mourocapital

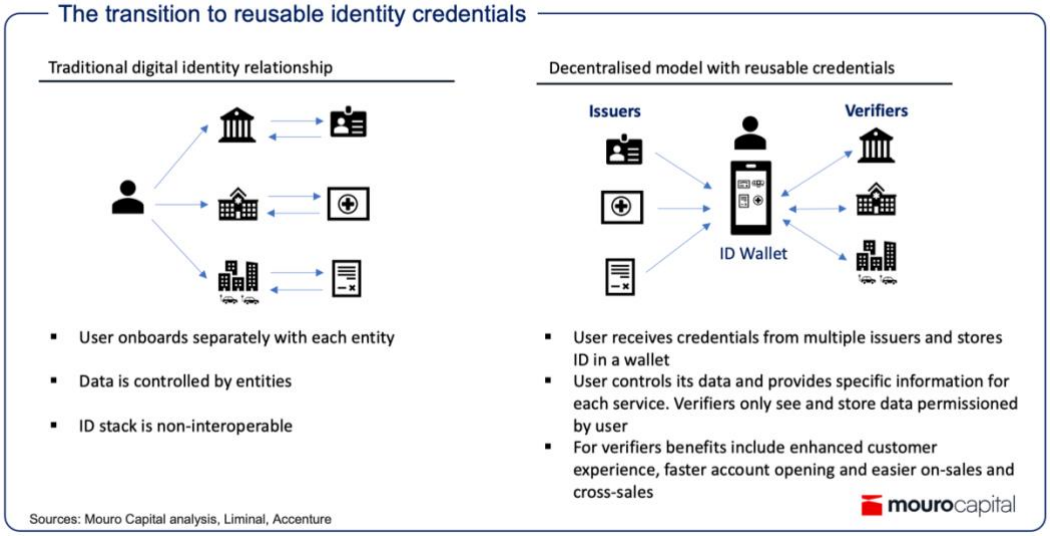
Moving to a decentralised identity model and reusable credentials – a paradigm shift or an implementation nightmare?

In commercial and financial terms, data is a regulated commodity: everyone, from banks and other financial organisations to healthcare providers, retailers and telecommunication companies, clamours for our information and (hopefully) goes to great lengths to manage it sensitively and securely.

But it can be a burden. Every online interaction begins with negotiating consent for what data we share and how it is managed; every transaction is wrapped up in the exchange of personal information from buyer to seller; every step in our online existence is cemented by the transfer of another – the same! – set of data about ourselves. And it remains unclear whether this endless sharing of data benefits us as individuals or the many organisations who covet so much insight into our behaviour.

At a high level, the problem is that the internet was not designed with a human identification layer. This led to centralised models where a consumer has to onboard separately with each entity and end with tens or hundreds of accounts and passwords.

While self-sovereign or decentralised identity initiatives have been launched over the past years, we believe Europe's Electronic Identification and Trust Services (eIDAS 2.0) can revamp the way we manage digital identity. In doing so, it creates a European Digital Identity Wallet (EDIW) that's valid for public and private services and readily available to citizens and businesses alike: in short, a single source of data that can be rolled out every time we're asked to credentialise ourselves. This is not insignificant since physical documents are being used in the digital world, which is far from optimal.



While the wallet will be voluntary for individuals, most public and private sector bodies that want our information will be required to use strong authentication protocols for online identification and accept the wallet as a means of doing so. And, as a consequence, its acceptance will be mandatory across areas like healthcare, energy and banking.

Such a paradigm shift in the EU's approach merits close attention (hence this article). Individuals are being handed more control over their data, rather than passing swathes of information with each unique transaction and compiling separate accounts and passwords for every online relationship. We expect eIDAS2.0 to set a new standard for governments and regulators to think about identity and how private and public agents engage with it, as a precursor to a new kind of decentralize or self-sovereign identity.

So, why are reusable credentials significant and what are the implications of the change?

For the customer: greater control, security and data privacy are key. For identity verifiers: we see new opportunities to drive further innovation and provide an online experience that was impossible until now. But let's look at that in more detail.

Individuals and businesses

The shift will ease scalability and remote onboarding to a vast number of user cases, from opening a bank account, to signing documents or renting a car. It will allow customers to select what credentials they pass on, without necessarily providing a whole sensitive document as evidence. If proof of age is required to make a purchase or sign an agreement, an individual will simply be able to show a trusted confirmation of age, nothing more.

What's more, the proposed changes should make it easier to create and use digital signatures to streamline agreements: to file and submit tax returns, for example, and complete other online applications. That presents a significant opportunity to reduce time, and therefore spend, on administrative tasks and procurement functions.

Identity verifiers

There are benefits for financial institutions, telcos, healthcare operators, energy, and utility providers, among others, in their ability to further digitise services and enhance the customer experience of

interacting with them (no more taking a recent utility bill into a bank branch or scanning documents to upload to a site). Faster account opening, easier on-sales and cross-sales should all flow out of the implementation of digital wallets, and the need to independently verify documents should dissipate.

Look at the example of BankID in the Nordics, where a similar scheme saw times for account opening fall from five days to just five minutes. In Sweden, BankID is now used by 8.4 million people, over 99% of the population. With an ecosystem of 6,000+ organization the scheme has been used 6.7 billion times which translates in ~800 times per person per year.

This has a compound effect of reducing compliance spend for regulated industries, where the cost of conforming with standards is high and the penalties for non-compliance are higher still. Banks will still have to hold on to customer data for regulatory purposes, as well as rely on third party solutions for things like monitoring politically exposed people, potential sanctions violations, fraud, and AML etc, but document verification and other authentication processes for the vast majority of customers could be concluded directly via the digital wallet.

Digital ID platforms

Merchant verification processes are expected to change from standalone and siloed to modular and flexible, with the ability to accept different forms of verification. Europe, with diverse regional government IDs, may be the optimal market to launch just such a platform to orchestrate verification.

Moreover, point solution identity vendors face challenges in a competitive market, struggling to differentiate themselves and requiring flexibility. As the market matures, enterprises demand a simplified vendor stack, and ID verification providers provide these solutions by offering a single platform that can integrate with specialty endpoint solutions.

We can already see evidence of a shift from point-solutions to multiplayer orchestration in vendors like Alloy, Sardine, or Persona in the US. These are emerging as one-stop-shops for identity solutions, offering one API integration for multiple access points from other vendors like Equifax and Experian for credit data, ComplyAdvantage for watchlist screening, and Onfido for ID verification. Mouro Capital's own portfolio partner, Trulioo, which enables instant online verification, recently acquired Denmark's HelloFlow to enhance its digital onboarding.

So, what's the big picture?

At Mouro Capital, we see the need to verify identity at all times as an opportunity touching multiple players in the value chain and are excited about the following areas.

The digital ID wallet space will likely get crowded pretty soon with multiple operators, including Big Tech like Google and Apple, bringing their own solutions to market. This proliferation should help to improve take up which, don't forget, is still optional for individuals in an area that is generally greeted with scepticism by the public. But as these players build partnerships and extend additional services to their enlarged user base, the shift to a customer-owned credential model means that providers will likely differentiate themselves by building capabilities across multiple use cases and verticals or by deepening a solution for a targeted customer segment.

Successful providers will be those who go from being a simple repository of documents (who are you?) to a provider of functional capabilities across multiple use cases (what can you do?). As an example, we see digital signature opening opportunities for contract lifecycle management and related services in the SME space.

The decentralization of data introduces the potential for data to be enriched and shared between financial institutions (subject to regulations). This has the potential to not only increase efficiency but also to drive deeper insight on KYC/AML and fraud review.

Interoperability can also enable the movement of credentials between different contexts and the creation of ecosystems. At a personal level, an example is around workforce solutions, where HR, payments and proof of skills and verification of education credentials are performed in one platform. But this could also enable enhanced supply-chain and shipping as credentials can also be applied to devices or goods.

The challenge, of course, is for Europe's regulators to adopt a degree of standardisation across their policy implementation to support this expanded platform. Without that, the risk of fragmentation and the need to integrate multiple digital wallet variants will send IT costs soaring once again and soak up any potential benefit. The paradigm shift to support interoperable networks will rely on public-private partnerships and fully fledged ecosystems – with supporting standards, policies and trust frameworks – that give consumers full data mobility.

Last word

If implemented well, eIDAS 2.0 will transform the online safety, privacy, and user experience of Europe's citizens, placing them at the centre of the identity ecosystem and giving them greater control of their own identity attributes. While the economics are still blurry, there is a long-term potential of cost savings to both public and private sector organisations, broadening the scope of their own operations and extended networks, consolidating whole industries and beyond. It's that rarest of things: a holy trinity of benefits to industry, consumers, and regulators alike …if implemented well.