EU Digital Identity ambitions: A look under the hood – weeks from the first deadline

In a few weeks, the EU Digital Identity Wallet is due its first real-life launch deadline. At the start of 2027, all EU countries will have at least one EUDI wallet offer live – At least, that is the plan. Yet, compared to five years ago; the public narrative for Digital Identity put out by EU institutions and countries sounds muted. The "privacy", "convenience" or "security" appeals still feature on Europa. But selling the idea to you or me, as end-users and "data subjects" is no longer the priority.

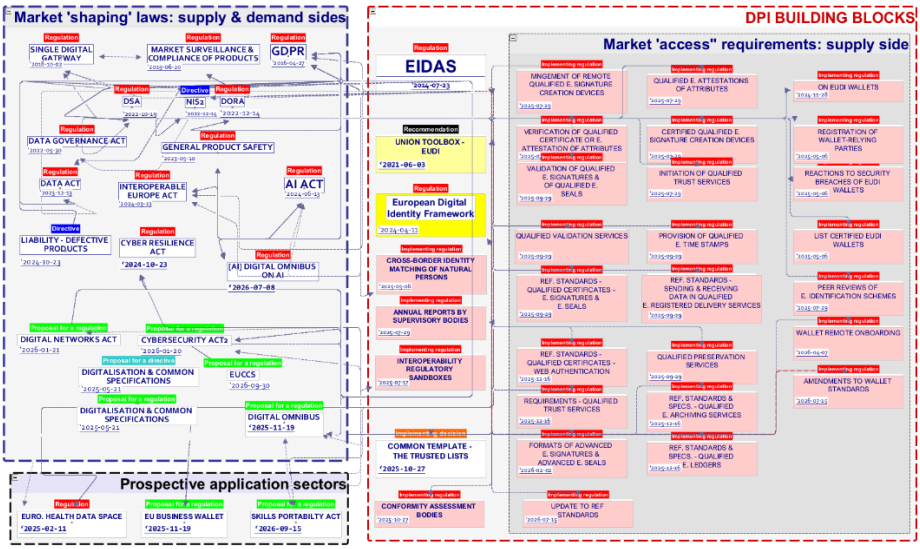
What matters to the EU right now is that the public-private supply-side ecosystem it has cultivated for years, delivers the various components of its live *Digital Public Infrastructure* (DPI) in time for December 2027, its second, and arguably more critical deadline. From 24 Dec 2027, operators in a number of key sectors including banking, healthcare, utilities, social-security, hospitality - those who already need a proof of ID from their customers/users – as well as large online platforms— will be required to accept EUDI wallets as an alternative to presenting one's legal ID. In EIDAS 2.0/EUDI lingo, these private sector operators become *wallet-relying parties.* In real life, the DPI will likely rely on those businesses to sustain its ecosystem.

It is not too difficult to imagine how this "requirement" to participate, from which SMEs are temporarily exempted, will play out on those large corporate players. It can, and probably will, nudge them into becoming a powerful constituency favouring the EUDI wallet over any other form of ID. The point of the EUDI wallet is to enable an entirely automated verification of your identity as *legally secure* as an in-person check of your ID/passport. To the corporate operator, this is not cost-free. But the first savings could come from eliminating the job of the person still employed because that legal obligation to check ID exists, including as you check in a hotel, a hospital, a flight or a train. Adding to this, sector-specific laws already adopted (in Banking and Healthcare), others in the pipeline (in Education), further reinforce the obligation to enable the EUDI wallet option. Theoretically, as the customer, user or patient, you can still turn up with your paper-based passport or ID. But if the law demands that a business goes to the effort of enrolling as a wallet-relying party while making the processing of your paper ID costs them extra (as for a Bank's KYC)..How long will it be before they decide this makes you too much trouble to bother with?

Exactly how much the operations of this ecosystem will cost and who will pay is not entirely clear yet. Member states may charge for professional use of qualified signatures but personal use must be available free of charge. Data minimization rules may mechanically reduce risk and costs on all involved. By law, the EUDI will be regarded as the highest security level option. How this is translated and implemented by the multiple participants in this ecosystem follows an interesting logic which deserves a visual explanation:

In EU law, access to the EU single Market follows the same logic for Software as applies to any other product.

Generically, the process involves
1) One or more law(s) which determine "essential requirements" applying to the product. For software, this also includes *cybersecurity* requirements
2) those "essential requirements" are translated into *Standards* made officially applicable by another law (typically an *implementing regulation*)
3) Compliance, verification, certification and audits are done through processes and by bodies, all officially identified through laws.

In this instance, the entire set had to be created from scratch – and this explains the quasi-uninterrupted flood of EIDAS 2.0/EUDI regulations issued in the last two years.

Let’s remember that the expected output of this complex machinery is *trust* and, for now, it only exists on paper. [Online version with active links here]