Using Trustworthy AI in the European Digital Identity (EUDI) Wallet

Joseba Martínez-Arrizabalaga, Claudia Franco, Carlos Lancha, Miguel Encina,
Daniel Flores, Rosario Arjona, and Iluminada Baturone
Microelectronics Institute of Seville (IMSE-CNM), University of Seville-CSIC
Electronics and Electromagnetism Department, University of Seville

Abstract

The European Identity Wallet requires a high level of assurance. Our solution achieves that by involving multifactor authentication (biometrics, password and user device) and hardware security (using Trusted Execution Environments (TEEs) for integrity and confidentiality). Trustworthy AI based on a Convolutional Neural Network (CNN) is used to extract facial biometric features. These sensitive features are extracted remotely in a Wallet Secure Cryptographic Device (WSCD) that uses a TEE based on Intel SGX. Trustworthiness is increased at the wallet instance (app at the user's smartphone) by using a foundation model for detecting facial presentation attacks.

Introduction

The European Digital Identity (EUDI) Wallet is a secure and user-controlled digital environment that will allow users to manage their personal identification data and attestation attributes to public and private services in the EU. The Wallet contains a Wallet Secure Cryptographic Device (WSCD) storing and managing the user's sensitive data, which communicates securely with the Wallet Instance (WI) at the user's device (typically a smartphone).

The Architecture and Reference Framework (ARF) [1] requires user binding to prevent identity theft attacks. This requires supporting Presentation Attacks Detection (PAD) in case of using biometrics. We use trustworthy AI for facial authentication (at the WSCD) and for PAD (at the WI) [2]-[5].

Methodology

We use a remote WSCD with a TEE for scalability and independence from smartphones' manufacturers [2]-[3]. Every communication between the WSCD and the WI is carried out through a secure TLS channel.

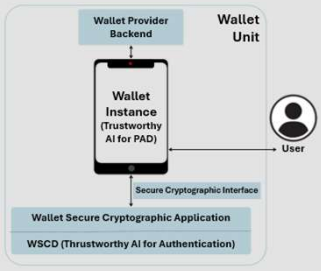

Figure 1: Wallet Unit workflow.

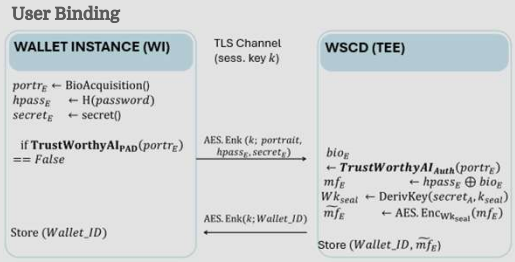

Figure 2: User Binding process. The PAD is verified in the user's app before the WSCD extracts the features from the portrait. k_{seal} is the enclave sealing key.

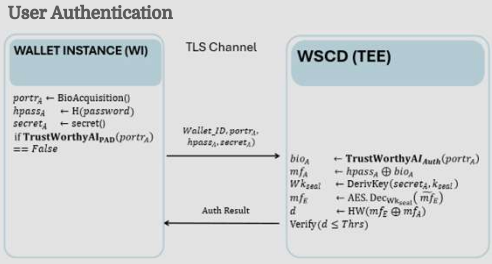

Figure 3: User Authentication Process. The PAD is verified in the user's app before user authentication. k_{seal} is the enclave sealing key.

Results

We implemented FoundPAD [6] as a ViT-B foundation model for facial PAD in an Android smartphone [5] and a 128-value FaceNet model [7] for the extraction of face features in an Intel laptop with Intel SGX TEE acting as a server. The computation costs of the FoundPAD implementation are shown in Table 1. In Tables 2-4 we summarize the computation costs for the user binding and authentication processes which include the FaceNet model. Screenshots of the user interface of our WI are shown in Table 5.

With FaceNet, we achieve an EER 1.18% with an accuracy of 99.2% for the LFW database.

Table 1: Weights and execution times for FoundPAD implementation.

Model	Found. model weight (kB)	Classif. Header weight (kB)	Exectution speed (ms)	Installation time (min)	App Weight (GB)
ViT-B	336792	9	750-1050	1	2.01

Table 2: Computation times in ms for user binding and authentication.

Binding	Authentication
374.2	373.8

Table 3: Computation times in ms for the operations performed in the WSCD.

Time (ms)	Feature Extraction (CNN)	Hamming Weight	XOR	Credential ID Generation	Key Generation
Inside Enclave	368	0.0056	0.0048	0.0106	0.3546
Outside Enclave	245	0.0004	0.0003	0.0026	0.3555

Table 4: Communication overhead in bytes.

	WI →WSCD	WSCD →WI
User Binding	307280	8
User Auth.	307328	89

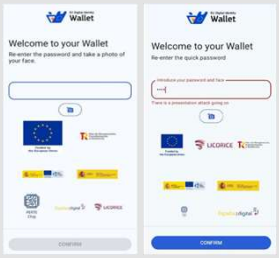

Figure 4: Screenshots of the modified EUDI Wallet with face recognition and facial PAD.

Conclusions

- The secure enclave provides hardware security without compromising the performance.
- The computational and communication costs and execution times are viable for a real case use application.

References

[1] European Commission, "Architecture and Reference Framework (ARF) v2.2.0," eu-digital-identity-wallet, Jun. 20, 2025. [Online]. Available: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.2.0/
[2] C. Franco, C. Lancha, D. Flores, R. Arjona, I. Baturone, "A High-Level-of-Assurance EUDI Wallet with a Remote WSCD Supporting Biometrics and Passkeys", 2nd International Workshop on Emerging Digital Identities (EDId), 20th International Conference on Availability, Reliability and Security (ARES), 2025.
[3] C. Franco, "Analysis and use of hardware-defined secure environments for crypto-biometric solutions of EUDI wallets", Master's Thesis, 2025.
[4] D. Flores, "Analysis of the European digital identity wallet reference implementation and integration of a multifaction authentication solution". Computer Science Engineering Bachelor's Thesis, University of Seville, 2025.
[5] M. Encina, "Study and realization of biometric systems implemented in smartphones and robust against presentation attacks". Computer Science Engineering Bachelor's Thesis, University of Seville, 2025.
[6] G. Ozgur et al., "FoundPAD: Foundation Models Reloaded for Face Presentation Attack Detection," in 2025 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW), Tucson, AZ, USA, 2025, pp. 697-707, doi: 10.1109/WACVW65960.2025.00084.
[7] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, Jun. 2015, pp. 815–823.

Acknowledgements

This research was conducted thanks to Grants PDC2023–145873-I00, CPP2022–009796, and PID2023-150809OB-I00 funded by MICIU/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR, thanks to the LICORICE Project with Grant Agreement No. 101168311 under the EU Horizon Europe, and thanks to the grant USECHIP (TSI-069100-2023-001), project funded by the Secretary of State for Telecommunications and Digital Infrastructure, Ministry for Digital Transformation and Civil Service and by the European Union–NextGenerationEU/PRTR.