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.

Advanced **N**etworked **A**gents for **S**ecurity and **T**rust **A**ssessment in **C**PS/**I**oT **A**rchitectures

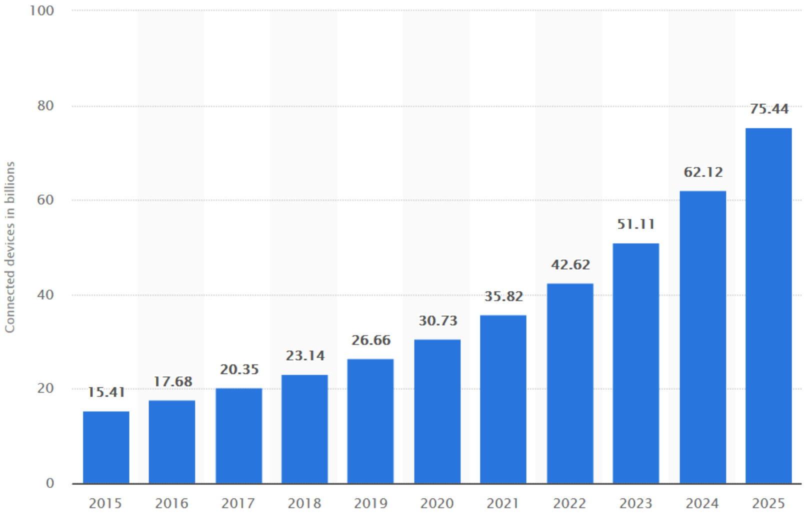
Managing Network-Level IoT Security and Privacy Risks with ANASTACIA

Adrian Quesada Rodriguez
MA. MSc. Lic. CIPP/E
Project Manager and DPO
Mandat International

IoT Week 2019
Aarhus, Denmark

The IoT Privacy/Security challenge

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

VS

GDPR principles (art. 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitations
- Integrity and confidentiality

Approach:

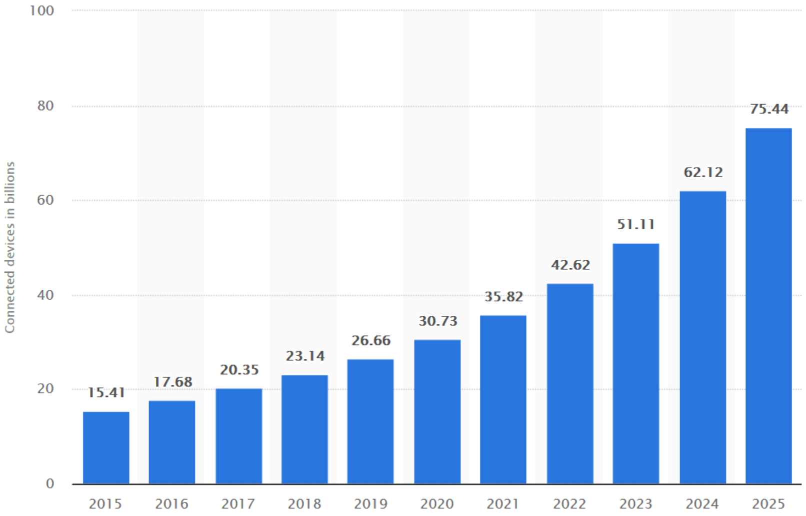
Personal data protection and security by design and default (art. 25)

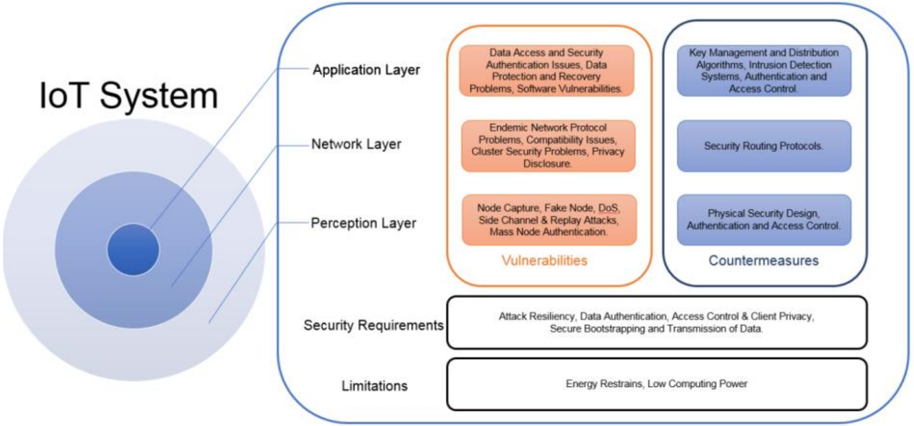
Requirements:

- Organizational: Consent and proof of consent, Underage consent, DPIA…
- Technical: Encryption, anonymization, access management…
- Administrative: Data breach reports to DPA

Who can solve the compliance puzzle?

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)





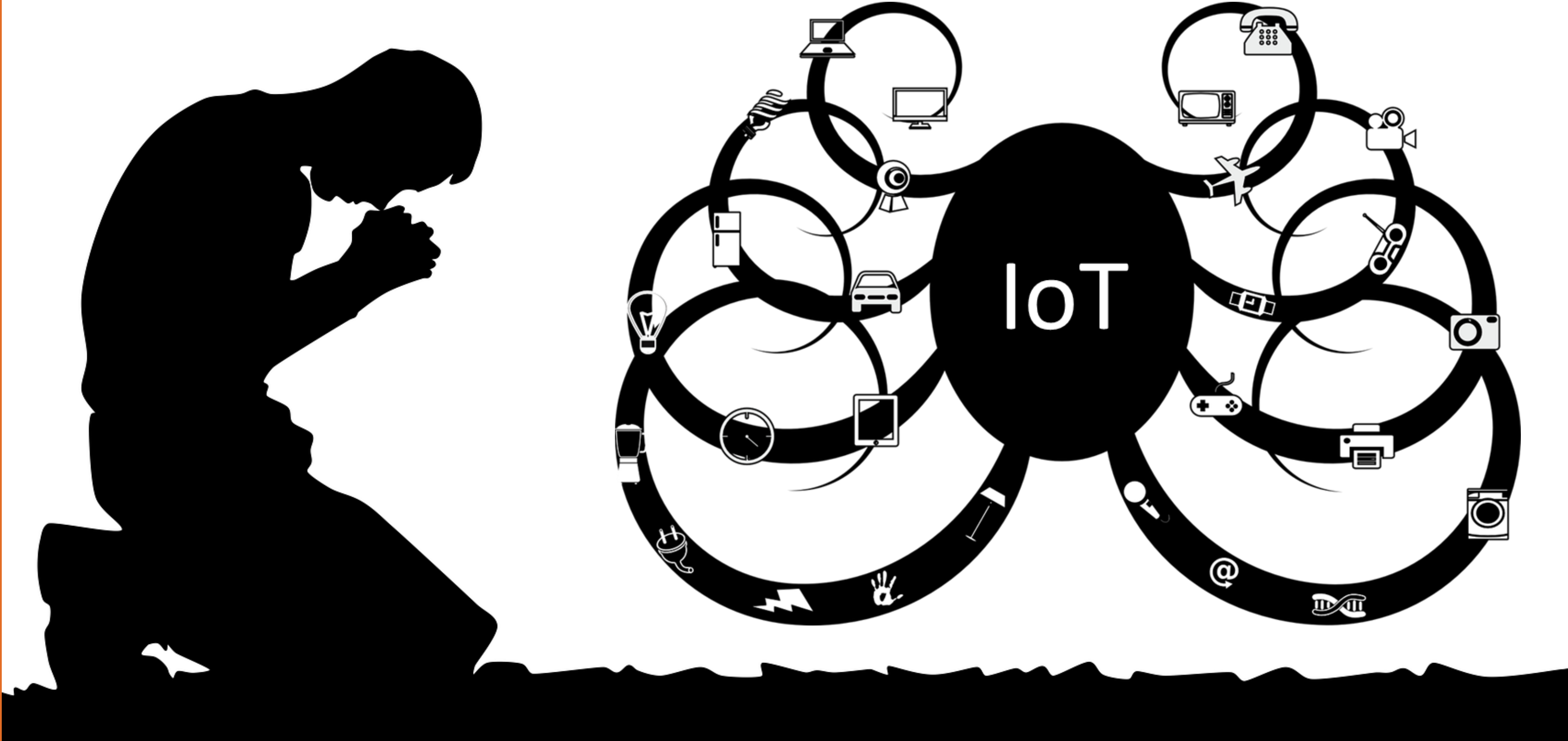
	Vulnerabilities	Countermeasures
Application Layer	Data Access and Security Authentication Issues, Data Protection and Recovery Problems, Software Vulnerabilities.	Key Management and Distribution Algorithms, Intrusion Detection Systems, Authentication and Access Control.
Network Layer	Endemic Network Protocol Problems, Compatibility Issues, Cluster Security Problems, Privacy Disclosure.	Security Routing Protocols.
Perception Layer	Node Capture, Fake Node, DoS, Side Channel & Replay Attacks, Mass Node Authentication.	Physical Security Design, Authentication and Access Control.

Security Requirements: Attack Resiliency, Data Authentication, Access Control & Client Privacy, Secure Bootstrapping and Transmission of Data.

Limitations: Energy Restrains, Low Computing Power

Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ and “Internet of Things: Survey on Security and Privacy” by Diego M. Mendez, Ioannis Papapanagiotou, Baijian Yang (Purdue University) https://arxiv.org/abs/1707.01879

How to enable Privacy/Security management for all?



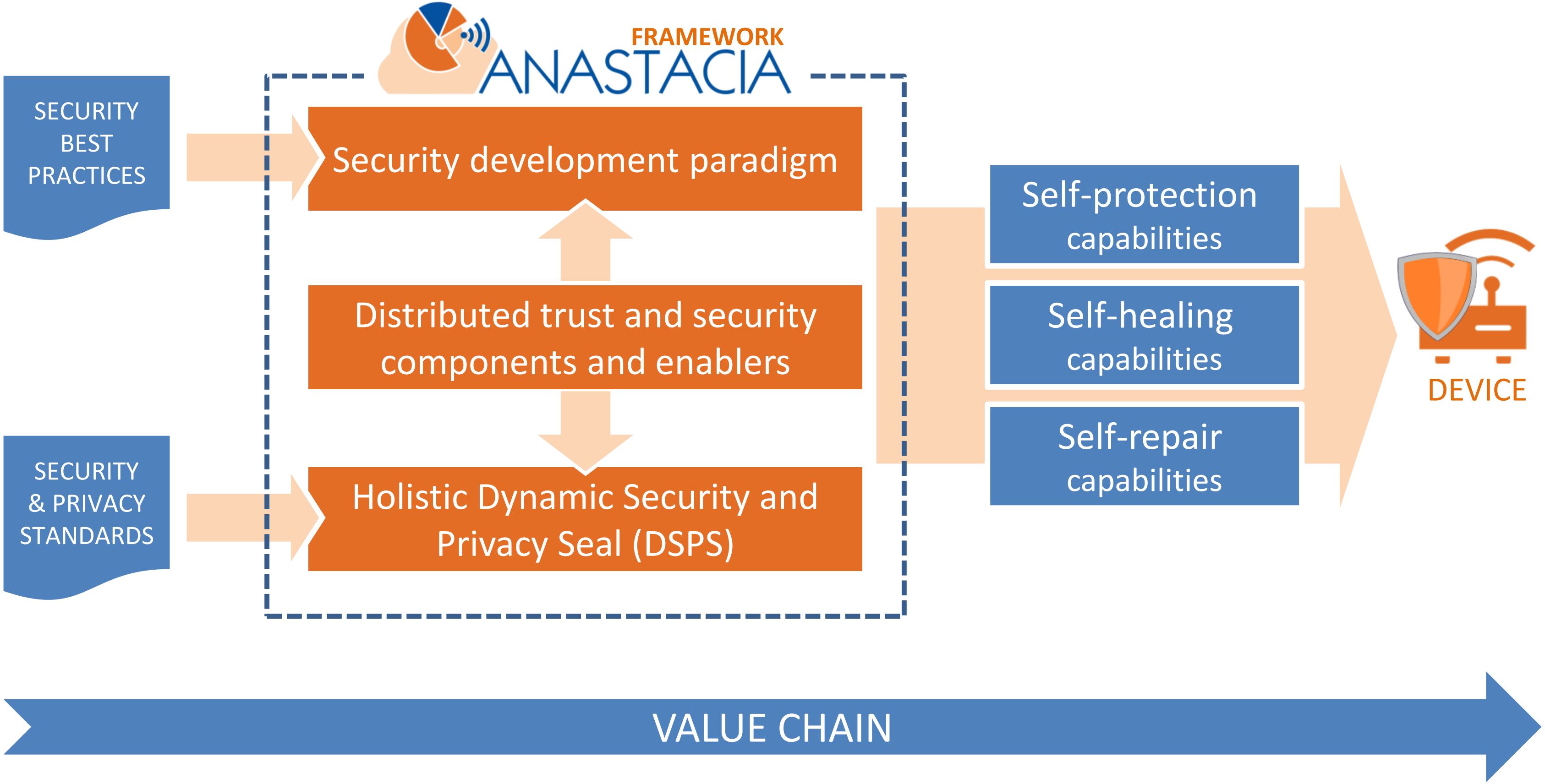
IoT pervasivity: VALUE ADDED vs (ACCEPTED?) RISKS

ANASTACIA's mission

- To develop a trustworthy-by-design autonomic security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools

- Holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures

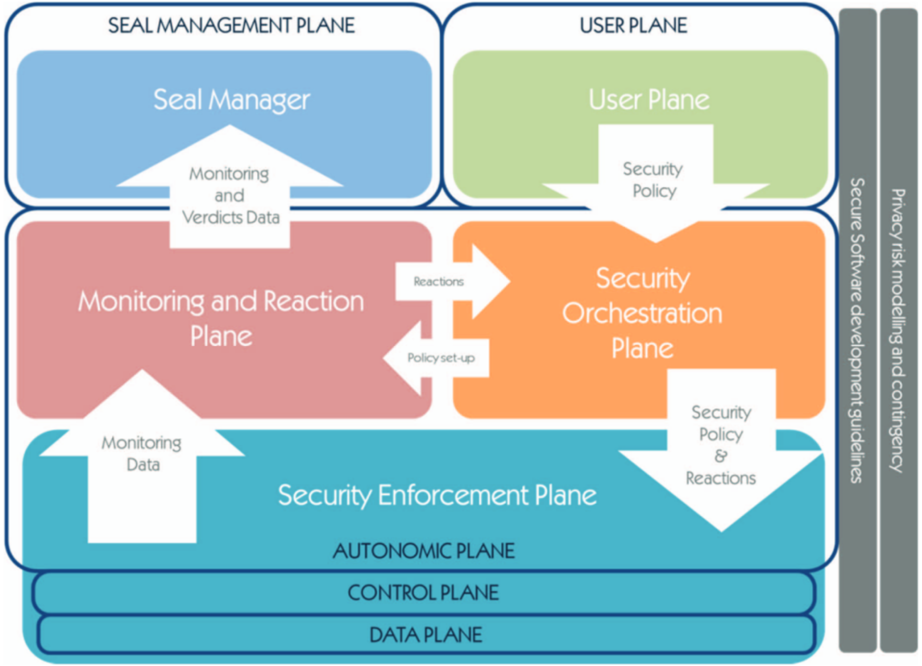
ANASTACIA framework



FRAMEWORK
ANASTACIA
SECURITY BEST PRACTICES
SECURITY & PRIVACY STANDARDS
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
DEVICE
VALUE CHAIN

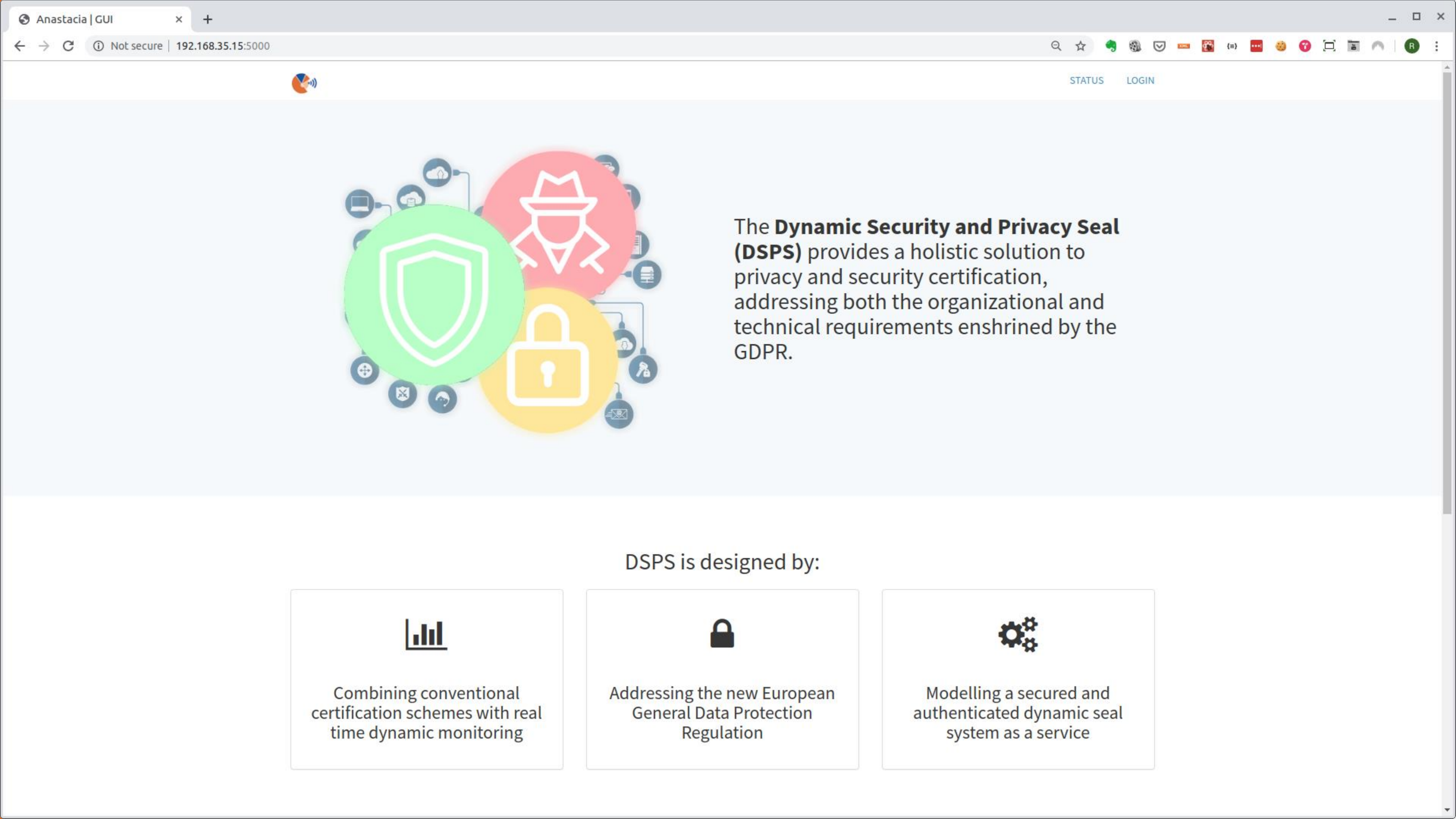
ANASTACIA's Aproach

- Focus:
  - network-level threats and network technologies (SDN/NFV)
- Security:
  - Trusted Security Orchestration in SDN/NFV-enabled IOT
  - Security monitoring: DPI/DNI
  - Automated Cognitive Reaction and Mitigation Components
    - Security Risk Assessment:
      - severity, asset importance, cost of mitigation
    - Consequence prediction and preventior
      - IDS/DPS + behavioral engine


SEAL MANAGEMENT PLANE
USER PLANE
Seal Manager
User Plane
Monitoring and Verdicts Data
Security Policy
Monitoring and Reaction Plane
Reactions
Policy set-up
Security Orchestration Plane
Monitoring Data
Security Policy & Reactions
Security Enforcement Plane
AUTONOMIC PLANE
CONTROL PLANE
DATA PLANE
Secure Software development guidelines
Privacy risk modelling and contingency

Security + Privacy: How to connect them?

1. DSPS (GUI): Meaningful and simple information for CISO/DPO
2. Mapping of monitored security threats to network-level privacy risks:
   - Risk 1, 2, 4: access, modification and deletion of personal data (malware, etc.)
   - Risk 3: lacking anonymization/encryption of information
   - Risk 5: intra-network monitoring (man in the middle)
   - Risk 6: external network monitoring (insecure communication channels)
   - Risk 7: data availability and downtime (DDoS)
3. ISO-based privacy risk assessment process
4. CISO/DPO signed feedback + non-repudiable audit trail



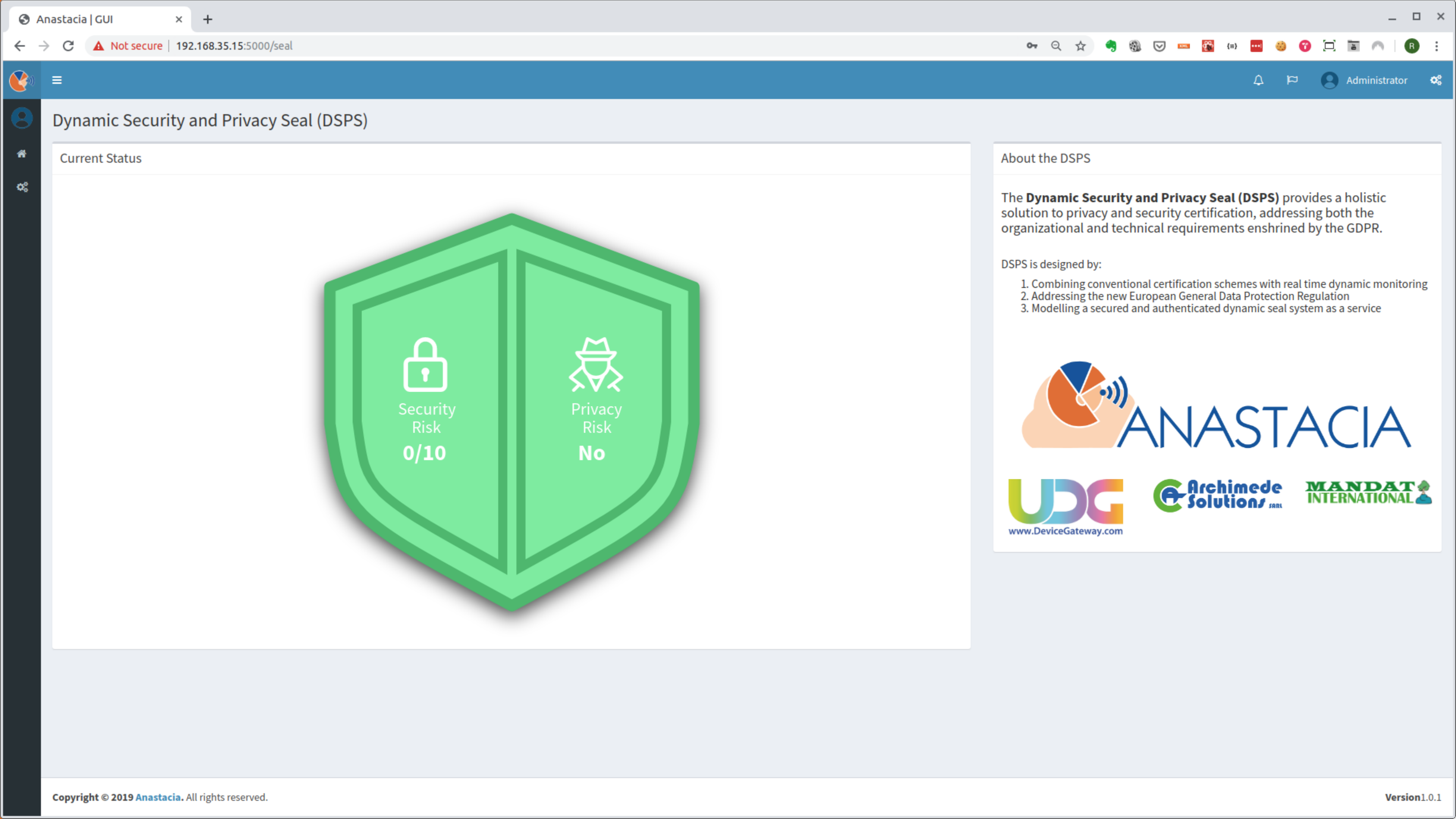
The **Dynamic Security and Privacy Seal (DSPS)** provides a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR.

DSPS is designed by:

Combining conventional certification schemes with real time dynamic monitoring

Addressing the new European General Data Protection Regulation

Modelling a secured and authenticated dynamic seal system as a service



Dynamic Security and Privacy Seal (DSPS)

Current Status

Security Risk
0/10

Privacy Risk
No

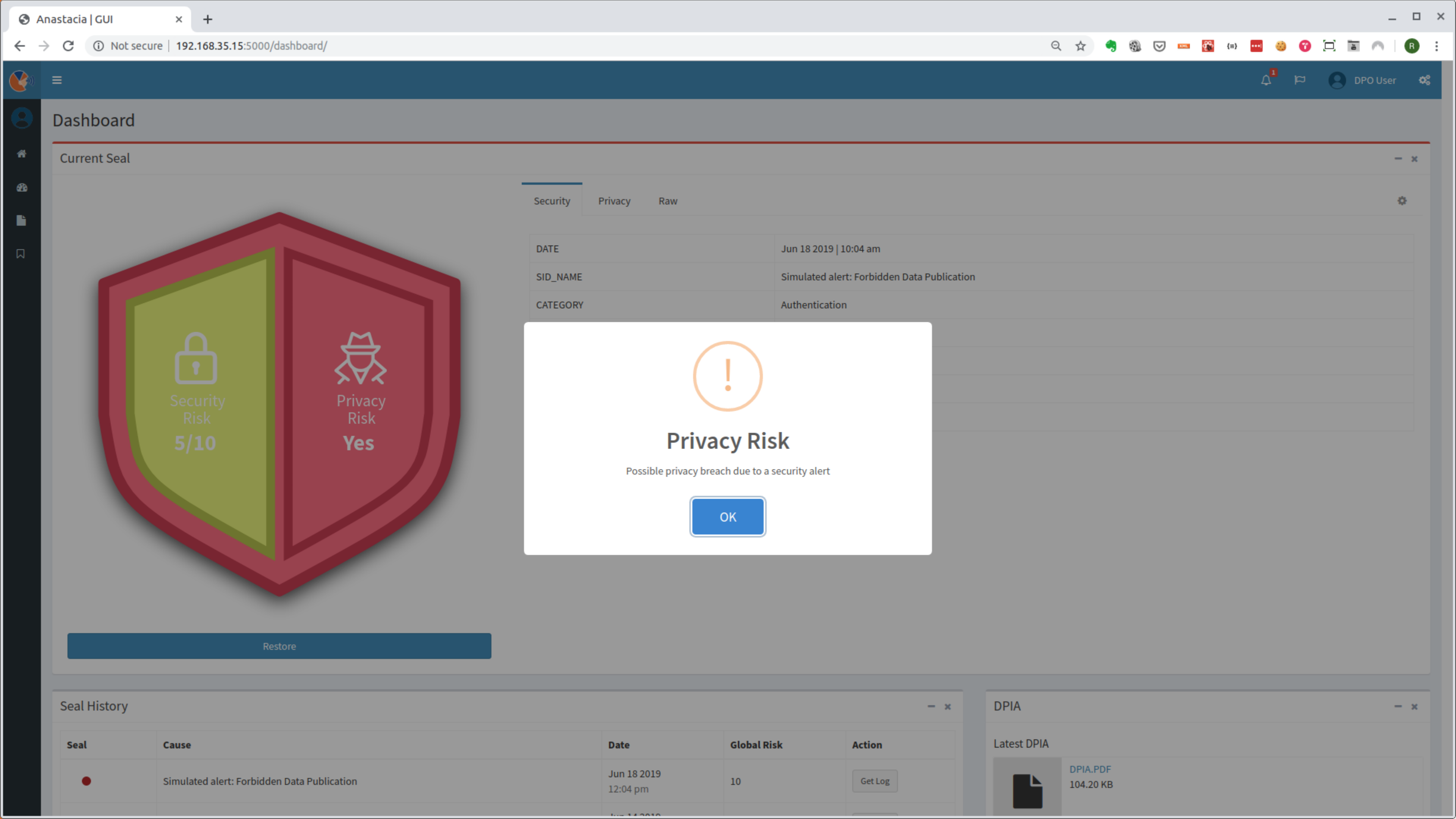
About the DSPS

The **Dynamic Security and Privacy Seal (DSPS)** provides a holistic solution to privacy and security certification, addressing both the organizational and technical requirements enshrined by the GDPR.

DSPS is designed by:

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

Version1.0.1



Dashboard

Current Seal

DATE	Jun 18 2019 | 10:04 am
SID_NAME	Simulated alert: Forbidden Data Publication
CATEGORY	Authentication

Privacy Risk

Possible privacy breach due to a security alert

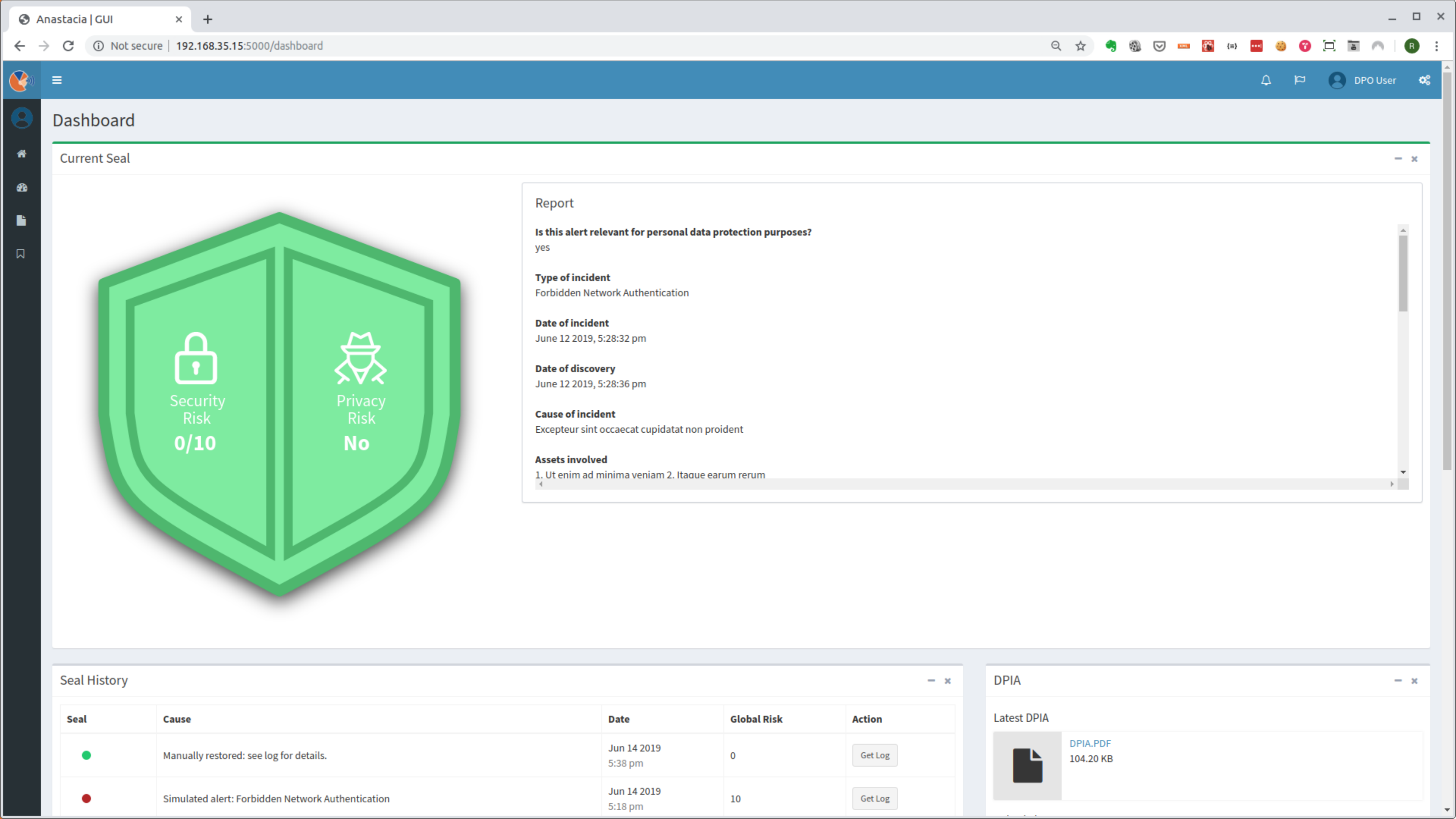
Seal History

Seal	Cause	Date	Global Risk	Action
●	Simulated alert: Forbidden Data Publication	Jun 18 2019 12:04 pm	10	Get Log

DPIA

Latest DPIA

DPIA.PDF
104.20 KB



Dashboard

Current Seal

Report

Is this alert relevant for personal data protection purposes?
yes

Type of incident
Forbidden Network Authentication

Date of incident
June 12 2019, 5:28:32 pm

Date of discovery
June 12 2019, 5:28:36 pm

Cause of incident
Excepteur sint occaecat cupidatat non proident

Assets involved
1. Ut enim ad minima veniam 2. Itaque earum rerum

Seal History

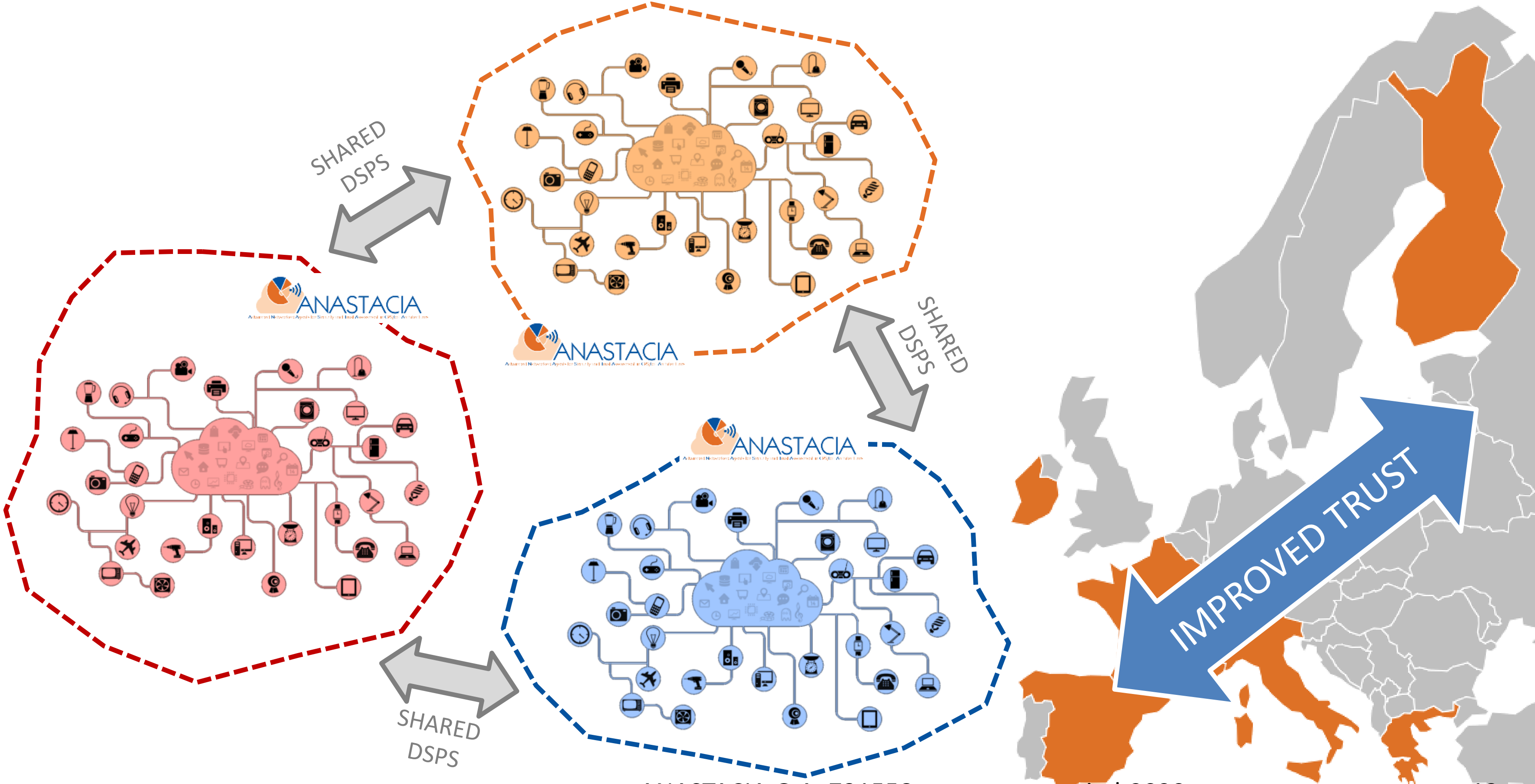
Seal	Cause	Date	Global Risk	Action
●	Manually restored: see log for details.	Jun 14 2019 5:38 pm	0	Get Log
●	Simulated alert: Forbidden Network Authentication	Jun 14 2019 5:18 pm	10	Get Log

DPIA

Latest DPIA

DPIA.PDF
104.20 KB

EU Security/Privacy-compliant IoT Business Ecosystem



Take-aways

- Human-focused Privacy and Security by design is necessary to enable trust
- ANASTACIA can help track the implementation of these principles in IoT/CPS architectures
- The DSPS aims to bridge privacy and security perspectives in a trustworthy manner

Contacts

- Project Coordinator

  Stefano BIANCHI (Softeco Sismat)

  stefano.bianchi@softeco.it

- Scientific and Technical Project Manager

  Antonio SKARMETA (Universidad de Murcia)

  skarmeta@umu.es

- DSPS Coordinator

  Adrian QUESADA RODRIGUEZ (Mandat International)

  aquesada@mandint.org

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.

ANASTACIA

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

www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

http://www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu