Digital Identities Across the World

Approaches, Challenges and Best Practices

Table of Contents

01

Executive Summary

Executive Summary

This study provides a comparative analysis of national electronic identity (eID) systems across 42 countries worldwide. Against the backdrop of rapidly evolving digital identity ecosystems and regulatory developments such as the European Union (EU) eIDAS 2.0 framework, it examines how countries design, operate, and scale their eID infrastructures. The study presents an overview of the diverse strategic approaches and technological models of eID systems across different countries, with a focus on the factors influencing their performance and user adoption. It then examines the most commonly identified challenges and offers recommendations for future development and design of national eID systems.

The evidence is drawn from a combination of primary and secondary research. Primary insights are derived from a structured 2025 survey conducted among PwC's global network of specialists with hands-on experience in eID implementation. Secondary sources include authoritative and publicly available materials such as EGDI rankings, EU eGovernment Benchmark results, and national documentation on eID-enabled services. This mixed-methods approach enables an internationally comparable assessment of strategic approaches, technological models, and levels of population uptake.

The study finds that eID systems increasingly function as foundational digital enablers for accessing public services, financial products, mobility solutions, and private-sector platforms. Adoption rates and the breadth of eID functionality, however, differ markedly across countries. On average, around 67% of the population in the countries analysed actively use their national eID solution, with user rates ranging from below 50% to well above 80%. In most countries, eID users can access more than 100 online services, and the majority of solutions support not only basic identification and authentication (98%), but also electronic signatures (62%) and digital credentials (67%). This underlines that underlying framework conditions and implementation choices are decisive for how widely eID systems are used and how deeply they are embedded in public and private services.

At the same time, fragmented institutional responsibilities, limited service coverage, and low public trust often impede usage. Looking ahead, countries face shared challenges, including ensuring interoperability across systems and borders, strengthening cybersecurity, scaling private sector use, and adapting to evolving regulatory frameworks, such as the rollout of the European Digital Identity (EUDI) Wallet.

Across the 42 countries, the research identifies four key success factors for effective eID ecosystems:	1. Regulatory and governance clarity, with clearly defined responsibilities and accountability 2. Robust and interoperable technical and infrastructural foundations 3. High standards of security, privacy, and public trust 4. Strong user inclusion and adoption, driven by everyday relevance and usability.

Building on these findings, the study formulates four core recommendations for the successful implementation and further development of eID systems:	1. Establish clear regulatory and governance frameworks with defined responsibilities and accountability. 2. Develop robust, interoperable technical infrastructures that enable seamless integration of public and private services. 3. Ensure strong security and trust mechanisms, underpinned by transparent data governance and effective communication. 4. Promote user inclusion by embedding eID in everyday use cases, so that it delivers tangible value and drives broad adoption.

Given the relevance and timeliness of this topic, the findings underscore the critical role of eID systems as a foundational step in the broader digitalisation process. The study is intended to provide policymakers and practitioners with a concise yet comprehensive overview, supporting informed decision making and effective implementation of national eID systems.

02

Introduction

Introduction

In an increasingly digitalised world, the digital transformation of public administration continues to advance. eID systems are evolving rapidly as governments seek to modernise public service delivery, enhance cybersecurity, and enable secure digital interactions for citizens and businesses. Many countries outside the EU, such as India and Australia, have already implemented large-scale digital identity ecosystems that support a wide range of online services and serve as important reference points for international best practice. Also, countries within the European Union like Denmark have established an eID system which experienced broad adoption within society. However, against this global uptake the European Union is undergoing its own major transformation in the field of digital identity.

A central driver of this development is the eIDAS 2.0 regulation, which requires all EU Member States to provide at least one Wallet to its citizens, businesses, and residents by the end of 2026. This strict deadline applies uniformly across the Union, yet the approaches to implementation differ markedly between Member States. These variations reflect differences in administrative traditions, digital infrastructures, and strategic priorities.

Despite the strategic importance of digital identity, there is still no systematic, internationally comparable overview that brings together cross-country evidence on national eID systems, their adoption and performance, and the lessons that can be translated into concrete recommendations. Existing analyses tend to focus on individual countries or specific aspects and rarely provide a structured comparison of maturity, user uptake, and everyday relevance across a broad set of states.

National eID systems are only valuable when they genuinely enhance citizens' lives, foster trust, and provide reliable, secure access to both public and private services. In today's increasingly digital world, they are not optional but a fundamental prerequisite for participation and economic inclusion. This study addresses the existing gap by providing an international comparison of national eID systems in 42 countries. It examines how these systems are embedded in public and private services, which factors drive or impede user adoption, and how eID can effectively support digital participation and inclusion. By offering policymakers, practitioners, and researchers an up-to-date, internationally comparable overview, the study illustrates how eID can be implemented worldwide in diverse yet effective ways and distils common success factors and actionable recommendations for future system design.

Given the rapid pace of change in eID systems and related statistics, some information may evolve over time, and we therefore welcome input from experts in all countries to help ensure that the underlying data and insights remain current.

03

Scope and Methodology

Scope and Methodology

This study provides an international comparison of national eID systems, with a primary focus on European approaches. Under the leadership of PwC Germany and PwC Strategy&, 42 countries were selected to reflect a broad range of eID implementation models. Country selection was based on the availability of reliable data and the presence of qualified local experts capable of validating findings.

The evidence base combines primary and secondary research. Primary data was collected through a structured survey conducted in 2025 among PwC's global network of specialists with extensive practical experience in the design, implementation, or operational use of national eID systems across public- and private-sector services. Secondary data was sourced from current, authoritative, publicly accessible materials. All inputs are transparently labelled by evidence type.

The analytical focus of the study is guided by the following research questions:

- What is the current level of maturity, performance, and implementation of national eID systems across countries?
- How do maturity, performance, and implementation approaches differ internationally?
- Which factors drive user adoption, governance effectiveness, technical delivery, and service expansion?
- Which barriers materially limit uptake and integration?
- Which operational and regulatory levers enable measurable improvement?

The comparative analysis is structured along four analytical dimensions that reflect the core components of national eID ecosystems:

1. Regulatory and governance frameworks
2. Technical and infrastructural foundations
3. Security, privacy, and public trust
4. User experience, inclusion, and adoption

These dimensions provide a common lens for assessing recurring challenges, key success factors, and country-specific implementation approaches. Based on this analysis, the study derives a set of practical recommendations for the design and further development of national eID systems.

A core output of the study is the set of individual country reports, which document the status quo of national eID systems and provide the empirical foundation for cross-country comparison. Each of the 42 country reports follows a standardised structure to ensure consistency and comparability.

The reports include:

- A system overview, describing the operational model, core functionalities, and administrative use cases;
- An analysis of key success factors and performance drivers, informed by available evidence and the study's research questions;
- An outlook, highlighting expected developments and persistent challenges affecting future system performance.

Each country report combines qualitative expert assessment with quantitative indicators, providing a structured evidence base on the respective national eID system. Together, these reports form the empirical foundation for the cross-country comparison, the derivation of common patterns, and the formulation of overarching success factors, challenges, and recommendations. To support systematic comparison, each country report is complemented by a consistent set of quantitative indicators:

- User adoption rate, based on a clearly defined reference population;
- The E-Government Development Index Rank (EGDI Rank), used as a standardized proxy for overall digital government readiness, based on UN data (2024);
- Results from the EU eGovernment Benchmark (2025), providing contextual insights into digital public service performance, including user-centricity, transparency, and cross-border service delivery;
- The number of eID-enabled services, reported where verifiable evidence is available; figures are indicative due to differing national counting methodologies.

In addition, each country report maps national eID capabilities against the EUDI Wallet framework to assess readiness regarding wallet-related functionalities.

Given the scope of 42 countries and the dynamic evolution of eID, some information may become outdated over time. Differences in national data collection methods further limit full statistical comparability. These constraints are acknowledged throughout the study, and findings are interpreted in context. The study is updated on an ongoing basis, and expert feedback is welcomed to ensure continued accuracy.

04

Research Findings

Research Findings

Global overview

The thorough investigation of the selected 42 countries that have already established their systems of electronic identification (eID) has revealed important insights into how these solutions are adopted within society, which services reach the highest usage, and in which situations eID systems significantly simplify citizens' daily lives. Subsequently, the key quantitative insights and patterns derived from these data are presented, alongside notable country examples.
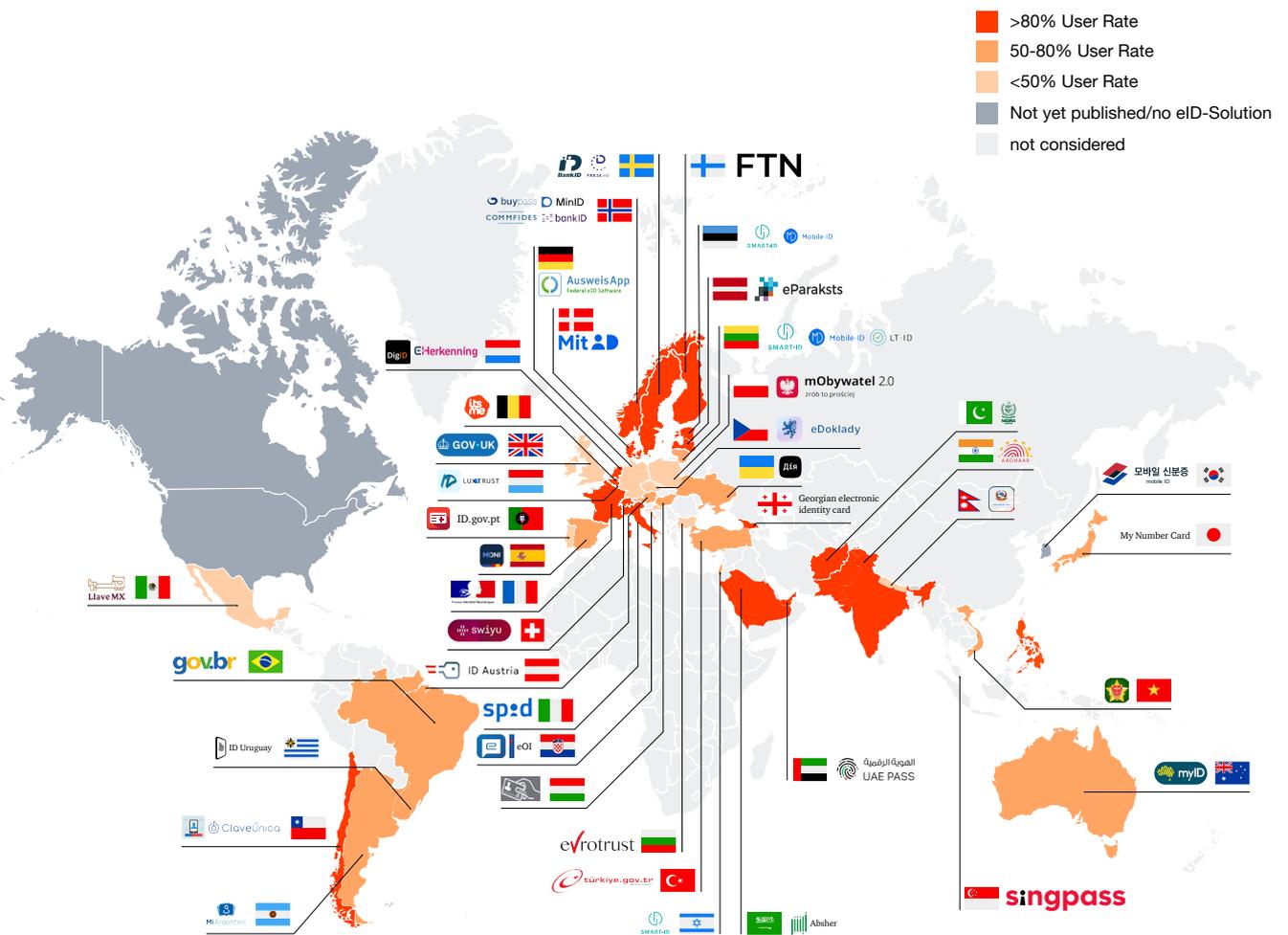
Figure 1: Overview of user rates of selected countries

Figure 1 presents a worldwide snapshot of the countries included in this study alongside their national eID solutions. For each country, the graphic shows the official logo or name of its digital identity program and groups it according to the reported level of national eID user adoption. Please note that the user rates shown in this figure are based on different calculation methods. The exact user rate for each country varies e.g. whether it is measured by the number of active eID users or by registered citizens. The figure also flags countries that have not yet released adoption statistics or that do not currently operate a nationally established eID system. Overall, the map suggests that many European countries – particularly in Northern and Western Europe – cluster in the higher adoption categories (above 50% and, in several cases, above 80%). At the same time, strong uptake is also visible in a number of non-European countries such as Brazil, Chile and India, indicating that high eID usage occurs across different regions and implementation models.

The subsequent summary graphic provides an aggregated overview of the main quantitative indicators for the eID systems analysed in this study:

Countries in scope

42

**countries
in total**

User rate

∅ 67%

- >80%
- 50-80%
- <50%

Service

>100

online services offered
via eID in most countries
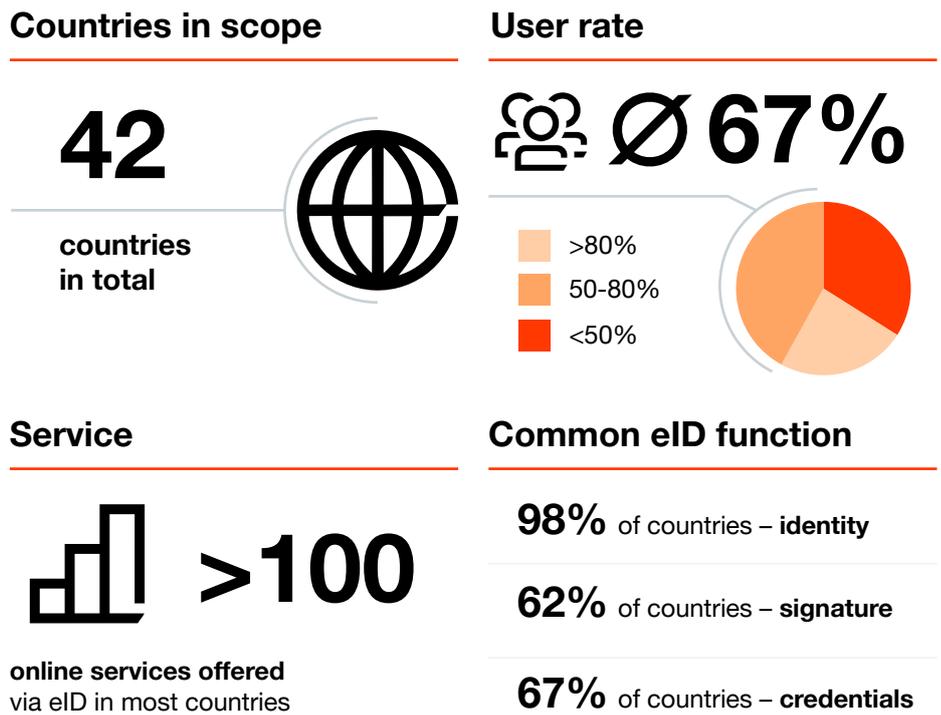
Figure 2: Summary study results

Common eID function

98% of countries – **identity**

62% of countries – **signature**

67% of countries – **credentials**

Figure 2 shows that 42 countries were analysed in total, 15 of which contributed through a dedicated expert survey. On average, around 67% of the population in these countries actively use their national eID solution, with user rates ranging from below 50% to well above 80%. In most countries, eID users can access more than 100 online services, and the majority of solutions support not only basic identification and authentication (98%), but also electronic signatures (62%) and digital credentials (67%).

Complementing this summary graphic, the following table provides a granular, country-by-country view of all systems in scope, including user rates, service coverage, and supported functions:

Country	Digital Identity	Numbers			Functions		
		User Rate	EGDI Rank	Services	Identity	Signature	Credentials
Argentina	Mi Argentina	~57%	42	2000+	✔		✔
Australia	myID	~55%	8	150+	✔		
Austria	ID Austria	~52%	22	400+	✔	✔	✔
Belgium	Itsme (private)	~80%	56	1000+	✔	✔	✔
Brazil	gov.br	~61%	50	12000+	✔	✔	✔
Bulgaria	Evrotrust	~20%	55	100+	✔	✔	✔
Chile	ClaveÚnica	~80%	31	1700+	✔		✔
Croatia	eOI	~46%	32	100+	✔	✔	✔
Czechia	eDoklady	~70%	54	~150	✔	✔	✔
Denmark	MitID	~93%	1	100+	✔	✔	
Estonia	Mobile-ID, Smart-ID	~92%	2	3000+	✔	✔	
Finland	FTN	~96%	9	100+	✔	✔	
France	France Identité	~88%	34	1400	✔		✔
Georgia	Georgian electronic eID	~88%	69	-	✔	✔	
Germany	ID mit Online-Ausweisfunktion	~25%	12	66	✔	✔	✔
Hungary	eSzemélyi igazolvány	~51%	59	4600+	✔	✔	✔
India	Aadhaar	~99%	97	2000+	✔		✔

Country	Digital Identity	Numbers			Functions		
		User Rate	EGDI Rank	Services	Identity	Signature	Credentials
Israel	Smart ID	~55%	23	200+	✓	✓	✓
Italy	SPID	~89%	51	500+	✓	✓	✓
Japan	My Number Card	~80%	13	200-500	✓		
Latvia	eParaksts Card	~85%	29	700+	✓	✓	
Lithuania	Mobile-ID, LT-ID, Smart-ID	~74%	21	500+	✓		✓
Luxembourg	LuxTrust & GouvID	~75%	45	-	✓	✓	✓
Mexico	CURP/Llave MX	~7%	65	200+			
Nepal	Nagarik	~5%	119	25+	✓		
Netherlands	DigiD & eHerkenning	~95%	10	100+	✓		
Norway	MinID, BankID, Buypass, Commfides	~97%	15	16000+	✓		✓
Pakistan	NADRA	~97%	136	-	✓		
Poland	mObywatel	~28%	37	40+	✓		✓
Portugal	ID.gov.pt	~39%	49	~397	✓	✓	✓
Saudi Arabia	Absher	~80%	6	460+	✓		✓
Singapore	Singpass	~97%	3	2000+	✓	✓	✓
South Korea	Mobile ID	-	4	-	✓	✓	
Spain	MiDNI/ Mi Carpeta Ciudadana	~59%	17	4600+	✓	✓	✓
Sweden	BankID & Freja eID	~92%	14	6000+	✓		
Switzerland	e-ID swiyu	-	26	50-100	✓	✓	✓

Country	Digital Identity	Numbers			Functions		
		User Rate	EGDI Rank	Services	Identity	Signature	Credentials
Türkiye	e-Devlet	~78%	27	7400+	✓	✓	✓
Ukraine	Diia	~58%	30	130+	✓	✓	✓
United Arab Emirates	UAE Pass	~95%	11	1000+	✓	✓	✓
United Kingdom	One Login	~19%	7	80+	✓		
Uruguay	ID Uruguay	~50%	25	1500+	✓	✓	✓
Vietnam	VNeID	~63%	71	100+	✓	✓	✓

In several countries, particularly in Northern Europe, eID usage rates already exceed 90%. Finland reaches about 96% penetration with more than 100 connected services, Denmark around 93% with over 100 services, and Estonia roughly 92% with more than 3000 digital public services. These countries regularly rank at the top of the E-Government Development Index Rank (EGDI Rank), reflecting advanced e government development enabled by strong online service provision, telecommunications infrastructure, and human capital.

In Latin America, Brazil and Chile also show high eID adoption, despite lower overall digitalisation rankings compared to the Nordics. In Brazil, around 61% of the population uses gov.br; Chile reaches approximately 80% usage with more than 1,700 services via ClaveÚnica. In Argentina, Mi Argentina is gaining traction at around 57% usage, supported by the integration of official documents and core administrative processes. These cases suggest that a broad and relevant service portfolio, especially in social benefits, identity verification, and mobility can drive high usage, even outside the global digital frontrunner group.

In developing countries such as Nepal, usage is still emerging. The Nagarik app currently offers a limited range of services (around 25+), mainly for central administrative processes such as police clearances, passports, and bank onboarding. This indicates that expanding both the number and relevance of services tends to increase adoption only gradually.

As mentioned, Denmark stands out with its national solution MitID among the most advanced cases. The country ranks first in the EGDI and has achieved rapid, broad adoption through close cooperation with the financial sector (e.g., mandatory use for online banking) and early integration into everyday services. MitID's two-factor authentication and strong data protection framework further support high trust and acceptance.

Another notable example is Ukraine. Since Russia's 2022 invasion, the digital platform Diia has become essential for maintaining government services. It enables online access to civil registration, social benefits, tax services, and permits, and additionally offers wartime functions such as compensation claims, veteran support, air-raid alerts, and reporting of troop movements. Diia illustrates how eID Systems can ensure continuity and resilience of public services in crisis situations.

Privately operated eID models also exhibit strong adoption dynamics. In Belgium, the identity solution itsme is widely used across public and private services, illustrating how market-driven solutions can gain broad trust and become embedded in everyday transactions. Similarly, the Bulgarian solution Evrotrust demonstrates how a mobile first design and deep integration with private-sector actors can accelerate user onboarding and electronic signing in areas such as banking, telecommunications, and insurance, while also supporting selected government processes.

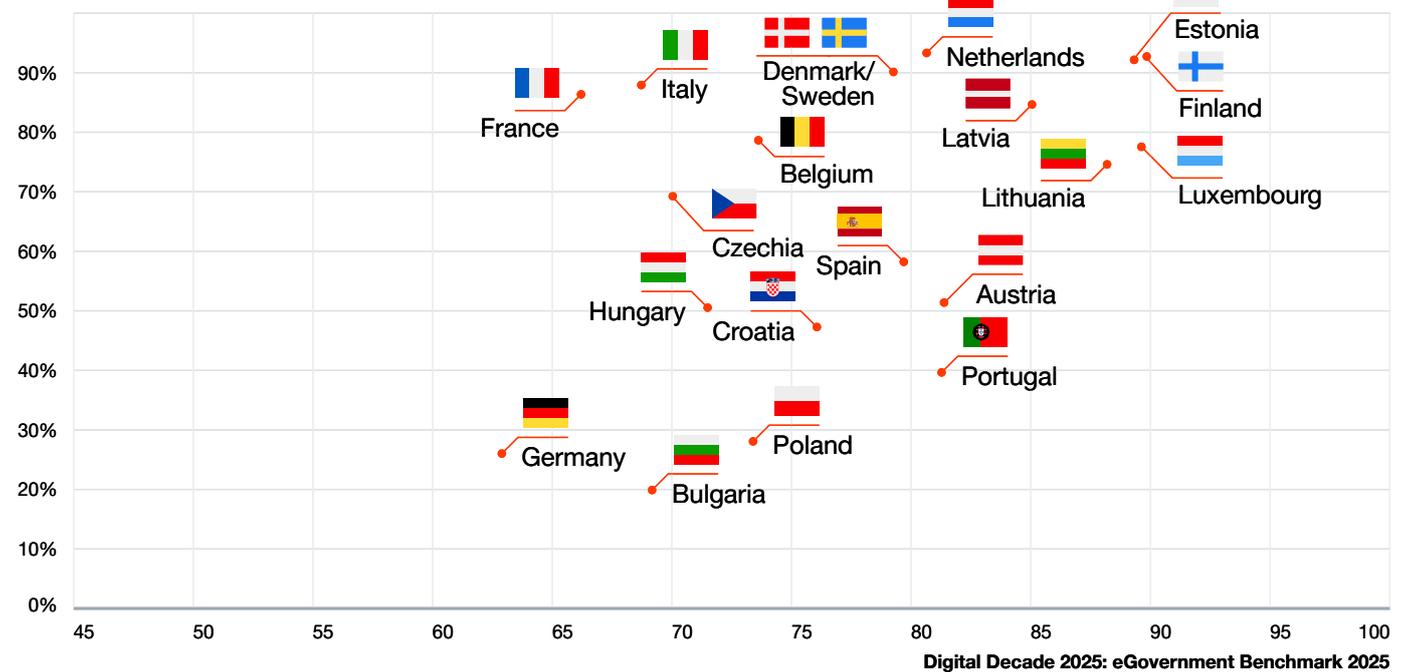**Deep dive I** Positioning of EU countries by eID usage

Figure 3: Visualization of user rates in correlation with the eGovernment Benchmark 2025. eGovernment Benchmark 2025: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-egovernment-benchmark-2025 User Rate: Check country reports for further information.

Figure 3 presents a scatter plot of selected EU member states by their projected eID user rate in 2025 and their performance in the Digital Decade 2025 eGovernment Benchmark, which indicates the overall maturity of digital public services. Nordic and Baltic countries cluster in the top-right quadrant, combining very high eID uptake with leading digital-government performance. A broad midfield of member states shows more mixed constellations, where advances in one dimension are not consistently matched by the other. Countries like Germany and Bulgaria appear in the lower range of the distribution, highlighting that eID adoption and e-government performance remain uneven across the EU and that targeted improvements are required. The distribution of countries also suggests that contextual conditions – such as the availability and usability of key digital public services, levels of trust in digital identities, and the overall digital maturity of society – may influence eID take-up. Consequently, the projected eID user rate should be interpreted together with broader measures of e-government performance rather than as a standalone indicator.

Challenges

Across the countries examined in this study, the development and use of national eID systems are shaped by diverse legal, technical and societal conditions. Despite these differences, the challenges that emerge can be grouped into a set of overarching dimensions. Organising the findings along these dimensions helps to provide a clearer and more systematic understanding of the obstacles involved and forms a coherent analytical basis for the success factors and recommendations discussed later in the report.

The first dimension concerns the regulatory and governance context. Several countries operate eID systems within legal frameworks that have not yet fully kept pace with technological and organisational developments. Japan's My Number Card illustrates this tension: while the system is intended to support public-sector digitalisation, the legal framework needs to be modernized to avoid unintended consequences and to ensure flexibility for private-sector solutions. Within the EU, countries such as Hungary and Lithuania face additional pressures arising from the alignment of national rules with the forthcoming European Digital Identity Wallet and eIDAS 2.0 standards.

A second dimension relates to the technical and infrastructural foundations of eID systems. Here, countries often encounter issues of interoperability, legacy system migration and system architecture. ID Austria highlights the difficulties that arise when federal, state and agency-level infrastructures are not fully aligned, complicating not only internal coordination but also user readiness for the eID system. Luxembourg faces a different but related challenge: the parallel operation of LuxTrust and GouvID requires additional technical coordination and governance alignment across public and private infrastructures. In Europe, several states are preparing for the transition to eIDAS 2.0, which requires substantial technical adjustments. Hungary's eSzemélyi igazolvány exemplifies the challenges associated with migrating older account structures and updating outdated system flows while maintaining operational stability. These transitions are critical to ensuring that eID systems remain reliable, scalable and compatible with emerging cross-border solutions.

A third, cross-cutting dimension involves security, privacy and public trust. Strong data protection and cybersecurity are preconditions for any successful eID ecosystem, yet concerns in this area remain widespread. Argentina's system has, for instance, been affected by recurring security issues that continue to undermine confidence. Switzerland's experience following the 2021 referendum similarly shows how privacy concerns and perceived shortcomings in security or legal safeguards can significantly slow user acceptance. The United Kingdom provides an equally compelling example, where public perception and a lack of trust have so far prevented the successful establishment of a national eID.

Historically, there has never been a general obligation to carry an identity card, and this tradition has contributed to a persistently low level of public trust for electronic identification systems. At the same time, in countries with very high uptake such as India, users increasingly question whether digital identity might become de facto mandatory, reflecting worries about autonomy and potential state overreach. These dynamics underline the central role of trust as a political, technical and societal variable.

The fourth dimension relates to user experience, digital inclusion and adoption. Differences in digital literacy remain one of the most persistent barriers to effective use. Italy's SPID system demonstrates the importance of straightforward onboarding processes and accessible design, particularly for older or less digitally confident users. Nepal faces even more pronounced literacy gaps, especially in rural areas, which directly limit adoption and everyday usability. Japan likewise needs to provide additional support for groups with limited digital skills to ensure broad participation. Even where usability barriers are low, adoption may remain modest if relevant use cases are lacking. The Netherlands provides an example: while DigiD and eHerkenning are widely known and technically reliable, their limited integration into digital wallet environments reduces everyday incentives to use them. In several countries, an additional challenge arises from the relationship between public-sector identity solutions and private-sector offerings. State-led approaches must ensure that they support, rather than suppress, innovation and competition in the wider identity ecosystem.

Taken together, these four dimensions - regulatory and governance, technical and infrastructure, security and trust, and user inclusion and adoption - offer a structured and comprehensive view of the challenges identified in the study. They form the analytical basis for the subsequent discussion of success factors and point of departure for the recommendations developed in the following chapters.

1 **Dimension of Regulatory and Governance**

- Legal and **governance frameworks often lag behind** developments in eID systems
- This creates **regulatory uncertainty** and implementation challenges

Examples:
Japan's My Number Card, the UK's One Login, and EU member states under eIDAS 2.0

2 **Dimension of Technical and Infrastructural Foundations**

- Technical and **infrastructural foundations** of eID systems are often **poorly aligned**
- This **hinders adaptation, interoperability**, and further development

Examples:
Australia's myID and Hungary's eSzemélyi, both affected by legacy system constraints

3 **Dimension of Security, Privacy and Public Trust**

- **Security, privacy, and public trust** are critical for successful eID adoption
- **Ongoing concerns** continue to **undermine user confidence**

Examples include Argentina's security issues, Switzerland's privacy concerns, and India's fears of de facto mandatory digital identity

4 **Dimension of User Experience, Inclusion and Adoption**

- **Digital literacy gaps** are a key barrier to effective use
- Adoption remains low **without relevant use cases**

Examples:
Nepal – rural literacy gaps; Japan – limited digital skills in some groups

Figure 4: Summary of the most common challenges

Success Factors and Recommendations

International comparison shows that the challenges described in the previous chapter can be addressed effectively when countries strengthen a corresponding set of success factors. Countries with the most mature eID ecosystems tend to exhibit similar patterns across these dimensions. The following section outlines these recurring factors, illustrates them with examples from different national contexts, and derives clear, actionable recommendations for each dimension.

Regulatory and Governance

Successful eID systems rely on **clear governance structures with well-defined responsibilities, legal accountability, and coordination** across agencies. Public–private partnerships are effective in combining the regulatory legitimacy and stability of the state with the innovation, customer reach, and agility of private actors.
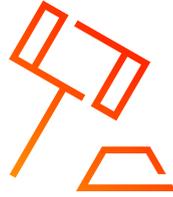
Technical and Infrastructural

Robust technical infrastructure and seamless integration of services are essential success factors. A single secure identity, integrated across public administration and sectors such as healthcare and finance, makes the eID indispensable in everyday life.

Security and Trust

Public trust is the fundamental driver of adoption. **Applying international standards** such as eIDAS **provide assurance and interoperability**. Success cases show that the pairing of strong authentication, certified infrastructure and transparent user control over data access with clear communication about security practices reinforce trust.

User Inclusion and Adoption

High adoption is achieved when eID systems are deeply embedded in everyday life, providing tangible value through routine use. Digital literacy, user-friendly onboarding, and design for less tech-savvy citizens support high user rates.

Figure 5: Summary of the most recurring success factors

A. Regulatory and Governance

Successful eID systems rely on clear governance structures with well-defined responsibilities, legal accountability, and coordination across agencies. Public–private ecosystem is particularly effective in combining the regulatory legitimacy and stability of the state with the innovation, customer reach, and agility of private actors. Belgium's itsme platform, developed by banks and telecom operators under government recognition, exemplifies this approach, while Finland's Finnish Trust Network allows banks and telecom providers to act as identity providers under a clear state framework.

Flexibility in legal and organisational structures ensures long-term adaptability. Norway's BankID illustrates how early joint decisions by banks, combined with integration into government services through ID-Porten, created broad adoption while ongoing reforms now aim to include individuals without bank accounts, demonstrating responsiveness to evolving societal needs. Ukraine's eID System further shows the value of adaptability, serving not only routine public services but also functioning as a crisis communication tool during wartime.

Alignment with international standards such as eIDAS 2.0 is another critical factor for governance, providing clarity for cross-border interoperability. Although the transition towards eIDAS 2.0 and the EUDI Wallet is demanding, countries such as Hungary and Lithuania, which are preparing for the European Digital Identity Wallet, demonstrate that legal alignment underpins both scalability and trust. Poland's mObywatel is among the more advanced initiatives in implementing eIDAS 2.0, participating in the EUDI-Wallet Large-Scale Pilots (LSPs) and conducting pilot programmes to test and develop use cases prior to implementation – illustrating how early alignment can become a strategic advantage by strengthening scalability, interoperability and trust.

Recommendation:

Countries should formalise eID governance with clearly assigned liability, oversight and regulated public–private roles, promote a regulated public–private ecosystem for innovation and reach, and use early alignment with international standards (such as eIDAS 2.0) to turn necessary regulatory adaptation into a long-term success factor – enabling national solutions to be scaled and integrated into cross-border wallet ecosystems without costly redesigns.

B. Technical and Infrastructural

Robust technical infrastructure and seamless integration of services are essential success factors. Estonia's eID demonstrates how a single secure identity, integrated across public administration, banking, healthcare, and even democratic participation, creates strong network effects. Brazil's gov.br platform similarly consolidates over 12,000 federal and state services, including digital credentials and legally valid e-signatures, making the eID indispensable in daily life.

Smooth transitions from legacy systems are equally important to avoid service disruption and enable long-term scalability. Hungary's eSzemélyi igazolvány illustrates the challenges of account migration, outdated system flows, and policy implementation under eIDAS 2.0, highlighting the need for modular, adaptable technical architectures. Fragmentation across federal or agency levels, as seen in Australia's myID ecosystem, demonstrates the importance of interoperability within and across administrative layers.

Mobile-first system design further enhances accessibility, as illustrated by ID Austria, Brazil's gov.br, and Bulgaria's Evrotrust app, allowing onboarding and daily use without hardware dependencies and facilitating broad participation.

Recommendation:

Technically, eID should be implemented as a scalable, mobile-first trust layer that can be reused across sectors, with explicit migration paths from legacy systems and strong interoperability between administrative levels, so that adding new services or moving existing ones to the eID infrastructure becomes routine rather than a bespoke project.

C. Security and Trust

Public trust is a fundamental driver of adoption and is closely linked to security and data governance. Denmark and Estonia exemplify systems that pair strong authentication, certified infrastructures, and transparent user control over data access with clear communication about security practices. Argentina illustrates how unaddressed security concerns can dampen user confidence, while Switzerland's experience after the 2021 referendum shows that inconsistent legal standards or privacy concerns can slow adoption even when the technology is sound. High-coverage systems also face the challenge of perceived state overreach, as seen with India's Aadhaar, underlining that even technically

robust systems must carefully balance security, privacy, and autonomy as a key condition for sustained legitimacy and uptake. Adoption of international standards such as eIDAS ensures cross-border interoperability and reinforces trust, providing citizens with assurance that their personal information is handled securely and consistently.

Recommendation:

To sustain trust at scale, eID strategies should combine independently audited cybersecurity with data-minimisation and clear, purpose-bound rules for data use. Citizens must retain meaningful control over how and where their identity data is used, supported by transparent communication and simple consent tools. Credentials should create real value at the point of use, for example by enabling secure re-use of verified data instead of repeated manual checks, and new features should be rolled out via focused pilots so that security, privacy and user experience can be tested and improved iteratively.

D. User Inclusion and Adoption

High adoption is achieved when eID systems are deeply embedded in everyday life, providing tangible value through routine use. Denmark's MitID, which is mandatory for online banking, healthcare appointments, and e-commerce, and India's Aadhaar, which enables access to social programmes, subsidies, and financial services, illustrate how everyday relevance drives widespread uptake. Another outstanding example for the integration of an eID system into everyday life is Ukraine's eID Diia, which already provided full access to key public services during the COVID-19 pandemic, including registration for vaccinations, tax payments and declarations, payments of fines and fees, and place-of-residence registration, as a legislatively approved electronic passport. Owing to this advanced functionality and user-centred design, Diia deservedly won the Red Dot Design Award in 2021 and gained international recognition.

Within Southeast Asia, Vietnam has emerged as a frontrunner in its adoption. Within four years of its launch, the VNeID system has scaled to over 70 million activated accounts by May 2025, with daily active users increasing three- to fourfold since 2023. The platform has processed more than 2.1 billion transactions, generating administrative cost savings of approximately USD 18.5 million. VNeID integrates 80% of public services online, digitizes six key document categories (ID cards, passports, driving licenses, vehicle registrations, health insurance, social insurance), and connects 13 commercial banks for biometric authentication covering 56.8 million customers, significantly reducing fraud. Beyond national deployment, Vietnam has strengthened its regional leadership by supporting Laos in developing its national eID system.

Furthermore, digital literacy and accessibility are critical for equitable adoption. Italy's SPID system shows the importance of user-friendly onboarding and design for less tech-savvy citizens. Nepal demonstrates pronounced gaps in rural digital literacy, while Japan highlights the need to support users with low digital skills to ensure broad engagement. Mobile-native solutions reduce barriers and facilitate adoption, as evidenced by ID Austria, Brazil, and Bulgaria, while practical use cases strengthen motivation. Systems such as the Netherlands' DigiD and eHerkenning, which provide credentials but limited functional services, underscore that technical readiness alone does not guarantee adoption.

Recommendation:

For broad and inclusive uptake, eID programmes should prioritise high-frequency, high-value use cases (e.g. banking, benefits, taxation and healthcare), couple them with simple, mobile-native user journeys, and be embedded in wider digital-literacy initiatives—otherwise, even well-designed credentials risk remaining under-used or excluding less digitally skilled groups.

The following figure summarises these findings and distils them into four concrete recommendation dimensions for the design and further development of national eID ecosystems:

1	**Dimension of Regulatory and Governance**	• **Set clear governance** with defined roles, accountability, and oversight • **Promote regulated public–private partnerships** for innovation and reach • **Align national systems with international standards** for interoperability
2	**Dimension of Technical and Infrastructural Foundations**	• **Build scalable, modular architectures** for multiple services and legacy transitions • **Implement mobile-first onboarding** to reduce hardware barriers for users • **Ensure seamless integration** and user-friendly access across all services
3	**Dimension of Security, Privacy and Public Trust**	• **Build trust** through strong cybersecurity, transparent data use, and proactive communication • **Maximize credential value** at verification points, not at issuance • Make piloting and **iterative learning core principles**
4	**Dimension of User Experience, Inclusion and Adoption**	• **Integrate eID use into essential, high-frequency services** to enhance everyday relevance and adoption • **Provide targeted support for digitally disadvantaged groups,** ensuring equitable participation and broad usability

Figure 6: Summary of the recommendations for further development of national eID ecosystems

05

Country Reports

Argentina

2018

Introduction

~57%

User Rate

42

EGDI Rank

2,000+

Services

Mi Argentina

Systematic secondary research

Overview:

Mi Argentina is a digital platform and mobile application in Argentina that serves as a citizen's digital profile, providing access to various government services and documents. It acts as a gateway for carrying out procedures, managing digital credentials, and receiving personalized information from the Argentine state. Users can store and access digital versions of their ID, driver's license, disability certificate, and other relevant documents. Furthermore, Mi Argentina facilitates scheduling appointments with various government agencies. Citizens complete identity verification at a RENAPER office, then activate the mobile ID via app - usable even offline and can be revoked if the phone is lost.

Success Factors:

Mi Argentina is a key component of the government's digital modernization. The platform includes Tina, a virtual assistant that guides users and automates services such as vaccination and disability certificates, criminal records, and appointment bookings. Tina already handled over 1.3 million conversations via WhatsApp, the app, and the government portal. Since its launch, Mi Argentina has grown from 3 million to more than 26 million users—over half the population.

Outlook:

In 2022, Mi Argentina was recognized as the Best Digital Transformation Solution in Latin America and the Caribbean at the Red GEALC meeting in Lima, an initiative supported by OAS and IDB. Future challenges for Mi Argentina include strengthening data protection and cybersecurity, especially in light of two recent severe cyberattacks that exposed vulnerabilities at both the platform and user-device levels.

Innovación, ciencia y tecnología. Argentina.gob.ar. (2025, April 7).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	✓
Signature	⏳	**Finance**	⏳
Credentials	✓	**Security**	✓

Data as of 2025

Australia

2019/
rebrand 2024

Introduction

~55%

User Rate

8

EGDI Rank

150+

Services

myID

Systematic secondary research

Overview:

Australia is currently undergoing a national rebranding and development initiative: the existing digital identity solution myGovID is gradually being transitioned into myID. myID is intended to serve as a central, government-verified digital identity wallet. In parallel, myGov will continue to operate as a service portal, offering access to over a dozen government agencies - for services such as tax returns, social benefits, Medicare, and pensions. Identity verification is handled through the myID app, which combines document checks, biometric authentication, and device binding. The solution is operated by the Australian Taxation Office (ATO) in collaboration with the Digital Transformation Agency (DTA).

Success Factors:

Australia's success in digital transformation lies in the close integration of identity and public services. The existing solution was embedded early on into large-scale platforms like myGov and now reaches millions of users. The introduction of different trust levels (Basic, Standard, Strong) allows for flexible usage depending on the service. A clearly regulated legal framework and high security standards (Face ID, device linking, 2FA) help build trust and encourage adoption. Additionally, the app supports multiple languages and is fully accessible.

Outlook:

Through the rebranding to myID, Australia aims to establish a full-fledged digital identity wallet. Plans include the integration of official credentials such as driver's licenses, birth certificates, professional qualifications, and the Tax File Number (TFN). Private-sector use - e.g., for banking, employment, or insurance - is also being pursued. The rollout is part of a federally coordinated whole-of-government strategy. Interoperability with other federal, state, and international systems is a medium-term objective.

Minister for Finance. Australian Government. (2025, December 4).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Credentials	⏳	Finance	✓
		Security	✓

Data as of 2025

Austria

2023

Introduction

~52%

User Rate

22

EGDI Rank

83

eGovernment Benchmark

400+

Services

ID Austria

Expert-informed primary data

Overview:

ID Austria, launched on December 5, 2023, is Austria's central digital identity system and a key pillar of its digital government strategy. Following the relaunch of the ID Austria app in mid-2025, adoption accelerated significantly through the nationwide ID Austria Servicetour, which brought registration and on-site support to over 220 locations. Between July and December 2025, around 900,000 new registrations were recorded, increasing the total user base to approximately 4.8 million people. Alongside authentication and qualified electronic signatures, ID Austria enables the use of digital credentials such as driver's licences and vehicle registrations, with more than one million activations each, demonstrating strong acceptance of mobile digital IDs among citizens.

Success Factors:

ID Austria's success is driven by the combination of a secure, user-friendly mobile solution and extensive on-site support. The replacement of the former Handy-Signatur with a modern app improved usability while maintaining high security standards. The Servicetour played a crucial role by offering personal assistance for registration and activation, significantly lowering entry barriers. Close cooperation between federal, regional and local authorities expanded registration points nationwide and strengthened trust in the system. At the same time, the growing integration of ID Austria into administrative and selected private-sector services reinforces its role as a unified access key within Austria's digital ecosystem.

Outlook:

Austria is well-placed to transition into the EUDI-Wallet framework. ID Austria already covers the core EUDI functions e.g. identification, signatures, and verifiable credentials. Future integration could involve incorporating additional document types (e.g. healthcare, digital student card), extending private sector use. Strong existing adoption and legal recognition position Austria ahead as a prospective EU digital identity leader, whereas organizational fragmentation across federal, state and agency levels as well as user accessibility remain a challenge. Austria can serve as a model for other member states adapting to eIDAS 2.0.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Transport**	✓
Signature	✓	**Finance**	✓
Credentials	✓	**Security**	✓

Belgium

2017
Introduction

~80%
User Rate

56
EGDI Rank

72.9
eGovernment Benchmark

1,000+
Services

Itsme (Private)
Expert-informed primary data

Overview:

Itsme is Belgium's leading mobile digital identity app, launched in 2017 by Belgian Mobile ID—a consortium of major Belgian banks (Belfius, BNP Paribas Fortis, ING, KBC) and telecom operators (Orange, Proximus, Telenet). It serves as a secure, user-friendly alternative to the physical Belgian eID card and as a card reader for online authentication, identity verification, and qualified electronic signatures. After a one-time onboarding - either by using the physical eID with a reader or by verifying through a bank account - users can log into public services, approve transactions, and sign legally binding documents directly from their phone. Itsme is recognized under the EU's eIDAS regulation at the highest assurance level (LoA High), meaning it has the same legal value as the Belgian eID card for digital transactions.

Success Factors:

Itsme's success rests on its strong public-private partnership model, which combines the credibility and reach of banks and telecom operators with legal recognition by the Belgian government. Its mobile-first approach removes the friction of card readers, making it far more accessible for everyday use. Widespread integration across both public sector services (tax declarations, municipal portals, healthcare) and private sector services (banking, insurance, utilities, e-commerce) has made it indispensable for millions of Belgians. Itsme is also accessible in other EU countries and can be used e.g. with the Luxembourgish ID as well.

Outlook:

Itsme is expected to remain central to Belgium's digital identity ecosystem and is well-positioned to serve as, or integrate with, the future EU wallet. Likely developments include expansion into cross-border and private-sector services, the implementation of the Once-Only Technical System (cross-border use cases), further pilots using SOLID technology, and the integration of biometric data. A key challenge is the reluctance by Federal Public Authorities to allow the use of eID beyond the public sector or regulates businesses (e.g. banks) that require it for KYC/AML.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Brazil

2019

Introduction

~61%

User Rate

50

EGDI Rank

12,000+

Services

gov.br

Systematic secondary research

Overview:

Brazil's electronic identity is centered on the gov.br app, launched in 2019, which serves as both a digital ID wallet and the main gateway to government services. The app allows citizens to log in securely using biometrics or bank-based verification, access more than 12000 digital services across federal and state administrations, and store official documents such as the national ID (CIN), digital driver's licence (CNH Digital), work card, and vaccination certificate. Each user is assigned an assurance level - Bronze, Silver, or Gold - based on the degree of identity verification, balancing accessibility with strong security. The integrated Assinatura gov.br feature enables users to sign documents electronically within the app, eliminating paper-based procedures and offering a full digital identity journey.

Success Factors:

Brazil's eID ecosystem stands out for its scale, inclusiveness, and integration. By 2025, more than 130 million unique users - around 61% of the population - had accessed gov.br, making it one of the world's largest eID Systems. The unified platform integrates over 4500 federal and 8000 state-level services, allowing citizens to manage taxes, healthcare, pensions, and employment from a single account. Its user-friendly design, biometric login, and in-app signing have significantly boosted public trust and everyday use, reflecting a strong commitment to citizen-centric digital government.

Outlook:

In the coming years, Brazil plans to extend the gov.br wallet by adding new credentials such as academic diplomas, property records, and professional licences, while encouraging more citizens to upgrade to Gold-verified accounts. The long-term vision is a universal digital identity layer that bridges public and private sectors, enabling secure and frictionless access to a growing range of services. With its rapid adoption and continuous innovation, Brazil's model is emerging as a global reference point for large-scale mobile identity systems.

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Transport	✓
Credentials	✓	Security	✓

Data as of 2025

Bulgaria

2018
Introduction

~20%
User Rate

55
EGDI Rank

68.2
eGovernment Benchmark

100+
Services

Evrotrust (private)
Expert-informed primary data

Overview:

Evrotrust offers a mobile application that enables remote identity verification, strong authentication, and qualified electronic signatures – all without the need for a physical smart card or card reader. The solution is fully compliant with the EU eIDAS Regulation, meaning that qualified electronic signatures created through Evrotrust have the same legal effect as handwritten signatures across the European Union. The platform supports secure remote onboarding by scanning official identity documents (such as a Bulgarian ID card or passport) and performing biometric facial recognition checks, followed by the issuance of digital certificates that are securely stored in the cloud and accessed via the mobile application. This enables users to sign contracts, submit official documents, and access both public- and private-sector services from anywhere.

Success Factors:

Evrotrust is integrated with a wide range of Bulgarian public services and is broadly used by banks, telecom operators, insurers, and utility providers for customer onboarding and contract execution. Recognized as a notified electronic identification scheme under eIDAS, Evrotrust is also used as a means of electronic identification for accessing e-government services in Bulgaria and, where applicable, in other EU Member States through cross-border recognition mechanisms. It's one of the few companies to be operating as the Bulgarian national notified eID scheme which allows them to be the PID provider.

Outlook:

Given that the company is predominantly Bulgarian and official communications between 2023 and 2025 report an increase in the number of clients from 1 million to 2 million users – without distinguishing active from inactive users, but counting anyone who has used the services – it is reasonable to assume that the majority of these users are Bulgarian. A very conservative estimate would be that at least 50 percent are domestic clients.

On this basis, assuming approximately 1 million Bulgarian users and an adult population (18+) of around 5.3–5.4 million people, the company reaches an estimated market penetration of roughly 19–20 percent. This appears plausible given the large number of private users and the structural limits of the market, as only about half of the adult population is economically active.

The Bulgarian market can therefore be considered relatively saturated, making sharp further growth unlikely due to demographic constraints, while international expansion offers significantly greater growth potential.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓		

Chile

2012

Introduction

~80%

User Rate

31

EGDI Rank

1,700+

Services

ClaveÚnica

Systematic secondary research

Overview:

Chile's digital identity ecosystem revolves around ClaveÚnica, a universally used digital authentication platform with over 15.8 million users, enabling more than 1600 public-sector procedures. In December 2024, Chile launched a digital national ID card embedded with advanced security features, accessible via a mobile app. This complements - rather than replaces - the physical ID, positioning Chile toward broader mobile identity use in the public and potentially private sectors.

Success Factors:

Chile's digital identity framework succeeds through mass adoption of Clave Única and deep integration with public services. The government's strategy of building on a trusted system while adding the new digital ID card in 2024 strengthens both usability and security. Combined with features like biometric safeguards and the first digital driver's licenses, these steps make the ecosystem both practical and credible, positioning it well for future expansion into healthcare and private services.

Outlook:

Chile is well positioned to evolve its system toward an EUDI-Wallet-like model, even though it operates outside the EU. Priorities ahead are expanding mobile digital ID adoption beyond government into healthcare, banking, telecom, and e-commerce, and ensuring international interoperability through global standards. The introduction of digital driver's licenses in 2025 and the 2024 digital ID card with mobile functionality already show Chile's ability to combine convenience with strong security. Going forward, the challenge will be sustaining citizen uptake while achieving trust and usability in private-sector contexts, making its ecosystem a potential benchmark for digital identity in Latin America.

Gobierno Digital Lanza Campaña Para proteger Y Mantener actualizados Los Datos de Claveúnica. GobDigital. (2025, May 27). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	⧖
Credentials	✓	**Finance**	✓
		Security	⧖

Data as of 2025

Croatia

2015

Introduction

~46%

User Rate

32

EGDI Rank

75

eGovernment Benchmark

100+

Services

eOI

Expert-informed primary data

Overview:

Croatia's eOI (electronic identity card) has been a cornerstone of the country's digital transformation since its launch in 2015. The card combines physical identification with digital credentials for authentication and qualified electronic signature (QES), making it a central tool for accessing the e-Građani (e-Citizens) portal. Recognized at the highest assurance level under eIDAS (LoA High), the eOI is legally valid across the EU. By April 2025, more than 2 million citizens actively used the e-Građani system to access a wide range of services, from tax filing to health insurance management and school records.

Success Factors:

Success rests on compulsory, chip-based IDs that come ready for online use, a central SSO (NIAS), and practical, high-demand e-services (tax, health, schools, driving). The addition of remote QES (Mobile.ID) removed card-reader friction, while eIDAS notification (High LoA) built legal trust for cross-border use. Uniquely, Croatia's scheme already combines identification, qualified signature, and digital credentials in one system, placing it among the EU's more mature eID models.

Outlook:

Looking forward, Croatia is well positioned for the transition to the EUDI Wallet under eIDAS 2.0. With a notified scheme already at the highest EU trust level, technical interoperability is more a matter of integration than reinvention. The next step will be to extend eOI credentials into the mobile wallet environment, enabling citizens to share verifiable attributes across borders in a privacy-preserving way. Planned expansions, such as mandatory B2B e-invoicing from 2026, will further drive digital adoption and strengthen private-sector involvement. Croatia's trajectory suggests it can serve as a regional frontrunner, showing how a national eID can evolve smoothly into the EUDI Wallet ecosystem.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Czechia

2021

Introduction

~70%

User Rate

54

EGDI Rank

70.4

eGovernment Benchmark

~150

Services

eDoklady

Expert-informed primary data

Overview:

Czechia's eID system is based on the Občanský průkaz (electronic ID card) and the online identity gateway Identita Občana. The eID card with chip and PIN enables authentication and qualified electronic signature for both government and private services. Since 2021, biometric eID cards have been issued under Act 269/2021 Coll. In 2024, the government launched the eDoklady mobile ID app, enabling citizens to present and verify digital identity documents via smartphone. The national infrastructure is aligned with eIDAS and linked to EU cross-border recognition schemes.

Success Factors:

The modernization of Czech eID benefited from the legal update in 2021, which introduced biometric cards and established clear assurance levels under eIDAS. Integration with Bank ID and Identita Občana portals simplified onboarding and expanded access. Cooperation between ministries, banks, and IT providers promoted technical stability and user convenience. Public acceptance grew through visible use cases in taxation, social security, and education.

Outlook:

Czechia's next milestone is the full rollout of eDoklady as a secure mobile ID wallet. The app will enable both online and offline verification and support additional credentials such as driving licenses and residence permits. The government aims for full interoperability with the EUDI Wallet and to increase adoption among younger citizens. Continuous service expansion and reliability improvements remain key, following recent outages in 2025.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Denmark
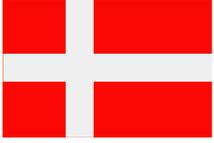
2010/2021

Introduction

~93%

User Rate

1

EGDI Rank

77.6

eGovernment Benchmark

100+

Services

MitID

Systematic secondary research

Overview:

MitID was introduced in 2021 as Denmark's national eID solution, replacing the previous system, NemID. The system is centrally operated by the Danish Agency for Digital Government and is accessible to citizens, residents, and organizations. The eID can be used across a wide range of applications, including public services, online banking, insurance services, and access to healthcare. The user rate above the age of 15 is around 97%, making Denmark one of the leading countries in terms of eID adoption. The data protection framework is based on the GDPR, ensuring a high level of personal data security.

Success Factors:

A key success factor in Denmark was the close collaboration with the financial sector, particularly with banks. Since MitID is required for online banking, this created a broad user base. Early integration into many everyday applications - from doctor's appointments to online shopping - also contributed to widespread acceptance. Technically, Denmark relies on two-factor authentication and grants users rights to control their data. A consistent focus on privacy and user-friendliness has built trust and established a stable infrastructure.

Outlook:

Looking ahead, it will be crucial to adapt MitID to new technological requirements and platforms. Earlier challenges, such as a lack of compatibility with mobile devices, have largely been resolved. However, rising demands for security and usability will necessitate the development of new features and use cases. In addition, efforts will need to be made to better engage younger users and those less familiar with digital technologies.

MitID statistics. MitID. (2025, January).
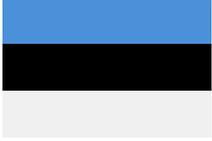Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	⏳	Security	✓

Data as of 2025

Estonia

2002
Introduction

~92%
User Rate

2
EGDI Rank

89.4
eGovernment Benchmark

3,000+
Services

Mobile-ID, Smart-ID, ID-Card
Systematic secondary research

Overview:

Estonia is internationally regarded as a digital frontrunner. Its eID solution consists of a physical ID card (introduced in 2002) and the complementary Mobile-ID (since 2007). The ID-Card is issued by the Police and Border Guard Board (Ministry of the Interior) and Mobile-ID/ Smart-ID are operated by SK ID Solutions (ecosystem with service providers/banks/telcos). They enable comprehensive digital access - from tax declarations to banking and retrieving medical records. Around 91.5% of the population uses the system, and more than 450 public & private organisations are connected to it. The data protection framework is based on the GDPR.

Success Factors:

Estonia's success is rooted in a long-term digital strategy, strong political commitment, and a consistent infrastructure policy. Public trust in digital administration is high, reinforced by transparency, technical standards, and broad user rights. The vast number of services compatibles with the eID system has made digital identity an integral part of daily life. Estonia was also one of the first countries to implement digital voting systems, electronic prescriptions, and a central patient health record.

Outlook:

Going forward, Estonia must continue modernizing its technical infrastructure to keep pace with growing demand. Key areas include improving compatibility with new platforms (e.g., browsers, operating systems), integrating additional digital services, and ensuring cybersecurity. International interoperability - especially with other EU countries via eIDAS - will also become increasingly important. Due to its pioneering role, Estonia is increasingly seen as an exporter of eGovernment solutions.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Private Sector	✓
Credentials	⧗	e-Residency	✓

Data as of 2025

Finland

2017

User Rate

~96%

User Rate

9

EGDI Rank

89.3

eGovernment Benchmark

100+

Services

FTN

Systematic secondary research

Overview:

The Finnish Trust Network (FTN) is Finland's national eID infrastructure, which has been state-regulated since 2019. Unlike centralized state-run wallets, FTN is based on a federated model: government-approved private identity providers (such as banks and mobile operators) offer eID services that can be used across both public and private systems. The platform supports secure authentication for government portals, financial services, mobile providers, and more. FTN is regulated by the Finnish Digital and Population Data Services Agency (DVV).

Success Factors:

A key success factor is the market-based model, supported by a strong banking infrastructure, high digital maturity, and clear government regulation. FTN enables a unified technical interface for all providers and services. Adoption rates are high because users can access eID services via existing banking or telecom credentials. The government ensures interoperability and oversight, while users benefit from low entry barriers and widespread availability.

Outlook:

Finland plans to complement FTN with a new state-operated eID, which will also be interoperable with the upcoming European Digital Identity Wallet (EUDI Wallet). The new solution will include qualified electronic signatures, digital credentials (e.g., driver's licenses, educational certificates), and mobile usability. This initiative is part of Finland's national Digital Strategy 2030. The existing FTN model is expected to remain in place and operate in parallel—with stronger alignment to the EU's eIDAS 2.0 framework.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	⧗	Security	✓

Data as of 2025

France

2022

Introduction

88%

User Rate

34

EGDI Rank

65.9

eGovernment Benchmark

1,400+

Services

France Identité

Systematic secondary research

Overview:

France Identité is widely available since February 2024. It offers secure, single-use identity credentials, integration with FranceConnect, and the ability to store digital versions of key documents such as the national ID card, driving licence, and soon vehicle registration and health insurance card. A certification process - via in-person verification - allows users to access sensitive e-services like electronic proxy voting.

Success Factors:

The effectiveness of France Identité stems from its strong alignment with user needs and state digital services. By enabling users to prove their identity securely with single-use credentials and storing key documents like ID cards and driving licenses, the app enhances convenience and security. Seamless integration with FranceConnect connects citizens to over 1,400 public services, while the certification process enables trust for sensitive processes such as electronic voting. Future additions like digital vehicle registration and health insurance cards further extend its utility and inclusiveness.

Outlook:

Looking ahead, France Identité is poised to become a core national digital identity enabler within the broader eIDAS 2.0 / EUDI-Wallet framework. With planned support for Carte Vitale and vehicle registration, the app's ecosystem will expand into healthcare and mobility. Ensuring interoperability across EU services, safeguarding high privacy and security standards, and promoting user adoption will be crucial - as will extending its applicability across both public and private sectors. Successful rollout could position France as a leading digital identity adopter in the EU.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	✓
Credentials	✓	**Transport**	✓
		Security	✓

Data as of 2025

Georgia

2011

Introduction

~88%

User Rate

69

EGDI Rank

Georgian electronic identity card

Systematic secondary research

Overview:

The Georgian electronic identity card (eID), introduced in 2011, is a mandatory national identification document for citizens aged 14 and above and serves both as an official photo ID and a secure digital identity credential. The eID is a smart card with an embedded chip that stores personal data, biometric information, and digital certificates for authentication and qualified electronic signatures. Holders can use the eID to access Georgia's unified e-government portal (my.gov. ge), perform legally binding transactions online, and interact securely with public and private sector services. In parallel, the Mobile-ID service allows citizens to authenticate and sign documents using their mobile phone SIM card, removing the need for a physical card reader.

Success Factors:

Georgia's eID success stems from strong political commitment to digital transformation, supported by legal reforms enabling electronic signatures with full legal effect. The rollout coincided with the creation of Public Service Halls, physical one-stop shops for administrative services, which increased public awareness and adoption. Broad integration with essential e-government services - from tax declarations to property registration - ensured that the eID became practically useful from the start.

Outlook:

The Georgian eID is expected to evolve toward a fully mobile-first digital ID wallet that consolidates physical and digital credentials into a single app-based solution, in line with global trends and EU digital identity principles. Given Georgia's aspirations for closer alignment with the EU, interoperability with the upcoming European Digital Identity (EUDI) Wallet framework is a likely priority.

According to the information of the Services Development Agency, 199,109 adult citizens of Georgia do not own a passport, an electronic ID card, or a non-electronic ID card. Interpressnews. (2024, October 18). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	⧗	Security	✓

Data as of 2024

Germany

2010

Introduction

~25%

User Rate

12

EGDI Rank

62

eGovernment Benchmark

Personalausweis mit Online-Ausweisfunktion

Expert-informed primary data

Overview:

The Online-Ausweis (eID) has been part of the German national ID card (Personalausweis) and electronic residence permits since 2010. It enables digital identification via an NFC-enabled smartphone or card reader – secured by a personal PIN and supported by the federal AusweisApp. The system is administered by the Federal Ministry of the Interior (BMI), with technical operations handled by Bundesdruckerei GmbH and Governikus GmbH & Co. KG.

Success Factors:

Despite low adoption, the eID offers high security – including end-to-end encryption, certified server communication, and full user control. Recent integration into portals like BundID and Elster, smartphone-based access, NFC use, default activation, and third-party providers like AUTHADA have improved accessibility and adoption. It is used for secure applications such as criminal record checks and digital tax assessments. However, the variety of services (BundID, Elster, eID) and independent authority decisions create uncertainty and inconsistent identification processes.

Outlook:

In light of eIDAS 2.0, Germany plans to evolve the current eID into a fully-fledged European Digital Identity Wallet (EUDI Wallet) under the leadership of the newly established Federal Ministry for Digital Transformation and Government Modernisation (BMDS). This will include verifiable credentials such as driver's licenses, academic qualifications as well as a qualified electronic signature. The federal government aims to increase everyday use, including in banking, contracts, and mobility services. Parallel efforts will focus on enhancing smartphone usability and improving user experience, introducing 'Digital First' to enable broader eID use, and reinstating the online PIN reset service, which had previously been discontinued for cost reasons. Germany is actively involved in EU pilot projects for the Digital Identity Wallet while the release of the national EUDI Wallet is currently scheduled for January 2027.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓
		Transport	✓

Hungary

2016

Introduction

~51%

User Rate

59

EGDI Rank

71.8

eGovernment Benchmark

4,600+

Services

eSzemélyi igazolvány

Systematic secondary research

Overview:

Hungary's electronic identity is built on the eSzemélyi (chip-enabled ID card, launched 2016) and the central login broker KAÜ (Central Authentication Agent) that connects to the national services portal magyarorszag.hu and sector portals (tax, justice, health). In 2024/25 the government introduced the DÁP – Digital Citizen mobile app as a progressively expanding eID / wallet front end that integrates KAÜ login, mobile digital ID and, since early 2025, qualified e-signatures replacing AVDH. The setup aims at alignment with eIDAS 2.0 / EUDI Wallet while maintaining the established card- and cloud-based eID stack. In the EU eGovernment Benchmark 2024, Hungary scores below the EU average but with solid "key enablers" coverage (eID, eDocuments) and ongoing work on cross-border and service-design transparency.

Success Factors:

Three drivers underpin adoption: (1) Broad coverage of credentials — the eSzemélyi is the standard national ID (with eID and eSignature capabilities) and KAÜ provides a single sign-on to hundreds of public services; (2) High reach of accounts — by January 2023 Hungary had >5.5 million Client Gate (Ügyfélkapu) accounts and >6.6 million chip eID cards in circulation, giving a strong base for digital access; (3) Deep sector integrations — notably EESZT (national e-health) for records and e-prescriptions, and full online journeys for tax and administrative filings through the SZÜF/Client Gate.

Outlook:

The DÁP app is the focal point for mobile first usage and EUDI-Wallet-readiness. Roll-out priorities through 2025–2026: consolidating logins (Ügyfélkapu+ and DÁP in KAÜ), expanding digital credentials in-app, and scaling qualified e-signature to everyday use cases. Key risks are transition frictions (account migration, legacy flows) and consistent policy/process implementation for cross-border services under eIDAS 2.0.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

<div style="background:orange">Link Here</div>

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Transport	✓
Credentials	✓	Security	✓

Data as of 2025

India

2006
Introduction

~99%
User Rate

97
EGDI Rank

2,000+
Services

Aadhaar

Expert-informed primary data

Overview:

Aadhaar is a 12-digit unique identification number issued to residents of India by the Unique Identification Authority of India (UIDAI), established under the Aadhaar Act of 2016. Launched in 2009, it has become the largest biometric eID system globally, with over 1.38 billion eID numbers issued as of October 2024. Enrolment involves demographic details plus biometric data (fingerprints, iris scans, photo). The service is free on first enrolment, and authentication requests now exceed 150 billion cumulatively, including face-based verifications across public and private services.

Success Factors:

Aadhaar's impact stems from its key strengths: it enables efficient welfare delivery across 500+ government schemes, supports millions of daily digital authentications and e-KYC transactions, and offers face recognition as an alternative authentication mode. Its close integration with services ensures secure online ID verification, while ease of use and high citizen awareness drive adoption. Experts view Aadhaar as a major technical achievement, boosting financial inclusion and improving access to bank accounts and government services, especially for marginalized groups. The most impactful use case is citizens' identity authentication and verification for the digital delivery of public services, which reduces leakages and corruption in public offices.

Outlook:

Looking ahead, Aadhaar's ecosystem continues to expand. Aadhaar aims to improve infrastructure, usability, and interoperability across sectors like healthcare, education, and e-governance. Furthermore, Aadhaar aims to link with other government documents like driving licenses and adopt Face ID authentication for greater security and convenience. Ongoing challenges include data privacy and unclear ownership, which remain key concerns. Aadhaar must ensure strong privacy controls, transparency, and ease of use for all citizens.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	⧗	Finance	✓
Credentials	✓	Security	✓

Israel

2017

Introduction

~55%

User Rate

23

EGDI Rank

200+

Services

Smart ID

Systematic secondary research

Overview:

Israel's Smart ID system, introduced under the 2009 Biometric Database Law, combines physical and digital identification using biometric fingerprints and facial data. The Ministry of Interior issues all Smart IDs, which contain embedded chips for secure authentication and digital signing. The system underpins online access to e-government portals, tax systems, and certain private-sector services. Its biometric infrastructure makes Israel one of the most technologically advanced identity ecosystems in the Middle East.

Success Factors:

The Smart ID's success lies in its strong legal basis and high security. The integration of biometric identifiers - stored separately in a protected national database - minimizes identity fraud and supports automated verification. The card's digital certificates allow for certified e-signatures, enhancing usability for administrative and financial processes. Public trust is strengthened by transparent legislation, data protection protocols, and continuous modernization of issuance systems.

Outlook:

Israel is expanding digital identity use toward online renewals and mobile services. A proposed reform in 2025 aims to introduce a companion digital wallet app, allowing citizens to store and share identity data via smartphone.
The Smart ID infrastructure will also support upcoming digital travel and entry-permit systems, positioning Israel for international interoperability. Long-term priorities include improved user experience, privacy-by-design, and broader private-sector integration.

Use of Biometric Identification Documents – ID Cards and Passports. c. (2023).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2023

Italy

2016
Introduction

~89%
User Rate

51
EGDI Rank

69.4
eGovernment Benchmark

500+
Services

SPID
Expert-informed primary data

Overview:

SPID provides Italian citizens and residents with a single set of credentials to securely access a wide range of online public services, as well as many private-sector services. Once a user obtains SPID credentials from an accredited Identity Provider (such as Poste Italiane, Aruba, TIM, etc.), they can log into thousands of services - from tax declarations and social security to municipal permits - without needing separate accounts. Namirial is one of these accredited Identity Providers, contributing to SPID by issuing and managing digital identities through compliant onboarding and verification processes. SPID is recognized under the EU's eIDAS regulation, enabling cross-border access to public services in other EU countries that accept foreign eIDs. The system has handled 1.3 billion accesses annually while averaging 2.7 accesses per user each month.

Success Factors:

One of SPID's major strengths is its broad service coverage: more than 6,000 public administrations and many private entities are integrated. The multiple identity-provider model has fostered competition and convenience, as users can choose a provider based on cost, features, and ease of onboarding. Integration with the CIE (Carta d'Identità Elettronica), Italy's electronic ID card, has improved adoption and interoperability. Government-backed promotion campaigns and mandatory adoption for certain services have significantly boosted usage - by 2025, SPID had over 41.5 million active users, covering most of Italy's adult population.

Outlook:

SPID is expected to remain a central pillar of Italy's digital public services, but its role may evolve as the EU Digital Identity Wallet initiative takes shape. Italy is likely to integrate SPID into the EU-wide framework, allowing it to coexist or merge with the CIE as part of a unified wallet. Key challenges include ensuring cybersecurity resilience, maintaining user-friendly onboarding, and addressing the digital divide for less tech-savvy citizens.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Japan

2016
Introduction

~80%
User Rate

13
EGDI Rank

200-500
Services

My Number Card
Expert-informed primary data

Overview:

Japan's national digital ID, the My Number Card, is managed by the Digital Agency and used through the Mynaportal app recently available on Iphone, with Android support already in place. Besides JPKI, the most notable new feature for My Number Card on iPhone is support for selective disclosure via mdoc. Furthermore, an integration with the Google Wallet is planned for autumn 2026. Strong government promotion and free core services have driven wide adoption, resulting in about 98.81 million valid cards and a user rate of roughly 79.4%. While the system has improved convenience and trust in online services, Japan still faces challenges around sustaining usage beyond initial incentives, updating legal frameworks, supporting users with low digital literacy, and avoiding crowding out private-sector innovation.

Success Factors:

A unified government stack (My Number + Mynaportal) underpins authentication, e-signing, and access to services, reducing fragmentation. The most impactful use case is one-stop online administrative procedures, allowing citizens to obtain certificates, submit notifications, and file taxes entirely online via eID. Key success factors include a scalable trust framework with strong governance, active private sector engagement, and alignment with international standards for interoperability. Transparent data practices and user control foster trust, while ongoing UI/UX enhancements deliver intuitive, future-ready experiences.

Outlook:

Japan is now expanding real-world use across government and private scenarios (e.g., rentals, medical check-in). As of now, the Digital Agency notes that Android phones and iPhone cannot be used as a "Myna driver's license". However, policy momentum is strong, with health, licensing and administrative services continuing to migrate to the My Number infrastructure. Ongoing EU–Japan cooperation on digital identity and trust services aims to increase interoperability with international wallets and standards.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Credentials	⧗	Security	✓

Latvia

2012
User Rate
~85%

29
EGDI Rank

84.5
eGovernment Benchmark

700+
Services

eParaksts card, eParaksts Mobile, eID card
Systematic secondary research

Overview:

Latvia has operated a national, PKI-backed eID System since 2012, centered on the personas apliecība (eID card). The card serves as both a physical identity document and a secure electronic credential, containing certificates for electronic identification and qualified electronic signatures. It is being rolled out as a mandatory ID for citizens and non-citizens from age 15, including those residing abroad. The Latvian eID can be used for travel within the EU/EEA and Switzerland, and for secure access to a wide array of public and private online services. Alongside the card, Latvia provides additional eID instruments - eParaksts card, eParaksts card+, cloud-based eParaksts, and particularly eParaksts mobile - all built on a shared state PKI and trust infrastructure. The scheme is notified under the eIDAS Regulation at a high assurance level, which ensures EU-wide legal recognition of Latvian eID and qualified electronic signatures.

Success Factors:

High uptake and active usage prove Latvia's success. In 2025, the eParaksts mobile signing service was used 2.5 million times per month, and eID card - based signatures increased yearly by 78%. Besides, integration is extensive: citizens use eID/eSignature tools for more than 700 state e-services without needing to visit offices. A legal requirement for the eID card further drives adoption.

Outlook:

Looking ahead, Latvia is positioning the eID card and related services as the backbone of a 'digital-by-default' state. Planned integration with the EU Digital Identity Wallet framework (eIDAS 2.0) will expand interoperability and usability across both public and private sectors. With already strong uptake, Latvia is well placed to expand cross-border digital identity use, promote mobile credentials and grow private-sector adoption (e.g., banking, KYC).

Use of electronic identification (eID). Eurostat. (2025, December). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Transport	⧗
Credentials	⧗	Security	✓

Data as of 2025

Lithuania

2017
Introduction

~74%
User Rate

21
EGDI Rank

85.5
eGovernment Benchmark

500+
Services

MobileID, LT-ID, Smart-ID

Systematic secondary research

Overview:

Lithuania has developed a robust electronic identification (eID) ecosystem centered around Smart-ID, the most widely used eID solution in the country. As of 2024, approximately 1.6 million Lithuanians actively use Smart-ID, which supports around 5 million active accounts across the Baltics and handles roughly 80 million monthly transactions. It is a state-approved solution that meets the High Level of Assurance requirements under Lithuanian regulations aligned with the EU's eIDAS framework. Another important solution is MobileID, used by about 25% of the population for secure electronic authentication and digital signatures.Both Smart-ID and MobileID are primarily provided by SK ID Solutions, which dominate the qualified e-signature market in Lithuania, issuing a significant portion of the over 3 million valid qualified e-signature certificates in the country by the end of 2023. Overall, 90% of all administrative procedures in Lithuania can be conducted digitally.

Success Factors:

Key success factors include strong public–private collaboration, widespread smartphone penetration, and the availability of convenient, secure, and legally recognized authentication and signature solutions. Lithuania's high citizen trust in these systems and the alignment with EU standards have enabled broad adoption and efficient use across both the private and public sectors.

Outlook:

Looking forward, Lithuania continues to focus on improving cross-border interoperability under eIDAS, expanding mobile and app-based solutions, and enhancing digital inclusion, ensuring that both citizens and residents can securely access online services and perform legally binding electronic transactions.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Credentials	✓	Finance	✓

Data as of 2025

Luxembourg

2014

Introduction

~75%

User Rate

45

EGDI Rank

89.4

eGovernment Benchmark

Unknown

Services

LuxTrust & GouvID

Expert-informed primary data

Overview:

LuxTrust is Luxembourg's national digital identity and trust services provider, operating under EU eIDAS regulation. It issues secure digital identities for individuals, businesses, and government agencies, enabling strong authentication, qualified electronic signatures, and encryption. It is closely integrated with the country's electronic ID card and serves as the main authentication method for MyGuichet.lu and other public or private online services which give access to e.g. online tax filing and reception of social benefits. LuxTrust credentials can be used both domestically and across EU borders for services that accept eIDAS-compliant logins. However, Luxembourgers can also decide to use the eID with their Luxembourg ID card (GouvID). This option is only possible for citizens of Luxembourg.

Success Factors:

LuxTrust's success stems from several factors. Being government-backed and officially recognized for public services has built strong trust among citizens and businesses. eIDAS compliance ensures cross-border recognition, which is particularly relevant for Luxembourg's highly international and cross-border economy. Integration with banking and finance has made LuxTrust part of daily life for many residents, while offering multiple authentication options—such as token, smart card, and the LuxTrust Mobile app—has helped address different user preferences. It is known for its comprehensiveness. High security standards, including qualified electronic signatures and two-factor authentication, reinforce its credibility. The fact that it originated as a joint venture between the state, banks, and the Chamber of Commerce means it benefits from broad institutional support.

Outlook:

LuxTrust's role is expected to transition to the EU Digital Identity Wallet which is currently being piloted to allow citizens to store their ID, driving license, and use for electronic document signing. Key impediments are legal delays in recognising digital credentials and the complexity of the transition into the wallet.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓		

Mexico

2025
Introduction

~7%
User Rate

65
EGDI Rank

200+
Services

CURP/Llave MX

Systematic secondary research

Overview:

Mexico's Unique Population Registry Code (CURP), introduced in 1996, has long functioned as a universal identification number, not as a physical or digital ID. It is required for passports, tax filings, school enrolment, and company registration. In late 2025, there were already more than 8.8 million registered users. Mexico began transforming CURP into a biometric-enabled electronic ID under the brand Llave MX, integrating fingerprints, iris scans, facial photos, and a QR code. This marks the shift from a static identifier to a full digital credential. The rollout is proceeding in phases, with nationwide coverage expected by February 2026.

Success Factors:

Mexico's legal framework, particularly in privacy and transparency, offers a strong base for digital identity innovation. CURP's near-universal use across public administration, banking, and education reduces adoption barriers for Llave MX. A UNESCO–Mexico readiness report even identifies the country as well positioned to lead in AI and digital identity in the region. By embedding biometrics into an already familiar system, Mexico can scale innovation while ensuring continuity and public trust.

Outlook:

The government's focus is on completing the nationwide rollout of Llave MX and establishing the Unified Identity Platform. This will allow real-time identity verification across government and private services, while institutions will be required to adopt Llave MX authentication. Expansion into finance, healthcare, education, and telecommunications is planned, creating a comprehensive digital ecosystem. By 2026, Mexico expects MX Llave to function as the country's official electronic ID and as the backbone of a secure, interoperable Digital Public Infrastructure (DPI).

México Presidencia de la República - 1er Informe de Gobierno(2024-2025).
Last access: 02.03.2026; PwC analysis

`Link Here`

(EUDI Wallet Functions)		Administration	✓
Identity	⏳	Healthcare	✓
Signature	⏳	Finance	✓
Credentials	⏳	Security	✓

Data as of 2025

Nepal

2021

Introduction

~5%

User Rate

119

EGDI Rank

25+

Services

Nagarik

Systematic secondary research

Overview:

The Nagarik App (Citizen App) is Nepal's unified digital platform launched in 2021 by the government to streamline access to public services. Hosted by the National Information Technology Center, it offers around 25–62 services, including police clearance, voter registration, PAN number processing, passport services, driving license lookup, and e-chalan for traffic fines. A pivotal update in early 2025 integrated Nepal's National Identity Card (NID) into the app, enabling users to link their NID or National Identity Number (NIN) to digitally access services like passport applications, bank account opening, and SIM issuance without needing the physical card.

Success Factors:

Nagarik App's growth stems from its comprehensive service bundling under one mobile interface, which significantly reduces the need for in-person visits to government offices. It also earned notable recognition—winning the World Summit Award in 2022 for Government and Citizen Engagement. Moreover, linking the National ID to the platform facilitated streamlined identity verification and service delivery, particularly for critical services such as social security, banking, and passport issuance.

Outlook:

Nagarik App is positioned to become the cornerstone of Nepal's digital governance ecosystem. Upcoming features like "Login with Nagarik App" signal a move toward a seamless authentication system for both public and private services, akin to "Login with Google". Further digital expansion is planned to include health records, pensions, property registrations, and more. However, challenges remain, including addressing digital literacy gaps in rural areas and reinforcing data privacy safeguards.

Digital systems: The Immediate National Imperative. Nepal News. (2025).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	✓
Signature	⌛	**Finance**	✓
Credentials	⌛	**Security**	✓

Data as of 2025

Netherlands

2008/2009

Introduction

~95%

User Rate

10

EGDI Rank

81.5

eGovernment Benchmark

100+

Services

DigiD & eHerkenning

Expert-informed primary data

Overview:

The Netherlands operates two central eID systems: DigiD for individuals and eHerkenning for organizations. Both systems enable authentication for hundreds of public and semi-public services - such as those related to taxation, education, healthcare, and local government. DigiD is designed for natural persons, while eHerkenning targets businesses and public authorities. The solutions are coordinated by the Ministry of the Interior and Kingdom Relations (BZK) and comply with the eIDAS regulation at the substantial level.

Success Factors:

A key success factor is the widespread integration of both systems into government and social services - for example, for tax filings, student financial aid, health insurance, and pension applications. The systems have grown steadily over the years and enjoy broad acceptance. DigiD supports two-factor authentication, biometric login via app, and ID card scanning. The modular structure of eHerkenning allows for customizable assurance levels depending on the service. The involvement of private identity providers, combined with clear governmental oversight, supports market diversity and fosters trust.

Outlook:

The Netherlands is actively preparing for the rollout of the EUDI Wallet. There are official plans to offer verifiable digital credentials such as driver's licenses, age verification, and educational certificates. In addition, DigiD is set to evolve into a mobile identity wallet with interoperable credentials and qualified electronic signatures whereas national and cross-border government services are planned to be accessible. Integration with healthcare systems (e.g., electronic health records) will be deepened, as will use cases in banking and insurance. The Netherlands is one of the EU's pilot countries for eIDAS 2.0. However, the challenge remains to boost its adoption, as currently only credentials are available, with no practical use cases implemented yet.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	⧗	Finance	✓
Credentials	⧗	Security	✓

Norway

2004

Introduction

~97%

User Rate

15

EGDI Rank

16,000+

Services

MinID, BankID, Buypass, Commfides

Expert-informed primary data

Overview:

Norway was one of the first countries in Europe to roll out a nationwide, large-scale eID scheme, and today it ranks among the most digitalised societies globally. Norway has one of the most advanced electronic identification (eID) ecosystems in Europe, with BankID as the dominant and most trusted solution, used by over four million citizens for banking, public services, and secure digital signatures. Alongside BankID, the government provides MinID, mainly for public services, and private providers such as Buypass and Commfides serve specific business and professional needs. All these eIDs are integrated through the national authentication hub ID-Porten.

Success Factors:

The success of Norway's eID system is built on several factors: the early digitalisation of financial institutions and government services such as NAV and Skatteetaten, which enabled the early widespread adoption of use cases such as online banking; strong public–private collaboration between government, banks, and other providers; a high level of citizen trust in institutions and technology; and a robust, secure infrastructure that meets strict assurance standards. BankID and Buypass are both eIDAS-notified at the High assurance level, allowing them to be used in other European countries under the EU framework for digital identity.

Outlook:

Looking ahead, Norway's 2024 eID action plan prioritizes universal access with high security, enhanced login solutions, and harmonized digital identity use across sectors. A key objective is expanding eID availability. By early 2026, Stø (owner of BankID) will issue eIDs directly, removing the need for a Norwegian bank account and simplifying access for minors and non-citizens. Additionally, a national sandbox has been launched to test digital wallets, while collaboration with the We Build consortium ensures compliance with eIDAS standards for interoperability

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	✓
Credentials	✓	**Finance**	✓
		Security	✓

Pakistan

2012

Introduction

~97%

User Rate

136

EGDI Rank

Unknown

Services

NADRA

Systematic secondary research

Overview:

Pakistan's national electronic identity system is managed by the National Database & Registration Authority (NADRA). Since 2000, NADRA has issued the Computerized National Identity Card (CNIC)—a smart card that includes a 13-digit unique ID number, biometrics (fingerprints, iris scans, and photo), signature, and embedded chip. In 2012, it upgraded to the Smart National Identity Card (SNIC), featuring 36 security elements and compliance with international standards. As of March 2025, NADRA launched Pakistan's first dematerialised (digital) identity card, embedded within the Pak ID mobile app. This move allows citizens to store their ID digitally on smartphones, reducing reliance on physical card.

Success Factors:

NADRA serves as a centralized, autonomous authority with vast infrastructure and a strong governance mandate, enabling consistent identity coverage nationwide. Constitutional and legislative frameworks (e.g., NADRA Ordinance 2000, its 2012 amendments) provide strong legal support, ensuring continuity regardless of political shifts. Rapid CNIC issuance—covering over 120 million citizens—has laid a solid foundation. (User Rate measured against the population aged 18 and above) Inclusion of biometric and smart-card enhancements strengthens the system's credibility.

Outlook:

Looking ahead, the short-term focus (late 2025–2026) will be on piloting and scaling the digital ID system, gradually reducing reliance on physical CNICs, and expanding biometric and digital integration in public and financial services. The medium-term (2026–2028) will likely see full adoption across government, banking, healthcare, and e-commerce, along with efforts to bridge the digital divide.

Pakistan shares its progress on crvs at ministerial conference in Bangkok. Daily Times. (2025, June). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	⧗	Finance	✓
Credentials	⧗	Security	✓

Data as of 2025

Poland

2017

Introduction

~28%

User Rate

37

EGDI Rank

73.7

eGovernment Benchmark

40+

Services

mObywatel, ePUAP, mojeID, etc.

Expert-informed primary data

Overview:

mObywatel is Poland's leading national digital identity solution and the central hub of a broad, interoperable eID ecosystem. The app (version 2.0) counts over 10 million active users and more than one million daily logins, with core modules such as the electronic ID, digital driving licence and vehicle data widely adopted. In combination with the Trusted Profile (15M+ users), the ePUAP administration platform, and bank-based eID (mojeID, 22M+ users), it enables secure access to both public and private sector services nationwide. Work on mObywatel 3.0 is ongoing to ensure full eIDAS 2.0 compliance and future integration with the European Digital Identity Wallet.

Success Factors:

High everyday relevance, strong legal foundations, and user-centric design underpin rapid adoption and excellent satisfaction (ratings >4.8). Poland's unique integration of bank-based authentication — covering 98% of e-banking customers — expands trust and reach across all sectors. Full legal validity of digital documents and interoperability between mObywatel, Profil Zaufany, ePUAP, and mojeID provide convenience and consistency. Further momentum comes from active participation in Large Scale Pilots for cross-border services, particularly European driving licence and public service authentication.

Outlook:

The roadmap focuses on EU-level interoperability and continued feature expansion. mObywatel 3.0 will deliver qualified e-signatures, cross-border capabilities, an AI virtual assistant based on a Polish LLM, and a child-oriented "mJunior" version. Upcoming services include military training workflows and further growth in healthcare, education, and public safety. Remaining tasks include seamless integration of legacy systems and addressing legal, technical, and digital-skills challenges. Overall, Poland's digital identity ecosystem is mature, widely trusted, and strategically positioned for full EUDI Wallet alignment.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	⌛	Transport	✓
Credentials	✓	Security	✓

Portugal

2014

Introduction

~39%

User Rate

49

EGDI Rank

82

eGovernment Benchmark

~397

Services

ID.gov.pt

Systematic secondary research

Overview:

Portugal's national digital identity ecosystem combines the physical Cartão de Cidadão and the mobile Chave Móvel Digital (CMD). The Citizen Card, introduced as a smartcard identity document, unifies tax, social security, and health identifiers, while the CMD (since 2014) enables secure mobile authentication without a card reader. Through the ID.gov.pt app, users can store and present digital credentials such as driving licenses, health cards, and professional certificates. The system is managed by the Agência para a Modernização Administrativa (AMA) and operates in full compliance with the EU eIDAS regulation. With nearly full national coverage and interoperability across public and private services, Portugal's eID stands among Europe's most mature identity infrastructures.

Success Factors:

A decisive success factor was the user-centric design of the CMD, which relies on simple mobile PIN + OTP login and broad accessibility. The inclusion of the private sector—particularly banks, telecoms, and utilities—boosted early adoption. Integration of the SCAP (Professional Attribute Certification System) introduced qualified electronic signatures for professionals, enhancing legal value and business uptake. A clear governance framework, open APIs (Autenticacao.gov), and full eIDAS notification have strengthened trust, interoperability, and scalability.

Outlook:

Portugal is now evolving from its dual model toward a unified digital wallet ecosystem aligned with the EUDI Wallet. Planned extensions include additional credentials (military ID, vehicle insurance, education records) and offline NFC-based verification. The ID.gov.pt platform is also expanding toward private-sector applications such as e-commerce, finance, and real estate. With strong legal backing and mature interoperability, Portugal is expected to play a leading role in shaping Europe's future digital identity landscape.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2025

Saudi Arabia

2021

User Rate

~80%

User Rate

6

EGDI Rank

460+

Services

Absher

Systematic secondary research

Overview:

Absher is Saudi Arabia's central eGovernment portal, operated by the Ministry of Interior. The platform provides citizens and residents with digital access to over 460 public services—ranging from passport and traffic management to residency permits and healthcare. In recent years, a digital ID function has been integrated into Absher, allowing users to identify themselves via smartphone—for both identity checks and digital administrative services. The Absher app acts as a digital wallet for ID data and supports authentication via QR code and biometric methods.

Success Factors:

Absher was designed early on as a comprehensive eGovernment platform and has been continuously expanded. The digital ID function benefits from the country's high level of technological adoption and centralized administrative model. A key success factor is its integration with national registries, security authorities, and private service providers. The platform is mobile-accessible and multilingual, with an intuitive interface and support for biometric authentication. Absher is also embedded in national digital transformation programs such as Vision 2030.

Outlook:

Saudi Arabia plans to develop Absher into a full-fledged digital identity wallet. Further integration with international travel and visa systems is also on the agenda. Looking ahead, Absher is expected to play a central role in the Gulf area with enhanced interoperability across GCC countries. Pilot projects are also exploring the use of blockchain and self-sovereign identity technologies.

Team, I. T. E. (2024, December 26). Saudi Arabia's Absher platform reaches 28 million digital identities milestone. ID Tech. Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Credentials	✓	Finance	✓
		Security	✓

Data as of 2024

Singapore

2003

Introduction

~97%

User Rate

3

EGDI Rank

2,000+

Services

Singpass

Systematic secondary research

Overview:

Singpass is Singapore's national eID solution and serves as a central access point to over 2000 digital services from both the public sector and the private sector. The platform includes identity verification, electronic signatures, and digital credentials. It is primarily used via a mobile app that supports biometric authentication. Singpass is available to citizens, permanent residents, and foreign individuals with registered status. Fully embedded in Singapore's Smart Nation strategy, it forms the foundation for digital interaction with the government, businesses, and the healthcare system. The User Rate shown is measured only against the population aged 18 and above.

Success Factors:

The widespread adoption of Singpass is driven by strong user orientation, technical security, and everyday practicality. Early integration of private-sector providers—such as banks and insurance companies—helped establish Singpass as the standard login in daily life. The app is intuitive, secure, and offers users full control over their data. Government investments in data protection, two-factor authentication, and cross-platform compatibility have further strengthened trust. Its clear strategic positioning as a multifunctional eID solution also supports high acceptance across all age and user groups.

Outlook:

Singpass is set to evolve into a full-fledged digital wallet. Plans include integrating additional credentials such as educational qualifications, driver's licenses, and property certificates. Singapore is also working on regional interoperability within the ASEAN area to enable cross-border identity verification. The goal is to establish Singpass as an international benchmark solution—combining high security, user-friendliness, and a broad range of functions.

Factsheet – SingPass, Singapore's National Digital Identity. (2024).
Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓		

Data as of 2024

South Korea

2020

Introduction

unknown

User Rate

4

EGDI Rank

Mobile ID

Systematic secondary research

Overview:

South Korea's Mobile ID was introduced starting in 2020, initially as a digital driver's license and later as a national eID for citizens and residents. The solution is based on a government-developed app, supported by mobile network operators and KOMSCO (Korea Minting and Security Printing Corporation). It enables identification in public administration, age verification, healthcare, and increasingly in the private sector. The Mobile ID is deeply integrated into mobile devices and also supports offline use via QR code or NFC.

Success Factors:

The Mobile ID benefits from South Korea's high smartphone penetration, seamless integration into everyday services, and concrete use cases such as driver's license checks or age verification. Close cooperation between the government, private sector, and technology providers enabled rapid market adoption. The app is user-friendly, secure, and supports biometric authentication. Its visibility in everyday life reinforces acceptance and usage—even among less tech-savvy users.

Outlook:

South Korea plans to expand the Mobile ID into a comprehensive digital wallet. In the future, it will include additional state-verified credentials such as educational degrees, professional certificates, or vaccination records. International connectivity—e.g., for digital travel or contract services—is to be improved through standardization and bilateral agreements. Looking ahead, South Korea is also exploring decentralized identity models (SSI) to strengthen user control and data portability.

South Korea Korean Culture and Information Service (KOCIS). (2025, March 14). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Security	✓

Data as of 2025

Spain

2016/2025
Introduction

~59%
User Rate

17
EGDI Rank

78.7
eGovernment Benchmark

4,600+
Services

MiDNI/ Mi Carpeta Ciudadana
Systematic secondary research

Overview:

Spain's eID system is built around two complementary apps: MiDNI and Mi Carpeta Ciudadana. The MiDNI app, introduced in April 2025, provides citizens with a secure digital version of their national ID card, allowing them to identify themselves safely at banks, hotels, pharmacies, and public offices through QR-based verification. Users can choose which personal data to share, ensuring privacy and control. Mi Carpeta Ciudadana, launched earlier, acts as a central access point for public administration, displaying documents, notifications, and appointments from national and regional services. Both rely on the Cl@ve login system and support electronic signatures via Cl@ve Firma, combining convenience with strong security.

Success Factors:

Spain's eID system succeeds thanks to high user trust, broad service coverage, and strong design consistency. More than 90 % of municipalities and nearly all regions are integrated into Mi Carpeta Ciudadana, giving citizens access to a wide range of administrative functions in a single interface. By mid-2025, the platform reached more than five million users, reflecting strong national adoption. The system's success also stems from its alignment with the trusted DNI identity infrastructure and from simple, seamless authentication flows via Cl@ve.

Outlook:

In the next stage, MiDNI will evolve beyond physical verification toward online authentication and qualified e-signatures. This development will align with the EUDI Wallet under the revised eIDAS 2.0 framework. Spain aims to merge identification, credentials, and signing into a single, secure digital experience for both public and private use.

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Transport	✓
Credentials	✓	Security	✓

Data as of 2025

Sweden

2003
Introduction

~92%
User Rate

14
EGDI Rank

77.6
eGovernment Benchmark

6,000+
Services

BankID & Freja eID
Systematic secondary research

Overview:

BankID is Sweden's central digital identity solution. It is entirely operated by private banks, yet state-recognized and widely accepted. It serves as the de facto eID for online identification across government services, healthcare, banking, insurance, telecommunications, and e-commerce. More than 8 million Swedes use BankID—primarily via a mobile app, secured through biometric authentication or PIN. There are multiple variants, including Mobile BankID, BankID on file, and BankID on card. A government alternative (e-legitimation från Skatteverket) has been announced but currently plays a minor role.

Success Factors:

BankID's success stems from its integration into the population's everyday payment and communication channels. Users rely on it for virtually all digital interactions—from tax declarations to booking medical appointments. The system is highly available, easy to use, and deeply embedded in the banking ecosystem. Public authorities accept BankID as a secure means of authentication without the need to develop their own separate solution. The system's success is built on a combination of market penetration, trust in the banking sector, and simple mobile usability.

Outlook:

Although BankID is not a government-issued solution, it is considered eIDAS-compliant at the substantial level. A qualified electronic signature is not currently integrated but is being discussed in the context of the EUDI Wallet. Additionally, the Swedish government is preparing to launch a complementary public eID to gain more control over sovereign credentials in the long term. While there are no official announcements yet regarding the addition of structured digital credentials (e.g., professional licenses, age verification), such features are technically feasible and could be introduced with appropriate regulatory support.

Use of electronic identification (eID). Eurostat. (2025, December).
Last access: 02.03.2026; PwC analysis

`Link Here`

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
		Finance	✓
		Security	✓

Data as of 2025

Switzerland

2026

Introduction

Not yet published

User Rate

26

EGDI Rank

50-100

Services

eID swiyu

Expert-informed primary data

Overview:

Swiyu is the Swiss Confederation's official digital wallet for the national electronic identity (eID) and is currently available in a public beta phase. The eID itself is defined in the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (BGEID) and constitutes an official proof of identity issued by the state. It is voluntary, free of charge and can be ordered – at the earliest from summer 2026 directly in the Swiyu app using a valid Swiss ID card or residence permit. Citizens will be able to obtain verifiable credentials and use them across government portals, tax administration, and pilot projects such as mobile driver's licenses, with expansion into finance and healthcare to follow.

Success Factors:

The Swiss eID project's greatest achievement has been regaining public trust after the 2021 referendum defeat. Switzerland's Swiyu wallet benefits from a state-run trust infrastructure, addressing past concerns by placing issuance and operation under federal control. It is built as a multi-purpose credential wallet, planned to support the eID, driving licences, residence certificates and membership cards. Privacy is preserved via data-minimisation and user-controlled disclosures, with decentralised storage and open-source components ensuring transparency and trust.

Outlook:

The Swiss eID is built on international standards (OIDC4VCI, SD-JWT) and is designed for interoperability with the EU's EUDI Wallet despite Switzerland being outside the EU. Early rollout will likely cover a limited set of government services, but adoption could grow rapidly as private-sector players join. By 2026–2028, Switzerland aims to expand into finance, healthcare, and mobility, making its eID a trusted, scalable system aligned with European best practice. However, due to the troubling history of digital identity usage in Switzerland, risks such as cybersecurity threats, privacy concerns, public trust issues, a fragmented identity management landscape remain affecting interoperability and scalability, and inconsistent legal standards remain.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Healthcare**	✓
Signature	✓	**Finance**	✓
Credentials	✓	**Security**	✓

Türkiye

2017

User Rate

~78%

Introduction

27

EGDI Rank

9,000+

Services

e-Devlet

Systematic secondary research

Overview:

Türkiye's e-Devlet eID, based on the 2017 electronic ID card rollout, is the backbone of the country's eID System. Integrated into the e-Devlet Gateway, it enables secure access to thousands of services across all sectors. With flexible login methods—ID card, password, mobile/digital signatures, or banking credentials—it provides both strong authentication and mass accessibility. With more than 68 million active users and more than 9,000 services, it has become one of the most adopted digital ID systems worldwide.

Success Factors:

The e-Devlet eID's success comes from combining secure technology (chip-based eID + qualified e-signature) with broad practical coverage (tax, healthcare, judiciary, education). The 2017 introduction of the national eID card was critical, providing citizens with a tangible, trusted credential. Legal recognition of e-signatures and multiple login pathways made the system inclusive, while the huge service portfolio turned e-Devlet into a daily necessity. The strong link between national ID infrastructure and the e-Devlet platform ensured consistency and reliability, encouraging citizens to adopt the system en masse.

Outlook:

While Türkiye is outside the EU, the e-Devlet eID already aligns with eIDAS principles: high-assurance authentication, qualified signatures, and credential access. Future evolution could include a wallet-style model that allows selective data sharing and improves interoperability with EU and regional partners. With near-universal penetration and functional maturity, e-Devlet eID is positioned to remain one of the most comprehensive national eID systems globally. In the medium term, Türkiye may leverage e-Devlet to build regional bridges for secure digital trade, mobility, and cross-border services.

e-Devlet Kapısı Kullanıcı İstatistikleri. Türkiye.com.tr. (2026, January 31). Last accessed: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2026

Ukraine

2020

Introduction

~58%

User Rate

30

EGDI Rank

130+

Services

Diia

Systematic secondary research

Overview:

Launched in 2020, Diia is Ukraine's "state in a smartphone" - a combined digital identity and services platform. It offers digital ID, passports, driver's licenses, and access to in-app services and over 130 portal services. With more than 24 million users, Diia already covers all core functions of a European eID: identification, digital credentials, and electronic signature (Diia.Signature), legally equivalent to handwritten signatures in Ukraine.

Success Factors:

Diia's success rests on its super-app design that unifies identification, credentials, and signatures under one interface. By making digital documents legally equivalent to physical ones in 2021, the government-built trust and accelerated adoption. Its personal, business, education, mobility, and social services ensured value for diverse users, while the quick-to-activate Diia.Signature strengthened utility. During the COVID-19 pandemic it even offered vaccination registration. Due to its user centric design and functionality, it has won the Red Dot Design Award in 2021. Since Russia's 2022 invasion, the app has become essential for many Ukrainians. With traditional government services often inaccessible, Diia allows users to manage civil registration, social benefits and permitting processes online. It also includes wartime functions such as compensation requests, veteran support, air-raid alerts, and reporting Russian troop movements. These factors drove adoption to over 50% of the population in just a few years, making Diia one of the world's most comprehensive eID ecosystems.

Outlook:

Looking ahead, Diia is positioned as a strong candidate for EUDI-Wallet interoperability. It already unites identification, signatures, and credentials within one system, while offering advanced features like in-app payments and wartime support. For EU alignment, the next steps will be recognition of Diia.Signature at Qualified Electronic Signature (QES) level, ensuring mutual cross-border acceptance, and expanding private-sector uses. With its wartime innovations and massive adoption, Diia illustrates how digital identity can evolve beyond administration into a pillar of national resilience.

Diia Reaches 23 Million Users: Ukraine's Digital Government Becomes the New Normal. Digital State UA. (2025, October 15). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2025

United Arab Emirates

2018

Introduction

~95%

User Rate

11

EGDI Rank

1,000+

Services

UAE Pass

Systematic secondary research

Overview:

UAE Pass is the official digital identity solution of the United Arab Emirates and serves as a unified access point to thousands of digital services across both the public and private sectors. The platform enables both identity verification and electronic signatures, and its app includes additional wallet functions— such as storing official documents. UAE Pass is jointly operated by the Telecommunications and Digital Government Regulatory Authority (TDRA), the Emirates Identity Authority, and local government entities. It is available to all citizens, residents, and registered businesses. By mid-2025, there were more than 11 million users registered.

Success Factors:

A key success factor is the complete integration of identity, signature, and credentials into a single mobile application. UAE Pass enables login to services provided by government agencies, banks, telecom operators, real estate platforms, and healthcare providers. Identity verification is conducted via NFC-based ID scanning, biometric matching, and device binding. The UAE's high level of digitalisation and strong central coordination have significantly accelerated adoption. The app is multilingual (including Arabic and English) and available across platforms.

Outlook:

The UAE plans to further expand UAE Pass into a full-featured digital wallet with cross-border usability, for example in travel, education, and commerce. The integration of additional verifiable credentials—such as driver's licenses, business licenses, and educational certificates—is planned. Broader use in the private sector (e.g., banks, insurance, employment contracts) is also under development. UAE Pass is a central pillar of the long-term Vision 2031, which aims to unify digital services and enhance international interoperability.
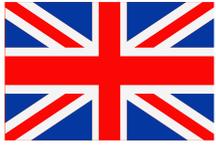
A National Forum Bringing Together Federal, Local, and Private Entities to Celebrate the UAE's Digital Achievements and Unveil a New Initiative. Gitital Dubai. (2025, September 13). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2025

United Kingdom

2023

Introduction

~19%

User Rate

7

EGDI Rank

80+

Services

One Login

Systematic secondary research

Overview:

"One Login for Government" is the United Kingdom's central digital identity project. It is being developed by the Government Digital Service (GDS) and is intended to eventually replace all existing access systems to public services—such as GOV.UK Verify and Government Gateway. The goal is to provide a unified, secure, and user-friendly login solution for all online services offered by the UK government. Since 2023, One Login has been gradually rolled out to selected government departments, including those responsible for tax, pensions, and visa services.

Success Factors:

Following the failure of earlier initiatives such as GOV.UK Verify, One Login was redesigned from the ground up with a focus on scalability, data protection, and user experience. Key to its success has been close coordination with government agencies and end users, along with the integration of biometric authentication, smartphone-based identity verification, and manual ID checks. Trust has been strengthened through transparent processes, cooperation with data protection authorities, and flexible login options. The platform is optimized for mobile use and accessibility.

Outlook:

The UK government plans to develop One Login into a full-fledged digital identity wallet. The integration of verified digital credentials—such as driver's licenses, educational qualifications, or visa information—is planned. In the medium term, the platform is intended to be available across all central government departments and may potentially be opened to the private sector. The legal framework is being shaped in parallel through the Digital Identity and Attributes Trust Framework. Future interoperability with international systems is under political discussion but has not yet been formally decided.

Verifying your identity for Companies House with GOV.UK One Login. Gov.UK. (2025, November 19). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	**Finance**	✓
Credentials	⏳	**Security**	✓

Data as of 2025

Uruguay

2019

Introduction

~50%

User Rate

25

EGDI Rank

1,500+

Services

ID Uruguay

Systematic secondary research

Overview:

ID Uruguay, launched in 2019, is the country's official digital identity platform. It operates as a federated identity broker, enabling citizens to log in securely to government and private-sector services. Integrated with Uruguay's national eID card and the state signature system (Firma.gub.uy), it has become the digital entry point for more than 190 services and 1,500 procedures, supporting around 90,000 daily authentications.

Success Factors:

ID Uruguay's success is built on centralization and trust: a mandatory eID card ensures universal coverage, while a robust legal framework for digital signatures and data protection provides confidence in security. Its interoperability-first architecture makes it easy to extend services across sectors, while integration with Firma.gub.uy delivers seamless electronic signing. Uniquely, it already combines identification, electronic signatures, and digital credentials in one system, making Uruguay not only a Latin American leader but also one of the most complete and advanced eID models worldwide.

Outlook:

Looking ahead, Uruguay is well positioned to serve as a regional and global reference case in digital identity. With identification, credentials, and signatures already unified, the next steps include adopting verifiable credential standards and strengthening cross-border interoperability. Early pilots with Brazil point toward a regional digital identity ecosystem, and further alignment with EUDI Wallet standards would open the door for seamless interaction with the EU. Expanding adoption in the private sector, particularly finance and commerce, and ensuring robust cybersecurity governance, will be key to deepening ID Uruguay's role as the foundation of a trusted digital economy.

Uruguay (AGESIC) - Digital ID and digital signature. Public Digital. (2023, November 29). Last access: 02.03.2026; PwC analysis

Link Here

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Data as of 2023

Vietnam

2021

Introduction

~63%

User Rate

71

EGDI Rank

100+

Services

VNeID

Expert-informed primary data

Overview:

VNeID is Vietnam's official digital ID platform, launched in 2021 and mandatory for online public services. It offers two account levels: basic and biometric-verified for full access to secure services. Users can store IDs and documents and access services like tax filing, health records, and digital contracts. By May 2025, it had over 62 million accounts, around 63% of the population.

Success Factors:

Vietnam's VNeID system has achieved remarkable scale and integration within four years of launch. By May 2025, it processed 2.1+ billion transactions and generating VND 469 billion (~USD 18.5 million) in administrative cost savings. The platform successfully integrated 80% of public services online, digitized six major document categories (ID cards, passports, driving licenses, vehicle registrations, health insurance, social insurance), and connected 13 commercial banks for biometric authentication of 56.8 million banking customers, significantly reducing fraud. Vietnam has also emerged as a regional leader, assisting Laos in developing their national digital ID system and positioning itself at the forefront of mobile identity adoption in Southeast Asia.

Outlook:

VNeID is set to evolve into a full-scale "super app" for citizenship, expanding its role beyond government services to include broader financial, health, and administrative functions. Planned developments include interoperability with more private-sector systems, the onboarding of foreign residents from July 2025, and further security enhancements to protect biometric and personal data. Key challenges include fragmented technical infrastructure, limited digital literacy, accessibility barriers for rural and minority populations, and ongoing privacy and security concerns.

(EUDI Wallet Functions)		Administration	✓
Identity	✓	Healthcare	✓
Signature	✓	Finance	✓
Credentials	✓	Security	✓

Authors

Your points of contact for further questions about this study

Martina Knierim
Partner
Public & Energy Consulting
martina.knierim@pwc.com

Malien Zehnpfenning
Senior Associate
Strategy&
malien.zehnpfenning@pwc.com

About us

Our clients face a wide range of challenges, want to implement new ideas, and seek our advice. They expect us to support them holistically and develop practical solutions that deliver maximum benefit. That's why, for every client—whether a global player, family-owned business, or public-sector organization—we draw on our entire potential: experience, industry expertise, specialized knowledge, commitment to quality, innovative strength, and the resources of our network of experts in 151 countries.

Building relationships based on trust with our clients is especially important to us, because the better we know and understand them, the more effectively we can support them.

Additional Experts on Digital Identity

Dr. Nicolai Bieber
Partner
Public & Energy Consulting
bieber.nicolai@pwc.com

Lucas Sy
Partner
Strategy&
lucas.sy@pwc.com

Robert Eickmeyer
Partner
Financial Services
robert.eickmeyer@pwc.com

Authors

**Further
Contributors and
Subject Matter Experts**

Johannes Jahnke
Senior Manager
Financial Services
johannes.jahnke@pwc.com

Dr. Lukas David Hoffmann
Manager
Strategy&
lukas.david.hoffmann@pwc.com

Johanna Möller
Associate
Public & Energy Consulting
johanna.moeller@pwc.com

Mika Pohl
Associate
Public & Energy Consulting
mika.pohl@pwc.com

Colin Abele
Intern/Trainee
Public & Energy Consulting
colin.abele@pwc.com

Konstantin Monath
Intern/Trainee
Public & Energy Consulting

Szabolcs Ugrai
Intern/Trainee
Public & Energy Consulting

Naemi Stephansson
Intern/Trainee
Strategy&
naemi.stephansson@pwc.com