ANASTACIA

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

D5.3

Dynamic Security and Privacy Seal User Interface

This deliverable presents the results of ANASTACIA Task 5.3 alongside with the DSPS demonstrator. This deliverable summarizes the user interface and enhancements of the initial design and implementation. A confidential annex further details the contents of this document.

Distribution level	PU
Contractual date	11.30.2019 [M35]
Delivery date	02.26.2020 [M35]
WP / Task	WP5 / T5.3
WP Leader	MAND
Authors	Eunah Kim (DG), Robert Navarez (DG), Zahid Muhammad (DG), Federico Sismondi (MAND), Adrian Quesada Rodriguez (MAND), Sébastien Ziegler (MAND), Fabio Queiros (AS), Olivia Doell (AS), Bojana Bajik (AS), Ana Maria Pacheco (AS)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

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

Table of Contents

Table of figures

PUBLIC SUMMARY

The deliverable D5.3 is presented alongside the demonstrator of the DSPS user interface to summarize the final result of T5.3, which develops the user interface connected to the secured and authenticated sealing service. Development of the ANASTACIA DSPS has been carried out in an iterative way. Year three of the project has served to perform updates and refinement of the system service deployment and functionality validation (handled in T5.2) and the planned development of the storage & user interface (T5.3). This deliverable provides the functionalities of the user interface of DSPS with detailed screenshots of the developed demonstrator.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document showcases the final end-user interface developed for the DSPS, which has been developed to provide real time monitoring of deployed systems on security and privacy status and the reliability of the system by the history of the seal logs. The seal has been designed 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. This document avoids reintroducing redundant information found in previous Deliverables 5.1 and 5.2 which focused on the model and services behind the DSPS.

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 D2.7 Privacy Risk Modelling and Contingency Final Report
- ANASTACIA Deliverable D4.1 Initial Monitoring Component Services Implementation Report
- ANASTACIA Deliverable D5.1 Dynamic Privacy and Security Seal Model Analysis
- ANASTACIA Deliverable D5.2 Dynamic Privacy and Security Seal service

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	28/10/2019	Eunah Kim	Initial document outline and structure
0.3	15/11/2019	Bojana Bajic, Fabio Queiros	Inputs on user validation and seal design
0.5	22/11/2019	Federico Sismondi, Robert Navarez	Inputs on DSPS server and GUI backend
0.6	27/11/2019	Zahid Muhammad, Fabio Queiros	Inputs on Privacy risk assessment, User story
0.7	28/11/2019	Eunah Kim	Updates on architecture section
0.8	06/12/2019	Eunah Kim, Bojana Bajic	Updates on User story, user validation
0.9	10/12/2019	Eunah Kim	Updates on Privacy risk assessment, Writing on summary
1.0	12/12/2019	Eunah Kim	Overall refinement of the document
1.1	14/1/2020	Adrian Quesada Rodriguez, Sébastien Ziegler	Update, generation of public version and confidential annex
2.0	24/02/2020	Adrian Quesada Rodriguez, Eunah Kim	Update, final version of public deliverable

1.4 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
DSPS	Dynamic Security and Privacy Seal
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HSPL	High-level Security Policy Language
ICT	Information and Communication Technologies
IoT	Internet of Things
MAS	Mitigation Action Service
MSPL	Medium-level Security Policy Language
PDP	Personal Data Protection
PIA	Privacy Impact Assessment
SAS	Security Alert Service
SMMI	Seal Manager Metadata Interface
SSSS	Shamir Secret Sharing Scheme
STIX	Structured Threat Information eXpression
VDSS	Verdict and Decision Support System

2 DSPS High-level Architecture

A number of updates have been carried out to enable the interactions of the diverse components of the DSPS, these activities build upon the descriptions found in D.5.1 and 5.2, and address some of the end-user requirements and validation activities undertaken since. The following image details the relation between ANASTACIA WP4 and the development activities undertaken in WP5.

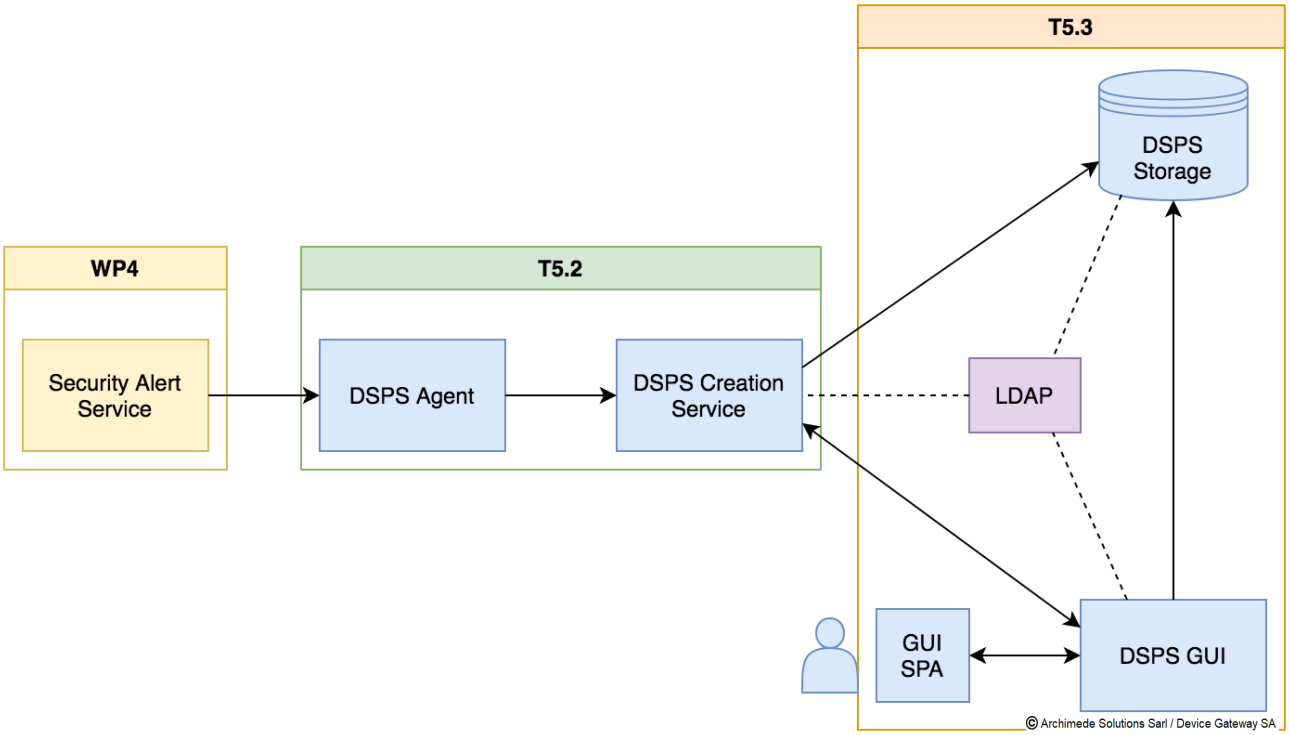

Figure 1 Relation of DSPS development

Development activities during year 3 have generated a number of final building blocks for the DSPS. While the high-level architecture of DSPS service has remained broadly as planned in deliverables 5.1 and 5.2, there are major updates inside of the components in DSPS Agent, DSPS Service Core, DSPS Storage and DSPS GUI. The confidential annex of this deliverable presents the activities undertaken in detail.

3 FUNCTIONAL OVERVIEW OF DSPS GRAPHICAL USER INTERFACE

The DSPS GUI has had drastic updates both on functionalities and design aspects in the second period of the project. Corresponding to the update seal logics in the server, the user interface includes separate handling of security seal and privacy seal together with demonstrating the integrated system status. It also includes CISO's reporting and seal restore functions. In addition, it adds human-intuitive messages on security events and related privacy risk assessment not only the raw data for non-technical users, particularly for DPOs. With one of the integration activities performed with other WPs, the information about mitigation actions by ANASTACIA system is also transferred to DSPS for providing to users more information on system level of actions. As a preparation of exploitable service beyond the project lifetime, the design of user interface has been redesigned by a professional designer and integrated into the user interface.

3.1 FUNCTIONALITIES

The DSPS GUI functionalities are specific to the user type: Administrator of the organization, DPO and CISO. The followings describe the functionalities of each user supported by DSPS.

Administrator of the organization

The administrator is capable of doing overall administrative actions over the DSPS. This includes the following:

User management	The administrator can create, delete and modify the right of the users in its organizations. The supporting user types are DPO, CISO, and Watcher.
Organization policy management	The administrator manages to put an organizational policy on monitoring and periodic reporting.
Monitoring of Seal Status	The administrator can see information about the latest seal and seal log as well as its history and its graphical representation.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is capable of the following actions:

Monitoring of Seal Status	The DPO can see information about the latest seal and seal log as well as its history and its graphical representation.
Restoration of the seal privacy component	When the privacy component of a seal has been raised by an alert (represented graphically as the privacy portion of a seal turning red), the DPO can start a procedure to mitigate the alert's privacy threats. To do this, the DPO fills in an alert questionnaire with relevant information regarding the alert. Once the questionnaire is submitted, the privacy status of the seal is restored and turns back to green.
Submission of Data Privacy Impact Assessments (DPIA)	The DPO can submit new DPIAs when it is necessary.
Periodic report submission	The DPO is notified on a periodic basis to provide a report about the status of the privacy situation of the organization.

Management of supporting documentation	The DPO can upload files related to a threat mitigation or any documentation relevant to the DSPS.
Report a privacy threat	The DPO can generate an alert reporting a privacy threat.

Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is capable of the following actions:

Monitoring of Seal Status	The CISO can see information about the latest seal and seal log as well as its history and its graphical representation.
Restoration of the seal security component	When the security component of a seal been raised by an alert (represented graphically as the security portion of a seal turning red), the CISO can start a procedure to mitigate the alert's security threats. To do this, the CISO fills in an alert questionnaire with relevant information regarding the alert. Once the questionnaire is submitted, the security status of the seal is restored and turns back to green.
Management of supporting documentation	The CISO can upload files related to a threat mitigation or any documentation relevant to the DSPS.
Report a security threat	The CISO can generate an alert reporting a security threat.

3.2 COMPOSITION

The DSPS GUI is composed of two separate codebases:

- The Single-Page Application (SPA)
- The Back-end

Single-Page Application (SPA)

The single-page application (SPA) is the main component that the DSPS user interacts with. It acts as a client to the GUI back-end.

The SPA is implemented in ReactJS and its supporting libraries and with Webpack as the project bundler.

Seal Visualization

The SPA provides a visualization of the current seal status.

Seals are implemented as SVG elements that are rendered as React components. The element properties change dynamically based on parameters passed to the components.

Seal Management Workflows

The SPA allows users, depending on their role, to take actions in order to create seals, answer questionnaires, etc.

Back-end

The back-end is responsible for the core business logic of the DSPS GUI. In a nutshell, the GUI:

- Acts as an intermediary for clients to create seals through its interaction with the DSPS Seal Creation Service
- Acts as an intermediary for clients to see seals and seal logs through its interaction with the DSPS Storage Service
- Stores data generated by the core business logic

It is developed as a *NodeJS* application.

REST API

The back-end provides a REST API to allow clients such as the SPA to take action on DSPS-related resources. Some of the resources are:

- Seals
- Questionnaire responses
- Reports
- Files
- Users
- Notifications

Integration with DSPS Seal Creation Service and Storage Service

The back-end integrates with the DSPS Seal Creation Service to create seals through the DSPS Seal Creation Service's REST API.

The back-end integrates with the DSPS Storage Service in order to obtain seal and seal log data. The back-end implements several procedures for decrypting raw seal and log data into usable JSON data.

Integration with DSPS GUI SPA

The back-end acts as a server to the DSPS GUI SPA.

User Management

The back-end implements a simple user management scheme where users can be either an admin, DPO, CISO or a watcher. The REST API provides several endpoints to manage users.

Authentication and Session Management

The REST API provides an endpoint for authentication of users. On successful authentication, a JSON Web Token (JWT) is returned to the authenticating client.

Caching

The back-end is configured to cache as much decrypted seal and seal log data as possible for performance management.

Background Jobs

The back-end implements some background jobs for managing some internal resources such as removing stale notifications and sending reminder emails.

Websockets

The back-end enables 2-way communication between itself and the SPA through WebSocket. This is used to notify users of seal status changes.

Database

For temporary storage needs that are not seal- or seal log-related, the back-end stores data on a *MongoDB* instance.

Emails

The back-end is responsible for sending email notifications to users. Email sending is triggered via events or through background jobs.

4 User Story of DSPS Graphical User Interface

In this section, we explain the DSPS seal image that visualizes the holistic monitoring information of security and privacy status of the monitoring system, and other visualizations for supporting users.

4.1 User Authentication

As described above, the DSPS provides interfaces for different types of end-users, to ease their authentication, the overall look and feel of the login page has been revamped.

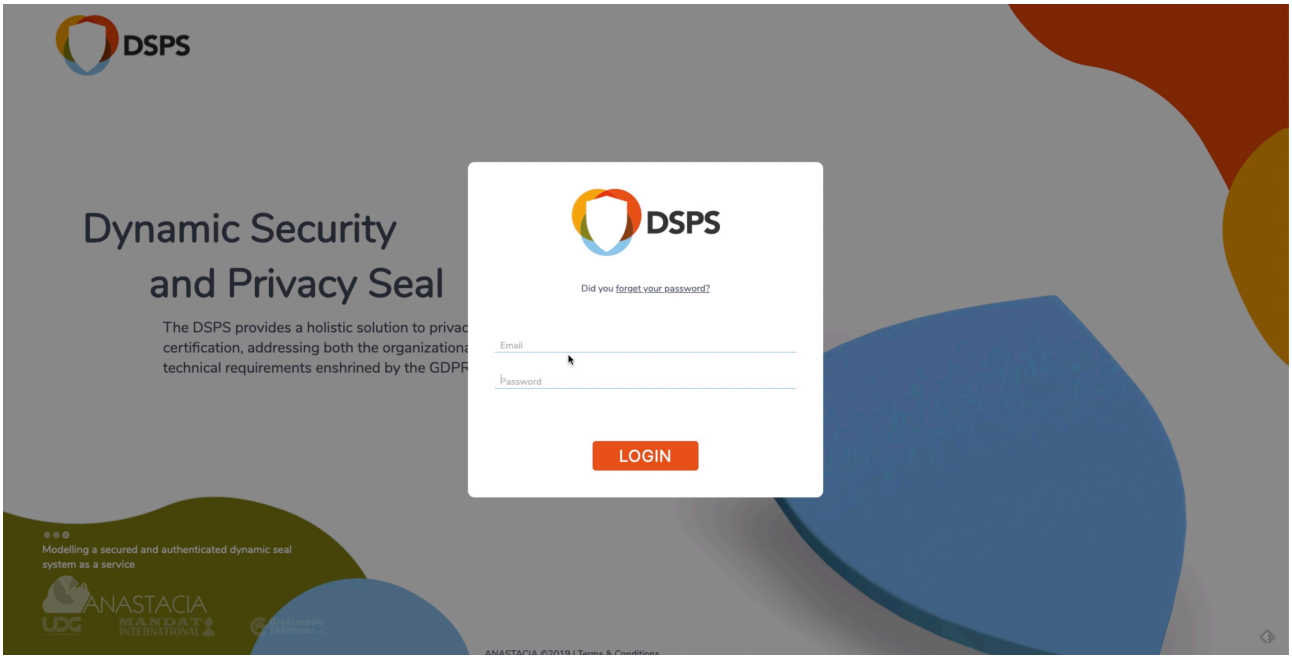

Figure 2 DSPS Login page

4.2 Design concept of DSPS Seal

The seal visual representation is composed of three main elements: Security Risk gouge (1), Privacy Risk gouge (2) and the inner health shield (3) indicating in Figure 3.

Both of Security and Privacy risk gouges display the current risk level by numerical values and colours. For example, it indicates 0% of risk with GREEN for intuitive identification of no risk, 50'% of risk with YELLOW illustrating medium risk, and 100 % of risk with RED identifying maximum risk. In-between percentage of risk is indicting with granular values of the colours.

The health shield shows the sum of the privacy risk and security risk giving a comprehensive visual feedback to the user of the overall health of the system.

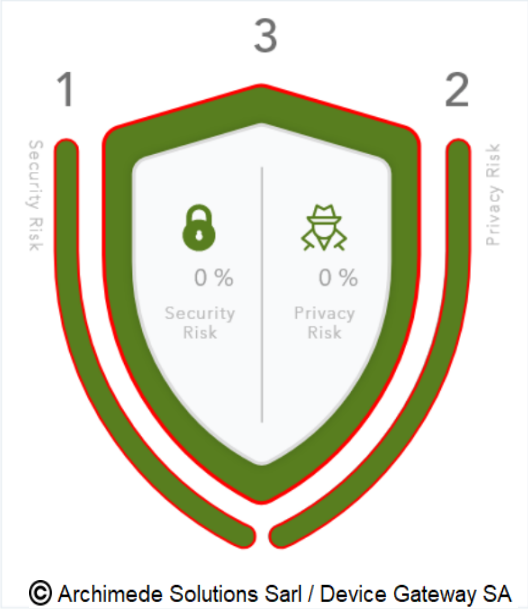

Figure 3 DSPS Seal image

4.3 DSPS DASHBOARD

Figure 4 shows the DSPS dashboard when a user logged in to DSPS service. The current dashboard is showing when a DPO logged in. In the top menu, it supports three major functions: dashboard, submit report, and DPIA tool. “submit report” and “DPIA tool” is also included in the bottom of the dashboard, and for the user’s convenient, it can be also linked from the top menu. The following description of the dashboard is provided from top to bottom and from left to right.

On the top left of the main dashboard, we can see the “current state of the seal”. The seal is composed of three main components, on the left we have the security health representation of the seal in the middle we have the overall seal health which is the cumulative health of both privacy and security risk, and on the right, we have the privacy risk health of the seal. Every component can be clicked to further display detailed information of the current state. We both represent the health of the seal graphically and numerically. Graphicly using a colour coded standard meaning red unhealthy, yellow average, green healthy and numerically from 0 unhealthy to 100 healthy. The “Restore” button at the bottom of the seal is used to trigger a modal with the steps needed for the restoration process.

In the middle section we have the graphical histogram that represent all the events by number of occurrences and dates. It allows us browsing all the events that occurred in the system by set date or date range. Those events are displayed in the graph and can be further consulted for more details in the area seal status above.

From left to right we have DPIA, Periodic reports and supporting documents.

The DPIA interface on the bottom left in the dashboard allows us uploading all new DPIA´s to the system and also consulting or downloading and navigating from most recent to oldest or by date range all previous DPIA´s submitted. A new DPIA can be produced by clicking either on the button “+ add new” or on the header “DPIA tool” button it will trigger a model that will direct us to the DPIA tool.

The periodic reports management interface follows the same logic as the DPIA interface. Tt allows consulting or downloading and navigating from most recent to oldest or by date range. To add a new report, we need to click the “+ add new” and it will trigger a form within a modal that after completion will be displayed in the interface.

In the bottom left of the dashboard we can see the area where the USER can upload all supporting documents. In the supporting documents interface you can navigate the documents, download and submit

in the same manner as the 2 previous interfaces. this interface functions to help the user have all documents needed to properly administer the DSPS accordingly to the set rules of the system where the DSPS is set up in.

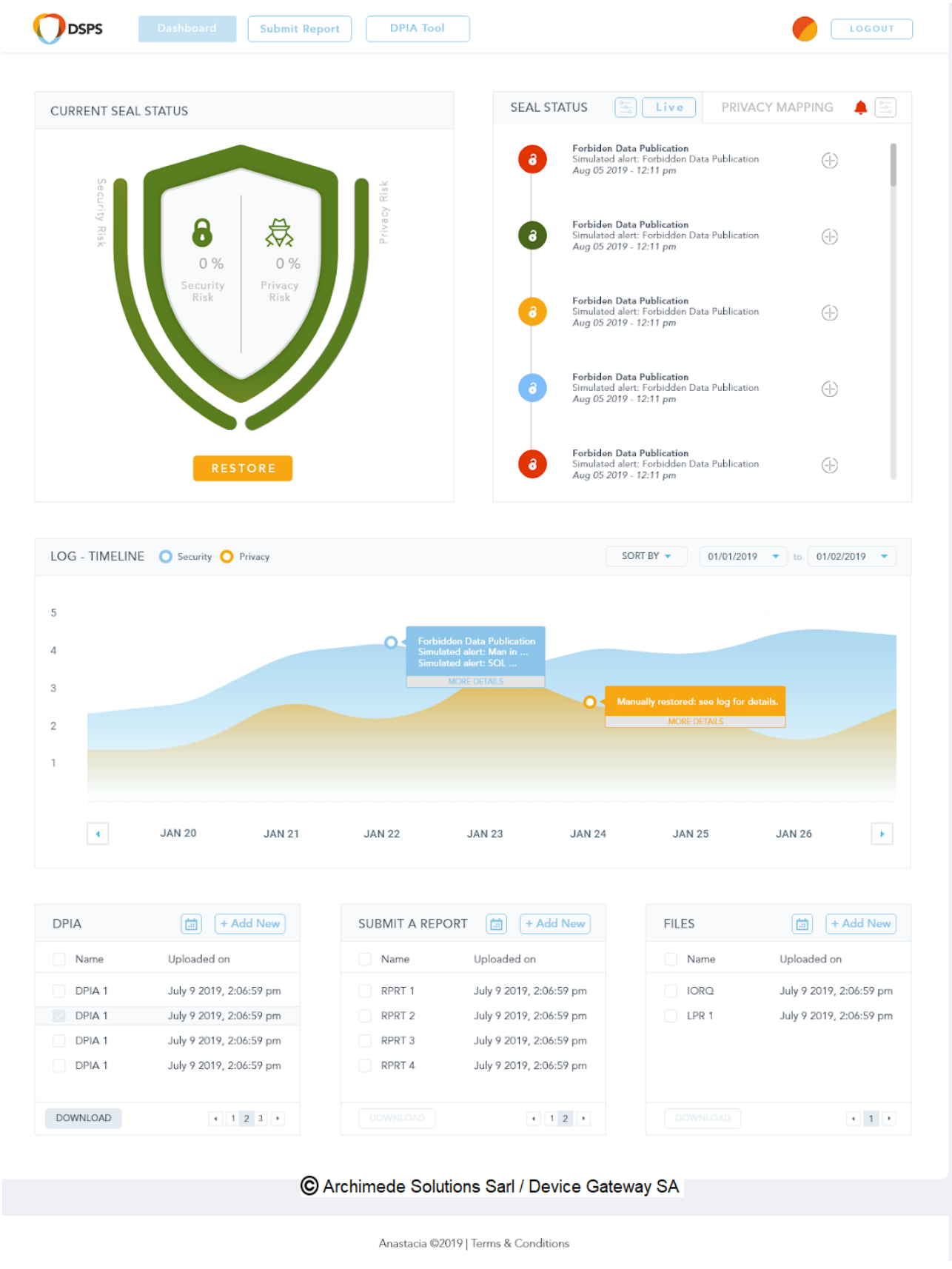

Figure 4 DSPS dashboard

The CISO's dashboard has the same interface except privacy mapping. Instead it links ANASTACIA VDSS page for security risk and mitigation management for the CISO's intervening of the management and monitoring of the security risk.

4.4 UPDATE OF SEAL STATUS

The "Seal status" on the top left of the dashboard displays the details of each seal in the seal history. in this area we display all the events occurring live. All the events are clickable/expandable to display further detail on that specific event thus giving us a live/precise understanding of the health of the seal. The details can be set to be live or filtrable by date range.

In normal situation, DSPS is used to monitor the system status, DPIA management, periodic report management for DPOs and CISOs, that explained in the DSPS dashboard. In such peaceful time, the DSPS seal is green indicating 0% of security risk and no privacy risk as shown in Figure 5.

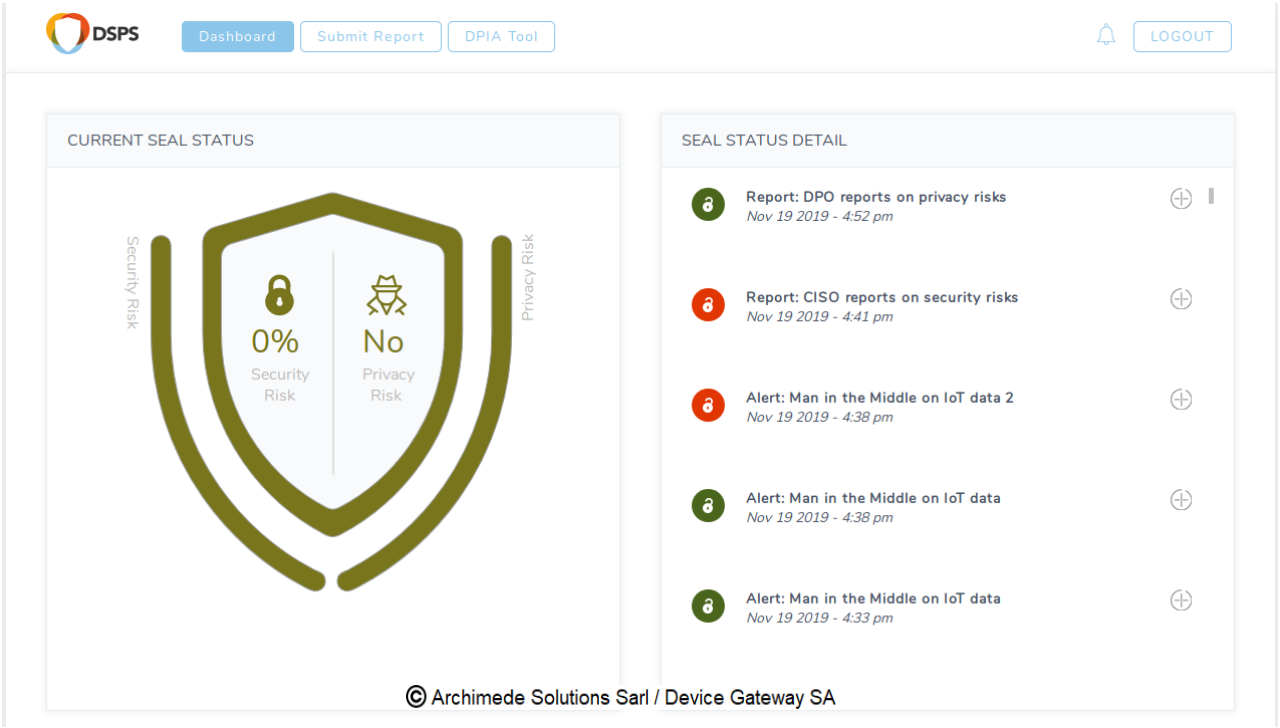

Figure 5 DSPS seal with no risk

When DSPS receives a security alert, it changes the seal status. The Figure 6 shows the example that ANASTACIA security monitoring system indicates a security attack and sends DSPS the alert. DSPS indicates it as 30% security risk which is illustrated in the Security Seal with yellow colour. Any Security risk is assumed to contain a Privacy risk and it changes the Privacy Seal to red and sends notification.

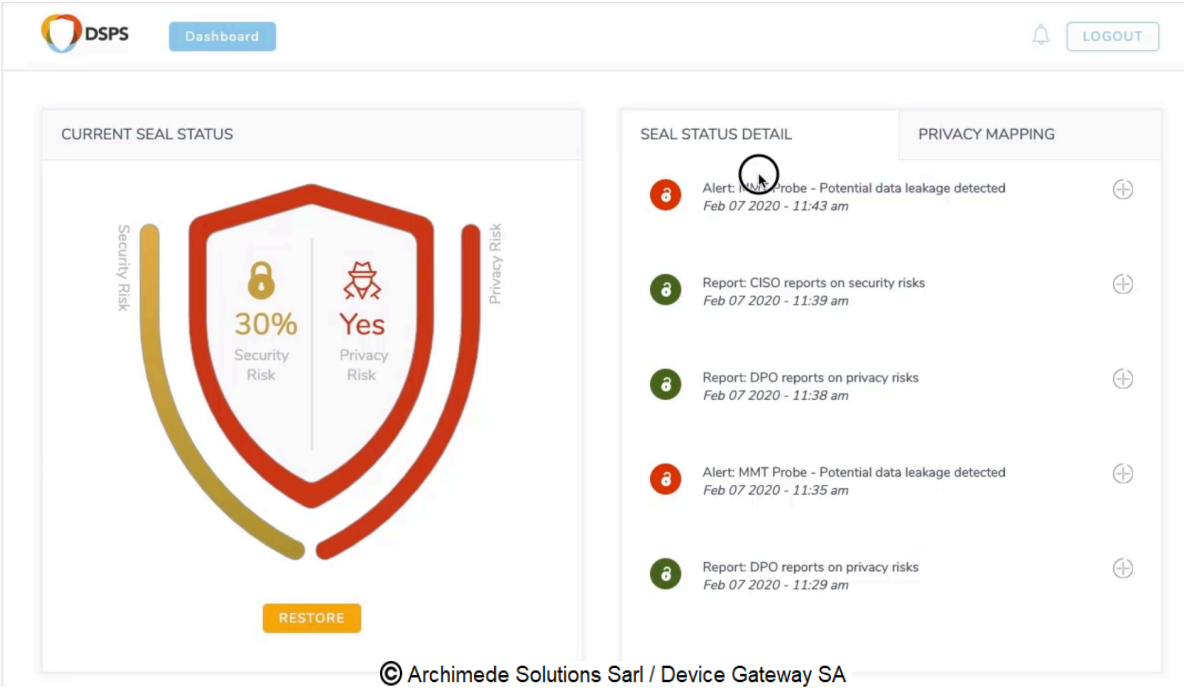

Figure 6 DSPS received a security alert

The Anastacia System runs automatic security mitigation and sends the mitigation results to DSPS. The Security Seal is automatically return to green when it receives the notification of the mitigation. Figure 7 indicates that the Security Seal changes to green by ANASTACIA's automatic mitigation of the security threat.

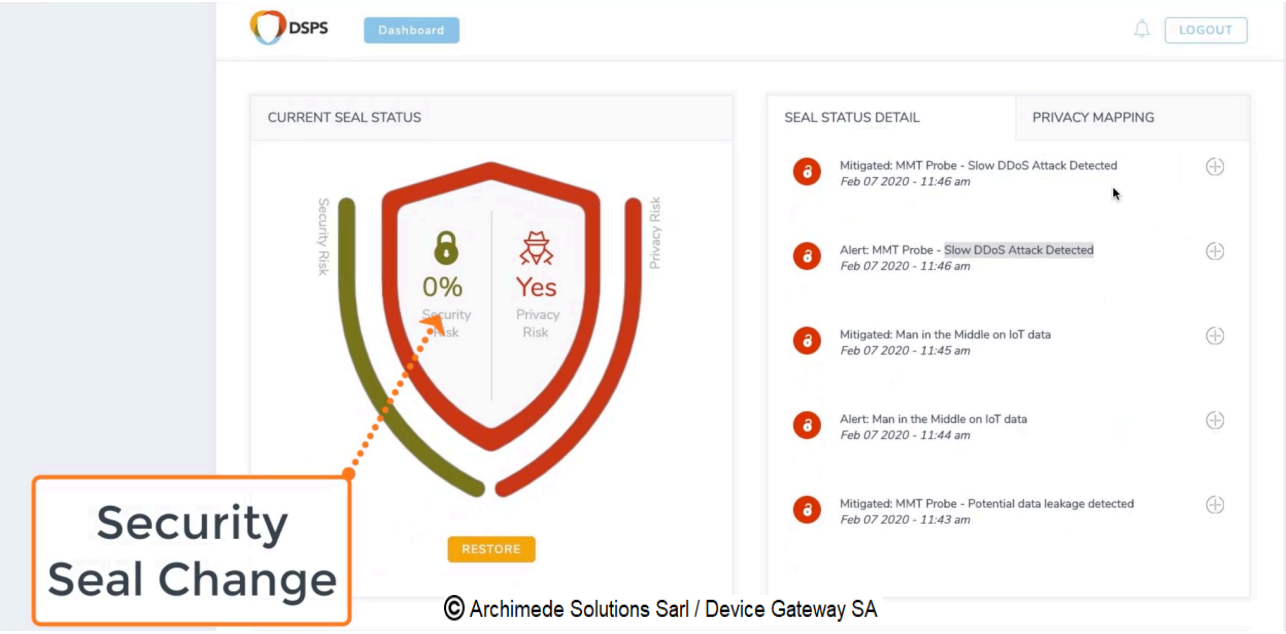

Figure 7 Security Seal update by mitigation

When the seal status changes by alert or mitigation, DSPS indicates the seal status changes in the top right corner as shown in Figure 8.

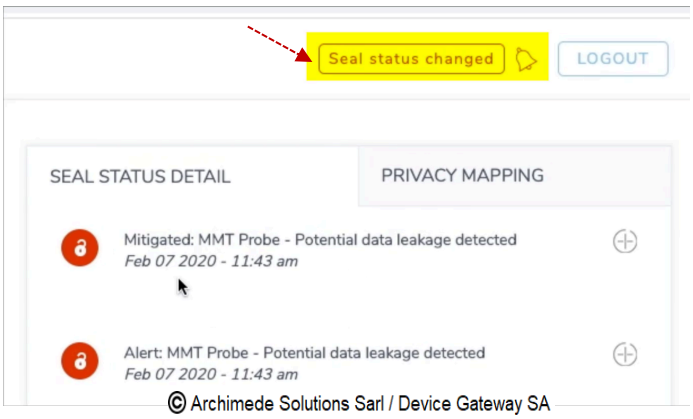

Figure 8 Indication of Seal status change

The restoring process of Privacy Seal always requires DPO's input. In the case of no automatic security mitigation has been performed, DSPS also requests to CISO to conduct restoring process. The DPOs and CISOs can restore the seal by clicking RESTORE button in the bottom of the seal image as indicated in Figure 9.

Figure 9 Restore button of the seal

The Figure 10 shows the questionnaire that CISO should answer after manual mitigation. In the case of automatic mitigation, it does not require this step.

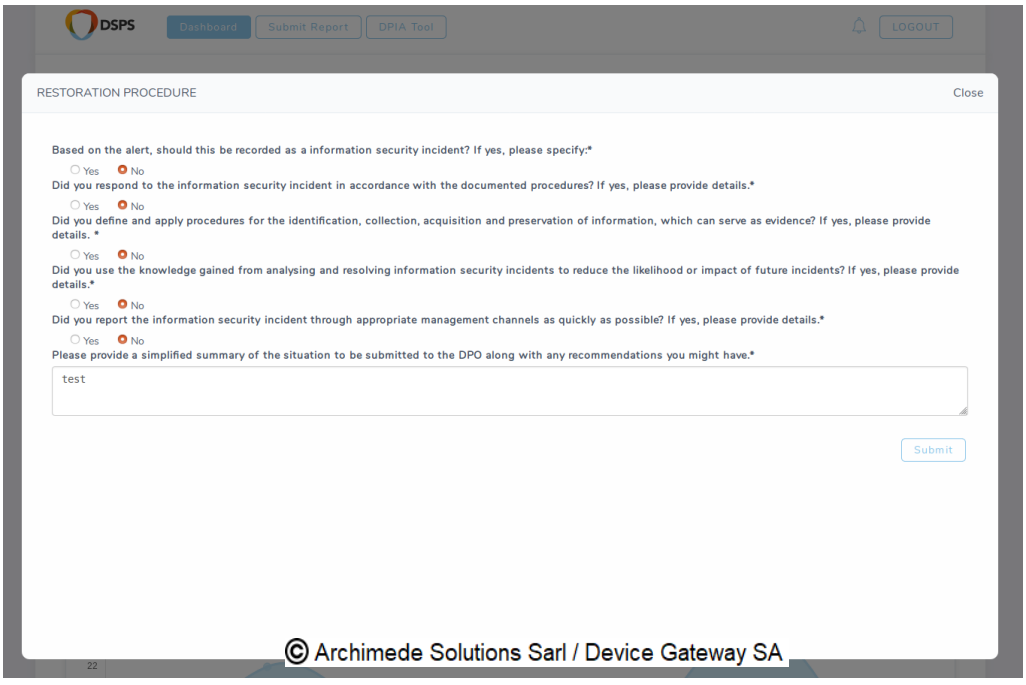

Figure 10 CISO's questionnaire to restore the security seal

DPO who received notifications via email and via its DSPS dashboard notification performs the recommended mitigation actions for the privacy risk, upon which he can trigger a restoration of the privacy section of the Seal. With DPO's restoration of the privacy seal, the Privacy Seal is updated to green as shown in Figure 11.

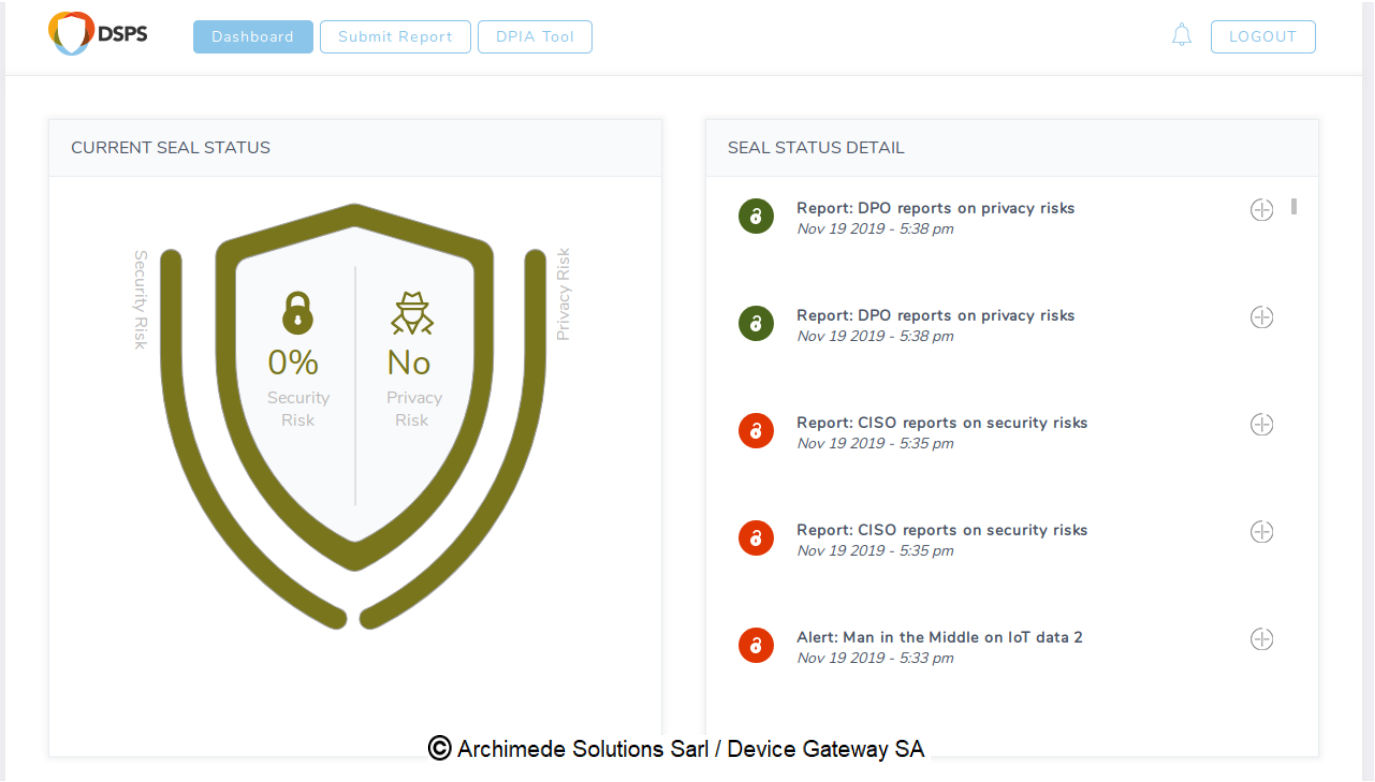

Figure 11 Both security and privacy seal have been restored

All the steps are grouped by type of information to facilitate the user inputs, this behaviour is replicated throughout all forms present in the GUI.

5 USER VALIDATION

The ANASTACIA project was presented at different international conferences during last two years of the project, which served directly to test the graphical design and functionalities offered by the DSPS and its components.

In 2018, the research activities were presented at the XVI Ibero-American Meeting for the Protection of Personal Data in San José, Costa Rica, the IoTweek, and the IAPP Europe Data Protection Congress 2018 in Brussels.

In 2019 our user validation activities were carried out in the following conferences:

- **IAPP world summit in Washington (April 2019)**

  IAPP summit in Washington is privacy and data protection conference that focuses on international topics, policy and strategy. Recognized as a leading forum for discussion, the Summit features expert speakers and top regulators, and delivers unmatched education and networking opportunities. MI promoted the project ANASTACIA during this conference reaching the most important stakeholders from the privacy domain.

- **ITU WSIS Forum in Geneva, (April 2019)**

  World Summit on the Information Society (WSIS) Forum is a global United Nations (UN) multistakeholder platform facilitating the implementation of the WSIS Action Lines for advancing Sustainable Development Goals (SDGs). It is co-organized by ITU, UNESCO, UNDP and UNCTAD, in close collaboration with all WSIS Action Line co-/facilitators and other UN organizations (UNDESA, FAO, UNEP, WHO, UN Women, WIPO, WFP, ILO, WMO, ITC, UPU, UNODC, UNITAR, UNICEF and UN Regional Commissions). MI and AS presented the Anastacia project with the booth during the 4 days of the conference and used the opportunity to receive the feedback regarding the DSPS thanks to the Survey made to engage the end-users in development of the DSPS. With more than 1000 visitors WSIS is one of the most important conferences in the domain of internet technologies.

- **ITU AI for Good global summit in Geneva, (May 2019).**

  AI for Good is a United Nations platform, cantered around annual Global Summits, that fosters the dialogue on the beneficial use of Artificial Intelligence, by developing concrete projects. MI and AS had the opportunity to present the Anastasia project during the conference and to disseminate the Survey for end-user engagement in the development of the DSPS.

- **IoT Week Aarhus (June 2019).**

  Europe's largest IoT conference, IoT Week was held 17 - 21 June 2019 in Aarhus, Denmark with more than 2000 visitors, 360 speakers from the worlds of research, industry, business, technology and science. The conference was complemented for the first time by a public exhibition that provided the experience of real IoT solutions and products, inspiring and showing how far IoT and digitization have come today. Anastacia was presented at the Public Exposition place during three days of the conference.

Project and the was promoted to the experts and professionals of security and privacy but also to many visitors from universities that had the chance to discover the project and Anastacia vision toward the emerging technologies.

- **Annual Privacy Forum 2019, Rome**

  ENISA, DG CONNECT, the University of Rome Tor Vergata and LUISS University organized the Annual Privacy Forum (APF) 2019 on 13 & 14 June 2019 in Italy, Rome. The event encouraged dialog with panel discussions and provided the room for exchange of ideas in between scientific sessions.

  MI had the booth during the conference where Anastacia was presented to European privacy professionals.

- **IAPP European summit in Brussels (Nov. 2019)**

  The IAPP Europe Data Protection Congress 2019 was held in Brussels, again with more than 2000 visitors. Main event in data protection, law and policy with wide-ranging discussions of strategic developments in regional and international data protection. ANASTACIA participated with a conference booth in order to explore the opportunities for the sustainability of the tools developed within the project.

These conferences gathered more than ten thousand privacy and security professionals from all over the world, participants that are active in different regions and countries and those who operate globally. Privacy and Security professionals attending these conferences were interested in the project and we used this occasion to ask them to fill in a survey on Privacy and Cyber-Security Tools in relation with the ANASTACIA project. The feedback obtained from respondents was then used to advance the DSPS logic and user experience. The confidential annex to this deliverable showcases the specific elements required by the survey and the obtained feedback.

Our participants were happy 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.

6 SUMMARY

This deliverable, alongside the developed demonstrator, summarizes the 3rd year results of DSPS User Interface development.

The DSPS is containerized and fully integrated into ANASTACIA security monitoring and mitigation system, providing real-time security monitoring and mitigation status. The automatic system mitigation of the alerted security risks is visualizing in real-time on DSPS GUI, as well as linking CISO's manual mitigation tool (XL-SIEM based tool developed by ATOS in WP4) in the case of the unknown security threats.

Substantial updates to the DSPS GUI (frontend and backend) has been made in the 3rd year of the project (the development results until 2nd year is described in D5.2), in both functionalities and visual effect as demonstrated in this deliverable.

Through the several iterations of the ANASTACIA system integration, DSPS is fully integrated, tested and demonstrated to the end users, of which details are included in WP6 deliverables. In addition, through several events, end-user validation has been performed and feedback considered in the development cycle.

Based on the feedback received, the DSPS can be considered as a useful tool for holistic system monitoring of both for security and privacy risks, integrating security monitoring and human-centric and organizational policy-oriented data protection monitoring, as well as assisting CISOs and DPOs' daily monitoring activities.