The New EU Digital Identity Wallet:

Four Key Challenges and the Route to Success

Introduction

The European Union's Digital Identity Wallet (EUDIW) initiative has a simple aim: to provide citizens and residents with a safe and easy way to prove their identity and share information with public and private organizations across the bloc, without needing physical credentials.

The wallet will be able to store all attestations, such as social security information, health-related documents and educational qualifications as well as identity documents, in one place on an app. It will also enable financial transactions.

It should help streamline access to critical services such as banking, healthcare, education and government benefits, and make service delivery more effective. Data protection and user control over identity data are core elements.

The goal is for 80% of EU citizens to be using digital IDs by 2030[1]. Other key performance indicators (KPIs) will focus on the number of wallet transactions completed and the number of qualified signatures issued by wallet users. To accelerate the initiative and increase its success, the European Commission has launched a pilot program. The EU member states, along with enterprises and technology partners, have been invited to submit a proposal to secure funding for their pilot and put the wallet to the test in real-world scenarios.

The EUDIW will need to overcome certain challenges if it is to succeed. Uptake by EU citizens and organizations, and evidence of significant ongoing usage, are critical. If citizens can't enroll in the wallet and complete transactions in a frictionless way the program will likely fail.

Usability must also be combined with trust and integrity. Unless the wallet is completely secure it will lose all credibility.

This report examines the four main challenges facing the EUDIW. It also highlights the solutions that will help ensure the KPIs can be met successfully.

[1] Europe's Digital Decade: digital targets for 2030, European Commission, https://www.google.com/url?q=https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en&sa=D&source=editors&ust=1662481802235348&usg=AOvVaw2JiDf7jrfbZhlQWhsK1Bxy

1st Challenge

Convincing Citizens To Enroll

The success of the EUDIW depends in large part on how many citizens sign up. The target – a core KPI of the project – is that by 2030 four out of five EU citizens will use a digital ID solution, allowing them to exercise their digital freedom while preserving their right to privacy.

The good news is that demand exists for single secure digital identity services. Globally, two-thirds of respondents to iProov's recent consumer survey said they already have a single digital identity service or would use one.

This suggests consumers understand that needing to use a separate username and password for every website or mobile app is inconvenient and represents a security risk. In Italy and Spain, acceptance tops 70%. German citizens are more wary though, with only half the respondents using or willing to use a single digital identity service.

Do you think it would be easier if you had one secure digital identity that you could use to help you access online services without sharing too much information with individual websites?

	Global	Spain	Italy	Germany
Yes, I already have one	14.5%	12.8%	25.3%	7.2%
Yes, I would use one	50.3%	58.0%	52.2%	42.9%
I'm not sure	25.7%	22.6%	16.3%	35.8%
No, I would not use one	9.6%	6.6%	6.3%	14.1%

Maximizing Wallet Uptake

Although there is clear consumer interest in having a single digital identity service, it will be incumbent on the EUDIW to turn that interest into action. It's also worth noting that 35% of global consumers say they are either not sure about digital identity services or that they would not use one. Overcoming citizens' reservations will be vital if the wallet is to maximize uptake. Security and ease of use will be paramount. Without them, trust in the system will be jeopardized and adoption limited.

If the system is not 100% secure, citizens will worry about digital identity theft. Criminals will be able to use fake or stolen identities to create digital wallets, while counterparty organizations will be unsure whether the person using an eID or signing an electronic signature is who they claim to be.

Enrollment will also need to provide:

- **A seamless user experience** – Once a citizen is convinced of a wallet's merits, getting one must be simple. A complex enrollment process raises barriers to sign-up, producing frustration and low completion rates.
- **Accessibility** – Enrollment must be open to all, regardless of technology literacy, or cognitive and physical abilities.
- **Device flexibility** – Many of the EU's 447 million people won't have the latest smartphones. The wallet must work across a wide range of devices and platforms to ensure as many citizens as possible can enroll.
- **Easy integration** – The pilots must integrate with existing eID programs.

The Biometric Face Verification Solution to Maximize Uptake

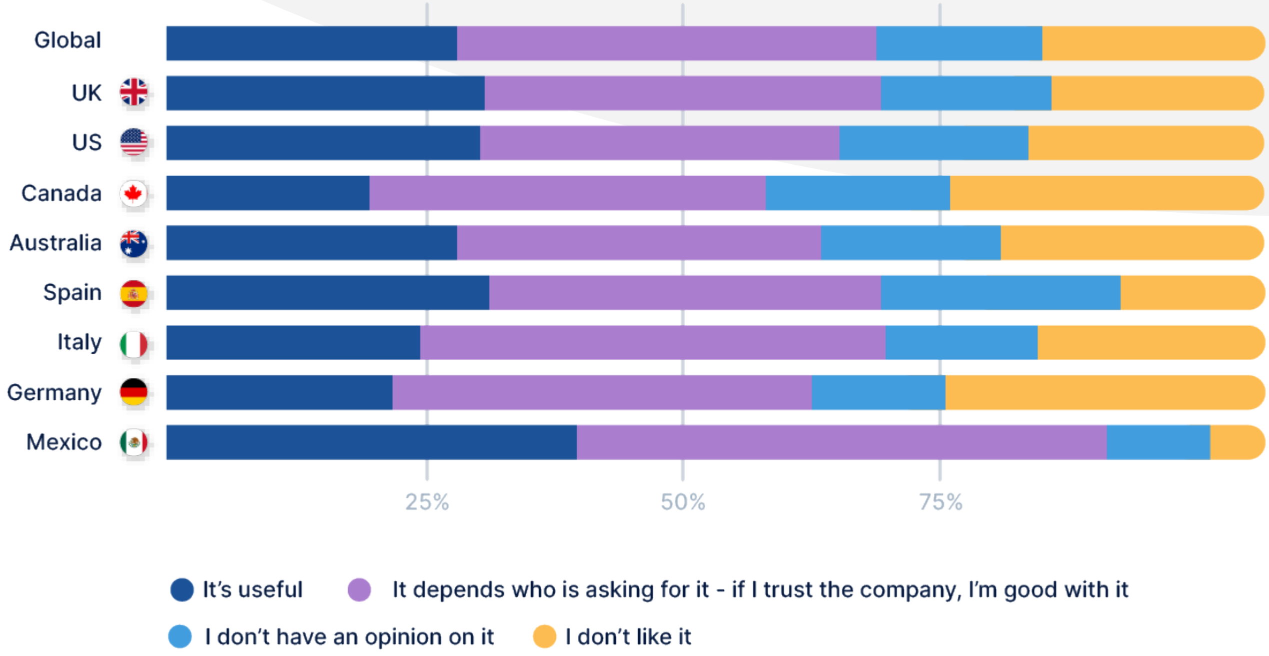
To enroll remotely and securely without needing a human check or a visit to a physical building, citizens will have to verify their identity online. The most secure, simple, inclusive and scalable way to prove that someone is who they claim to be remotely is by using a government-issued ID document and biometric face verification with liveness detection.

Other remote verification options do not provide the same security, simplicity, inclusivity or scalability. For example:

- Knowledge-based security (e.g. passwords) can be shared or stolen and does not allow an organization to be certain that the individual is who they claim to be.
- Device-based security (e.g., mobile devices) can be shared, stolen, lost and compromised – again, making it impossible to be certain that the user is who they claim to be.
- Other biometric identifiers, such as irises or fingerprints, are not typically included in government-issued ID documentation, such as ID cards, driver's licenses or passports. This means that it is not possible to verify the biometric remotely against the person's photo ID. Plus, many consumer devices are not equipped with infrared or fingerprint readers, while they usually have a user-facing camera.

Biometric face verification is also popular with the majority of consumers. The iProov survey found that more than two-thirds of respondents globally are happy to use it – provided they trust the organization asking for it.

Which of the following best describes your attitude to using face verification when you need to prove who you are online?



Biometric verification systems need to offer protection against three types of attack:

Impersonation: Where someone pretends to be someone else. The imposter is a real person, but not the legitimate owner of the asserted identity.

Presentation attacks: In which an artifact – either a physical object such as a photo or mask, or digitally created images or videos presented on screen – is held up to user-facing camera on a device. Advances in screens and 3D printing capabilities make it easier to create realistic artifacts.

Digital injection attacks: Where digitally-created synthetic imagery is injected into the data stream between the user's device and the organization's server. The videos can be deepfakes, manipulated imagery, or replays of a previous authentication. Digital injection attacks can be deployed at scale, are difficult to detect and pose a high risk.

What's more, digitally injected deepfakes are on the rise. Relatively simple to create, criminals only need a plug-in to inject synthetic imagery directly into data streams. In doing this, they're able to spoof the face verification process and compromise accounts.

Many biometric verification solutions use liveness detection to protect against impersonation and presentation attacks. But not all liveness is equal, as we will explore in the next section.

Proving It's the Right Person, a Real Person, Right Now

To ensure that enrollment to the EUDIW is secure, the verification process must protect against the full range of impersonation, presentation and digital injection attacks. Only then can organizations be assured that the person they are interacting with is who they claim to be. This requires technology that can:

- **Identify the right person** – does this person exist and have the right to access the information in the wallet?
- **Determine the person is real** – is this a human being, rather than a photo, mask or other presentation attack?
- **Authenticate right now in real-time** – is this person authenticating themselves right now, and is it not a digitally injected video, deepfake, or other replay attack?

The only way to ensure that all three of these are met is with Genuine Presence Assurance®. Other liveness detection solutions can verify identity and protect against presentation attacks but they can't protect against digitally injected attacks.

Online biometric face verification is the most inclusive and secure way to conveniently enroll citizens into the EUDIW and Genuine Presence Assurance ensures that this is done with the highest levels of security.

2nd Challenge

Ongoing Usage

As well as enrollment, another major KPI for the EUDIW project will be to maximize the number of transactions completed. To avoid becoming a forgotten program, with high initial sign-up and rapid obsolescence, the EUDIW will need to ensure that use continues and grows over time. Here's how the EUDIW can promote ongoing usage.

Flexible Authentication and Verification

Easy authentication will be critical. If every transaction is complex and/or time-consuming, citizens won't use the wallet. Too little security though heightens the risk of compromised accounts.

Striking the right balance demands flexibility. Provided their identity has been properly established during enrollment, an existing user won't need to be verified to the same extent as a completely new one. A biometric face scan can then provide the fast and easy authentication returning users seek.

Authentication should also vary according to the type of activity. Where a citizen is signing a financial document, the strongest authentication is needed. If they are logging in to check all their documents are in place before going on vacation, a lower level of identity confirmation may be more appropriate.

A similar balance applies to identity recovery. If a citizen loses or breaks their phone and needs to use a different device, they must be able to confirm they are who they say they are. Such circumstances create a huge risk that an account could be compromised, so the recovery process must be highly secure, yet not so stringent that recovery becomes near impossible.

Scalability

The EU has 447 million citizens. For the EUDIW to work, the technology will need to support a huge number of users and transactions and withstand peaks in usage.

Take-up can be broad and rapid. Among Estonia's 1.3 million citizens, 98% use its eID national identity. In the UK, millions of people rushed to create an NHS login after Covid-19 struck to prove their vaccination status. The wallet enrollment and authentication processes, therefore, have to be ready, robust and scalable.

How Biometric Face Authentication Can Ensure Ongoing Usage

By making the right face biometric authentication technology available to users, the EUDIW can enable flexible, convenient yet secure ongoing access to the wallet's services.

Usability

Biometric authentication is a quick, convenient and easy way for users to access online services. iProov survey data found that over half of consumers in EU countries are already using biometrics to unlock their mobile devices, rather than using a passcode. Once users get used to the simplicity of face verification, the alternatives of passwords and other authentication methods seem dated and slow.

Flexibility

The EUDIW must support a whole range of interactions, from secure payments through to checking a balance. Some face biometric authentication solutions will offer the flexibility to accommodate all levels of security in a way that increases the reassurance for the user while keeping the experience consistent to minimize confusion and abandonment. For example, ascertaining genuine presence will be essential for higher-risk transactions, such as signing financial documents. Meanwhile, the lower security and lighter ceremony of basic liveness would be more suitable for lower-risk transactions, such as checking documents before a holiday.

Scalability

Biometric authentication offers excellent scalability, especially when compared to identity checks through video interviews. Secure, highly usable face verification technology enables the identity verification and authentication process to be fully automated, without the need for human intervention

3rd Challenge

Providing Value for Organizations

Organizations across the EU will be required to accept the EUDIW as a form of identity verification.

What Benefits Will the EUDIW Bring to Organizations?

If the EUDIW can deliver on usability and security, it promises real benefits for businesses and public institutions.

Improved customer acquisition and retention: A smooth identity verification experience should lead to easier onboarding and access to an organization's services. As a result, organizations could expect to see higher completion rates and fewer users abandoning the onboarding process.

This would ultimately lead to a lower cost of customer acquisition and optimized revenue. Simplified authentication will then encourage repeat usage and prevent customer frustration and drop-off if accessing an existing account proves too difficult.

Protection against cybercrime: Likewise, if the identity wallet offers maximum security, then organizations can rely on it as a safeguard against online crime. According to analyses by Forrester Consulting and Hiscox, the cost of cybercrime to European organizations reached $57,000 (€50,000) per incident in 2020.[2]
A highly secure EUDIW, then, will help protect organizations from a host of criminal activities, ranging from account takeover and identity fraud to highly sophisticated digital injection attacks.

Enhancing digital transformation programs: From healthcare to banking, organizations across a cross-section of sectors have committed themselves to become digital-first. Identity authentication and verification play a large role in this as progressively more people need to carry out activities remotely.

As a means of authenticating and verifying citizens' identities, the EUDIW should help organizations progress their digital transformation programs. Relying on the EUDIW instead of building their own identity verification models has the potential to act as a large cost saver.

The potential benefits for businesses and public sector agencies are clear. To get their buy-in, however, the EUDIW must deliver on certain criteria from the start. Here's how the EUDIW can achieve that:

[2] Source:
https://www.consultancy.eu/news/4409/cost-of-cybercrime-per-incident-jumps-six-fold-to-50000

Strong security to establish trust

The wallet must offer exceptional security. For instance, financial services organizations will rely on the wallet as a digital alternative to traditional physical ID documents. This means that they will need to rely on it to carry out their anti-money laundering (AML) and know your customer (KYC) due diligence processes during customer onboarding and for providing payment authorizations. Counterparty organizations need to be sure the person using an eID or signing an electronic signature is who they claim to be.

If criminals are able to create eIDs with stolen or synthetic identities, trust in the wallet will evaporate. With the threat landscape evolving continually, the EUDIW will need to safeguard against future dangers as they emerge.

High levels of security and usability for cost efficiencies

One of the biggest potential benefits of the EUDIW is the cost reduction that it offers to participating organizations. KYC processes can be laborious and expensive. A digital identity wallet will remove many of the existing checks required, enabling customer acquisition costs to be lowered.

The EUDIW must balance strong security with usability if organizations are to take advantage of these benefits. Firms in regulated industries risk financial penalties if appropriate levels of due diligence are not met. At the same time, the need for an effortless user experience is of paramount importance. Public sector agencies and enterprises cannot afford to accept reduced completion rates or fail to meet inclusivity goals because of poorly designed enrollment and authentication processes. The best possible user experience must be delivered.

Flexible security

Security is critical but not every transaction will require the highest levels of security. Organizations will require an authentication process that is appropriate to the risk profile of the interaction. The EUDIW will need to provide the necessary flexibility to assure high risk and low risk transactions.

An effortless user experience

Security has to be balanced against user experience. The EUDIW enrollment process should not be complicated for the user. Too much security risks an increase in the effort involved, which could result in low usage levels. This, in turn, would undermine support from organizations that are obliged to accept it. Enrollment and the subsequent identity authentication process for completing transactions and attestations must be effortless yet secure if organizations are to depend on it.

How Biometric Face Verification Can Inspire Organizational Uptake

Biometric face verification will ensure that organizations see tangible value from the EUDIW.

Highest levels of security

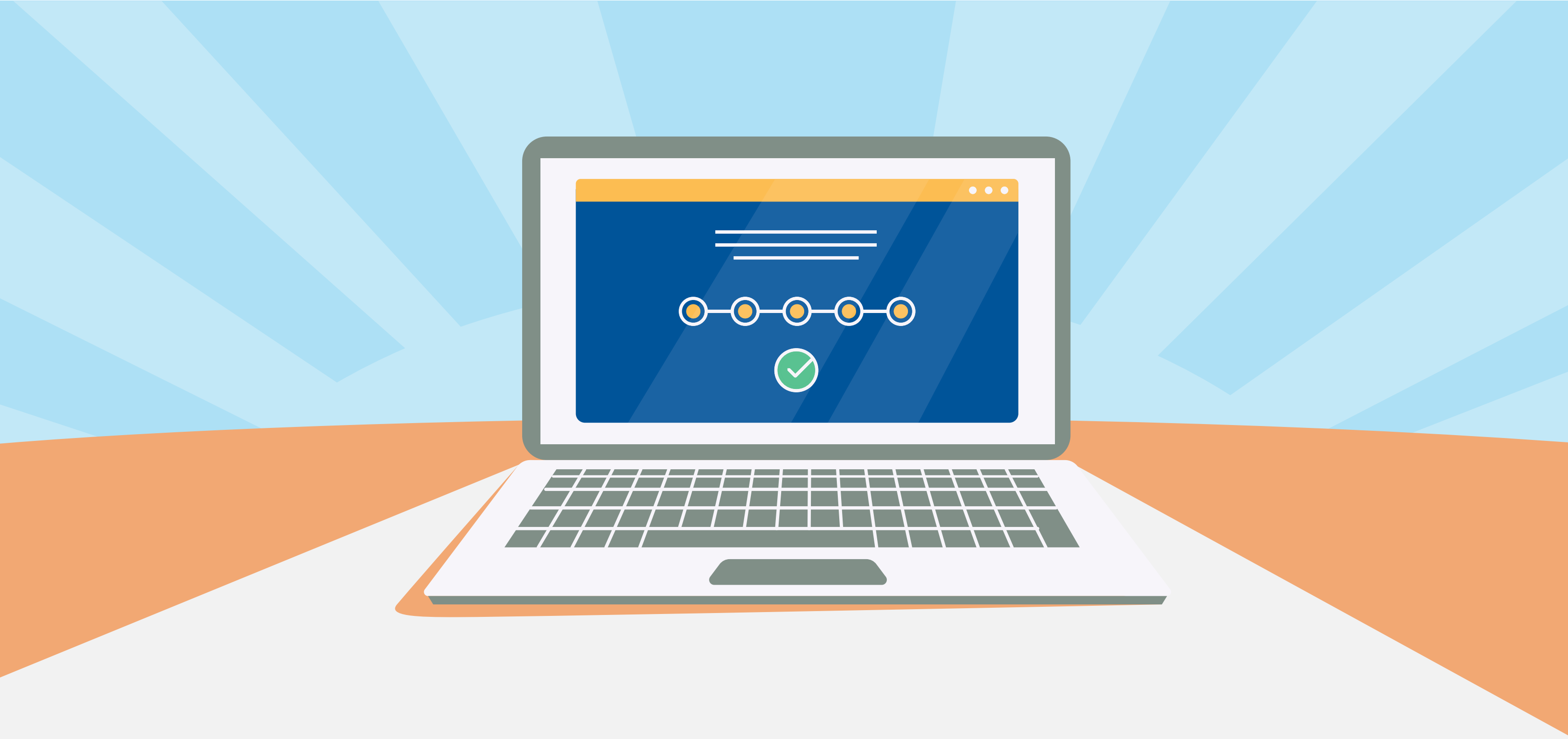
By using Genuine Presence Assurance® to verify user identity at enrollment or for high-risk transactions, organizations can be confident that the highest levels of security are being delivered. This ensures that an individual is the right person, a real person and that they are authenticating right now, protecting against identity theft and synthetic identity fraud.

Seamless user experience

Some biometric face verification technologies require a user to move their heads, or move the device, or read out letters or numbers. To ensure the simplest user experience, the EUDIW should use passive authentication. With passive authentication, the user has to do nothing more than look at their device and the technology does the work.

This is very important. Let's take European financial services as an example. According to research by Signicat, **68%** of Europeans abandoned the onboarding process when signing up for a financial service in 2021. This number was actually up from 2020 when the number was **63%.**

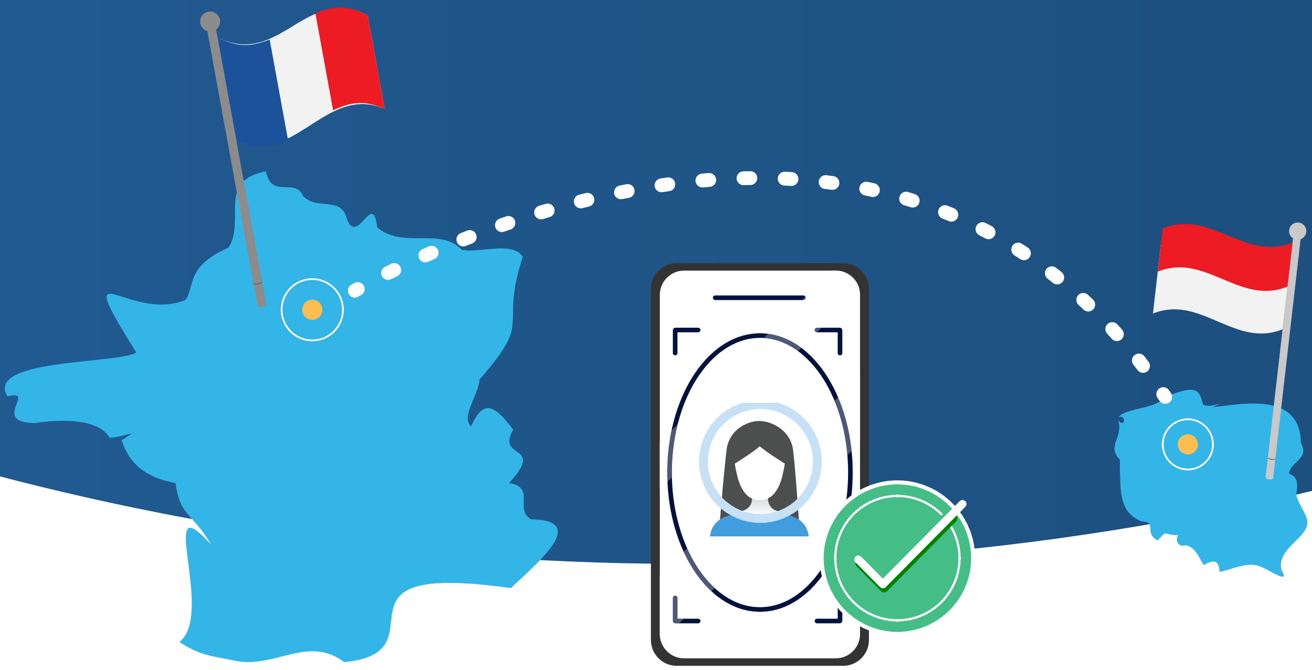
If implemented correctly, biometric face verification should enable the EUDIW to deliver an onboarding process that optimizes completion rates. iProov technology, for example, achieved a **98.4%** completion rate with over 3m UK Home Office users in 2020.



4th Challenge
Ensuring Smooth Pan-European Deployment

Each of the consortia bidding for the pilot funding will be made up of several organizations. Each of those organizations will need to meet a set of standards if the EUDIW is to be deployed smoothly and in a harmonized way across the European Union.

The Commission's proposal for a European digital wallet builds on the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation, which introduced the first cross-border framework for trusted digital identification and trust services (such as electronic signatures). eIDAS sought to give EU citizens access to public services across the EU using electronic identification issued in their home country and recognized mutually by other member states[2].



[2] Revision of the eIDAS Regulation: Findings on its implementation and application, European Parliamentary Research Service, March 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

While a total of 19 national eID schemes from 14 member states have been launched under the eIDAS Regulation, only about 60% of EU citizens can benefit from cross-border electronic identification services, "which is considered a relatively low level of application."[3]

Several member states either have not created an eID program or have chosen not to seek mutual recognition for it, with a lack of incentives for member states and private service providers to join the cross-border infrastructure a major barrier to its effective implementation.

Under the current Commission proposal, each member state will be required to issue a European Digital Identity Wallet within 12 months of the Regulation's entry into force. Notification of at least one eID program is proposed to be mandatory. A toolbox will define a set of common standards and technical specifications, common guidelines, and best practices to support the smooth functioning of the European Digital Identity Framework[3].

The European Parliament has "emphasized the importance of a trusted and secure electronic identification system to the development of digital services." A user-centric design, mobile-first thinking, and procedures to establish common standards are expected to contribute to a consistent and accessible user experience.

Delivering Trust and Integrity with eIDAS

eIDAS regulation and module certification is essential to how the EUDIW will be implemented. In achieving eIDAS certification, trust service providers can enable governments and organizations to verify users across Europe with a high level of certainty and security. What's more, having eIDAS certification in place will allow for the technology behind the EUDIW to be deployed quickly. This, in turn, mitigates audit risk and can help ensure the timeliness and success of the EUDIW pilots.

Face biometric solutions that are audited at the highest level of assurance through eIDAS certify that the technology is compliant with regulations for the provision of verification and authentication services. Having this level of certification means the technology can be deployed immediately, and provides the security protections needed to support the EUDIW.

iProov Biometric Face Verification: The Solution

The success of the EUDIW depends then on a number of factors:

1. Maximizing citizen uptake with secure effortless remote enrollment
2. Encouraging ongoing usage with convenient secure authentication
3. Providing value for organizations across the EU
4. Adhering to standards for simple integration

[3] Ibid

To achieve those four deliverables, the EUDIW must offer:

1. The highest levels of security, to achieve trust and integrity
2. Flexibility for all scenarios, from high risk to lower risk uses
3. Usability to maximize usage and prevent user drop-off
4. Inclusivity to support as many users as possible
5. Scalability to cope with high peaks of usage
6. Compliance with eIDAS

iProov's face biometric technology enables EU states and participating organizations to achieve all of these goals.

Highly secure for enrollment and authentication

iProov's Genuine Presence Assurance delivers the highest levels of security to ensure that an online individual is the right person, a real person and that they are present in real time, right now.

Unlike other liveness detection solutions, Genuine Presence Assurance protects against impersonation, presentation, and digital injection attacks. This is imperative during online enrollment, to prevent identity theft and synthetic identity use, and for authentication during higher risk transactions.

Genuine Presence Assurance® combines with iProov's Security Operations Center (iSOC), an active threat management service that guards against the ever-evolving threat of machine-driven cyberattacks to provide organizations and users with continuous, sustainable security.

Flexible authentication for multiple use cases

Some EUDIW transactions will require a lower level of security and iProov's Flexible Authentication supports that. In situations with a lower risk profile, iProov's Liveness Assurance™ ensures that the user is the right person and a real person, delivering the appropriate protection.

Usability

iProov has been designed to maximize usability as well as security (and has a WCAC 2.1 AA rating). iProov delivers passive authentication, enabling a user to verify or authenticate themselves simply by looking at their device. There are no complex instructions to follow and no movement or reading of numbers is needed. For the EUDIW, this means a simple enrollment process for maximum registrations and effortless authentications for ongoing usage.

Inclusivity

iProov uses light for verification and authentication, which means it works on any device with a user-facing camera. This includes smartphones and tablets, as well as computers and kiosks. By supporting the broadest range of devices and platforms, iProov ensures that all EU citizens can enrol and use the EUDIW.

Scalability
iProov technology has been proven to withstand huge and sudden peaks of usage, as was shown with the NHS during the COVID pandemic. This will be essential for the EUDIW - an unforeseen event should be an opportunity for uptake and usage of the wallet but if the system cannot cope, the opportunity will be lost.

eIDAS compliance
iProov's Genuine Presence Assurance technology has been audited and certified to the eIDAS eID Level of Assurance High. This means that EU citizens, nations and enterprises can be certain that iProov offers the highest levels of security for enrollment into the EUDIW and for ongoing authentications.

iProov also received eIDAS module certification as Qualified Trust Services. This certification means that iProov can supply onboarding and authentication services to Qualified Trust Service Providers (QTSPs) throughout the European Union (EU) without complicated integration audits being required.

Trusted by governments
Governments around the world have entrusted iProov with verifying and authenticating citizens online. These include:

- US Department of Homeland Security
- UK Home Office
- UK National Health Service (NHS)
- Australian Taxation Office
- Singapore Government

Read more case studies.

iProov and the NOBID Consortium for the EUDIW

iProov is proud to be a key member of a multi-country consortium of Europe's most trusted identity experts, working on a proposal for a large-scale, cross-border payments pilot strongly aligned with the aims of the European Commission's EU digital identity wallet program.

Six countries (Denmark, Germany, Iceland, Italy, Latvia and Norway) are part of the consortium, led by NOBID (Nordic-Baltic eID Project). The consortium's proposal will bring to life the most widely used of the EU's priority use cases for the wallet – payments. In addition to iProov, technology partners participating in the consortium include Thales, Signicat, RB, Auðkenni, IPZS, Poste Italiane, Intesi Group, InfoCert, FBK and Latvian State Radio and Television Centre.

The consortium's proposal focuses on payments, one of the top priority use cases in the EU's Digital Identity Wallet vision. Its use case will leverage existing payment infrastructure to enable payment issuance, instant payments, account-to-account transfers and payment acceptance both in-store and online. It is designed to also complement wider EU plans to empower member states and streamline cross-border payments, such as the European Payments Initiative (EPI) and the Digital Euro. The project has unrivaled support from leaders in banking and payments including DNB, DSGV, Intesa Sanpaolo and Nets.

iProov's patented face biometric authentication technology is used by governments and enterprises around the world to verify and authenticate digital user identity. Its Genuine Presence Assurance® and Liveness Assurance™ technologies help prevent identity theft and other online crime using a passive authentication experience. iProov's face verification technology works on all platforms and devices with a user-facing camera and does not require the user to follow complex instructions.

For more information, visit the NOBID Consortium website.

Next Steps

For a demo: to see how remote face biometric verification and authentication can support the EUDIW, please e-mail contact@iproov.com and we will contact you to arrange a demo.

For more information: visit our website at www.iproov.com to find out more about how we use face verification to help organizations to complete secure processes online.

Methodology

This report is based on research carried out by an independent agency on behalf of iProov in April-May 2022. Eight countries were included in the research (the US, Canada, Mexico, Germany, Italy, Spain, the UK and Australia) with 2,000 consumers surveyed in each country.

contact@iproov.com

iproov.com