MUSAP: Multiple SSCDs with Unified Signature API Product Fact Sheet v.1.0

MUSAP is a project dedicated to develop a novel software interface known as the Unified Signature API (USAPI) Library. Serving as an intermediary layer, MUSAP abstracts the complexities of various Secure Signature Creation Devices i.e SSCDs (key stores/ secure elements or security technologies, etc).

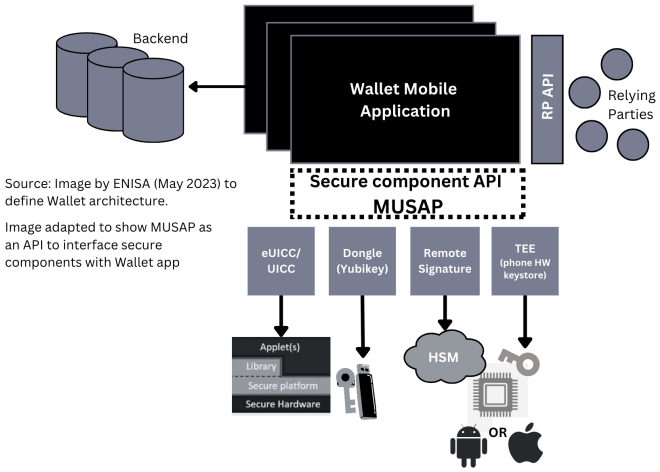
Primary goal of MUSAP is to harmonize current digital identity secure key technologies with the context of emerging eIDAS2 regulations, while affording end-users flexible control over their credentials management. In simpler terms letting users choose how they want to store/access their private keys.

MUSAP addresses both security and convenience aspects, offering a resilient and adaptable implementation for end-user-app(s) requiring high level of trust. MUSAP offers end-users methods to diversify their key storage and use existing SSCD (from already deployed Digital ID system). Eventually avoiding the concentration of all keys in a single basket.

MUSAP Background

From Methics experience in this business sector, few core problems which exists today related to Digital ID are privacy, security, interoperability, usability and adoption among the masses. Adoption depends on users choice and it varies in each market. Since 2021 when eIDAS2 and European Digital Identity Wallet (EDIW) were announced, Digital Wallets and their architecture have gained momentum. We believe, new identity systems should complement existing state of the art, rather than completely replacing it.

As EDIW progressed, ENISA (European Cybersecurity Agency) has been releasing recommendations related to a need for harmonized interface that allows access to cryptographic operations.



Source: Image by ENISA (May 2023) to define Wallet architecture.

Image adapted to show MUSAP as an API to interface secure components with Wallet app

Figure 1: MUSAP as a secure component API for end-user-app

MUSAP will act as a secure component API, as it is needed for implementing interoperability between different security technologies for EDIW.

MUSAP Features/Functionality

MUSAP will provide common set of definitions for a universal taxonomy to enable SSCDs interaction with end-user-app. MUSAP provides following features for end-users & end-user-apps:

1. *Integration of multiple SSCDs into MUSAP:* Allows end-user to select where they want to store their private keys.
2. *Open Interface for integrating new/ multiple SSCDs*: Speed up the app development of trust applications.
3. *Digital Signatures with different LoAs (High, Substantial)*: One tool to create different LoA signatures.
4. *Key Discovery*: To use correct key for each service.
5. *Key lifecycle management*: Provide key management operations such as generation, revoke, etc.
6. *Key attestation*: Verify key material security.
7. *Key metadata definitions and import/export*: Integrate existing SSCDs with MUSAP and store SSCD metadata.
8. *Sign data and cryptographic format*: Support different applications and maintain non- repudiation of data.
9. *Link library for Web-apps*: To allow web-apps to call and perform signature through end-user-app having MUSAP.
10. *KeyURI scheme*: New URI scheme to be published to store and identify each key in a unified way.

MUSAP never shares actual cryptographic keys of the SSCD. With user's consent, only SSCD metadata is shared. To implement MUSAP in an end-user-app, developers can import MUSAP library in their Android/iOS app projects, defines what kind of SSCDs they want to support and its configurations.

Use Cases solved by MUSAP

MUSAP project is to provide a MUSAP Library and MUSAP Link which can be used for following use cases:

1. Sign any data format (X.509, VC, DID, etc)
2. Provide multiple SSCDs for end-users to sign/auth
3. Handling Key Management methods and operations
4. Enable EDIW Type 1 and Type 2 config in one device

MUSAP has been developed from user-centric perspective to let end-users choose what SSCD they trust more. This will allow end-users to adopt to the new end-user-app.

Impact created by MUSAP

MUSAP actively utilizes and promotes for a diverse range of security standards and concepts. There are multiple impactful benefits for using MUSAP.

- MUSAP extends support to both Type 1 & Type 2 configs of EDIW within a single device implementation.
- MUSAP is committed to delivering robust authentication and verification mechanisms, coupled with strict security measures, to safeguard the exchange and storage of key data.

Furthermore, Users can have multiple X.509 certificates (individual or corporate), multiple DIDs, multiple VCs who once signed through MUSAP allows end-user-app to construct a VP.

About MUSAP Project

MUSAP Project has received funding from the NGI TrustChain project. Project is funded under the NGI initiative by the European Union (GA No 101093274). MUSAP will be released as an Open-Source Library in Github (TRL7 or higher) by April 2024.

About Methics

Methics is a Finnish technology vendor specializing in Digital Identity and Mobile Signatures services. Methics specializes in delivering standards based identity solutions across Europe and Asia.

Methics Ltd, Lars Sonckin kaari 14, FIN-02600 Espoo.
Business ID: 1778566-8
www.methics.fi www.trustchain.ngi.eu/musap/