14 December 2020
10.00 AM - 01.30 PM

# CRITICAL CHAINS

## FINANCIAL SECTOR INFRASTRUCTURE CYBER-PHYSICAL SECURITY AND REGULATORY STANDARDS

Cyber Security for Europe

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

CS-AWARE CYBERSECURITY

SOTER

cyberwatching.eu
The European watch on cybersecurity & privacy

# Agenda

## Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

## Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

## Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)

**Topics:**

- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Agenda

**Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm**

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

**Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector**

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

**Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)**

**Topics:**

- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A

Prof. Atta Badii
**Critical-Chains Project Coordinator**
University of Reading

Dr. Alper Kanak
ERARGE

Massimiliano Aschi
Poste Italiane

Kristo Klesment
Guardtime

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Agenda

**Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm**

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

**Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector**

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

**Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)**

**Topics:**

- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A


Karmele Garcia
SOTER Project Coordinator
Everis Spain

David Goodman
Cybersec4Europe
Trust In Digital Life


Laurentiu Vasiliu
CS-AWARE
Peracton Ltd.

Prof. Dr. Paolo Balboni
Cyberwatching
ICT Legal Consulting

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Agenda

**Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm**

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

**Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector**

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

**Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)**

**Topics:**

- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A

Ramon Martin De Pozuelo Genis
CONCORDIA representative partner
CaixaBank

Giorgio Carbone
Stakeholder community representative
Ub technologies

Martin Griesbacher
SOTER representative partner
RISE

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Agenda

## Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

## Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

## Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)

**Topics:**

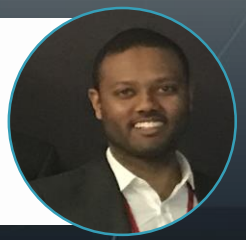
- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A


Prof. Atta Badii
**Critical-Chains Project Coordinator**
University of Reading



Ivan Tesfai
**Critical-Chains Dissemination manager**
RINA


This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm

CRITICAL CHAINS

**Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm**

**Moderator:**

- **Ivan Tesfai** *RINA*

**Topics:**

- **Authentication & Accountability Models** in Financial Flows
- **eiDAS- Compliant Authenticated Access** to the Critical-Chains Framework using the National Digital Identity (SPID),
- Fintech **Cloud Environment Trust & Security** Challenges

Poll / Q&A

Atta Badii, Critical-Chains project coordinator, University of Reading

University of Reading

Alper Kanak, ERARGE - Ergünler Co. Ltd. R&D Center

erGE

Massimiliano Aschi, Poste Italiane

Posteitaliane

Kristo Klesment, Guardtime

guardtime

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Authentication & Accountability Models in Financial Flows

**Prof. Atta Badii**, Critical-Chains project coordinator, University of Reading

- Chair of Secure Pervasive Technologies at the Department of Computer Science, University of Reading, leading the Data Intelligence Research Lab
- Project coordinator of Critical-Chains, and previously VideoSense Centre of Excellence amongst many projected coordinated and led in collaborative international research.
- Pioneered several paradigms and architectures with significant contributions to high impact research and innovation e.g. in the areas of high-speed real-time hardware assisted malware intrusion detection, secure semantic middle-ware framework, IOT-enabled X-as-service, robotic cognitive control, multi-modal multi-media indexing and semantic-cooperative search, image processing, secure computation, context-aware privacy engineering.

**Dr. Alper Kanak**, ERARGE - Ergünler Co. Ltd. R&D Center

- R&D Director in ERARGE
- published more than 25 papers in the fields of privacy-security-trust models, biometric security, speech and language technologies, semantic web, smart city, ontology design and image/video processing
- contributed to Turkey's ICT strategies as the national representative
- lead biometric studies and AUTHaaS with a deep focus on ENISA taxonomy, supporting semantic studies and ontology design

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Authentication & Accountability Models in Financial Flows

## Critical-Chains Consortium

Atta Badii, Alper Kanak, Salih Ergün

atta.badii@reading.ac.uk , alper.kanak@erarge.com.tr , salih.ergun@erarge.com.tr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Financial Sector Challenges: Security - Accountability

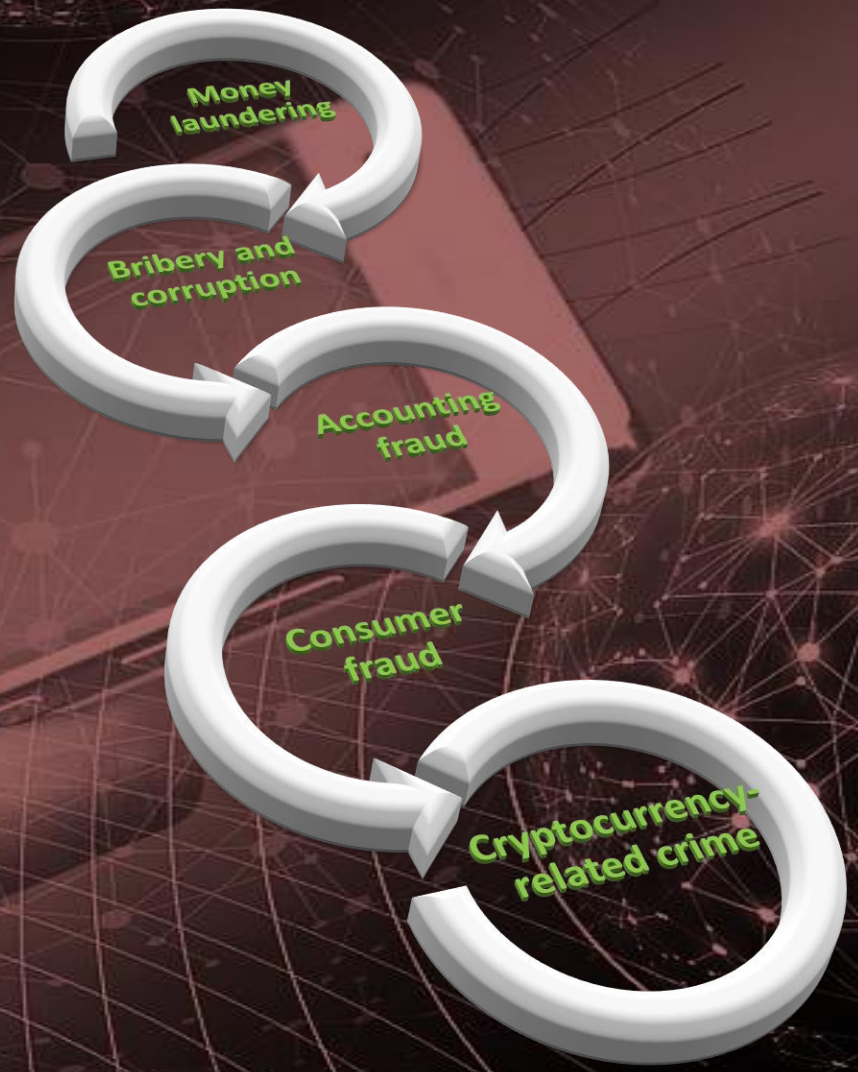
Cyber criminals have netted $4.3 billion from digital currency exchanges, investors and users in 2019.

#users attacked by banking malware (like Trojans) was about 900 thousand with ~16% increase as compared to 2017

#users who encountered Android banking malware tripled to 1.8 million worldwide.

Cybercrime is the most commonly experienced fraud- 31% globally (2018)

Data analytics detected only 1% of frauds in the UK (compared to a global average of 4%) as of 2018

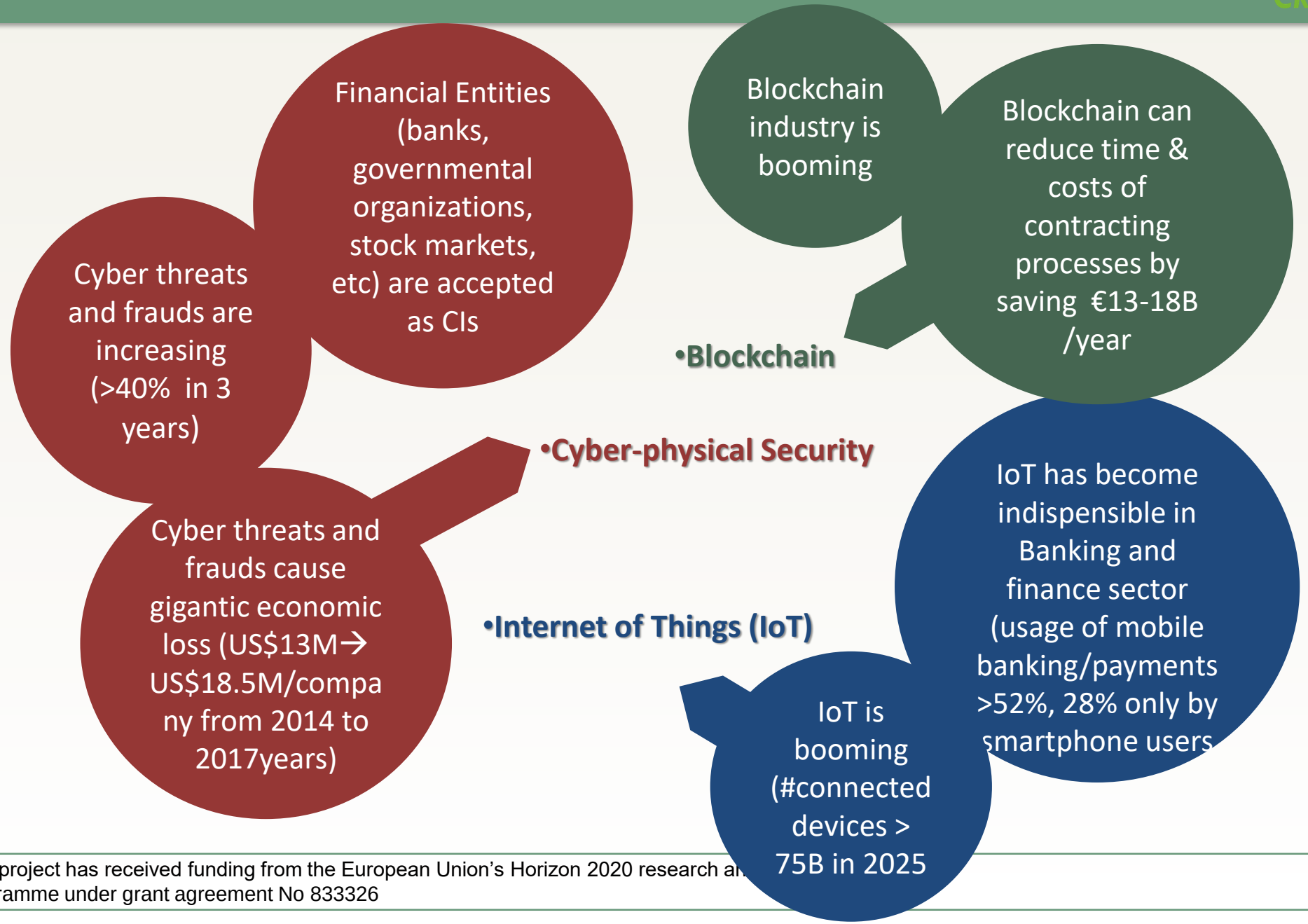



**Digital technologies are profoundly changing the financial sector, but also a source of massive threat**

https://cointelegraph.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study
https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2018---uk-findings.html
Kapersky. *Financial Cyber threats in 2018.* March 07, 2 https://securelist.com/financial-cyberthreats-in-2018/89788/ (accessed November 11, 2019).

Image from https://www.piqsels.com

# Cyber-Physical Risk Exposures Evolving




This project has received funding from the European Union's Horizon 2020 research a
programme under grant agreement No 833326

# Responsive Measures

**Increased digitization, growing complexity of cyber-attacks certain sectors/subsectors more critically exposed e.g. banking, and financial market infrastructures as part of critical infrastructure**

## Digitally transformative innovation

Support cyber security, privacy, accountability and efficiency

## Standardisation

Enable the rapid adoption of cybersecurity best practices in the domain

## Need to promote common standards

Conducting stress and resilience testing across systemic financial market infrastructures and institutions

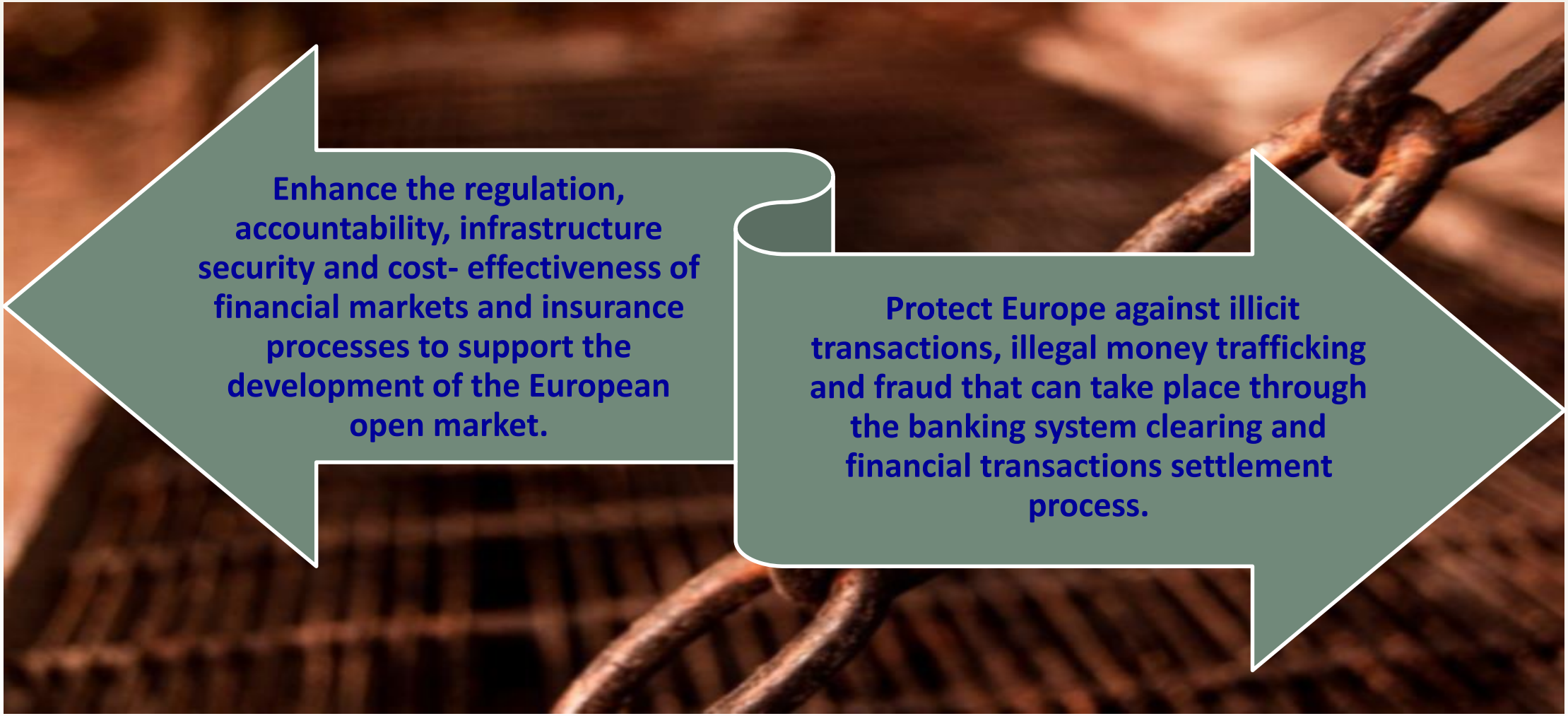
## Need to ensure harmonised compliance assurance

Compliance Audit required to confirm compliance status of processes

**Asymmetries: New Kids on the Block sometimes Operating in a Regulatory Void**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Priority Objectives towards Security-Accountability in the Emerging Financial Sector



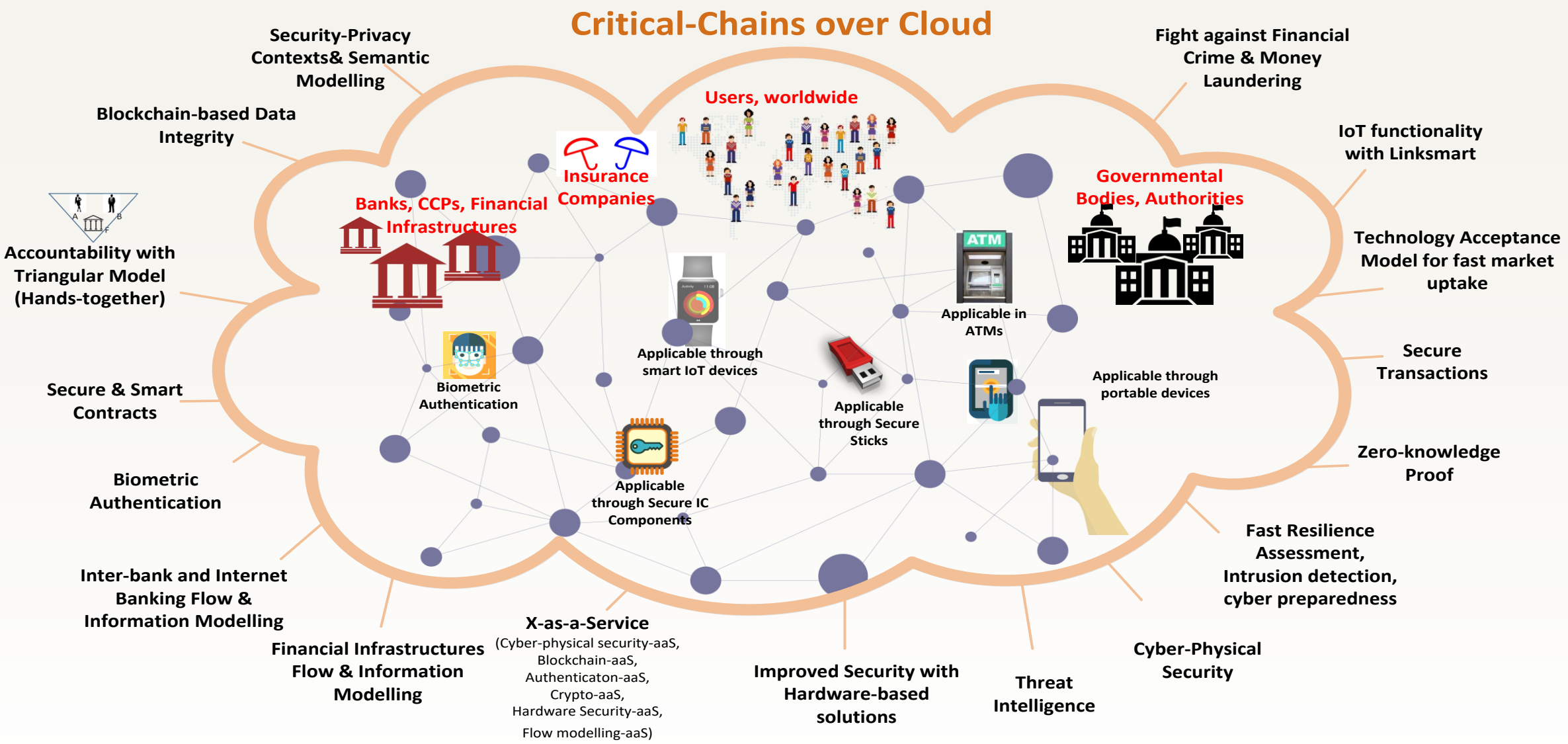

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

- **Critical-Chains Main Framework:**
  - Cloud-based data transmission, communication
  - and financial transactions horizontal framework
- **Cyber-Physical Security as a Service:**
  - Blockchain-as-a-Service
  - Authentication-as-a-Service: Authentication and
  - authorization services using secure IoT sticks and
  - biometric authentication.
  - Cryptography-as-a-Service
  - Data and information security and privacy preservation
  - at all layer of cloud
- **Flow Modelling-as-a-Service:**
  - Data flow and information modelling
- **Critical-Chains-supported Compliance Audit**


5. Consider privacy, ethical and legal concerns, socio-economic analysis, public acceptance and elaborated impact analysis aligned with Fintech industry

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Critical-Chains Solution Stack




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Expected Results

Development of new/enhanced, parameterized, automated and collaborative ICT tools for the financial sector

- Needed for security, privacy, personal data protection and accountability requirements
- Coping with the possible new risks arising from the compliance with new directives

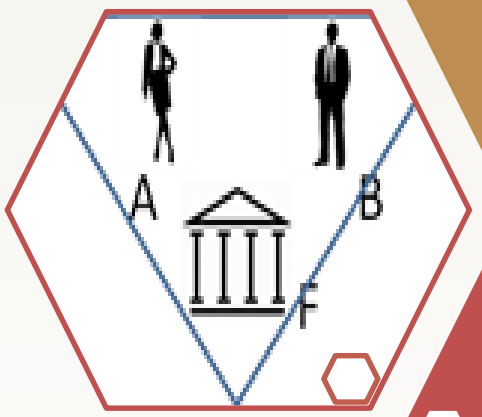
Delivering tools for making the exfiltration of data for attackers unattractive

- Both for ‘data at rest’ and 'data in transit'; considering incipient trends (e.g. digital on-boarding based on biometric data)
- Enhanced collaboration with CERTs/CSIRTs

**Critical-Chains security measures for Blockchain transactions can also be used for cryptocurrencies**
**TRLs ranging from 5-6 initially and 7-9 as final deliverables**

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833326

# What's new?



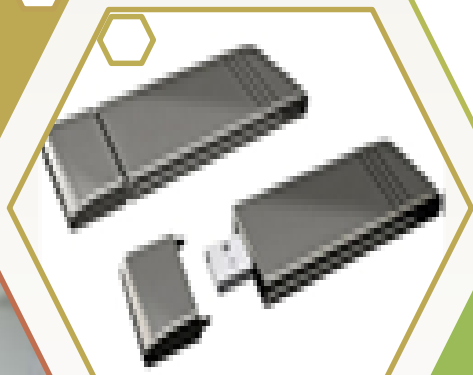

**Elastic cyber-physical security and AI in the form of X-as-a-Service services** over an integrated web-based cloud platform (holistic approach)

**New authentication/ authorisation mode** with IoT-enabled cyber-physically-secure sticks and **biometric authentication over blockchain**

**New accountability model** by adding authorities in the decentralised network

More **resilience with hardware-based cyber-physical security services** in XaaS form and smarter with effective flow and information models

**Data integrity with blockchain & Audit and Compliance models** applicable to the context.



**Sobjective assessment of technology** and its uses in practical Fintech world

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Target End Users

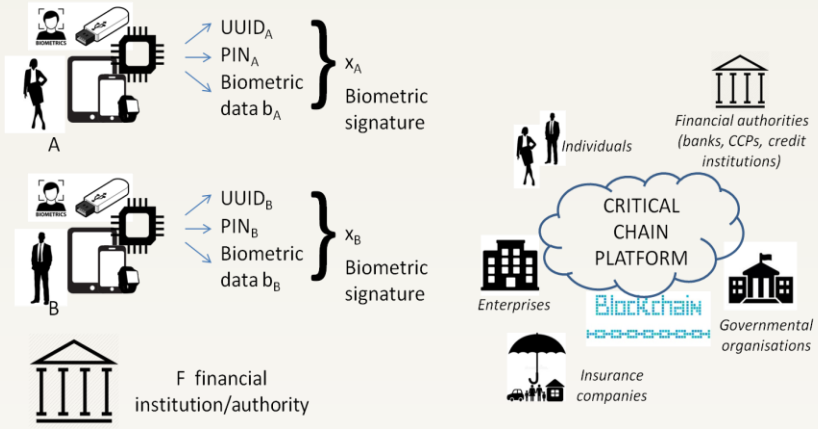
Use Cases and Target Sectors

Financial Sector, Internet Banking, Inter-Banking, Clearing

Insurance Processes

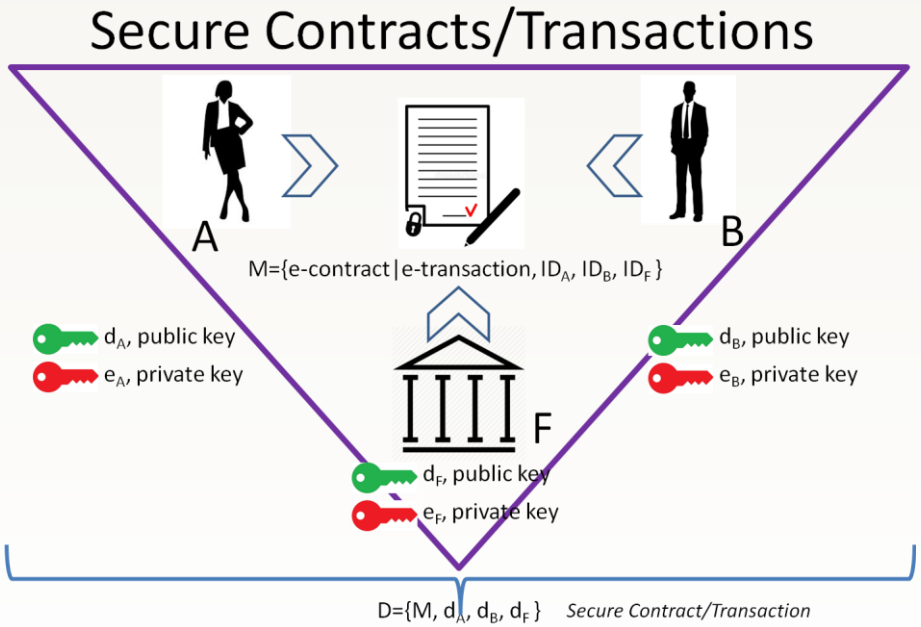
Highway Toll Collection

# The Accountability Model



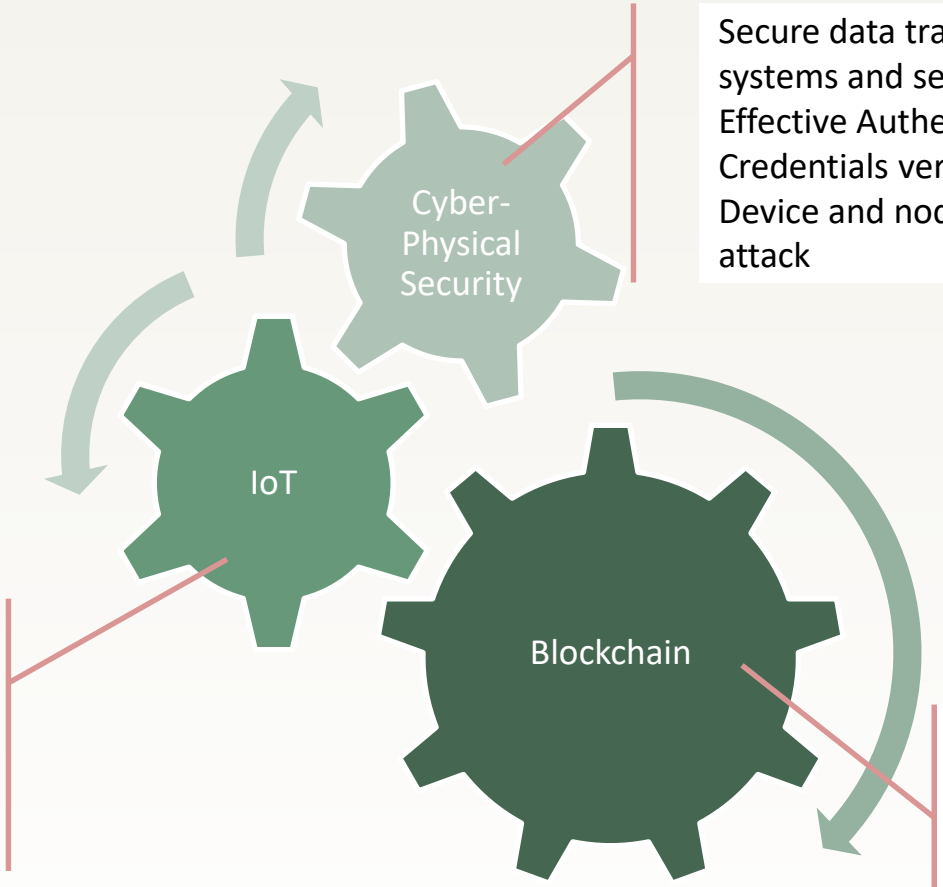


**Accountability-by-design** where financial authorities are put in multiparty blockchain-enabled triangular integrity and security for legal framework and further accreditation.




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

## Not only Blockchain can improve accountability and efficiency! We need a holistic approach




Secure data transmission among IoT nodes, systems and services
Effective Authentication and authorization
Credentials verification of stakeholders
Device and nodes security and safety against CPS attack

- IoT-enabled heterogeneous Communication infrastracture
- Controller connection

- Decentralized trusted collaboration
- Cross-hierarchical and cross-sectoral working
- Accountability at all layers

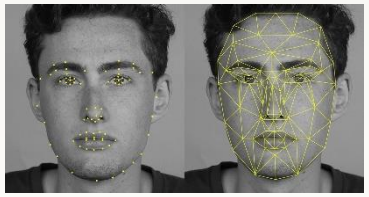
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Hardware-based Solutions

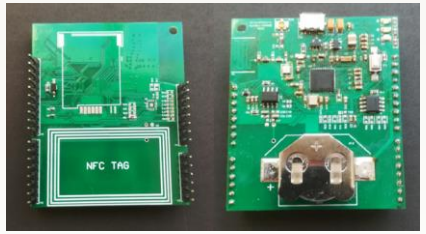
Why don't we make authentication to blockchain-based main framework simpler and more secure?

FIDO-compliant Authentication-as-a-Service


## Person Authentication



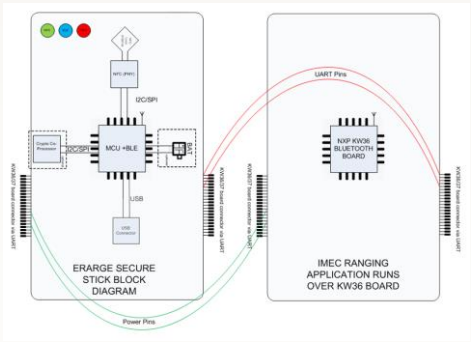
*Biometric*
*(who you are)*




*Facial signatures are **encrypted** and **biohashed** before loading*

*Match-on-Device*
*(what you have+know)*

## Node Authentication





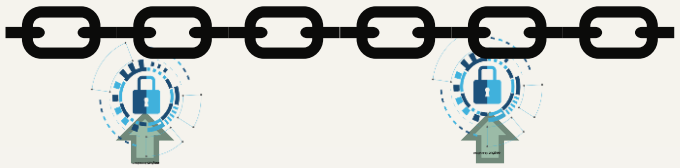
**SecureStick**, a multipurpose authentication token, designed in Critical-Chains (FIDO- and GDPR-compliant)

**Vulnerability Assessment**

**Secure Distance Bounding** integrated with IMEC's specified BLE chip (designed for IoT-enabled payment systems in Critical-Chains)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Hardware-based solutions



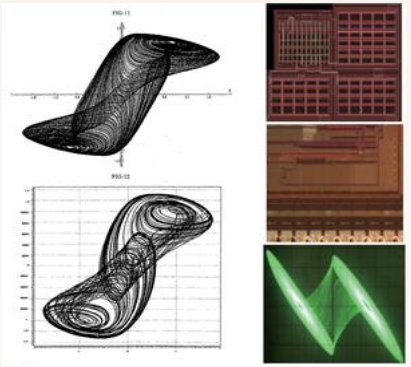

Why don't we encrypt the data before injecting in the blockchain ?
(if the solutions are **fast** enough with high **throughput** and assure the **security**)

According to **Kerckhoffs's** assumpion, a cryptosystem cannot be accepted as secure if the cryptographic keys are **predictable** and the secrets are **cancelable** (once compromised compromisd forever).

**Pseudo**-random number generators (guessable) and Physical Unclonable Functions (**PUFs** - static) are not sufficient

The solution is the hardware-based Truley Random Numbers applied in **Hardware Security Modules** and node authentication

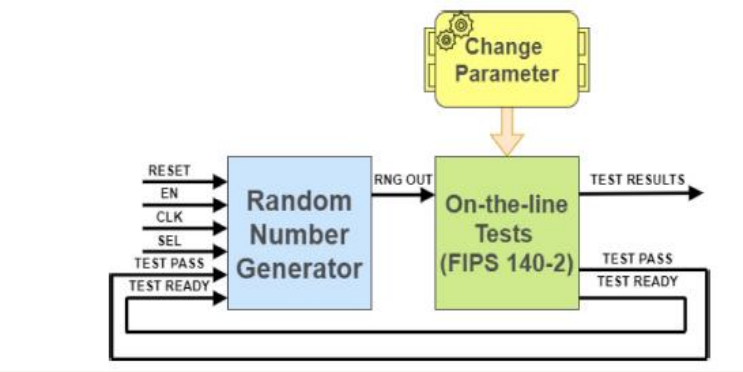
*Varius alternatives improved in Critical-Chains, based on Chaos© theory or ring oscillators, all fulfills NIST-800-22*

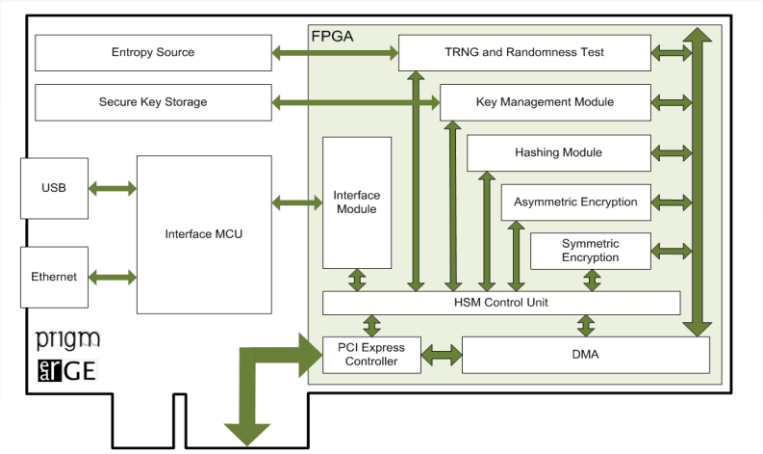


*Prigm©, Hardware Security Module with very high throughput (e.g. up to 1 Gbit/s TRNG), EAL4+ soon*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Hardware-based solutions



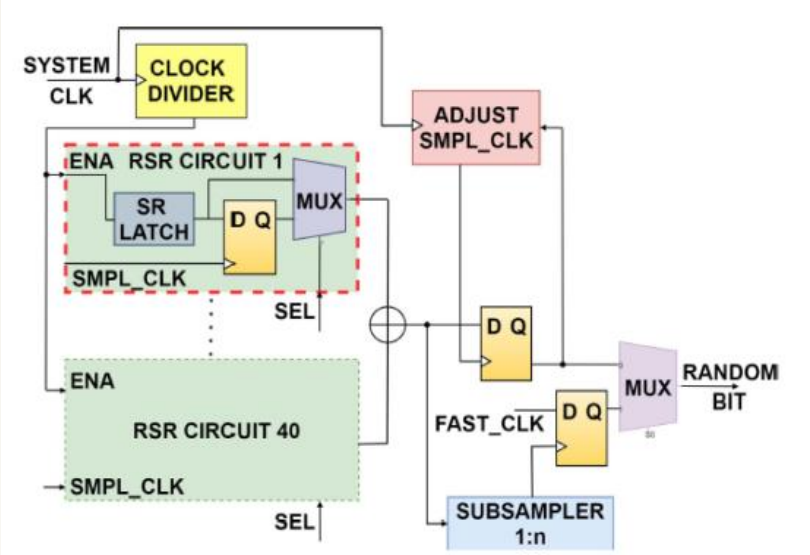

HSM, at server side, enabling

- Hardware Security-as-a-Service (at HW level)
- Crypto-as-a-Service (at SW level)

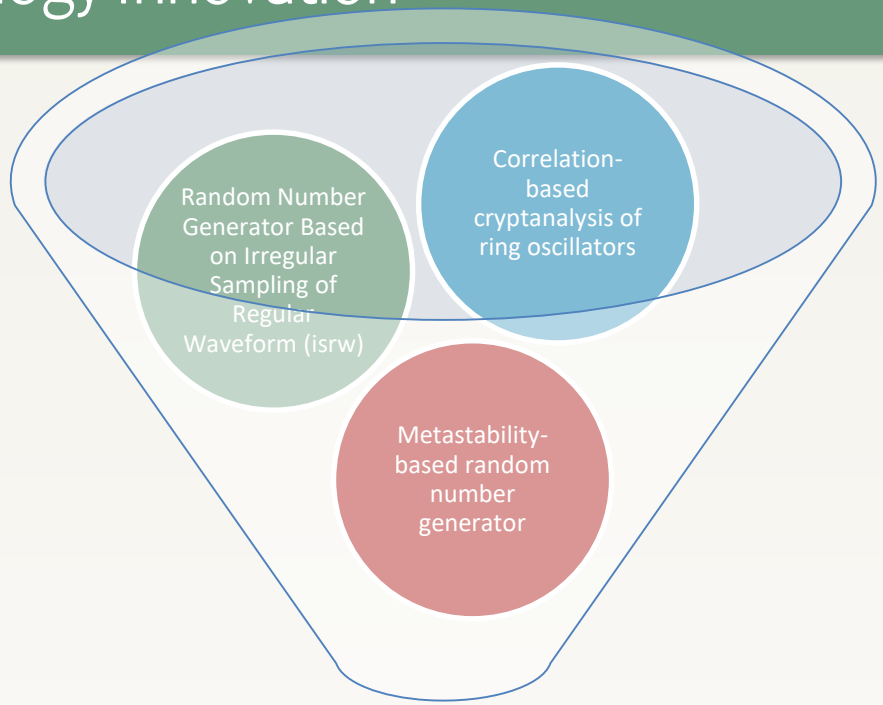
- Utilises the True Random Number Generator
- On-the-line randomness test
- Symmetric and Asymmetric Cryptography (AES, 3DES, ECDSA, RSA, customised algorithms)
- Public Key Cryptosystem (PKCS#11)
- Resilient against tampering attacks
- Very high througput suitable for big data application
- Background: 12 patents, 50+ papers
- New techniques for vulnerability analysis based on non-linear signal analysis techniques
- 9 international papers so far (1 journal + 8 conf) within the Critical-Chains
- Presentation in 5 conferences

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Achievements in the Forefront of Technology Innovation




*Reconfigurable Transient-Effect based RNG, designed within Critical-Chains*




A More Robust Reconfigurable Transient-Effect based RNG

**Cost-effective**

A Robust Random Number Generator Based on Chaotic Ring Oscillators

**Faster**

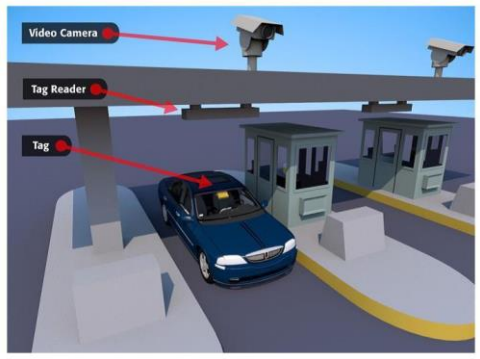
**Both Fulfills FIPS-140-2**

Visibility & Dissemination

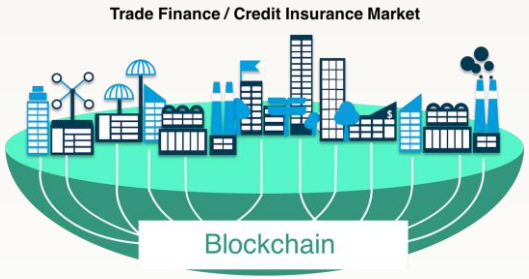
- IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)
- IEEE Asian Hardware Oriented Security and Trust Symposium
- International Midwest Symposium on Circuits and Systems (MWSCAS
- IEEE EUROCON
- IEEE International Symposium on Circuits and Systems (ISCAS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

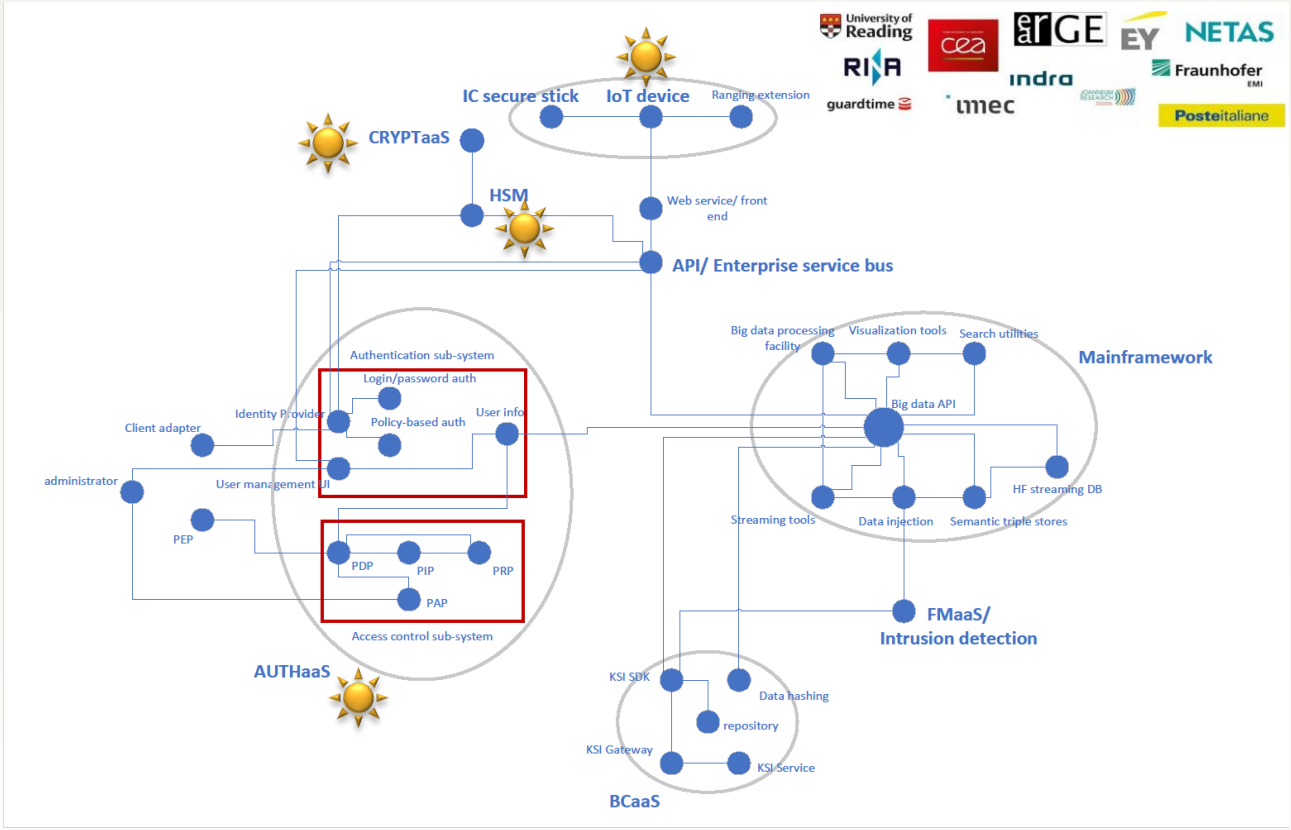
# Wide range of application relevant for consumers and financial service providers




Toll collection, Secure payment by BLE-enabled security tokens and payment with cryptocurrencies (Critical-Chains)




Secure insurance processes, accountability in insurance policies and field inspection, credit scoring, … (Critical-Chains)




Hardware-based solutions within the Critical-Chains main architecture (special thanks to all partners)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Authentication & Accountability Models in Financial Flows

**For more information on Critical-Chains project**:
Prof. Atta Badii,
**Critical-Chains Project coordinator**,
University of Reading
atta.badii@reading.ac.uk

University of Reading

For more information:
Alper Kanak, PhD,
alper.kanak@erarge.com.tr
Salih Ergün, Assoc. Prof.
salih.ergun@erarge.com.tr

erGE

CRITICAL CHAINS

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# eiDAS- Compliant Authenticated Access to the Critical-Chains Framework using the National Digital Identity (SPID)


**Massimiliano Aschi**, Poste Italiane


- Information Security Professional Master at the Information Security Department of Poste Italiane
- Information Technology Expert, digital forensics investigator (CHFI) and certified CISSP (Certified Information Systems Security Professional)
- Permanent member and active contributor of the European Electronic Crime Task Force
- Certified BCMS Lead Auditor (ISO 22301, ISO27001), member of the FI-ISAC and of the Anti-Phishing Working Group


**Marco Avallone**, Poste Italiane


- Cyber security specialist at Poste Italiane
- Expertise in Identity Management and Mobile Security topics
- Involved on application security, focused on IAM (Identity and Access Management) Infrastructure, coordinating activities about development and integration of the infrastructure
- Holding various certification related to security and IT field such as security products certifications, CISSP (Certified Information Systems Security Professional), ITIL, and Intermediate (Service Transition) certifications


This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# eIDAS-compliant authenticated access to the Critical-Chains Framework using the National Digital Identity (SPID)

Massimiliano Aschi, Security Management and Innovation
Poste Italiane Spa – Banking, Insurance, Parcels, Logistics & Mail Company

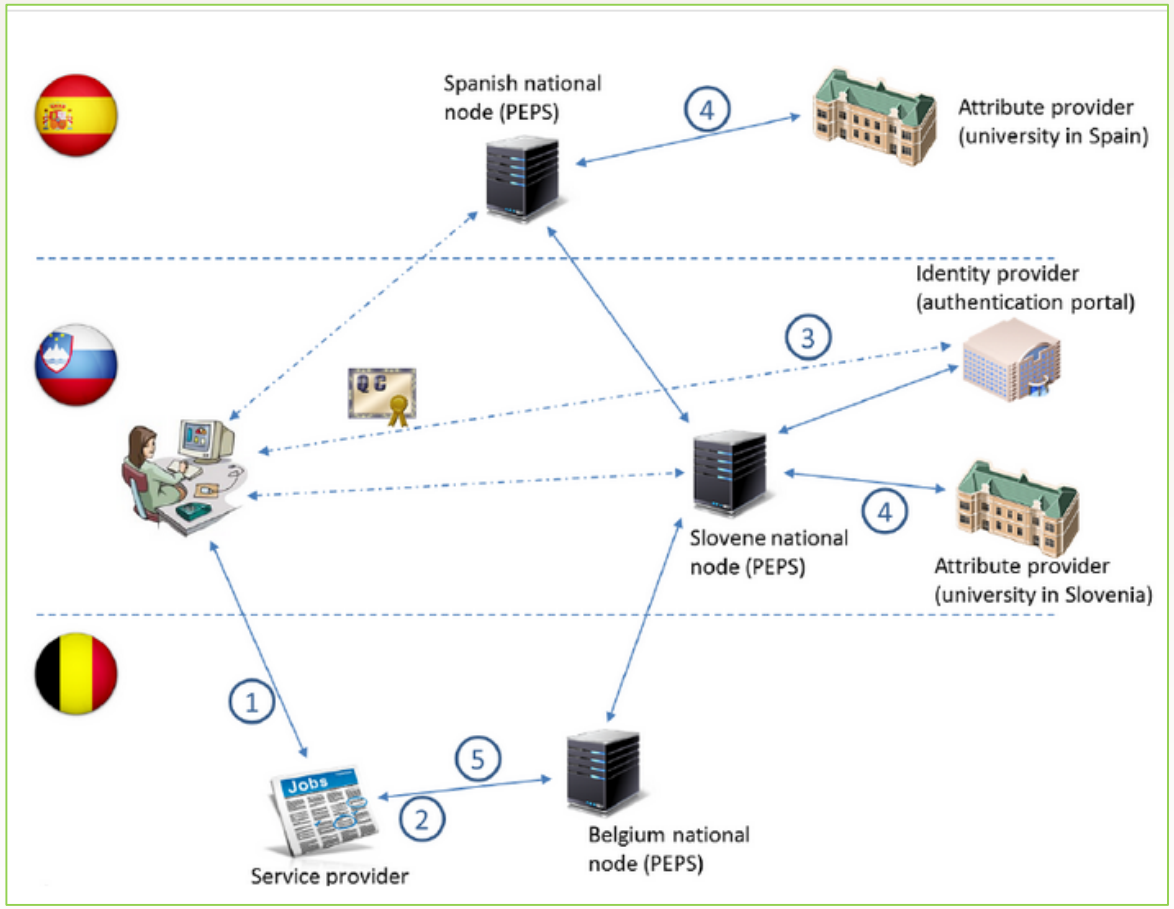
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# eIDAS authentication: a step towards a digitally integrated Europe

The *eIDAS Regulation* on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Regulation (EU) No 910/2014) was adopted by EU co-legislators on 23 *July 2014*.

The regulation aims to *promote cross-border cooperation* and the *interoperability* of national digital identity (eID) systems to make it more convenient for *citizens and businesses to access* online public and private services in the various member states.

The cross-border interoperability is enabled by means of *National eIDAS-Nodes* that are currently being rolled-out in all Member States.

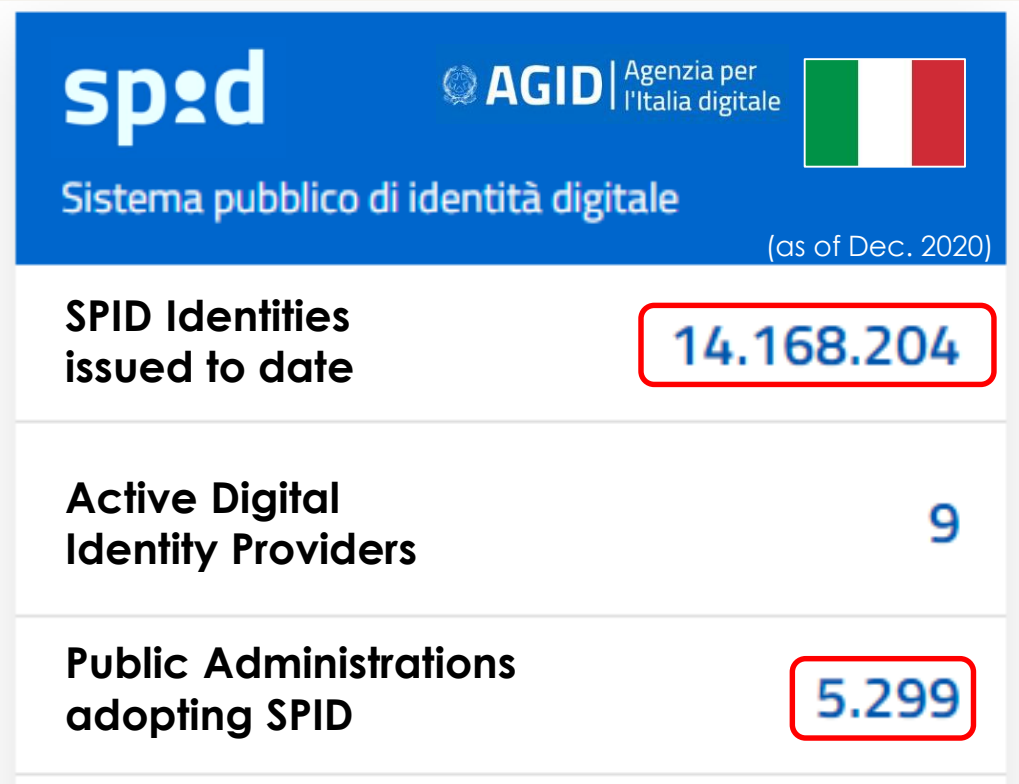



*Example of an eIDAS Digital Identity cross-border usage scenario*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# SPID - Public Digital Identity System

- SPID is the Italian Public Digital Identity System that guarantees all citizens and businesses a single, secure and protected access to the digital services of the *Public Administration* and *Private Service Providers*.
- SPID identity is issued by *Identity Providers*, private entities accredited by the *National Agency for Digital Italy* (AgID), which provide digital identities and *manage user authentication* in line with the rules issued.




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# SPID – Services Providers and Type of Services

- Municipalities
- Central Public Administration
- Public Agencies
- Private Companies

- Subsides for teachers and students
- Basic income of citizenship
- Public pension plans
- e-Health services
- e-Tax services
- e-Payments
- Vouchers
- …

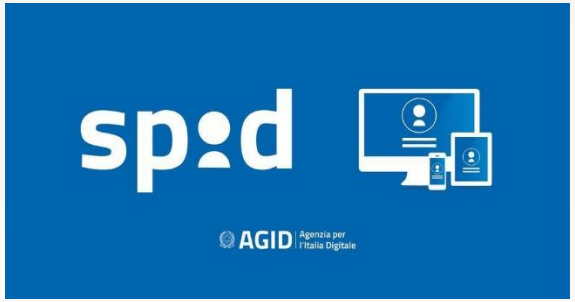

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# SPID is an eIDAS-compliant ecosystem

*Starting from September 2018, SPID is eIDAS-compliant,* therefore online digital services offered through *SPID are now accessible to European citizens* by using their own national digital identity (eID).

*Poste Italiane* is the biggest Italian Digital Identity Provider and brought into *CRITICAL-CHAINS* the know-how, technology and experience needed to let *EU citizens access our framework's services by means of their National e-ID*

eIDAS-compliant





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Integration between eIDAS, SPID and CRITICAL-CHAINS

One of the building blocks in the CRITICAL-CHAINS' framework architecture is the **Authentication-as-a-Service**

The service, will be a complete Identity Access Management (IAM) system, supporting standard authentication protocols and providing Indentity Broker functionalities.

Based on this technology, we modified an existing component in order to allow CRITICAL CHAINS' users to authenticate by means of a SPID Digital Identity

On Aug 2020, CRITICAL-CHAINS *successfully completed the integration with SPID* Provider Test Environment

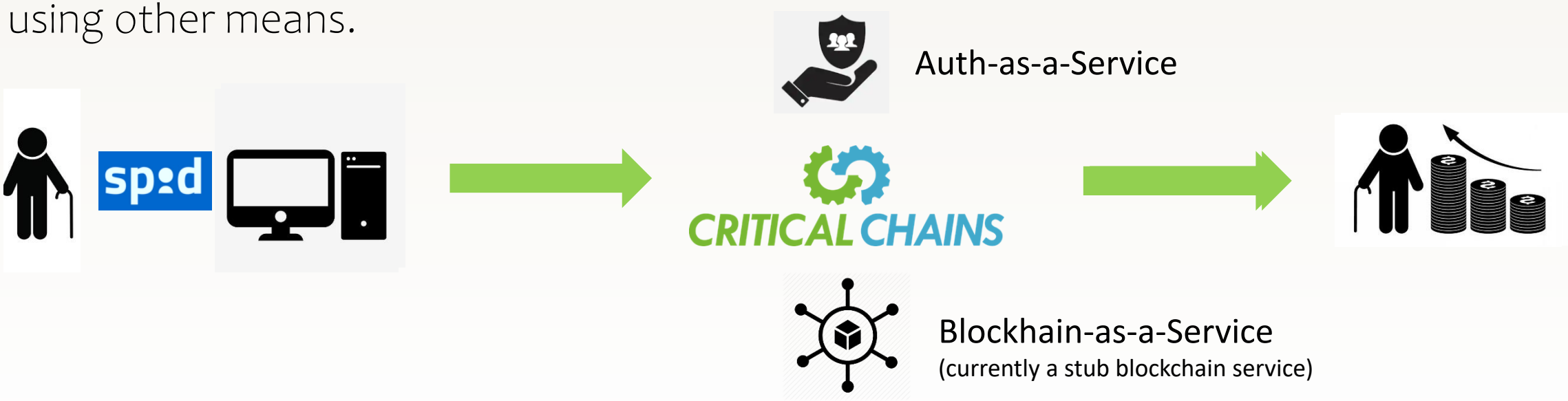
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# The Pension Fund Management Pilot

A CRITICAL-CHAINS' - phase 1 - Pilot software is currently under testing, leveraging on SPID identities for users' authentication.

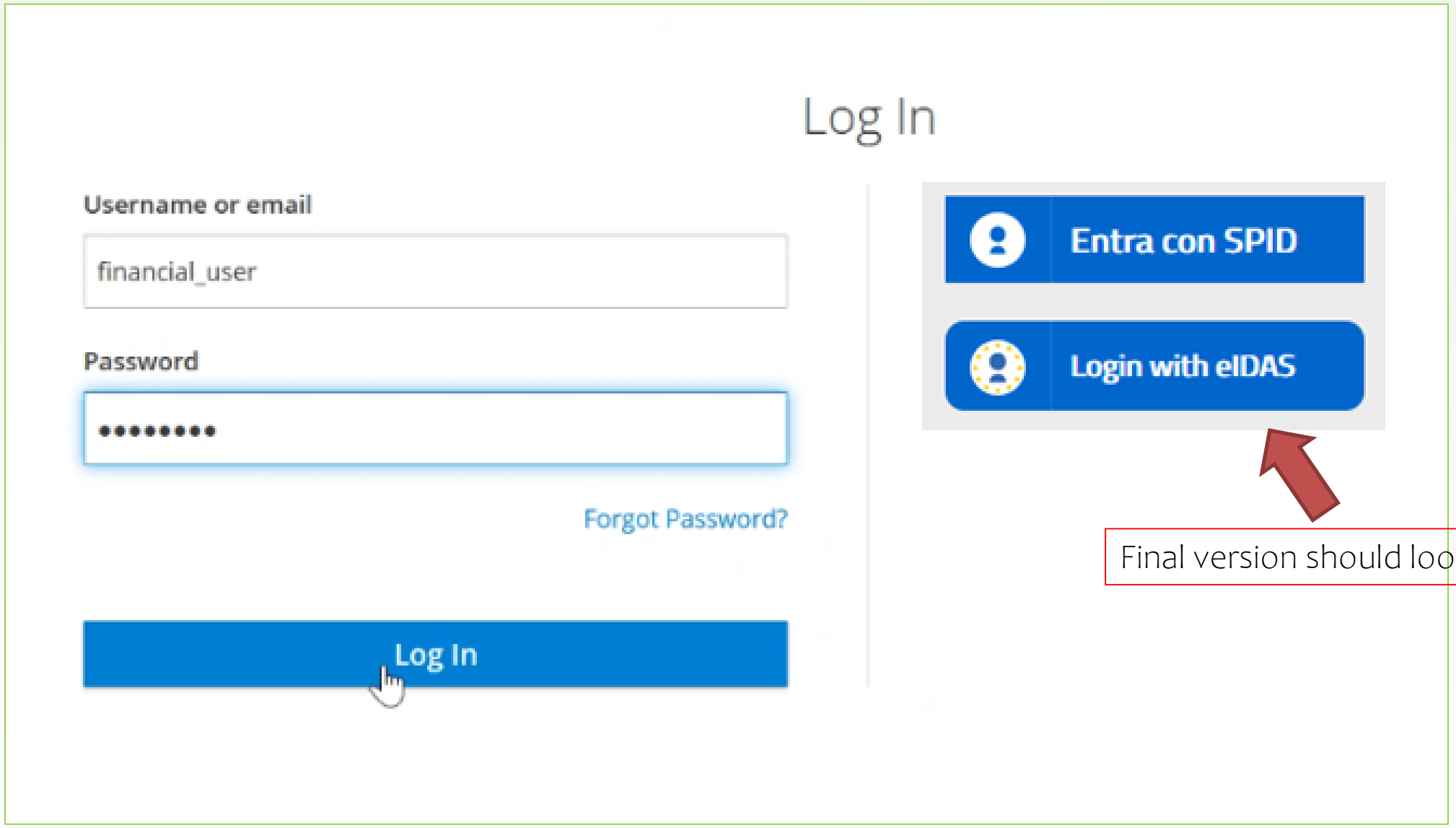
PILOT SCENARIO:

An employee of the public administration, wants to subscribe to a **pension fund** and he wants to do it through CRITICAL-CHAINS because he knows it is much safer than by using other means.



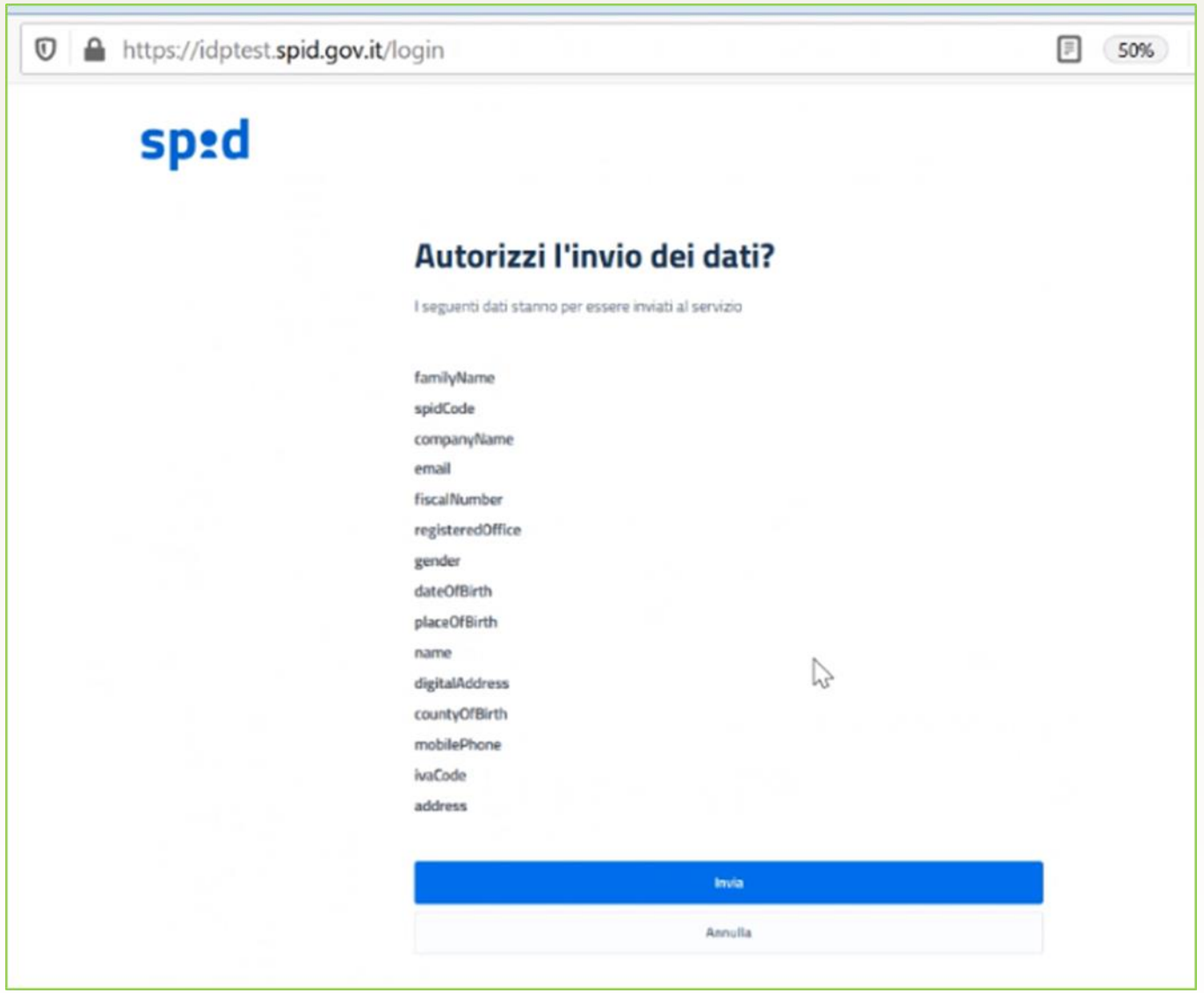

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# The Pension Fund Use Case - Authentication



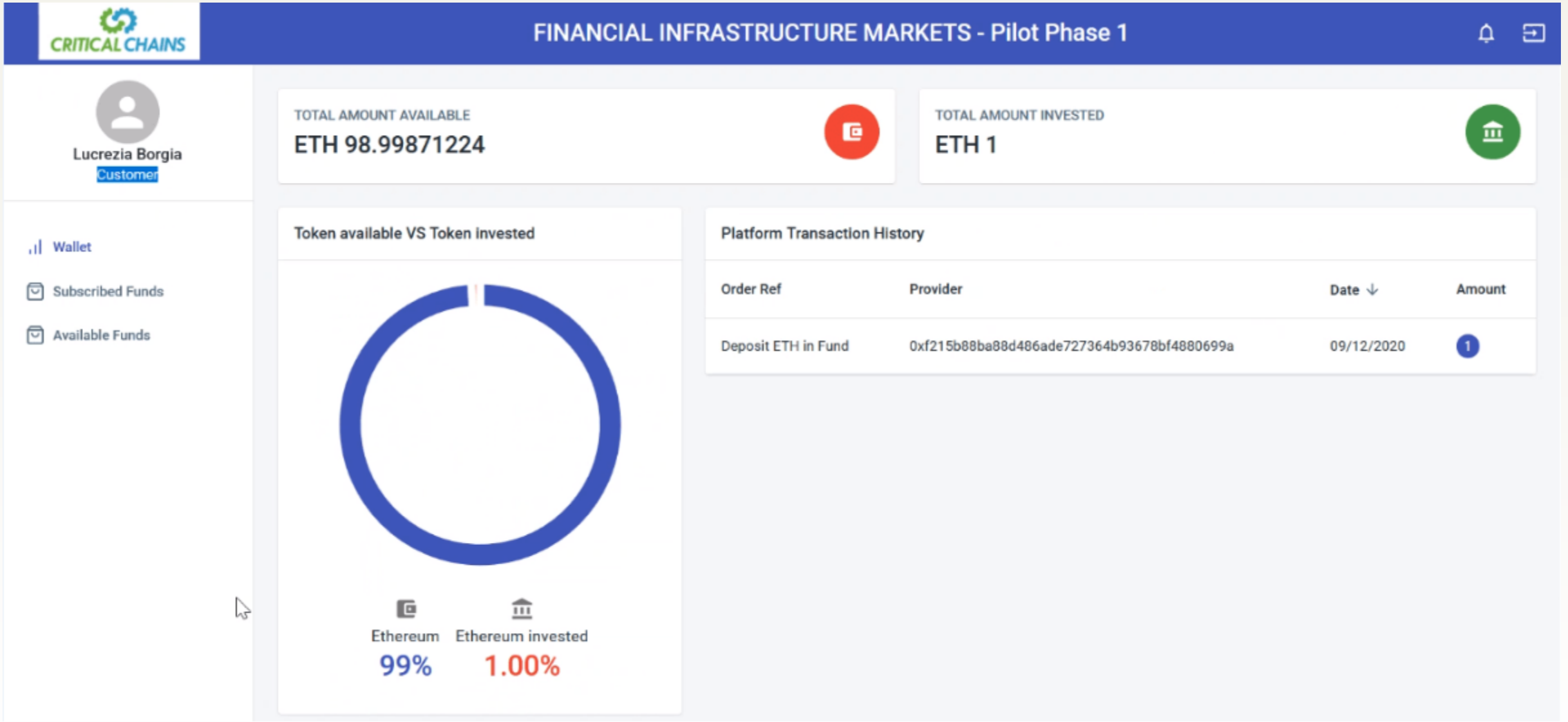

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# The Pension Fund Use Case –
# Request authorization to share personal infos with the Service Provider



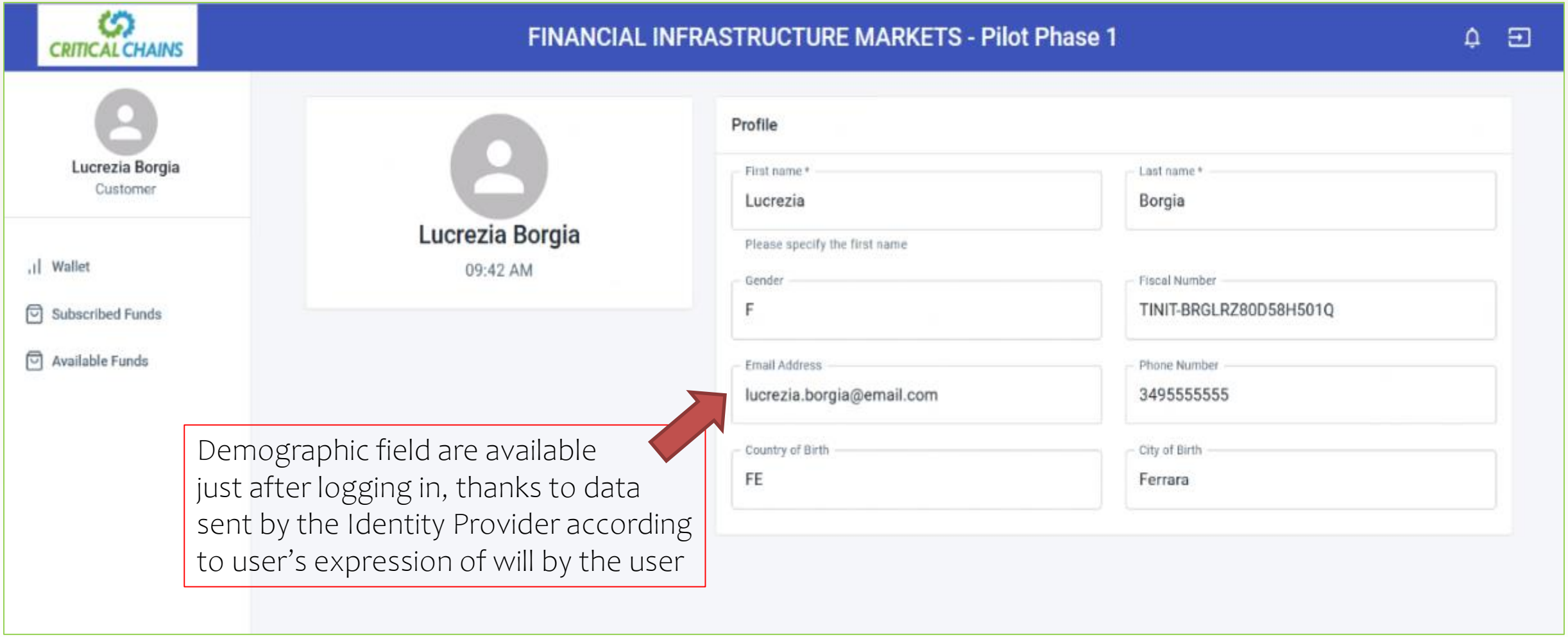

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Pension Funds Pilot – Dashboard – Users' view




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

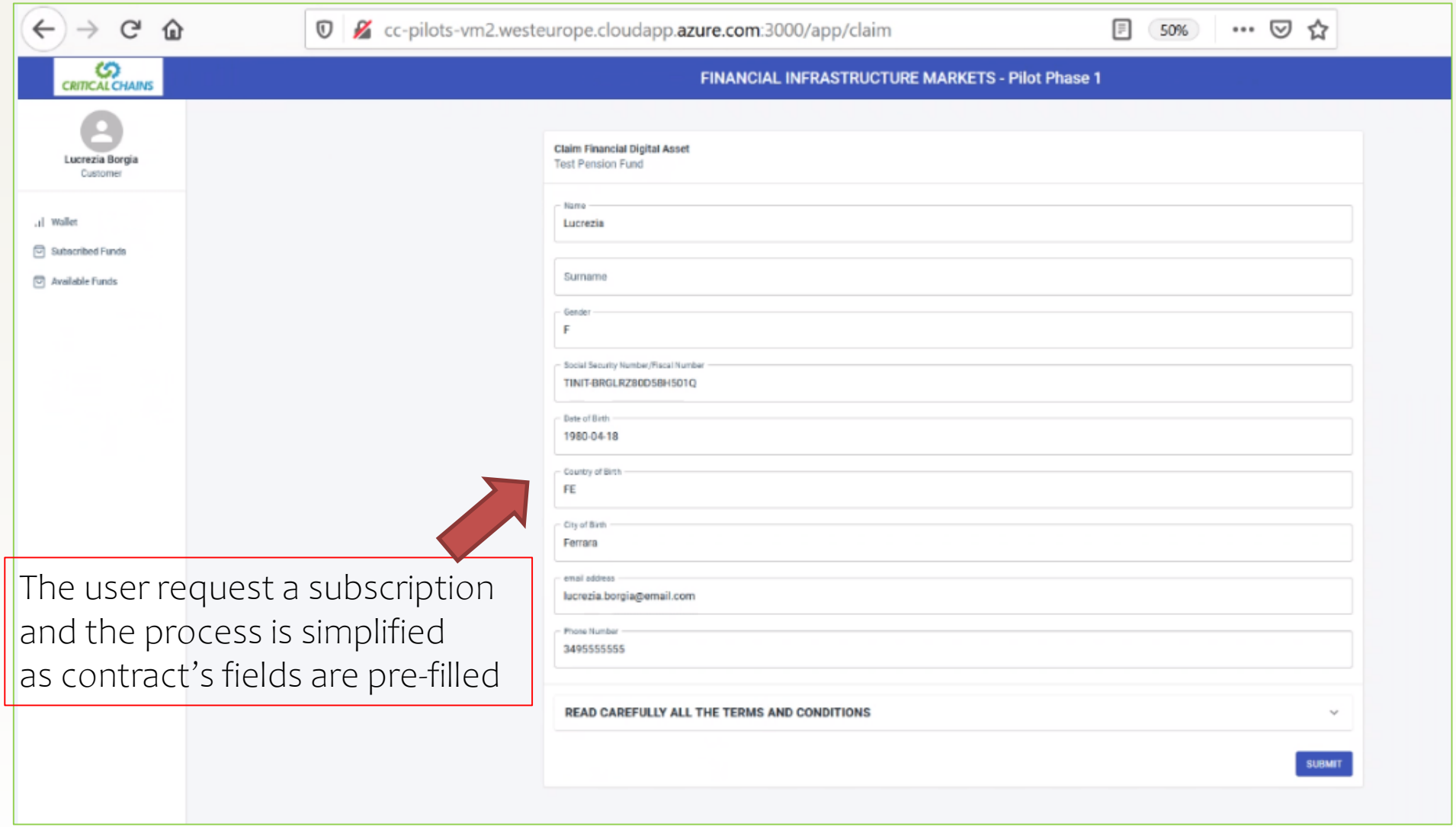
# Pension Funds Pilot – User profile




Demographic field are available just after logging in, thanks to data sent by the Identity Provider according to user's expression of will by the user

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

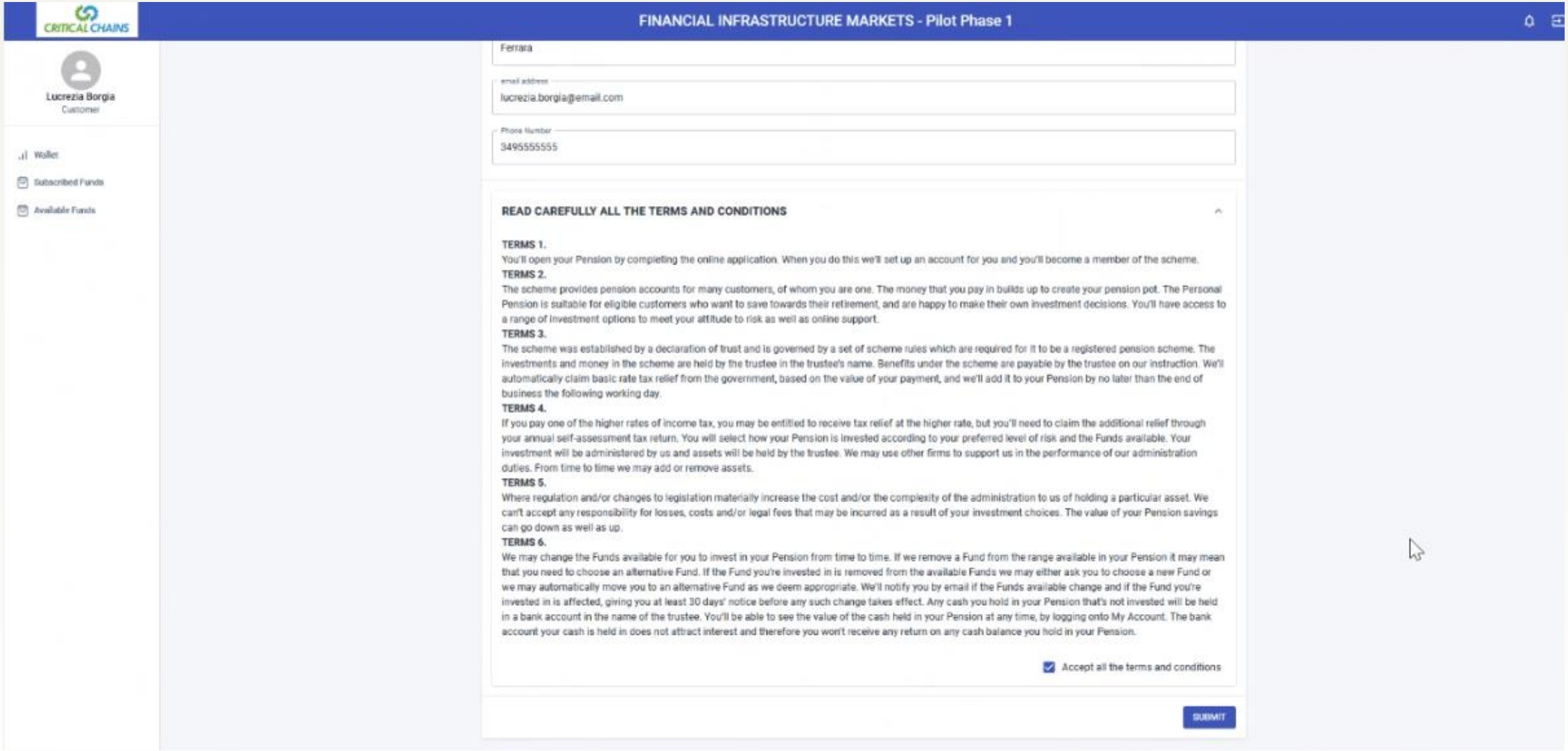
# Pension Funds Pilot – User requests subscription to the fund




The user request a subscription and the process is simplified as contract's fields are pre-filled

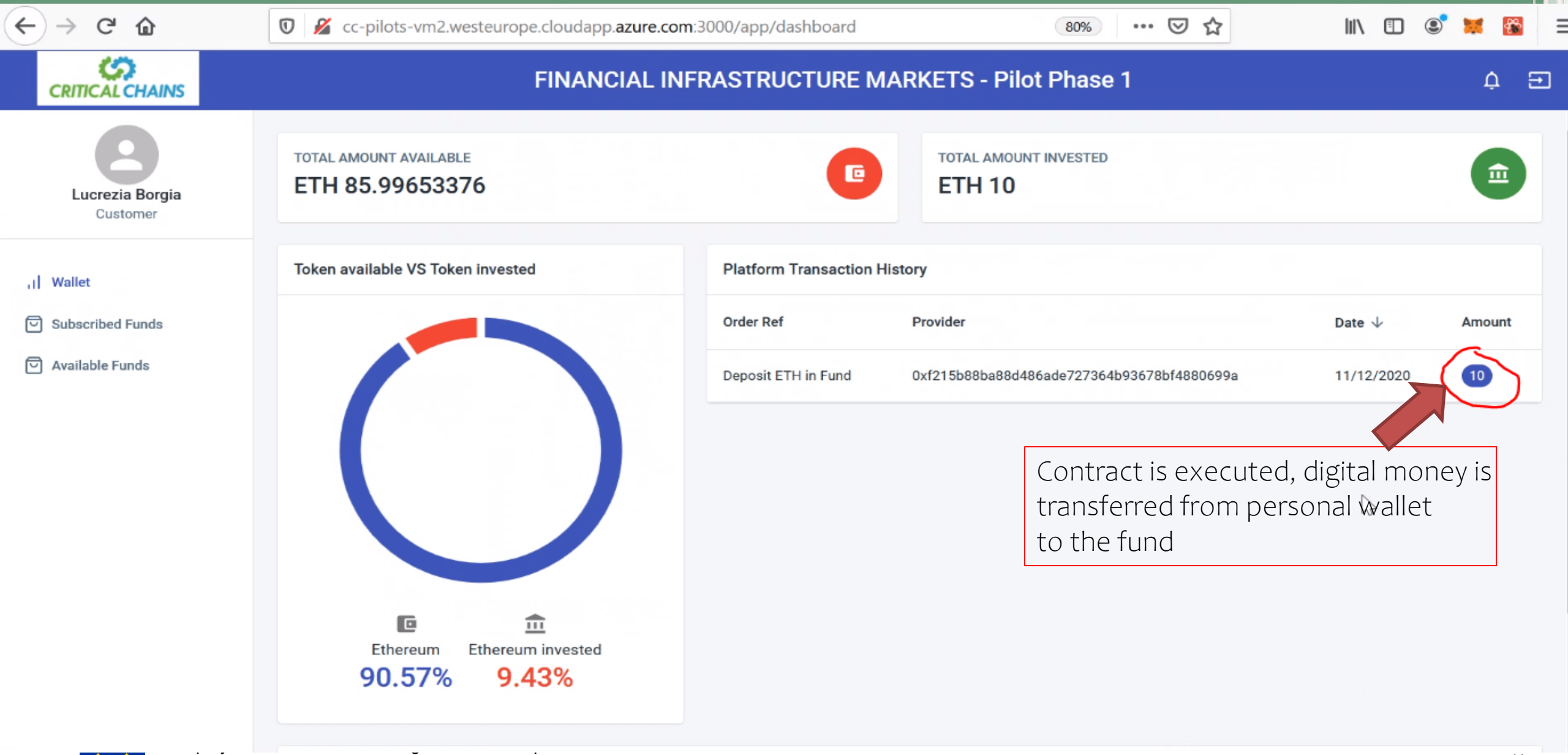
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Pension Funds Pilot –
# User reads contract's terms and conditions and finally subscribe




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Pension Funds Pilot – Digital Money is transferred to the fund

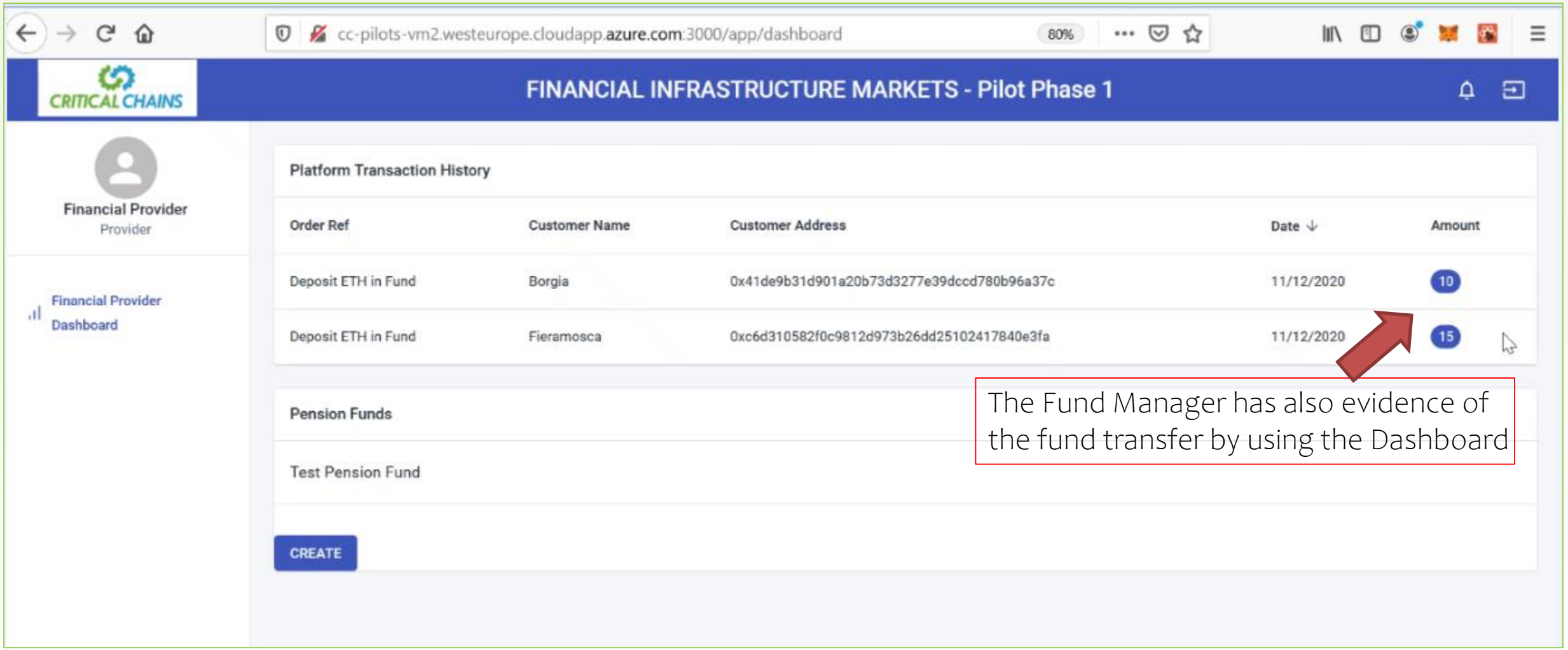



programme under grant agreement No 833326

# Pension Funds Pilot – User can check contract conditions anytime


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Pension Funds Pilot – Fund manager's view on Dashboard




The Fund Manager has also evidence of the fund transfer by using the Dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Conclusions

SPID/eIDAS integration in CRITICAL-CHAINS' Auth-as-a-Service building block, effectively opens to cross-border usage scenarios of the entire framework as the developed Pilot demonstrates. At the same time, by supporting with our technologies the European standard for eID authentication, we are open to a very-wide audience of potential users.

Futhermore, usage of Qualified Digital Identities in banking and financial applications enabled by the CRITICAL-CHAINS framework, could greatly simplify some heavy and costly operational processes like customer on-boarding, KYC processes or simply the customer identification phase thus paving the way to CRITICAL-CHAINS' "on field" exploitation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# eiDAS- Compliant Authenticated Access to the Critical-Chains Framework using the National Digital Identity (SPID)

For more information:
Massimiliano Aschi,
aschim@posteitaliane.it
Marco Avallone,
marco.avallone@posteitaliane.it

Posteitaliane

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# Fintech Cloud Environment Trust & Security Challenges


Kristo Klesment, Guardtime

- R&D Project Manager, IPMA certified project manager in Guardtime
- Technical coordinator of Guardtime activities in Critical-Chains project
- Experienced in enabling technologies dealing with IT protection of critical infrastructures (telco, retail, banking, water, electricity, gas utilities).



This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

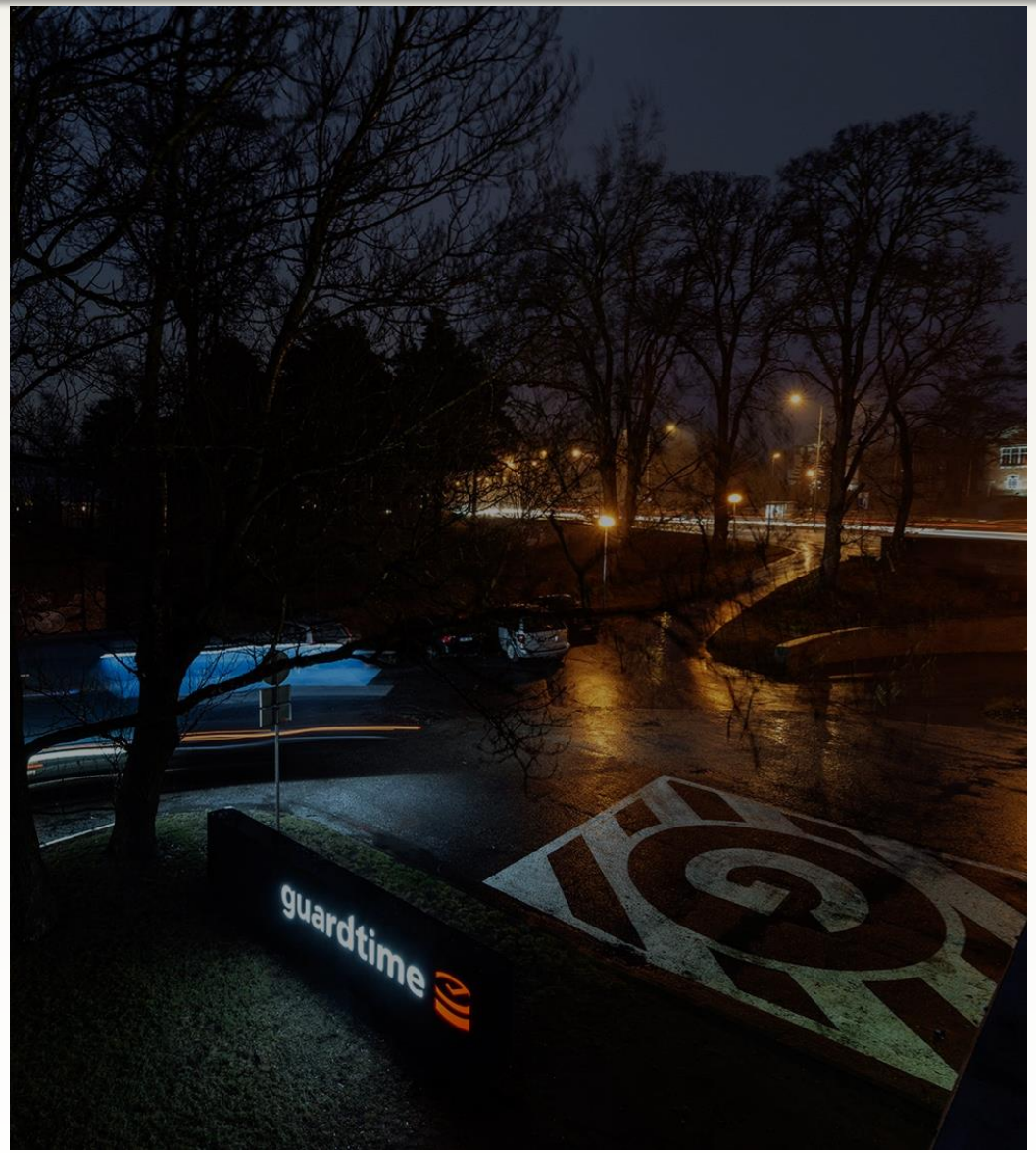

# Cloud Environment Trust and Security Challenges

Kristo Klesment
**Guardtime Ltd**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

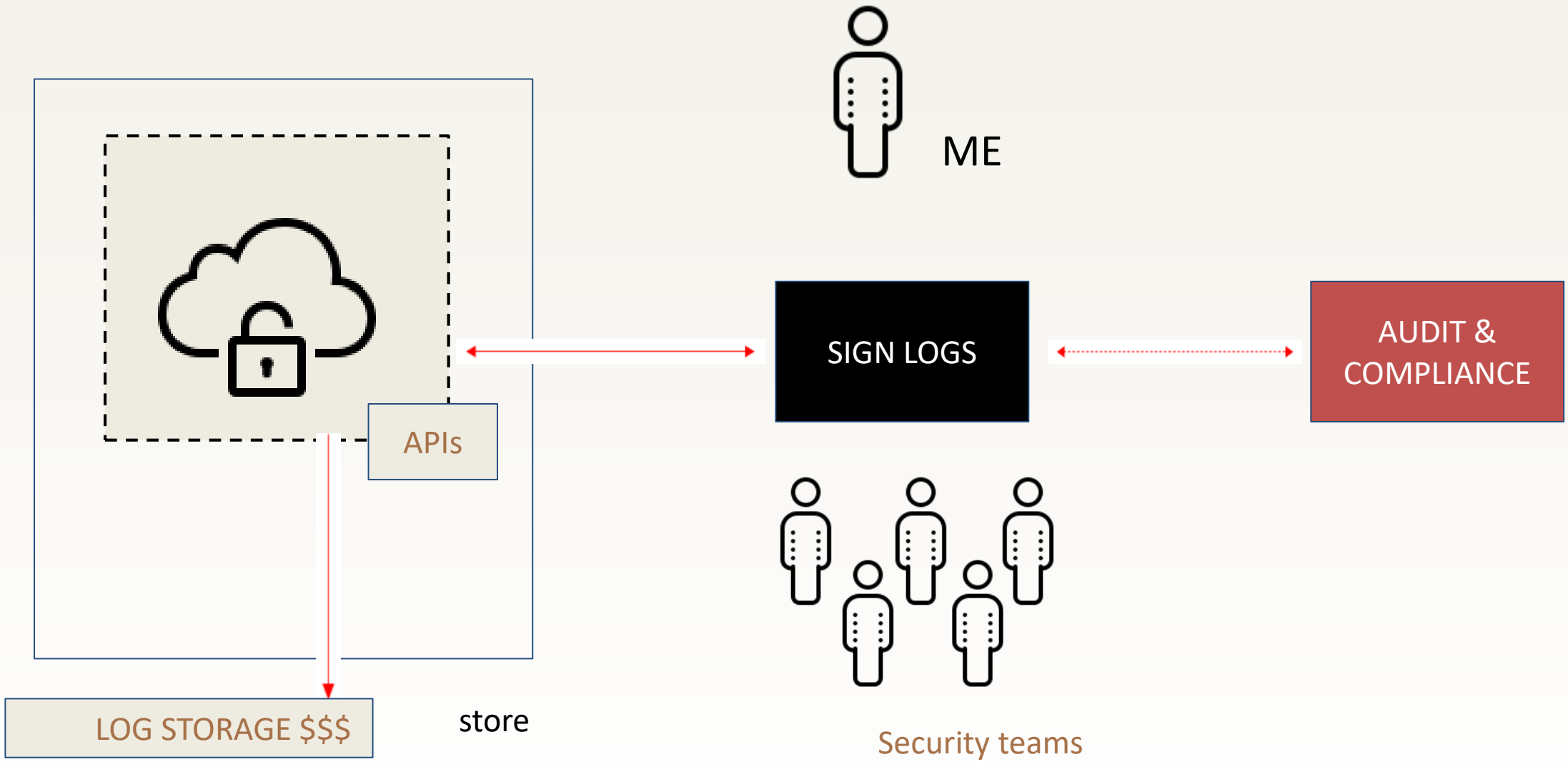
# Guardtime

+ FOUNDED: 2007 in Tallinn, Estonia
+ VALUE PROPOSITION: The *only* blockchain technology platform that is proven to work at scale, used in production to solve data management and cybersecurity challenges.
+ SECTORS: Finance, Insurance, Telecoms, Space, Health, Defense, Government
+ REFERENCES: Lockheed Martin, Airbus, European Space Agency, Maersk, Ericsson, Verizon, UK NHS, Governments (US, China, EU, Estonia, Netherlands, etc.)
+ ACCREDITATION: Technology has been accredited by US, EU and China regulators for deployment on to government networks.



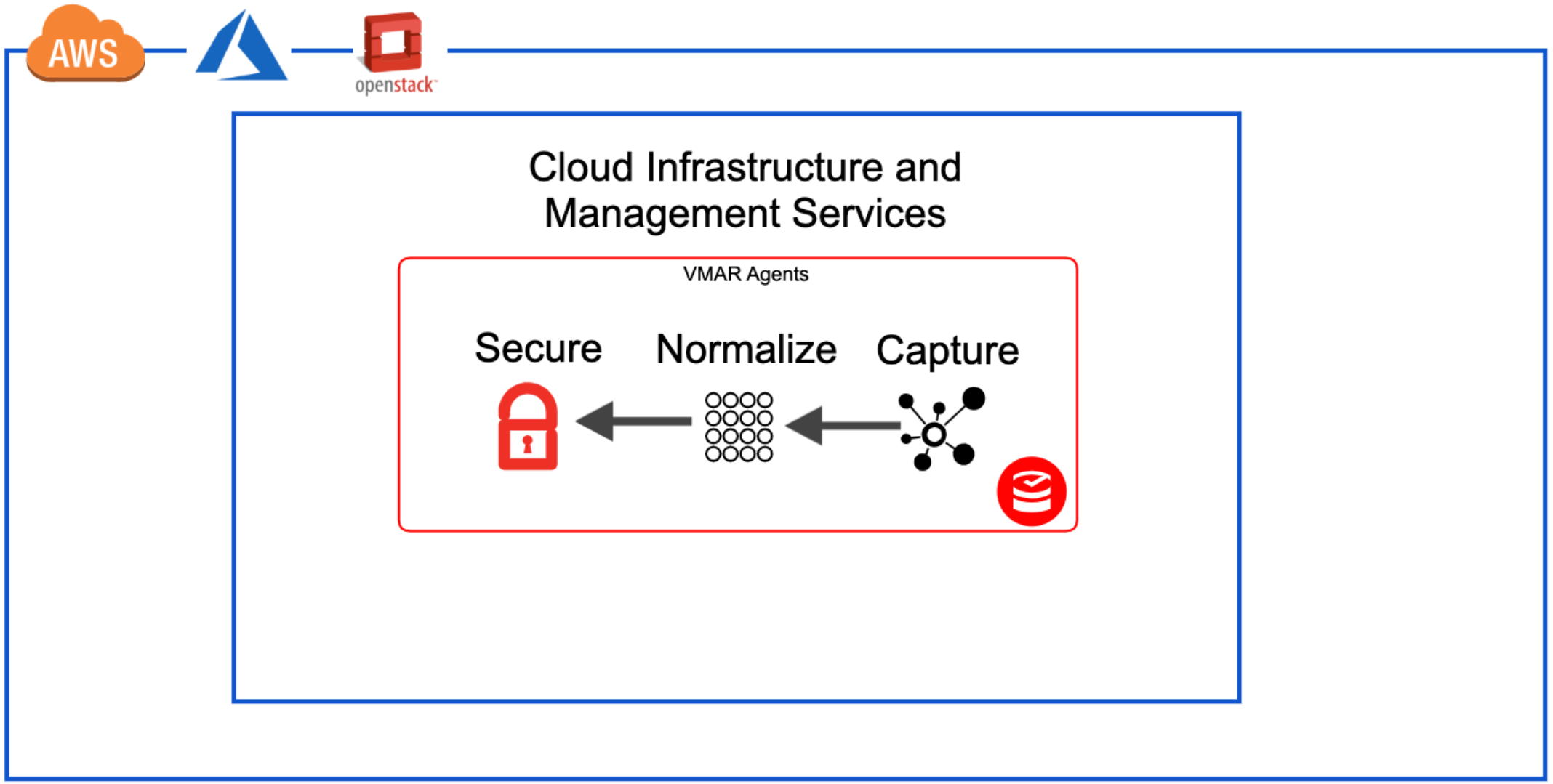

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Public Cloud

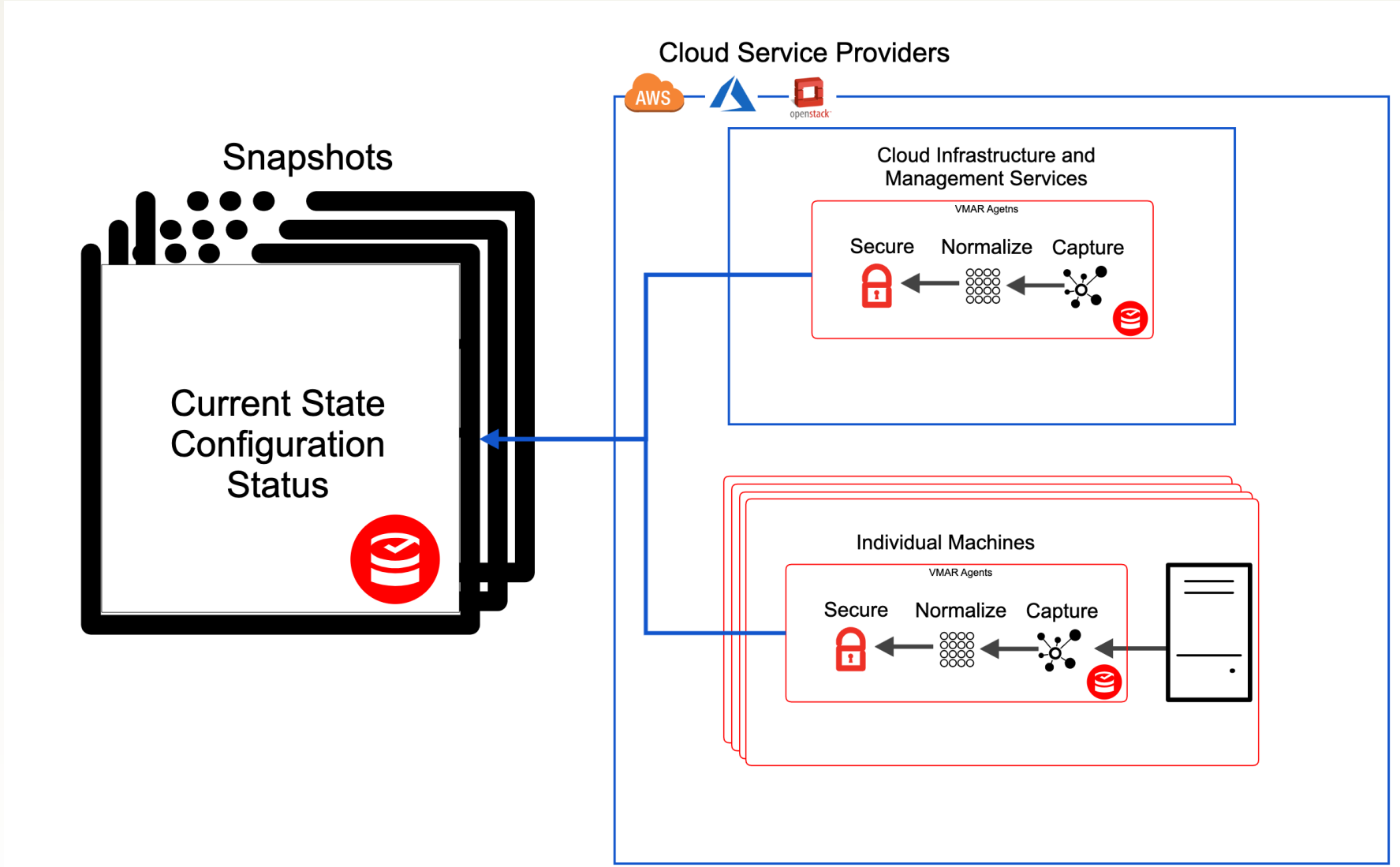



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

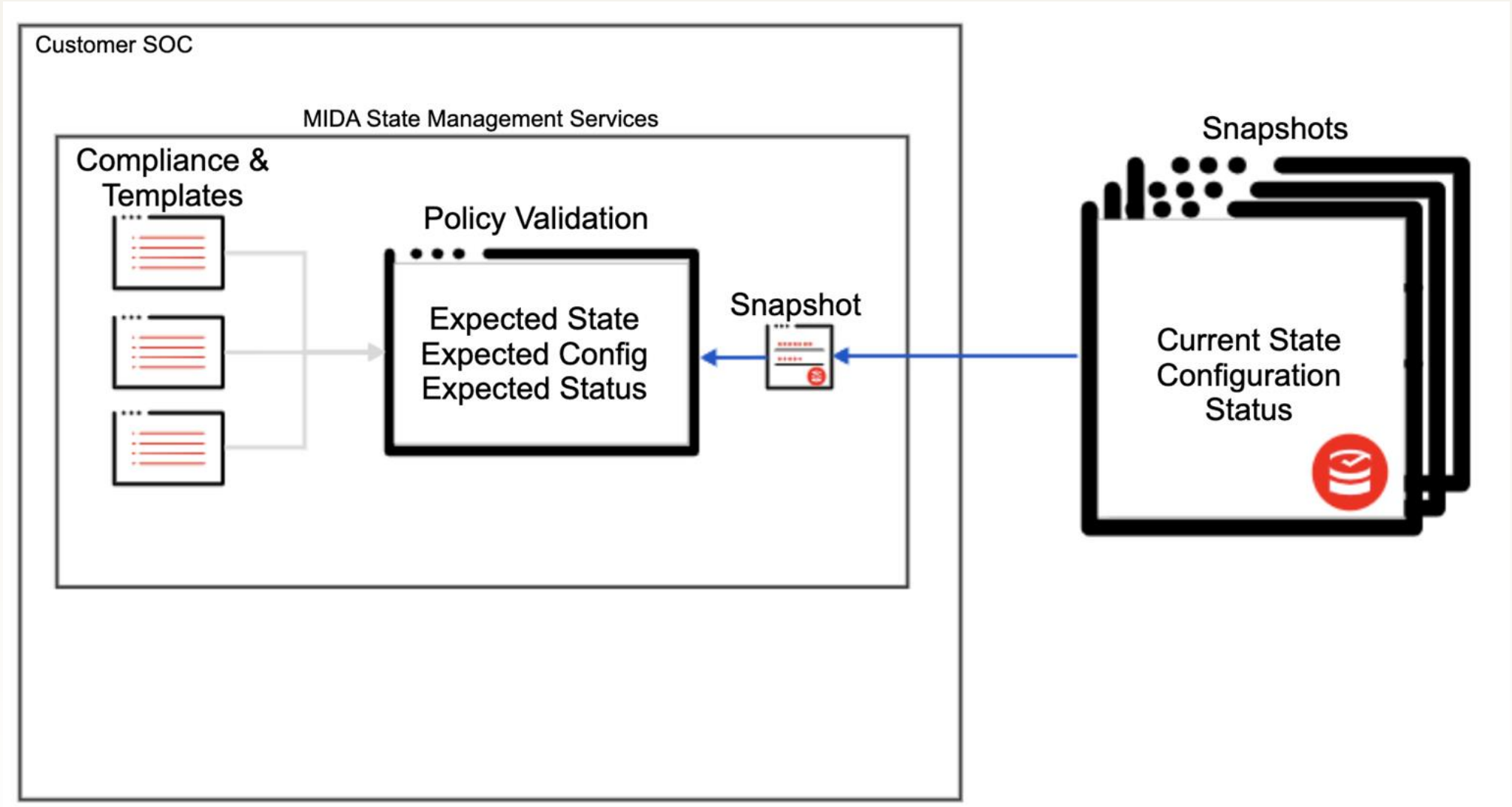
# Cloud services



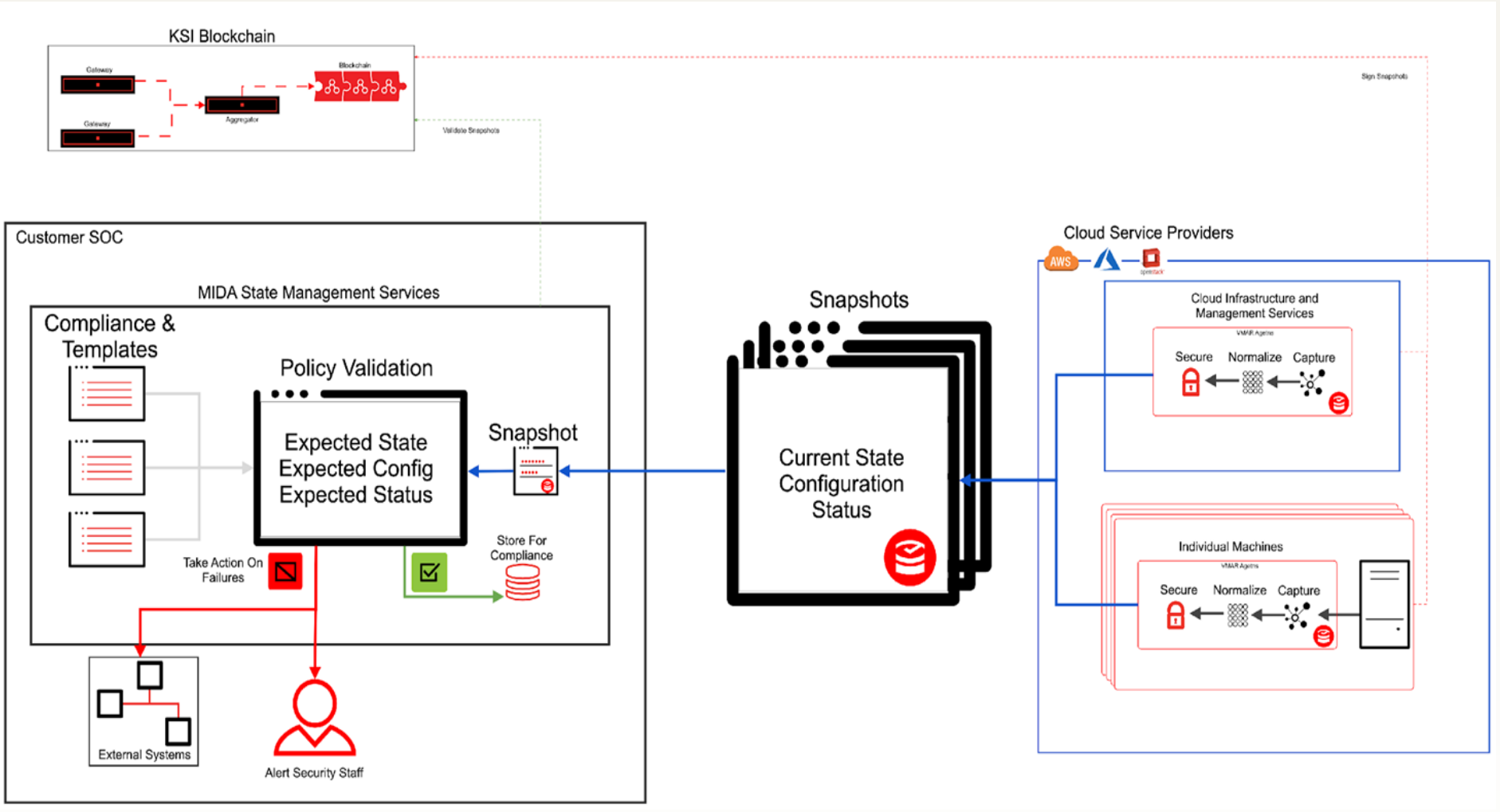

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

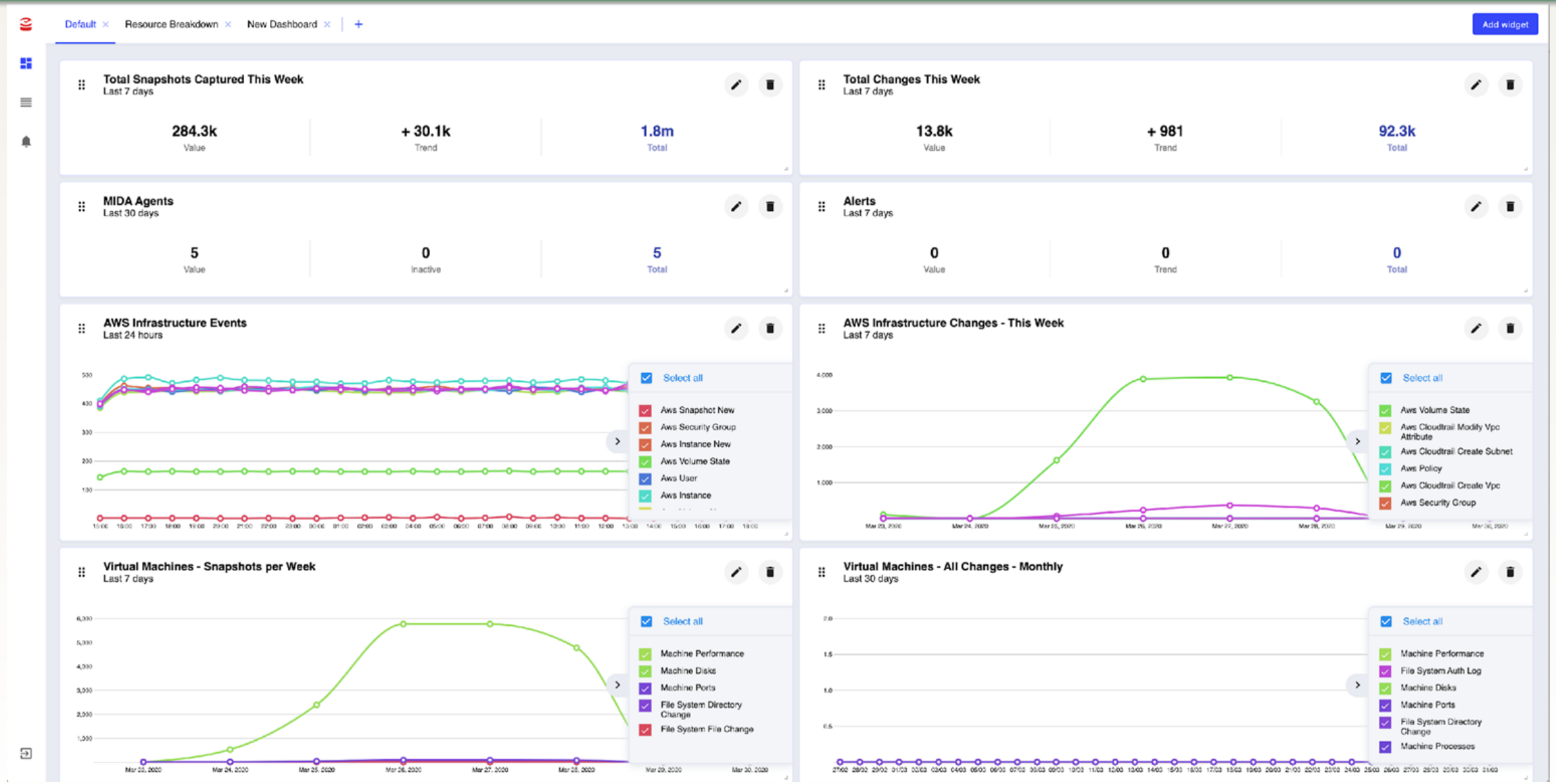



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Dashboard




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# MIDA for Cloud

## EMPOWERS CLOUD OWNERS WITH REAL TIME TRUTH

DECREASED TIME TO DETECTION

AUTOMATE OPERATIONS

SIMPLIFY RESPONSE

CONTINUOUS AUDIT / COMPLIANCE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326

# Fintech Cloud Environment Trust & Security Challenges

For more information:
guardtime.com/mida
MIDA@guardtime.com

guardtime

CRITICAL CHAINS

This project has received funding from the **European Union's Horizon 2020** research and innovation programme under grant agreement **No 833326**

# QA Session

# Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector

**Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector**

**Moderator:**

- **Ivan Tesfai,** *RINA*

**Topics:**

- **Digital Identity and the Biometric Pattern** as a Key Factor in Authentication
- **Regulatory Disharmony & Disruptive Technologies** in the Financial Sector
- **Cyber Security Awareness**: A Pre-emptive Move Against Cyber-Threats
- **Artificial Intelligence, Data Protection & Cybersecurity** in the Fintech Sector

Poll / Q&A

Karmele Garcia
SOTER project coordinator
everis Spain

David Goodman
Cybersec4Europe
Trust in Digital Life

Laurentiu Vasiliu
CS-AWARE
Peracton ltd.

Paolo Balboni
Cyberwatching.eu
ICT Legal Consulting

# Digital Identity and the Biometric Pattern as a Key Factor in Authentication

CRITICAL CHAINS


Karmele Garcia, SOTER project coordinator, everis Spain

- Team leader in everis, an NTT DATA Company
- Technical coordinator of SOTER
- Focused in technical, management and coordination of the work teams
- Extensive experience in the performance of both private and public sector projects and strongly focused on client orientation


SOTER

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SOTER

Cyber Security for Europe

CS-AWARE CYBERSECURITY

cyberwatching.eu
The European watch on cybersecurity & privacy

everis
an NTT DATA Company

Liberbank

InAuth

trunomi
switch on trust

TRILATERAL RESEARCH

UNI GRAZ

Aerospace and Defense
everis

RISE
Research Industrial Systems Engineering

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SOTER

# Digital identity and the biometric pattern as a key factor in authentication

Karmele García

December 14th, 2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

# Digital identity as key element

## What is digital identity?

The digital identity is the Electronic Alter Ego of a person together with all the information and attributes related to it.

One of the challenges associated with digital identity comes from ensuring trust in transactions in a medium such as the Internet.

## IDENTIFICATION vs AUTHENTICATION

### Identification

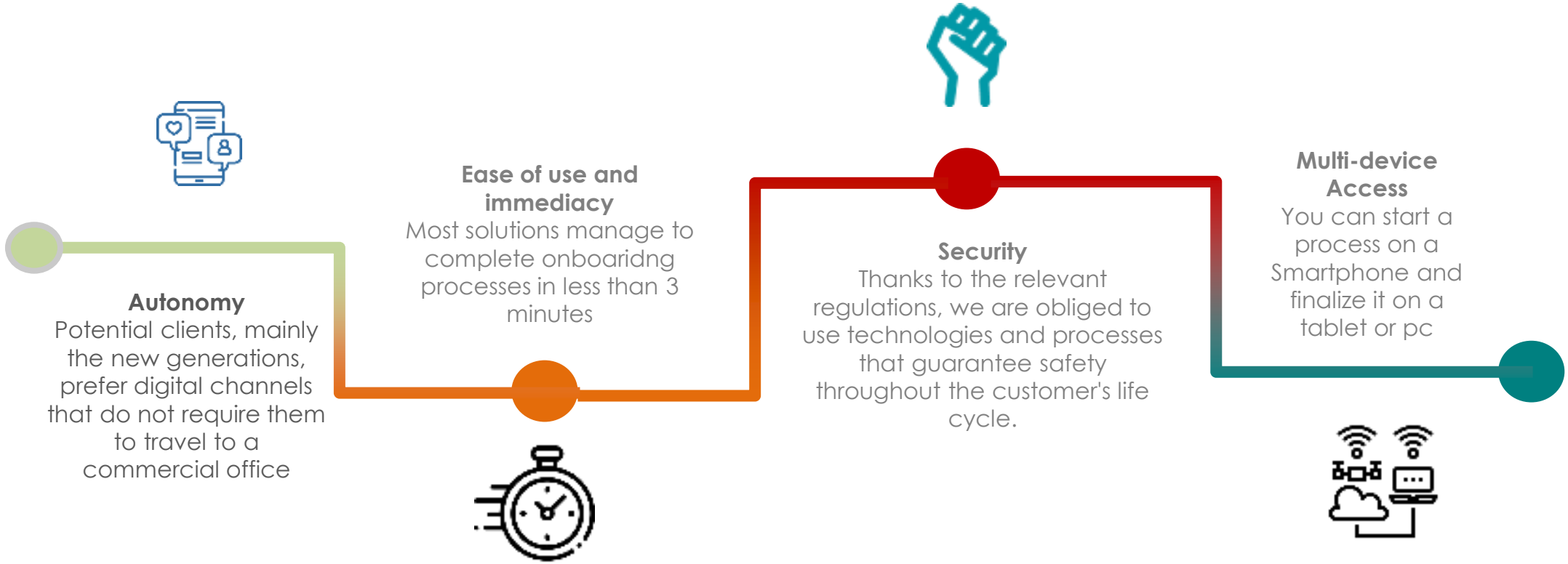
Is the ability to uniquely identify a user of a system or an application running on the system.

### Authentication

Is the ability to prove that a user or an application is really who that person or application claims to be.

# Digital identity as key element

## From the users' point of view…



# Biometrics pattern as key element

## What is biometrics?

Biometrics is the science of analysing the physical characteristics of people.

The objective of using biometrics is to confirm the identity of our clients in order to ensure access to our applications, normal operations and to contract new services.

Biometric authentication is the process in which the data of a customer's characteristics are compared with a pre-established template established in an initial registration, in order to look for similarity.

Facial recognition | Voice recognition | Fingerprint | Behavioral biometrics | Emerging biometrics

# Biometrics pattern as key element

**Depending on the channel in which you operate it is more advisable to use some biometrics or others**

### Non-presential channels

| Type | Mobile | Web | By telephone |
|---|---|---|---|
| Facial | Adequate | Adequate | Null |
| Dactilar | Adequate | Null | Null |
| Iris/Retina | Limited | Limited | Null |
| Voz | Adequate | Limited | Adequate |

### Presential channels

| Type | Office |
|---|---|
| Facial | Adequate |
| Dactilar | Limited |
| Iris/Retina | Limited |
| Voz | Adequate |

Adequate: the type of biometrics reasonably and completely covers the needs of the channel
Limited: the type of biometrics covers the needs of the channel in a technically limited way or would require proprietary hardware and additional support for reasonable security beyond the customers' own standard devices.
Null: the type of biometrics cannot be used in this channel or has a very high limitation.

# Biometrics pattern as key element

## User experience is influenced by registration types

| Biometrics type | Complexity of the process |
|---|---|
| Facial | Low |
| Dactilar | Medium |
| Iris/Retina | High |
| Voz | Medium |

High: the user interacts in the registration process and the interaction is high and complex due to its technical requirements.
Medium: the user interacts in the additional registration process but the interaction is minimal and simple due to its technical requirements.
Low: the user does not interact in the registration process. The registration could be done automatically and without extra steps in the customer's KYC enrolment process.

# Biometrics pattern as key element

## Benefits of using biometric patterns

### Security

Computers have the ability to effectively evaluate user identities, in order to allow an operation to be completed.

### Easy to use

Compared to traditional systems using cards, keys and passwords

### Can’t be forgotten

They cannot be lost or forgotten. Nor can they be forged or stolen.

### Accesibility

No one is excluded, we all have unique biometric characteristics.

### Increased privacy

It helps to increase the security of the transmission of customers' personal data, as it encrypts them using a unique and personal key

### Cost reduction

Maintenance costs are reduced.

# Thank you

Karmele García

miren.karmele.garcia.garcia@everis.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

# Regulatory Disharmony & Disruptive Technologies in the Financial Sector

David Goodman, Cybersec4Europe, Trust in Digital Life Association

- Senior consultant with Trust in Digital Life association
- Cybersec4Europe representative as leader in Open Banking roadmapping and demonstrators as well as communication and dissemination
- Consultant working in digital transformation, specifically the areas of identity management and security, data protection and privacy regulation as well as emerging technologies
- Wide range of companies in Europe and North America from start-ups to global brands as well as University College of London
- Principal consulting analyst with TechVision Research, chief evangelist with iGrant.io, and, until recently, executive director of the Open Identity Exchange (OIX)

Cyber Security for Europe

# Regulatory Disharmony & Disruptive Technologies in the Financial Sector

David Goodman, Trust in Digital Life

14 December 2020

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

# About CyberSec4Europe

Regulatory Disharmony

Disruptive Technologies

CyberSec4Europe is a research-based consortium …

… with 50+ partners in 22+ European countries …

… working across four different but inter-related areas with a strong focus on openness and citizen-centricity …

… one of four projects piloting a European Cybersecurity Competence Centre and network of competence centres

Open Banking is a featured topic:

- A demonstrator use case
- In short, medium and long term roadmapping
- Involving Groupe BPCE, ABI Lab, UPS-IRIT and NEC as well as CaixaBank, Poste Italiane

Cyber Security for Europe

# About CyberSec4Europe

## Regulatory Disharmony

## Disruptive Technologies

# Regulatory Divergence

Differences in national regulations are not converging quickly enough.

Leading international companies practise ‘regulatory arbitrage’ choosing the most favourable regulatory environment – where

- the control of data is weakest
- the regulator most tolerant
- the costs least
- the processes most electronified
- their most relevant regulations are interpreted in the most industry-friendly way.

Hence, in the “single” market, there is no level playing field and large regulatory divergence.

# Regulatory Divergence

This fragmented situation massively favours large companies which have large compliance offices to analyse the complexity and can set up their headquarters where it suits them best and give them the biggest strategic advantage over competitors.

And then there will be the increasing regulatory divergence between continental Europe and the UK due to Brexit …

# PSD2 vs GDPR

Cyber Security for Europe

Both the GDPR and PSD2 share the same objectives – to put customers in control of their own data and to keep that data safe.

> *But because they were designed independently of each other, there are deployment incongruities that could lead to security holes and vulnerabilities.*

The link between PSD2 and GDPR is not just about the handling of money but also the management of personal data.

> *The discernible weaknesses are in ensuring that a third-party respects the GDPR and is adequately compliant as well as ascertaining where liability lies if there is any data breach.*

# PSD2 vs GDPR

(1) Under PSD2, third parties are able to access customer account information directly, provided they have the customer's explicit consent, and enable the customer to exercise their right to data portability under the GDPR.

*However, in the payment process, 'silent parties' , such as persons who have a bank payment account to which the PSU transfers money through the PSP, do not have a direct contractual relationship with the PSP..*

(2) In the GDPR the data controller (the bank or ASPSP) is responsible for safeguarding customer data with the threat of considerable fines if there is a failure to do so.

*It's not clear which party is responsible for obtaining the customer's consent and, significantly, which organisation – the PISP or the ASPSP – is culpable if the customer suffers any loss due to a data breach or cyber attack.*

# PSD2 vs GDPR

(3) PSD2 states that PISPs must not use, access or store any data for purposes other than the provision of the payment initiation service explicitly requested by the payer.

*Consequently, a PISP is not entitled to use the data collected other than for providing payment initiation services, even if the PISP had the PSU's consent under the GDPR.*

(4) In making a payment to a third party, unless the third party is trusted by the PSU, the PISP opens up a potential vulnerability in terms of financial loss but more importantly a lack of certainty in case of a data breach or data misuse.

*PSD2 forbids banks sharing "sensitive payment data" with third parties, but there is no clear definition of what it is. Without clarification banks will err on the side of safety, particularly from the perspective of GDPR compliance.*

# A European Strategy For Data

*A European Strategy For Data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty. Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping companies and individuals who generate the data in control.*

## Digital Finance Package, adopted on 24 September 2020

## Digital Finance Strategy

- removing fragmentation in the Digital Single Market
- adapting the EU regulatory framework to facilitate digital innovation,
- promoting a data-driven finance
- addressing the challenges and risks with digital transformation, including enhancing the digital operational resilience of the financial system.

Cyber Security for Europe

# About CyberSec4Europe

# Regulatory Disharmony

## Disruptive Technologies

# The Impact of Technology (1/2)

The impact of technologies on banking and payments has been massive for some time, from the start of the Internet to multimedia/multi-channel, to mobile and NFC (contactless).

- QR codes, the basis of an Asian explosion of apps
- Biometrics, face/finger recognition to improve user experience and security
- Wearables, where your watch, you glasses, your ring are connected and can make payments with a blink or a touch

# The Impact of Technology (2/2)

- BLE, enabling beacons to pay automatically as you leave a shop, for example, Amazon Go - and general wireless device connection
- IoT, where your fridge will replenish food on your behalf
- “connectedeverything” such as cars paying for toll gates as they pass)
- APIs, enabling “Open X” – the interconnection and mashup across all industries)
- And more – AI, cloud, DLT et al.

# Quantum

The impact of quantum computing on banking will be gigantic - several banks have been exploring the potential for a year or two

- Only a few, expensive, qubits can currently be managed at a time but when they do NP-complete problems are suddenly “easy”.
- For security applications this would mean that RSA encryption is broken and previously secure systems which it would now take centuries to crack with the biggest supercomputers become open.
- BBVA expect it to fundamentally change the face of banking

# Summary

## Regulatory Disharmony

The areas of regulatory disconnect between PSD2 and the GDPR still have not been satisfactorily ironed out, and we haven't gone into AML5, eIDAS, MiFiD and many others.

## Disruptive Technologies

Technological innovation provides shiny new toys with immense benefits to the financial sector but without due consideration can add more complexity and unforeseen difficulties

Cyber Security for Europe

# Thank you

david@trustindigitallife.eu

cybersec4europe.eu

# Cyber Security Awareness: A Pre-emptive Move Against Cyber-Threats

CRITICAL CHAINS


Laurentiu A. Vasiliu, CS-AWARE, Peracton Ltd.


- CEO and Founder of Peracton Ltd.
- Within CS-AWARE project, he and his Peracton team ensured the development of the 'data analysis' component as well as dissemination and commercialization effort
- Drove the creation of a new spin-out from the project, namely "CS-AWARE Corporation OÜ"
- experienced IT project manager and researcher that managed and ensured the execution of large R&D IT projects

CS-AWARE CYBERSECURITY

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SOTER

Cyber Security for Europe

CS-AWARE CYBERSECURITY

cyberwatching.eu
The European watch on cybersecurity & privacy

# CS-AWARE

## Cybersecurity Awareness: a pre-emptive move against cyber-threats

LAURENTIU VASILIU

**PERACTON LTD**

14-12-2020

**HORIZON 2020**

PROJECT 740723

CS-AWARE CYBERSECURITY

European Commission

Peracton

# Project Overview

- **Provide a cybersecurity situational awareness solution for local public administrations** in line with the current and upcoming legal cybersecurity framework in the European Union and its member states**.**
- **Advance the automation of cyber incident detection, classification and visualisation to provide situational awareness.** This includes socio-technical system analysis, data collection, data analysis and decision making as well as the visualisation of the findings.
- **Include a cybersecurity information exchange framework that embraces the collaboration and cooperation initiatives of European cybersecurity strategies.** This includes the utilisation of cybersecurity data for threat detection as well as sharing of newly discovered cyber incident data.
- **Illustrate that cyber situational awareness is a key technology in cybersecurity by building advanced features like system self-healing on top of the situational awareness capabilities**
- **Evaluate and validate the user needs through end-user involvement and pilot testing.**

# Cyber-threats awareness in big data

- **Potential/Actual Threats - needles in a haystack: how to find them fast ?**
  - Unique changes may not be suspicious by themselves
  - Various (sometimes unusual) work behaviours
    - Hours, locations, IPs, data volumes, etc
  - Various (sometimes unusual) operations
    - Delete, copy, move, upload, download
  - Apparently legitimate actions
  - BUT: when combined/correlated some look suspicious!
    - Unusual /suspicious patterns
    - Domain dependent

# eGov case studies: lessons learned

- **Dedicated resources/skills required to implement cybersecurity analytics**
- **A cybersecurity solution implementation increases the organization's self-understanding and cyber knowledge**
- **GDPR compliant**
- **Dedicated processes modelling required**
- **Not a plug & play solution – tailoring required for each implementation**
- **However, 95% of CS-AWARE platform stays unchanged.**
  - New patterns
  - New data integration and data pre-processing required.

# Pivoting between industries: from eGov to Finance – cyber-threats

- **Switching domain means:**
  - Different data
  - Different threat concepts
  - Different data volumes
  - Different processes structures
- **CS-AWARE platform is domain independent:**
  - New cyber-patterns
  - New data adaptors
  - New type of threats to be defined

# How can finance/banking can benefit from CS-AWARE

- **A ready to implement system**
  - In the cloud / private cloud / local implementation
- **3 years of R&D**
- **2 eGov successful pilots in Roma Capitale/Italy and Larissa/Greece**
- **Most of the eGov lessons learned (technical/modelling) can be of use for finance/banking world**
  - Similar or related type threats
  - Similar technologies to protect
  - Similar internal processes modelling challenges

# Conclusion & future steps

- **CS-AWARE know-how and expertise gathered is unique**
  - Approach/technologies/vision
- **Working platform, live in pilot sites**
- **Work continues via its new spin-out!:**
  - CS-AWARE Corporation OÜ, Estonia, 2020
- **Consortium team regrouped around the spin-out**
- **Currently raising funds and looking for prospects**
- **Open to looking at Finance/Banking CS-AWARE new implementations**

## For more details please contact:

laurentiu.vasiliu@peracton.com

# Artificial Intelligence, Data Protection & Cybersecurity in the Fintech Sector

Paolo Balboni, Cyberwatching.eu, ICT Legal Consulting

- Founding Partner of ICT Legal Consulting
- Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law
- Top tier European ICT, Privacy & Cybersecurity lawyer and serves as Data Protection Officer (DPO) for multinational companies
- Lead Auditor BS ISO/IEC 27001:2013
- Member of the EUMETSAT Data Protection Supervisory Authority and Co-Chair of the Cloud Security Alliance Privacy Level Agreement (PLA)
- Recommended Lawyer ranked by The Legal 500 EMEA 2020 in the areas of Data Privacy and Data Protection and Industry Focus: TMT

# Artificial Intelligence, Data Protection & Cybersecurity in the Fintech Sector

**Prof. Dr. Paolo Balboni** – Founding Partner ICTLC
Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre for Privacy & Cybersecurity at Maastricht University
E: paolo.balboni@ictlegalconsulting.com
M: +39 335 668 5806
balbonipaolo
www.paolobalboni.eu

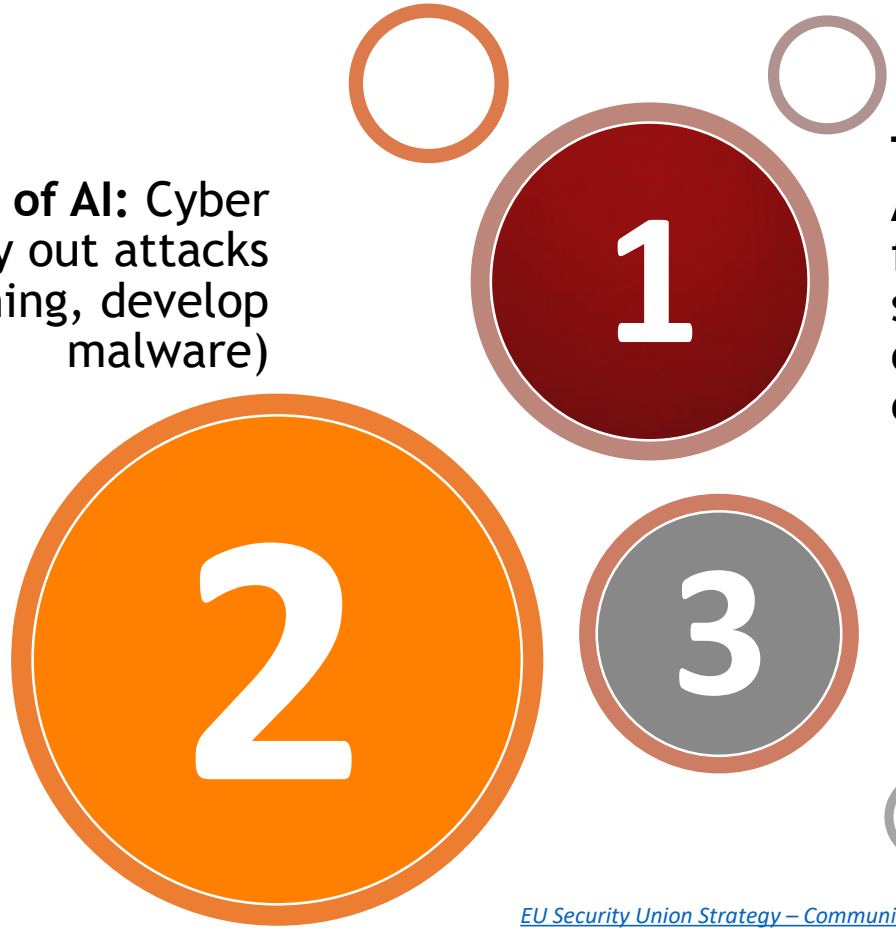
Milan - Bologna - Rome - Amsterdam – Madrid - Helsinki - Melbourne

# Agenda

1. Multiple dimensions of AI and cybersecurity
2. EU Policy landscape
3. FinTech: Impact of AI & cybersecurity on the sector
4. Cyber attacks and data breaches
5. The EU in the fight against cybercrime in the financial sector
6. Risk management and governance for financial institutions
7. Concluding remarks

# Multiple dimensions of AI and cybersecurity

**Offensive use of AI:** Cyber criminals use AI to carry out attacks (identity fraud, phishing, develop malware)




**Targeting and exploiting AI:** Increasing proliferation of AI in finance (and other sensitive sectors) makes need to establish cybersecurity requirements for AI ever-more relevant

**Defensive use of AI:** AI is used to fight against cyber-attacks (can be applied in the financial sector as a preventative measure)

*EU Security Union Strategy – Communication from the Commission to the European Parliament, the European Council, The Council, The European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. Brussels 24.7.2020*

# EU Policy landscape

*"Cybersecurity is the foundation of trustworthy Artificial Intelligence solutions. It will serve as a springboard for the widespread secure deployment of AI across the EU."* - Juhan Lepassaar, Executive Director ENISA

**Trust** between customers and financial institutions / banks and their related apps

AI + Cybersecurity = Trust = **Benefits for society and the economy**

No concrete baseline for cybersecurity in AI (coming soon)

| Main legal issue/area | EU legislation applicable |
|---|---|
| Algorithmic transparency | Regulation 2016/679; Directive 206/680 |
| Unfairness, bias and discrimination | Article 2, 3(3), 9 TEU; Article 10 TFEU; Article 20-26 EU Charter on Fundamental Rights; Council Directive 200/78/EC; Council Directive 2000/43/EC; Council Directive 2004/113/EC; Directive 2006/54/EC, Council Directive 79/7/EEC, Directive 2010/41/EU, Council Directive 2010/18/EU, Regulation (EU) 2016/679, Directive (EU) 2016/680, Directive (EU) 2016/681. |
| Intellectual property issues | Article 118 TFEU, Article 17 (2) EU Charter on Fundamental Rights; Directive 2001/29/EC; Directive 2006/115/EC; Directive 2001/84/EC; Directive 2009/24/EC; Directive 2004/48/EC; Directive 96/9/EC; Directive 2012/28/EU; Directive 98/71/EC; Regulation (EU) No 1257/2012; Regulation (EU) 2017/1001; Directive (EU) 2016/943; |
| Legal personhood of AI | Not covered. |
| Vulnerability and cybersecurity | Directive (EU) 2016/1148; Regulation (EU) No 910/2014; Directive 2013/40/EU; Regulation (EU) No 526/2013; Directive 2002/58/EC |
| Impact of AI on workers | Article 3(1)(3) TEU; Article 9, 107(3)(a), Articles 145-166 TFEU; Articles 14-15, 27-32 EU Charter of Fundamental Rights; Regulation (EU) No 1304/2013 |
| Privacy and data protection | Articles 7-8 EU Charter of Fundamental Rights; Regulation (EU) 2016/679; Directive (EU) 2016/680; Directive (EU) 2016/681; Directive 2002/58/EC |
| Liability | Articles 4(2)(f), 12, 114 and 169 TFEU; Articles 38, 47 EU Charter of Fundamental Rights; Council Directive 85/374/EEC |
| Accountability for harm | Regulation (EU) 2016/679 |

Table 5: AI Legal issues and examples of relevant EU legislation, SIENNA project, as seen in EPRS, European framework on ethical aspects of artificial intelligence, robotics and related technologies

# Shortcomings of European data protection framework for AI

Necessity to address risks brought about by use of AI (including cyber risks!) for adoption to flourish

Need for an adequate safety and liability framework for AI

Must prevent abuse (hacking of AI, manipulation of data) AND at the same time ensure consumer safety and effective redress mechanisms

The EU legislative framework should address **"possible risks raised by the use of, and interactions with the technology, including cybersecurity concerns."** (Coordinated Plan on Artificial Intelligence)

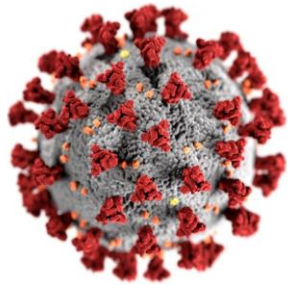
The European Commission has already suggested that cybersecurity requirements for AI should be specified as well as certified under the proposed European Cybersecurity Certification Framework, noting that for:

*"businesses acting in security relevant fields (e.g. **financial institutions**, producers of radio-active materials, etc.) the use of certain AI products and processes serves public interest therefore their use may be made compulsory."*

# FinTech: impact of AI & cybersecurity (and coronavirus) on the sector

FinTech sector is characterized by its high level of innovation inside of a **complex ecosystem** comprised of banks, financial service providers, and start-ups, etc. which are driven by data.

Attractive target for cybercrime, presenting risks to the rights and freedoms of data subjects and to their financial assets.



"The coronavirus pandemic has been connected to a 238% surge in cyberattacks against banks." - ZDNet

"Financial organizations experienced a massive uptick in cyberattack attempts between February and April this year — the same months in which COVID-19 began to spread rapidly across the globe" - Modern Bank Heists report



Alongside a 72% rise in the use of Fintech apps in the period of the coronavirus, so too have malware and ransomware been driven by the pandemic. - Forbes

# Cyber attacks and data breaches

**Dave:** US FinTech giant suffered a major "breach of customers' personal data via a third party supplier, after researchers found a database containing millions of records for sale online." Allegedly more than 7.5 million records (associated to 3 million addresses) are for trade on the dark web.

**2014 JPMorgan Chase data breach:** allegedly more than 83 million accounts and 7 million small businesses were impacted. Exposed data in this case consisted of names, email addresses, physical addresses and phone numbers, something which is known to opening victims to phishing attempts.

**Unicredit: EUR 600.000 fine** (Italian DPA) following a complex investigation into a data breach caused by abusive access to the personal data of over 700.000 customers which took place between April 2016 and July 2017.

**Cense AI:** 2.5 million medical records had been leaked, compromising information such as insurance records, medical diagnoses, and payment records. It is said that researcher Jeremiah Fowler, discovered "two folders of medical records available for anyone to access on the internet. The data was labelled as 'staging data' …hosted by artificial intelligence company Cense AI, which specializes in 'SaaS-based intelligent process automation management solutions.'"

# Cyber attacks

As distributed denial-of-service attacks, malware, phishing and ransomware attacks increase over time and FinTech solutions become more established and widespread, **innovation in the cybersecurity field will become ever-more important to protect users from financial cybercrimes.**

## Mobile banking malware surged

Mobile applications designed to steal payment data, credentials and funds from victims' bank accounts increased by 50% in the first half of 2019.[14] Traditionally, threat actors have used phishing techniques to gain bank credentials, either by displaying a fake page that mimics the bank's login page or by introducing fake mobile apps that resemble the original banking apps. However, in 2019, cybercriminals became more creative, as in the case of Trojan-Banker.AndroidOS.Gustuff.a, which was able to control a legitimate banking app by misusing the operating system's accessibility functions, thereby automating malicious transactions.[15] New versions of mobile financial malware were commonly found for sale in underground forums[15] and new evasion techniques were continuously being developed. A notable new addition discovered in 2019 was the ability of malware to use motion sensors and be triggered only when a smartphone is moving, as used by the mobile banking trojanAnubis in an effort to detect a sandboxed environment.[16] The most popular banking malware during 2019[11] was Asacub (44,4%), Svpeng (22,4%), Agent (19,1%), Faketoken (12%) and Hqwar (3,8%).

ENISA Threat Landscape 2020 – Malware
https://www.enisa.europa.eu/publications/malware

# The EU in the fight against cybercrime in the financial sector

In 2018, a cybercrime syndicate that infiltrated over 100 financial institutions in 40 countries, resulting in losses of over EUR 1 billion was arrested in Spain! Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist.

In September 2020, an operation supported by Europol and Eurojust in cooperation with Estonia, Lithuania, and Romania successfully dismantled a criminal organization that carried out phishing, fraud, and money laundering activities. Using the obtained credentials, the organization made unauthorized wire transfers to a number of bank accounts in EU countries, stealing more than EUR 200.000 from nearly 600 individuals.

One of the three mandates of Europol's European Cybercrime Centre (EC3) is that of countering payment fraud. Thanks to its Joint Cybercrime Action Taskforce (J-CAT), Europol has already "supported several high-profile cybercrime operations and investigations, such as Operation Imperium, which targeted an organised crime network active in payment fraud."

# Risk-based approach

The responsibility of the controller to **ensure** and **demonstrate** compliance is challenging:

- Risk-based approach in security: **assessing the risk** of the processing activities; and implementing **security and organisational measures**
- European Union Agency for Cybersecurity recently published a tool for carrying out a risk assessment for the security of personal data processing


# Risk management and governance for financial institutions

As the sector is ripe with risk, financial institutions must ensure that they adequately govern privacy, data protection and cybersecurity matters and have appropriate organizational and technical measures, procedures and policies in place.

Organizational governance of cyber risk must take into consideration the vast number of players involved in the provision of financial services (supply chain).

Chief Information Security Officer (CISO) and risk officers can help ensure Resilience.

*"The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs" (See NIST SP 800-39 under Information System Resilience and NIST SP 800-53 Rev. 4 under Information System Resilience).*

# Risk management and governance priorities to be considered by organizations in the financial services sector

1. Provide products and services that are designed and developed - *along the whole value chain* - according to the principles of **Data Protection and Security by Design**.

2. Promote an **organizational culture of cybersecurity**, e.g., employee awareness and alertness regarding data protection and cyber risks.

3. Use of **Integrated Data Protection Impact Assessments** (DPIAs) and Security Risk Assessments to identify and manage real or potential risks.

4. Follow the **Zero-trust security approach** (verifying any actor internal or external to the perimeters before granting access).

5. Ensure **resilience** and the ability, also **of supply chain partners**, to quickly respond to both actual breaches and any potential threats and risks that may arise.

6. Invest in **AI-enabled cyber protection systems**.

7. Develop new **innovative approaches for risk management** to address current and future cyber challenges.

# Concluding remarks

**55% of people in the EU are concerned about their data being accessed by criminals and fraudsters.**

**EU Security Union Strategy:**

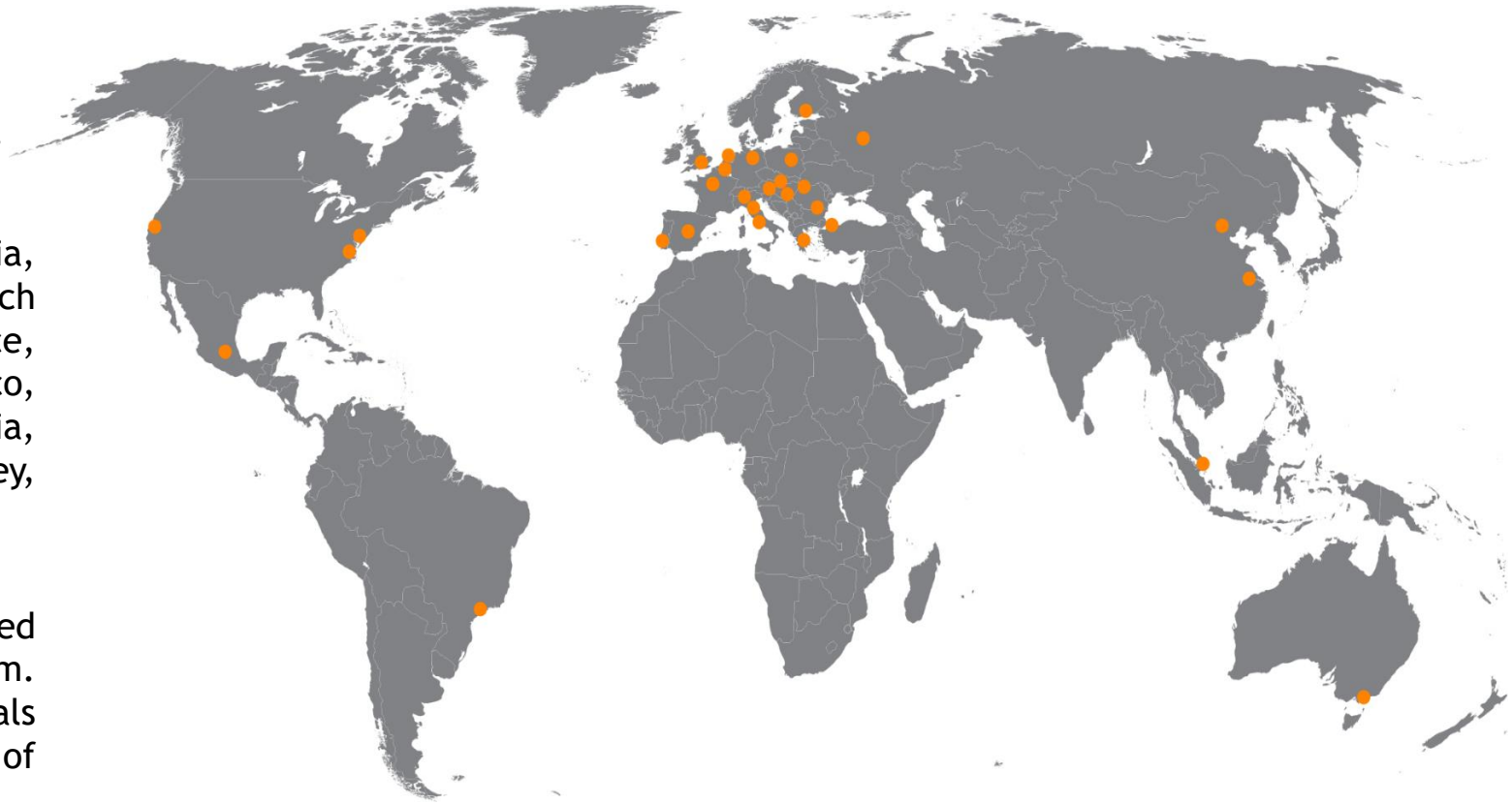
- Third country industrial policy, "combined with the continued cyber-enabled theft of intellectual property, are changing the strategic paradigm for protecting and advancing European interests."
- *"Industrial espionage has a significant impact on the EU's economy, jobs and growth: cyber theft of trade secrets is estimated to cost the EU €60 billion."*
- The *"Use of Artificial Intelligence, new technologies and robotics will further increase the risk that criminals exploit the benefits of innovation for malicious ends."*

# The Firm

**ICT Legal Consulting is an international law firm with offices in Milan, Bologna, Rome, Madrid, Amsterdam, Helsinki and Melbourne.**

The firm is present in 28 other countries: Albania, Austria, Belgium, Brazil, Bulgaria, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Luxembourg, Macedonia, Mexico, Moldova, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Sweden, Switzerland, Turkey, the United Kingdom and the United States.

In each of these countries we have established partnerships with more than one law firm. Depending on the task, we contact the professionals who are best able to meet the specific needs of customers.



# In Detail

ICT Legal Consulting is an international law firm. It was established by Paolo Balboni and Luca Bolognini, who have successfully assembled a network of trusted, highly-skilled lawyers and cyber security advisors specialized in the fields of Information and Communication Technology, Privacy, Data Protection/Security and Intellectual Property.

We have developed significant expertise working with multinationals and companies in the communications, media & entertainment, IT, healthcare, pharmaceutical, fashion, food & beverage, energetic and smart grids, banking/financial services, automotive, industrial manufacturing and eGovernment sectors.

In more detail, we provide complete assistance in the fields of personal data protection, IT contracts, eHealth, eCommerce, eMarketing, advertising, cloud computing, web 2.0 service provider liability, internet and mobile content, online gambling, online gaming, electronic signatures, digital document retention and online storage, renewable energy and administrative responsibility and corporate liability.

We also deal with the protection and management of intellectual property and competition rights: copyright, design, patents, unfair competition, consumer protection and media law, unfair commercial practices, misleading and comparative advertising, the labeling and sale of foodstuffs.

Our professionals regularly advise multinational companies on legal and technical issues, offering a strategic and holistic approach. Our goal is to turn legal advice into a competitive advantage for our clients.

# Main Practice Areas

# Services

- Privacy and data protection
- Cloud Computing
- E-commerce
- Information Technology
- Cybersecurity
- Big Data & Analytics
- Internet of Things
- Intellectual property
- Marketing and advertising
- Legal training & e-learning
- Telecommunications
- E-Health

# Our History

| | |
|---|---|
| 2011 | ICTLC is founded by P. Balboni and L. Bolognini in Milan |
| 2012 | Inauguration of the Bologna office |
| 2013 | The Rome office is operational |
| 2014 | The international hub is established in Amsterdam |
| 2015 | Our services are offered in 21 countries |
| 2016 | The IT/Security practice is launched |
| 2017 | The new Milan office is operational |
| 2018 | Over 45 high-skilled professionals are active worldwide |
| 2019 | The Helsinki (Finland) office is operational |
| 2020 | ICTLC Australia and ICTLC Spain are established |

# The People

ICT Legal Consulting relies on more than 70 highly-skilled lawyers worldwide to carry out our clients' daily operations.

We are capable of scaling up anytime required. The core team consists of 40 selected professionals.

# Paolo Balboni Prof. Dr. Founding Partner

**Paolo Balboni, Ph.D., is a top tier European ICT, Privacy & Data Protection lawyer and serves as Data Protection Officer (DPO) for multinational companies. Professor of Privacy, Cybersecurity, and IT Contract Law. Lead Auditor BS ISO/IEC 27001:2013.**

Paolo Balboni (qualified lawyer admitted to the Milan Bar) is a Founding Partner of ICT Legal Consulting (ICTLC), a law firm with offices in Milan, Bologna, Rome, Helsinki, an International Hub in Amsterdam, and multiple Partner Law Firms around the world.

Together with his team he advises clients in the fields of Personal Data Protection, Data Security, Information and Communication Technology (ICT) and Intellectual Property Law, also acting as Data Protection Officer in outsourcing. Paolo Balboni has considerable experience in Information Technologies including Cloud Computing, Big Data, Analytics and the Internet of Things, Media and Entertainment, Healthcare, Fashion, Insurance, Banking, Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT).

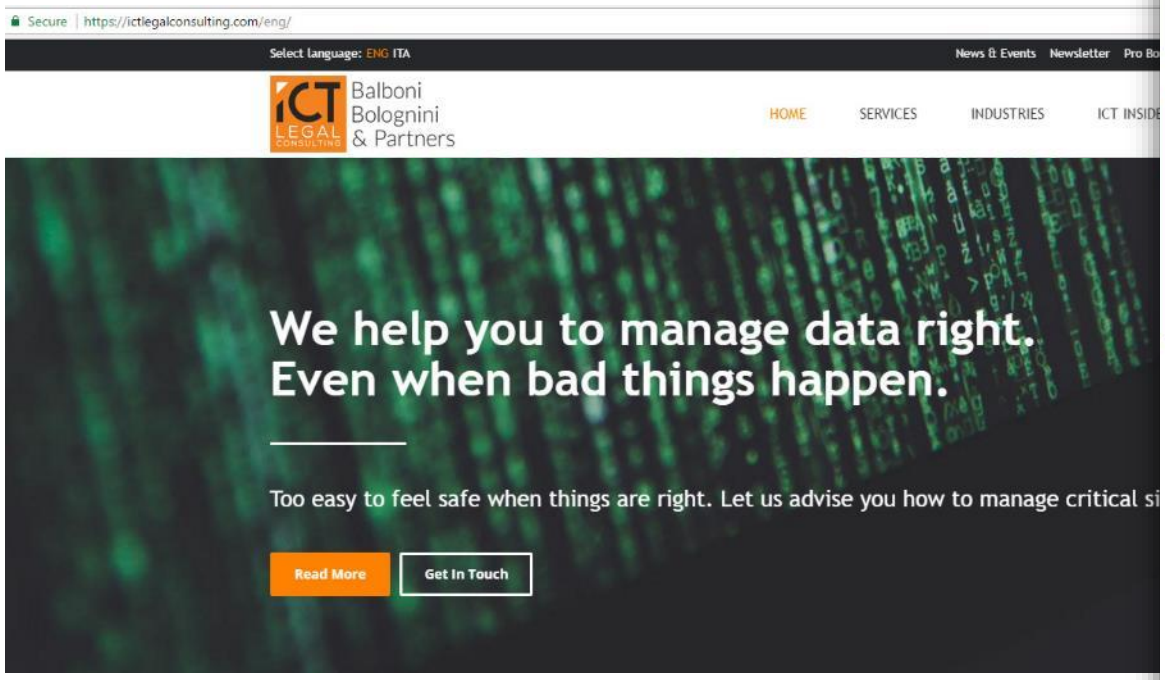
Paolo Balboni is Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law. He is involved in European Commission studies on new technologies and participated in the revision of the EU Commission proposal for a General Data Protection Regulation. Paolo Balboni played an active role in the drafting of the European Union Commission Data Protection Code of Conduct for Cloud Service Providers. In 2019 he was appointed as a Member of the EUMETSAT Data Protection Supervisory Authority.

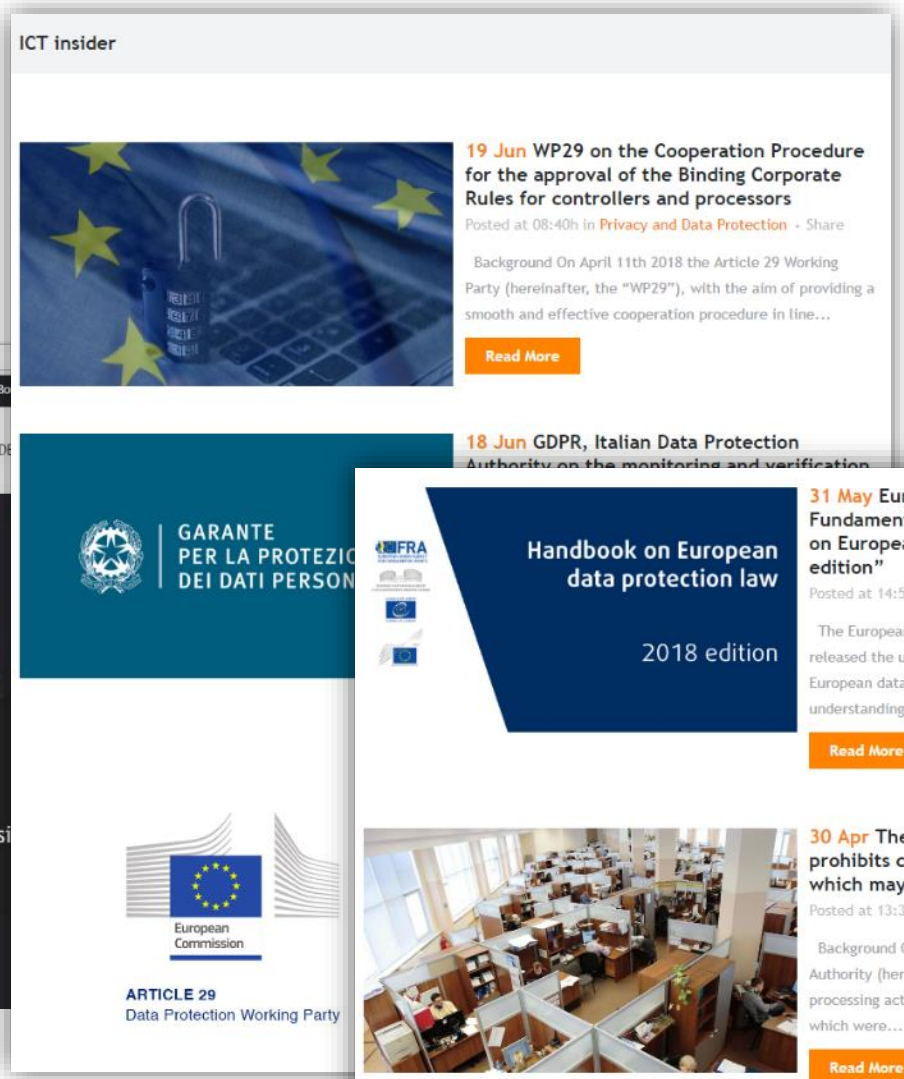
He co-chairs the Privacy Level Agreement (PLA) Working Group of Cloud Security Alliance and has acted as the legal counsel for the European Network and Information Security Agency (ENISA) projects on 'Cloud Computing Risk Assessment', 'Security and Resilience in Governmental Clouds', and 'Procure Secure: A guide to monitoring of security service levels in cloud contracts'. As a frequently invited speaker, Paolo Balboni has spoken on the legal aspects of ICT, Privacy & Data Protection matters at more than 30 international conferences around the world in the last 2 years. Paolo Balboni is the author of the book Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers (T.M.C Asser Press), and of numerous journal articles published in leading European Law reviews.

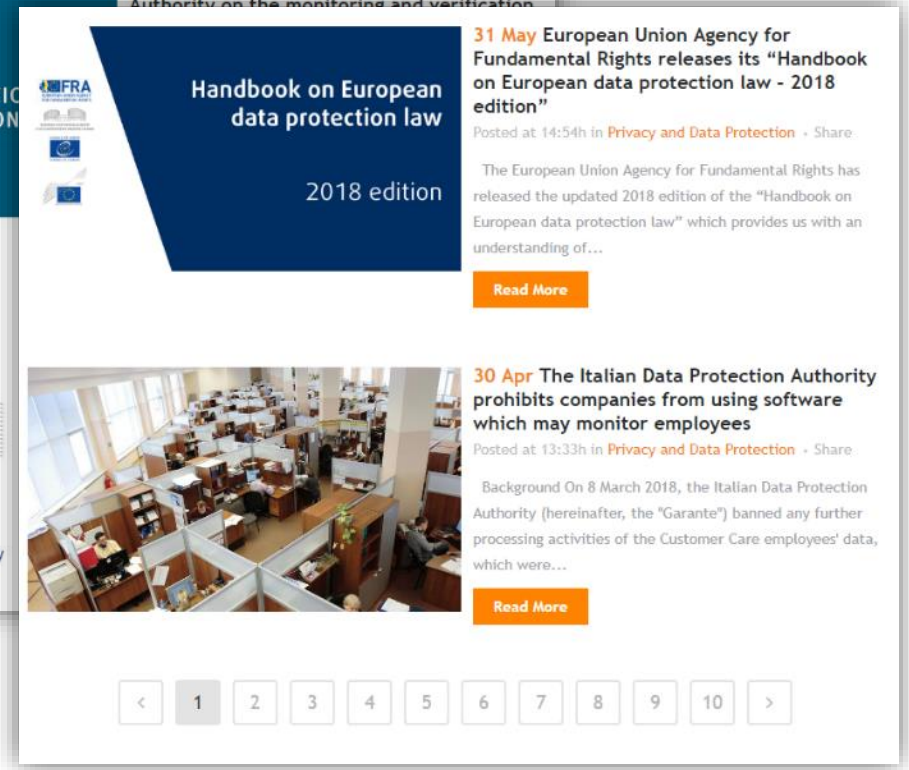
Graduated in Law at the University of Bologna (Italy) in 2002, Paolo Balboni completed his Ph.D. in Comparative Technology Law at Tilburg University (The Netherlands) in 2008.

He speaks Italian, English and Dutch fluently and has good knowledge of French, Spanish, and German.

# Website & Publications



# Newsletter

**ictlegalconsulting.com/eng/newsletter/**

# Awards



ICT Legal Consulting has been ranked by **The Legal 500 EMEA 2020** in the **Data Privacy and Data Protection** (Italy) practice area. Both of our Founding Partners, Paolo Balboni and Luca Bolognini, are Recommended Lawyers. Luca Bolognini has also been listed as a "Leading Individual".

In the **Industry focus: TMT** practice area (Italy), both our Founding Partners, Luca Bolognini and Paolo Balboni, and Francesco Torlontano, Of Counsel, have been listed as Recommended Lawyers.

Read more at legal500.com/ict-legal-consulting/milan-italy

# Awards








# ICT Cyber Consulting

*Consultancy and services for data and digital information security*

# ICT Cyber Consulting

*Consultancy and services for data and digital information security*

**ICT Cyber Consulting** was born as a spin-off of ICTLC – ICT Legal Consulting firm, with the aim of providing guidance, assistance and quality services to companies and to entities in terms of cybersecurity, technology and data protection. The security of data and information, particularly where new technologies are involved, is an integral part of requirements of the utmost importance, that derive from numerous and diverse norms. Not only because of the GDPR (EU General Data Protection Regulation) and the NIS (Network and Information Security) Regulations, but also in regard to the field of trade and industrial secret, which always require setting major attention and effort in particular towards the levels of adequacy of ICT security.

Some of our services:

1. NIS Gap Analysis & Compliance Action Plan
2. Cybersecurity Gap Analysis
3. Cybersecurity alignment to GDPR
4. Hotline Cybersecurity & Data Breach Management Unit
5. Data Protection Impact Assessment - Cybersecurity
6. Cybersecurity assessment of applications
7. Verification of ISO/IEC 27001:2013 controls (Information Security)
8. Verification of ISO 22301:2019 controls (Business Continuity)
9. Verification of ISO 37001:2019 controls (Anti-Bribery)
10. Management and configuration Privacy by Design
11. Penetration Test (PT) and Vulnerability Assessment (VA)
12. Security Assessment external suppliers
13. GDPR second part audits
14. Training

# Contacts


**Milan**
Via Borgonuovo, 12
20121 - Milan - Italy
Phone: +39 02 84247194
Fax: +39 02 700512101

**Bologna**
Via Ugo Bassi, 3
40121 - Bologna - Italy
Phone: +39 051 272036
Fax: +39 051 272036

**Rome**
P.zza di San Salvatore in Lauro, 13
00186 - Rome - Italy
Phone: +39 06 97842491
Fax: +39 06 23328983

**International**
Piet Heinkade 55
1019 GM Amsterdam
The Netherlands
Phone: +31 (0)20 894 6338

**Madrid**
Calle de Alcalá, 75
28009 - Madrid
Spain
Phone: +34 91 577 50 20

**Helsinki**
Neitsytpolku 5 B 49
00140 – Helsinki
Finland
Phone: +358 50 4801292

**Melbourne**
Clarence Chambers, Level 11
456 Lonsdale Street, Melbourne VIC 3000
Australia
Phone: +61 (03) 9070 9847


**ICTLC** is present in further 28 countries: Albania, Austria, Belgium, Brazil, Bulgaria, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Luxembourg, Macedonia, Mexico, Moldova, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Sweden, Switzerland, Turkey, United Kingdom and United States.

**Follow us on:**


**Email contact**
Info@ictlegalconsulting.com

Balboni
Bolognini
& Partners

# Thank you for your attention!

**Prof. Dr. Paolo Balboni** – Founding Partner ICTLC
Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre for Privacy & Cybersecurity at Maastricht University
E: paolo.balboni@ictlegalconsulting.com
M: +39 335 668 5806
@balbonipaolo
www.paolobalboni.eu

# QA Session

# Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)

CRITICAL CHAINS

**Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)**

**Moderator:**

- **Atta Badii,** *University of Reading*

**Topics:**

- Financial Sector Infrastructure **Cyber-Physical Security-Privacy Protection Challenges**
- Financial Services **Regulatory & Compliance Challenges** (PSD2, eiDAS, GDPR, AML, NIS)
- Cyber Security & Compliance **Training Challenges**

Poll / Q&A

**Session 1 Speaker**

Atta Badii

Alper Kanak

Kristo Klesment

**Session 2 Speaker**

Karmele Garcia

Laurentiu Vasiliu

David Goodman

Paolo Balboni

**Additional speakers**

Ramon Martin De Pozuelo Genis
CONCORDIA
CaixaBank

Giorgio Carbone
Ub technologies

Martin Griesbacher
SOTER
RISE Research Industrial Systems Engineering

CONCORDIA Cyber security cOmpeteNCe fOr Research anD InnovAtion
SOTER
Cyber Security for Europe
CS-AWARE CYBERSECURITY
cyberwatching.eu The European watch on cybersecurity & privacy

# Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)

**Ramon Martin De Pozuelo Genis**, CaixaBank, CONCORDIA representative partner

- Project Manager for Technical Fraud Prevention and Security Innovation and Transformation in CaixaBank
- Expertise in design of heterogeneous data networks and information systems for Smart Grids and Smart Cities, and the definition of network architectures, ICT and security solutions

**Giorgio Carbone**, Ub technologies b.V., Stakeholder community representative

- CTO at Ub Technologies
- Responsible for Ub Technologies technology stack including R&D, client deployments, innovation and internal QC
- Extensive experience in quantitative financial and risk roles, including risk pricing, banking books optimisation, quantitative trading, complex derivatives engineering

**Martin Griesbacher**, RISE, SOTER representative partner

- Founding member and coordinator of the research network “Human Factor in Digital Transformation” at the University of Graz
- Human factor cybersecurity expert at Research Industrial Systems Engineering (RISE), Vienna

# Panel Discussion

# Thank you and stay safe

14 December 2020
10.00 AM - 01.30 PM

*Follow us!*

- ***https://research.reading.ac.uk/critical-chains/***
- ***Critical Chains H2020 Project***
- ***@ChainsH2020***
- ***Critical Chains***

# CRITICAL CHAINS

## FINANCIAL SECTOR INFRASTRUCTURE CYBER-PHYSICAL SECURITY AND REGULATORY STANDARDS

Cyber Security for Europe

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

CS-AWARE CYBERSECURITY

SOTER

cyberwatching.eu
The European watch on cybersecurity & privacy