Unlocking Financial Inclusion With Digital Identity and Biometric Verification

European Digital Identity Wallet Use Case

Executive Summary

Digital identity programs promise not only to provide a secure, convenient digital alternative for individuals to assert their identity but to also to open essential pathways for the unbanked and disenfranchised to access financial and welfare services. For governments, digital IDs offer reduced administrative burden and economic growth. For financial institutions, they can facilitate Know Your Customer (KYC) processes and enable access to the unbanked.

However, without resilient identity verification at enrollment and throughout the user lifecycle, digital IDs present risks in addition to the opportunities – they could be misused for fraud, money laundering, and other illicit activities.

Traditional identity assurance technologies rely on either possession, like a device, or knowledge, such as a password. Passwords can be stolen or shared and devices can be compromised or lost, meaning these methods no longer provide the requisite defense against today's threat landscape, nor do they meet user demands for convenient, low-friction digital experiences.

Biometric face verification resolves the security and usability issues of traditional authentication methods, and can enable convenient identity verification for remote onboarding. This report illustrates how biometric face verification must incorporate resilient liveness detection for digital identity programs to provide high accessibility and assurance that remote users are who they claim to be.

Key Findings:

1. Cyber-enabled financial crime is a rife and growing threat globally. The challenge for digital identity programs is to unlock inclusion while mitigating the risk of the technology being misused for criminal purposes.

2. Ethical hackers have proven that video call verification is susceptible to attacks using synthetic imagery and forged IDs. Biometric face verification with liveness detection is the only secure and inclusive method for remote enrollment and authentication to provide a high level of assurance that a user is who they claim to be.

3. Biometric face verification systems must defend against synthetic media, such as generative AI, and be resilient to the biometric threat landscape, securing digital identities from current and future threats.

4. To realize their full potential, digital IDs must be valuable to all stakeholders: governments, organizations, and end-users, including those who are unbanked or disenfranchised.

5. Video call verification and CAPTCHA risk limiting accessibility to certain groups.

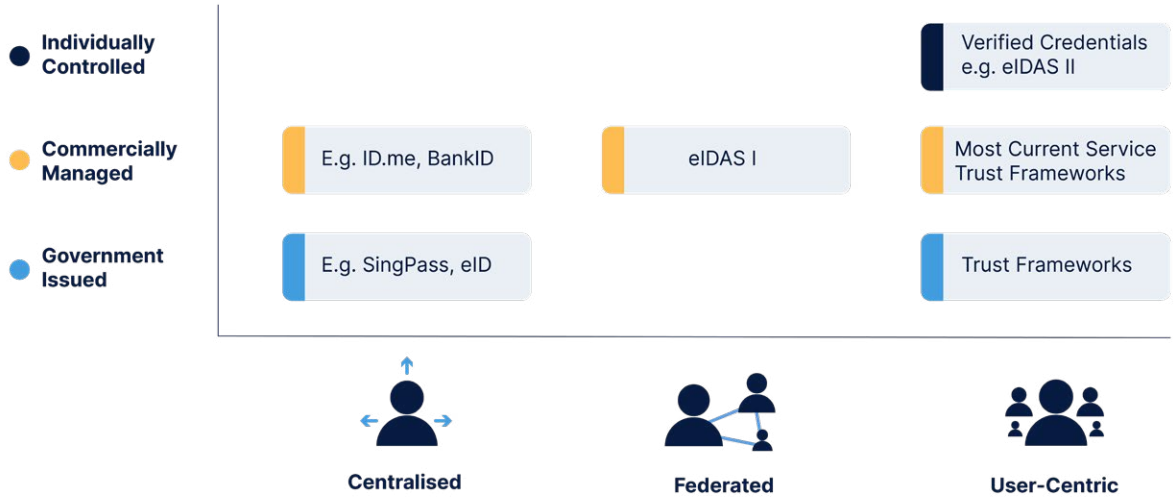
6. Biometric face verification with liveness detection must exhibit bias mitigation and adhere to accessibility standards.

Introduction

Everybody has the right to an identity.[1] Yet, an estimated 850 million people worldwide lack a legal form of identification.[2] Without ID, people struggle to gain employment, access healthcare, and vote.[3] In lacking the means to open a bank account, take out loans and make secure payments, they also face financial exclusion.

To solve this issue, governments are teaming up with organizations worldwide to develop digital identity programs. These programs aim to enable users to digitally store and exchange identity documents, such as a driver's license, and credentials, such as diplomas. They will offer the convenience end-users now demand and open essential pathways for previously disadvantaged or marginalized individuals to access financial and welfare services.

Architectures of Identity



The challenge for these initiatives is to provide the maximum number of people with digital identities and financial access while mitigating the risk of cybercrime. As with any technology that enables access to a broad range of secured data and monetary benefits, digital identity programs are at risk of being misused for fraud, money laundering, and other illicit activities.

[1] Universal Declaration of Human Rights, United Nations, 1948
[2] 850 million people globally don't have ID—why this matters and what we can do about it, Worldbank, 2023
[3] Proving who you are: addressing the plight of those with no legal identity, United Nations, 2023

Providing digital identities – and, by extension, financial inclusion – is an opportunity for governments and organizations. According to McKinsey, extending full digital ID coverage could unlock economic value equivalent to 3-13% of GDP by 2030.[4] Likewise, the financially excluded – or the 'unbanked' or 'underbanked' – represent an untapped market of long-term profitability for financial institutions. In the US, for example, the underbanked spend $189bn annually on alternative financial services, like payday loans.[5]

Due to its ease and convenience, biometric face verification has been the chosen method of identity verification for many programs. Liveness detection is a technology incorporated into biometric systems that detects whether the user is a real, 'live' person and not a recording, picture, or other non-living spoof. However, it is essential to ensure the highest levels of risk mitigation are deployed. Not all biometric verification or liveness detection is created equal, and solutions vary in accessibility, bias mitigation, and protection against biometric threat vectors, including sophisticated generative AI-produced attacks.

We focus on the EU Digital Identity Wallet (EUDIW), as this large-scale initiative is already in pilot. We explore why its imperative that digital identity programs like the EUDIW must incorporate good biometric face verification at onboarding and authentication to provide maximum accessibility, security, and financial inclusion for all.

[4]Digital identification: A key to inclusive growth, McKinsey Digital, 2019
[5]Investing In The Underbanked: An Opportunity At The Intersection Of Fintech And Proptech, Forbes, 2023

Use Case:
The EU Digital Identity Wallet (EUDIW)

Current Status

The EU Digital Identity Wallet will be a decentralized, interoperable digital tool that aims to provide all 447.7 million EU citizens with the ability to store and exchange identity documents and credentials, securely and conveniently, while having full control over their data.[6] Organizations, such as government agencies, banks, universities, travel companies, and more will be expected to accept the EUDIW as official identification.

The EU Commission has selected four consortia comprising public and private organizations to create large-scale pilots focusing on different use cases. Use cases include domestic and cross-border payments, eServices, travel, and education. As of April 2023, the consortia will begin working on their large-scale pilots. By 2024, every EU member state must make the Wallet available to all EU citizens.[7] By 2030, 80% of citizens should be using the Wallet.

To be successful, large-scale pilots must deliver utility and value to both organizations and end-users and exhibit ongoing usage and scalability.[8]

[6] Digital Identity for all Europeans, European Commission
[7] The Year 2024 Will See European Digital Identity Wallet Credentials Accepted by All EU Service Providers in Public-Private Partnerships, ABI Research, 2022
[8] EU countries endorse agreement on European digital identity, Euractiv, 2022

Securing Digital Identity Programs

The Challenge

Digital identity programs promise to provide the disenfranchised and unbanked with societal and financial inclusion. While reaching these new-to-market individuals can create value for governments and organizations, it also heightens risk. Those with little to no financial or credit history create the ideal cover for fraudsters devising sophisticated identity fraud schemes, such as synthetic identity fraud.[9]

Fraud and cyber-enabled financial crime are rife and growing globally. Cybercrime is predicted to cost $10.5 trillion annually by 2025.[10] Meanwhile, the United Nations Office on Drugs and Crime (UNODC) estimates that between 2 and 5% of global GDP is laundered each year.[11]

[9] Synthetic Identity Fraud is a Complex and Growing Challenge, LexisNexis, 2021
[10] Why we need global rules to crack down on cybercrime, World Econonic Forum, 2023
[11] Money Laundering, Europol, 2022

In the case of the EUDIW, financial institutions will rely on the Wallet to undertake and streamline their AML and KYC due diligence processes on their customers.[12] In adhering to PDS2 requirements (that authentication is based on the use of two or more elements that only a customer could know, could possess or are unique to the user), facilitating Strong Customer Authentication, and stemming the threat of cyber-enabled crime, the EUDIW can win and maintain trust with financial institutions, governments, and end-users. However, the pilots can only achieve this if resilient technology is employed at the point of identity verification and authentication.

How Can Biometric Verification and Liveness Detection Secure the EUDIW?

To mitigate the risk of being exploited for criminal purposes, the EUDIW must deliver high assurance that end-users are who they claim to be at remote enrollment and when making transactions, such as payments.

Users will enroll into the EUDIW and re-authenticate their identity each time they use it. To enroll, they must download the Wallet onto their smartphone. Then they must bind it with Personal Identification Data (PID), an official document normally accepted as proof of identity, such as a passport or driver's license.[13] Exactly what PID will be accepted and how it is to be bound to the Wallet is as yet unclear.[14]

[12] Towards a European digital identity wallet: competitive, business-enabling, and safe, The Paypers, 2021
[13] The European Digital Identity Wallet Architecture and Reference Framework, European Commission, 2023
[14] Understanding the EU Digital Identity Wallets' Architecture Reference Framework, Biometric Update, 2023

One way to verify a user's identity is through automated biometric verification. This involves the user capturing a clear image of their identity document and performing a facial scan using a front-facing camera on a device such as a smartphone. Face matching, such as this, on its own, is not enough to provide assurance that the person is the true owner of the genuine identity. In the Guidelines on the Use of Remote Customer Onboarding Solutions, the European Banking Authority (EBA) states that liveness detection is the "preferred option" for unattended onboarding with financial institutions.[15]

Biometric face verification with liveness detection can either be cloud-based or hosted on the device. On-device solutions, such as Apple's Face ID, can deliver a high level of user convenience. However, they cannot verify a digital identity by binding it to a real-life person, so they provide no assurance that a user is who they claim to be – only that it is the same device owner returning each time. Cloud-based solutions, on the other hand, can identity-proof users in this way.

Video call verification is an alternative to liveness detection at onboarding, as mentioned by the EBA. This involves a one-to-one video call between the user and a trained operator. The user is asked to hold up an identity document, and the operator matches it against their face. However, video call verification is proven to provide little assurance that the end-user is a 'live' person and not generative AI-produced artificial imagery convincingly superimposed onto the threat actor's face.

In 2022, researchers at the Chaos Computer Club managed to circumvent video call verification technology by using generative AI and a forged ID.[16] The case displayed how this technology, and the human operators it relies upon, are highly susceptible to synthetic imagery attacks. The German Federal Office for Information Security has since warned against video call verification for its vulnerability to these attacks.[17]

If digital identity programs cannot defend against the threat of deepfakes at onboarding and authentication, they will be exploited for criminal purposes, such as payment fraud, money laundering, and terrorist funding. Unlike video call verification, liveness detection relies not on the human eye to detect spoof attacks but on machine-learning and deep-learning techniques that are far more reliable.

[15] Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849, European Banking Authority, 2022
[16] Chaos Computer Club hacks Video-Ident, Chaos Computer Club, 2022
[17] Newsletter SAFE, Bundesministerium des Innern und für Heimat, 2022

Providing Resilience To the Evolving Biometric Threat Landscape

This is not to say that all liveness technology is impervious to synthetic imagery. Biometric attacks comprise presentation attacks (where an object is presented to the camera) and digital injection attacks (where imagery, such as synthetic imagery, is injected into the data stream). While presentation attacks and Presentation Attack Detection (PAD) are well understood, digital injection attacks are by far the greater threat.[18]

The biometric threat landscape is evolving rapidly, perpetuated by a Crime-as-a-Service economy and easier access to the tools needed to create advanced sophisticated imagery and launch injection attacks. Pre-packaged generative AI and General Adversarial Networks (GANs) attack toolkits are increasingly available on code-depository websites, allowing low-skilled criminals to launch advanced attacks with little effort.[19]

At the same time, the increased demand for technology that circumvents liveness technology has even led to a Deepfakes-as-a-Service market. According to Europol, illicit companies are offering to create tailor-made deepfakes for as little as $16,000.[20]

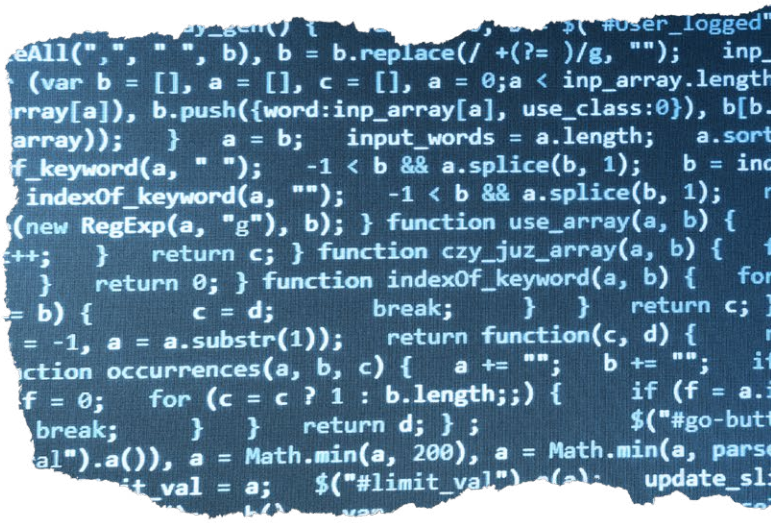
	Presentation Attacks	Digital Injection Attacks
Deployment:	An artifact is presented to the camera	Imagery is injected directly into the video stream
Detection:	Detected via clues in the imagery	Detected either via analyzing metadata or imagery-based testing
Scalability:	Limited in scale. Threat actors can deploy one attack at a time	Unlimited in scale. Threat actors can create highly automated attack machines
Testing:	Existing globally recognized standards for Presentation Attack Detection (ISO/IEC 30107)	No existing globally recognized standards for Digital Injection Attack Detection

[18] iProov Threat Intelligence Report 2023, iProov, 2023
[19] Ibid
[20] Law enforcement and the challenge of deepfakes, Europol, 2022

Biometric liveness detection remains the only secure way for digital identity programs to identity-proof and authenticate end-users. Yet, with millions of identities on the line, the liveness technology incorporated must provide proven defenses against current and future biometric attacks to national-level security standards and show resilience to the evolving biometric landscape. Failure to do so harms individuals and organizations and undermines trust in digital identity initiatives.

Level of Assurance Standards and Testing

Performance testing for Presentation Attack Detection (PAD) exists and is provided by iBeta and the National Institute of Standards and Technology (NIST). No such testing or accreditation exists for Digital Injection Attack Detection (DIAD). However, PAD accreditation is inadequate to defend against the current biometric threat landscape, and liveness vendors must demonstrate digital injection attack detection ability.



How can Digital Identity Programs Achieve Inclusivity and Equality?

The Challenge

Financial and societal exclusion affect certain demographics more than others. Those in low-income households, the disabled, single mothers, the elderly, immigrants, and refugees are more likely to be unbanked, at risk of poverty, and socially excluded.[21]

The population of the EU is large and diverse. 24% of citizens have some form of disability, and 10% of the EU are racial or ethnic minorities.[22][23] Furthermore, tech literacy is sporadic across the bloc. While 79% of the Dutch exhibit basic digital skills, such as finding information online, only 28% of Romanians show such literacy.[24]

To achieve maximum uptake and ongoing usage of the EUDIW, the large-scale pilots must provide equal value for all EU citizens, irrespective of their ethnicity, socioeconomic status, language, physical or cognitive ability, or digital skillset. In accomplishing this, the pilots will improve access to services for marginalized groups and win favor with the EU population at large; 90% of whom are in favor of the principle that everyone, including people with disabilities, should benefit from easily accessible and user-friendly digital services.[25]

[21] FDIC National Survey of Unbanked and Underbanked Households, Federal Deposit Insurance Corporation, 2021
[22] Disability in the EU: facts and figures, European Council, 2022
[23] Diversity and Power in the European Union, European Policy Centre, 2022
[24] Which European countries have the most digital skills? World Economic Forum, 2022
[25] Europeans show support for digital principles, Eurobarometer, 2021

How Can Biometric Verification Deliver Inclusion and Accessibility?

Biometric face verification provides a quick, convenient experience for enrollment and authentication and, when deployed correctly, can offer high levels of inclusivity and accessibility. To verify their identity, the user needs only to scan an identity document and their face using any device with a front-facing camera, such as a smartphone or laptop. To re-authenticate, the user simply scans their face. The technology, therefore, does not rely on the end user's technical ability.

Other remote identity verification methods lack such accessibility. Video call verification, whereby the user verifies their identity via a one-to-one call with a trained operator, is liable to exclude people with language barriers or cognitive impairments. These individuals may be unwilling to engage in a two-way conversation with a stranger.[26] Likewise, biometric face verification is a marked improvement on traditional authentication technologies, such as passwords and CAPTCHA. These not only lack user convenience but also limit access to people with disabilities.[27]

However, not all biometric verification or liveness detection is created equal, and solutions vary in accessibility and bias mitigation. Systems must ensure the datasets used to train the algorithms are balanced according to age, gender, and skin tone. Yet, this on its own is not enough to sufficiently reduce bias. Systems must also perform operational testing to mitigate bias based on differences in camera types, user behavior, and environmental conditions, which can affect performance.

Someone with a low income may use a lower-quality camera than someone with a high income. If the biometric technology cannot perform equally well for both these user groups, identity programs will fall prey to bias. The biometric systems used must test for, and mitigate, these causes of bias.

To deliver maximum inclusivity, security, and utility, digital identity programs must incorporate biometric verification and liveness detection for enrollment and authentication. Nevertheless, large-scale pilots must ensure these components exhibit bias mitigation and accessibility.

Accessibility Standards and Testing

The Web Content Accessibility Guidelines (WCAG) is the best-practice standard for various digital experiences. Biometric vendors compliant with WCAG 2.1 AA and Section 508 (US) provide improved accessibility to users with cognitive or learning disabilities, low vision, or those with disabilities.[28]

[26] Why is Biometric Face Verification Better Than Video Call Verification?, iProov, 2022
[27] Inaccessibility of CAPTCHA, W3C, 2021
[28] Web Content Accessibility Guidelines (WCAG) 2.1, W3C, 2018

Summary

We will see the progress of the EUDIW over the next few years. The rest of the world is following suit. In the UK, there have been calls for a 'decentralized digital-ID system for the benefit of both citizens and businesses' that's similar in nature to the EUDIW.[29] In the US, the National Institute of Standards and Technology (NIST) published a draft project description, Accelerate Adoption of Digital Identities on Mobile Devices, which intends to evaluate and implement international standards on mobile driver's licenses.[30]

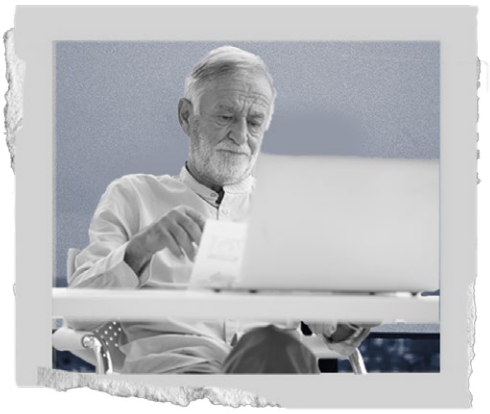
These initiatives share both goals and challenges: they intend to provide value and inclusion to individuals using digital IDs and reduce the administrative burden for organizations that will accept them as proof of identity. At the same time, they must ensure the technology is not exploited for criminal gain and provide a high level of assurance that users are who they claim to be.

As reflected in the March 2023 White House National Cybersecurity Strategy, end-users cannot bear the burden of this security. Instead, "it must be the responsibility of the owners and operators of the systems....and the technology providers that build and service these systems."[31]

Equipped with biometric face verification with liveness detection, digital ID initiatives will win on all fronts – they can achieve wide-scale uptake, unlock financial and societal inclusion and mitigate the risk of cybercrime. The onus, meanwhile, is not put upon the user: they need not arrange a call with a trained operator for onboarding nor remember complex passwords to authenticate. They simply use their face to verify and authenticate their identity.

Not all biometric face verification is created equal, however. To deliver full equality and inclusion, the technology incorporated into digital ID solutions must exhibit robust bias mitigation and comply with WCAG or other accessibility standards. They must also go beyond standard presentation attack detection and provide resilience against the rapidly evolving biometric threat landscape.

[29] A New National Purpose: Innovation Can Power the Future of Britain, Tony Blair Institute of Global Change, 2023
[30] Accelerate Adoption of Digital Identities on Mobile Devices, National Institute of Standards and Technology (NIST), 2023
[31] National Cybersecurity Strategy, The White House, 2023



iProov delivers eIDAS-certified advanced biometric attack detection to governments and organizations globally. iProov technology complies with Web Content Accessibility Guidelines (WCAG) 2.1 AA and section 508.

iProov is a key member of NOBID, 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.

contact@iproov.com

iproov.com