Crypto-biometric techniques and hardware-enabled solutions to achieve High Level of Assurance in the EUDI Wallet

Rosario Arjona, Claudia Franco, Carlos Lancha and Iluminada Baturone

{marjona, cfranco, clancha, lumi}@us.es

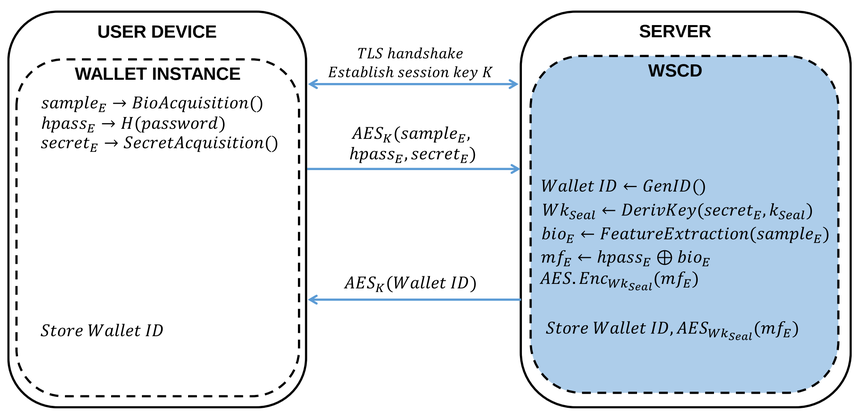
Abstract: In a digital world, electronic transactions require secure digital identities (also known as electronic identities or eID). In Europe, the eIDAS (electronic IDentification, Authentication and trust Services) regulation 910/2014, in its revision of 2021, established the requirements for the European Digital Identity Wallet (EUDI Wallet). The EUDI Wallet will give full control to users on their personal data or credentials (claims about the user) to share with third parties, and keep track of such sharing, as can be done by Self-Sovereign Identity (SSI). The wallet should be univocally associated to its true user (holder) so that any other people should be unable to hold that identity. This is known as holder binding. Biometric recognition is very suitable for holder binding since it provides an intrinsic and physical association to authenticate the user of the EUDI Wallet. In order to achieve high level of assurance in the holder binding, we propose crypto-biometric techniques and hardware-enabled solutions to protect against security attacks. Homomorphic encryption and Trusted Execution Environments (TEEs) are considered. Long-term security and privacy-preserving verifiability can be achieved by the use of homomorphic encryption through cryptographic algorithms selected in the NIST Post-Quantum Cryptography Standardization Process.

Motivation

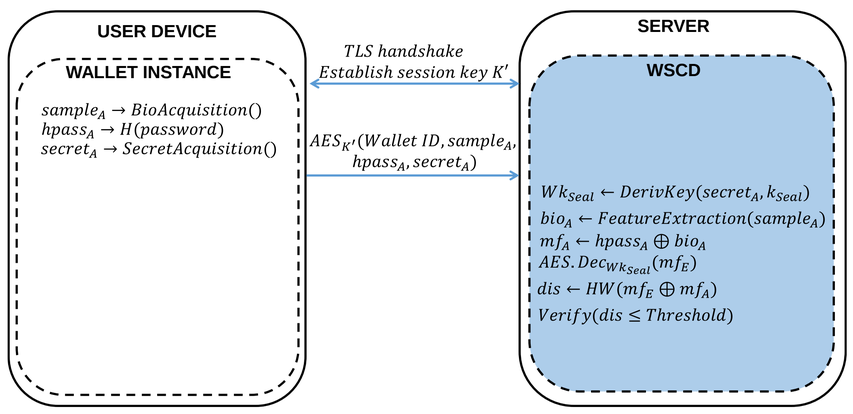
The higher levels of assurance of the eIDAS require multi-factor authentication with at least two factors, among them, biometrics. In addition, the Architecture and Reference Framework (ARF) defines that the Wallet Instance can access a Wallet Secure Cryptographic Device (WSCD) to achieve a high level of assurance. The WSCD is a tamper-resistant device with hardware security to protect critical assets (such as biometrics data and secret keys) and to securely execute cryptographic functions. As possible security architectures for the WSCD, a remote WSCD such as a remote Trusted Execution Environment (TEE) is convenient if the User Device lacks sufficiently secure hardware, if a local external WSCD such as a smartcard is not desired, or if a local internal/native WSCD such as a e-SIM or an embedded TEE has a dependency on proprietary software.

Solution based on One server

ENROLMENT



AUTHENTICATION

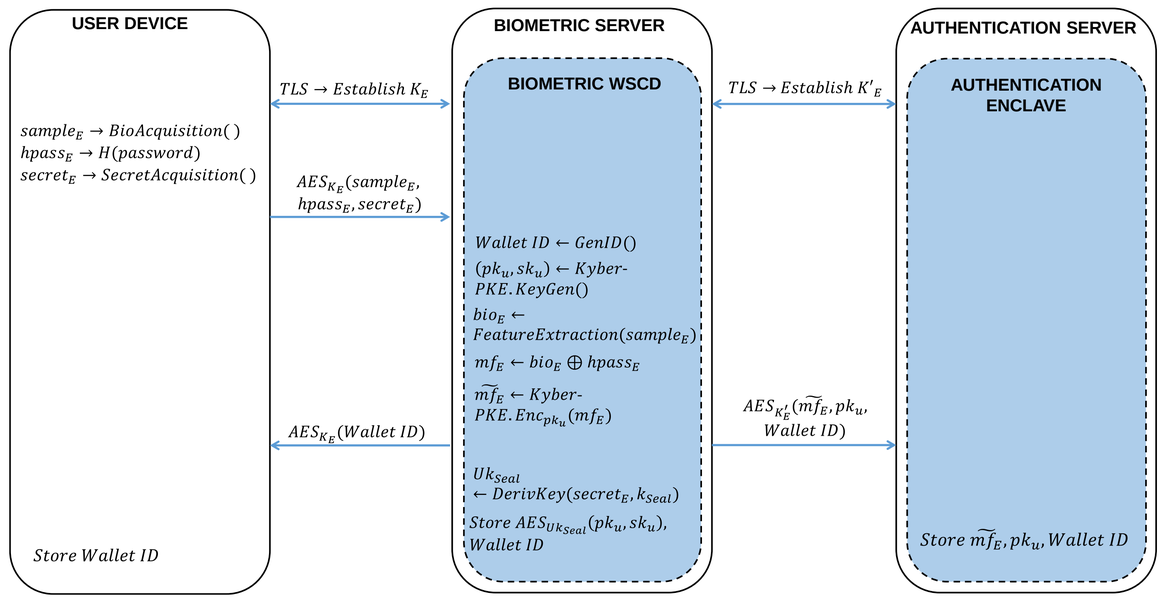


Realization Proposal

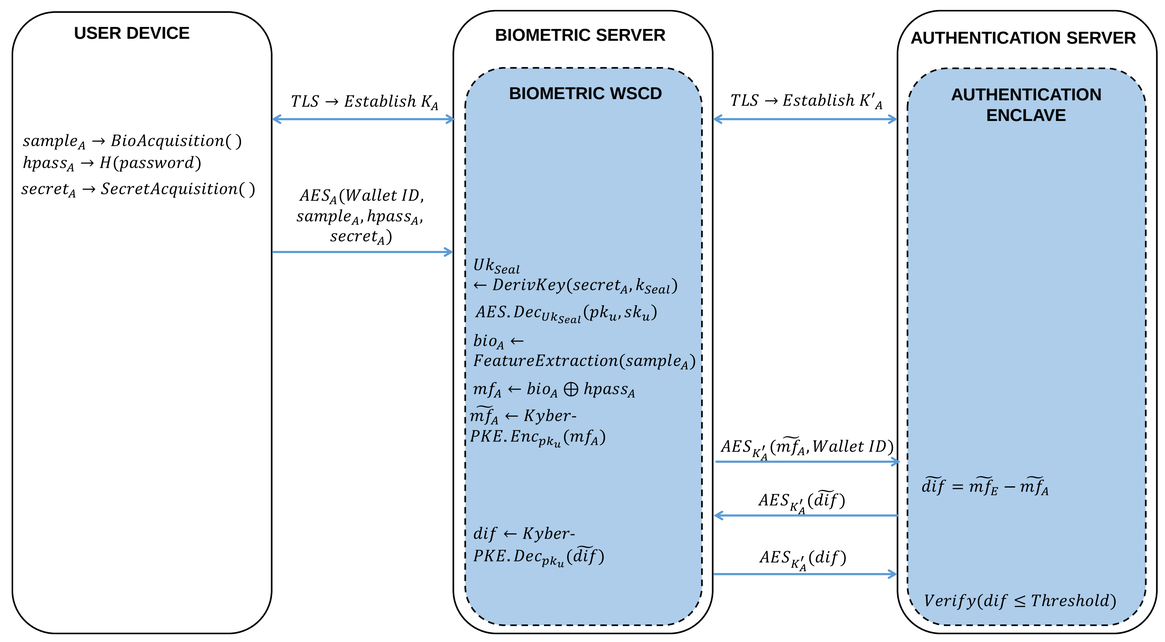
A combination of user's biometrics, password and device secret is protected by the enclave in the 1-server solution. In addition, the protection is post-quantum by using homomorphic properties of CRYSTALS-Kyber public-key encryption (Kyber768) in the 2-server solution. A Samsung Galaxy A52 acts as User Device with the Wallet Instance. Intel SGX1 secure enclaves act as TEEs for the WSCD and authentication enclave in a laptop with an Intel® Core™ i7-10750H at 2.60GHz and 16GB RAM. Face recognition is employed with BlazeFace and a FaceNet Tensorflow-Lite model. The resulting 128-value embeddings are binarized with 3 bits using a Linearly Separable SubCode (LSSC). A 512-bit hash of the password is calculated with SHA-512.

Solution based on Two servers with Post-Quantum Security

ENROLMENT



AUTHENTICATION



Experimental Results and Discussion

- Execution times (in ms) are less than 0,5 seconds for enrolment and authentication, and for the main operations which work with multi-factor data:

Operation	Feature Extraction	Hamming Weight	XOR	Key Generation	AES Encryption	AES Decryption	Kyber Encrytion	Kyber Decryption	Encrypted Data Subtraction
Inside Enclave	368.9140	0.0056	0.0053	0.2436	0.0252	0.0192	0.5528	0.1510	0.0520
Outside Enclave	245.6370	0.0004	0.0004	0.1772	0.0036	0.0004	0.4409	0.1232	0.0290

- The recognition performance considering only the biometric factor is evaluated by an EER of 1.69% with an accuracy of 98.9% in the FERET database and an EER of 1.18% with an accuracy of 99.2% in the LFW database.
- Storage requirements for the multi-factor template are: 64 bytes with AES encryption, and 2,176 bytes with Kyber encryption.
- Communication overhead (in kB) is: 307.3 from UD to BS, 0.2 from BS to UD, 3.4 from BS to AS and 9.9 from AS to BS during enrolment; and 307.3 from UD to BS, 0.1 from BS to UD, 2.3 from BS to AS and 2.2 from AS to BS during authentication. (UD: User Device, BS: Biometric Server, AS: Authentication Server)
- Our proposal provides confidentiality and integrity, is scalable for many users and is secure against malicious adversaries.
- Future work will explore the detection of presentation and injection attacks, and the fusion with veins acquired from ordinary smartphones.

References:

[1] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[2] European Digital Identity Wallet Architecture and Reference Framework, 2025: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/
[3] Román, R., Arjona, R., López-González, P., Baturone, I.: A Quantum-Resistant Face Template Protection Scheme using Kyber and Saber Public Key Encryption Algorithms. International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-5 (2022).
[4] Arjona, R., Franco, C., Román, R., Baturone, I.: Combining CRYSTALS-Kyber Homomorphic Encryption with Garbled Circuits for Biometric Authentication. International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-5 (2024).

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 Cátedra USECHIP (TSI-069100-2023-001) of PERTE Chip Chair program funded by European Union – Next Generation EU.