Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Response to ARF Discussion topics: Topic X "Relying Party Registration" (refinement round)

On the desirability of implementing the RP registration certificates

Implementing these certificates is essential to ensure, by design and by default, compliance with transparency, data minimisation, and purpose limitation principles established in Article 5 of the GDPR.

Article 5b(1) of eIDAS2 makes it clear: Relying Parties (RPs) must register in the Member State where they are established. Article 5b(3) strictly prohibits RPs from requesting any data beyond what is indicated during their registration. This registration is a legal act that must be complemented by enforcement technical measures, such as registration certificates. The certificate is the technical measure that enables the user's wallet to verify compliance in real time, automatically, by design and by default. Without these machine-readable certificates, the wallet may not detect when an RP, for example, attempts to authenticate the user unnecessarily or to request attributes that are not registered as needed.

The EUDI Wallet, as required by eIDAS2 (in various recitals and Article 5a), must unequivocally enable users to exercise full control over their data. Registration certificates are essential to this control. They allow the wallet instance to verify that the presentation request aligns with the registered uses. This enables users to receive warnings, make informed decisions, and reject requests that do not align with, for example, the intended use at registration. Without such certificates, users cannot exercise adequate control by default.

Furthermore, these registration certificates should be mandatory across all Member States to ensure harmonised enforcement and the same level of protection for all European citizens. Under the current version of IAs, each Member State can decide whether to implement the registration certificates. This decision may make them more attractive for establishing RPs. If only one Member State decides not to require registration certificates, the benefits of these certificates will not be fully realised by all citizens.

On the risks posed by not implementing the registration certificates

We need more than a legal promise; given the high risks in this specific ecosystem, we also need technical enforcement measures. GDPR Article 25 mandates data protection by default. If the verification of an RP's request relies on voluntary API calls or user-

initiated checks (*"the Wallet Unit offers to the User an option to verify the information registered for the Relying Party"*), as proposed at this time, the system is not protecting personal data "by default" because the default state is to proceed without verifying the RP's request.

The argument for strict registration and machine-readable certificates in the EUDI Wallet ecosystem, as opposed to the "self-declaration" model used by generic websites (through privacy policies and notices), is that the Wallet is not just another web tool, but a legally mandated, high-assurance infrastructure designed to fulfil fundamental rights. Because the Wallet stores official, verified person identification data, the risk of "over-identification" or "over-sharing" is far greater than on the general web or other digital services. Registration certificates ensure that the Wallet can verify the lawfulness, fairness, etc. of an RP's requests before allowing it to interact with the citizen and these high-value credentials. The ecosystem needs, by design and by default, to prevent RPs from using vague, self-declared policies to hide systemic linking of user behaviour, profiling, tracking and surveillance.

Only a mandatory registration certificate, which contains a machine-readable list of registered attributes, allows the Wallet Unit to automatically warn the user or block a transaction if the RP requests information beyond its registered scope. This would transform the legal act of registration into an active technical barrier against "over-identification" and "over-sharing".

Furthermore, if a user's wallet must query a central registrar API to verify an RP request, that registrar (often managed by the State or a mandated entity) can compile a history of the user's access activities and the services they visit (it receives *"the unique identifier of the Relying Party"* and *"the identifier of the intended use of the Relying Party for this presentation request"*). Such queries constitute behavioural tracking (via "phoning home"), allowing the registrar to observe user behaviour in real-time and materialise different data protection threats (linking, non-repudiation, detecting, etc.). In contrast, a mandatory registration certificate allows the wallet to perform verification locally, without leaving the device and making no external queries, ensuring that the registrar remains blind to which RPs the user is accessing. We are also sceptical that Member States can comply with the SLA for an API of this nature if registration certificates do not exist (will all requests be answered in a reasonable time? will there be an adequate level of availability for such a critical function?).

Therefore, from the AEPD's point of view, it is imperative to implement mandatory registration certificates to fully meet the GDPR and eIDAS2 principles and requirements across all EUDI Wallet scenarios and use cases in all Member States. Both the Implementing Acts and the ARF must explicitly mandate/support this obligation to ensure compliance and protect fundamental rights.