DSR PROTOCOL · PROCUREMENT BRIEF

Why DSR is with the grain of the EU Digital Product Passport architecture

The EU chose a specific design: a thin central registry that points to passports each company hosts itself, with the standards work pointing to Verifiable Credentials rather than public blockchain. DSR was built to that exact shape.

This brief sets out, plainly, what the regulation's architecture is and why DSR's design matches it on the points that are expensive to retrofit — ownership and lock-in, how authenticity is proven, and how you pay. It also states clearly what is live today versus what switches on per product group as the EU's acts take effect.

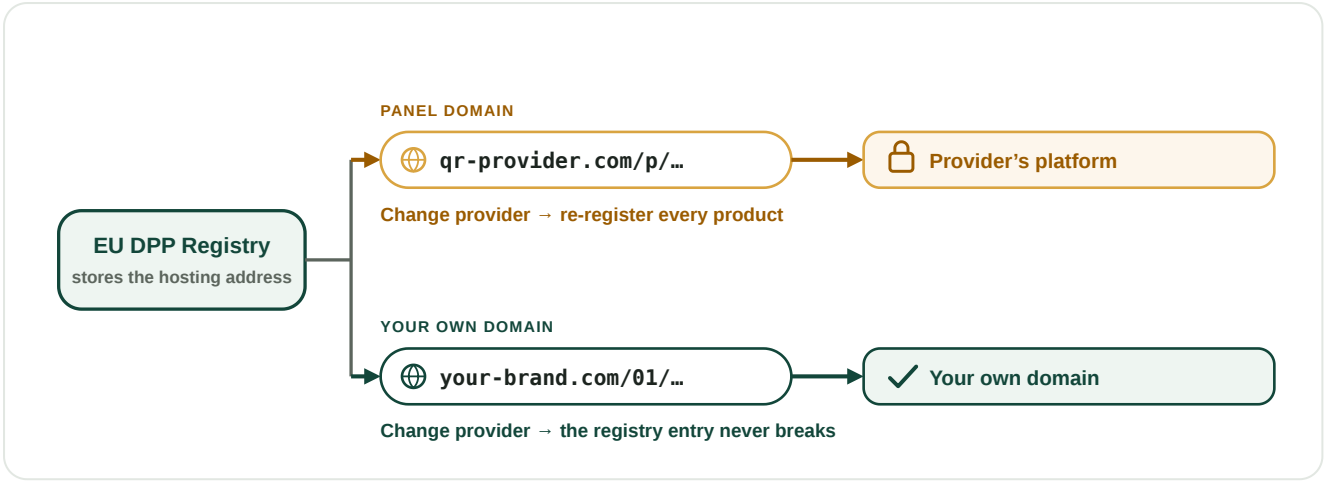
The architecture the EU actually chose

- A **thin central registry** (ESPR Article 13), operated by the European Commission, that stores the product **identifier, the hosting address, the operator's identity and the customs code** — **not** the passport content.
- The **passport content stays with the economic operator** or its provider; the registry simply **resolves** to wherever the passport is hosted. This is what "decentralised hosting" means in the regulation — a statement about the ecosystem, not about any one vendor.
- The identifier is carried by a **GS1 Digital Link** in a QR or DataMatrix on the product.
- The standards work (CIRPASS, JRC, CEN/CENELEC) points to **Verifiable Credentials / decentralised identifiers**. "Blockchain" is an optional layer someone can sell you; it is never a mandate.

Three design choices, side by side

DESIGN CHOICE	DSR PROTOCOL	COMMON ALTERNATIVE MODELS
Where the passport lives	**On your own domain** — the hosting address the EU registers is **yours**. Change platform or re-point later and the registry entry never breaks. This is **decoupled** (your data, your domain, one authoritative copy), not "decentralised".	On the provider's panel domain — so the EU registry records the **provider's** address. Migrating means re-registering the hosting address for **every product**: lock-in at the registry layer, not just on the label.
How authenticity is proven	Offline-verifiable **W3C Verifiable Credential** signatures plus an **append-only, tamper-evident** version history. Trust is decoupled from the host: a scan verifies **without** calling back to a server, and the chain shows nothing was silently rewritten. No blockchain, token or wallet.	Either a **live database lookup** (verification depends on the provider staying up) or a **public blockchain / token** layer you must keep running — heavier to operate and against the direction the EU standards bodies are taking.
How you pay	**One flat, published subscription.** Passports, scan volume and your own domain are included; **no per-passport fee and no per-scan overage**, so a popular product is never an extra bill.	A **fee on every passport** (often layered: application, registration, verification, hosting, platform) plus year-one onboarding — so cost rises with the size of the catalogue and with success.

What the EU registry actually stores: your hosting address



The registry is a thin index of **hosting addresses**. Register a **provider panel-domain** and migrating means re-registering every product; register **your own domain** and the entry never breaks when you change platform.

What this means for you

NO LOCK-IN AT THE REGISTRY LAYER

Because the registered hosting address is your own domain, you can change provider without re-registering a single product with the Commission.

VERIFIES ANYWHERE, EVEN OFFLINE

Authenticity is proven from the signed credential on the scan itself — no round-trip to a server, no dependence on anyone’s uptime at the border.

COST THAT DOESN’T PUNISH SUCCESS

A flat plan with passports and scans included means a viral product is a win, not a rising invoice.

Scope — what is proven today

Live today: the passport, the GS1 Digital Link resolver, own-domain hosting, W3C VC signatures, the append-only tamper-evident version history, and an independent continuity back-up for the regulated availability period (ESPR Art. 10(4)).

Registry registration is credential-ready across Simulated, Acceptance and Production environments; **live production registration activates per product group** as the EU’s delegated and implementing acts take effect.

Roles are clear: DSR hosts the data and the edge-resolvers and is **Registry-Integrated and eIDAS-ready**. DSR is **not** the registry and **not** a Trust Service Provider — the economic operator remains the regulatory addressee and applies its own seal at the registry gate (Bring-Your-Own-Seal).

Architecture summary for evaluation; not legal advice. The applicable scope and dates for each product group are set in the relevant delegated act under ESPR (Reg. (EU) 2024/1781).