EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Cybersecurity and Trust
Digital Identity and Trust

Luxembourg
CNECT.H.4.001/ÅB

Anton Thomasson
antonthomasson@gmail.com

By email only

Subject: EU Digital Wallet and Digital Sovereignty feedback

Dear Mr Thomasson,

Thank you for your email to EVP Virkkunen of 30 June 2026, which we have registered under reference Ares(2026) 6598975. She has asked me to reply to you.

In your email you question why EU Digital Wallet implementations are required to depend on Apple/Google remote attestations. I would like to start by underlining that neither the eIDAS Regulation nor the Architecture and Reference Framework (ARF) mandate or recommend the use of any specific mobile platform API for device or application integrity checks and, most importantly, neither designate any commercial integrity service.

Instead, the framework requires that a Wallet Unit present a Wallet Instance Attestation when a PID or a credential is issued to it. Such attestation is signed by the Wallet Provider, which must therefore be able to establish that a given instance is authentic and uncompromised, to keep that attestation up to date and to revoke it when it no longer holds.

Practically speaking, there are different approaches depending on context and technical choices, including openly available platform and operating system APIs, hardware backed key attestation and so on. Alongside instance attestation, application level hardening is addressed through established practices, and implementers are encouraged to work against the OWASP Mobile Application Security Verification Standard (MASVS).

It is important to note that the Reference Implementation published by the European Commission is a demonstration and not a normative instrument or a product. As such, Member States are under no obligation to use and deploy it and choices made within it carry no regulatory weight. In this ecosystem, each Member State is responsible for providing and certifying its own Wallet Solution, including its security architecture and the demonstration of conformity against the applicable certification scheme.

Finally, please note how both the ARF and the Reference Implementation are developed in the open and contributions are always welcome in an open source fashion. The community is encouraged to propose and develop alternative approaches to all the features and specifications. We would therefore very much welcome you to continue the discussion in the public discussion spaces on GitHub (https://github.com/eu-digital-identity-wallet), where it can benefit from broader input.

Yours sincerely,

Norbert SAGSTETTER
Head of Unit