Wi-fi: MARRIOT_CONFERENCE
EVDT04

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Break-out 3 – Policy, governance, ethics, human aspects, trust and usability

Chair: Linda Strick, Fraunhofer FOKUS & EU - SEC

cyberwatching.eu
The European watch
on cybersecurity & privacy

Participants

Break-out 3 – Policy, governance, ethics, human aspects, trust and usability

Family Name	First Name	Project
Markatos	Evangelos	PROTASIS
Ursa	Yolanda	AEGIS
Loi	Michele	CANVAS
Koch	Klaus-Michael	certMILS
Sutton	Lorenzo	COMPACT
Röning	Juha	CS - AWARE
Giampaolo	Francesca	DOGANA
Aguzzi	Stefania	E - SIDES
Strick	Linda	EU - SEC
Blanc	Gregory	EUNITY
Shamah	Jon	FUTURETRUST
Shamah	Jon	LIGHTest
Martin	Griesbacher	TRUESSEC.EU

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Evangelos Markatos, Coordinator
The PROTASIS project
markatos@ics.forth.gr

PROTASIS Project

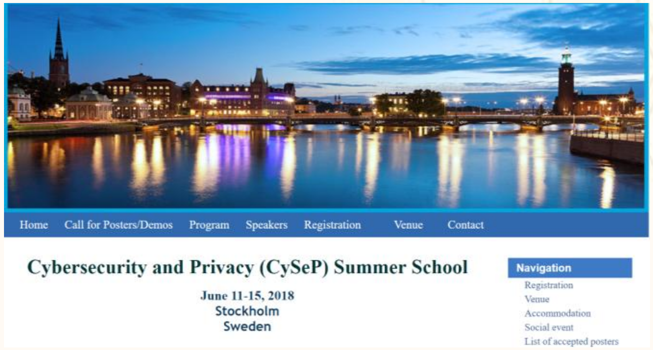
- A Marie Skłodowska-Curie
  - Research and Innovation Staff Exchange
  - RISE Action
- Who?
  - FORTH, VU, PoliMi, RUB, F-SECURE, Telefonica
  - In collaboration with
  - MIT, Columbia, UCSB, UIC, Stony Brook, Northeastern, BU, Stevens IT

PROTASIS Objectives, challenges & results for end users

- Objectives
  - State of the Art Research
    - Cyberattacks, exfiltration, defences, IoT
  - Transfer knowledge
    - Inter-sectoral (Academia-Industry)
    - international (EU-US)
  - Facilitate the professional development
    - Of the secondees
- Results
  - Code, defences, papers, etc.
  - code/data repository (available to Academia at present)

PROTASIS next steps & collaboration opportunities

- Collaboration opportunities
  - Participate in PROTASIS'
    - Summer schools:
      - June 10-11 2018 collocated with CySeP 2018 Stokholm
        - https://cysep.conf.kth.se/
    - PROTASIS workshop (2019)
  - Participate in Joint EU proposals
    - For Marie Curie and H2020 projects



Cybersecurity and Privacy (CySeP) Summer School

June 11-15, 2018
Stockholm
Sweden

AEGIS Vision and Goals

Yolanda Ursa

Inmark Europa

aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 740647

aegis

Accelerating EU-US Dialogue in Cybersecurity and privacy

- Horizon 2020 CSA - Coordination & Support Action
- Main purpose - facilitate exchange of views, policies and best practices to stimulate EU – US cooperation around cybersecurity and privacy Research & Innovation (R&I)

The Consortium

inmark europa

Consiglio Nazionale delle Ricerche

Waterford Institute of Technology

Hewlett Packard Enterprise

european american chamber of commerce new jersey

THE PROVIDENCE GROUP

RUTGERS

Co-funded by the Horizon
2020 Framework Programme of
the European Union

Objectives

Provide **support to EU-US dialogues** related to cybersecurity and privacy, by providing a practical and effective international collaboration platform engaged in:

a. discussing progress and **priorities**;

b. setting the cybersecurity and privacy **research agendas** to be pursued at an international scale; and

c. **coordinating** the sharing of policies and best practices, knowledge and experience in an effort to stimulate cooperation around cybersecurity and privacy research and innovation approaches and thus contribute in shaping the future global cybersecurity landscape.

Co-funded by the Horizon
2020 Framework Programme of
the European Union

aegis

Cybersecurity Reflection Group EU-US

A multi-stakeholder collaboration platform to facilitate interaction, debate and exchange of views between European and US relevant stakeholders.

Two Working Groups

Cybersecurity and Privacy R&I

Cybersecurity and Privacy Policies

JOIN US!

Co-funded by the Horizon
2020 Framework Programme of
the European Union

aegis

Thank you

Yolanda.Ursa
Yolanda.Ursa@Grupoinmark.com
www.aegis-project.org

Co-funded by the Horizon
2020 Framework Programme of
the European Union

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

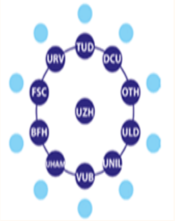
26 April 2018

Brussels, Belgium

Michele Loi

CANVAS

CANVAS Project Objectives, challenges & results for end users



1. We have created an '**alliance**' to enable and strengthen intra-academic and industry-academia networking activities and knowledge sharing

2. We are developing **briefing packages** for policy makers and industry stakeholders

3. We are developing a **'reference curriculum**' for academic and industry stakeholders

4. We are developing **MOOCs** for academic and industry stakeholders

CANVAS Project next steps & collaboration opportunities

- 2018/05/28–29: Workshop Workshop “Towards a value-sensitive Cybersecurity Industry”, Helsinki, Finland
- 2018/09/05–07: Workshop “Value-sensitive Cybersecurity in National Security”, Bern, Switzerland
- 2018/09/24–26: ETHICOMP 2018 – Living with Cybersecurity: A Shared Responsibility

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Klaus-Michael KOCH

certMILS

Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats

CertMILS Project Objectives, challenges & results for end users

- Functionality density is increasing
  - Integrate functions on small numbers of ECU
  - Reduce the number of ECUs or keep (at least) the same
  - Benefit on powerful COTS HW and SW
  - Need proper separation and c

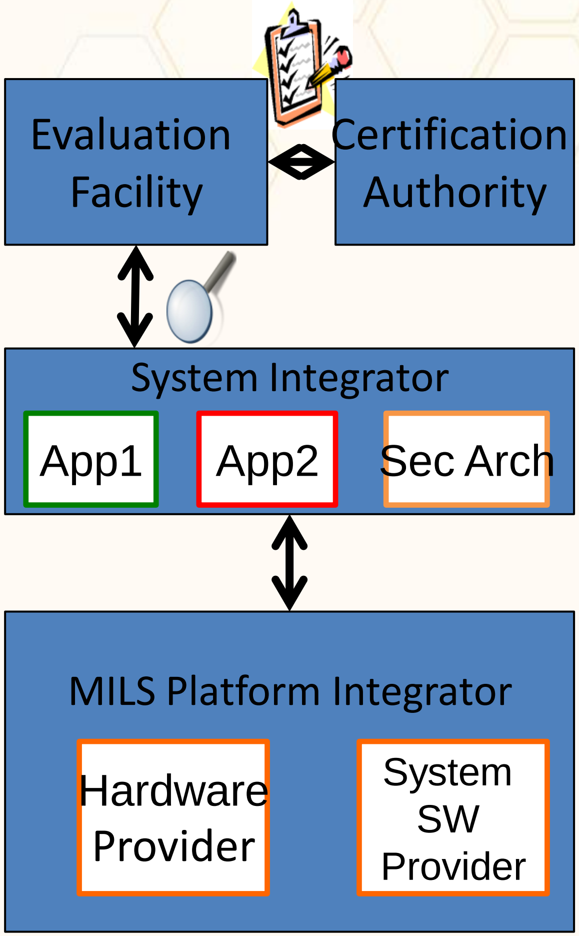
- Heterogeneous inform
  - Systems are interconnected and ex ternal world
  - Usage of common network infras cture
  - Need proper separation and control of inform flows

- High-assurance for mixed-critic
  - Functionalities have different ass nce requirements, e.g. safety vs. security
  - The overall assurance design shall b to run the most demanding one
  - Need proper compositional certification approach

Affordable assurance

CertMILS Project next steps & collaboration opportunities

- Main security challenge: Integration of components
- Pilots based on a separation kernel with system integrators from railway, subway + smart grid
- Focus pilots on modular and compositional security evaluation of integrated system
- Develop security architecture and employ the guarantees of the MILS foundational components
- Apply developed MILS Integration Profile
- Evaluate results with respect needs (e.g., for IEC 62443) and interpretations
- We're looking for partners
  - Interested in joining Common Criteria standardization of separation kernels at Common Criteria Users Forum and/or mils.community
  - Interested in doing (lightweight) certification on system using separation kernel
- Available:
  - Modular Protection Profile (Base PP for separation kernel + models)
  - Security Architecture Templates for CC- and IEC 62443-certifying composed systems



cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Lorenzo Sutton

Engineering Ingegneria Informatica

COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

COMPACT Project Objectives, challenges & results for end users

- COMPACT addresses key **challenges** in helping Local Public Authorities (LPAs) tackle cyber-threats:
  - Overlooking the human element is the most common mistake in cyber security.
  - LPAs are becoming an attractive target for cybercriminals while trying to leverage on the benefits of internet/cloud services
  - consequences of cyber-threats can be considerable and impact both individuals and organisations
- To address these challenges, the key objectives of COMPACT are:
  - Empower LPAs to become the main actors of their cyber-resilience;
  - increase **awareness**, skills and protection;
  - foster information **exchange** between European LPAs;
  - link LPAs to major EU **initiatives**, including the newly created cyber-security PPP;
  - Use **best-in-class** solutions and tools tailored to LPA needs
- **Users** from local public authorities will **benefit** from the training and information sharing services allowing them to learn how to identify cyber threats in their daily work and to reduce risky behaviour
- COMPACT adopts innovative gamification approaches based on studies in 5 European municipalities
- Key Results include:
  - risk assessment and monitoring tools;
  - integrated approaches featuring applicability, usability, automation, and flexibility.
  - easy-to-use and accessible interfaces

COMPACT Project next steps & collaboration opportunities

- **Adaptation** of existing components to LPAs **needs** identified through the user requirements and specifications activities.
- Creation of the **contents** for the **gamified** awareness and training.
- Definition of the COMPACT **trials** with the objective to validate the COMPACT platform by means of the use case applications against the requirements.
- Opening of the COMPACT **Information Hub** which will allow the community to exchange information, involve relevant stakeholders and stimulate interaction.
- Collaboration **opportunities** with projects working in the cybersecurity domain
- Collaboration with LPAs interested in the project results and to become potential users of COMPACT

COMPACT consortium partners 14 organisations from seven EU member states.
Austria | Belgium| Germany | Italy | Portugal | Spain | United Kingdom

ENGINEERING

cini consorzio interuniversitario nazionale per l'informatica

inov inesc • inovação

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

S21 SEC Your Cybersecurity Company

silensec

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

KASPERSKY lab

KU LEUVEN

Wirtschaftsbetrieb der Stadt Bremerhaven BIT

Comune di Bologna

AMADORA Câmara Municipal

DONOSTIA SAN SEBASTIÁN

Comune di Afragola

cyberwatching.eu
The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Prof. Juha Röning,
University of Oulu, Finland

CS-AWARE
CYBERSECURITY

CS-AWARE objectives, challenges & results for endusers

- Challenge

  Cybersecurity is one of today's most challenging societal security problems, affecting large commercial companies, SMEs, NGOs or governmental institutions. Deliberate or accidental threats and attacks threaten digitally administered data and processes.

- Results for end users

  to provide a cybersecurity situational awareness solution for small to medium sized IT infrastructures.

Prof. Juha Röning, jjr@ee.oulu.fi

CS-AWARE next steps & collaboration opportunities

- Next steps
  - Q3/18: initial deployment in Larissa (Greece) & Rome.
  - Q4/18: commercialisation intensifies
- Collaboration opportunities
  - platform for new information security awareness systems – open for additional technologies / practises.
  - new pilots – become the InfoSec vanguard

- More at: https://cs-aware.eu/

Prof. Juha Röning, jjr@ee.oulu.fi

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Francesca Giampaolo (Engineering Ingegneria Informatica S.p.A.)

Dogana

ADVANCED SOCIAL ENGINEERING AND
VULNERABILITY ASSESSMENT FRAMEWORK

DOGANA- Project Objectives, challenges & results for end users

DOGANA aims at developing a framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment“

DOGANA aims to provide enterprises with a complete framework to assess their exposure and consequently adopt secure countermeasures.

Two relevant features of the proposed framework are:

- The presence of the **"awareness" component** within the framework as the cornerstone of the mitigation activities;
- The **legal compliance** by design of the whole framework, that will be ensured by a partner and a work package explicitly devoted to this task.

DOGANA- Project next steps & collaboration opportunities

- An extensive **field trial plan** to test and validate the DOGANA platform with six users (4 partners and 2 supporting users) operating in the critical areas of energy, finance, transport, utilities, and public authorities.

- Around **20 international projects** possibly **related to DOGANA** have been identified, 11 have been contacted, with the following results:
- INOV participated at the FP7 ECOSSIAN Workshop about European Control System Security Incident Analysis Network (PARIS)
- KUL participated at the H2020 CANVAS Workshop about Cybersecurity Challenges in Healthcare Ethical, Legal and Social Aspects (GENEVA)
- A webinar will be held by a member of the DOGANA consortium on the legal issues of gathering informations from social networks

cyberwatching.eu
The European watch
on cybersecurity & privacy

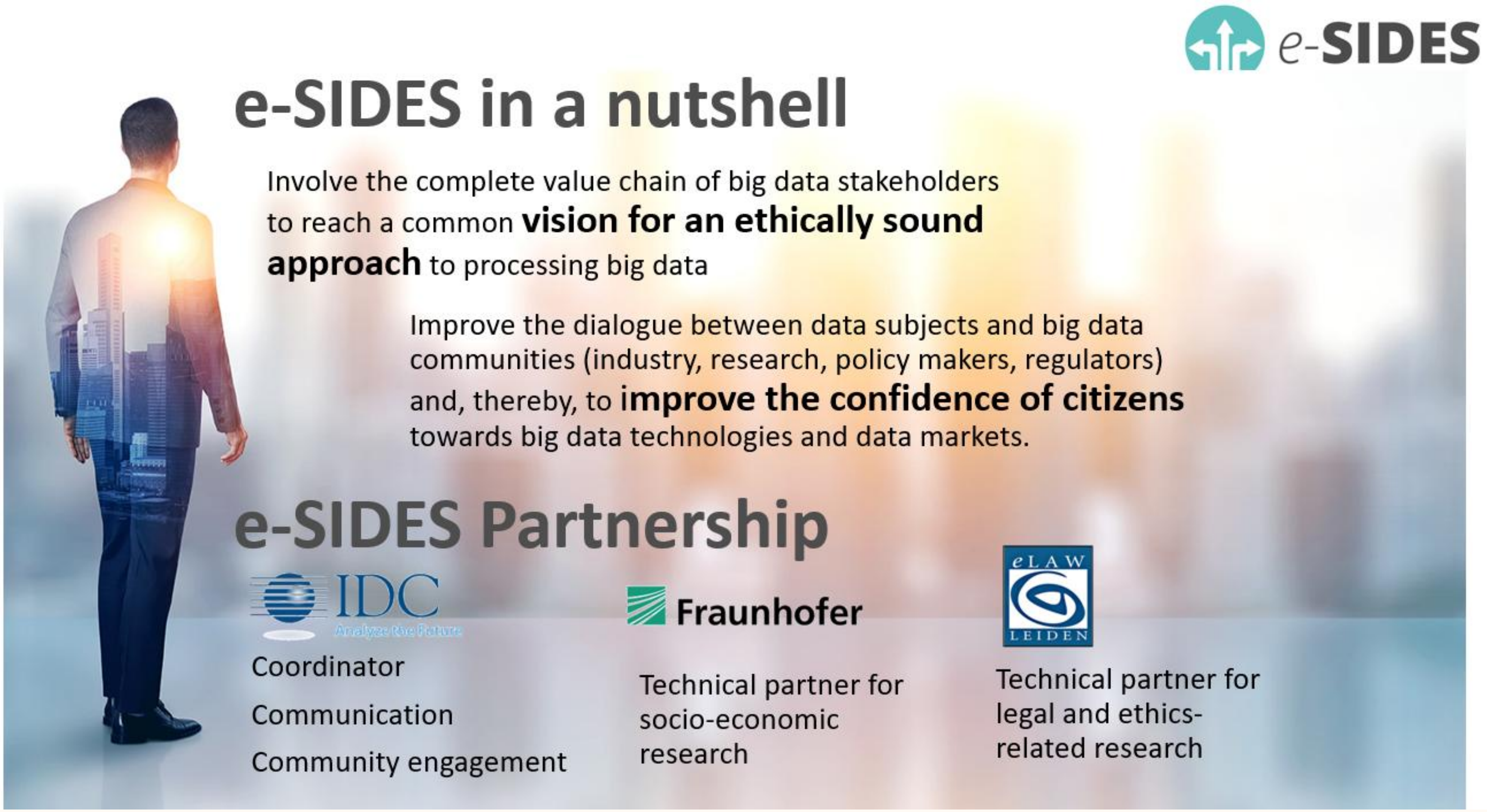
First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Stefania Aguzzi, Senior Consultant, IDC

Communication Manager, e-SIDES

e-SIDES



e-SIDES

e-SIDES in a nutshell

Involve the complete value chain of big data stakeholders to reach a common **vision for an ethically sound approach** to processing big data

Improve the dialogue between data subjects and big data communities (industry, research, policy makers, regulators) and, thereby, to **improve the confidence of citizens** towards big data technologies and data markets.

e-SIDES Partnership

IDC
Analyze the Future

Coordinator

Communication

Community engagement

Fraunhofer

Technical partner for socio-economic research

eLAW
LEIDEN

Technical partner for legal and ethics-related research

Data-driven innovation is transforming the economy and the society we live in.
How do we back these technological changes with a firm ethical position?

Towards the next generation of next Big Data Technologies

Ethical issues:

BD profiling, categorising, classifying of data about individuals may…

Weaken social cohesion

Weaken individual autonomy

Create bias about some groups of people

Legal issues issues:

The volume, variety and velocity of Big Data sets may have unintended negative consequences…

Lack of fully informed consent

Ineffective purpose limitation

Harmful consequences from data processing

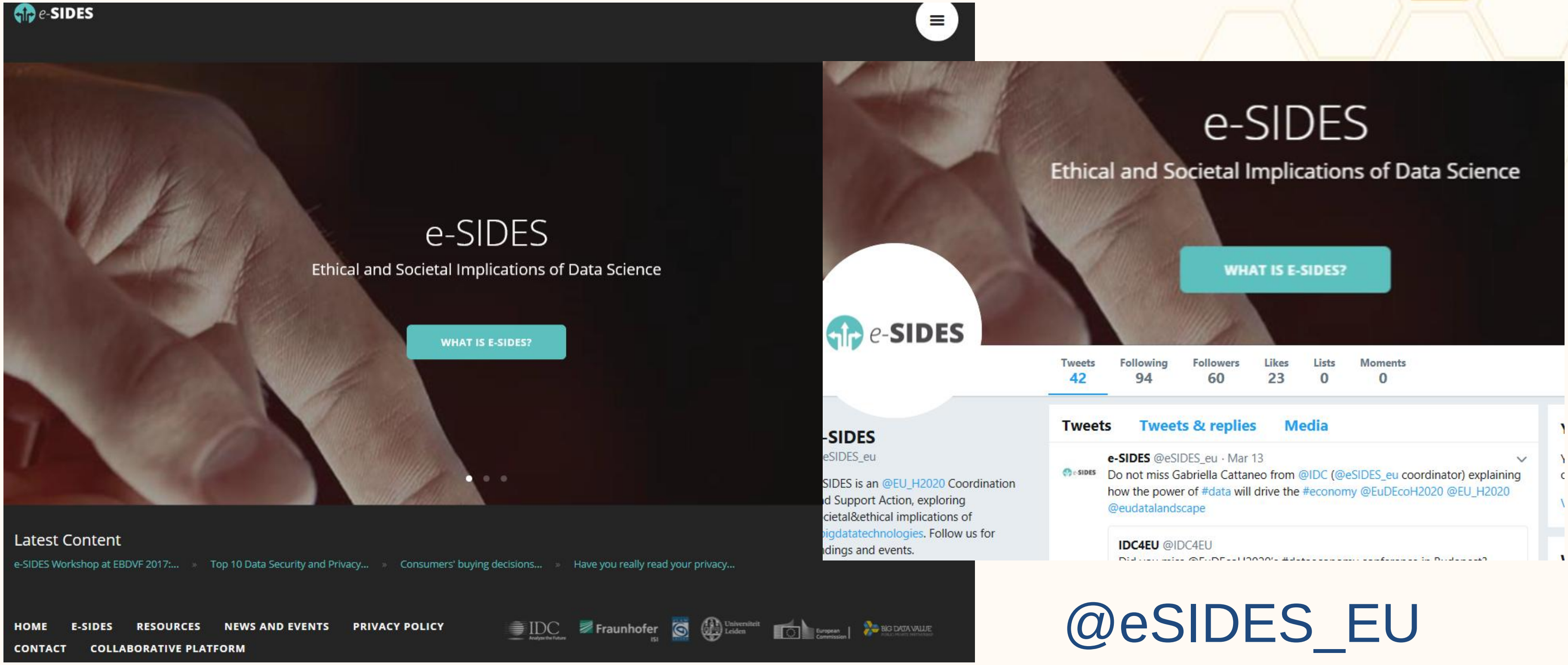
e-SIDES

Next steps & collaboration opportunities

- Future events: BDV-PPP Meetup and ICT2018
  - Organization of joint sessions
  - Other events for collaboration
- Upcoming reports to be published
  - Sharing results
- Community position papers on the requirements for the next generation of BDT
  - Have your say as data science/ big data expert
  - Leveraging synergies with your project

e-SIDES

Connect with us..



e-SIDES

e-SIDES

Ethical and Societal Implications of Data Science

WHAT IS E-SIDES?

Latest Content

e-SIDES Workshop at EBDVF 2017:... » Top 10 Data Security and Privacy... » Consumers' buying decisions... » Have you really read your privacy...

HOME E-SIDES RESOURCES NEWS AND EVENTS PRIVACY POLICY
CONTACT COLLABORATIVE PLATFORM

e-SIDES

Ethical and Societal Implications of Data Science

WHAT IS E-SIDES?

e-SIDES

Tweets	Following	Followers	Likes	Lists	Moments
42	94	60	23	0	0

-SIDES
eSIDES_eu

SIDES is an @EU_H2020 Coordination
d Support Action, exploring
cietal&ethical implications of
igdatatechnologies. Follow us for
dings and events.

Tweets Tweets & replies Media

e-SIDES @eSIDES_eu · Mar 13
Do not miss Gabriella Cattaneo from @IDC (@eSIDES_eu coordinator) explaining how the power of #data will drive the #economy @EuDEcoH2020 @EU_H2020 @eudatalandscape

IDC4EU @IDC4EU

@eSIDES_EU

www.e-sides.eu
info@e-sides.eu saguzzi@idc.com

e-SIDES

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

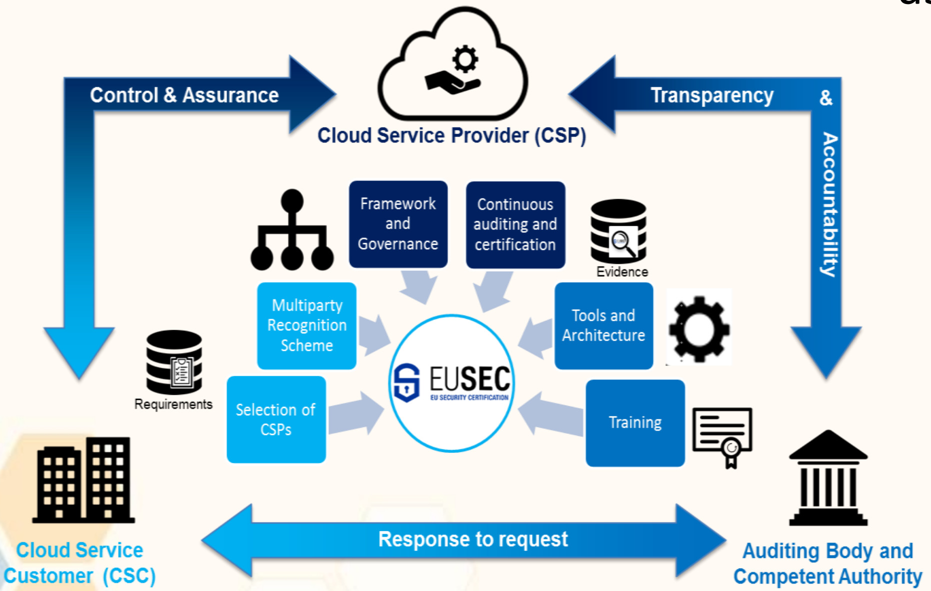
Linda Strick, Fraunhofer FOKUS

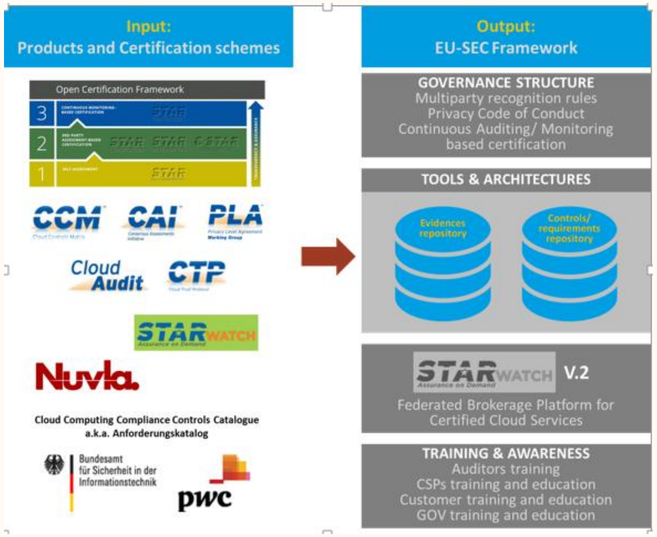
EUSEC
EU SECURITY CERTIFICATION

EU-SEC Project Objectives, challenges & results for end users

European Security Certification Framework (EU-SEC) is an innovation project with an aim to create a framework under which existing certification and assurance approaches can co-exist. It has a goal to improve the business value, effectiveness and efficiency of existing **cloud security certification schemes**

increase the level of efficiency and trustworthiness of the cloud market by offering solutions that makes the companies' compliance effort **more cost-effective** and high-level assurance

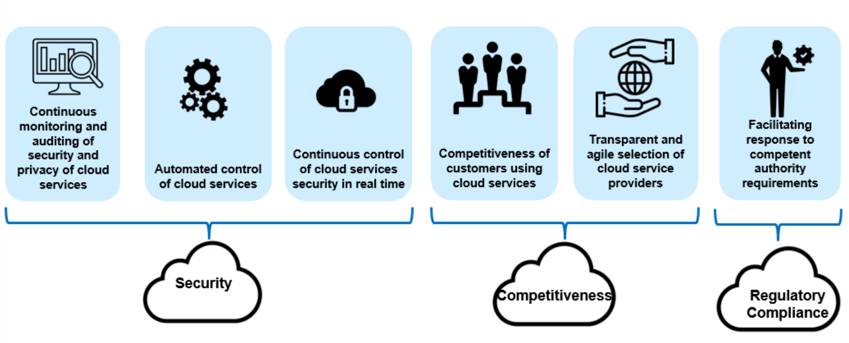

Control & Assurance
Cloud Service Provider (CSP)
Transparency & Accountability
Framework and Governance
Continuous auditing and certification
Evidence
Multiparty Recognition Scheme
Tools and Architecture
EUSEC
EU SECURITY CERTIFICATION
Requirements
Selection of CSPs
Training
Cloud Service Customer (CSC)
Response to request
Auditing Body and Competent Authority


Input:
Products and Certification schemes
Open Certification Framework
3
2
1
STAR
STAR STAR C-STAR
STAR
CCM
CAI
PLA
Cloud Audit
CTP
STARWATCH
Assurance on Demand
Nuvla.
Cloud Computing Compliance Controls Catalogue a.k.a. Anforderungskatalog
Bundesamt für Sicherheit in der Informationstechnik
pwc
Output:
EU-SEC Framework
GOVERNANCE STRUCTURE
Multiparty recognition rules
Privacy Code of Conduct
Continuous Auditing/ Monitoring based certification
TOOLS & ARCHITECTURES
Evidences repository
Controls/ requirements repository
STARWATCH V.2
Assurance on Demand
Federated Brokerage Platform for Certified Cloud Services
TRAINING & AWARENESS
Auditors training
CSPs training and education
Customer training and education
GOV training and education

EU-SEC Project next steps & collaboration opportunities

Validation of the approach with 2 pilots (public sector and banking)

innovative framework that will increase efficiency in **Cloud Security Certification** through the following benefits:


Continuous monitoring and auditing of security and privacy of cloud services
Automated control of cloud services
Continuous control of cloud services security in real time
Competitiveness of customers using cloud services
Transparent and agile selection of cloud service providers
Facilitating response to competent authority requirements
Security
Competitiveness
Regulatory Compliance

Training and awareness events

- **Multi-party Recognition Framework**

  reduce multiple certification efforts

- **Continuous Auditing Scheme**

  improved security and privacy in "real time"

Join the stakeholder group

contact@sec-cert.eu

www.sec-cert.eu

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Gregory Blanc (IMT)

EUNITY

EUNITY Objectives, challenges & results for end users

Promote and foster cybersecurity activities in EU and Japan

- Encourage and support the ICT dialogue
- Identify potential opportunities for future cooperation
- Foster and promote European cybersecurity innovation activities

- Engage ICT dialogue with Japan
- Reach out to relevant stakeholders
- Analyze the gap between JP and EU activities
- Produce strategic R&I agenda

- Set up a website : eunity-project.eu
- Engaged with many stakeholders on both sides
- Held a workshop in Japan with around 50 attendees

EUNITY next steps & collaboration opportunities

- Produce a gap analysis of cybersecurity between EU and Japan
- Organize a workshop in Europe to showcase the analysis
- Produce a SRIA to drive cybersecurity research funding on both sides

- Provide inputs to the gap analysis
- Attend the 2nd workshop in Europe and discuss the analysis
- Support the SRIA for its integration into future WPs

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Jon Shamah

FutureTrust

FutureTrust objectives, & results for end users

- FutureTrust will design and develop innovative Open Source components and services complementing the current eIDAS ecosystem
- FutureTrust will show how practical eIDAS compliant applications can be constructed and utilized with the aid of the developed FutureTrust components
  - Identity Management Service
  - Validation Service
  - Preservation Service
  - Mobile Signing and Sealing Service
  - Global Trust Lists

FutureTrust next steps & collaboration opportunities

- Deploying FutureTrust demonstrators for Use-Cases
- Helping increase global visibility and acceptance for interconnectivity between eIDAS and other trustworthy schemes

- Support us across Europe, in Washington DC and in Singapore!

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Jon Shamah

LIGHTest

COMMUNITY

LIGHTest objectives, challenges & results for end users

- Countries and companies have a vested interest in cross-border trust services
- However without transparency of policies and rules between counterparties trust cannot be achieved

- LIGHTest builds trust transparency by using a standard way of publishing trust lists, schemes and formats, relevant delegation schemes and trust translation schemes – all over a global trust infrastructure

- LIGHTest uses DNS as the most trusted global infrastructure that is widely available, but utilises both technical and legal code to facilitate and accelerate this emerging market.

LIGHTest next steps & collaboration opportunities

- Deploying LIGHTest demonstrators for Use-Cases
- Joining the LIGHTest Community Forum
- Helping increase global visibility and acceptance.

- Support us across Europe, in Boston and in Singapore!

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

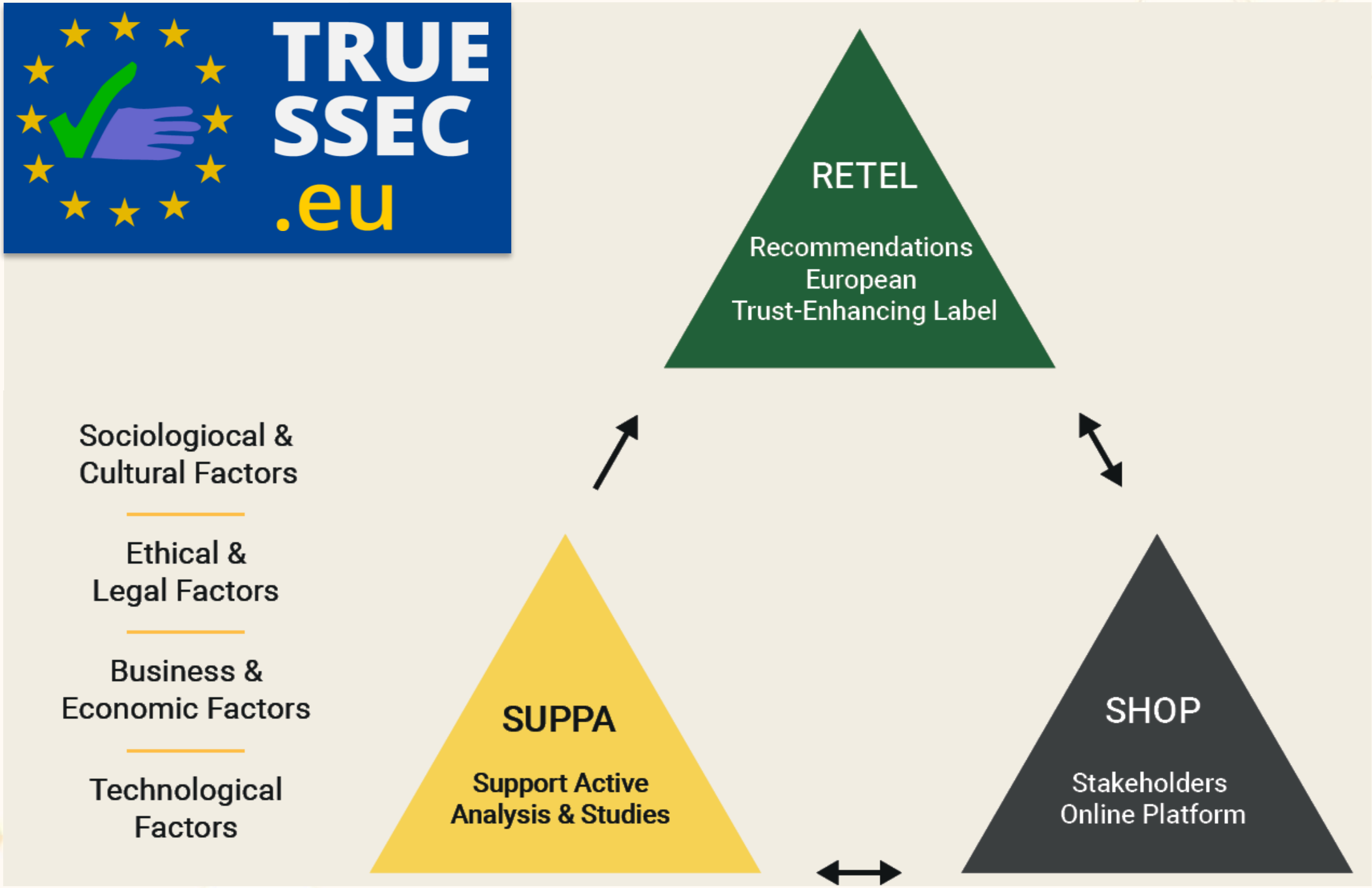
Brussels, Belgium

Martin Griesbacher, University of Graz

TRUESSEC.eu

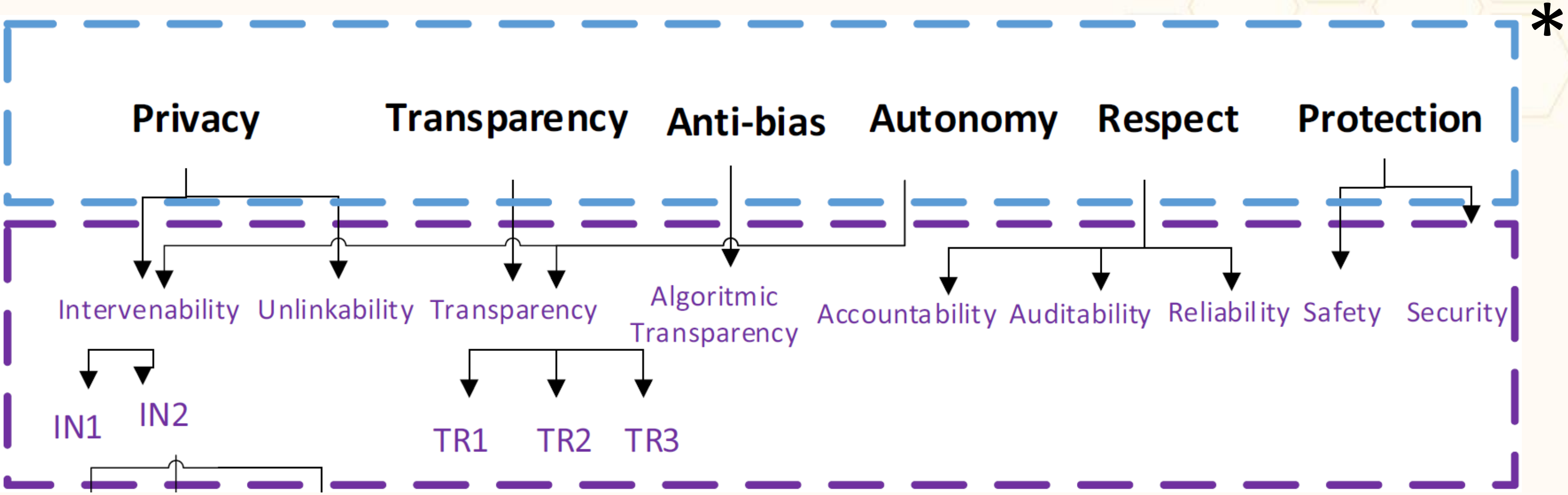
TRUESSEC.eu

Objectives, challenges & results for end users



TRUE
SSEC
.eu
Sociologiocal & Cultural Factors
Ethical & Legal Factors
Business & Economic Factors
Technological Factors
RETEL
Recommendations European Trust-Enhancing Label
SUPPA
Support Active Analysis & Studies
SHOP
Stakeholders Online Platform

TRUESSEC.eu
next steps & collaboration opportunities



- Discussion of Trust-Attributes of your project
  → contact michele.nati@digicatapult.org.uk
- Go to **https://truessec.eu** and contribute!

* source: Guamán/del Álamo/Martín/Yelmo: D5.2 Technical Gap Analysis

5 R&I Challenges

1.				
2.				
3.				
4.				
5.				

Top 5 Cross-cutting themes

1.				
2.				
3.				
4.				
5.				

Top 5 New collaboration opportunities and new ideas.

1.				
2.				
3.				
4.				
5.				