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 1 – Applications & user-oriented services

Chair: Bharadwaj Pulugundla, Verizon & Re-Cred

Participants

Break-out 1 – Applications & user-oriented services

Family Name	First Name	Project
Kurth	Helmut	CITADEL
Striecks	Cristoph	CREDENTIAL
Diaz Rodriguez	Rodrigo	CIPSEC
Tzovaras	Dimitrios	FORTIKA
Komnios	Ioannis	KONFIDO
Christos	Douligeris	MITIGATE
Claudia	Diaz	PANORAMIX
Chochliouros	Ioannis	PRIVACY FLAG
Pulugundla	Bharadwaj	RECRED
Steger	Marco	SCOTT
Larrucea	Xabier	SHIELD
Diaz Rodriguez	Rodrigo	SMESEC
Dépinay	Jean-Loup	SpeechXRays
Diaz Rodriguez	Rodrigo	YAKSHA

cyberwatching.eu

The European watch
on cybersecurity & privacy

CITADEL: Critical Infrastructure Protection using Adaptive MILS

Project Overview

CITADEL Objectives

- Build upon D-MILS and EURO-MILS accomplishments toward Progressive MILS vision for adaptive MILS for protecting critical infrastructures

- Specific technology objectives
  - Declarative languages
  - Compositional verification
  - Configuration monitor synthesis
  - Assurance cases for dynamic systems
  - Dynamic MILS – reconfigurable MILS platform
  - Enforce configuration change policies and "blueprints"
  - Adaptive MILS – adaptive MILS-based systems
  - Monitoring framework
  - Demonstrations in industrial contexts

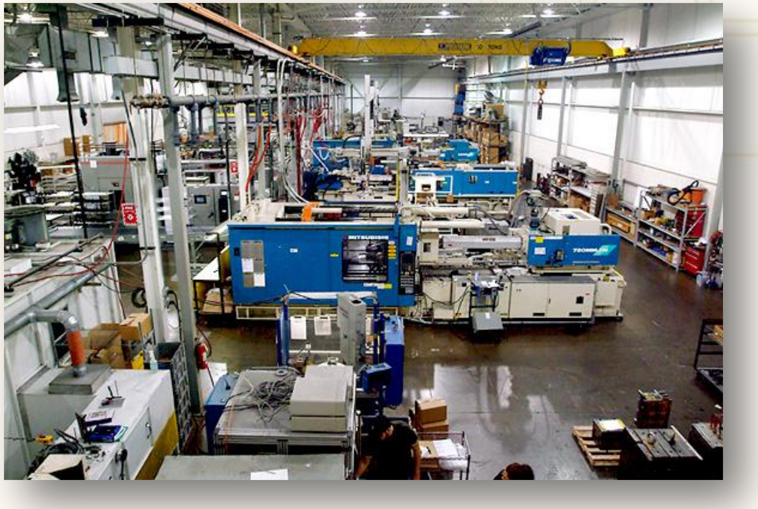
Beyond State-of-the-Art

- Develop an architecture description language able to express dynamic architectures and essential properties to provide basis for verification
- Apply well-established techniques from Aerospace, including diagnosability, FDIR analysis, and observer synthesis to fault/attack detection in communication channels and their impact on safety and security of critical infrastructures
- An integrated formal compositional verification framework, employing various verification techniques, to verify functional, safety and security properties of reconfigurable systems
- Assurance framework integrating language for dynamically changing architectures with runtime assurance of on-going operations and maintenance of certification objectives during configuration change
- Reconfigurable MILS platform including system software and networking
- Generation of target configurations to achieve desired properties and synthesis of reconfiguration plans that maintain necessary conditions
- Foundations for certification of adaptive systems in critical infrastructures

Industrial Demonstrators

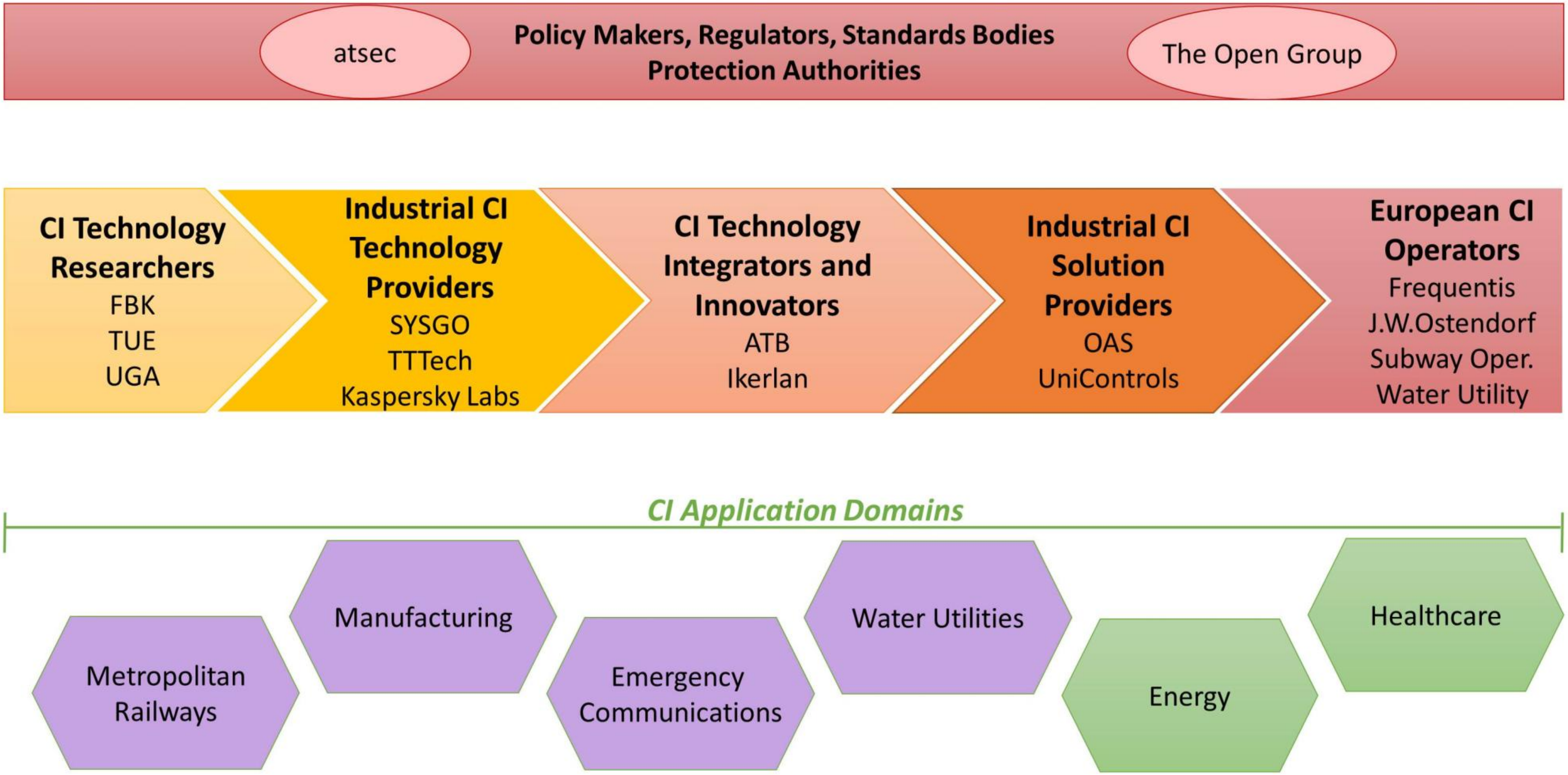
Railways

Manufacturing



Communications

CITADEL Project Ecosystem



atsec

Policy Makers, Regulators, Standards Bodies
Protection Authorities

The Open Group

CI Technology Researchers
FBK
TUE
UGA

Industrial CI Technology Providers
SYSGO
TTTech
Kaspersky Labs

CI Technology Integrators and Innovators
ATB
Ikerlan

Industrial CI Solution Providers
OAS
UniControls

European CI Operators
Frequentis
J.W.Ostendorf
Subway Oper.
Water Utility

CI Application Domains

Metropolitan Railways

Manufacturing

Emergency Communications

Water Utilities

Energy

Healthcare

Adaptive MILS for
Critical Infrastructure Protection

More info: www.citadel-project.org

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Dr. Christoph Striecks

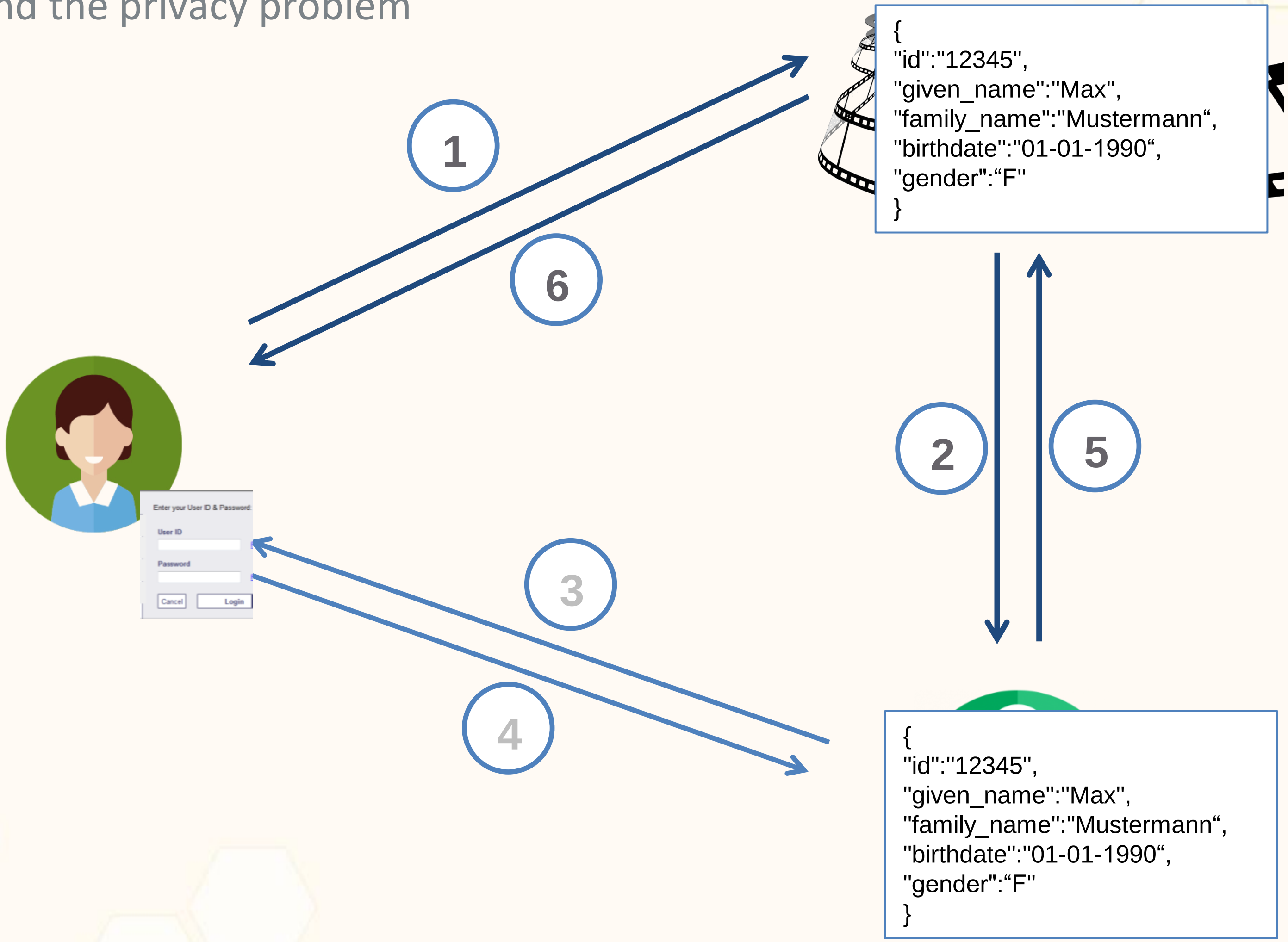
CREDENTIAL

YOU ARE WHAT YOU KEEP!

A Secure Cloud-Identity Wallet

Showcase: Current Single Sign-On (SSO) Flow

Or: Find the privacy problem

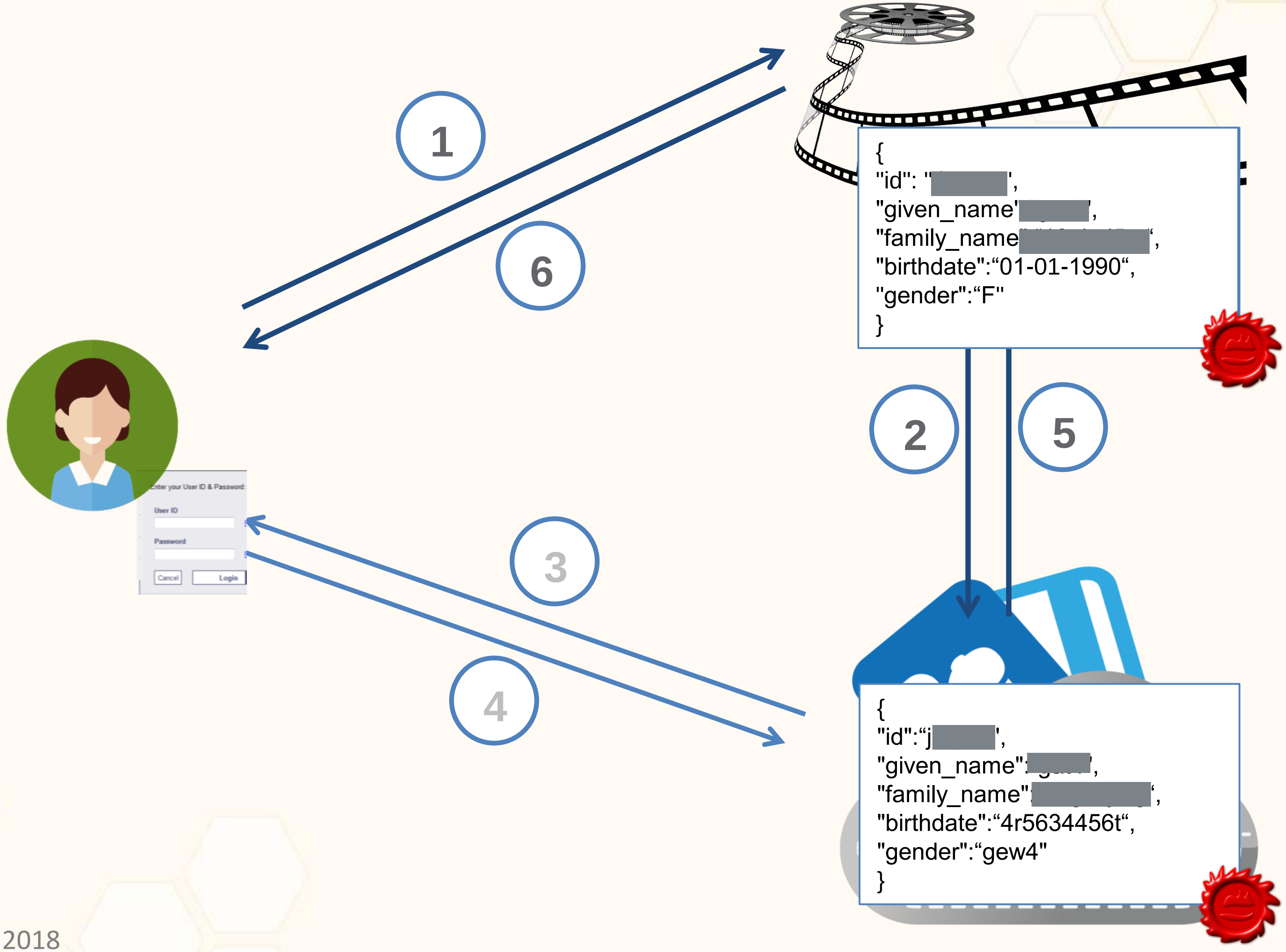


```
{
"id":"12345",
"given_name":"Max",
"family_name":"Mustermann“,
"birthdate":"01-01-1990“,
"gender":“F"
}
```

```
{
"id":"12345",
"given_name":"Max",
"family_name":"Mustermann“,
"birthdate":"01-01-1990“,
"gender":“F"
}
```

Showcase: CREDENTIAL Wallet

Or: CREDENTIAL SSO

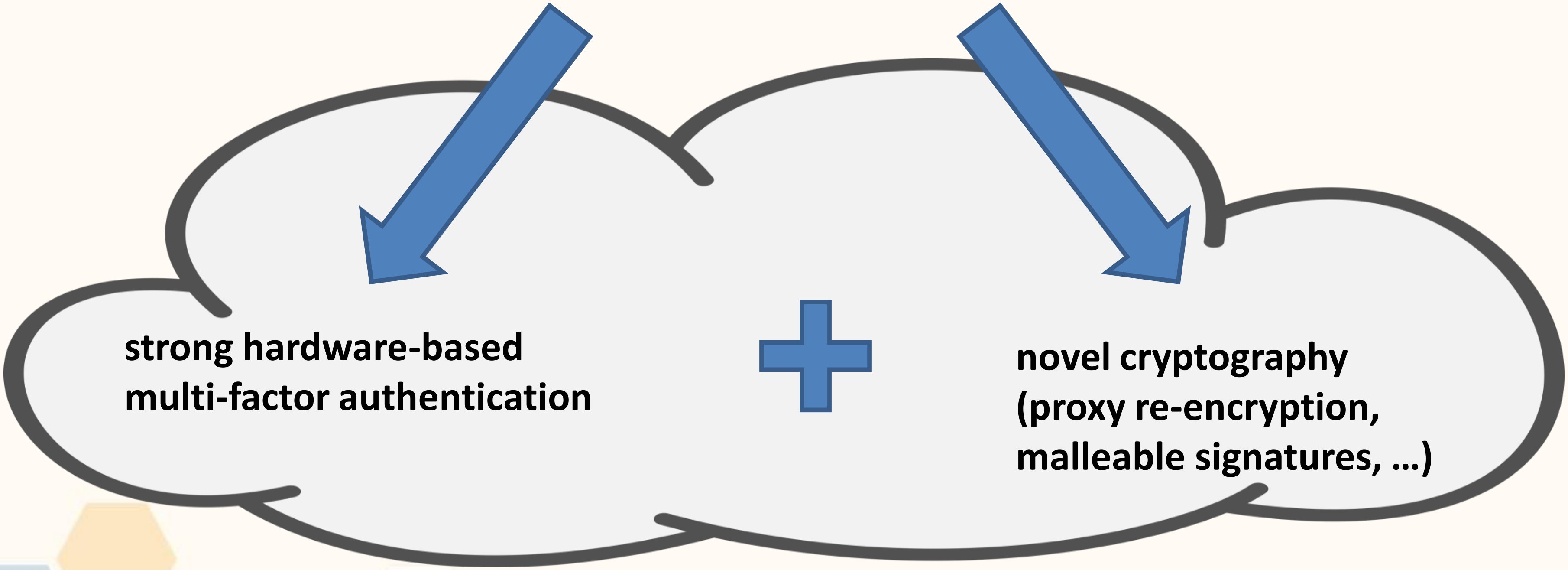


```
{
"id": "[redacted]",
"given_name"[redacted]",
"family_name[redacted]",
"birthdate":“01-01-1990“,
"gender":“F"
}
```

```
{
"id":“[redacted]",
"given_name":[redacted]",
"family_name":[redacted]",
"birthdate":“4r5634456t“,
"gender":“gew4"
}
```

CREDENTIAL Vision & Objectives

The vision of the CREDENTIAL consortium is to **develop, test, and showcase innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions**.

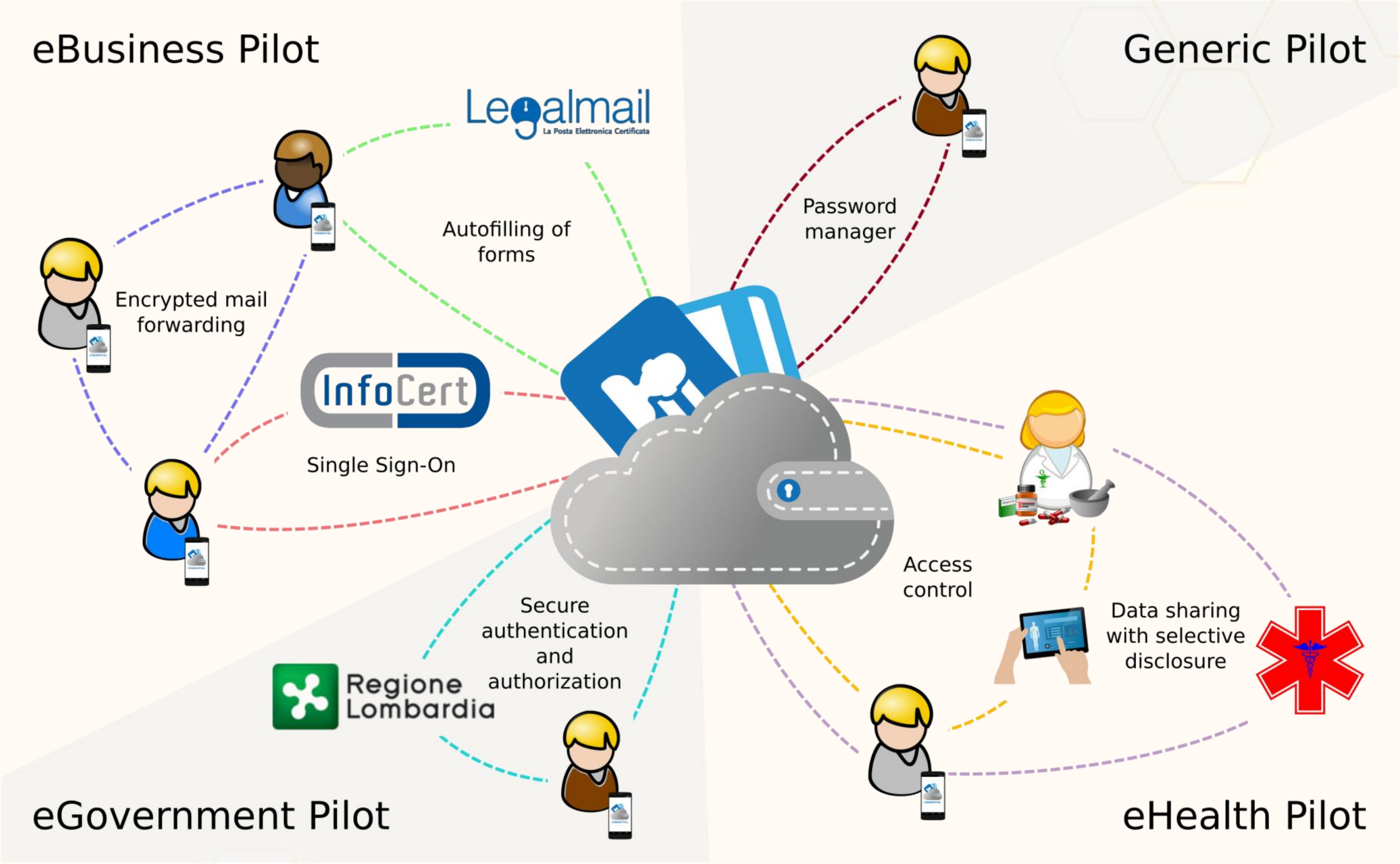


strong hardware-based multi-factor authentication

+

novel cryptography (proxy re-encryption, malleable signatures, …)

Next: Piloting & Standardization



April 26, 2018

CREDENTIAL Takeaway Ambition

Development of a

privacy-preserving, cloudified, end-to-end authentic

platform for

***secure identity provisioning* and *data sharing*.**

Achieved by advancing **novel cryptographic technologies** and improving **strong authentication** mechanisms.

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Rodrigo Diaz Rodriguez, rodrigo.diaz@atos.net

CIPSEC

CIPSEC In a Nutshell

CHALLENGES

Improve the performance of critical infrastructures thanks to ICT Technologies, without compromising their security

OBJECTIVES

Orchestrate security products and services
Cover security gaps in IT/OT networks
Multi-domain application
Highly marketable product (TRL 8)
Alignment with policies and standards

CIPSEC

END-USERS

Baseline reference architecture applicable to a wide range of verticals

Three use cases:

- Health
- Railway
- Environment

RESULTS

FRAMEWORK OF PRODUCTS AND SERVICES

- SIEM
- Network intrusion detection
- Jammer Detector
- Integrity MGT
- Anonymization
- Honeypots
- Vulnerability assessment
- Identity access
- Antimalware
- Forensisc tools
- Continency plans
- Trainings

CIPSEC Project next steps

- **So far**
  - Consolidated architecture
  - First prototype software release
  - Initial pilot deployment
- **For the final year**
  - Final prototype software release
  - Final pilot deployment
  - Testing and validation
  - Exploitation & business models

CIPSEC collaboration opportunities

- **Collaboration with synergistic projects**
  - MF2C, WISER, SMESEC, CYBERWATCHING.EU, RecRED, SAINTS
- **Participation in Forums**
  - PPPs
    - ECSO, Big Data Value Association, 5G PPP, FI PPP
  - Transportation-focused:
    - ETSI Intelligent Transports Forum, German TuV
  - Other
    - US NIST CIP Cybersecurity Standards Forum
- **Workshops**
  - Barcelona (May 2018), Heraklion (September 2018 - RAID 2018)
- **Trainings**
  - Frankfurt (October 2018), Torino (early 2019)

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

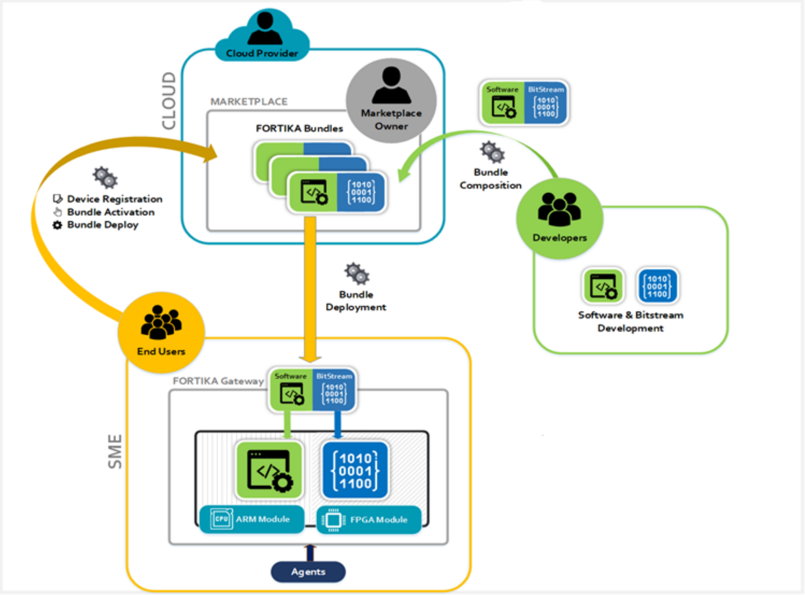
Anastasios Drosou

FORTIKA

Cyber Security Accelerator for trusted SMEs IT Ecosystems

FORTIKA Project Objectives, challenges & results for end users

- Objectives
  - Cyber security solution for small businesses
  - Security-by-design approach for integration of HW/SW with business needs and behavioural patterns
  - FORTIKA marketplace ecosystem for provision of virtualised security services



- Challenges and results for end users
  - minimize the exposure of SMEs to cyber security risks and threats
  - help SMEs to successfully respond to cyber security incidents
  - cyber-security solution through hardware-enabled middleware security layer
  - encourage security friendly behavioural and organizational changes

FORTIKA Project next steps & collaboration opportunities

- To provide a first version of the core security components
- Development of the FORTIKA marketplace
- Evaluation of the solution through five major types of SMEs (support from 2 local SME/ICT clusters and 1 EU alliance)

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Ioannis Komnios, EXUS Software Ltd

KONFIDO

Secure and Trusted Paradigm for Interoperable eHealth Services

KONFIDO Project Objectives, challenges & results for end users

- Enhancement of trust and security in interoperable eHealth services
- Cross-border exchange of Patient Summary and ePrescription
- Holistic secure solution (storage, dissemination, processing and presentation layers)
- Intel SGX security extension
- Blockchain-based logging and consent management Homomorphic encryption
- Photonic encryption key generation
- Security Information and Event Monitoring (SIEM) eIDAS compliant eID

KONFIDO Project next steps & collaboration opportunities

- First component prototypes (May 2018)
- First integrated prototype (October 2018)
- First pilots in Italy, Spain and Denmark (November-December 2018)

- Collaboration opportunities
  - One of the six KONFIDO technology pillars
  - eHealth data exchanges

MITIGATE: a Dynamic Risk Management System for protecting SCS from cyber-criminal activities

MITIGATE Consortium

Fraunhofer
CML

UNIVERSITY OF PIRAEUS
RESEARCH CENTER

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

EUROPHAR

SingularLogic
Innovation at your doorstep

GRUPPO
Maggioli

FEPORTS
Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana

University of Brighton

IMSSEA
IMO

ΟΛΠ
ΟΡΓΑΝΙΣΜΟΣ
ΛΙΜΕΝΟΣ
ΠΕΙΡΑΙΩΣ

FUNDACIÓN
valenciaport

dbh
dbh Logistics IT AG

PORT OF RAVENNA
AUTHORITY

Autorità portuale Livorno

Hansestadt
Bremisches
Hafenamt

MITIGATE

The MITIGATE Research EU Project

MITIGATE stands for **M**ultidimensional, **I**ntegra**T**ed, r**I**sk assessment framework and dynamic, collaborative risk mana**G**ement tools for critical information infr**A**strucTrur**E**s and is a collaborative research project co-funded by the European Commissions under its Research and Innovation program Horizon 2020.

MITIGATE Official website

http://www.mitigateproject.eu/

MITIGATE system

http://mitigate.euprojects.net

A Supply Chain Service (SCS) is . . .

a complex network of interconnected business partners, including all the information, processes and assets required for the movement of goods and the performance of services.

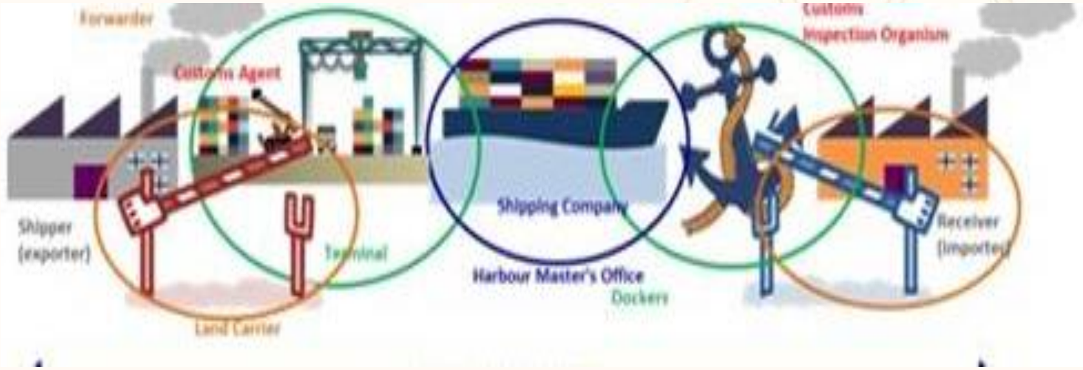
Maritime transport is . . .

the backbone of international trade and a key engine driving globalization: **around 80 per cent (80%) of global trade** *by volume* and over **70 per cent (70%)** *by value* is carried by **sea** and **is handled by ports worldwide**[1]

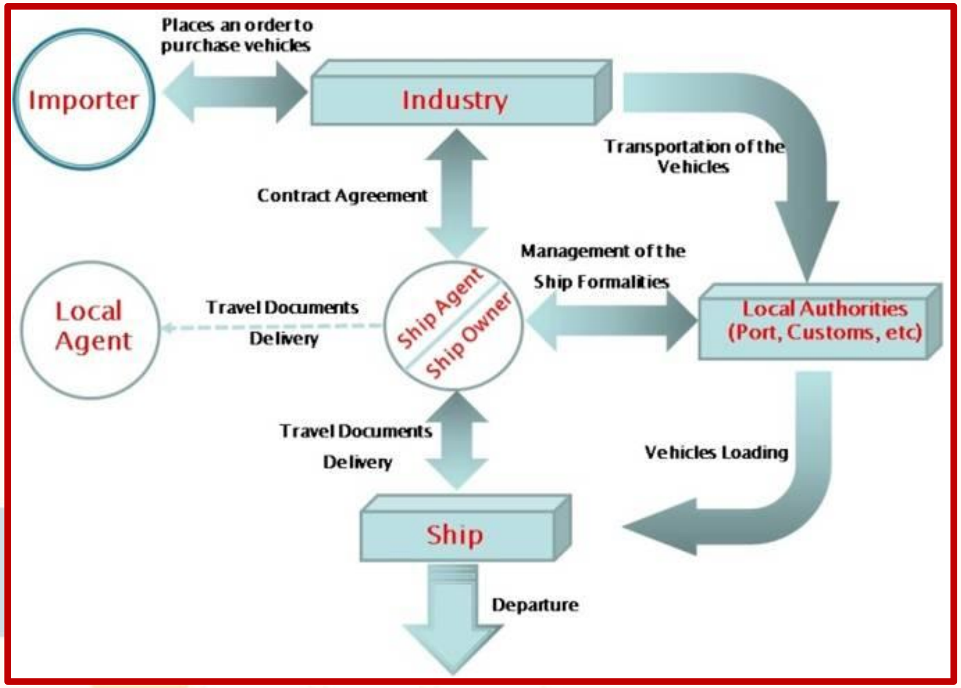
[1] according to the United Nations Conference on Trade and Development (UNCTAD2012) http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1374

Typical SCSs in Maritime Industry

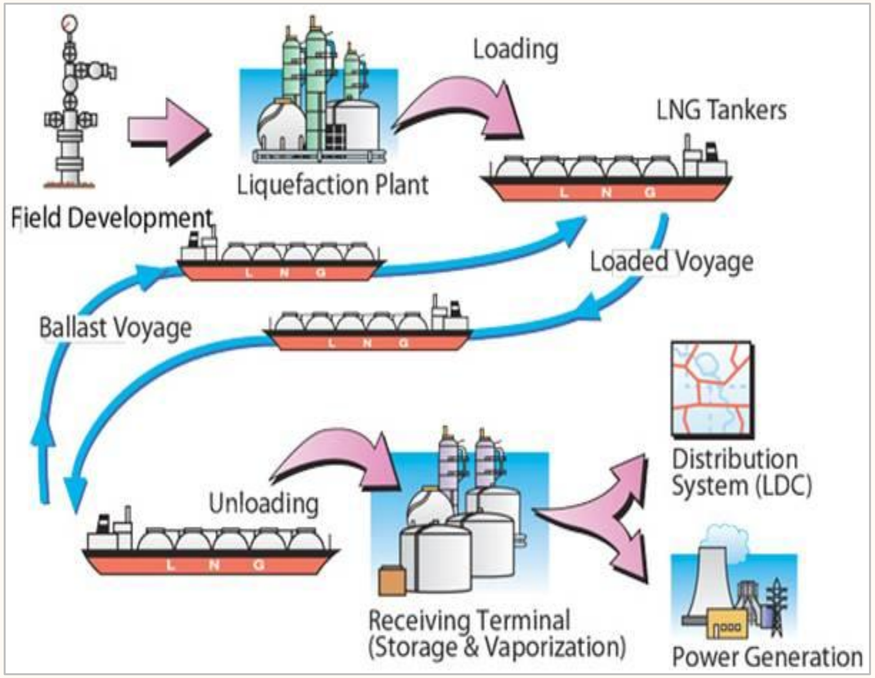
SCS 1 : Container Cargo Management



SCS 2 : Vehicle Transport Service


Importer
Places an order to purchase vehicles
Industry
Transportation of the Vehicles
Contract Agreement
Management of the Ship Formalities
Local Agent
Travel Documents Delivery
Ship Agent
Ship Owner
Local Authorities (Port, Customs, etc)
Travel Documents Delivery
Vehicles Loading
Ship
Departure

SCS 3 : LNG Transport Service



cyberwatching.eu
The European watch on cybersecurity & privacy

Interruptions

The smooth operation of Supply Chain Services (SCS) could suffer from interruptions and delays due to

- ✓ **business and financial factors**

  (e.g. frequent change in business partners leadership, demand uncertainty)
- ✓ the **exploitation of physical threats** (e.g. bombing of a storage room)
- ✓ the **exploitation of cyber threats** (e.g. gaining unauthenticated access to an alarm system and changing the alarm settings)

In the modern competitive digital maritime markets, where the provision of a SCS depends more than ever upon interrelated cyber assets (e.g. networks, equipment, software, digital data), internal and external emerging **cyber risks** have become the **main cause of a SCS disruption**.

The estimation of security risks in Maritime & Logistics SCS relies on:

- **the attacker's profile** (e.g. terrorist, disgruntled employee and insider, state or non-state Hacker, hobbyist, hacktivist intruding for political reason)
- **the prominent cyber-attack vectors** (e.g on the communication stack, hardware, software, UDP port, application layer)
- **the causes of vulnerabilities** (e.g misconfiguration of the wireless devices, high level of interdependency among transportation infrastructure systems, deficiencies in security controls as lack of cryptography policies used in industrial communication networks)

Supply Chain security risk assessment methodologies contribute towards the identification of

✓ **the physical and cyber risks** of the supply chains
✓ **the individual business partners** involved

How can we record the prominent business partners that are participating within the Port Supply Chain Service?

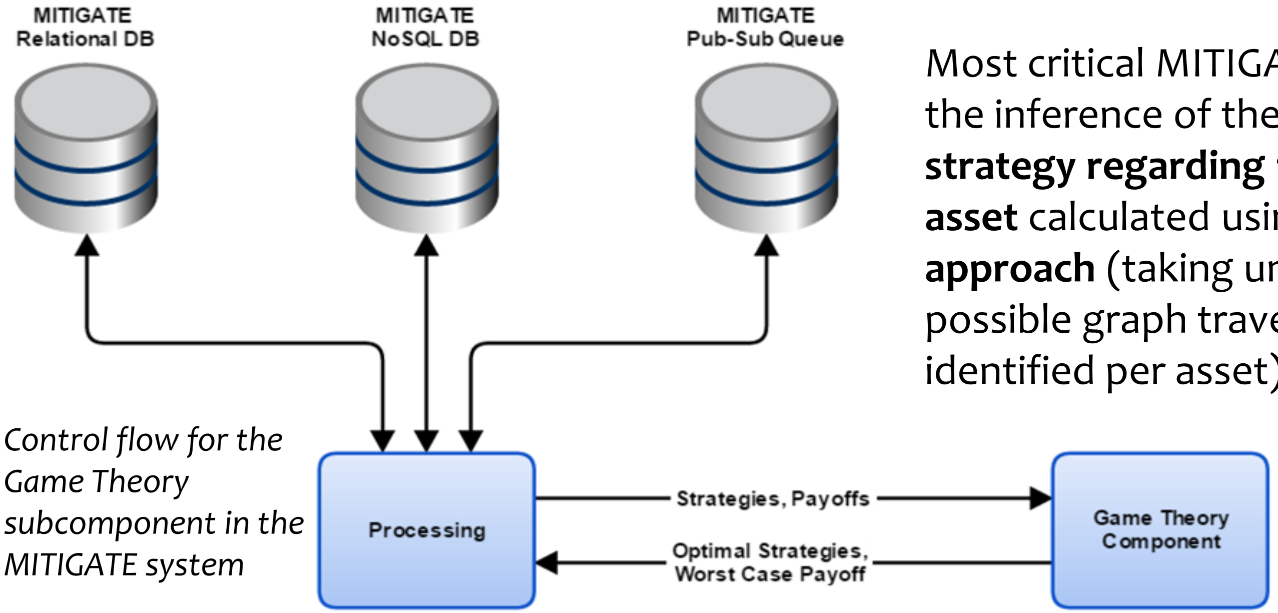
How can we visualize the physical and cyber risks lurking in Port Information Infrastructures ?

The main goal of MITIGATE is

to **realize a radical shift in risk management methodologies for the maritime sector** towards a collaborative **evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA) approach** that alleviates the limitations of state-of-the-art risk management frameworks.

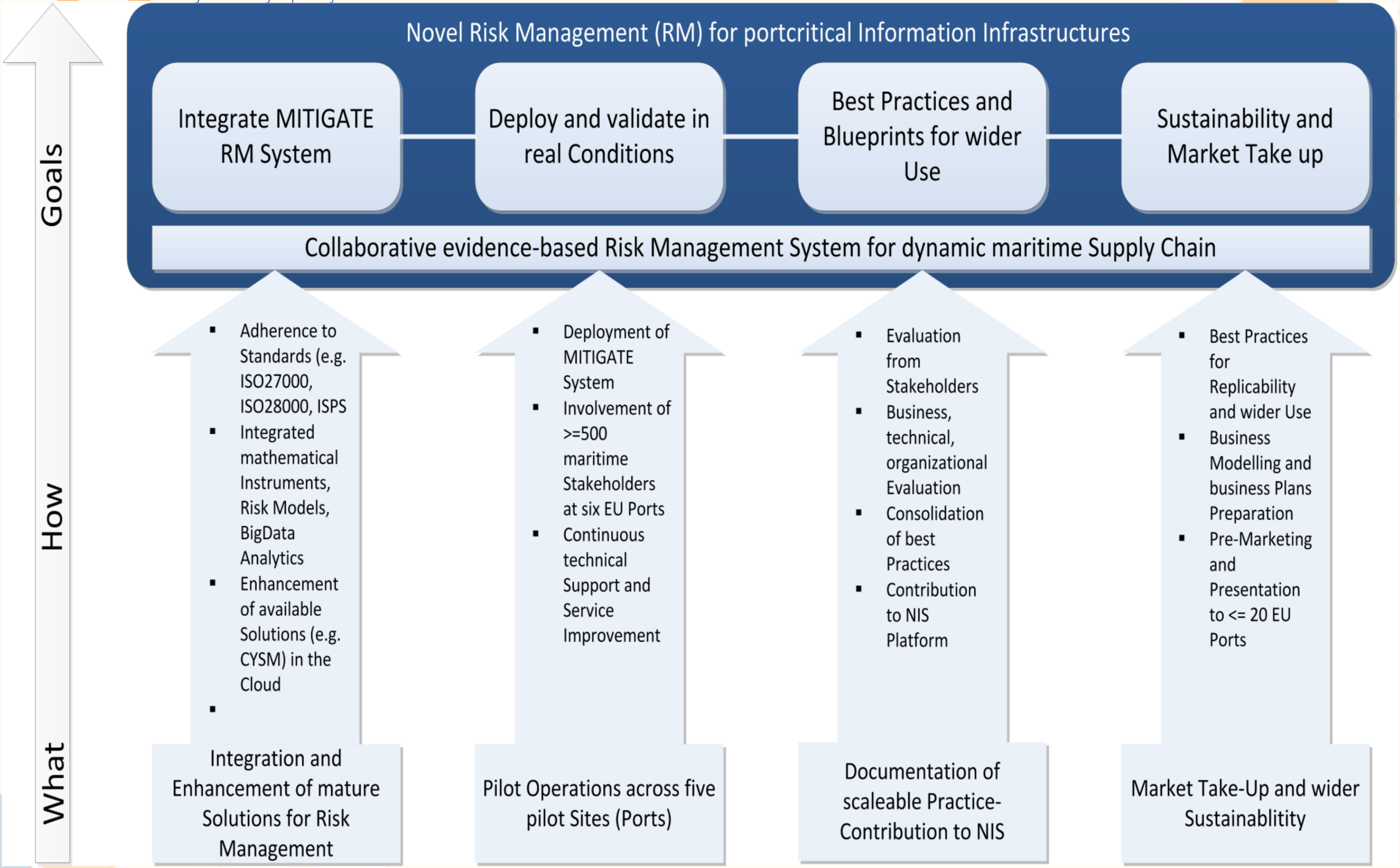
The *Mitigate system is*

an effective, collaborative, standards-based risk management (RM) system for ports' Critical Information Infrastructures (CIIs), considering all the threats arising from the supply chain, including threats associated with port CIIs interdependencies and associated cascading effects.



Control flow for the Game Theory subcomponent in the MITIGATE system

Most critical MITIGATE system functionality: the inference of the **optimal defensive strategy regarding the protection of one asset** calculated using a **game theoretic approach** (taking under consideration all the possible graph traversals and vulnerabilities identified per asset).



Novel Risk Management (RM) for portcritical Information Infrastructures

Goals

Integrate MITIGATE RM System

Deploy and validate in real Conditions

Best Practices and Blueprints for wider Use

Sustainability and Market Take up

Collaborative evidence-based Risk Management System for dynamic maritime Supply Chain

How

- Adherence to Standards (e.g. ISO27000, ISO28000, ISPS
- Integrated mathematical Instruments, Risk Models, BigData Analytics
- Enhancement of available Solutions (e.g. CYSM) in the Cloud
-

- Deployment of MITIGATE System
- Involvement of >=500 maritime Stakeholders at six EU Ports
- Continuous technical Support and Service Improvement

- Evaluation from Stakeholders
- Business, technical, organizational Evaluation
- Consolidation of best Practices
- Contribution to NIS Platform

- Best Practices for Replicability and wider Use
- Business Modelling and business Plans Preparation
- Pre-Marketing and Presentation to <= 20 EU Ports

What

Integration and Enhancement of mature Solutions for Risk Management

Pilot Operations across five pilot Sites (Ports)

Documentation of scaleable Practice-Contribution to NIS

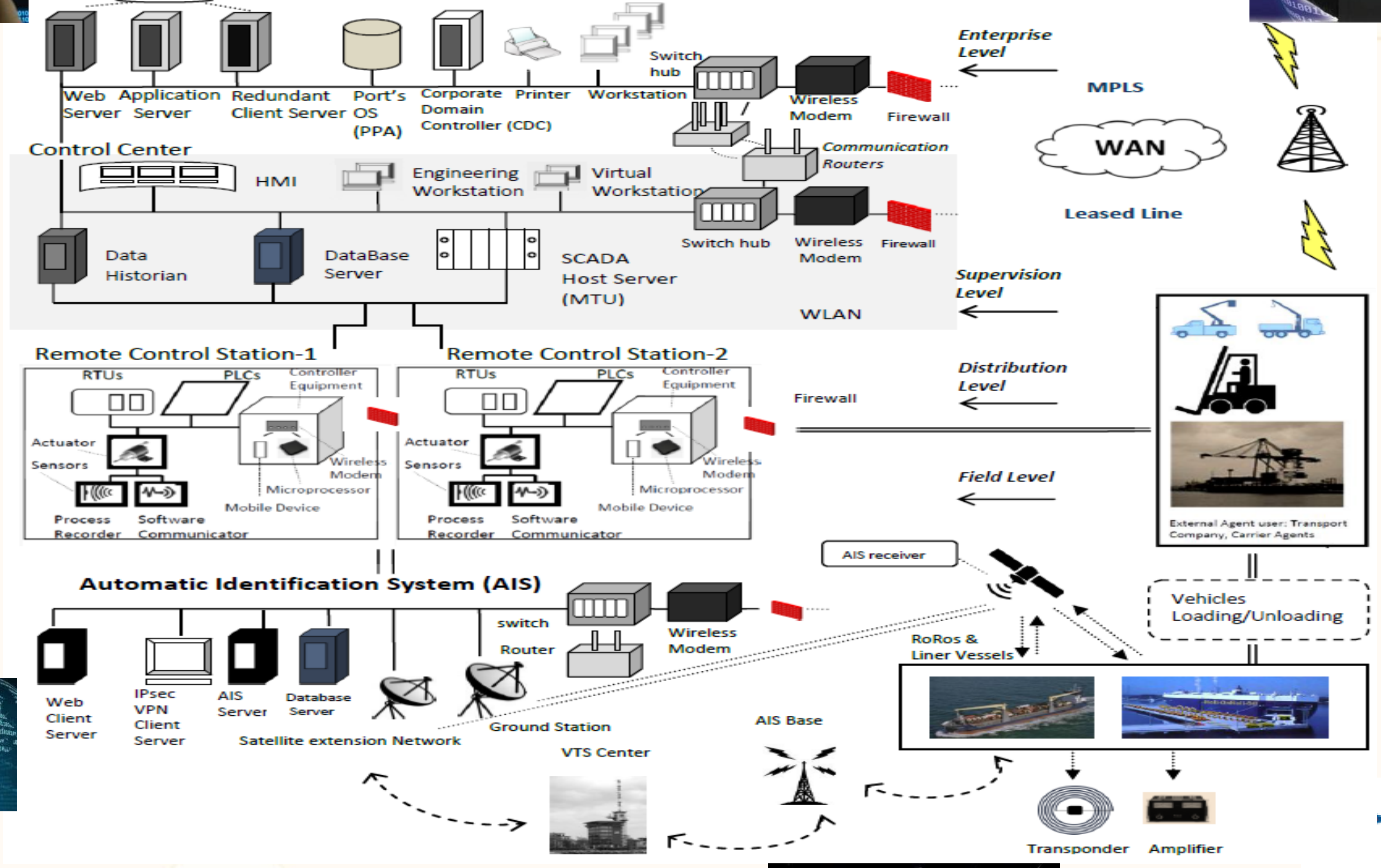
Market Take-Up and wider Sustainablitity

cyberwatching.eu
The European watch
on cybersecurity & privacy

ICT Maritime Supply Chai

SCADA system

Port Authority



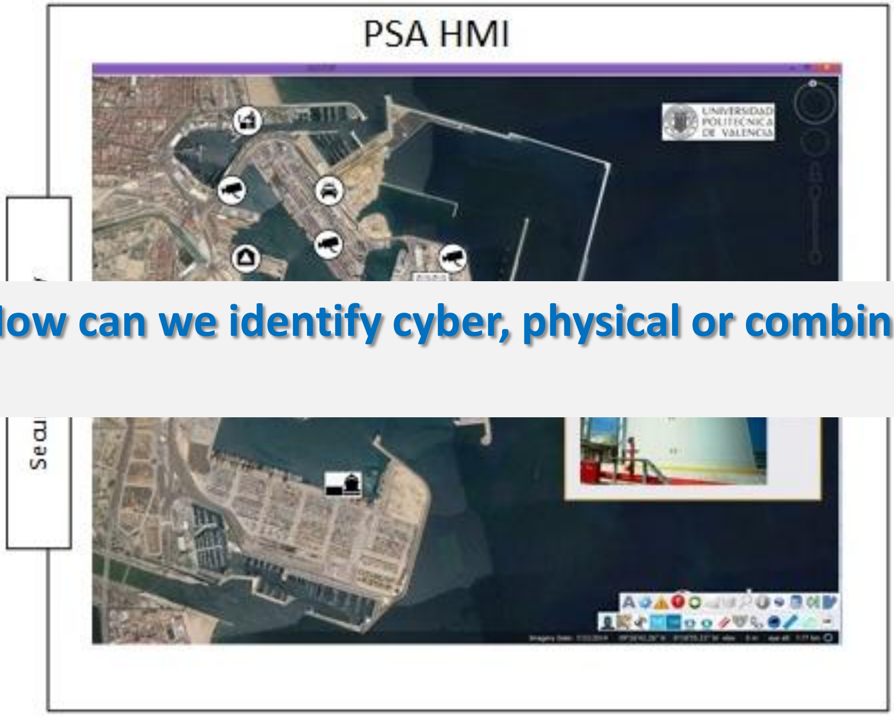
Vehicle Transport Service (VTS) SCS

MITIGATE

Future research & objectives

cyberwatching.eu
The European watch
on cybersecurity & privacy

Commercial Ports



QUESTION D: How can we identify cyber, physical or combined threats???

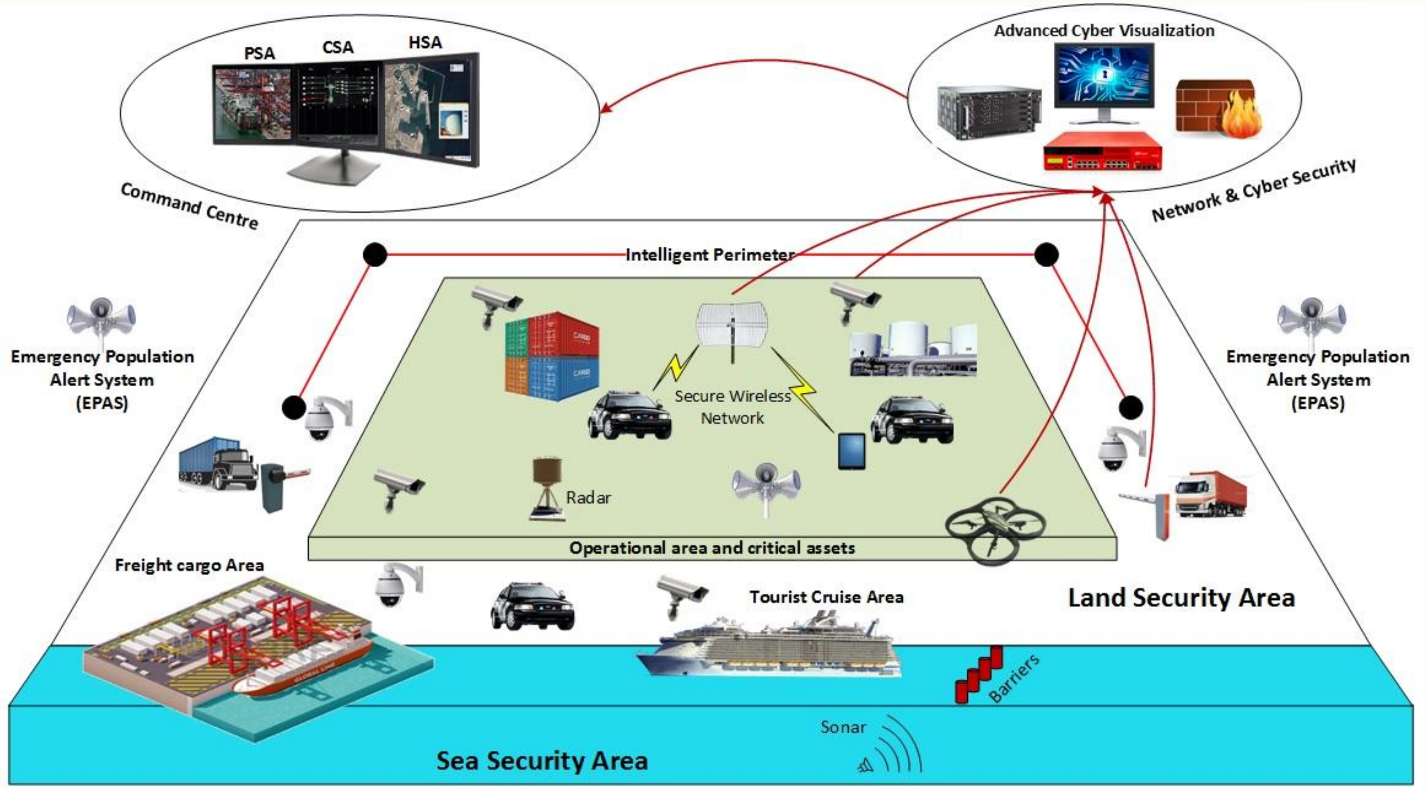
Sauron

SAURON :Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports

The vision of SAURON is to provide a multidimensional yet installation-specific **Situational Awareness platform** to help port operators anticipate and withstand potential **cyber, physical or combined threats** to their freight and cargo business and to the safety of their employees, visitors, passengers and citizens in the vicinity.

Sauron

- Spanish Army Friendly Force Tracking (FFT) system.
- Intrusions and Anomalies Detection Systems
- Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE Methodology)
- MEDUSA Supply Chain Risk Assessment Methodology
- CYSM: Collaborative Cyber-Physical Security Management System



cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Dr. Ioannis CHOCHLIOUROS

Head of Research Programs Section, OTE, Greece

MY DATA PRIVACY FLAG

Privacy Flag Project

Objectives and challenges

Objectives

- **Privacy Flag (PF) combines crowdsourcing, ICT technology and legal expertise to protect citizen privacy** *when visiting websites, using smart-phone applications, or living in a smart city*, by leveraging user-friendly solutions provided as a smart-phone application, a web-browser add-on and a public website.
- It develops a **highly scalable privacy monitoring and protection solution** as well as a **global knowledge database of identified privacy risks**, together with **online services** to support companies and other stakeholders in becoming privacy-friendly.
- Furthermore, it **collaborates with standardization bodies** and it **disseminates towards the public and specialized communities** (such as ICT lawyers, policy makers and academics).

Challenges

Provision of a new paradigm of privacy risk assessment, combining:

- A crowdsourcing model of risk identification and evaluation;
- a Universal Privacy Risk Area Assessment Methodology (UPRAAM) tool;
- Distributed agents to monitor, assess and inform on the privacy risk level of any application;
- Full “anonymization” and privacy technology for server connection;
- Legal expertise in privacy and personal data protection;
- Personal data valuation mechanism;
- A voluntary legal binding mechanism for companies located outside of Europe.

Privacy Flag Project
Results for end-users

- **Three user-friendly and freely available tools for citizens**, including an Android application, an add-on for their Internet browsers (both enabling users to monitor/identify threats on their privacy) and a public website.
- **Distributed crowdsourcing privacy monitoring platform,** enabling the crowd to mutualize their efforts and resources by running a local application.
- **Universal Privacy Risk Area Assessment tool and Methodology** (UPRAAM) for evaluating the level of risk on privacy and personal data protection, “matching” the European and international norms/standards.
- **Privacy enablers** integrated into the application and browser add-on for privacy risk assessment and traffic analysis/protection.
- **Global knowledge database on privacy risks** indexing websites, smartphone applications and IoT deployments, fed by the crowd (applying the UPRAAM), by alerts received.
- **Voluntary Compliance Commitment tool (VCCT)** enabling any company or public administration to formally and publicly commit/abide to respect the European standards, even if located outside of Europe.
- **On-line resources** to improve privacy.
- **In-depth privacy risk analysis on-line tool** for experts**.**
- **Labelling and certification process** proposed to companies with solutions fully compliant with the privacy requirements.
- **Standard on privacy labelling** by exploring the possibility to cooperate with the ESOs.

Privacy Flag Project
Next steps & collaboration opportunities

- **Privacy Flag has already developed and tested a platform providing several user-friendly and freely available tools to the citizens to be accessed as:**
  - an add-on in their Internet browsers;
  - an Android application on their smart-phone;
  - a public website.
- **Further actions aim to extend the applicability of those tools and promote their usage in a wider framework**, accessing more end-users and potentially offering updates/enhancements, where relevant.
- In addition, **Privacy Flag has developed a Voluntary Compliance Commitment Tool (VCCT) enabling any company or public administration to formally and publicly commit and abide to respect the European standards, even if located outside of Europe**. *This will remain active*.
- **A legal entity has been formulated within the Privacy Flag consortium aiming to support the long-term maintenance and exploitation of the platform.**

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Claudia Diaz (KU Leuven)

Panoramix

Project Objectives, challenges & results for end users

- Building a Mix-Net Infrastructure for Europe, by creating a European mix-network open-source codebase and infrastructure.
- Use cases
  - e-Voting
  - Privacy-preserving data collection for processing in the cloud
  - Privacy-preserving e-mail messaging

Project next steps & collaboration opportunities

- Make the deployable mixnet framework publicly available
- Further building an open source development community around the Panoramix framework
- Exploring options for financial sustainability of the code and framework

ReCRED

From **Re**al-world Identities to
Privacy-preserving and Attribute-based
CREDentials for Device-centric Access Control

Concertation Meeting @Cyberwatching.eu

Brussels, April 26

Bharadwaj Pulugundla, MBA

Manager Digital Innovation,

Verizon Enterprise Solutions

ReCRED Consortium

- Project funded by EU under H2020
- Call Identifier: H2020-DS2-2014-1

European Commission

HORIZON 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Telefónica
Telefónica I+D

wedia

EXUS®

THE PRODUCTIZERS

verizon

cnit

UNIVERSIDAD CARLOS III DE MADRID

institute imdea networks

upcom
Bringing business and IT together

certSIGN® BY UTI

BAKER & MCKENZIE

www.recred.eu

ReCRED Context

8.5 billion Mobile connections

5.09 billion unique subscribers

$1.06trillion Revenue/year

8.4 billion Connected "Things" Will Be in Use in 2017*

81%of confirmed data breaches involved leveraging weak, default or stolen passwords.

2017 Data Breach Investigations Report

Executive Summary

verizon

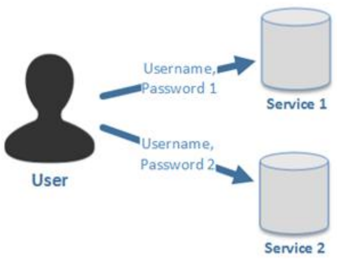
Source: https://www.gsmaintelligence.com/

**Gartner*

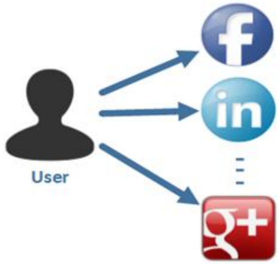
ReCRED’s goal

- To promote the **user’s personal mobile device** to the role of a unified **authentication** and **authorization proxy** towards the digital world.

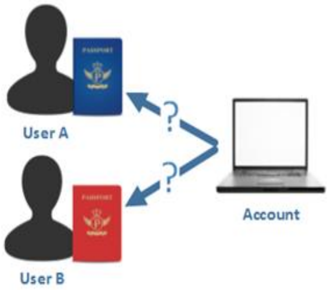
1. Password overload



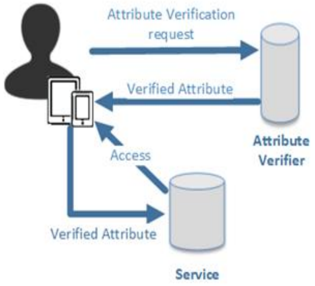
2. Identity Fragmentation



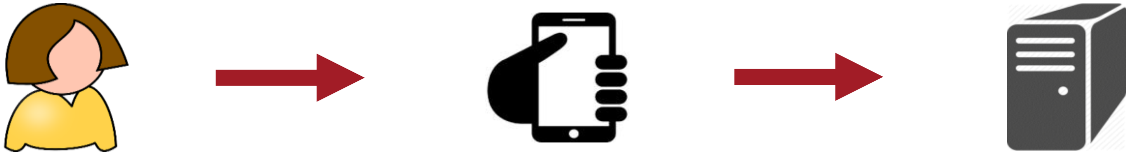
3. Lack of real-world binding



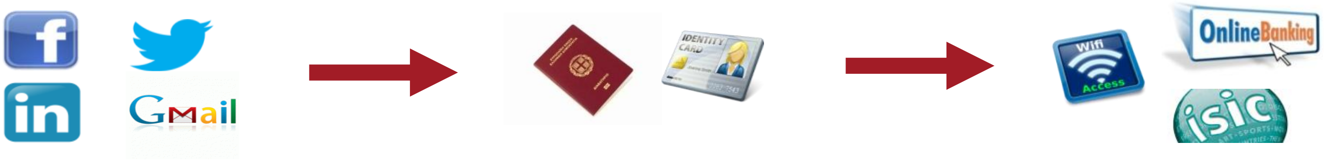
4. Lack of support for Attribute based access contol



ReCRED concepts



- User to Device & Device to Service authentication



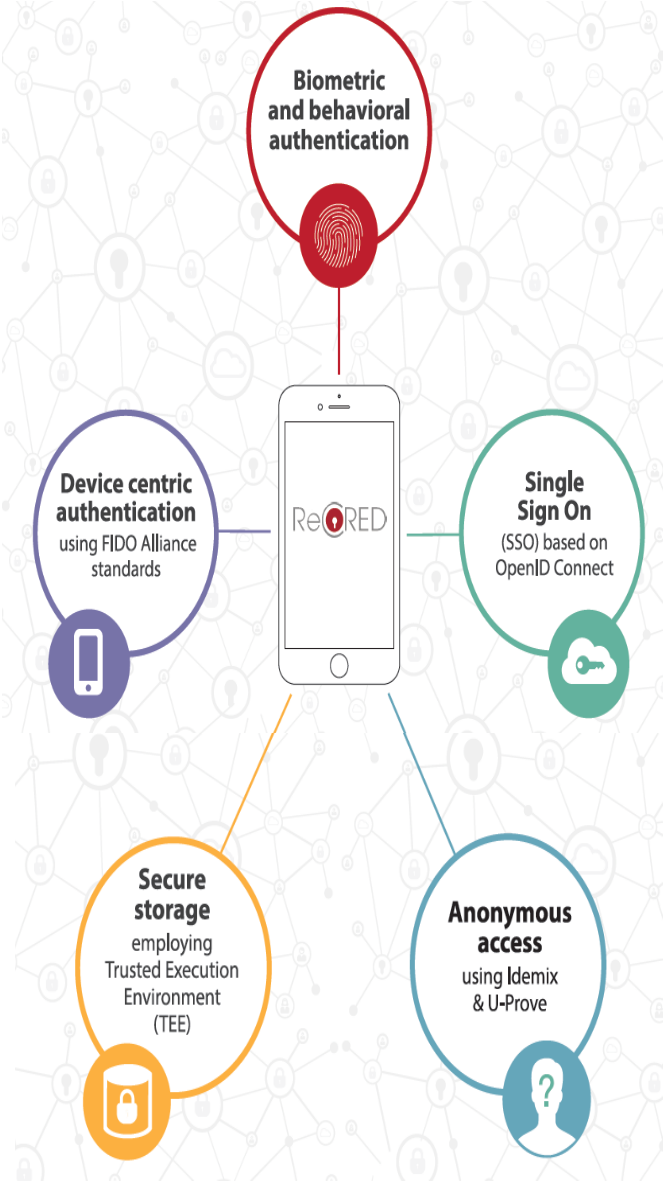
Binding digital Identity with Real-world Identities

R 18+
RESTRICTED
Restricted to 18 and over

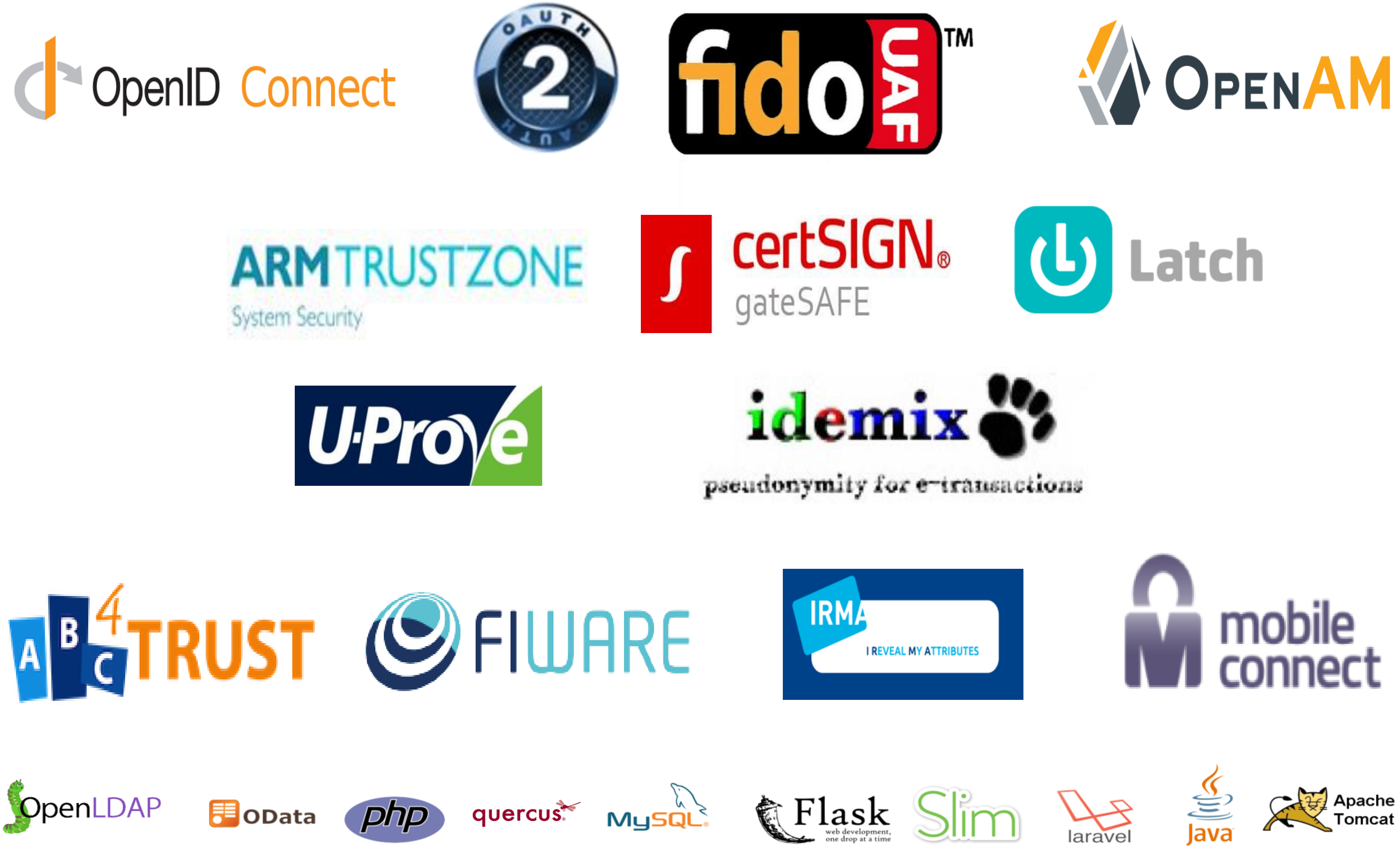
Account less access through verified identity attributes

(eg. Age, location etc)

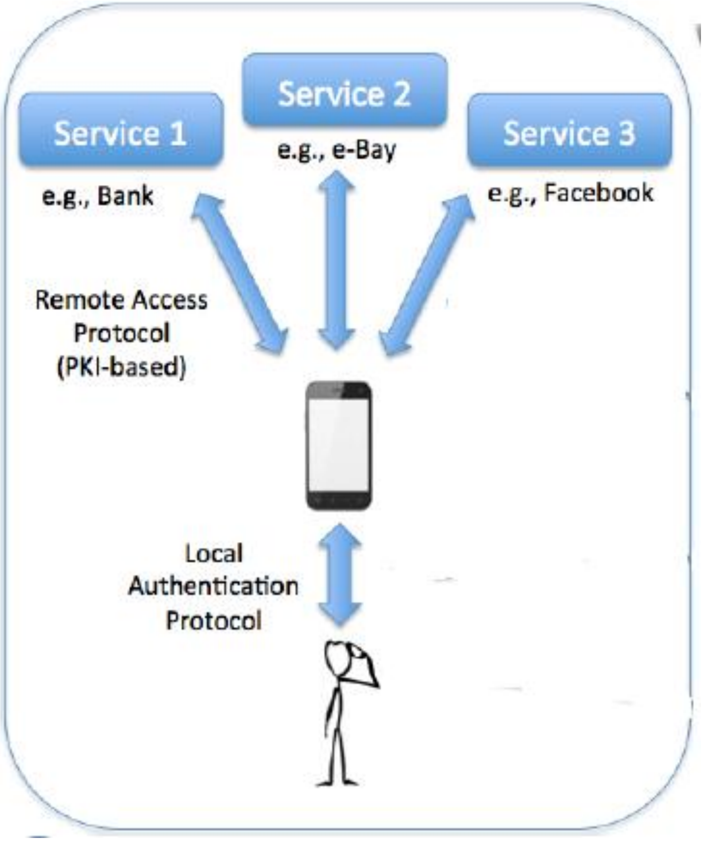
ReCRED reference Architecture

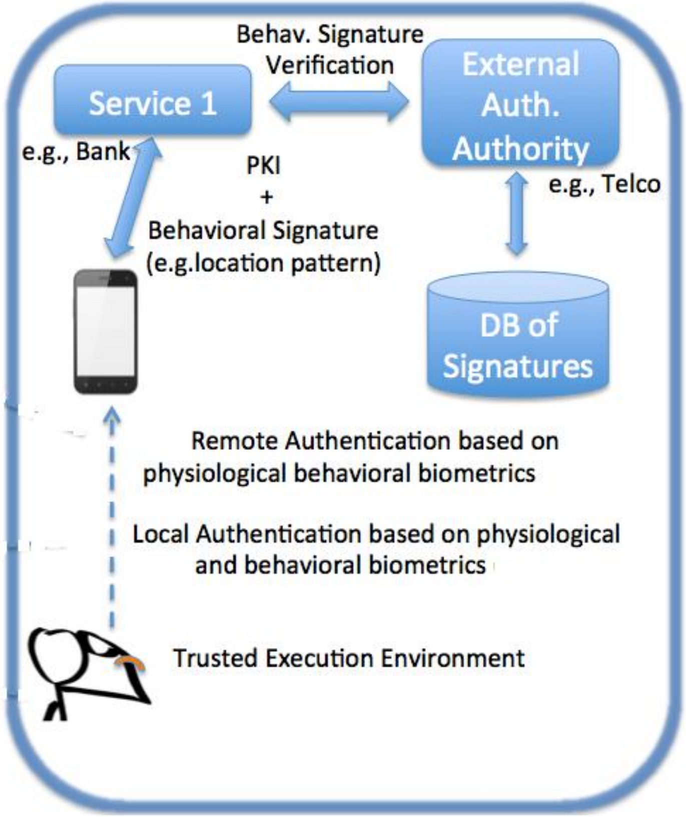

Biometric and behavioral authentication
ReCRED
Device centric authentication using FIDO Alliance standards
Single Sign On (SSO) based on OpenID Connect
Secure storage employing Trusted Execution Environment (TEE)
Anonymous access using Idemix & U-Prove

ReCRED's adopted Technologies and Standards



ReCRED's adoption of FIDO




Behav. Signature
Verification
Service 1
External
Auth.
Authority
e.g., Bank
PKI
+
Behavioral Signature
(e.g.location pattern)
e.g., Telco
DB of
Signatures
Remote Authentication based on
physiological behavioral biometrics
Local Authentication based on physiological
and behavioral biometrics
Trusted Execution Environment

infineon AMERICAN EXPRESS ARM Google Bank of America intel

PayPal SAMSUNG VISA MasterCard Lenovo

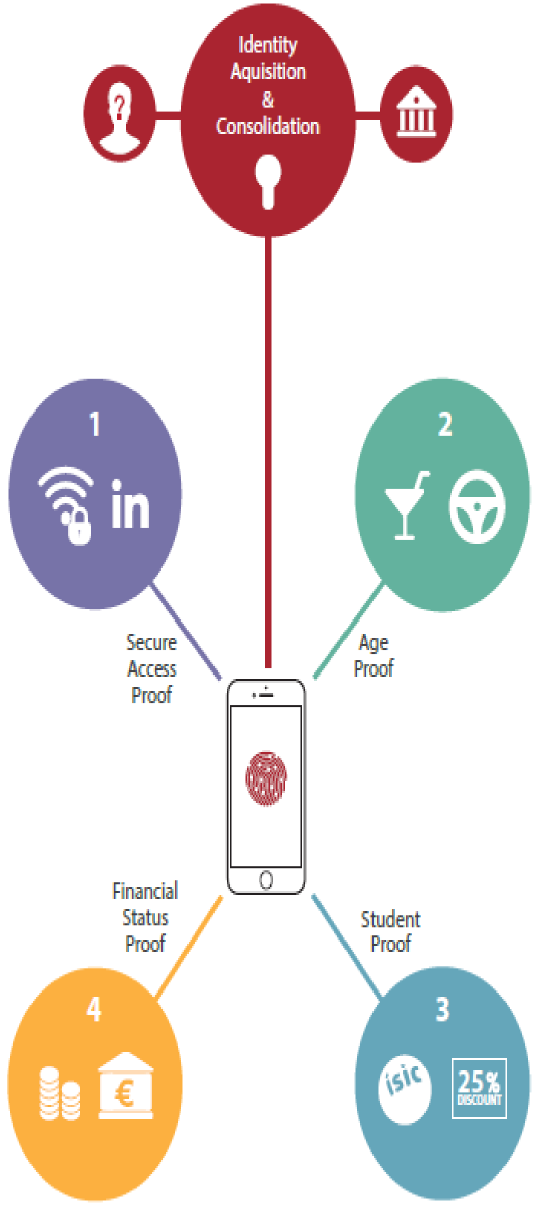
ReCRED Pilot Use Cases

Pilot 1: Device-centric campus WiFi and web services access control

Pilot 2: Student authentication and offers

Pilot 3: Attribute-based age verification online gateway

Pilot 4: Financial services – microloan origination



ReCRED's Innovation

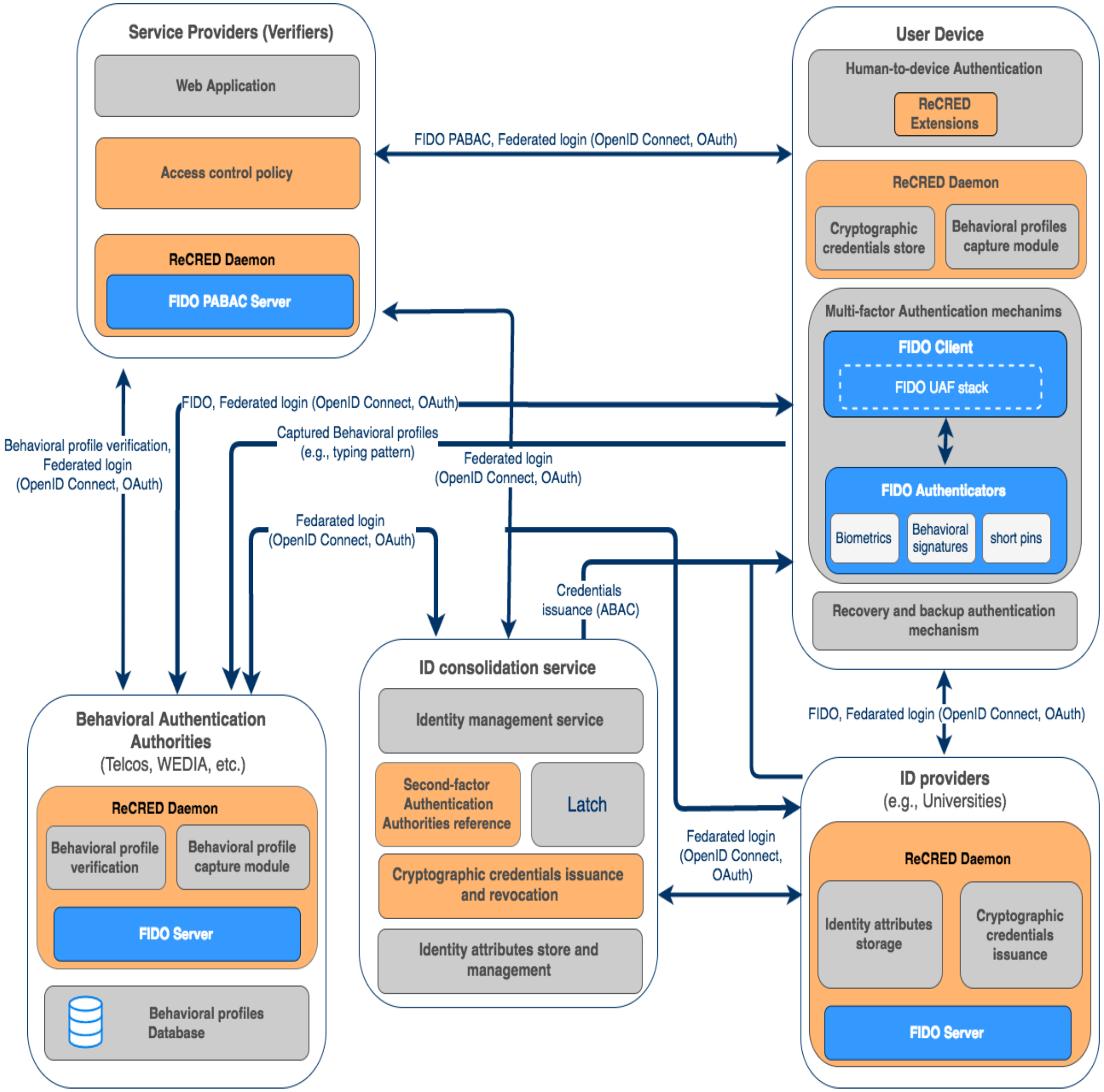
1. Device-centric Authentication, Password-less experience, FIDO UAF
2. Fine-grained control of identity attributes to be revealed (ABAC)
3. FIDO + OpenID Connect Integration
4. Support for privacy-preserving ABAC (Idemix, U-Prove, CP-ABE)
5. Biometrics and behavioral authentication
6. Single Sign On (SSO) with federated identities
7. Enhanced security & privacy by employing the crypto functions and secure storage of TEE
8. Unlinkability & untraceability

Where to find more information

- www.recred.eu
- **Linkedin::** ReCRED - H2020
- **Facebook:**https://web.facebook.com/ReCRED-393935714133064/
- **Twitter:** @ReCRED_H2020
- DBIR REPORT: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Thank you.

ReCRED reference Architecture


Service Providers (Verifiers)
Web Application
Access control policy
ReCRED Daemon
FIDO PABAC Server
FIDO PABAC, Federated login (OpenID Connect, OAuth)
User Device
Human-to-device Authentication
ReCRED Extensions
ReCRED Daemon
Cryptographic credentials store
Behavioral profiles capture module
Multi-factor Authentication mechanims
FIDO Client
FIDO UAF stack
FIDO Authenticators
Biometrics
Behavioral signatures
short pins
Recovery and backup authentication mechanism
FIDO, Federated login (OpenID Connect, OAuth)
Captured Behavioral profiles (e.g., typing pattern)
Federated login (OpenID Connect, OAuth)
Behavioral profile verification, Federated login (OpenID Connect, OAuth)
Fedarated login (OpenID Connect, OAuth)
Credentials issuance (ABAC)
ID consolidation service
Identity management service
Second-factor Authentication Authorities reference
Latch
Cryptographic credentials issuance and revocation
Identity attributes store and management
Behavioral Authentication Authorities (Telcos, WEDIA, etc.)
ReCRED Daemon
Behavioral profile verification
Behavioral profile capture module
FIDO Server
Behavioral profiles Database
FIDO, Fedarated login (OpenID Connect, OAuth)
ID providers (e.g., Universities)
Fedarated login (OpenID Connect, OAuth)
ReCRED Daemon
Identity attributes storage
Cryptographic credentials issuance
FIDO Server

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Marco Steger (Virtual Vehicle)

Secure COnnect Trustable Things – SCOTT

SCOTT
Secure Connected Trustable Things

SCOTT: Objectives, Challenges & Results

- **Create trust in wireless solutions,** by
  - Increasing their **social acceptance**
  - Bring out the **full potential of the IoT**
- **Security, Safety, Privacy & Trustability**
  - Trustable Connected Things: **Trust Framework**
  - **Security Classes –** Measureable security & privacy
  - Privacy in IoT: applicability of **Privacy Labels**
  - **Security and Privacy** in system design processes

SCOTT: Next steps & collaborations

- Apply **Trust Framework** in 6 industrial domains
  - Trust Assessment -> Trust Assurance
- Apply **Security Classes** and **Privacy Labels** in multi-domain, technical use cases
- Collaborations
  - AIOTI, Partnering Trust, Zeker Online
  - Standardisation: ISO 26262, 3GPP, 5G PPP, etc.
  - <u>Open for collaboration with other initiatives!</u>

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Marco Steger (Virtual Vehicle)

marco.steger@v2c2.at

SCOTT

Secure Connected Trustable Things

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Xabier Larrucea

SHIELD

SHIELD Project Objectives, challenges & results for end users

SHiELD aims to create an **open and extendable security architecture** (OpenNCP) supported by **security mechanisms** and **privacy by design modelling and analysis tools** to provide systematic protection for the **storage and exchange** of health data across European borders, subject to control by the data subjects, compatible with **existing regulatory frameworks**, ensuring the **privacy, availability and correctness of the data** while improving trust of patients in the security of their data and its use to address their needs.

SHIELD Project Objectives, challenges & results for end users

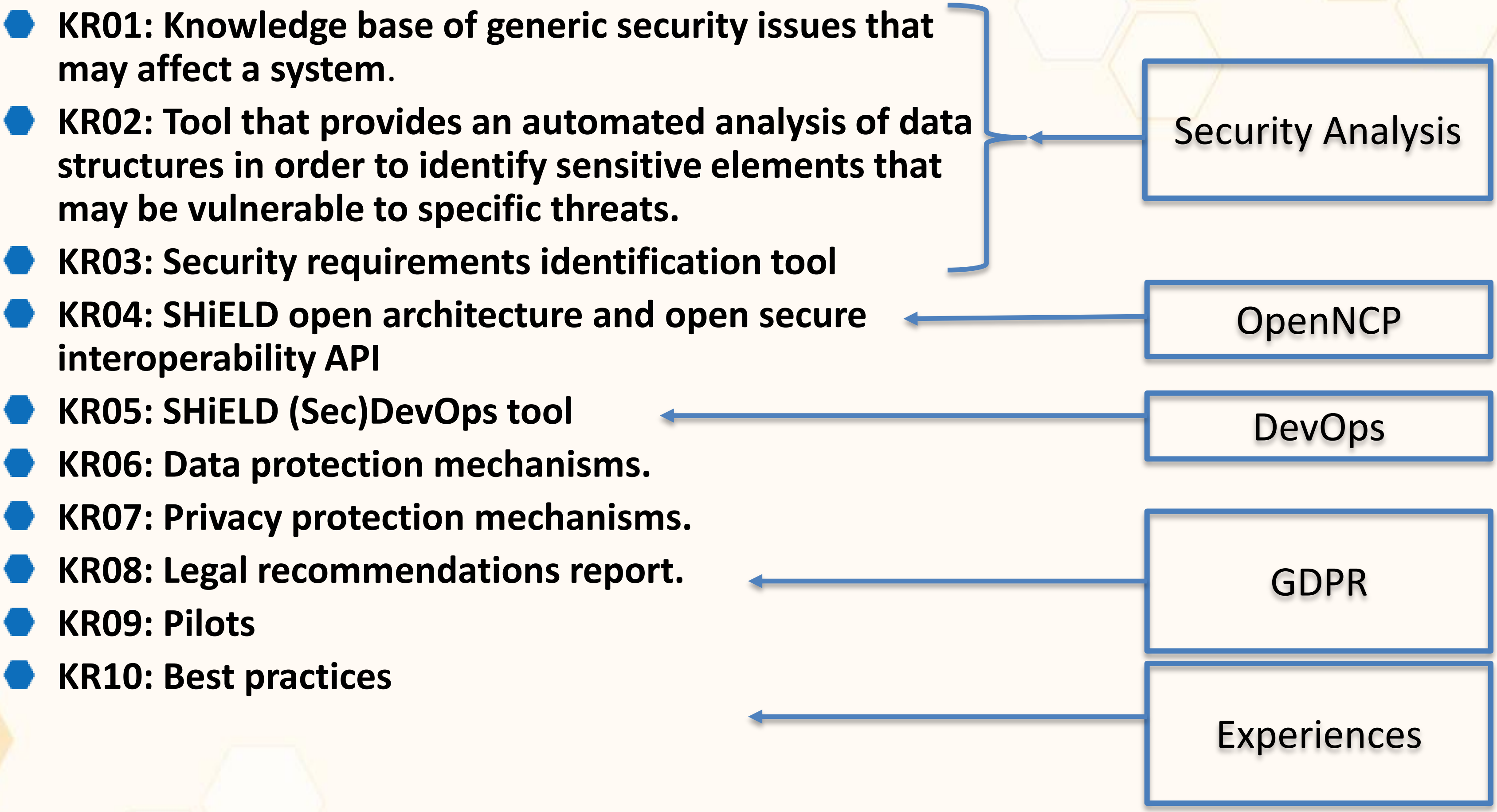
- **O1) Systematic protection of health data against threats and cyber-attacks**.
  - **KR01: Knowledge base of generic security issues that may affect a system**.
  - **KR02: Tool that provides an automated analysis of data structures in order to identify sensitive elements that may be vulnerable to specific threats.**
  - **KR03: Security requirements identification tool**
- **(O2) Definition of a common architecture for secure exchange of health data across European borders.**
  - **KR04: SHiELD open architecture and open secure interoperability API**
  - **KR05: SHiELD (Sec)DevOps tool**
- **(O3) Assurance of the protection and privacy of the health data exchange.**
  - **KR06: Data protection mechanisms.**
  - **KR07: Privacy protection mechanisms.**

SHIELD Project Objectives, challenges & results for end users

- (O4) To understand the legal/regulatory requirements in each member state, which are only partly aligned by previous EU directives and regulations and provide recommendations to regulators for the development of new/improved regulations.
  - KR08: Legal recommendations report.
- (O5) Validation of SHiELD in different pilots across three Member States
  - KR09: Pilots
  - KR10: Best practices

SHIELD Project next steps & collaboration opportunities

- Collaborations:



- KR01: Knowledge base of generic security issues that may affect a system.
- KR02: Tool that provides an automated analysis of data structures in order to identify sensitive elements that may be vulnerable to specific threats.
- KR03: Security requirements identification tool
- KR04: SHiELD open architecture and open secure interoperability API
- KR05: SHiELD (Sec)DevOps tool
- KR06: Data protection mechanisms.
- KR07: Privacy protection mechanisms.
- KR08: Legal recommendations report.
- KR09: Pilots
- KR10: Best practices

SHIELD Project next steps & collaboration opportunities

- Collaborations:
  - Cyber security challenges applied to eHealth
  - Cyber Threats
  - Audits
  - Security Analysis
  - Conferences

cyberwatching.eu

The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Rodrigo Diaz Rodriguez, rodrigo.diaz@atos.net

SMESEC

SMESEC challenges

SMEs and cybersecurity

68% of SMEs have no systematic approach for ensuring cybersecurity

60% of all cyberattacks and data breaches in 2016 are aimed to SMEs

40% of SMEs would struggle to recover from data loss, and 20% would not be able to

SMESEC objectives

Define cybersecurity guidelines

Cybersecurity recommendations

Discover threats and vulnerabilities

Solve cybersecurity issues

Protection using various commercial heterogeneous security products

Provide solutions for the detected threats

Restricted budget

Multiple SME environments

Cybersecurity training activities

Guidelines and recommendations for cybersecurity awareness

SMESEC Project

Current status

Unified architecture

Extending cybersecurity tools with new mechanisms

Developing of the SMESEC Framework initial version

Working in training and awareness plan

Initial pilot deployment

Next steps

Final SMESEC Framework

Cybersecurity tools enhanced for special needs of SMEs

Complete plan for training and awareness (together with cloud support)

Final deployment of the SMESEC Framework in the pilots

Open call for SMEs for evaluating SMESEC

Joint exploitation

SMESEC collaboration opportunities

Relevant EU projects:

- FORTIKA (collaboration in ICT'18 networking session and future events)
- WISER/CYBERWISER (collaboration for enhancing SMESEC Framework with external tools)

Other EU research projects with focus in SMEs or technology relevant (e.g. IoT, cloud, BYOD, etc.)

Workshops:

RAID 2018, Heraklion (Greece)

Training sessions:

Collaboration with CIPSEC project to provide a common cybersecurity training approach for SMEs.

Open Call:

Open call for SMEs [TBD]

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Jean-Loup Dépinay

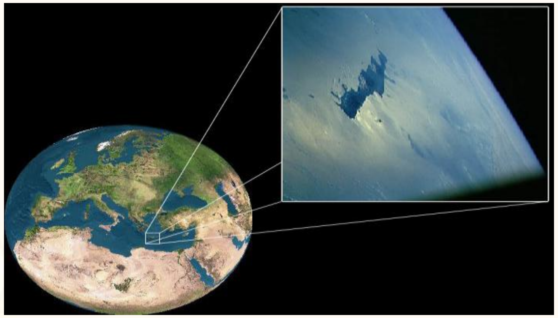
SPEECHXRays

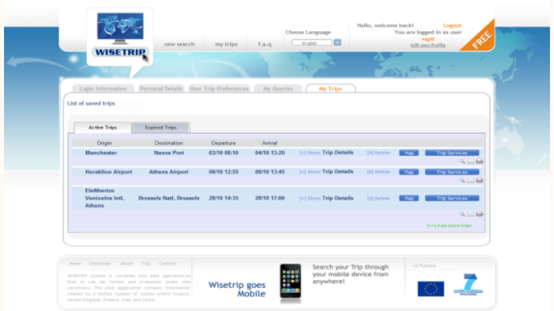
SpeechXRays Project Objectives, challenges & results for end users

- SpeechXRays project will develop and test a user recognition platform based on voice acoustics analysis and audio-visual identity verification in real-life environments.
- Advantages:
  - Security: high accuracy solution, due to the effective combination of speaker recognition, face biometrics and their combination.
  - Privacy: biometric data stored in the device (or in a private cloud under the responsibility of the data subject).
  - Cost-efficiency: use of standard embedded microphone and cameras (smartphones, laptops).

SpeechXRays Project next steps & collaboration opportunities

- ENISA Annual Privacy Forum Barcelona 2018
- EAB Research Projects Conference (EAB-RPC) 2018 Darmstadt
- Workforce Use Case test at IFIN-HH
- eHealth Use Case test at FORTH
- Consumer Use Case Test at FNET



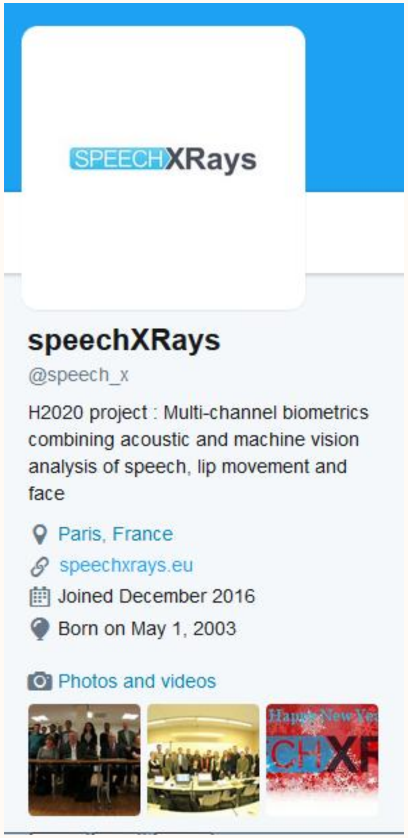


List of saved trips

Origin	Destination	Departure	Arrival				
Manchester	Naxos Port	03/10 08:10	04/10 13:20	[+] Show Trip Details	[X] Delete	Map	Trip Services
Heraklion Airport	Athens Airport	08/10 12:55	08/10 13:45	[+] Show Trip Details	[X] Delete	Map	Trip Services
Eleftherios Venizelos Intl, Athens	Brussels Natl, Brussels	28/10 14:35	28/10 17:00	[+] Show Trip Details	[X] Delete	Map	Trip Services

WISETRIP system is currently into pilot operation,so that it can be tested and evaluated under real conditions. This pilot application contains information related to a limited number of routes within Greece, United Kingdom, Finland, Italy and China.

Search your Trip through your mobile device from anywhere!



speechXRays

@speech_x

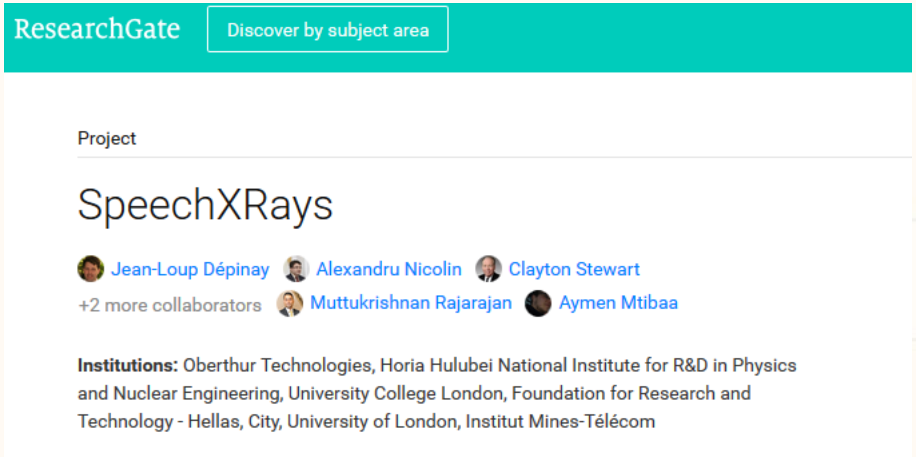
H2020 project : Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face

Paris, France

speechxrays.eu

Joined December 2016

Born on May 1, 2003

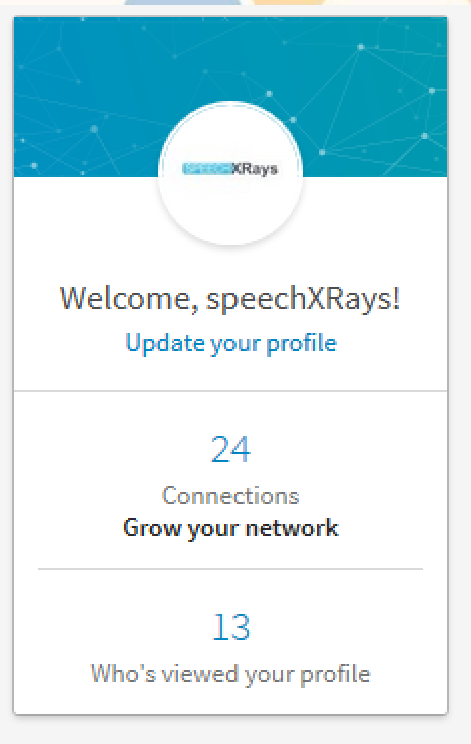


Project

SpeechXRays

Jean-Loup Dépinay, Alexandru Nicolin, Clayton Stewart, +2 more collaborators, Muttukrishnan Rajarajan, Aymen Mtibaa

Institutions: Oberthur Technologies, Horia Hulubei National Institute for R&D in Physics and Nuclear Engineering, University College London, Foundation for Research and Technology - Hellas, City, University of London, Institut Mines-Télécom



Welcome, speechXRays!

Update your profile

24 Connections

Grow your network

13 Who's viewed your profile

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Rodrigo Diaz Rodriguez, rodrigo.diaz@atos.net

YAKSHA

YAKSHA Objectives

- YAKSHA (http://project-yaksha.eu/) aims at reinforcing cooperation and building EU-ASEAN partnerships by developing a cybersecurity solution tailored to specific national needs leveraging EU Know-How and local knowledge.

- The project will enhance cybersecurity readiness levels for its end users, help better prevent cyber-attacks, reduce cyber risks and better govern the whole cybersecurity process. YAKSHA is ideally positioned to help secure the global manufacturing supply chains, given its focus on IoT Security.

YAKSHA Specific Objectives

- To assess the Cyber Security state of the art in the ASEAN area and future developments
- To develop and validate a distributed, flexible, cybersecurity solution
- To enable the sustainable uptake of scientific, technical and economic results and foster cooperation and partnerships between EU-ASEAN

YAKSHA’s Target Groups

SMEs and large organisations

Critical infrastructure organisations

Government organisations

50th
ASEAN
TELMIN 2017
THE 17TH ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING AND RELATED MEETINGS
"ICT Connectedness and Readiness: Towards a Digitally Integrated Community"
30 November – 01 December 2017, Siem Reap, Cambodia

Policy makers

Associations, Network of Organisations and other interested parties incl. media representatives and NGOs

YAKSHA’s Benefit for End-Users

- Provide an automated framework for deploying honeypots and correlating the collected information.
- Enhance cybersecurity readiness levels for its end-users.
- Provide mechanisms to prevent cyber-attacks.
- Reduce cyber risks and better govern the whole cybersecurity process.
- YAKSHA Label of Excellence:
  - European certification of technology excellence and will serve as a sustainable recognition of the product’s qualities.

Project Next Steps

- Co-creation workshops to identify current trends and possible optimal ecosystem to be organised in September 2018 in:

  - Kuala Lumpur, Malaysia
  - Bangkok, Thailand
  - Hanoi, Vietnam
  - Jakarta, Indonesia (to be confirmed)

- The project will develop four versions of software:

  - Prototype (October 2018)
  - Beta Version (February 2019)
  - Release Candidate (August 2019)
  - Final Version (June 2020)

- Data collection methodology and architecture necessary for the YAKSHA pilots
- YAKSHA Ambassadors (Voluntary representatives of the YAKSHA project in the ASEAN countries) Deployment Plan
- Two end-user events focusing on YAKSHA's software promotion:
  - October 2019
  - April 2020

Opportunities to collaborate

- Co-creation workshops in September 2018 (Kuala Lumpur, Hanoi, Bangkok and Jakarta)
- CSM-ACE 2018 (http://www.csm-ace.my/info.html) where one the Co-creation workshop in KL is an official satellite event

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.				