

Welcoming the Wallet

What the new European Digital Identity Framework means for citizens, governments and businesses



[thalesgroup.com](https://www.thalesgroup.com)





The concept of digital identification is already well established, and using a smartphone to board a plane or prove vaccination status is second nature to many millions of people. In the EU however, while many states have made electronic identification available and domestic use is growing, the development of internationally accepted electronic identity (eID) systems has been piecemeal and inconsistent.

Today only 14% of key public services across all EU Member States allow cross-border authentication with eID and, according to the European Commission there is a need to improve the:

- coverage of notified eID schemes
- acceptance of these schemes by the Member States
- use of cross-border authentication
- user experience of the service
- acceptance of national eID schemes by the private sector.

This is all about to change, with the introduction of the Commission's latest legislation on European Digital Identity - what we're calling eIDAS2. The first iteration of eIDAS was adopted in 2014 and created an EU regulation on electronic identification and trust services for electronic transactions.

eIDAS2 brings a major update meaning that by September 2023, each EU Member State must make a digital 'wallet' available to every citizen who wants one. At the same time, service providers in both public and private sector organisations, such as banks and telcos, will have to accept it as proof of certain personal attributes. From providing electronic signatures to paying fines or accessing health services, EU citizens will be using the eIDAS wallet, in every Member State, and generating millions of authentications every day.

This paper seeks to provide a background to the changes, and to explain how the new system will impact citizens, private businesses and public sector organisations.

"... the Commission will propose a secure European eIDentity ... that any citizen can use anywhere in Europe... a technology where we can control ourselves what data and how data is used."

Ursula von der Leyen,
President of the European Commission,
in her State of the Union address, 16 September 2020



Section One

Where we are now, and how we got here

Over the past few decades, as life and business have become increasingly reliant on digital transactions, the need for trust online has become critical. From booking a flight to signing a major business deal, our transactions depend on a robust, efficient way to prove we are who we say we are, electronically.

Businesses, services and nation states have developed trust infrastructures in different ways, and at different rates. This can lead to interoperability issues on a technical or legal level. For example, an electronic document issued in one country - like an electronic driving licence or a business contract - might not be readable or legally acceptable in another.

While this could be an inconvenience anywhere in the world, in the EU it's essential to the objective of giving equal rights to citizens across the Single Market. The EU is all about making cross-border business smooth, secure and efficient, so there's an added urgency to the search for solutions. In 2014, the EU Regulation on Electronic Identification and Trust Services - eIDAS - was adopted, and was intended to sort everything out.

By creating consistent standards across the EU for electronic authentication, eIDAS has made great progress in establishing norms and developing infrastructure. However, take-up and implementation has been patchy, to say the least.

Today about 60% of the EU population has access to digital ID, but only 14% of public services allow cross-border authentication. Meanwhile, citizens want to see this improved, with 63% saying they want a single secure digital ID to access services, according to a 2020 Eurobarometer survey¹.

The reality today is that while some institutions in the public sector issue and accept cross-border eID, many still don't. Acceptance in the private sector varies from poor in some countries to non-existent in others. This clearly isn't good enough for the EU Commission.

The new proposal sets out to amend eIDAS to solve the problem by introducing a Digital Identity wallet. Any EU citizen or company will be able to request one from their Member State (on a voluntary basis) while its acceptance will be mandatory for specific service providers in all EU Member States.

¹ Attitudes to the impact of digitalisation on daily lives - European Commission
<https://europa.eu/eurobarometer/surveys/detail/2228>



Section Two

The Commission's Proposal

Published in June 2021, the Commission's proposal for eIDAS 2 will make issuing eIDs mandatory. Implementation is expected from late 2022, and Member States will have 12 months to make European Digital Identity Wallets (EDIW) available to all citizens who want them.

The wording of the initial proposal describes a transition 'from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities'. In practice, this means states will have to notify at least one eID scheme, and have a unique and persistent identifier in the dataset. This will take the form of a digital wallet - the EDIW - with common technical specifications, and every Member State will have to issue one.

eIDAS2 brings changes for nine existing types of Trusted Services, as well as adding four new ones. These are:

- 1 Qualified electronic attestation of attributes verified against authentic sources
- 2 Electronic ledgers
- 3 Qualified electronic archiving services
- 4 Qualified service for the management of remote eSignature creation devices (QSCD).

Final regulation and a Toolbox of resources and measures for implementation is expected by September 2022. Member States will then have a year to roll out the EDIW, either by issuing it directly to citizens, or by contracting private businesses to do it on their behalf.

"The European digital identity will enable us to do in any Member State as we do at home without any extra cost and fewer hurdles. Be that renting a flat or opening a bank account outside of our home country. And do this in a way that is secure and transparent. So that we will decide how much information we wish to share about ourselves, with whom and for what purpose.."

Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age

in a Press Conference on June 3rd 2021 announcing the EU Digital ID wallet





Section Three

The Wallet

We're familiar with branded wallet products from private sector organisations like Apple, Google, Samsung and others. So how different will the EDIW be?

First and foremost, as Ursula Von der Leyer stated, it will be “a technology where we can control ourselves what data and how data is used.” Sovereignty and data privacy will be at the heart of EDIW design. As such, it will be compliant with existing EU legal frameworks such as the General Data Protection Regulation and the Cyber Security Act, as well as benefitting from greater security and privacy measures.

Strong cryptography will be a feature of the EDIW when issued as part of an official eID scheme and will have the highest level of assurance (High). It's also a condition of the Commission's proposal that Member States must provide mechanisms to validate attributes. There's also a special article - 10a - within the legislation on preventing and managing security breaches.

In terms of privacy, a key feature will be the selective disclosure of attributes. The user provides only the authentication needed for a given transaction, and all other data remains private. To take a simple example, if you use the wallet to prove your age, you won't also have to show your address, or any other information as you do today when showing your physical ID card.

Behind the interface, personal data relating to EDIW is held separately (both physically and logically) from any other data. In addition, information about the use of the wallet remains private i.e. the issuer won't collect data on wallet usage.

Second, it will share common features with all others across 27 Member States. Most significantly, the EDIW will be, by law, useable cross-border in the EU. Adoption will be favoured by a strong push towards the ecosystem as Public and Private relying parties across Member States will be required to accept EDIW as a proof of identity and attributes. As an EU citizen you then have the guarantee that you can use the data stored in your EDIW everywhere in EU just like if you were in your home country.

In terms of look and feel though, you may see many different designs. That's because Member States and the providers they commission will be able to make the wallet look and perform how they want. We expect there to be a wide range of designs, skins, tools and features, just as we see now in competing products from the tech giants.

² Digital identity: towards a European digital wallet? - European Commission
<https://hellofuture.orange.com/en/digital-identity-towards-a-european-digital-wallet/>

60% of the EU population has access to digital ID²

Section Four

Uses for the Wallet

The wallet's use is still being defined. However, it is pretty certain to include the provision of online identification and electronic signatures. The wallet probably won't equate to a digital version of a physical card, so it won't necessarily replace ID documents in everyday use immediately. However, for online transactions, including applications for public services, the wallet should provide acceptable cross-border ID.

Other priority services which should be part of the scheme include driving licences, prescriptions and health records, digital travel credentials (which could replace passports and ID cards within the EU), payment instruments, and proof of qualifications.

As use of the Wallet develops and acceptance grows across the block, other uses will probably be added. These are likely to include a digital version of the European Health Insurance Card, and documents needed to register a motor vehicle, register a change of address, or claim a pension.

The wallet could be used in education to apply for admission or for study grants, and it should be possible to request and upload proof of diplomas and certificates.

These are largely within the domain of public services. In the private sector, we expect the wallet to be used for identity proofing, age verification, banking, hotel check-in, mobile subscriptions and so on. As 5G develops across the continent, the wallet should gradually become integrated with the Internet of Things, and it may become commonplace to store your digital car keys in the EDIW.





Section Five

Who will issue the Wallet, and who will accept it?

Each EU Member State will be mandated to notify to the European Commission at least one form of EDIW. The wallet can be issued directly by a department of the state, or by a private-sector provider commissioned by the state and notified as such.

Banks, telecoms businesses and utilities are likely private-sector providers, with potential benefits in customer relationship management, retention and cross-selling. However, private businesses won't be able to monetise the wallet directly, as the EDIW must be freely available to all citizens who want it. Private issuers will also need to attain precisely the same levels of security and privacy as government providers, and are likely to turn to third party experts for guidance.

The wallet must enable verification of minimal ID attributes (name, date of birth) as well as additional attributes like address, age, gender, civil status, nationality, qualifications, permits and licences, and financial and employment data.

The EDIW will be accepted for authenticating people for public services from launch. It's also expected that private services in transport, energy, banking and other sectors will accept EDIW at an early stage. Smaller businesses - for example gyms and hire-car companies - should begin to accept it shortly after implementation.

The initial list of sectors that should use the wallet is:

- 1 Transport
- 2 Energy
- 3 Banking and financial services
- 4 Social security
- 5 Health
- 6 Drinking water
- 7 Postal services
- 8 Digital infrastructure
- 9 Education
- 10 Telecommunications

Very large online platforms - defined as having more than 45 million average monthly consumers in the EU and covering social media and other global providers - will also be obliged to accept the wallet.

A Commission review is expected within 18 months of implementation. If that review finds that uptake and adoption have been sluggish, there could be renewed effort or stricter enforcement to widen acceptance.

Section Six

Building the Toolbox

The new eIDAS initiative is about establishing common practice and compatible systems. If it's going to succeed, Member States will need to work from the same principles, and follow the same rules.

The toolbox for a European Digital Identity Framework' will be developed through cooperation between Member States, the Commission and, where relevant, private sector operators. The Toolbox should describe everything the Member States need to build the appropriate technical architecture to provide the EDIW, and to implement the architecture to support it. It will contain a set of common standards and technical references, practices and guidelines.

A big chunk of the Toolbox will be familiar, in that it will re-use European and international standards where appropriate. However, there'll also be some important work around generating and using identity attributes, as well as functionality and security. The Toolbox also looks at governance of the whole, EU-wide eIDAS system.

An outline on the technical architecture for the Toolbox is currently being finalised, and in 2022 specific standards, references and guidelines will be agreed before publication. Tests and pilots will follow, with Member States expected to implement their plans by autumn 2023.



"EU citizens not only expect a high level of security but also convenience whether they are dealing with national administrations such as to submit a tax return or to enroll at a European university where they need official identification. The European Digital Identity wallets offer a new possibility for them to store and use data for all sorts of services, from checking in at the airport to renting a car. It is about giving a choice to consumers, a European choice..."

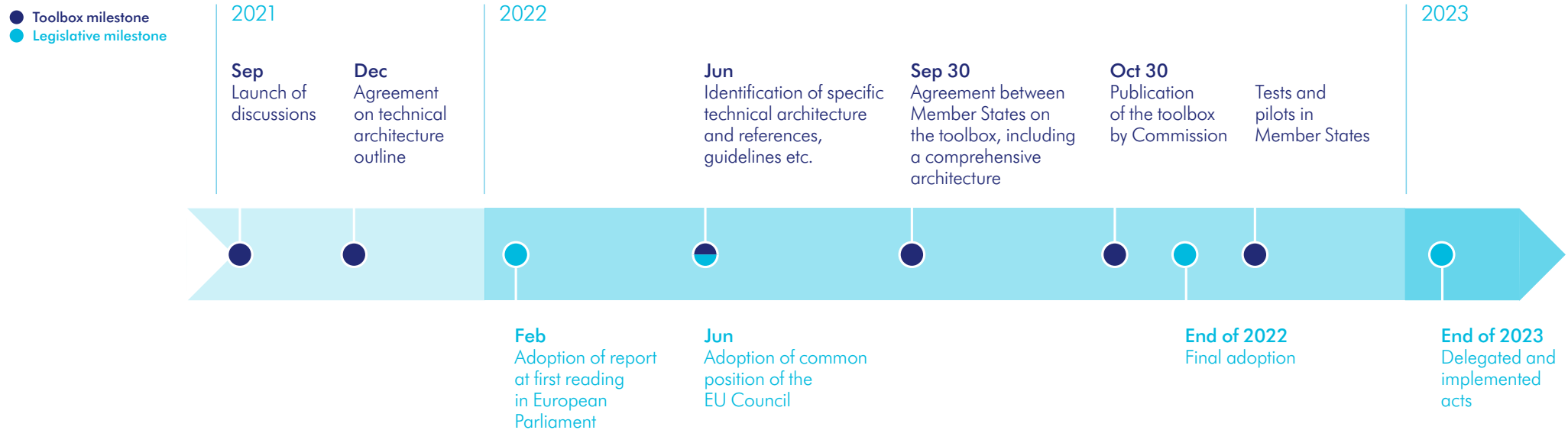
Thierry Breton, Commissioner for Internal Market

in a Press Conference on June 3rd 2021 announcing the EU Digital ID wallet.

Section Seven

The Timeline

- European Commission's
initial planning



Section Eight

How Thales can help you prepare for eIDAS2



Thales is a global leader in the technology of trust. Our work in data security, trusted identities, and encryption has made us a partner of choice to government agencies and major international corporations, as well as to clients in defence, aerospace and transportation. Within the field of identity, we are the global leader in the production and issuance of civil identity documents. We're building on this experience by taking a role in a growing number of digital identity schemes such as the Queensland Digital License and the Florida Digital Drivers' License.

Our teams have been collaborating with governments, public services and businesses on eIDAS since its first iteration in 2014, and we have a range of eIDAS-certified solutions that are currently used in identity schemes in Europe. We're currently working with dozens of clients on preparation for the new eIDAS2. Our technology and expertise can help support the EU and its Member States accelerate the deployment and adoption of the wallet by providing support for:

- The definition of the technical architecture
- Standards and references guidelines
- Toolbox
- Tests and pilots

As a European player with experience in data protection solutions, we can help providers manage privacy compliance and put the citizen in control of their personal data and who can access it. This expertise also ensures that any service built on our technology will meet the required security certifications and comply with the Cybersecurity Act.

While security is at the heart of our business, we also understand that any technology in people's hands must be user-friendly for it to be widely adopted. This is why we place great importance on the user experience of our Digital Identity solutions.

We are a long-standing identity solutions provider to the Public and Private sectors and, as such, we understand the needs of various industries as well as the need to work with all actors in the eco-system to ensure broad acceptance of the solution by relying parties and consequently, citizens.

Thales supports Digital Identity deployments with the following products and services:

- Secure digital identity wallets
- Identity proofing
- eAttestation issuance solutions (eDiplomas, health certificates, banking credentials etc.)
- Trusted authentication
- Digital signature
- Data encryption
- And much, much more

Glossary of key terms



Attestation - evidence or proof, in this case in electronic form and delivered through the European Digital Identity Wallet (EDIW).

Attestation provider - public and private sector body providing evidence of attributes and eligibility. These could include transport departments, health boards, insurance companies, employers and universities.

Attributes - personal details, which a Relying Party may need to verify in order to provide their service; for example age, address, nationality, permits and licences.

Authentication - a “one-to-one” verification of a specific person’s identity. It compares specific attributes (PIN code, biometric information etc.) with reference data already stored in a system

European Digital Identity Wallet (EDIW) - a service that allows the user to store identity data, credentials and attributes, to use them for authentication on and offline, and to create qualified electronic signatures and seals.

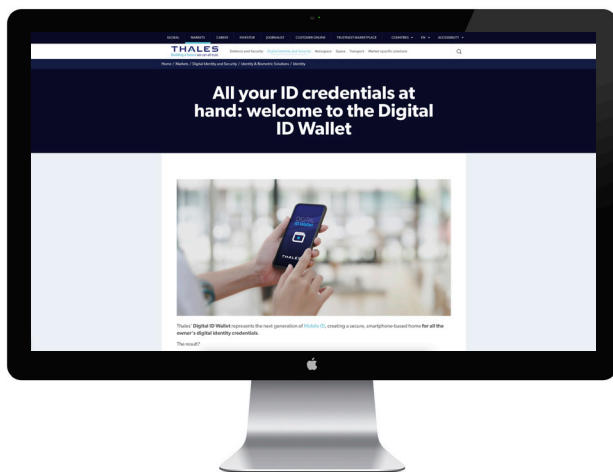
eIDAS - the EU Regulation on Electronic Identification and Trust Services. The original eIDAS regulation (eIDAS1) was implemented in 2014, while a new, significantly strengthened version (eIDAS2) is due for implementation in September 2023.

Identification - The action or process of collecting and verifying information to represent unambiguously a natural or legal person

Level of Assurance – Under the eIDAS regulation the term “level of assurance” refers to the degree of confidence in the claimed identity of a person i.e. how certain a service provider can be sure of the identity of the person authenticating to the service. The three levels of assurance are as follows:

- **Low:** for instance, enrolment is performed by self-registration in a web-page, without any identity verification;
- **Substantial:** for instance, enrolment is performed by providing and verifying identity information, and authentication of the user thanks to either a user name and password and a one-time password sent to your mobile or through facial recognition.
- **High:** for instance, enrolment is performed by registering in person in an office, with identity verification carried out against an ID document.

Public and Private Relying Parties – public sector bodies and businesses whose services are required to use strong user authentication, and who will be required to accept the EDIW as proof of identity and attributes.



For more information or to discuss any aspect of this paper, please visit:

www.thalesgroup.com/en/digital-id-wallet

THALES
Building a future we can all trust



Welcoming the Wallet

What the new European Digital Identity Framework means for citizens, governments and businesses

thalesgroup.com