NGI TRUST CHAIN

MUSAP PROJECT

Multiple SSCDs with Unified Signature API Library

WORKSHOP TITLE: DIGITAL IDENTITY AND DIGITAL WALLETS, COMMON GROUND TO ENHANCE SCALABILITY AND ADOPTION PROJECT

Date: 16th November 2023
By: Ammar Bukhari

methics

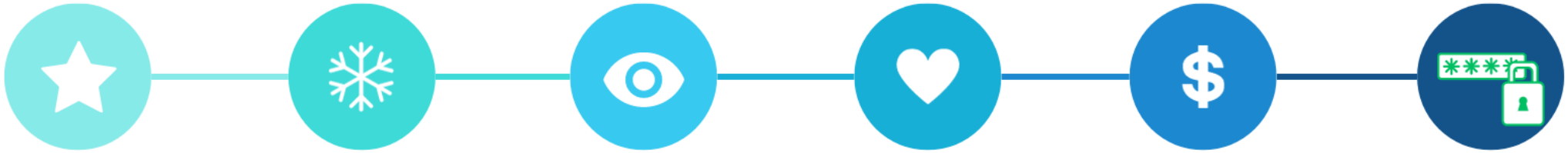
SUPPORTED BY NGI

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

EUROPEAN DYNAMICS · FGS · University of Ljubljana Faculty of Computer and Information Science · ALASTRIA · Athens University of Economics and Business · CIBER VOLUNTARIOS.org · TIMELEX · City University of London · HELLENIC REPUBLIC National and Kapodistrian University of Athens

MUSAP JOURNEY TIMELINE

A brief history of events behind MUSAP's design and unique value proposition



2010 - 2021

Methics provided solutions for citizen identity in Finland, Switzerland, Armenia, Vietnam and Mongolia.

Developed eIDAS compliance Remote Signature solution

2021

eIDAS 2 and EUDIW plans unveiled

EUDIW use cases definition

2022

Thales' Users perception survey

First EUDIW toolbox outline published

2022/23

ENISA's definition of EUDIW
Its building blocks and problems related to it

2023

First version of EUDIW ARF published

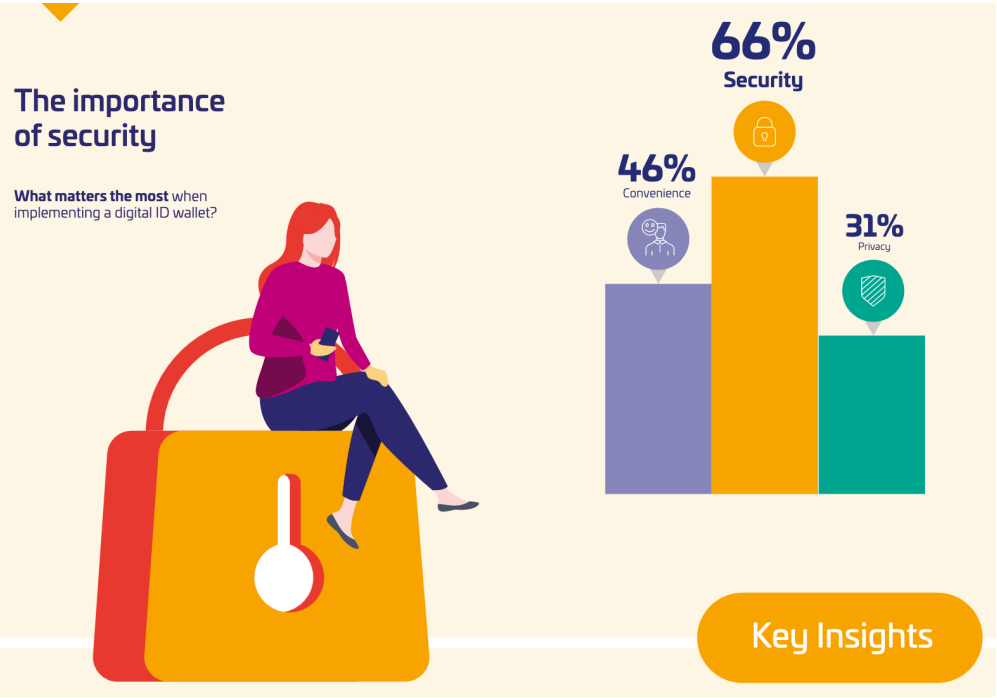
Methics receives NGI Trustchian OC1 funding for MUSAP

PRESENT

MUSAP being developed and tested with use cases

Wait for Reference Implementation of EUDIW

WHAT DO USERS CARE ABOUT DIGITAL ID?



- Users rely on having a favorite method to authenticate themselves For example:
  - In 2022 out of more than 200 million online authentications of Suomi.fi, more than 16 million authentications happened through Finnish Mobile ID Mobiilivarmenne with zero fraud rate

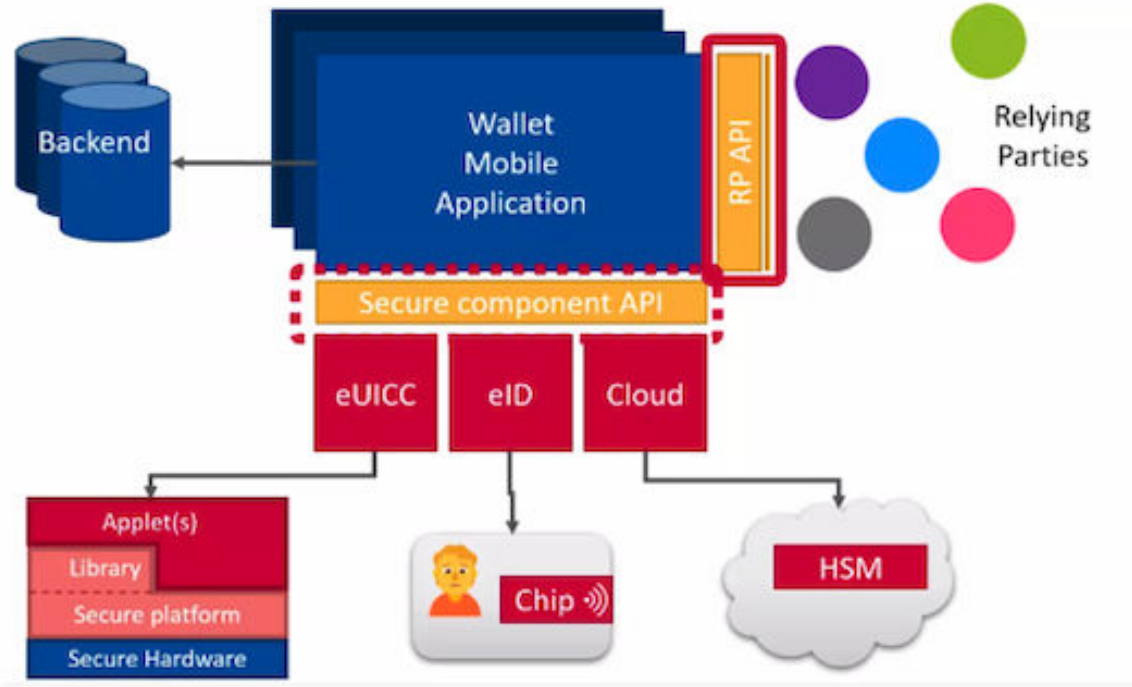
- According to survey by Thales (conducted in 2022) to understand needs for EUDIW:
  - Most important aspects for future users of Digital Identity wallets is:
    - Security and
    - Convenience

  - More than 70% are already using some form of Digital ID

Source: Thales Survey related on EUDIW and user's identity experience.
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/EU-ID-wallet-survey-insights

ENISA'S OPINION ON EUDIW COMPONENTS AND NEEDED API

Secure component API is needed for implementing **interoperability** between different security technologies used for EUDIW.



ENISA gave recommendation to "develop a **unique API from the mobile app to the security anchor provided by the secure element.** This is crucial for the provision of full interoperability…."

"The **harmonised interfaces** that allow direct access to the **internal** and **external mobile device cryptographic security** that the EUDIW can use to perform cryptographic security functions are an essential and instrumental function."

Source: ENISA EUDIW Standardisation Workshop (May 2023), Digital Identity Standards report (June 2023)

WHAT IS MUSAP? 1/2

MUSAP is a Unified Signature API that allows users to choose their preferred SSCD

MUSAP will act as an **intermediary layer** that abstracts the complexities of different SSCDs /key stores/ secure elements.

MUSAP will allow:

1)End-User app(s) to outsource their key management operations

2)End-Users to have multiple identities i.e multiple X.509 certs, VCs etc provisioned at different LoA

3)Developers to quickly build apps which require cryptographic interfaces and components of a SSCD

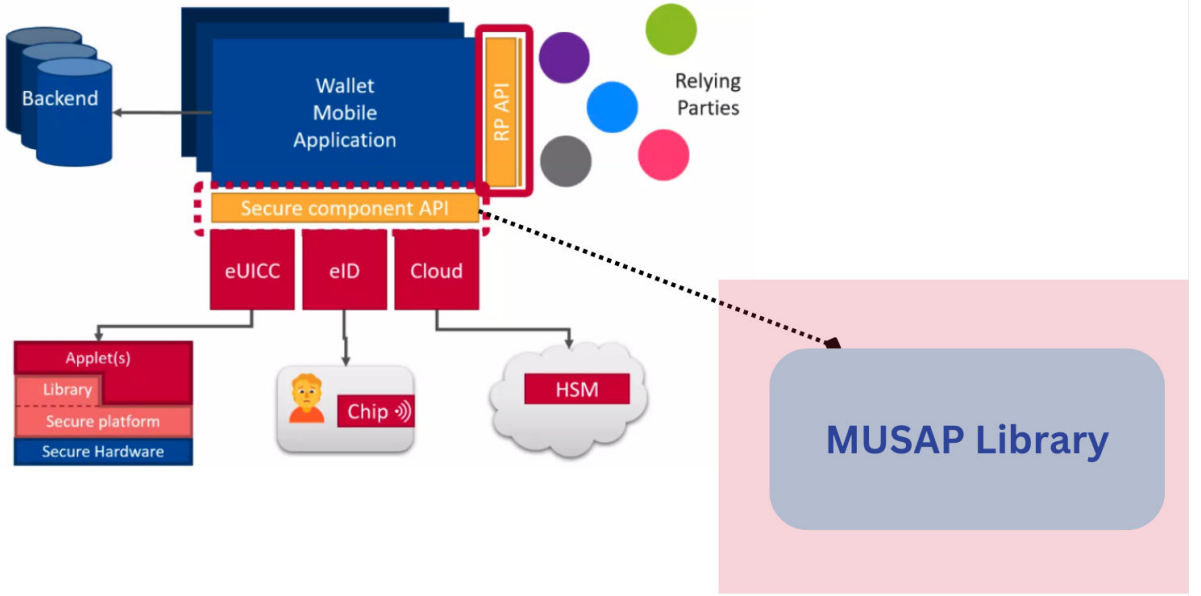


Image Source: ENISA EUDIW Standardisation Workshop (May 2023)

WHAT IS MUSAP? 2/2

MUSAP is Unified Signature API for allowing multiple SSCDs in end-user app

MUSAP will provide common set of definitions for a universal taxonomy to enable SSCD/key store/ secure element interaction with identity wallets.

MUSAP can interface **both** 'Substantial' and 'High' Level of Assurance devices with one end-user application.

Multiple security technologies / key stores / SSCDs can be interfaced with help of MUSAP

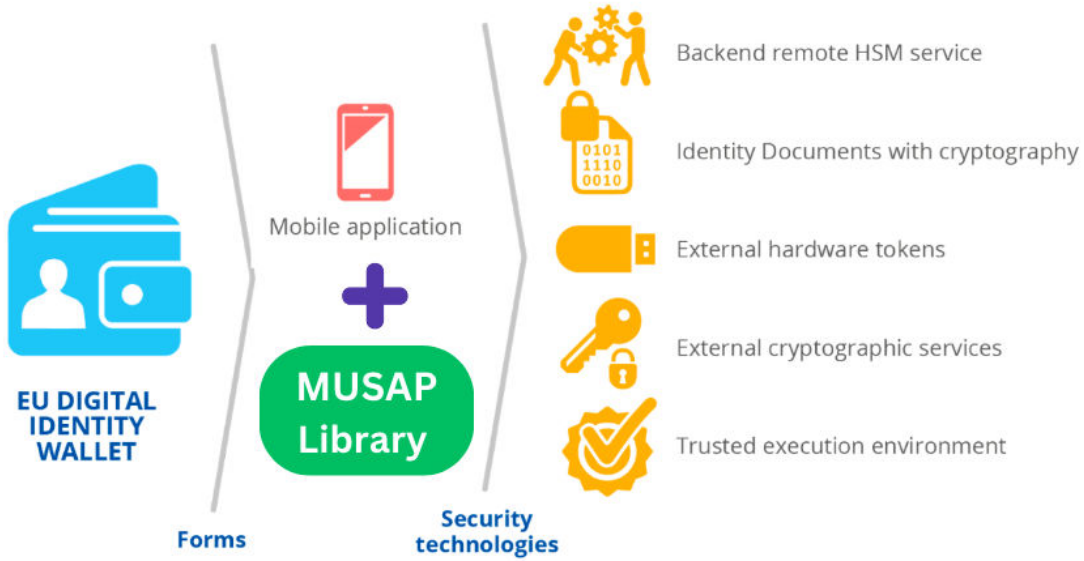


Image Source: Image adopted from ENISA Digital Identity Standards report (June 2023)

NGI TRUST CHAIN

Don’t put all your KEYS in one basket.

Jarmo **Miettinen**

CEO, Methics Oy

MUSAP DEVELOPMENT WITH USER-CENTRIC APPROACH

1. Reliance on existing survey results → Thales conduced end-users survey related to Wallets use. Users pointed out **Security** and **Convenience** as most important points.

2. Feedback from multiple parties → Current Methics customers, Other projects in OC1 such as Danube Tech (Client-DID), some other 3rd parties to use MUSAP for their tasks.

3. End-users survey in Mongolia → Users of VSign are currently being surveyed to determine user's attitude in that market. Survey to conclude by 20th December 2023.

4. Benefits for end-users →

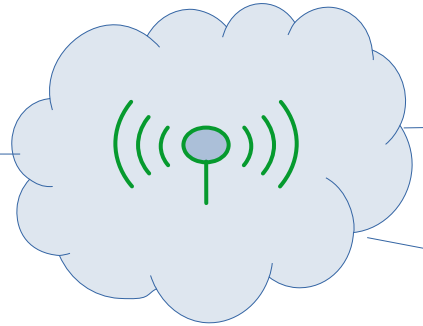
1. Choice for end-user to make how they want sole control implemented
2. Key selection logic improvements and proper/convenient defaults
3. Provide option to sign with individual or corporate certs/keys
4. Evaluations of why one method is safer than another
5. Option to continue their existing Digital ID solution of choice.

USE CASES SOLVED BY MUSAP 1/2

1. Sign any data format either provided by centralized or decentralized system→ MUSAP can sign any data format with SOG-IS agreed signing scheme.

2. Provide multiple SSCDs for end-user to sign → MUSAP allows end-user to select their preferred keystore

EUDI Wallet/ Custom App 1
UI for Authn/ Sign



Centralized ID
X.509v3

Decentralized ID
SSI
VC/DID

SSCDs (key stores) interfaced because of MUSAP:
1. Phone key store
2. SIM/eSIM
3. USB Dongle (Yubikey via NFC)
4. eIDAS Remote Signature

USE CASES SOLVED BY MUSAP 2/2

3. Enable both config types for EUDI Wallet →

MUSAP can enable both EUDIW configuration types i.e 1 and 2 in **one** mobile device

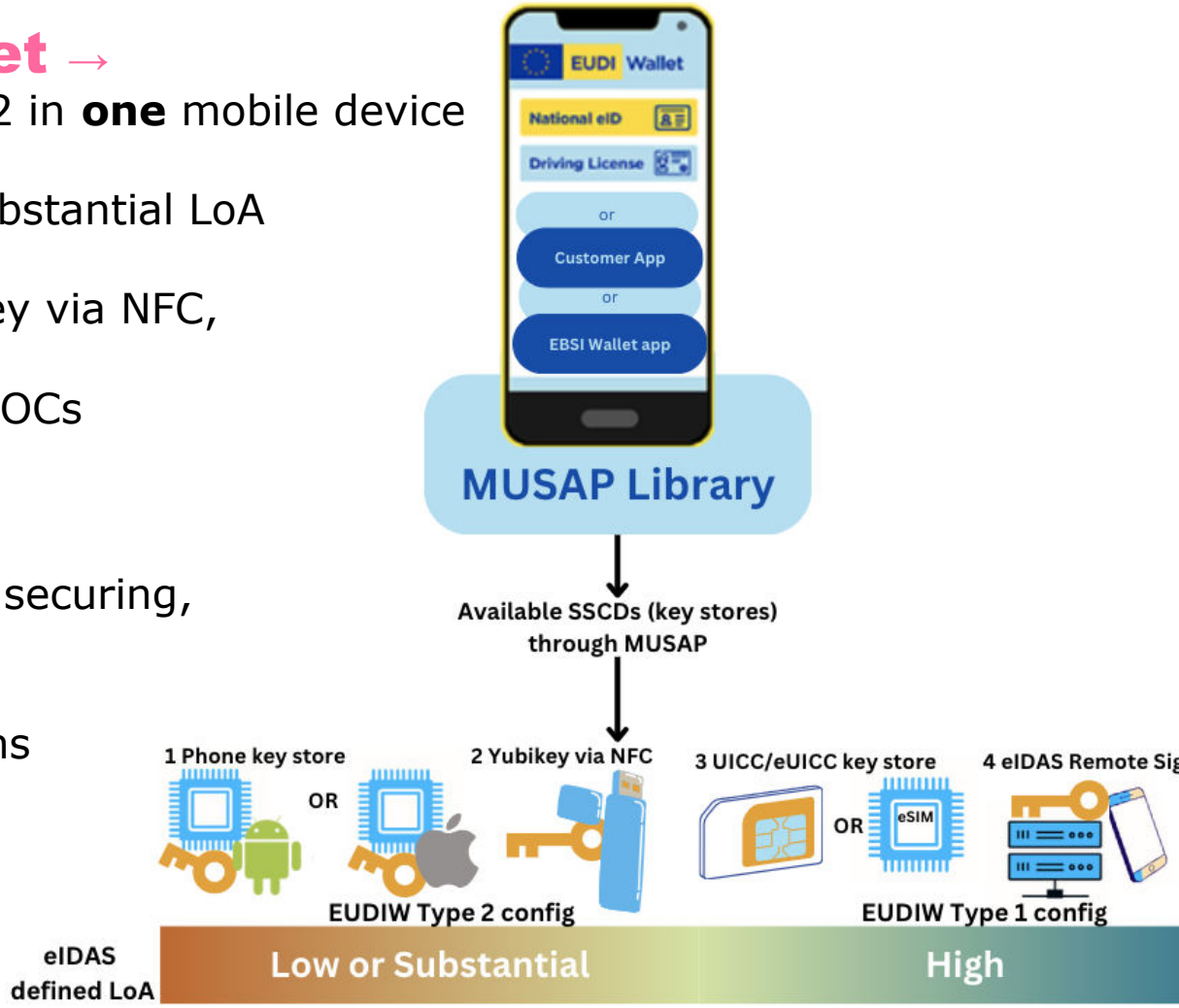
MUSAP enabled EUDIW to authenticate/sign with High and Substantial LoA

Multiple security technologies (HSM+app, eUICC/UICC, Yubikey via NFC, Phone key store) will be interfaced in OC1.
More SSCDs like (eID card, TEEs, etc) can be added in future OCs

4. Handles Key management →

MUSAP handles operations related to key generation, storing, securing, and to manage and protect identities and associated data.

MUSAP provides a set of cryptographic methods and operations (Initial release in D2, final version in D4)



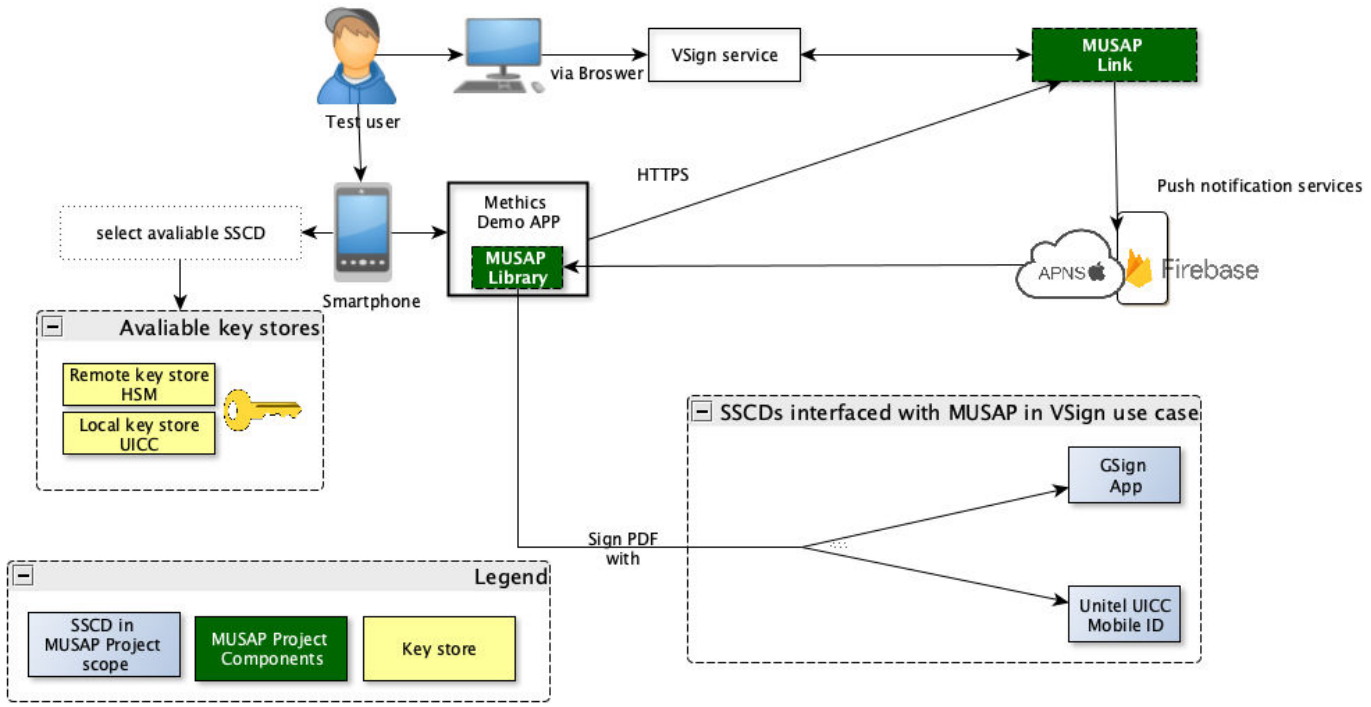
MUSAP DEMO/PILOT DURING OC1

1. **Three type of users during OC1→**
   i) Test users by Methics, ii) Danube Tech and other third parties and iii) VSign users in Mongolia

2. **Provide MUSAP Library + Link →**
   Current plan is to share complete MUSAP package with agreed 3rd parties by Week 50.

3. **Pilot in Mongolia →** Survey ongoing.
   Methics plan to launch VSign pilot by early 2024 with 2 SSCDs.

4. **MUSAP for EUDIW? →** Methics is open to share MUSAP with EU and Large Scale Pilots for testing Type1/2 config with actual EUDIW.



STAY UPDATED AND GET INVOLVED!

trustchain.ngi.eu

Visit our website to learn more at: www.methics.fi

Contact us at:

Telephone: +358 (0)9 5840 0188

Email: methics.info@methics.fi

Address: Stella Business Park, Lars Sonckin kaari 14, FI-02600 Espoo, Finland

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.