributed Ledger and Distributed Storage: Performance Evaluation ..... 32

4.5 DSPS Graphical User Interface ..... 35

4.5.1 Functionalities ..... 35

4.5.2 Composition ..... 38

5 Summary and Future Work ..... 40

6 References ..... 41

7 Annexes ..... 42
Annex 1: PIA Questions ..... 42
Initial Questionnaire ..... 42
Short feedback questionnaire: ..... 44
Annex 2: Relevant Metrics and Indicators for additional visualization capabilities ..... 45
Annex 3: Survey on Privacy and Cyber-security Tools ..... 50

## Table of figures

Figure 1 DSPS Service Overview ..... 14
Figure 2 Privacy assessment need ..... 17
Figure 3 Currently implemented architecture ..... 21
Figure 4 Security alert message ..... 22
Figure 5 DSPS Agent composition ..... 22
Figure 6 Process to add a new seal ..... 24
Figure 7 Creation Service ..... 24
Figure 8 HyperLedger Fabric architecture ..... 28
Figure 9 ANASTACIA Fabric architecture ..... 29
Figure 10 Information contained into the seal ..... 29
Figure 11 Full signature included into the seal ..... 30
Figure 12 DSPS composition with secret sharing models ..... 32
Figure 13 GUI Dashboard ..... 35
Figure 14 GUI Status change alert ..... 36
Figure 15 GUI alert detail overview ..... 36
Figure 16 GUI Privacy risk overview ..... 37
Figure 17 GUI seal restore form ..... 37
Figure 18 DSPS GUI composition ..... 38

## Index of Tables

Table 1 Likelihood evaluation criteria (Adapted from IEC 62198 Managing Risk in Projects, 2013, P. 38) ..... 19
Table 2 Impact evaluation criteria (Adapted from ENISA Handbook on Security of Personal Data Processing, Dec. 2017, p. 11) ..... 19
Table 3 Privacy Risk Assessment Table ..... 20
Table 4 available HTTP requests ..... 25
Table 5 Privacy mapping example ..... 26
Table 6 Seal storage methods ..... 31
Table 7 Secret sharing methods ..... 32

Table 8 Summary of the benchmark values ..... 34
Table 9 available HTTP requests ..... 39

# PUBLIC SUMMARY

The deliverable D5.2 is a demonstrator of the DSPS monitoring service generated as of today, which develops the secured and authenticated sealing service. This document provides the overview of the demonstrator, which followed the model specification defined in Task 5.1 and detailed in D5.1. The dynamic seal will take into account the history and reliability over time of the system providing several levels of trust of the monitored system.

The deliverable reviews conformity of the implemented architecture with the relevant principles and requirements, provides an overview of the DSPS service, the deployed architecture and the implemented functions and finalizes by identifying the future work that remains to be performed.

# 1 INTRODUCTION

## 1.1 AIMS OF THE DOCUMENT

This document is to explain the demonstrator of Dynamic Security and Privacy Seal (DSPS) service, which is on the development and implementation under the Task 5.2 (T5.2). The DSPS monitoring service is based on the background studies and model specification performed under the Task 5.1 (T5.1) and work together with DSPS user interface development performing in the Task 5.3 (T5.3). It develops the secured and authenticated sealing service by interacting with monitoring components developed in WP4 and adapting the policies defined in WP2. The DSPS will provide the history and reliability over time of the system on security and privacy together with real time monitoring of deployed systems. The seal is to provide several levels of trust, 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. As the DSPS monitoring service is not completed without stating the user interface and its relevant development on the secure registry, this deliverable introduces the current version of DSPS development including both the demonstrator of DSPS service (developing in T5.2) and user interface and related distributed ledge and storage development (developing in T5.3).
A demonstrator of the Dynamic Security and Privacy Seal Monitoring Service is the expected outcome of T5.2 and is described in this accompanying document.

## 1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- Grant Agreement – Number 731558 – ANASTACIA
- ANASTACIA Deliverable D1.2 User centred requirements initial analysis
- ANASTACIA Deliverable D1.3 Initial Architecture Design
- ANASTACIA Deliverable D2.2 Attack Threats Analysis and Contingency Actions Initial Report
- ANASTACIA Deliverable D2.3 Privacy Risk Modelling and Contingency Initial Report
- ANASTACIA Deliverable D4.1 Initial Monitoring Component Services Implementation Report
- ANASTACIA Deliverable D5.1 Dynamic Privacy and Security Seal Model Analysis

## 1.3 REVISION HISTORY

| Version | Date | Author | Description |
|---|---|---|---|
| 0.1 | 06/11/2018 | Adrian Quesada Rodriguez | Initial document outline and structure |
| 0.6 | 19/12/2018 | Adrian Quesada Rodriguez, Bojana Bajic, Eunah Kim, Matteo Filipponi, Vincent Loup, Adriano Perlini, Cédric Crettaz, Sébastien Ziegler, Ana Maria Pacheco Huamani | Restructured document and added implementation elements |
| 0.8 | 22/12/2018 | Adrian Quesada Rodriguez, Eunah Kim, Bojana Bajic, Emilia Evequoz | Integrated inputs and fixed formatting. |
| 1.0 | 24/12/2018 | Eunah Kim | Refinement of the overall document |

| | | | |
|---|---|---|---|
| 1.1 | 27/12/2018 | Antonio Skarmeta, Stefano Bianchi | Overall revision and consistency check |
| 1.2 | 5/01/2019 | Adrian Quesada Rodriguez, Eunah Kim, Sébastien Ziegler | Final version |

## 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, 2011)
2. **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.
3. **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.
4. **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).
5. **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, 2012).
6. **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)
7. **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))
8. **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)
9. **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 Interface |
| 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 |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| SMMI | Seal Manager Metadata Interface |
| SSSS | Shamir Secret Sharing Scheme |

# 2 DSPS OBJECTIVES AND REQUIREMENTS

The Dynamic Security and Privacy Seal aims to generate a novel approach to monitor ICT security and privacy that 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 informative resource which can facilitate the work of privacy and security personnel by providing an easy to understand, highly trustable, overview of the system status. It will introduce encryption and verification mechanisms as additional trust-enhancing measures, which will guarantee end-to-end security of the information 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 distributed ledger (an immutable, non-refutable seal history for validation and verification activities) and a distributed storage solution (to record the associated datasets, feedback and proof/documentation obtained from the DPO/CISO upon threat mitigation).
As noted in D5.1, the DSPS will leverage the information provided by ANASTACIA WP2, WP3 and WP4 to verify 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 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 possible status (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 (Distributed Ledger and Distributed Storage Solution) 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; 2) actions (e.g. mitigation plans and modification in device/topology configurations); and 3) feedback (documentation or organizational activity reports obtained from the end-user). 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.[1]

## 2.1 GUIDING PRINCIPLES

According to the elements described by D5.1 (Section 5.2.1), the following principles must be considered when deploying the DSPS and implementing the diverse architectural elements that support it:

- **Accessibility**: Seal-related information should be easily accessible and 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, 2012).
    - This principle has been considered when designing the initial iterations of the DSPS GUI. Task 5.3 will continue research on this direction.
- **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).
    - This principle has been considered when designing and implementing the DSPS service and user interface. The current demonstrator includes the seal display to the end users as well as storing the log. The seal logic is under research in T5.2 following this guideline.

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

- **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.
    - This principle has been considered throughout integration activities and the design of the distributed ledger and the off-chain storage that support the DSPS.
- **Real time update**: 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 principle has been introduced in current iterations of the DSPS demonstrator. Future iterations will strive to further enhance the system's performance.
- **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).
    - This principle has been considered throughout the design and implementation phase of the distributed ledger. Task 5.3 will continue this line of work, particularly as relates to the end-user verification and validation activities.
- **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.
    - The principle has been fundamental to the design decisions of DSPS GUI that led to the introduction of a distributed architecture for the DSPS ledger and storage.
- **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[2] 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.
    - This requirement is used as a basic guideline of the Privacy Impact Assessment (PIA) that is performing in T5.2. The on-going research results will be directly applying to the DSPS service and user interface implementation.
- **Auditability**: 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 has been considered when developing the DSPS storage solution and the process that will support end-user feedback that will be extended in the further development of the user interface.
- **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

[2] The European Union Agency for Network and Information Security (ENISA) provides expert advice and recommendations on the implementation of the eIDAS Regulation. The ENISA's security guidelines on the appropriate use of qualified electronic seals (ENISA, 2016) will be taken into account to develop DSPS.

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).

- This principle has been instrumental in the implementation decisions that led to the hybrid distributed ledger and storage solution envisioned by D5.1 and implemented in T5.2 and T5.3.

## 2.2 IMPLEMENTATION REQUIREMENTS

The following requirements were defined by T5.1 as relevant for T5.2. This section briefly reviews the identified requirements and describes their implementation level throughout the relevant elements of the DSPS Monitoring Service.

### 2.2.1 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).

- Predictability:
  - D. 5.1 definition: Every interaction facilitated by the API/Agent shall have a predictable outcome
  - This requirement has been fully implemented as no component shows non-deterministic behaviour.
- Systematization:
  - D. 5.1 definition: Every interaction facilitated by the API/Agent shall be correctly integrated in the frame of the wider ANASTACIA platform.
  - This requirement has been partially implemented as integration with WP4 has not yet been completed.
- Information Security:
  - D.5.1 definition: All transactions taking place through the API shall be secure and transactional logs kept for posterior audit/verification. Access 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.
  - This requirement has been fully implemented, all communications are encrypted and authentication/authorization is managed with LDAP. Logs are securely kept in the off-chain DSPS storage (see Section 4.4).
- Equal reliability:
  - D.5.1 definition: Equal security requirements are to be applied to all programs that attempt to interact with the API/Agent.
  - This requirement has been partially implemented, not all components are completed and the principle will be kept in further development.
- Interoperability:
  - D.5.1 definition: 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.
  - This requirement has been partially implemented. It is under studying to introduce STIX2 and TAXII standards for data format and transport in order to provide wider interoperability.
- Openness:

- D.5.1 definition: The standards (both for data format and transport mechanisms) to be introduced as part of the API/Agent shall be open.
- This requirement has been partially implemented. To meet this requirement together with the interoperability requirement, open standards have been selected and the research is on going on potential applicability.

- Data consistency:
  - D.5.1 definition: Requests performed through the API/Agent shall be addressed by the ANASTACIA platform in a consistent manner.
  - This requirement has been fully implemented as the data format with APIs are defined and implemented.
- Consistency of response delivery:
  - D.5.1 definition: 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.
  - This requirement has been fully implemented. The DSPS APIs always return status code and response.
- Quality of service:
  - D.5.1 definition: 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.
  - This requirement has been partially implemented since architecture and the associated functionalities are still under development. The QoS measures may still change.
- System stability:
  - D.5.1 definition: 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.
  - This requirement has been fully implemented in design stages of the agent.
- Unification:
  - D.5.1 definition: Unified forms of information shall be adopted to maximize trust while maintaining the uniqueness of the content that is to be transmitted.
  - This requirement has been partially implemented as integration with other ANASTACIA WPs has not been concluded yet.

### 2.2.2 Secure Communications

- Encryption:
  - D.5.1 definition: All communications between the DSPS Servers and the DSPS Agent shall be encrypted to maximize security.
  - This requirement has been fully implemented as all data is encrypted in DSPS service.
- Secure communication channels:
  - D.5.1 definition: Secure communication channels should be implemented.
  - This requirement has been introduced from the initial implementation, and further refinement may be introduced throughout the further development of DSPS services and user interface.

### 2.2.3 DSPS Servers and Core DSPS Network

The following requirements were 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.

- Application software security:
  - D.5.1 definition: 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 requirement has been fully introduced by the DSPS monitoring service and will be taken into account throughout the full implementation expected by end of the project.
- Authentication:
  - D.5.1 definition: The DSPS Server shall implement access enforcement and account management tools, alongside with strong authentication mechanisms.
  - The requirement has been fully taken into account. The details of the user management are under development and the further development of the DSPS user interface will strengthen the user authentication.
- Authorization:
  - D.5.1 definition: The DSPS Servers shall be capable of generating an inventory of authorized and unauthorized devices, software/processes and users.
  - Fully implemented, it is managed with LDAP under the current architecture.
- Availability:
  - D.5.1 definition: 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.
  - DSPS services are permanently available. Will further enhance implementation measures as architecture evolves.
- Boundary defence/continuous vulnerability assessment and remediation:
  - D.5.1 definition: Control of internal and external network traffic should be implemented by the DSPS Servers so as to minimize possible attack vectors.
  - Implementation foreseen on the final DSPS architecture.
- Configurability:
  - D.5.1 definition: The DSPS Servers shall be configurable to comply with the constraints or the requirements not mentioned or defined in this document.
  - Requirement has been fully implemented. Further functionalities and value-added services have been foreseen and the system has been configured accordingly.
- Data protection:
  - D.5.1 definition: The DSPS Server shall introduce constant data protection mechanisms to ensure all data (including personal data) remains under its control.
  - The DSPS has followed the privacy by design/default approach in all elements of its architecture and the requirement has been fulfilled (see DSPS storage).
- Redundancy and Data recovery capability:
  - D.5.1 definition: Servers in the Core DSPS network shall introduce extensive data recovery capabilities based on redundant hardware and data recovery solutions/processes.
  - This requirement has been fundamental for the design of the DSPS storage solutions and has been fully introduced in the architectural decisions made thus far.
- Effectiveness:
  - D.5.1 definition: The DSPS Servers shall be designed and programmed in such a manner as to enable the effective processing of information that is necessary to meet the goals and minimum functionalities required of the DSPS.
  - Effectiveness of the system has been proven and measured thus far (see section 4.4.3)
- Encryption:
  - D.5.1 definition: Standards-based encryption should be implemented
  - As previously defined, all current communications are encrypted with TLS and the storage has considered this requirement accordingly.
- Extensibility:

    - D.5.1 definition: 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.
    - Extensibility of the DSPS architecture has been considered from the modelling phase and implementation decisions have followed accordingly. This requirement led to the decision to integrate the outputs of PIA tools into the DSPS in the future.
- Incident response and management:
    - D.5.1 definition: Each detected incident shall be reported and the DSPS Server shall answer automatically to each identified incident.
    - This requirement has been partially implemented, handling multiple simultaneous incidents is a planned feature that needs to be further refined in connection to WP4.
- Malware defences:
    - D.5.1 definition: The DSPS Server shall put in place all the measures to avoid the installation of malware on the system.
    - The requirement has not been fully implemented given the virtualized nature of the architecture that currently supports the DSPS. It should be fully implemented before offering the service to a client.
- Minimum service:
    - D.5.1 definition: The DSPS Server shall be designed in a way that ensures the constant provision of the minimum functionalities and to achieve the goals of ANASTACIA.
    - Fully implemented: the system is able to provide minimum functionalities to the end-user at all times.
- Secure baseline configurations:
    - D.5.1 definition: Secure baseline configurations should be implemented
    - Baseline security considerations have been fully integrated into the latest version of the DSPS demonstrator.
- Secure network engineering:
    - D.5.1 definition: The Core DSPS network shall be designed in a way that respects the security design and coding principles and provides end-to-end security.
    - This element has been partially implemented given the wide scope of the requirement. Physical elements have yet to be integrated given the virtualized character of the demonstrator.
- System logs and auditability:
    - D.5.1 definition: Each DSPS Server shall generate logs for various events and activities. 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.
    - The DSPS storage solution has been tailored to handle logs and prepare for audit scenarios. The range of activities detailed has been partially implemented thus far but work is on-going to this end.

# 3 DSPS SERVICE OVERVIEW

With the DSPS Creation Service ANASTACIA aims to combine the conventional conformity assessment model with dynamic monitoring in order to inform the end-user of any change in the trust level when it comes to privacy and security.

The DSPS aims to provide a holistic solution to privacy and security monitoring process, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a two-step process during which:

1) the end-user (DPO/CISO) will receive information from the DSPS (based on the alerts and other data provided by ANASTACIA's monitoring and reaction service); and
2) the end-user will provide feedback on the alerts and data obtained from the DSPS, and use the DSPS tools to securely store data to support any organizational claims for compliance with relevant regulations or proof of security/privacy control performance.

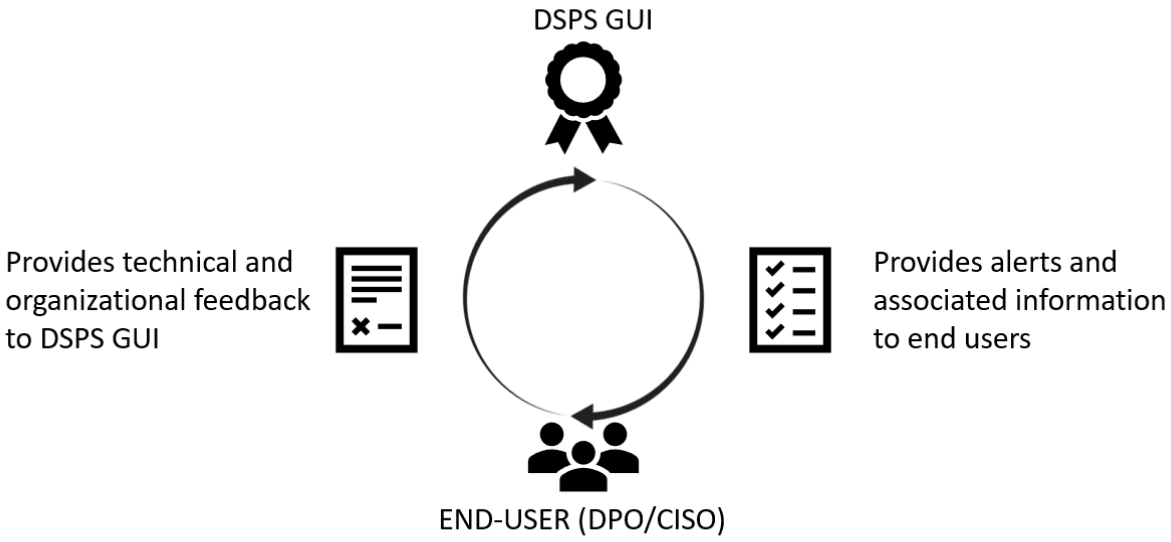



Figure 1 DSPS Service Overview

## 3.1 EXPECTED DSPS SERVICES

The DSPS will support three main services, namely:

1. **Monitoring and reporting**

   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 of variations and potential threats to the sealed system.

   DSPS will leverage the security information provided by ANASTACIA (alerts, warnings and vulnerabilities) to verify 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.

The user (DPO/CISO) will be requested to fill in the simplified questionnaires to compile a set of data on the monitored system on organizational privacy policy and will be informed through the DSPS about any irregularity regarding the security and privacy and be requested to act on the relevance of the received alerts. The DPO/CISO feedback to alerts (or other information from DSPS) will be used to update the status of the seal.

2. **End-user feedback on privacy risks**

A trained auditor or expert (including the DPO/CISO) will receive alerts and reports generated by the DSPS along with a set of questions in order to assess the privacy and security elements within the organization. The questionnaire will enable the end user to check both the product or system and the organizational policies and processes to ensure post-alert compliance with the most relevant privacy standards and regulations.

The questionnaire will help end-user to assess and declare potential privacy risks and to declare any mitigation activities that have been carried out from an organizational or application-specific point of view. They will be able to submit any supporting documentation to demonstrate performance of these activities (including uploading the Data Protection Impact Assessments, internal audit reports, or technical logs of mitigation activities) for safekeeping in the DSPS storage. Any feedback submitted by the end-user will be electronically signed to ensure the organization can demonstrate that due-diligence has been carried out in case a third- party audit is carried out. The DSPS will secure all received information through the distributed ledger and storage solutions.

3. **Change and restoration of the seal**

Change in the level of the DSPS seal will indicate a change in the status of the network and the level of risk when it comes to security and privacy. In order to provide easy understanding of the seal level that is agnostic from the used language, colours will indicate the level of seriousness of the threat in the system:

1) Green: No security and privacy risk is identified.
2) Yellow: The level of the security and privacy risks is high enough to check what is happening with the system. The user will receive the alert by DSPS GUI as well as by email and will be required to provide feedback on the mitigation activities carried out.
3) Orange: The level of security and privacy risks is at the very high level; the user will be informed about the alert by DSPS GUI and by email and will be required to immediately solve the problem and to provide feedback on the raised issue and any mitigation activities that were carried out.
4) Red: The number of security and privacy risks is so high that the system cannot function any more. This status also requires the feedback from the user in order to restore the seal.

All the information about the change of the seal will be stored in the off-chain storage solution, which will receive and securely store all data associated with the actions the organization has undertaken to address the threats and to minimize the impact. Upon reception of the electronically signed feedback from the user, the seal will be restored to a normal status.

Change of the colour of the seal will always be followed by the explanatory legend for the different possible scenarios that can help end user to react properly and to manage security and privacy in the deployed system. The information will also be made available for certification monitoring and compliance self-assessment as described by D5.1 (Section 6.8).

### 3.1.1 Privacy Assessment

As of now, there is a divide between tools aimed to facilitate organizational compliance with personal data protection requirements and the GDPR. As of our best knowledge, no tool provides both security monitoring for IoT and CPS deployments with an associated examination of the privacy threats and the organizational response they trigger.

Traditional tools are unable to provide the real-time assessment and verification of a system's compliance with the privacy and security requirements. Privacy measures can be different from those adopted by security measures including the General Data Protection Regulation (GDPR) introduced by European Parliament and Council of the European Union.

The DSPS aims to introduce a synthetic model to address the need for real-time monitoring tool that examine a system's protection of user privacy and system security. By introducing diverse sources of the privacy and security data, the DSPS service will generate an integrated view of the potential threats and the associated actions. Additionally, it will enable the secure, authenticated storage of end-user feedback to the identified threats and of data supporting the organization's claims for compliance with relevant requirements and controls, through the DSPS architecture.

In this context, the DSPS will use the Security Assessment that is automatically generated by ANASTACIA WP4[3] as reported to WP5 by the monitoring and reaction enablers, the organizational nature of privacy threats and mitigation activities prevents a fully automated privacy assessment to be introduced. For this reason, DSPS will address privacy assessment through the following process:

1) Baseline privacy threat values: upon initial installation of the ANASTACIA framework and the DSPS, the end-user (DPO and CISO) will be required to fill in a questionnaire on the privacy threats that are relevant to the monitored system, in accordance with the personal data held or processed by the monitored system, etc. The data obtained through this questionnaire will include the baseline privacy threat values that have been considered to be relevant by the DPO/CISO in consideration of the contextual elements of the monitored system.
2) ANASTACIA correlation of security/privacy threats: The specified threats will be correlated to the set of security threats and mitigation activities by ANASTACIA T.2.3. The correlation that is generated by this Task will be implemented by ANASTACIA WP4, which will in turn inform the DSPS of any security alert that is also relevant for privacy. The risk correlation table will be dynamically updated based on the end-user feedback obtained by the DSPS.
3) Upon receipt of an alert that is privacy-relevant, the DSPS will proceed to modify the privacy value of the DSPS and to inform the end-user (DPO) of the privacy alert. The DPO will then perform the manual verification of the alert, carrying out all the tasks that are required by law (GDPR and any relevant national regulations) and will report back through the DSPS GUI feedback forms:
    a. The relevance of the received alert
    b. Any mitigation activities performed
    c. Any supporting documentation to demonstrate the activities has been carried out.

This process will link the automated alerts and mitigation activities that ANASTACIA can provide from a technical perspective, with the organizational and data-centric perspective that is necessary to comply with privacy regulations. As mentioned in ANASTACIA D. 5.1, it is important to remember that the ANASTACIA framework is focused only on network-level activity. Given the lack of application-layer insights, it is very difficult for the security enablers to provide in-depth personal data protection monitoring and mitigation activities, which would require in-depth knowledge of the nature of the data processed by the organization and the various dataflows that are associated with it. The DSPS will seek to overcome this limitation by providing privacy threat indicators to the end-user, which will be then verified and validated by the DPO.

[3] The security risk assessment will be carried out by WP4's monitoring and reaction modules and the logic that support their assessment will be specified in a future WP4 deliverable.

The system will aim to cross-reference the security alerts obtained from ANASTACIA with the insights on the organizational perspectives on privacy and the minimization activities that are carried out to address the identified threats. Furthermore, it will seek to obtain the expert inputs of the end-users (DPOs/CISOs) to calculate the baseline privacy risks measurements for the monitored system that are to be raised to the user's attention upon the identification of a privacy-related alert, safely storing and cross-referencing PIA's tool's insights of the organizational perspectives.

The general rationale to support this decision is as follows:

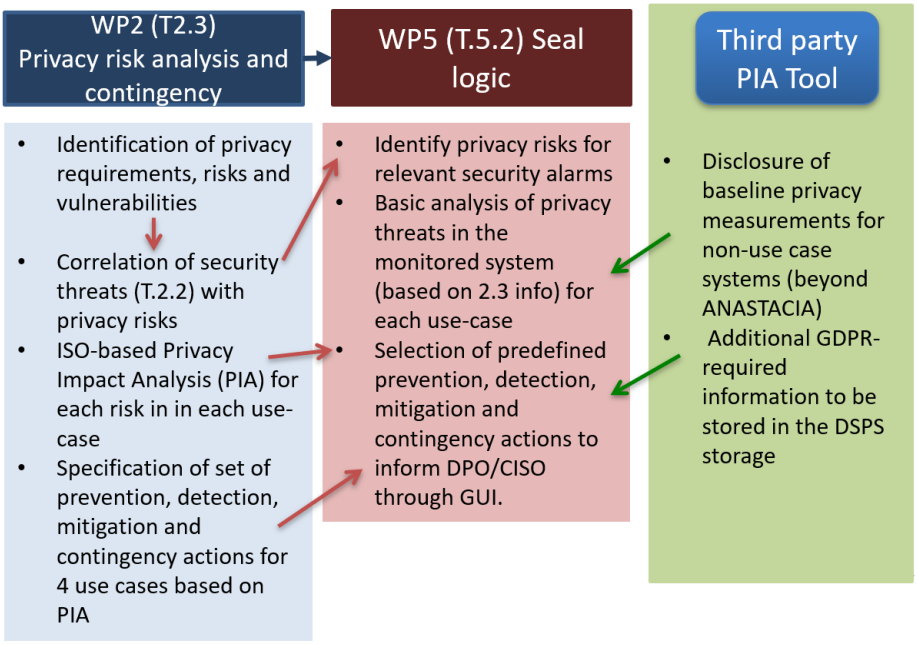



**Figure 2 Privacy assessment need**

In order to cover the whole range of systems where ANASTACIA and the DSPS could be potentially implemented, end-user feedback on the privacy alerts and mitigation activities with the DSPS service will remain as open as possible. The DSPS GUI will seek to support data import functionalities from existing Privacy Impact Assessment tools for assessing the privacy risks in accordance with the international standards in risk management.[4] In this context it is important to note that the DSPS will ensure the end-user is well aware of his/her responsibility to truthfully fill in the various feedback forms, as all potential liability raising from any data breach that is mishandled by the DPO will fall upon the organization. This fact will be restated numerous times by the system, which will additionally require DPO to electronically sign any feedback submitted to the DSPS system in relation to privacy alerts.

[4] For example, officially recognized open source PIA software made by CNIL can help implementing the data protection impact assessment to demonstrate compliance to the GDPR. The PIA tool by CNIL is based on General Data Protection Requirements and made to carry out the analysis through four main steps:

1. Defining the context of the processing of personal data under consideration
2. Analyse the controls guaranteeing compliance with the fundamental principles
3. Assess privacy risks associated with data security
4. Validation of the Privacy Impact Assessment

The inclusion of third-party PIA tools will enable the inclusion of privacy risks that are not covered by the ANASTACIA platform into the due-diligence activities that are recorded in the DSPS storage. This in turn will position the DSPS as a holistic solution that covers both, privacy and security, two distinct parts of the possible data breach incidents, and which serves organizations to demonstrate their correct handling of security and privacy issues. (ENISA Threat Landscape Report 2017, p74).

### 3.1.2 The role of Privacy Assessments and DPO's feedback in the DSPS

This section states the basic principles and functions of the feedback of DPOs collected by the DSPS Questionnaire. An initial iteration of the expected questionnaires can be found in the Annexes.

To support the DSPS model, a survey on the relevance of the privacy-related functionalities of the DSPS has been conducted as part of this research. The most relevant feedback obtained can be found in Annex 3: Survey on Privacy and Cyber-security Tools.

#### Questionnaire

The DSPS will provide the user with two questionnaires (see Annex 1: PIA Questions) that will enable the assessment and documentation of the privacy risks associated with the organization system. It must be clear that role of DSPS service to DPOs is not to verify the inputs of the DPOs but to assist DPOs to check and monitor the organization' system on privacy issues compliant to the relevant regulations and guidelines.

The goal of the DSPS questionnaire is to provide DPOs a check-list to perform and evaluate the necessary actions for the change of the system back to a normal status after a privacy alert has been raised to his attention. The DSPS will inform the security alert that received from ANASTACIA (WP4) system, and also will inform the results of the mitigation action by ANASTACIA: however, the final responsibility is under DPOs and the privacy part of the seal should only be restored if the DPO declares that all relevant actions on privacy risks have been taken. It means that any potential liability is into his/her hands. Any data (files in any format such as logs, documents from the organization, etc.) a DPO provides to prove that the mitigation actions have been carried out will be stored in the off chain DSPS storage and associated with the restored DSPS seal so as to constitute proof of his/her actions in case of an audit takes place. The user (DPOs) will be requested to digitally sign (in a manner that complies with the contents of the EIDAS regulation) the questionnaire and the data he/she has provided, not only to ensure that the information contained is complete, truthful and non-refutable, but also to discharge the DSPS platform or the ANASTACIA project of any potential liability, as it is finally the legal responsibility of the DPO to perform any necessary due-diligence activities once a potential threat has been notified.

As part of both the general and post-alert questionnaires, the user will be requested to fill a Privacy Risk Assessment Table to add or update the baseline privacy threat values for the monitored system.

#### Privacy Risk Assessment Tables

The Privacy Assessment is the necessary element of the DSPS that should collect from the end user of the system in order to set up the baseline privacy risks. It must be noted that DSPS service is created for a trained auditor or experts (DPOs/CISOs) who have enough knowledge on the system and make necessary actions on the privacy events of the system. The user is required to identify Privacy risks associated with the organization system with awareness that the information will be of great importance for DSPS.

DSPS will guide the user to determine the likelihood and the impact of the risk on the organization by implementing the ISO methodology (ISO 31000:2018). The degree of risks should be determined by a combination of their impact and their likelihood of occurrence. The example of the likelihood scale (Table 1) is the variation of the likelihood scale table from IEC 62198 – Managing Risk in Projects (IEC, 2013, P.38) and the Impact scale Table taken from Enisa, Handbook on Security of Personal Data Processing (ENISA, 2017, P.11).

Potential risks should be evaluated and categorised as follows:

1. Assess the likelihood of risk (Table 1)
2. Assess the level of impact (Table 2)
3. Define the overall Risk Category (Table 3)

| LIKELIHOOD | |
|---|---|
| **Category** | **Criteria** |
| **Almost certain (1)** | Consequence is highly likely to arise |
| **Likely (2)** | Balance of probability will occur, expected at some time |
| **May occur (3)** | Could occur, but there is a distinct probability it won't |
| **Not likely to occur (4)** | Occurrence requires exceptional circumstances, Exceptionally unlikely, even in the long-term future |
| **NA/NR (5)** | |

Table 1 Likelihood evaluation criteria (Adapted from IEC 62198 Managing Risk in Projects, 2013, P. 38)

| IMPACT | |
|---|---|
| **Level of Impact** | **Description** |
| **Very High (5)** | Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.). |
| **High (4)** | Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.). |
| **Medium (3)** | Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.). |
| Low (2) | Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.). |
| NA/NR(1) | |

Table 2 Impact evaluation criteria (Adapted from ENISA Handbook on Security of Personal Data Processing, Dec. 2017, p. 11)

The combination of the likelihood and impact with the values will be considered the baseline risk level of those risks identified by the end-user as relevant for the monitored system. These values will be showcased to the end-user once a relevant alert has been raised by ANASTACIA's monitoring and reaction enablers. Additionally, the inputs of the end-user (all values and risks found on these tables) will be kept in the DSPS

storage as non-modifiable proof of due diligence. The end-user will be able to update these tables at any time through the DSPS GUI and will be prompted to do so as well after a privacy related alert is raised.

| RISK CATEGORY | | | | | | |
|---|---|---|---|---|---|---|
| LIKELIHOOD | 1 | MEDIUM | HIGH | VERY HIGH | VERY HIGH | VERY HIGH |
| | 2 | MEDIUM | HIGH | HIGH | VERY HIGH | VERY HIGH |
| | 3 | LOW | MEDIUM | HIGH | HIGH | VERY HIGH |
| | 4 | LOW | MEDIUM | MEDIUM | MEDIUM | HIGH |
| | 5 | NEGLIGIBLE | LOW | LOW | LOW | MEDIUM |
| | | 1 | 2 | 3 | 4 | 5 |
| | LEVEL OF IMPACT IMPACT | | | | | |

Table 3 Privacy Risk Assessment Table

In summary, the DSPS will support the assessment of privacy threats by an expert user (DPO) in accordance to the information found on the organization's Data Protection Impact Assessments. The Questionnaires and the Privacy Assessment Tables will help them to declare the baseline privacy risks that will be showcased once a security alert has been raised by WP4. These elements will be carried out by the expert upon installation of the ANASTACIA platform in a monitored system and will be updatable by the end-user as necessary.

After the end-user has provided the answers and any supporting documentation regarding the action the organization has undertaken to address the threats and to minimize their impact, the off-chain storage solution will securely store all associated data.

While the current privacy risk assessment has been focusing on introducing standards based categories and steps, the further research will be performed to enhance the logics how the privacy risk map to the security risk particularly taking into account the multiple threats. It will also continue to research on the efficient methodology to apply the PIA into developing DSPS logc.

# 4 DSPS ARCHITECTURE AND FUNCTIONAL COMPONENTS

This section explains the architecture and functional components that have been implemented for DSPS monitoring service under T5.2 and T5.3.

## 4.1 FUNCTIONAL BUILDING BLOCKS AND PROCESSES

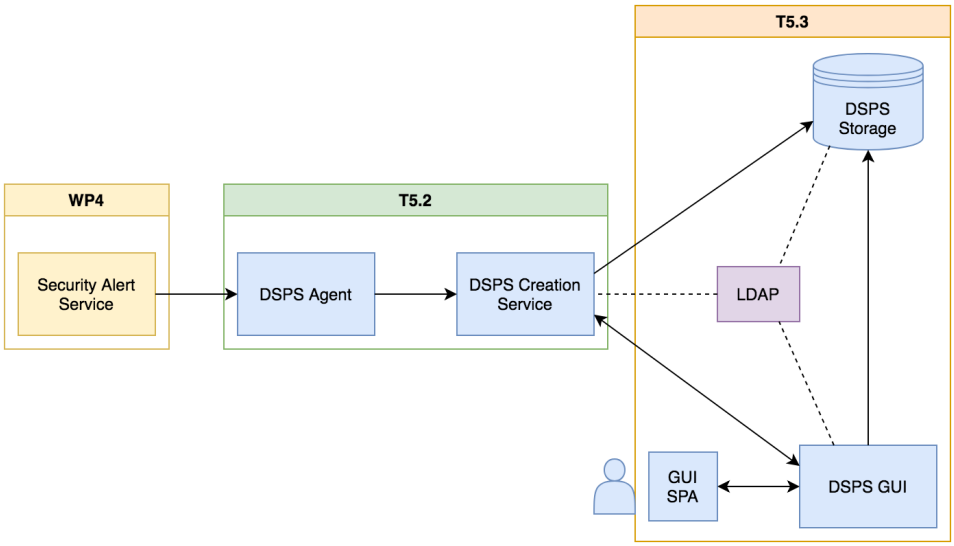



Figure 3 Currently implemented architecture

According to requirements and design specifications described in D5.1, the current implemented architecture, presented as initial demonstrator, is shown in Figure 3 from a high level point of view. There are four main components: the **DSPS Agent**, the **DSPS Creation Service**, the **DSPS Storage** and the **DSPS GUI**. The Agent is basically the intermediary between WP4 services and the DSPS plane, its role is to provide the Creation Service with security alert information received from WP4. The Creation Service main task is to create signed seals and to store them in the DSPS Storage. The Graphical User Interface (GUI) allows regular users to check the system status by inspecting the seal and its history and allows auditor users to manually modify the seal status.

In the following sections we describe the components of the DSPS architecture (coloured in blue). The LDAP server is used to authenticate and authorize API calls and it is also a necessary component of the framework implementing the DSPS Storage. It is note that the DSPS storage is based on permissioned block-chain to implement distributed ledger and distributed storage for DSPS service.

## 4.2 DSPS AGENT

The DSPS Agent is a component placed between the Security Alert Service (SAS) (developed by WP4) and the DSPS Creation Service.

### 4.2.1 Functionalities

The main functionality of the Agent is to provide information about the monitored system to the DSPS layer. The Agent listens to events produced by the SAS and triggers the consequent actions by using the DSPS Creation Service API.

The received events are:

- Security Alert: ANASTACIA detected a potential security threat
- Mitigation Action is triggered
- Mitigation Action is deployed

The currently implemented receiving event is only the Security Alert. When the Agent receives such a message, it will then forward it to the DSPS Server. A more generic interface is currently being researched. The Agent will take care of the adaption of the SAS output to the DSPS Creation Service input.

The communication between the SAS and the Agent is based on AMQP, implemented by RabbitMQ. In particular the Agent is a RabbitMQ consumer that subscribe for alerts to the SAS queue. By this way, the Agent will be asynchronously notified by the SAS, avoiding implementation of a polling-based behaviour.

The Security Alert message obtained by WP4 is serialized as a JSON. An example of the message is shown on Figure 4. This object structure is described in details in the SAS documentation. Upon receipt of the JSON file by the DSPS Agent, the file is formatted to comply with STIX as described by ANASTACIA D. 5.1.


```
{
  "AlarmEvent": {
    "USERNAME": "",
    "SRC_IP": "0.0.0.0",
    "BACKLOG_ID": "5588c551ab834cceaffe0d77d0ddefbd",
    "DATE": "2018-09-18 17:23:55",
    "DST_IP": "0.0.0.0",
    "USERDATA7": "",
    "USERDATA6": "",
    "FILENAME": "",
    "PRIORITY": 5,
    "RELIABILITY": 10,
    "ORGANIZATION": "ATOS",
    "SENSOR": "",
    "SID_NAME": "Man in the Middle on IoT data",
    "USERDATA2": "Probing attack",
    "USERDATA3": "0.79",
    "USERDATA1": "low",
    "PROTOCOL": 6,
    "RISK": 10,
    "USERDATA4": "09 10 13:24:00",
    "USERDATA5": "IoT",
    "EVENT_ID": "9af112fff7464d979d6d14e0603da4e5",
    "USERDATA8": "",
    "USERDATA9": "",
    "PLUGIN_NAME": "cyber-monitor",
    "DST_IP_HOSTNAME": "00000000",
    "RELATED_EVENTS": "[b4fc11e8bb1d080027ea052cc79b0c86]",
    "PASSWORD": "",
    "PLUGIN_SID": "8",
    "CATEGORY": "Attack",
    "SRC_IP_HOSTNAME": "00000000",
    "SUBCATEGORY": "compromise",
    "RELATED_EVENTS_INFO": { ...
    },
    "PLUGIN_ID": "70000",
    "SRC_PORT": 0,
    "DST_PORT": 0
  }
}
```


Figure 4 Security alert message

## 4.2.2 Composition

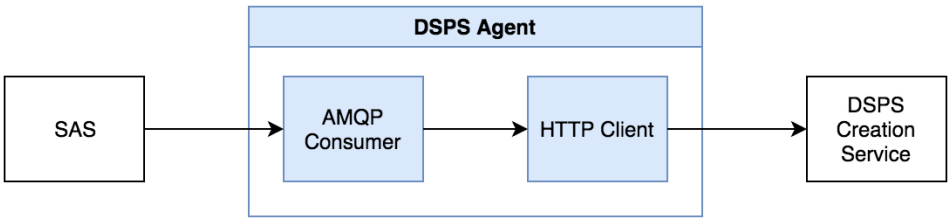



Figure 5 DSPS Agent composition

As shown in Figure 5, the DSPS Agent is composed by two modules.

#### 4.2.2.1 AMQP Consumer

The AMQP consumer is a single-process RabbitMQ client based on asynchronous I/O. The communication with the SAS is encrypted with TLS. After the client subscribes to the queue, it will be notified about every security alert emitted by the SAS, which will be then adapted (eventually) and sent to the DSPS Creation Service by using the HTTP Client module.

#### 4.2.2.2 HTTP Client

This module is a client implementing the HTTP API of the DSPS Creation Service. To be authorized to use the API, the client must authenticate himself by providing, every time, the necessary credentials passed using the Basic Authorization method. The communication is encrypted with TLS. The Agent user it is registered in the LDAP server and it will be better defined in the DSPS Storage section.

## 4.3 DSPS CREATION SERVICE

The DSPS Creation Service (CS) is the component responsible for the creation of the seal. For each created seal, the service creates a log, containing detailed information about the seal that cannot be published. The service will then use the DSPS Storage API to store the seal and its log. Another role of the service is to trigger the alert messages to notify the interested parties in real-time about the change of the seal status.

### 4.3.1 Functionalities

The main functionality is the creation of a seal given an Alert. When the service receives a Security Alert from the Agent, the following steps are executed:

1. Given the security alert, a set of potential privacy risks is derived as described in ANASTACIA D2.3.
2. A log containing all the details about the security alert and privacy risks is created
3. Given the security/privacy risks, a seal is created
4. The seal is signed with the key of the Agent that sent the alert
5. The seal is stored in the permissioned blockchain-based DSPS Storage
6. The log is stored in the private secret-sharing-based DSPS Storage
7. Interested parties (CISO, DPO, users connected to the GUI) are notified

Another functionality is the manual upgrade of the seal, which is a particular case of seal creation. This action is triggered from the GUI and allows a DPO to prove that, for example, a PIA has been performed on the monitored system. When the Creation Service receives an upgrade request, the following steps are executed:

1. The privacy and security risks are set to zero
2. A log containing all the details about the upgrade (PIA) is created
3. Given the security/privacy risks, a seal is created
4. The seal is signed with the key of the Agent related to the concerned system
5. The seal is stored in the permissioned blockchain-based DSPS Storage
6. The log is stored in the private secret-sharing-based DSPS Storage

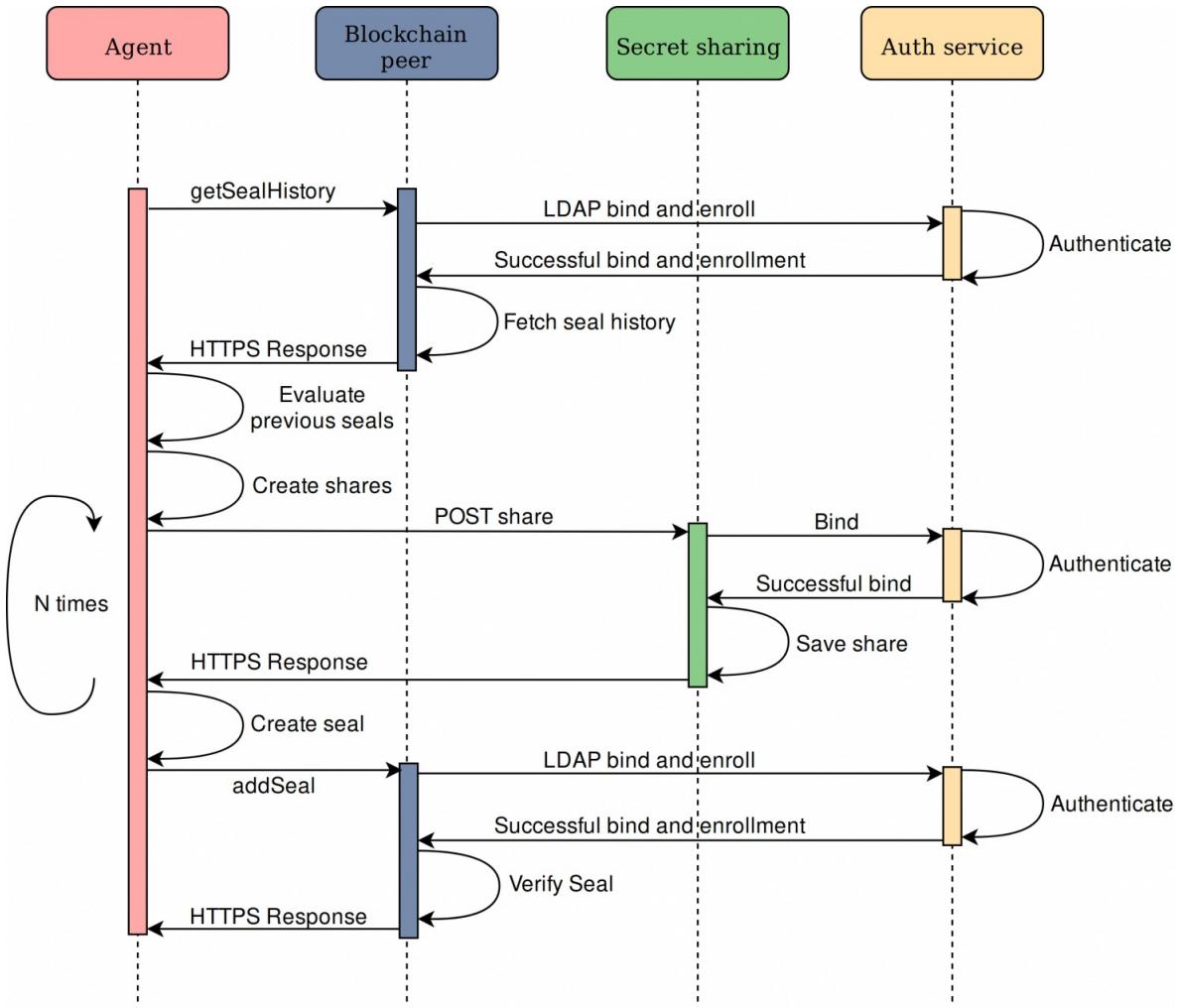



Figure 6 Process to add a new seal

## 4.3.2 Composition

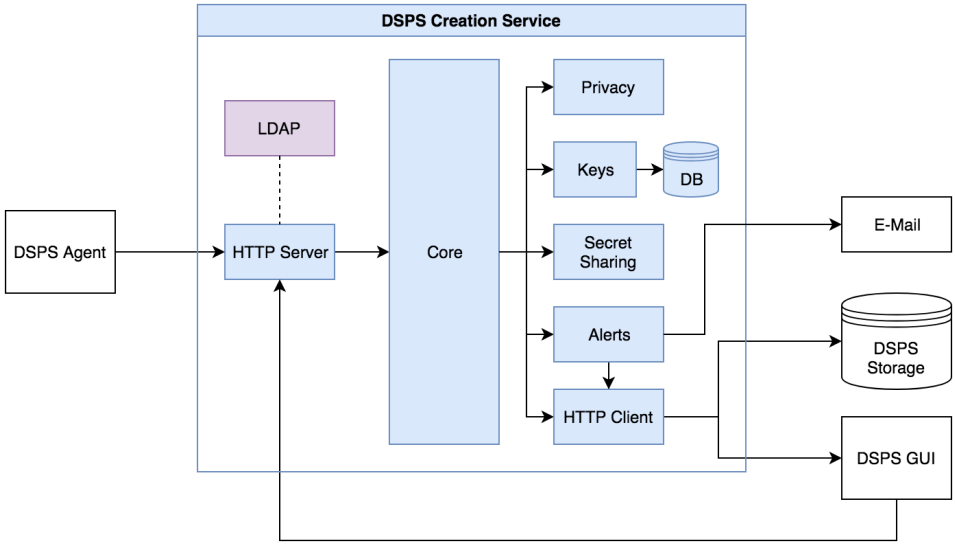



Figure 7 Creation Service

Figure 7 shows the modules present inside the Creation Service. In the following sections a short description of the modules is given.

#### 4.3.2.1 HTTP Server

This server exposes the HTTP API, allowing the use of the Creation Service functionalities. The following HTTP requests are available:

| Method | Path | Description |
|---|---|---|
| POST | /api/v1.0/seal | Trigger a seal creation given an alert |
| POST | /api/v1.0/seal/restore | Trigger a seal upgrade |

Table 4 available HTTP requests

The Access Control uses Basic Auth. Every HTTP request must contain username and password that are checked against the LDAP server. If the user exists and it is authorized, then the request will be executed.

#### 4.3.2.2 Core module

This module implements the functionalities described in section 4.3.1. To do so, it will use and combine the functions provided in the modules described below.

The seal logic defining the how exactly the global risk and the privacy risks are derived from the security alert (and the security asssessments received from ANASTACIA WP4) were still under research and in this demonstrator, a simplified logic is used for demonstration purpose of the service. The privacy risks are derived from the mappings (see Privacy module) while the global risk is simply the worst risk between the two risks, as an indicative representation of the situation. Since the privacy risks were based on a four values scale, we needed to rescale it to a ten values scale of the range of the security risks. The global risk is then computed as *max(security_risk, rescaled(privacy_risk*)). The seal logic will be further refined with the security assessment logic used by the WP4 monitoring and reaction service.

#### 4.3.2.3 Privacy module

Since the message received from the Agent only contains security information, we need a method to infer privacy risks that such security alert can cause. This module implements the mappings between security alerts and privacy risks developed in ANASTACIA T2.3. The mappings are a relationship between the type of a security alert and the current use-case as input and a privacy risk level plus a description of such risks as output. The mapping depends also on the use-case because depending on the context of the monitored system (thus the input of the end-user becomes relevant), the same alert would have different implications in terms of privacy. In the final iteration of the DSPS, these mappings will consider the initial and subsequent inputs of the DPO.

An example of such mapping would be as following Table:

| Alert Type | Use-case | Risk Level | Risk Description |
|---|---|---|---|
| MITM on IoT data | BMS4 | ¾ | Unauthorized access or disclosure of personal data (loss of confidentiality) – Access or disclosure to/of personal data generated or held by a device or object, by an unauthorized user or device.<br>Unauthorized modification of personal data (loss of integrity) – Modification or affectation to the integrity of the personal data generated or held by a device or object, |

| | | | |
|---|---|---|---|
| | | | by an unauthorized user or device.<br><br>Unauthorized or inappropriate linking of personal data (Potential for data re-identification) – Unauthorized interconnection of two or more data sources by a device, object or user in the network.<br><br>Unauthorized removal or deletion of personal data (loss of availability) – Personal data is removed or deleted by an unauthorized user or device. |

Table 5 Privacy mapping example

#### 4.3.2.4 Keys module

This module handles the public and private keys of the Agents that are allowed to write seals into the DSPS Storage. The keys for every registered Agent are encrypted and stored inside an internal database following the steps below:

- The private key and public key are put in a JSON object and encoded as UTF-8 string
- The agent password is hashed (and salted) with *SHA-256* based on the *PBKDF2* algorithm
- The keys are encrypted with the *XchaCha20* variant of *ChaCha20-Poly1305* with the hashed agent password as key and a nonce
- The encrypted keys, the nonce and the hash are then stored in an internal database and linked to the identifier of the Agent owning the keys

All used crypto functions are implementations of the *libsodium* library.

The reason of the existence of this module is due to a design decision of the DSPS Storage. For each ANASTACIA system (*device_id*) there can be only one Agent writing seals. This Agent must register his public key (bound to *device_id*) into the DSPS Storage and then only seals signed with the related private key will be accepted for that *device_id*. Later, it was introduced the necessity to manually upgrade the seal from the GUI. The new upgraded seal needs to be signed by the Agent to be stored and therefore we introduced this keys storage system to sign seals on behalf of the Agent. Since the keys are encrypted with the Agent password, Auditors willing to manually upgrade the seal will be requested to provide that password every time such operation is triggered.

#### 4.3.2.5 Alerts module

The module is responsible for generating notifications about the changes of the DSPS status in real-time. Two communication channels are used: E-mail and HTTP/Websockets.

E-mail alerts are sent to all the addresses that are registered to a particular system, which is identified by a unique identifier (*device*_id). Such entities are typically the CISO and the DPO of the system.

The second channel is about sending notifications through the GUI. All the users connected with their browsers to the GUI will be notified about changes if the seal that they are inspecting suddenly changes of status. The Creation Service will just use the GUI HTTP API to notify the backend about an update. The backend will then use WebSockets to notify the users through their User-Agents.

#### 4.3.2.6 Secret sharing module

This module is used to split the seal log according to the Shamir Secret Sharing Scheme (SSSS) so as to store it inside the off-chain DSPS Storage. According to the DSPS Storage API, the log is split by the following steps:

- The numbers *N* (total number of shares) and *k* (minimum number of shares necessary to reconstruct the secret) are defined.

- A random key is generated.
- The log is encrypted with the *XchaCha20* variant of *ChaCha20-Poly1305* with the randomly generated key and a nonce.
- The key and the nonce are split by using SSSS with *N* and *k* as parameters.
- Each triplet (encrypted log, key share, nonce share) is stored in a different node of the DSPS Storage implementing the secret-sharing service.

The SSSS functions are implementations of the *ssss* library.

## 4.4 DSPS STORAGE

In the frame of ANASTACIA project, a permissioned private ledger (known as permissioned blockchain) has been implemented and deployed. The goal to use the permissioned private ledger technology is to provide a secure and reliable storage of the continuous privacy and security seals which are measured by the ANASTACIA platform and to enable the authentication of the information stored in the off-chain log.

The design of the implemented blockchain strictly follows the requirements announced in the deliverable D1.2 and also the deliverable D5.1 about the DSPS and the associated seals. The permissioned blockchain component owns specific APIs which are used by the developers to store and to retrieve electronic seals. Of course, the blockchain is distributed by a secure manner across several virtual machines. After a deep examination of the requirements needed to store the seals, the permissioned blockchain technology is the only good candidate to ensure the immutability and the distribution of the seals, as explained in the revision of D5.1. The chosen implementation avoids a central authority and allows more flexibility than a central database cluster, for instance. The implemented blockchain is of course completely compliant with the new GDPR.

### 4.4.1 DSPS Distributed Ledger Solution

The analysis of the different requirements has determined the choice of the blockchain type. So, the implemented blockchain is a permissioned private ledger to store the seals. This allows doing the user management and the access control for the blockchain.

The chosen framework for the blockchain is HyperLedger Fabric 1.1 and 11 virtual machines are used to run our blockchain implementation. The virtual machines are running Ubuntu 16.04 LTS as operating system and a Docker swarm was set up for their deployment. A Docker swarm is a tool to cluster and orchestrate Docker containers.

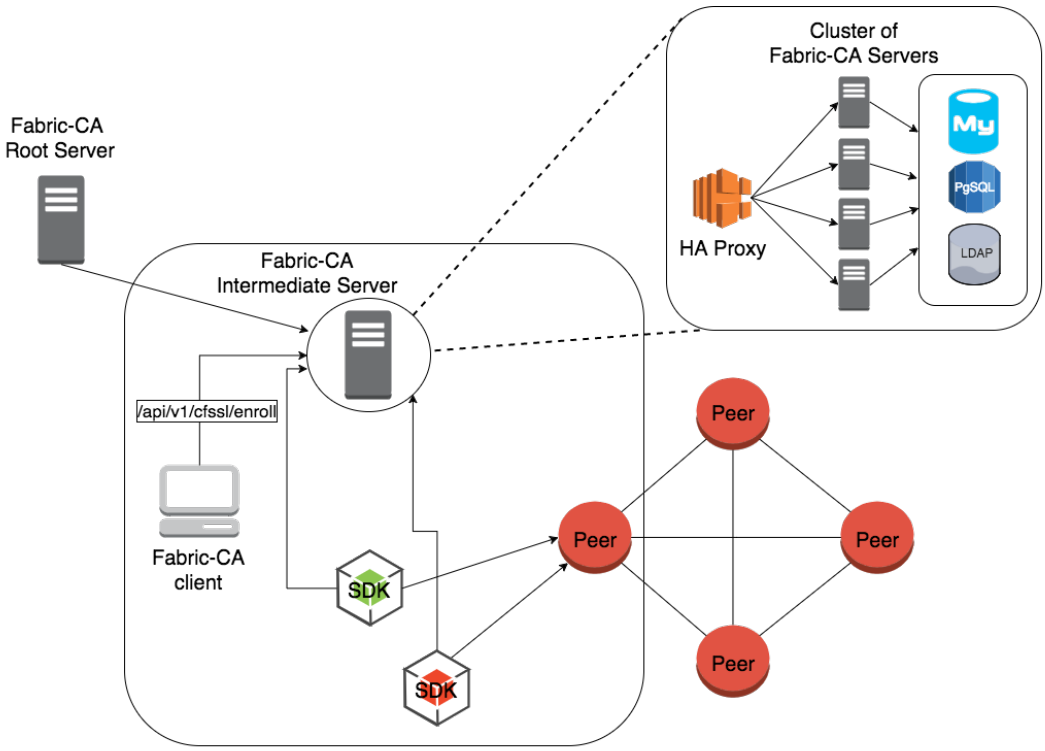



Figure 8 HyperLedger Fabric architecture

10 virtual machines are used as blockchain nodes and the last one is running the certificate authority (CA) component needed by Fabric. A CouchDB database is also used to store all the blockchain data for quick access. The architecture of a CouchDB database is document-oriented NoSQL database architecture; so, the database is a collection of independent documents. The document metadata contains revision information.

A Web server was written to get an easy access to the chaincode endpoints through a REST API. The transactions made through this API are secured by TLS. The data exchanged between the Web server and the counterpart client is formatted in JSON with a classical Base-64 encoding.

On the virtual machine running the CA component, a LDAP server was installed for the user management. The users registered on the LDPA server are pseudonymised and so, there is no explicit name in the access control process on the blockchain. Four groups of users have been defined inside the LDAP server: admin, auditor, user and agent. The admin has a total freedom to do everything. The auditor can read anything, but he cannot write anything. The user in the agent group is the only one able to submit a new seal and he is considered as the initial author of the seal. Finally, the user group can only read the seals assigned to them. The access control of the different groups of users is made through an attribute-based access control (ABAC) paradigm; in this case, the access rights are granted to users through policies combining several attributes together. The groups of users are written to the LDAP server using RSA certificates and S/MIME messages to ensure the encryption and the digital signature. For instance, the Data Protection Officer's (DPO) and the Chief Information Security Officer's (CISO) email addresses are stored in the LDAP server in a secure way.

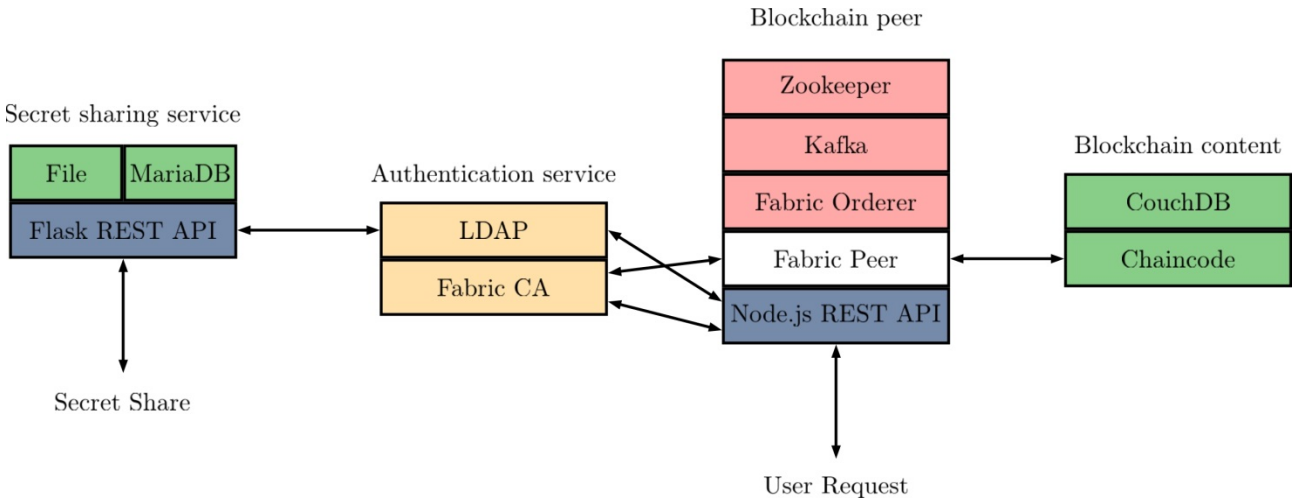



Figure 9 ANASTACIA Fabric architecture

The format of the seal is defined like the following example. The text highlighted in blue is the most important values which are also shown on the graphical user interface.

```
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
    micalg="sha-256"; boundary="----B61365C995FD5B62C722AC4BAE43ED50"

This is an S/MIME signed message

------B61365C995FD5B62C722AC4BAE43ED50
{
  "date": "2018-07-18T13:39:00.554017+02:00",
  "expiration_date": "2018-07-25T13:39:00.554017+02:00",
  "colour": 0,
  "stars": 3,
  "rm_uuid": "a3fcea9e-89cf-4c05-b229-4ff816a9d71d",
  "cause": "cause",
  "mitigation_action": "mitigation_action",
  "log": {
    "salt": "68d954f01a72c12752d4583635004e}
a048ca1f7487d44849b4adb6715c00f6db",
    "hash": "6e20653b1a2a05bbeafa78089e531874e75fb9aa55c191c423304be0476d6874c
8a98257a12dc90cd96d4dfaff54082c63237b1ab6ea6986e6b4139fa6111fac",
    "threshold": 6,
    "peers": [
      "10.1.17.201",
      "10.1.17.202",
      "10.1.17.203",
      "10.1.17.204",
      "10.1.17.205",
      "10.1.17.206",
      "10.1.17.207",
      "10.1.17.208",
      "10.1.17.209",
      "10.1.17.210"
```

Figure 10 Information contained into the seal

```
    ]
  }
}
------B61365C995FD5B62C722AC4BAE43ED50
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"

MIIGGwYJKoZIhvcNAQcCoIIGDDCCBggCAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIDdjCCA3IwggJaoAMCAQICCQCi/b00QA+6YzANBgkqhkiG9w0BAQsF
ADBOMQswCQYDVQQGEwJDSDEPMA0GA1UECAwGR2VuZXZhMQ8wDQYDVQQHDAZHZW51
dmExHTAbBgNVBAoMFE1hbmRhdCBJbnRlcm5hdGlvbmFsMB4XDTE4MDUxNjA4MzMy
MFoXDTE5MDUxNjA4MzMyMFowTjELMAkGA1UEBhMCQ0gxDzANBgNVBAgMBkdlbmV2
YTEPMA0GA1UEBwwGR2VuZXZhMR0wGwYDVQQKDBRNYW5kYXQgSW50ZXJuYXRpb25h
bDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMXHLTY4GMgJ9An5tX/N
6dvkKMziOCN2zYkggl/Hilm6NdFFECt9s1kYgJrQzbnBbJ5T5uypKs6s2FpdWkPh
OzKoOnkSE+K/TiYXSi967G8AFN3SPK3F/20thuOrQQVHp11oOsgzEFCRyWdPc2xZ
3zApgFcFsOU3tpHizGW2lNo3XW/7iWGi83C5dd+Pnlxn+t25YeUpbIvK4C28/QpG
DZRl0pHKPpnbA7mYBqVZ+YXtv9xwAIE347jmIAIoxRq9bencolh9Ji4mwQXW74Zz
j1aD2cx10zQ4q1RE51Zohko/aCAmA+Hin836LXjt01v24tiYdMrginIg5c6ywfSn
OFECAwEAAaNTMFEwHQYDVR0OBBYEFKLVvc0O2R0ZRQEZcVIUt30ZOBJiMB8GA1Ud
IwQYMBaAFKLVvc0O2R0ZRQEZcVIUt30ZOBJiMA8GA1UdEwEB/wQFMAMBAf8wDQYJ
KoZIhvcNAQELBQADggEBAKanW3QTrxOTXhvrF0/PjCiVWKPCFS7AmoxJzrBCNiVn
pK/GeFbk9x3y3pzAuTaP9+Uz9h2OEP5bl+1M9aq6/SdgrstS4S9Dktl+YjelOk4x
Y8v+MRdlu4V2cqKWdpkAzwQU2UwRy/iv0yy8hLARsvm/Xm/Suf6aHpo6+QwBzFVp
9AhU4MSXjMTKTanveSQiIlFzyxWobx6sX1o5gQOUNhLSzBCFH/wnNelc9OkY6Pv6
OqHJ158MA7rCbtxtFOseAFjoRL89GjWT4KCX0US0SoYGO8LaDLPniRS+YQlHYf6q
8fOMCYaJRFq6EUXWj9EGVCbOK10KYdTJRrrrNeZXbtYxggJrMIICZwIBATBbME4x
CzAJBgNVBAYTAkNIMQ8wDQYDVQQIDAZHZW5ldmExDzANBgNVBAcMBkdlbmV2YTEd
MBsGA1UECgwUTWFuZGF0IEludGVybmF0aW9uYWwCCQCi/b00QA+6YzALBglghkgB
ZQMEAgGggeQwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUx
DxcNMTgwNzE4MTEzOTAwWjAvBgkqhkiG9w0BCQQxIgQgFxMGtcWIxjtg8UwjjER9
NUNfXnXqUspnNiOJnVuq7C8weQYJKoZIhvcNAQkPMWwwajALBglghkgBZQMEASow
CwYJYIZIAWUDBAEWMAsGCWCGSAFlAwQBAjAKBggqhkiG9w0DBzAOBggqhkiG9w0D
AgICAIAwDQYIKoZIhvcNAwICAUAwBwYFKw4DAgcwDQYIKoZIhvcNAwICASgwDQYJ
KoZIhvcNAQEBBQAEggEAZwljrNS3FQA/9HM9HqYR4zbecm4OyUu4JvrNxz8ZBF80
gSlOtBLRlouyoj85ly+7rL6HOq/VhJEKz5S3bbtqmKj4LKecOHwpr3/UgPl5wrlD
b6r9pTT4dUGEsofObUq+gulHkxSK6AT3yMPqiphA1NkdSJkvOhtNkHYyfP00AO+L
FOvn9EjpZ+CL7qapb64zPKybcsCryZfVp7T8NWGfJcgR3UNCFicOB2joCBxJkLu5
T3WxmBdBXKwL9RlcmnQSkBNxLktbJJUUWsattsqmlnCgp2r19ndftIfQwzr8WdSX
IwtisdRhcFbdn55eyuGKO9GDrebGcQ3dJicvVnEnDA==

------B61365C995FD5B62C722AC4BAE43ED50--
```


Figure 11 Full signature included into the seal

The API for the seal storage permits to add a new device, the user's registration and a new seal. On the same manner, the history of a seal can be retrieved using the API. The data is using the principle of a Key-Value (KV) store: so, a unique identifier is linking the seal to a particular device. The access control to this API is made through the blockchain and the login to the LDAP server. Indeed, the blockchain determines if a given user is authorised or not to read or write some information. This is also valid for the access control of the off-chain storage API. As mentioned previously, the API calls are secured by the TLS protocol. On the same time, the problem of Cross-Origin Resource Sharing (CORS) was taken into account to ease the remote access to the seal storage API. The following table displays the available methods of the seal storage API used to talk to the peer blockchain node:

| Method | Path | Description |
|---|---|---|
| GET | / | Check if the REST API is up and running. |
| GET | /status | Check if the chaincode is deployed or not on the node. |
| POST | /addDevice | Add a new device to the blockchain. |

| | | |
|---|---|---|
| POST | /deleteDevice | Delete a device from the blockchain. |
| POST | /addUserRegistration | Add a new registration for a user to allow reading seals for a specific device. |
| POST | /addSeal | Add a new seal on a device. |
| POST | /setDevicePubkey | Set a new public key for a device. |
| POST | /deleteUserRegistration | Remove access from a user to see device seals. |
| POST | /setDevicePublicAccess | Set a device public access right. |
| GET | /getUserRegistration | Get a list of registrations for a specific user. |
| GET | /getDeviceRegistration | Get a list of registrations for a given device. |
| GET | /getLastSeal | Get the last seal for a device. |
| GET | /getSealHistory | Get the entire seal history for the device. |
| GET | /getAllDevicesHistory | Get the entire history of the devices. |
| GET | /getDevicePubkey | Get the device public key. |
| GET | /getDevicePublicaAccess | Get the accessibility of the device. |
| GET | /pub/getLastSeal | Get the last seal. |
| GET | /pub/getSealHistory | Get the history of the seal. |
| GET | /pub/getDevicePubkey | Get the public key of the device. |

Table 6 Seal storage methods

### 4.4.2 DSPS Distributed Storage Solution (OFF-CHAIN STORAGE)

For the sensitive information, an off-chain storage based on Shamir secret sharing was built. This is required to be fully compliant with the new GDPR. The definition of the blockchain implies to have an immutable copy forever written in a ledger, which is not compliant with the right to modify or to erase data. The off-chain storage positively answers to this issue by providing a more conventional access to the data; in this case, the data can be edited or deleted. The data is stored into a different encrypted system than the blockchain, but a proof of its existence and its integrity is written into the blockchain. This ensures at the end the protection of the user's privacy. With the off-chain storage, no blockchain node has the full information and only the combination of the information provided by each node permits to obtain useful information. The Shamir secret sharing can be seen as a Key-Value (KV) store with the same access control as the blockchain. A specific API was designed for the off-chain storage and has the same properties as the seal storage API, in particular for the security aspect. The following table shows all the available methods of the secret sharing API used in the context of the off-chain storage:

| Method | Path | Description |
|---|---|---|
| GET | / | Give the status of this API. |
| PUT | /log | Add a new share to the storage of this node. |
| GET | /log | Get the data from the storage. |
| DELETE | /log | Delete data from the off-chain storage. |

Table 7 Secret sharing methods

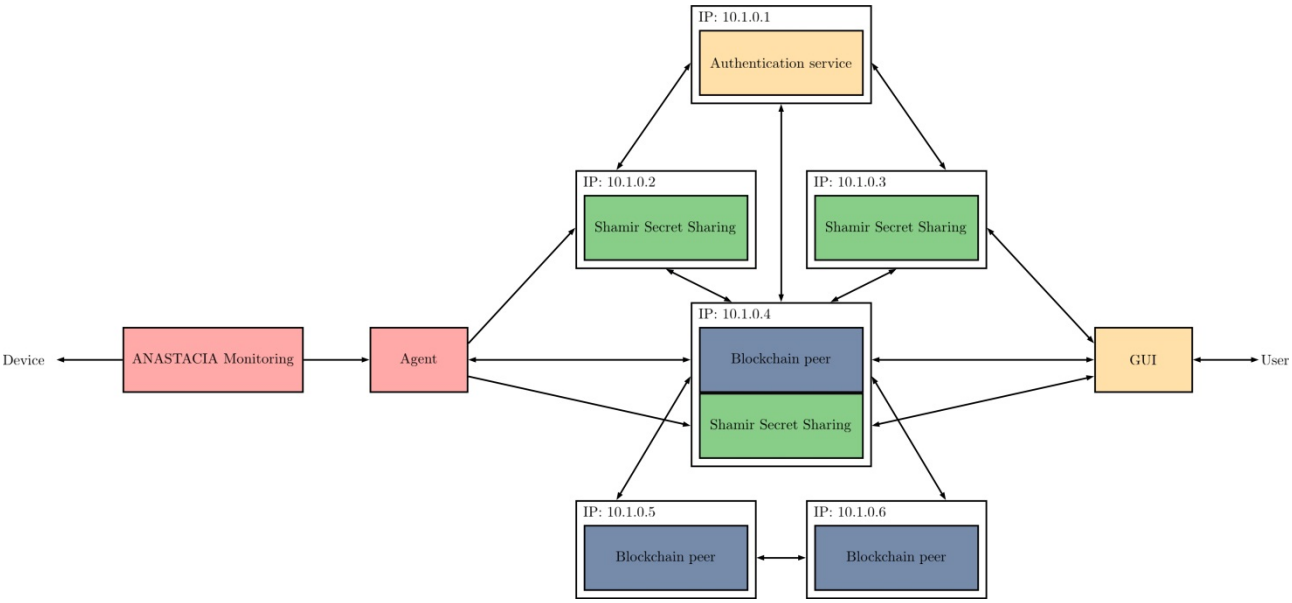



Figure 12 DSPS composition with secret sharing models

### 4.4.3 DSPS Distributed Ledger and Distributed Storage: Performance Evaluation

After implementing our system, we wanted to know if our solution is scalable, or simply how fast it processed seals. Surely, HyperLedger has some big advantages over other blockchain technologies because of the lack of Proof-of-Work and because chaincodes are not getting executed on all nodes. Yet, it is important to make the performance evaluation with the quantifiable measurement of the speed of the system we built.

#### 4.4.3.1 Methodology

Our setup is running on 11 Vmware virtual machines. Each of them has 4 logical Intel Xeon E5-4607 cores (2 physical cores that are HyperThreaded) clocked at 2.20GHz, 4GB of memory and 25GB of ATA hard disk. We were initially a bit reluctant to run any benchmarks since we are running our setup on shared hardware, which means that it is not similar to a real-world setup. CPU clocks are shared, as well as hard disk I/Os, networking or memory. If a third party VM starts to have heavy load, this is possible that it will monopolize the resources, thrash memory or CPU caches, creating noise in the values of our benchmark. All in all, this bias should be minor when dealing with our full setup.

Then, we choose to bench the most important functions, namely “addSeal” and “getSealHistory” since they will be the main functions called by the GUI and other components for DSPS service. The other functions will either have similar performances, or would not make any sense to benchmark (as specific function are exclusively used by the administrator of the system).

Two types of measurements are performed – throughput and latency. For throughput, it was measured the number of transactions (seals for us) per seconds that we can submit to the blockchain. We can modify the number of seals to add, the number of users pushing those seals and, finally, the number of nodes that should push seals concurrently, and see how long it takes our system to ingest the data. The latency of our system is also measured by finding the delay it takes for a single transaction to be added in the ledger. A similar methodology compared to the throughput should be used.

For testing, it was measured the entire pipeline of the data, not only a sub-component. For that matter, the time it took to perform REST queries (/addSeal or /getSealHistory) with Python and Bash scripts.

Since, we are using a Kafka cluster coupled with Apache Zookeeper for the consensus, it means that many options can be tweaked in terms of block size or creation time. We fixed those options so that a block can be created every second, with a maximum of 1000 transactions or 99MB of data (whichever reaches the limit first) into each block. We initially changed those values from a 2 seconds time to create blocks and 10 transactions per block. If we change these values, we do observe that our results change as well.

When benchmarking throughput, we would asynchronously send, with the help of cURL, numerous requests. The benchmark machine had 8 vCPU and 32GB of memory, in the same VM cluster as the blockchain nodes. This means that we may have resources conflicts between the benchmark machine creating curl processes and the blockchain network. We tried to measure the time when sending between 1 and 20 seals, from 1 to 25 users, on 1 up to 10 nodes.

For latency measuring, we went the simple route of putting work on the system and add transactions that we track how long they take to be processed. To have better values, we would constantly add new transactions while the system was on load, and take the median of those values as the processed measurement.

When measuring the performance of /getSealHistory, we decided to exclusively measure the throughput because latency was really too small to be significant. We measured the performance on one node, since chaincodes are getting executed locally on the machines, and will not perform writes with queries. So, no consensus and communication with other peers is needed in queries. We did modify the number of seals that returns to our request and the number of users that fetches concurrently their seals to get our time value.

We decided not to measure our Shamir secret sharing service or seal creation code since it would be too dependent of the client machine. For example, our implementation of secret sharing greatly varies in speed if we use a *Nodejs* implementation or the C implementation of *libsodium* because of the cross compilation overhead of JavaScript. This would not make sense to provide values since the throttling factor is the client creating the shares or the seal, and we do not have a specific definition of the performance of this machine.

Finally, some performance goals were mentioned within deliverable D6.1. The initial target was to have latency under 1 second, be able to manage more than 20 users with a low error rate. No real throughput goal was mentioned since seals do not get created at a regular speed. Already, we can comment that the target latency does not seem to be realistic for a blockchain since we only emit a block every second, which is already very low compared to other solutions. Most likely, this is some remains of previous work on ANASTACIA that predated the blockchain design.

#### 4.4.3.2 Evaluation results

The measurement results of the main values for latency, throughput and query speed is shown in Table **8**. We rounded our results to the two digits after the comma, and we decided to provide the minimum, the maximum, the median, the average as well as the standard deviation of our measurements.

| Method | Min | Max | Median | Average | Standard deviation |
|---|---|---|---|---|---|
| **addSeal throughput** | 0.67 seals/sec | 33.21 seals/sec | 22.00 seals/sec | 21.49 seals/sec | 6.17 seals/sec |
| **addSeal latency** | 1.40 sec | 13.14 sec | 1.94 sec | 2.77 sec | 2.11 sec |
| **getSealHistory throughput** | 3.64 seals/sec | 1339.93 seals/sec | 604.01 seals/sec | 582.64 seals/sec | 387.02 seals/sec |

Table 8 Summary of the benchmark values

We saw that we had a lot of noise in our measurements. The reason is that it comes from the benchmarking solution that overloaded our blockchain network and may even have caused some errors we observed. We did try to minimize its effect but for the moment it cannot be avoid a small error margin with the current benchmarking solution.

In terms of adding new seals, we can see that it takes linearly more time to add more seals. This was something to be expected by adding all the operations required to add a new seal. We did see that adding more nodes allows adding more seals without reaching this saturation limit.

For latency, we did see that it was a more or less flat line, and only increased if we added more users. This is probably caused by the time it takes to broadcast the new seals to all peers. But, compared to throughput, this is a relatively negligible slowdown.

For queries, no communication was required with other peers. This means that queries are way faster to execute than any other operation. With queries, we did see that we do have a linear increase of throughput if we increase our amount of seals to fetch. The only appearing limit seemed to be the underlying CouchDB database that was overloaded.

Finally, compared to the project's requirement evoked in deliverable D6.1, we can see that we have more or less matched our goals. Our solution is able to manage more users pushing more seals that what ANASTACIA is supposed to do, while still being really close to our latency objectives. We can try to lower the block creation time even more, but we decided against this since we think it is more important to be able to manage more users than have an even smaller latency.

## 4.5 DSPS GRAPHICAL USER INTERFACE

The GUI allows users to inspect the current status of the seal for a given monitored system. In principle there should be three groups of users with different levels of authorization:

- Users
- Auditors
- Admin

Users are any user willing to check a system status, Auditors are CISO and DPO of a system and Admin is the administrator of the DSPS for all systems. This section provides brief description of the current version DSPS GUI developed for the initial DSPS demonstrator. It is continuous on development under T5.3.

### 4.5.1 Functionalities

There are currently four implemented functionalities. The first one is the possibility to inspect the current seal status and the history of changes and it is available to all user groups. Only global information is shown such as:

- Global status
- Security risk
- Privacy risk
- System identifier (*device_id*)
- Cause

Figure 13 shows the main dashboard displaying the seal status (on the left) and the seal history (on the right).

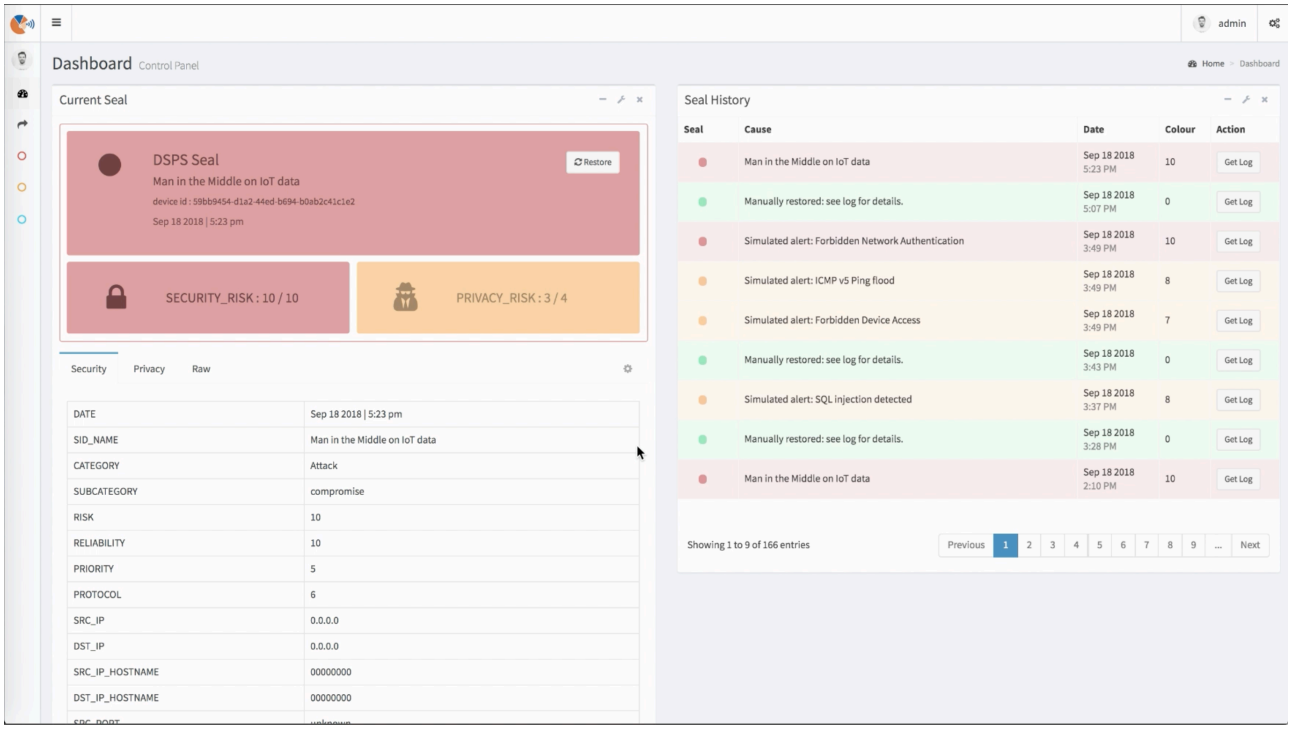



Figure 13 GUI Dashboard

The second functionality allows connected users to be notified in real-time about a change of the seal status. This is implemented using WebSockets. When a user login in the GUI, a WebSocket connection is established with the GUI backend. When the DSPS Creation Service creates a new seal, it will notify the GUI backend about what system changed. Then, the backend will send a message to all connected users that

are currently inspecting that system. This functionality is available to all user groups. Figure 14 shows the notification message received by a user, displayed on top of the dashboard.

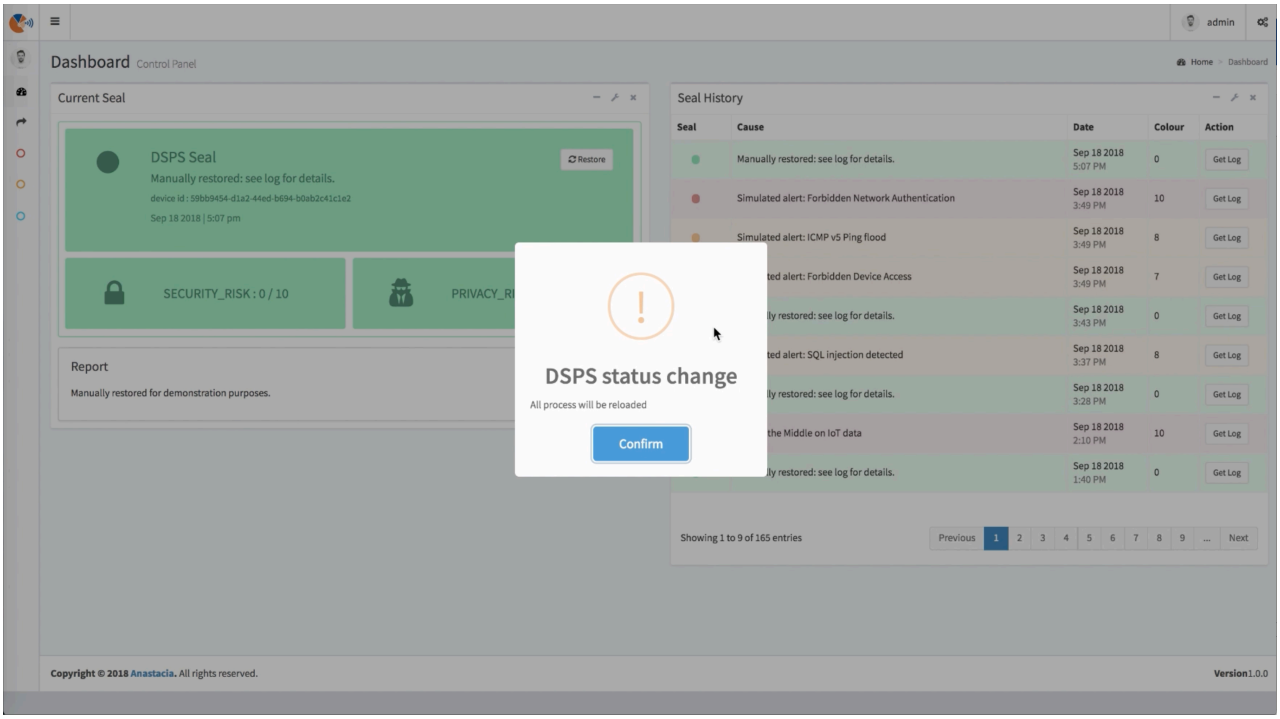



Figure 14 GUI Status change alert

The third functionality allows retrieving and inspecting the log related to the current and past seals. This action is only available to Auditors and Admin as it is private data that may contain sensible information. Figure 15 and Figure 16 show respectively the security and privacy details contained in the seal log.

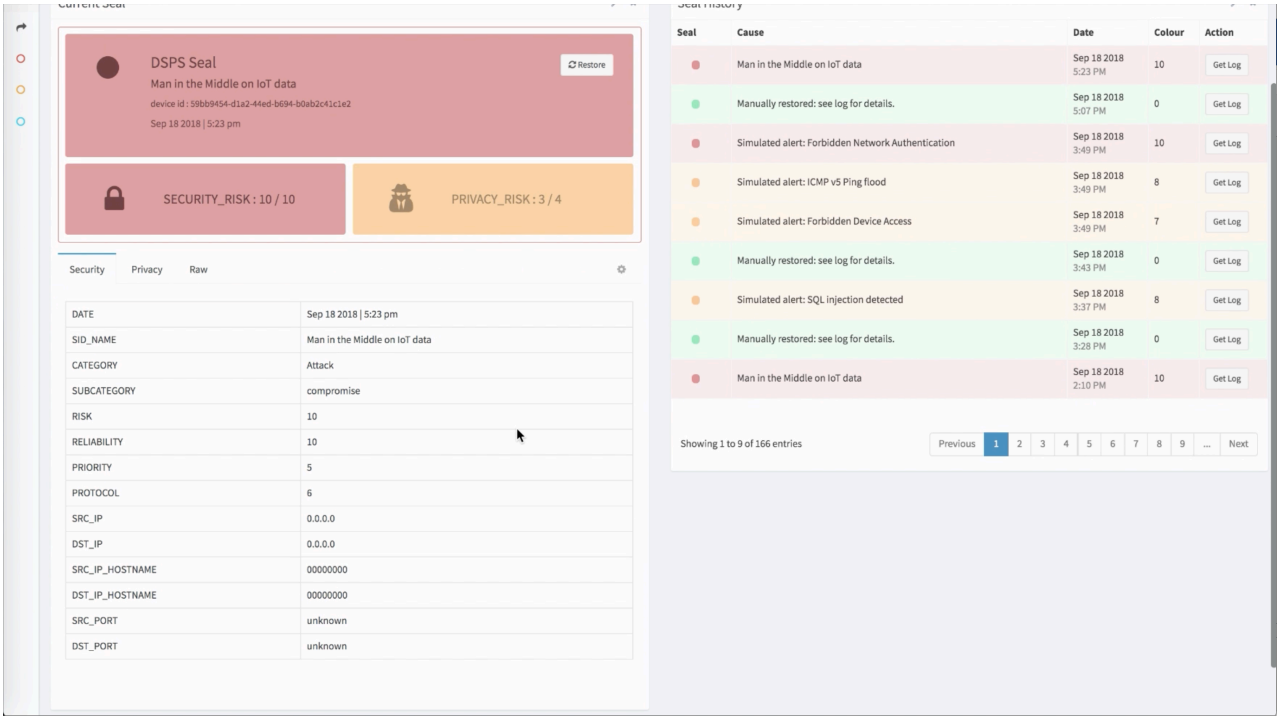



Figure 15 GUI alert detail overview

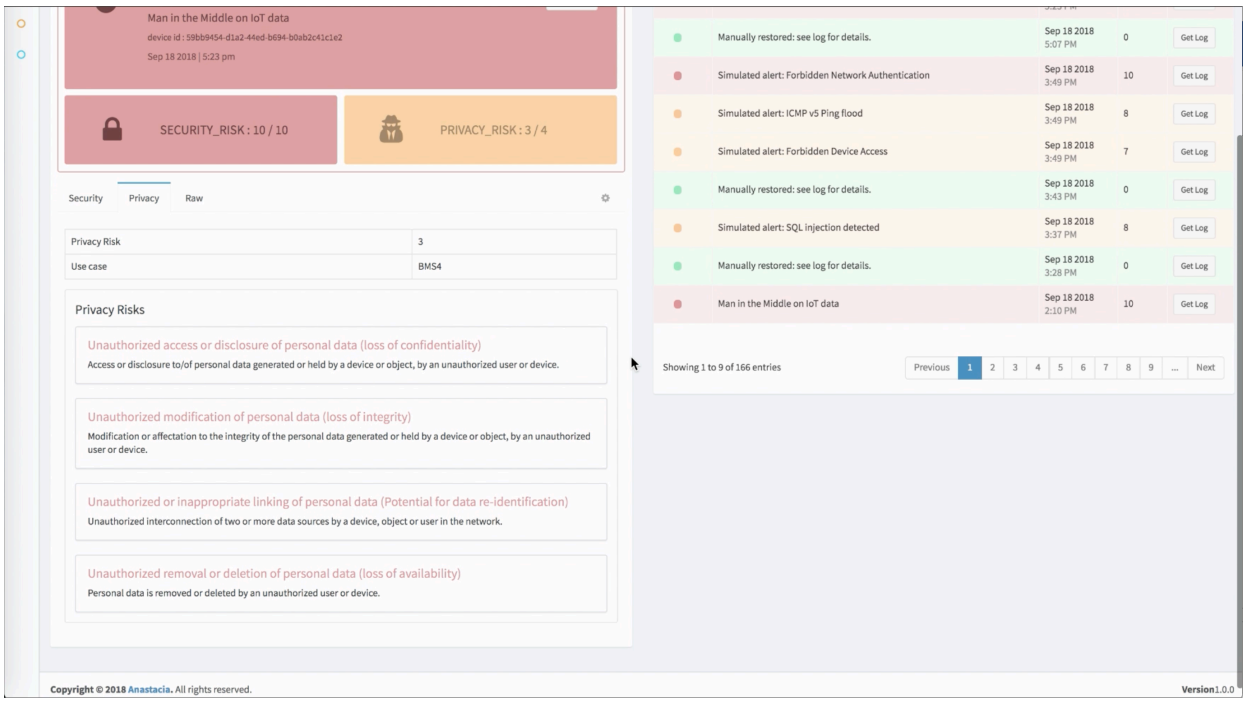



Figure 16 GUI Privacy risk overview

The fourth functionality is the possibility to manually upgrade the seal to a zero-level risk. This action requires the user to provide detailed information about the reasons of such upgrade and it is only available to Auditors and Admin. Figure 17 shows this scenario.

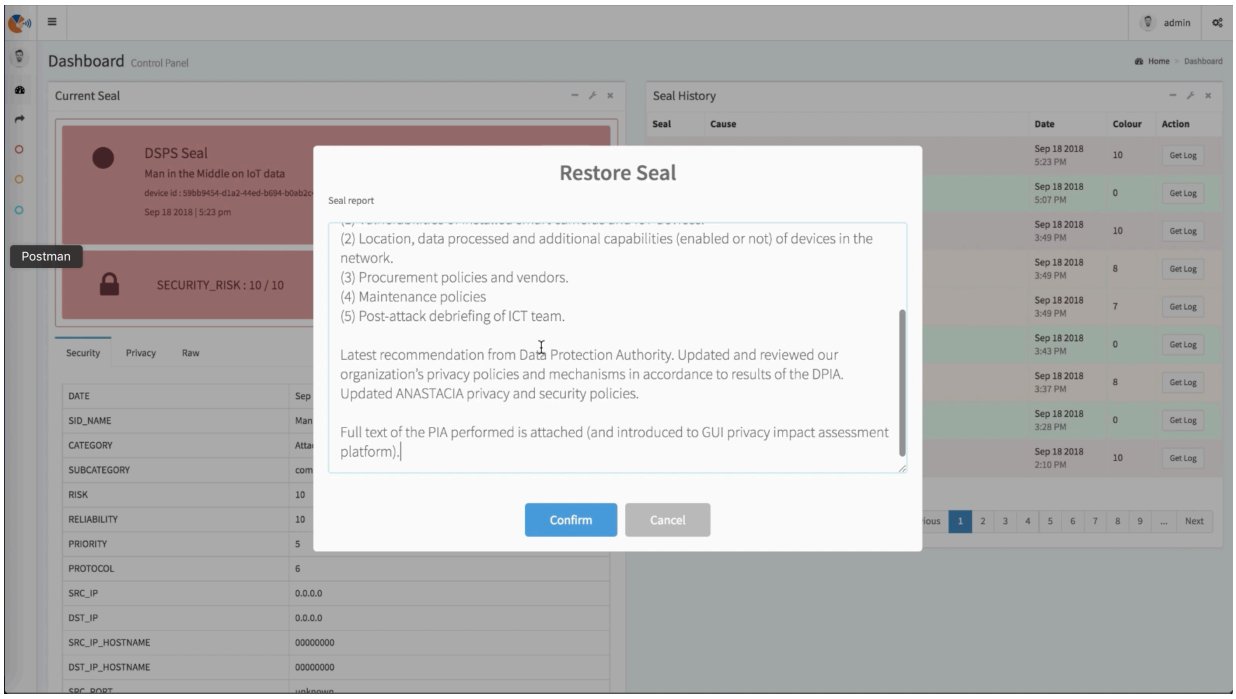



Figure 17 GUI seal restore form

A more detailed explanation of the GUI is given in the video demo available at the following URL:

https://www.youtube.com/watch?v=opb8fWSP_-w

## 4.5.2 Composition

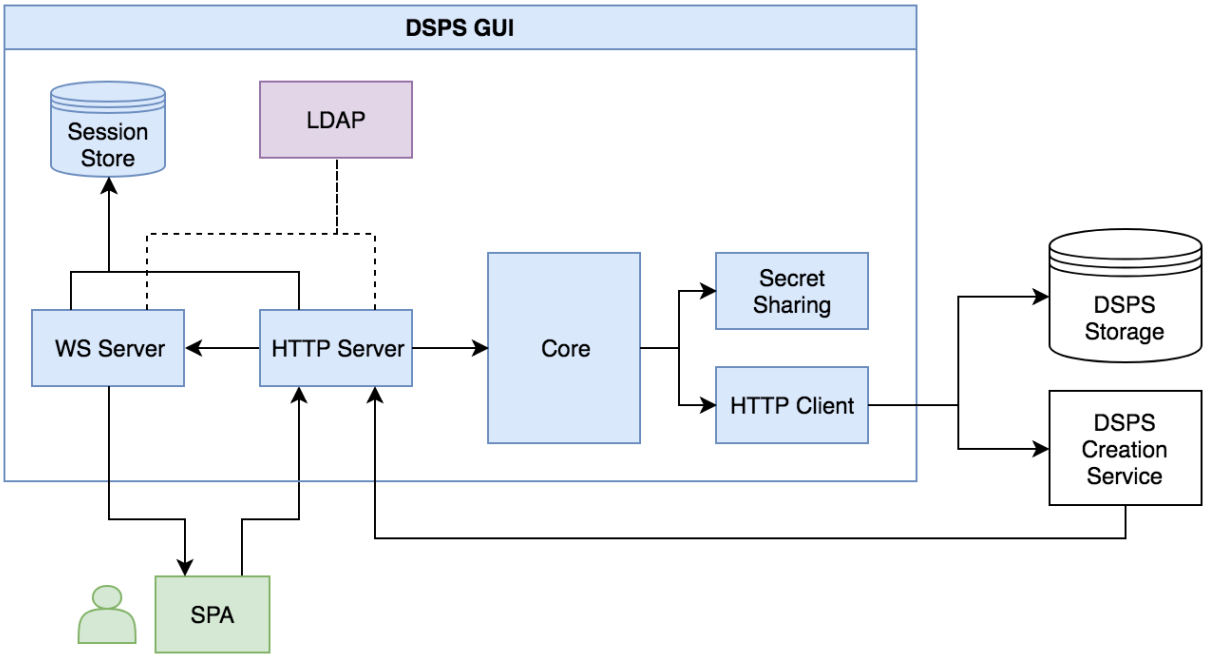



Figure 18 DSPS GUI composition

The GUI is basically divided in two parts, the backend server (blue) and the frontend Single Page Application (SPA) running inside the User Agent (the browser of the user). The SPA and the backend communicate in two ways. One is driven by the user and will cause the SPA using the backend HTTP API to perform some requests. The other is driven by the backend and it uses the WebSocket connection established between the two sides to push notifications of the status change of the seal to the SPA and therefore to the user. Seal status updates are always received from the DSPS Creation Service.

### 4.5.2.1 HTTP server

This server exposes the HTTP API, allowing the user to obtain the Single Page Application and to use the GUI functionalities. It is worth to recall that in the API terminology a *device_id* is a unique identifier representing a single system monitored by the ANASTACIA framework. The following HTTP requests are available:

| Method | Path | Description |
|---|---|---|
| GET | / | Get the Single Page Application (SPA) |
| POST | /login | Login the user and set the session cookie |
| POST | /logout | Logout the user and destroy the session |
| GET | /api/seal/<device_id> | Get last seal for a given system |
| GET | /api/seal/<device_id>/history | Get all the past seals for a given system |
| GET | /api/seal/<device_id>/badge | Get the badge representing the last seal (SVG icon) |
| GET | /api/seal/<device_id>/log | Get the log of a given seal |

| | | |
|---|---|---|
| POST | /api/seal/<device_id>/upgrade | Upgrade the seal for a given system |
| POST | /api/seal/<device_id>/downgrade/notify | Notify connected users about a status change of the seal (this request can only be executed by the DSPS Creation Service) |

Table 9 available HTTP requests

API requests must include Basic Auth credentials that are checked in the LDAP server. The HTTP server provides an encryption layer (TLS).

#### 4.5.2.2 Core module

This module implements the functionalities described in section 4.5.1. To do so, it will use and combine the functions provided in the modules described below.

#### 4.5.2.3 Secret Sharing module

This module recombines the log of a seal after a sufficient number of shares is retrieved from the DSPS Storage. The log is recombined by following the steps above:

- A sufficient number of log shares is retrieved from the DSPS Storage API. This number and other information necessary to perform these requests is present inside the seal we want to inspect.
- From the received triplets (encrypted log, key share, nonce share) the key and the nonce are combined using the *ssss* library implementing Shamir Secret Sharing Schema.
- The log is decrypted by using the key and the nonce (*XChaCha20* variant of *ChaCha20-Poly1305*).

#### 4.5.2.4 HTTP client

This module is a client that uses the HTTP APIs of the DSPS Storage and of the DSPS Creation Service. Since the Storage is a distributed ledger, the client implements a specific behaviour in case a request fail, which consist of re-trying the request on other nodes. The Creation Service API it is only used to manually upgrade the seal. This action can only be executed by an Auditor user.

#### 4.5.2.5 WebSocket server

This module allows the connected users to be notified in real-time about changes of the seal status. When the SPA is started on user browser, it will establish a WebSocket connection with the backend server. If the connection is authorized, it will be registered as listener for the given system. This means that every time the backend server is notified by the DSPS Creation Service about a status change of the seal related to the system represented by *device_id*, the backend server will then send a message to all WebSocket clients that are registered to that *device_id*. The SPAs will receive that message and will notify the users through their browsers. This schema is an implementation of the observer design pattern.

#### 4.5.2.6 Access control and sessions

Access control is managed with classic login and cookie session. The cookie session contains only a session identifier and the user information is kept server-side on the session store. The cookie can only be set if HTTPS is used and it is not accessible from Javascript. It also has the *sameSite* attribute to prevent CSRF attacks, however this attribute is not yet fully supported by all browser. The alternative way was to use a CSRF token that the SPA will attach to every non-GET request of the API.

# 5 SUMMARY AND FUTURE WORK

The D5.2 is a demonstrator of DSPS developing under WP5 in ANASTACIA and this document explains the design principle and requirements it follows for its implementation, and states the privacy impact assessments and its role in DSPS service, describes DSPS implementation architecture together with the DSPS components and APIs. It also provides the evaluation results of the DSPS system with implemented distributed ledger (permissioned blockchain) on throughput and latency with number of seals and number of users.

The development is ongoing under T5.2 and T5.3, and it will continue on research and development on the following points, that will be delivered in D5.3:

- Interoperability of the DSPS with privacy management software.
- The adaptation of the Agent/Creation Service interface to future research results, in particular about a standardization of the security alert definition.
- The enhancement of the seal creation service considering the outputs from official PIA tools (such as the one developed by CNIL). Particularly as related to the Privacy Risk Assessment Tables.
- Iterative development and evolution of the seal logic in line with the rest of the ANASTACIA framework and enablers. With close collaboration with WP4 on the capabilities of the Monitoring and Reaction Service, additional functionalities will be introduced to the DSPS logic. The research results will be adapted to the implementation of the Seal Creation Service, in particular about the seal logic and the management of multiple threat tickets.
- Continuation of implementing the interface with WP4 services, in particular the receiving of information about the mitigation actions.
- Continuation of the GUI development and adaptation of the future research results, particularly on PIA taken into account to the requirements set by T5.1.

# 6 REFERENCES


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

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 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

International Organization for Standardization. (2011, November). ISO 19011:2011 Guidelines for auditing management systems. Retrieved from https://www.iso.org/standard/50675.html

International Organization for Standardization. (2012). 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. (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 Telecommunications Union. (2012, 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. (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

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

# 7 ANNEXES

## ANNEX 1: PIA QUESTIONS

This annex presents two questionnaires to be presented to the DSPS end-user at two stages of the process:

- The initial questionnaire precedes the implementation of the Dynamic Security and Privacy Seal within the system of the end user. This questionnaire will enable the end user to assess the Privacy Risks before the connection with the ANASTACIA Network. Created as a check list the next 30 questions will help DPO and CISO to evaluate the privacy requirements in accordance with the GDPR obligations. The end user of the DSPS will be required to submit all the necessary documentation that will help DSPS to anticipate possible issues when it comes to privacy and to propose the mitigation activities.
- The short feedback questionnaire will be presented to the end-user after an alert has been raised and will serve to provide additional information on the threat and the mitigation activities the organization has been carried out. These questions will be complemented with the supporting data that is provided by the end-user.

### Initial Questionnaire

In order to connect to ANASTACIA platform and to implement the Dynamic Security and Privacy Seal you need to check the privacy practices within your organization. If your organization process the personal information of EU citizens, you need to submit the risk assessment in accordance with the international standards in risk management. This questionnaire is based on the General Data Protection Regulation requirements.

Please answer on the following questions that will qualify you for the further analysis (YES or NO):

#### Introduction questions

1. Does your organization have publicly accessible Information Privacy Policy that explains the processes related to personal data? (If yes, attach the document)

2. Does your organization have the Data Protection guidelines and data protection goals defined? (If yes, attach the document)

3. Does your organization have the Information Security Policy defined? (If yes, attach the document)

4. Does your organization have the processes for the implementation of the Privacy Policy, Data Protection Guidelines and Information Security Policy? (If yes, attach the document)

5. Does your Management System ensure the monitoring process of the implementation of the Privacy Policy and Data Protection Guidelines and enables the continual improvement of the implementation of these rules?

6. Do you inform the data subjects about the changes of your Privacy Policy?

7. Did you perform an audit to ensure compliance with data protection regulations? (If yes, please attach the Audit Report)

8. Did you implement the certification on personal data protection? (If yes please attach your certificate/s)

CISO and DPO

9. Do you have an appointed Data Protection Officer (DPO)?

10. Is the Data Protection Officer (DPO) function separated from the Chief Information Security Officer (CISO) function within your organization?

11. Did you designed your DPO on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of GDPR? (If yes, attach the Curriculum Vitae)

12. Are the contact details of the data protection officer published by your organization and communicated to the supervisory authority regarding the Data Protection? (If yes, attach the link)

13. Does your DPO work independently respecting the principals of confidentiality and impartiality and is involved, properly and in a timely manner in all issues which relate to the protection of personal data?

14. Does your organization support the work of appointed DPO by providing resources necessary to carry out all its tasks related to personal data and processing operations, and to maintain his or her expert knowledge?

## General assessment

15. Does your organization collect the personal data for "specified, explicit and legitimate purposes" and doesn't process that data in a manner that it is not compatible with those purposes"? (Article 5.1.c, GDPR)

16. Does your organization process the Personal Data lawfully, fairly and in a transparent manner in relation to the data subject? (Article 5.1.a, GDPR)

17. Are you able to demonstrate that the data subject has consented to processing of his or her personal data and that is easy to withdraw the consent? (Article 5.1.a, GDPR) (If personal data processing within your organization is based on consent of data subjects)

18. If you process children's personal data, have you asked for consent from their legal representatives? (Recital 38, GDPR)

19. Are the personal data that you collect "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"? (Article 5.1.c, GDPR)

20. Are the personal data that you collect kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed? (Article 5.1.e, GDPR)

21. Are the personal data that you collect processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure? (Article 5.1.f, GDPR)

22. Where personal data that you collect relate to a data subject, can the data subject easily request the access to their personal information from you, update its personal data, request you to delete, to stop processing the data or to ask the data to be returned or distributed to third parties? (Article 14, GDPR)

23. Has your organization implemented appropriate technical and organisational measures to ensure and to be able to demonstrate that data processing is performed in accordance with GDPR regulation? (Article 24, GDPR)

24. Does your organization only use the processors that guarantee the implementation of appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject? (Article 28.1, GDPR)

25. Did your organization carry out appropriate technical and organisational measures to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR? (Article 25.1, GDPR)

26. Did your organization implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed? (Article 25.2, GDPR)

27. Did your organization implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk:

1) pseudonymisation and encryption of personal data,

2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(Article 32.1, GDPR)

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

28. Does your organization respect the duty to notify the data breach to no later than 72 hours after having become aware of it?

29. Did your organization carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, the data protection impact assessment? (If yes, attach the document)

30. If your organization transfer personal data to third countries or international organizations, do you have a proof that the level of protection of data is not undermined?

Disclaimer

The information above does not constitute legal advice. You should consult an attorney if you'd like advice on your interpretation of this information or its accuracy.

## Short feedback questionnaire:

1. Was this alert relevant?

If YES:

3. Was this a privacy related issue?
4. Did the technical contingencies mitigate the threat?
5. Did you carry out any mitigation activities? (Please provide documentary proof of your actions)
6. What is the scope of the compromise?
7. How many systems or IoT devices are affected?
8. How do you contain the attack?
9. How you are going to prevent future attacks?

10. Are you going to communicate the alert and to whom?
11. Are you going to mobilize the Cyber Security team?

# ANNEX 2: RELEVANT METRICS AND INDICATORS FOR ADDITIONAL VISUALIZATION CAPABILITIES

Potential metrics to be introduced from ITU-T X.1208 (01/2014) include:

- Mean time to mitigate vulnerabilities
- Remote access control with security functionalities for intrusion prevention or intrusion detection
- Personally identifiable information protection (to be measured throughout DPIA)
- Mean time to patch (to be applied to address Personal Data Breaches)
- Personally identifiable information leakage (to be measured in post-breach PIA)
- Ratio of authorized devices (information could be obtained from orchestrator, network topology and PIA)
- Mean time to incident discovery
- Distributed denial of service measures (import this information from WP4)
- Audit log performance (based on the audit logs collected in the DSPS)

These indicators have been defined by ITU-T X.1208 (01/2014) as follows:

**Table 8-4 – Indicator 4: Mean time to mitigate vulnerabilities (system level and programme level, smaller-better)**

| Field | Data |
|---|---|
| Indicator ID | Mean time to mitigate vulnerabilities. |
| Goal | The indicator is designed to indicate the performance of the organization in addressing identified vulnerabilities. The less time required to mitigate vulnerabilities, the more likely an organization can react effectively to reduce the risk of exploitation of vulnerabilities. |
| Indicator | Mean-time-to-mitigate-vulnerabilities quantifies the average time to mitigate vulnerabilities identified in an organization. |
| Formula | Sum (Date_of_Completion_Mitigation – Date_of_Detection)/Count (Mitigated_Vulnerabilities) |
| Raw data | • Date of detection of vulnerabilities.<br>• Date of mitigation of vulnerabilities.<br>• Total number of detected vulnerabilities.<br>• Total number of reported mitigated vulnerabilities. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | • Effectiveness/efficiency. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | Recommendation ITU-T X.1521, Common vulnerability scoring system, [b-ITU-T X.1521] and Recommendation ITU-T X.1520, Common vulnerabilities and exposures/[b-ITU-T X.1520]. |

**Table 8-14 – Indicator 14: Remote access control with security function for intrusion prevention or intrusion detection (system/programme level, bigger-better)**

| Field | Data |
|---|---|
| Indicator ID | Protected remote access points. |
| Goal | The organization should implement a security function for intrusion detection or prevention to protect the organization's internal assets. |
| Indicator | Percentage of protected remote access points. |
| Formula | (Number of remote access points that implement the security function with intrusion detection and prevention/Total number of remote access points ) × 100. |
| Raw data | • Number of protected remote access points that implement the security function for intrusion detection or prevention.<br>• Number of remote access points. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | • Effectiveness/efficiency. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table 8-17 – Indicator 17: Personally identifiable information (PII) protection (system/programme level, bigger-better)**

| Field | Data |
|---|---|
| Indicator ID | Percentage of protected sensitive personally identifiable information. |
| Goal | The organization should protect the organization's sensitive personally identifiable information in an encrypted way. |
| Indicator | Percentage of protected sensitive personally identifiable information. |
| Formula | (Number of sensitive personally identifiable information encrypted/Total number of personally identifiable information) × 100 |
| Raw data | • Number of protected personally identifiable pieces of information.<br>• Total number of personally identifiable pieces of information. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | Effectiveness/efficiency and implementation. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table 8-6 – Indicator 6: Mean time to patch (system level and programme level, smaller-better)**

| Field | Data |
|---|---|
| Indicator ID | Mean time to patch. |
| Goal | Mean time to patch quantifies the average time taken to deploy a patch for the organization's systems. The more quickly patches can be deployed, the less the mean time to patch is, and the less time the organization operates systems in a state known to be vulnerable. |
| Indicator | Average time taken to deploy a patch for the organization's systems. |
| Formula | Sum (Date_of_Installation – Date_of_Availability)/Count (Completed_patches). |
| Raw data | • Date of installation.<br>• Date of availabilities.<br>• Total number of completed patches. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | • Effectiveness/efficiency. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table 8-26 – Indicator 26: Personally identifiable information leakage (programme level)**

| Field | Data |
|---|---|
| Indicator ID | Personally identifiable information leakage. |
| Goal | The organization should protect personally identifiable information from being leaked to outside organizations. |
| Indicator | Percentage of personally identifiable information units that are leaked during a defined time frame in the reported PII incident.<br>NOTE – Developers of this indicator should define their own unit of PII. |
| Formula | (Number of personally identifiable information units that are leaked within the organization-specified time frame in the reported PII incident/Total number of personally identifiable information units) × 100. |
| Raw data | • Number of personally identifiable information units leaked within the organization-specific time frame in the reported PII incident.<br>• Total number of personally identifiable information units. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | Impact. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table 8-28 – Indicator 28: Ratio of authorized device (bigger-better)**

| Field | Data |
|---|---|
| Indicator ID | Ratio of organization's authorized devices to all devices. |
| Goal | The organization should track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network. |
| Indicator | Ratio of the organization's authorized devices to all devices. |
| Formula | (Number of authorized devices/Number of devices) × 100. |
| Raw data | • Number of authorized devices.<br>• Number of devices. |
| Frequency | • Weekly, monthly, quarterly, annually. |
| Type | Impact. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table III.3 – Indicator III-3: Bot infection (system level, smaller-better)**

| Field | Data |
|---|---|
| Indicator ID | Percentage of end-point devices infected with bot. |
| Goal | The organization should reduce the presence of bots in the network of an organization. |
| Indicator | Percentage of end-point devices infected with known bots in an organization.<br>The organization is assumed to employ the bot infection detection system. |
| Formula | (Total number of end-point devices infected with known bots/Total number of end-point devices ) × 100. |
| Raw data | Number of end-point devices infected with bots. |
| Frequency | Weekly, monthly, quarterly, annually. |
| Type | Effectiveness/efficiency. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

**Table III.4 – Indicator III-4: Distributed denial-of-service (DDoS) measures (system level, smaller-better)**

| Field | Data |
|---|---|
| Indicator ID | DDoS measures. |
| Goal | The organization should protect its end-point systems against DDoS (or denial-of-service (DoS)) attacks for the organization-defined time frame. |
| Indicator | Percentage of organization's systems that are unavailable for a specified time duration due to DDoS (DoS) attacks. |
| Formula | (Number of organization's systems that are unavailable for a specified time duration due to DDoS attacks during the organization-specified period/Total number of websites that an organization has) × 100. |
| Raw data | Number of websites that are unavailable for a specified time duration due to DDoS attacks within the organization-defined time frame.<br>Total number of websites. |
| Frequency | Weekly, monthly, quarterly, annually. |

**Table III.5 – Indicator III-5: Audit log performance (system level and programme level, bigger-better)**

| Field | Data |
|---|---|
| Indicator ID | Percentage of computer security incidents for which an audit log has captured observable traces. |
| Goal | The organization should assess the effectiveness of audit logs. |
| Indicator | Percentage of computer security incidents for which an audit log has captured observable traces. |
| Formula | (Reported incidents that left observable traces in logs/Total number of reported incidents) × 100. |
| Raw data | Number of reported incidents for which observable traces have been found in audit logs. (Either centralized log or logs aggregated from end-points)<br>Total number of reported incidents. |
| Frequency | Weekly, monthly, quarterly, annually. |
| Type | Effectiveness/efficiency. |
| Requirement level | |
| Applicable to | Organizations, (a community by aggregation). |
| Reference from CYBEX techniques | |

# ANNEX 3: SURVEY ON PRIVACY AND CYBER-SECURITY TOOLS

We had the opportunity to present the ANASTACIA project at two international conferences during November 2018, XVI Ibero-American Meeting for the Protection of Personal Data in San José, Costa Rica and the IAPP Europe Data Protection Congress 2018 in Brussels. In this context, privacy professionals provided feedback on the envisioned DSPS services as proposed by ANASTACIA WP5. The full results of the survey will be presented in full by ANASTACIA WP6, however it is necessary to introduce some of the obtained feedback throughout this deliverable.

When the privacy and security professionals were asked how important it would be to monitor and to be informed of any problems related to data protection, cybersecurity and the end-user trust. The values of the answers show that it is very important for them to monitor and to be informed about all three proposed components, data protection (GDPR) with the value of 9,19 of 10 then end-user trust with the value of 8,88 and the last in comparison the cybersecurity also with a very high value of 8,84.

We also asked our participants what kind of information on data protection they would like more specifically to monitor and to be able to consult remotely. The majority of them answered that data flows, processing of data, data breach, personal data flows and cyber security are significant for them to monitor. Participants note that the most relevant elements for their organization to decide to use a tool like the DSPS include Simplicity and user-friendliness and confidentiality (value 9 of 10), followed by reliability of the monitoring process (8,95 of 10), non-falsifiability of data (8,91 of 10), real time monitoring process (7,81 of 10), number of users (7,28 of 10), mobile device compatibility (6.86 of 10) and at the end multi-linguism with the value of 6,35 of 10.

Finally, we received feedback regarding the use of any privacy and cyber security support system by participants. 42 percent of them answered with no while 31 percent didn't want to declare. 27 percent

declared that they are using the support system within their organizations and more specifically Kaspersky, ISO standards, ISO 27001, Codisa, OneTrust and their own privacy and security system support.

The participants were pleased to answer the questions and were actually satisfied that they had the opportunity to say something about this topic. This survey showed us that privacy and security issues are significant for the organizations and how much important it is for the professionals in this area to have advanced security support systems to ensure that its reputation will not be compromised for these reasons. All examinees think that a platform like the DSPS which can offer a combined view over security and privacy issues can be precious in dealing with privacy and security requirements.