

Towards the Certification for IoT

IoT Week

Geneva, 6-9 of June 2017

Session: GDPR&IoT

Avv. Lucio Scudiero

Researcher on data protection law

Personal Data Protection Officer

Certification in the GDPR

Data protection certification mechanisms, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Art. 42.1 GDPR)

Issued by **Certification Bodies** accredited by

- DPAs/EDPB or
- National Accreditation body named in accordance with Regulation (EC) No 765/2008

On the basis of EN-ISO/IEC 17065/2012 + criteria identified by the DPAs/EDPB (Art. 43.1.a –b GDPR)

Certification should last for a maximum period of 3 years, should not prevent DPAs from exercising their powers

The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means

The strategy towards a IoT Certification Mechanism

Leveraging on and facilitating access to privacy certification solutions developed by the European research community

Delivering a set of methodologies for privacy and security compliance within the IoT domains

Advising institutional stakeholders on criteria for IoT certification mechanisms and certification bodies accreditation

Proactively supporting the development of global standards on IoT privacy and personal data protection

Research Projects



Privacy Risk Assessment Methodology Privacy & GDPR Certification



**End-User Engagement
in Large Scale Pilots on IoT**



**IoT Privacy & Cybersecurity
Privacy & Security Seal**



**CSA for Large Scale Pilots on IoT
Trusted IoT Label**

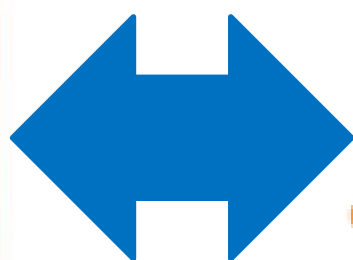


PRIVACY FLAG

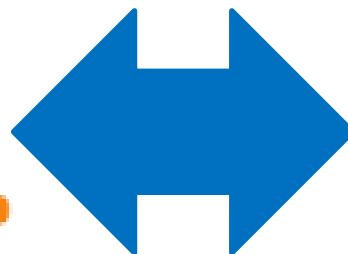
UPRAAM



Law

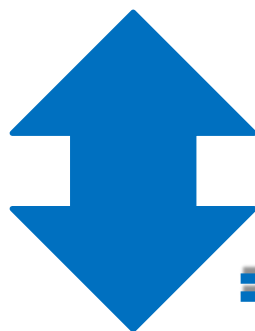


PRIVACY FLAG



ICT

Users



= Scalability



Dynamic Security and Privacy Seal

ANASTACIA has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558

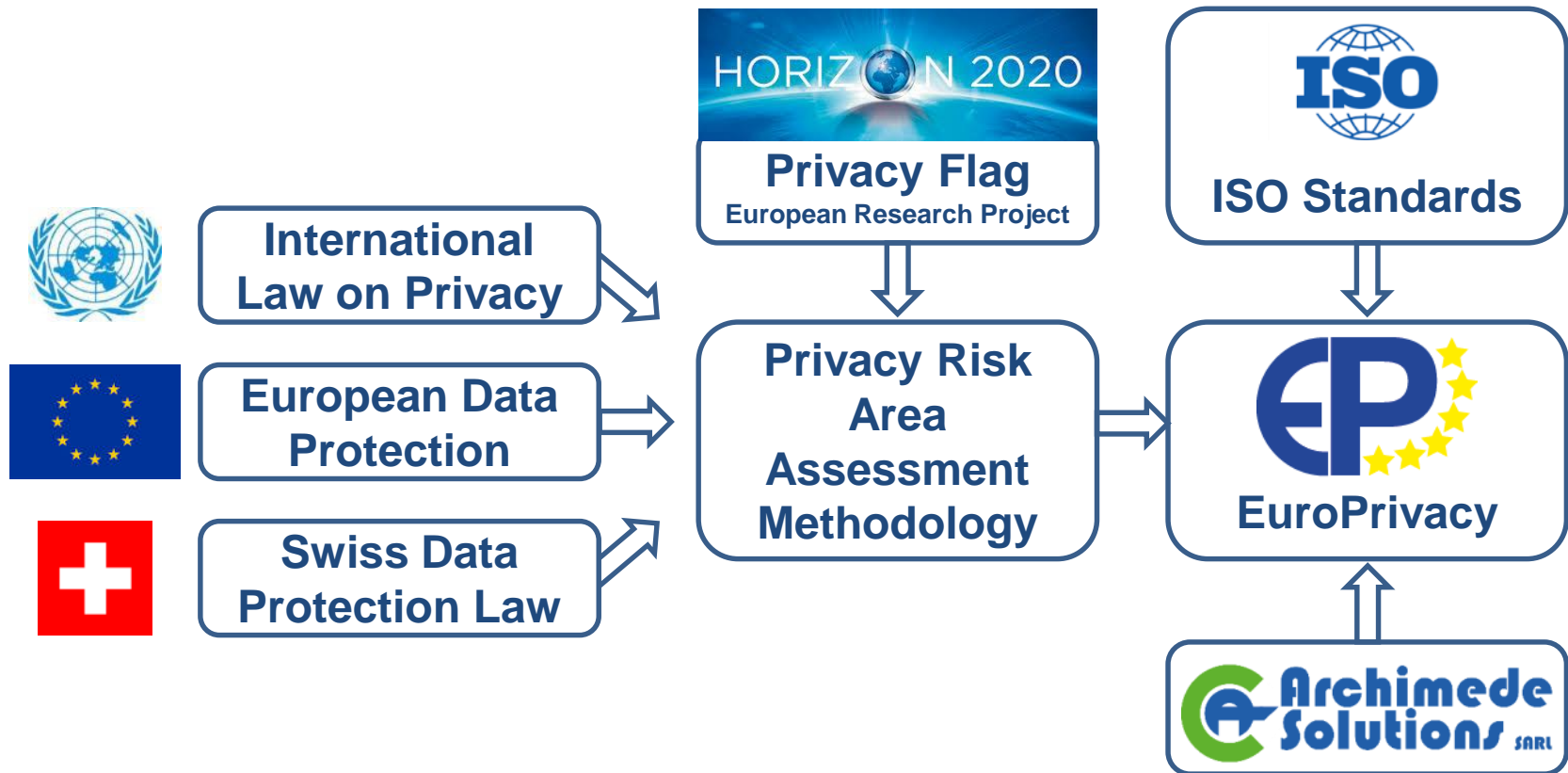


WP 5 - Dynamic Security and Privacy Seal

Trusted IoT Label



European Certification Scheme on Personal Data Protection for the GDPR



www.europprivacy.org



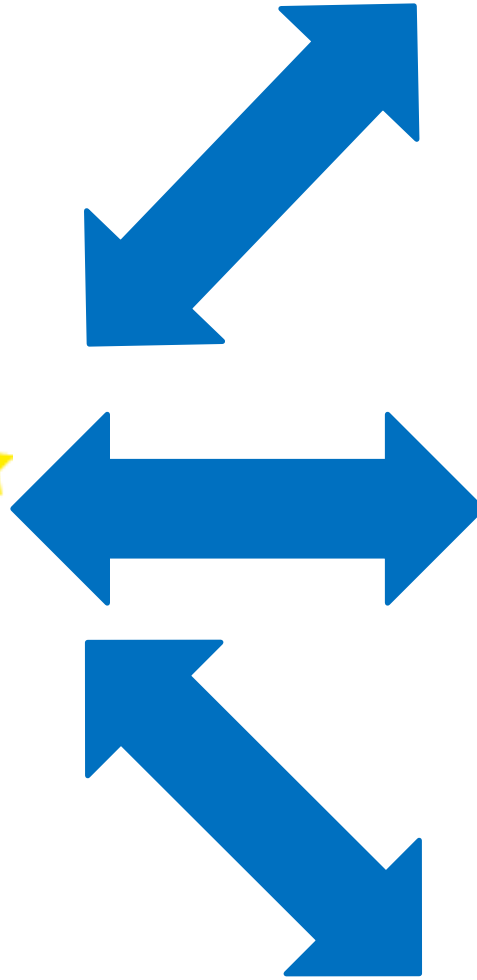
IoT Deployments



Websites



Apps



European Center for Certification and Privacy



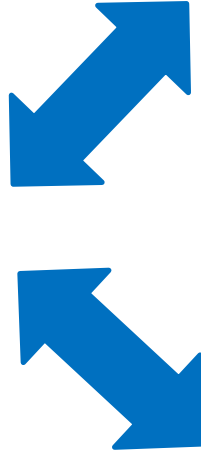
Archimede Solutions
Istituto Italiano per la Privacy
University of Luxembourg
IPv6 Forum

**Privacy / GDPR
Certification**



EuroPrivacy

**IoT Standards
Certification**



Exploring new models in privacy certification

Convergence of GDPR towards the eIDAS Regulation model

GDPR Certification Bodies (CBs) like (Qualified) Trust Service Providers (TSPs)

CBs issue Certificates, under DPAs' supervision

Certificates are relied upon by Privacy Electronic Seals

Privacy Electronic Seal

Privacy Electronic Seal


guarantees adherence of a IoT deployment to a predefined privacy sticky policy

is uniquely linked to the creator of the seal

is linked to the data to which it relates in such a way that any subsequent change in the data or in the data processing is detectable.

Certify to simplify

Legitimate Interest (at least for cybersecurity purposes)



Recital 49 GDPR - The processing of personal data to the extent strictly necessary and proportionate for the purposes of **ensuring network and information security (...)** by providers of **electronic communications networks and services** and by providers of security technologies and services, **constitutes a legitimate interest of the data controller concerned**. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.



Thank you for your attention!
iscudiero@archimede.ch