VISA

Digital Identity

What to know and how to prepare

November 2024









Effective digital identity schemes and their adoption are key for the digitalisation of private and public services

Today, digital interactions and transactions permeate every facet of our lives. Paying for goods, interacting with government services, or accessing digital content are just some of the ways we engage online.

For any of these services to function effectively, they need to register and recognise us as individuals. Yet physical verifications and means of identification aren't suited to the online world. And, to date, most of the equivalents have been found wanting.

The share of digital over traditional face-to-face interactions is only expected to increase. Effectively, almost every sector is directing significant investment and effort into the digitalisation of services, while consumers increasingly demand end-to-end experiences. With the rapid evolution and adoption of Artificial Intelligence (AI), the Internet of Things (IoT), and machine-to-machine systems, the digitalisation of more products and services seems inevitable.

In a landscape where digital transactions are the norm, a robust set of digital identity frameworks and verification systems is essential. It is needed to maintain security, trust and privacy, while offering a frictionless user experience. Arguably, their availability will become the foundation for all future online transactions, communications, and services.

Reflecting the importance, several jurisdictions across the world have introduced regulations to specify when a user must be identified and at what level of assurance.

Typically covered in Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, new technological solutions and common standards are being developed to reduce the risk of identifying or authenticating an individual incorrectly.

Financial services and retail businesses are set to be two of the most impacted sectors, as the adoption of digital identity standards and technologies has the clear potential of notably reducing friction throughout the digital banking and payments journey. This transforms the effective integration of eIDs into a value play for banks and merchants alike.

Besides the more obvious security, operational and compliance benefits, eIDs are also expected to be a catalyst for a streamlined customer experience, increased engagement and positively impact overall profitability and retention.

In this paper, we provide a high-level introduction to digital identity frameworks, discuss the current landscape, and provide key concepts for financial institutions and businesses in the payment ecosystem to prepare for the upcoming changes.

© 2024 Visa. All Rights Reserved

Contents



Understanding digital identity (eID)

- A classification of digital identity systems 5
- Summary of eID attributes 6
- Introduction to the digital identity value chain 7
- Digital identity trust frameworks 10

eIDs will unlock value across verticals

- Financial services and payments set to benefit from eIDs 13
- Key benefits of eIDs for financial institutions 15

Europe is uniquely positioned to set the pace for eIDs

- Main eID schemes in Europe 16
- Regulatory initiatives to drive European eID expansion 17

What Visa is doing to accelerate eID development and adoption

- Introducing our strategy to accelerate eID 19
- Active participation in major industry initiatives in Europe 20
- Visa assets to benefit the ecosystem 22

How financial institutions and merchants can prepare and benefit

- Six key strategic considerations 26
- Visa can help with eID planning and implementation 30
- About Visa Consulting & Analytics 30

Disclaimer: All brand names, logos and/or trademarks featured in this paper are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

© 2024 Visa. All Rights Reserved.

Understanding digital identity (eID)

Digital identity – commonly referred to as eID – is a rapidly evolving concept which doesn't have a consistent definition across sources and publications.

At Visa, we define an eID as a digital representation of an individual or organisation, comprised of a collection of identifying attributes that can be authenticated with a certain level of assurance, via digital channels.

We see eIDs emerging as a set of technologies that enable interactions between individuals and institutions, providing a robust foundation for a wide range of digital applications. When implemented at scale across multiple use cases, eIDs have the potential to generate substantial economic value for both individuals and institutions – and reduce friction in the digital economy. In the most formal definition, eIDs are exclusively issued by governments, generally created from an official identity document (such as a passport or ID-card), and serve as a legal form of identification for multiple purposes.

Government entities may also manage an array of functional ID systems to enable the verification of identities for specific verticals or use cases.[1]

A wider definition of the term may include eIDs that are issued and managed by private entities (like application providers and platforms) or industry consortia (typically formed by banks or telecommunication companies). These are typically endorsed by governments through trust frameworks, which are legislations that give legal equivalence to the eID and stipulate the conditions under which they can be trusted.



The four main purposes of eIDs[2]

01 Identify
An individual, organisation, or machine during a digital interaction.

02 Authenticate
That someone is who they claim to be.

03 Authorise
A digital interaction or transaction the identified user is eligible for.

04 Sign and seal
Electronic documents with a timestamp to prevent tampering.

1. The World Bank, ID4D Practitioner's Guide, Types of ID Systems, 2019: https://id4d.worldbank.org/guide/types-id-systems
2. The World Bank, ID4D Practitioner's Guide, ID101: Basic Concepts, 2019: https://id4d.worldbank.org/guide/id-101-basic-concepts-0

© 2024 Visa. All Rights Reserved

A classification of digital identity systems

Although the definition and classification of eIDs lacks standardisation, a useful way of thinking about them is to consider who issued them and how broad the scope of application is.

Issued by	Foundational Reusable and general purpose	Functional IDs Vertical/specific purpose
Government entities	National ID Civil registration Population registration	Voter registration Tax ID Social security number Driver's licence
Private entities (incl. consortia)	Bank ID Telco ID	BigTech user profile Patient ID Student ID



An eID can be issued by government or private entities, and the broadness of its scope can be either for general use (foundational IDs) or specific purposes (functional IDs).

According to The World Bank's definition, an ID system can be regarded as foundational if it enables an individual to establish their identity using legally recognised credentials. These primarily encompass civil registers, national IDs, and population registers, enabling the identification of citizens across a broad range of applications.[3]

In addition, governments, private organisations and consortia often issue IDs for specific sectors and use cases. These are not generally considered as legally recognised credentials outside of their intended use cases. However, in some instances, they have been adopted more widely – in the United States, for example, social security numbers and driver's licenses are functional IDs but also serve as valid forms of general-purpose identification.[4]

eIDs can be issued as single-use or reusable credentials, with the latter being the industry's focus due to the versatility across multiple use cases and the capacity for repeated use.

3. The World Bank, ID4D Practitioner's Guide, Types of ID Systems, 2019: https://id4d.worldbank.org/guide/types-id-systems
4. *ibid.*

© 2024 Visa. All Rights Reserved

Summary of eID attributes

An eID contains a set of distinct data elements that, either independently or collectively, can be verified with a certain degree of assurance.



These elements are known as eID attributes and can take multiple forms[5] – from biographic and biometric features to knowledge and online-based data that is defined by the individual themselves.

Attributes are the basis for identifying an individual unequivocally (deterministic) – or tied together to form a likelihood that someone is who they say they are (probabilistic).[6]

The selective disclosure of attributes is gaining ground due to shifting market demands.

The focus used to be on eID use and provisioning, where users show their identification in its entirety. However, demand is now moving towards the provisioning of specific attributes related to those identities. The ability of eIDs to break down national identifications into distinct attributes allows for increased flexibility and security.

While the issuance and acceptance of such attributes require the person to be identified, it is the attribute and the fulfilment of its requirements what provides access to specific services. eID systems will need to enable an effective link with attributes in order to address future demands.

A. Identify

Biographic data
Descriptive information about the individual. For example, birthplace, nationality, sex, etc.

Biometric data
Biological or physical characteristics of an individual. These include, fingerprints, iris scans, face recognition, voice recognition, etc.

Online-based data
Online behaviour or activities of an individual collected through online tracking technologies. For instance, browsing history or IP addresses.

B. Access, authorise, or sign

Knowledge-based data
Information known or remembered by the individual. These include, passwords, security questions, etc.

Cryptographic data
Data transformed into a secure format, that is unreadable without the necessary decryption key or cipher. For example, Passkeys, tokens, public key cryptography, etc.

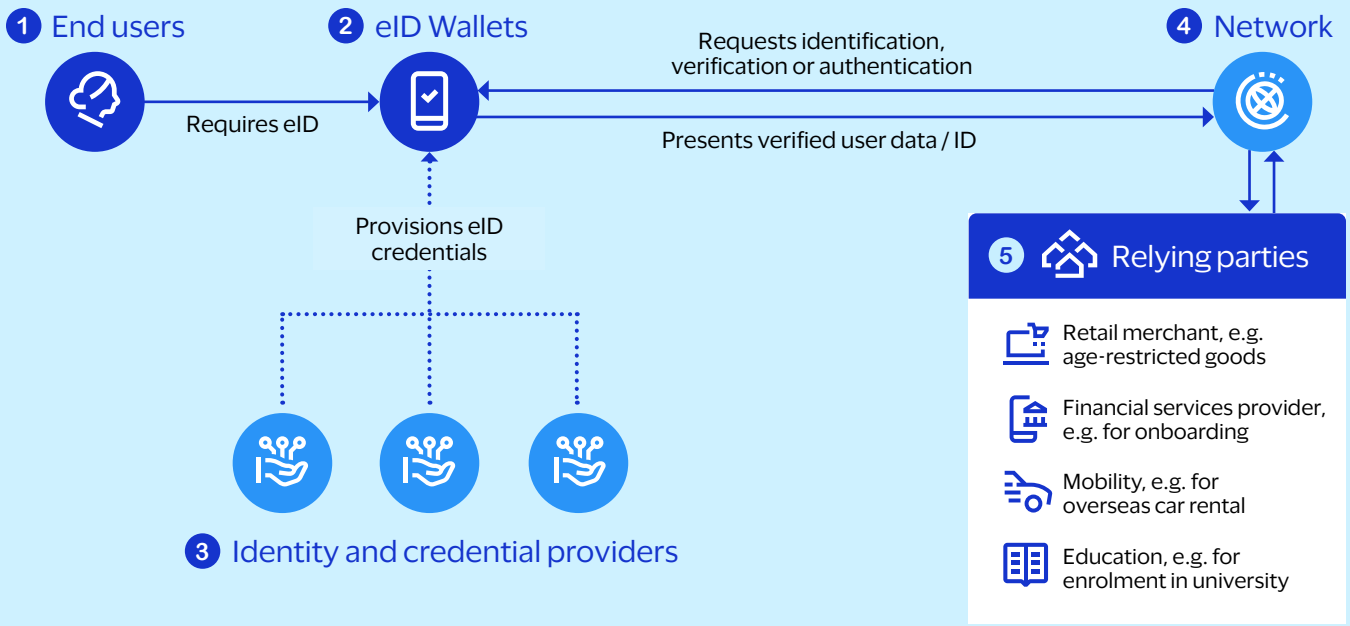
5. Juniper, Digital Identity, page 7
6. eMarketer, Guide to ad measurement and identity resolution for marketers, 2024: https://www.emarketer.com/insights/guide-ad-measurement-id-resolution/

© 2024 Visa. All Rights Reserved

Introduction to the digital identity value chain

Effective eID networks have similar dynamics to payment schemes, with a market structure which is analogous with the cards' four-party model.

eID players and dynamics



ENABLED BY Regulatory Entities | Standards & Trust Framework | eID Consortia | Security & Privacy Services

Simplified value chain scheme

KEY ·····→ Only for wallet-based decentralised eID schemes ● Network and providers are optional



© 2024 Visa. All Rights Reserved

eID players and dynamics

End users

Are individuals, entities, or technologies (servers, IoT devices, smartphones, etc.) that use an eID to prove attributes and access products or services.

Use cases may include accessing government services, validating online transactions, or verifying one's identity during online onboarding. Typically, end users look for a seamless experience and user-friendly digital journey, transparency regarding data usage, and a robust privacy protection.[7]

Relying parties

Are entities, such as government bodies or private companies, that request end users to provide digital identification in instances where they require access to specific goods or services.

Their incentives to adopt eIDs include mitigating fraud, complying with Know Your Customer (KYC) regulations, increasing conversion rates, enhancing the user experience by reducing friction, and reducing operating expenses.

Networks

Act as brokers, enabling extensive coverage of eIDs. They provide a single interface to connect wallets, identity providers, and relying parties

They also establish a framework – with rules and policies – to ensure trust, predictability, reliability, and scalability. The requirement for networks is dependent on the functional design of the eID scheme.

Identity providers

Include government agencies, private companies, and global organisations that are authorised by governments or relevant trust frameworks to issue and manage eIDs.

Their key responsibilities are to create reliable digital identities, store ID data securely, and provide dependable eID services. Vendor and technology neutrality are of paramount importance for these players, to enable compatibility and increase reach among end users, wallets, and relying parties.[8]

Enablers

Facilitate the proper functioning of the ecosystem through either its development, standards definition, regulation, or privacy services.

Depending on the nature of the eID, the role of enablers may differ (for example, identity providers and standard-setting committees can be the same for some functional eIDs). At Visa, we regard the three key enablers as:

- **Trust frameworks**
  Ensure effective interaction between players and interoperability among schemes.
- **Standard setters**
  Establish industry and/or regulatory guidelines.
- **Privacy services**
  Safeguard user data.

7. The World Bank, ID4D Practitioner's Guide, Stakeholders and roles, 2019: https://id4d.worldbank.org/guide/stakeholders-and-roles
8. *ibid.*



© 2024 Visa. All Rights Reserved

A day in the life with eID

Marta has an eID wallet with her credentials provisioned on it. This scenario showcases the convenience and efficiency of using a digital identity in everyday life, streamlining processes and ensuring security.



Taking a taxi

Marta hails a taxi to take her to work. When she arrives at her destination, she decides to pay with her eID wallet.

The taxi sends an authorisation request through its payment service provider, for the amount of the ride.

Through her eID wallet, Marta authenticates and confirms the payment.

Entering the office

When she gets to the office entrance, the security guard asks Marta for identification.

From her eID wallet, she selects her work credential. She shows the guard her phone screen displaying only her name, picture, and work credential, safeguarding the rest of her data.

Opening a bank account

Marta decides to open an account at a new bank, recognised for its focus on digital user experience.[9]

She loads the bank's app on her phone, chooses her eID wallet to register and uses biometrics to unlock the eID wallet.

Marta reviews the attributes the bank would like to access, with both required and optional data, and completes any missing fields.

She reviews the information and confirms the terms and conditions. To complete the process, she signs the agreement using the electronic signature capability of her eID wallet.

Filing a tax return

Marta opens the government's tax filing portal, she sees her eID wallet as a method of identification and provisioning documents, so she chooses this option.

She is redirected to her eID wallet and unlocks it with biometrics.

The wallet receives a request to access certain attributes: income statements, deductible expenses stored, and personal identifiable information (PII).

She is prompted to complete any additional information required. After reviewing the calculated tax form and confirming the information, she signs the tax report with the eID wallet.

Going to the movies

When purchasing her ticket, she is asked for an ID to verify she is over 18.

She opens her eID wallet and chooses the age attribute to be verified using zero-knowledge proof, proving she is over 18 without revealing her exact age.

She shows her verified attribute with an 'Over 18' message and is able to procced with her purchase.

Note: Illustrative examples.
Actual implementation and user journeys will vary among markets and eID schemes

9. The Paypers, What is the impact of EU digital ID wallets on banks and financial institutions?, 2022: https://thepaypers.com/thought-leader-insights/what-is-the impact-of-eu-digital-id-wallets-on-banks-and-financial-institutions--1255579

© 2024 Visa. All Rights Reserved

Digital identity trust frameworks

There are several eID trust frameworks, but three schemes stand out as the most relevant: Centralised, Federated and Decentralised.

Centralised | Federated | Decentralised



These models are not new.

They are deeply embedded in our daily routines, ranging from the existing federated login credentials issued by the likes of Google and Apple that already enable end users to access services from various relying parties, to the digital wallets that are widely used in the payments ecosystem.

However, the introduction of a standardised eID, through regulation or simply wide adoption, provides these existing models with **an additional layer of security and verification**, thereby enhancing trust and convenience.

Centralised eID schemes

A single entity is responsible for the entire eID lifecycle, providing the end-to-end solution, and controlling the creation, issuance, use, and management of the user journey. This model is secure and reliable, but faces challenges in terms of privacy, surveillance, scalability, and flexibility.

Federated eID schemes

Network effects are leveraged, enabling end users to choose among multiple providers to issue their eID credentials and provides them with the flexibility to reuse them across different relying parties. This model relies on trust and coordination among identity providers, but brings many efficiencies through interoperability. Federated schemes are typically implemented by bank or telecommunications consortia.

Decentralised eID schemes

End users have full control over their data. Their eID credentials are stored in a wallet that they manage and credentials are provisioned through APIs connected to identity providers. This model allows end users to fully own and manage how and with whom they disclose their identity. In some schemes, they may even be able to create composite wallets with additional attributes.

© 2024 Visa. All Rights Reserved

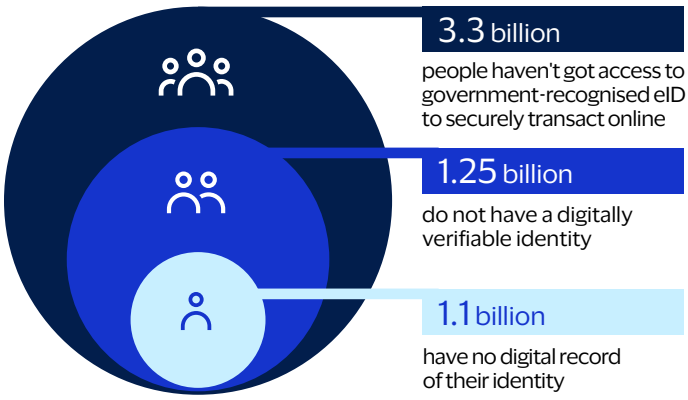
eIDs will unlock value across verticals

The eID market is seeing remarkable growth and transformation, offering convenient and reliable access to services across both the public and private sectors.

Despite potential benefits, adoption rates of eID programmes vary significantly among markets, with some struggling to gain traction while others reach high penetration.

The McKinsey Global Institute suggests that eID could unlock economic value equivalent to 3-to-13% of GDP by 2030,[10] while the World Bank believes it could extend access to financial services to over 1.7 billion underserved individuals.[11]

The most recent edition of the World Bank's ID4D Global Dataset shows that some 850 million people worldwide have no official ID, and many more have no official form of eID. This includes at least 1.1 billion people who have no digital record of their identity, 1.25 billion people who have no digitally verifiable identity, and 3.3 billion people who have no access to a government-recognised eID to securely transact online.[12]





16%

projected CAGR for the global digital identity market from 2020 to 2025.[13]

10. McKinsey Global Institute, Digital identification: A key to inclusive growth, 2019: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
11. World Bank/Financial Inclusion Global Initiative, Digital ID to Enhance Financial Inclusion, 2021: https://documents1.worldbank.org/curated/en/099650005162214653/pdf/P16477001277440f10b8080dc6f51daf2dc.pdf
12. World Bank, Global ID4D Dataset, 2022: https://datacatalog.worldbank.org/search/dataset/0040787
13. Strategy & , Digital identity: Opportunities and challenges, 2021

© 2024 Visa. All Rights Reserved



eID-based onboarding processes could release significant efficiencies

With sources estimating a potential 90% reduction in onboarding costs, representing a saving of some 110 billion hours through streamlined e-government services.[14]

The variation in adoption rates of eID programmes, implemented by both national governments and private companies, underlines the potential impact of eID and the crucial importance of successful implementation.

eID has the potential to deliver significant value across various industries, each with its unique needs and regulatory context.

Government services

For instance, in government services, eID can streamline interactions with citizens, enhancing processes like tax collection and budgeting. However, as the user base of eGovernment services is projected to reach 1.4 billion globally by 2028,[15] safeguarding personal information is a critical challenge.

Healthcare sector

In the healthcare sector, eID serves a dual purpose: giving patients secure access to their medical records and limiting access to patient data to authorised medical personnel. The industry is increasingly adopting advanced document verification and biometric technologies to enhance the Know Your Patient (KYP) process, as with Know Your Customer (KYC) in the financial sector.[16]

High-risk sectors

For high-risk sectors like online gambling and gaming, eID can help mitigate risks associated with data breaches, identity theft, and multiple account fraud. Given the gaming industry's susceptibility to these issues, its age-restricted nature, the degree of scrutiny it faces, and its links to financial and mental health concerns, robust eID verification checks are widely called for.[17]

The potential use cases of eIDs extend to many other types of digital interaction, including those yet to be conceived, that will be spread through regulatory, industry, and technological developments.

14. McKinsey Global Institute, Digital identification: A key to inclusive growth, 2019: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
15. Juniper, Global Digital Identity Verification Market, page 17-19
16. *ibid.*
17. *ibid.*

© 2024 Visa. All Rights Reserved

Financial services – and payments in particular – are set to benefit from eIDs

Financial services is one of the sectors pushing for advancements in eID, reflecting the growing digitalisation across the industry, the need for robust authentication solutions, and the rising consumer demand for a seamless, friction-free user experience.

Use cases here include KYC during onboarding, verification when accessing/using mobile banking, and regular payment authentication. Security concerns among both banks and consumers have given rise to a trend towards the use of zero-trust authentication, where continuous verification is applied across different stages of a digital interaction. There are strong incentives for further innovation around eID. The McKinsey Global Institute estimates that, **through improved customer registration, financial institutions stand to benefit from a reduction in onboarding costs and reduced payroll fraud, saving up to US$1.6 trillion globally.**[18]

Over recent years, payments in particular have experienced a radical transformation. **An explosion in the use of ecommerce has given rise to targeted fraud** aimed at this segment, while mobile payments have become the second or third most common payment type in many countries.

When considering the value of eID for financial institutions, onboarding stands out as the top priority. A recent survey showed that 75% of financial institutions prioritise onboarding, followed by KYC (25%), and then digital signatures and embedded finance (both at 8%).[19]

However, the widespread adoption of digital identity is expected to have an even broader impact on the overall banking and payments experience. It presents a strategic opportunity for merchants and banks to increase revenues, engagement, and customer loyalty.



~10%

is the total volume growth of digital identity checks in banking from 2019 to 2023[20]

18. McKinsey Global Institute, Digital identification: A key to inclusive growth, 2019: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
19. Mobey Forum, The Rise of Digital Identity Wallets: Will banks be left behind?, 2023: https://mobeyforum.org/the-rise-of-digital-identity-wallets-will-banks-be-left-behind/
20. Juniper, Global Digital Identity Verification Market, 2023

© 2024 Visa. All Rights Reserved



eID use cases in commerce, financial services and payments*

Customer onboarding
- Opening a bank account
- Creating a digital wallet
- Adding authorised cardholders

Service sign-up
- Setting up a robo-advisor account
- Applying for a credit card
- Registering for benefits

Account access authentication
- Accessing online banking
- Initiating a funds transfer

Payments
- Conducting Strong Customer Authentication (SCA) for digital payments
- Age verification when purchasing good and services

Sharing and verification of attributes
- Providing identity for KYC
- Signing transactions with attribute verification

Legally binding consent or contract
- Signing a loan agreement
- Authorising a direct debit
- Creating a proof of account ownership

Account changes
- Setting up a new address
- Changing a password
- Adding beneficiaries

Service termination
- Closing a bank account
- Terminating a credit card agreement
- Ending subscriptions

*Non-exhaustive

© 2024 Visa. All Rights Reserved

Key benefits of eIDs for financial institutions**

Improved customer experience

eIDs have a direct impact on NPS by eliminating the need for burdensome interactions and reducing manual data entry. When seamlessly integrated into financial institutions' digital platforms, eIDs can help streamline user experiences and improve data security control. This improvement in convenience and security can lead to increased engagement, loyalty, and overall client profitability.

Reduced cost of onboarding

The cost of KYC compliance is, on average, US$60 million per bank per year.[21] This includes employee time and branch, back office, and processing costs. With eID, the cost can be reduced by up to 90%.[22]

Reduction in fraud

Fraud levels resulting from stolen or incorrect customer information or poor authentication can be reduced with a multi-layered approach to mitigating fraud. When eID solutions are used to authenticate online payment transactions, fraud rates can improve by up to 500 basis points, and authorisation rates can double, while abandonment rates plummet.[23]

New revenue streams

A trusted eID solution and customer data is a valuable asset in the digital economy ecosystem, and enables identity providers to generate income from providing identity services to other service providers.

More reliable customer data

A uniform customer experience and the flexibility of eID systems enables financial institutions to capture a larger set of high-quality data points at onboarding, helps to keep data up to date, and brings a single, consistent customer view.

Frictionless ecommerce

Current ecommerce checkout process can be improved by integrating eIDs through financial institutions or directly into platforms. This ease of use, combined with the enhanced security and customer trust, can reduce cart abandonment, simplify the checkout process, and increase online shopping, leading to higher payment volumes and merchant sales.

Cross-selling opportunities

Given the simplified use of eID, there is a greater opportunity for financial institutions to cross sell their own products and other partnership offerings at each customer interaction.

Increased conversion rates

There is an increased conversion rate on product acquisition as fewer customers abandon applications thanks to the simplicity of identification. As many as 46% of customers abandon digital onboarding due to poor user experience and 51% due to the length of the process.[24]

Aligning with government ambition

National and regional governments across the globe are reaching the view that citizens should be able to cross borders and access services seamlessly while gaining back control over their data.

Innovation

Financial institutions can diversify their business models, innovate, and create new value-adding service propositions.

**Note: Deloitte information commissioned by Visa, eIDAS Digital Identity, 2023

21. ThomsonReuters, The cost of compliance for banks, 2020: https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-for-banks-with-new-cdd-rule
22. IDEMIA, Digital Identity for enterprises, 2020: https://www.idemia.com/wp-content/uploads/2022/12/whitepaper-idemia-digital-id-for-enterprises-202004.pdf
23. Visa, Visa Navigate Europe, How to prove you're not a dog, 2022: https://navigate.visa.com/europe/how-to-prove-youre-not-a-dog/
24. Experian, Customer digital onboarding: https://www.experian.co.uk/assets/business-services/brochures/digital-onboarding.pdf



©2024 Visa. All Rights Reserved

Europe is uniquely positioned to set the pace for eIDs



eID schemes have been widely introduced across Europe – but have uneven degrees of adoption and lack interoperability.

Thanks to a dynamic financial services ecosystem and a focus on related regulations, **most European countries are moving ahead with eID at pace and scale**. These solutions have had varying degrees of success and are at different levels of maturity. However, the scene is highly fragmented and the use of most eID schemes is limited to the country of issuance. Through regulations such as eIDAS, **Europe is emerging as a leader in promoting cross-border reliance on national eIDs** by setting standards for interoperability, reliability, and privacy.

Estonia

With a coverage close to 99%, Estonia's state-issued eID is one of the most developed in the world and can be used to access any public e-service. It can be used for identity verification and digital signatures.[25]

Denmark

The MitID solution is intended for both private and public sector applications as a single log-in electronic personal identification system.[26]

Finland

Finnish BankID and Mobile-ID (FTN) is a framework established by the Finnish government to provide a single point of access to all the eIDs issued by Finnish banks and mobile telecom operators. [27]

Sweden

The BankID system is managed by a consortium of banks that charge relying parties for their authentication services. As of 2023, its adoption had reached 9 million users.[28]

Italy

SPID is a public identity system that provides identity proofing in online services from both public administrations and private entities.[29]

Belgium

A scheme co-created by banks and telecom providers in Belgium. With 7 million users, representing 80% of adults, it has one of the world's highest adoption rates, and is used for more than 1 million actions every day.[30]

UK

A digital identity scheme set to establish alignment across the ID providers and relying parties in the UK.[31]

Germany

An eID platform offering secure, convenient solutions for accessing and using online services. Backed by a consortium of banks, technology companies and car companies, it processed 10m transactions in 2023.[32]

Poland

A government-backed eID system which enables citizens to access public services, based on user data extracted from Poland's PESEL (national identification number) registry.[33]

Disclaimer: All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

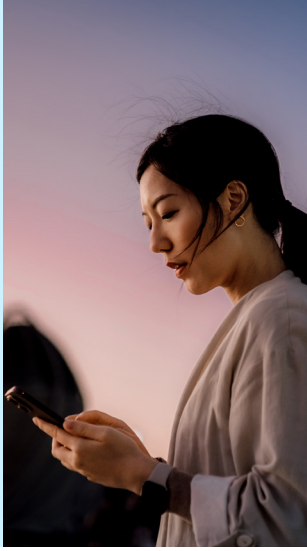
25. YOTI, Digital Identity Toolkit, Section 5: Digital identity solutions, 2023: https://www.yoti.com/wp-content/uploads/Digital-Identity-Toolkit_Section-5_Digital-identity-solutions.pdf
26. Nordic Co-Operation, Electronic ID in Denmark - MitID: https://www.norden.org/en/info-norden/electronic-id-denmark-mitid
27. Nets, Finnish Trust Network: https://www.nets.eu/solutions/digitisation-services/identification/Pages/%E2%80%8BFinnish-Trust-Network.aspx
28. YOTI, Digital Identity Toolkit, Section 4: Case studies: https://www.yoti.com/wp-content/uploads/Digital-Identity-Toolkit_Section-4_Case-studies.pdf
29. SPID, Public Digital Identity System: https://www.spid.gov.it/en/
30. Fintech Belgium, itsme, has exceeded 7 million users in Belgium, 2023: https://www.fintechbelgium.be/news/itsme-has-exceeded-7-million-users-in-belgium
31. Select ID: https://www.selectid.co.uk
32. Verimi, About us: https://verimi.de/en/about-verimi/
33. Transactionlink, mObywatel: https://www.transactionlink.io/integrations/mobywatel

© 2024 Visa. All Rights Reserved

Regulatory initiatives to drive European eID expansion

Generally, the region has benefited from a proactive and progressive approach to eID by the regulatory community.

The two regulatory initiatives within Europe, the Pan-European and the UK, have adopted very different regulatory approaches.



EU regulatory initiative

The European Commission is prioritising eIDs to enable pan-European solutions that are interoperable across borders through the eIDAS2 regulation reform, finalised in April 2024. Through eIDAS2, the European Commission is specifying the technical architecture and standards to be used. All governments in Europe are to offer their citizens a European Digital Identity Wallet (EUDIW) for accessing both public and private services. eIDAS also pushes for strict requirements on interoperability and obliges certain relying parties to accept eIDs.[34]

Member States

- Must develop or certify – at least one-third party EUDI Wallet no later than two years after the entry into force of certain implementation acts.
- Must help confirm/provide information in eIDs through certifications or appointing qualified accrediting entities:
  - Age, gender, marital status, family composition
  - Address, nationality/ citizenship
  - Education, titles, authorisations

Requires registration in order to request information from wallets

Must identify itself as registered relying party and request needed information

Relying Parties

- Required to verify the authenticity and validity of user wallet.
- Can only retrieve information for which they have registered with the member state.
- Cannot refuse the use of pseudonyms if identification of user is not legally required.

Public companies
Must accept eIDs from other member states

Private* companies and very large online platforms
(that require user identification) must accept EUDIW for logins

Wallet

- Must be available online and offline.
- Must confirm/provide certain information, as determined by the state.
- Must prevent tracking and ensure unlinkability of user behaviour, with the ability to report suspicious activity.
- Should offer the possibility to sign documents free of charge** and communicate with other wallets.
- Can only allow access to eIDs to registered relying parties.

Provides identity or attributes

*Excludes Micro & Small Businesses.
**Specific to commercial use.

34. Juniper, Digital Wallets, page 35-36 & Juniper, Digital Identity, page 30-33

© 2024 Visa. All Rights Reserved

The UK has established a trust framework for eIDs and attributes

UK regulatory initiative

The UK system includes a certification and trust mark to certified organisations. The private sector is participating by creating identity schemes under this trust framework such as "Right to Work" and "Right to Rent." [35]



It's not just the regulatory community who are enthusiastic. There is strong demand across the digital ecosystem. Consumer expectations for a seamless digital experience have given rise to several payment wallets and, when robust eIDs are available, people are comfortable using them.

In Belgium, for example, more than 80% of the adult population use the itsme eID service, trusting it to process more than 1 million identify verifications every day.[36]

Similarly, commercial businesses see eIDs as an opportunity to improve the quality of customer service and generate new business, as indicated by the emergence of more than 20 such schemes across the European region.

80%

of the adult population in Belgium use the itsme eID service, trusting it to process more than 1 million identify verifications every day.[36]

35. Gov UK, Enabling the use of digital identities in the UK: https://www.gov.uk/guidance/digital-identity#latest-news & Juniper, Digital Identity, page 33-34
36. Itsme, Passing the milestone of 7 million users in Belgium, itsme® records a profit of EUR 1,6 million, 2024: https://www.itsme-id.com/en-BE/business/blog/figures2023

© 2024 Visa. All Rights Reserved

What Visa is doing to accelerate eID development and adoption

At Visa, we believe that digital identity can have a transformative impact on payments and other digital services to the benefit of our clients. We are actively participating in the digital identity ecosystem to ensure that Visa continues to be the best way to pay and be paid.

Introducing our strategy to accelerate eID



Harmonising user experience when eIDs are used for payments

- Encourage adoption of common standards
- Foster a great payment user experience to improve conversion and customer satisfaction
- Enable easy access through single interface and harmonised output

Provide identity and authentication services for Relying Parties

- Offer payment authentication services through Visa Payment Passkeys
- Enable eID and DI wallets as token requestors to support payments and money movements such as peer-to-peer, disbursements, and account payments
- In the future, leverage Visa rails to share identity attributes with merchants

Active participation in Digital Identity ecosystem

- Leading EU DI wallet payment pilots with the European Commission to ensure connectivity with existing and new payment infrastructure, regardless of scheme or rail
- Participating in the Open Wallet Foundation to facilitate card payments via digital identity wallets
- Developing rules and policies to ensure trust, predictability, reliability, and scalability through participation in Select ID, a UK digital identity scheme
- Active participation and contribution to identity related standards to ensure future proofed services (e.g. OIDF, W3C, Fido, EMVCo, Berlin Group)

© 2024 Visa. All Rights Reserved

Active participation in major industry initiatives in Europe



Initiative 1

eIDAS 2.0

The European Commission has selected a European Wallet Consortium (EWC) to conduct an eIDAS 2.0 large-scale pilot on the EU Digital Identity Wallet (EUDIW), to test and prepare for its use in public and private services.

The EUDIW will be used for authentication, identity validation, and to hold payment credentials, for consumers and businesses. It is set to provide all 447.7 million EU citizens with the ability to store and exchange identity documents and credentials securely and conveniently.

Visa is leading and managing the payment task force, working on two main use cases for EUDIWs:

Payment authentication for ecommerce

An e-commerce authentication solution which complies with the regulatory obligations for SCA and, via a robust registration process, links the wallet holder with a payment account. The EUDIW is to be invoked by the bank to perform SCA for both card-based payments and open banking payments. In effect, the responsibility for authentication will be delegated to the EUDIW.

Payment initiation for both in-person and ecommerce payments

Providing the ability to use EUDIW to initiate a payment transaction with a merchant, either in-store or online. The EUDIW will be able to request and store card and account tokens. For in-store NFC card payments, there will be no impact on merchant acceptance. For ecommerce payments, the EUDIW will push the card or account token payload to the online merchant for payment processing.

Disclaimer: The features and functionalities described are currently in development and may change prior to release.

© 2024 Visa. All Rights Reserved.

Active participation in major industry initiatives in Europe

Initiative 2

Open Wallet Foundation

The Open Wallet Foundation (OWF) is an initiative by the Linux Foundation to create an open-source codebase for wallets.

Its goals are to develop best practices and standards-based open-source components which enable user choice, security and privacy for digital wallets.

Visa is a founding partner, sits on the governing board and the technical advisory committee and, at the time of writing, holds the board seat.

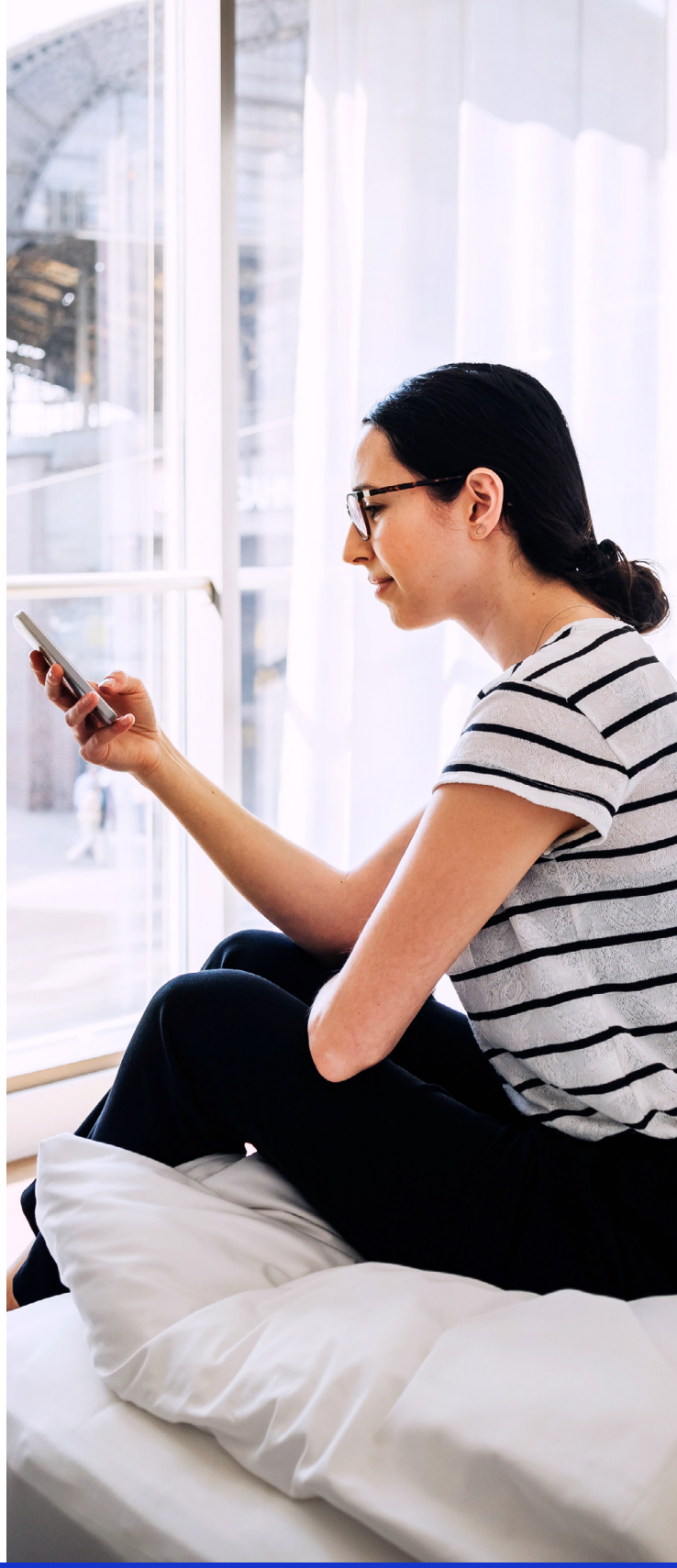
Initiative 3

Select ID

The Select ID is a UK identity scheme designed to simplify access to eIDs for Relying Parties.

Its core services include a marketplace for reusable eID providers, orchestration, and a scheme specifically for financial services.

Visa is a founding partner in Select ID, aiding in the establishment of common rules and ensuring predictability in the use of eID wallets.



© 2024 Visa. All Rights Reserved



Visa assets to benefit the ecosystem

Recent Visa releases showcase the company's commitment to enable eID innovation and adoption, leveraging the existing Visa trust network. To accelerate the implementation and adoption of eID services in payments and beyond, Visa is introducing two inititatives:

01

Visa Payment Passkeys

Enabling easy authentication with device biometrics/PIN across products such as Click to Pay and Digital Authentication Framework.

02

Visa Data Tokens

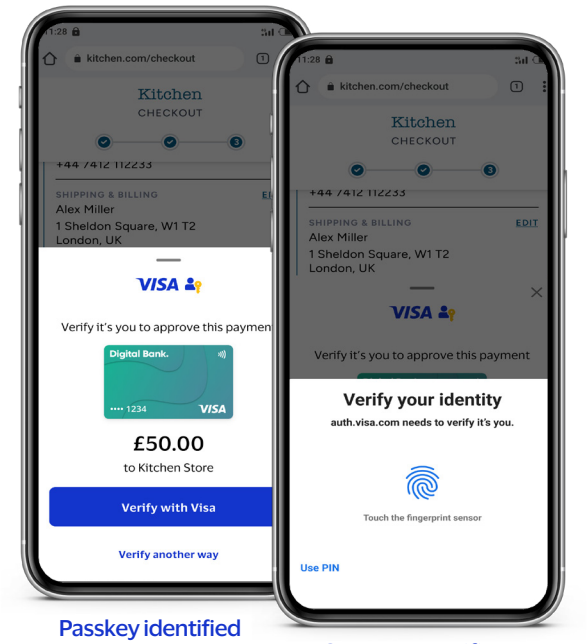
Allowing merchants and acquirers to get customer spend insights, while providing customers with a consent-based interaction of the data they would like to share.

© 2024 Visa. All Rights Reserved

Visa Payment Passkeys

Next generation authentication powered by Visa.

Using FIDO standards, the Visa Payment Passkey Services allows easy authentication with device biometrics/PIN. By reducing the reliance on traditional passwords/OTPs and replacing it with biometric authentication on consumer devices, passkeys reduce checkout friction while simultaneously reducing fraud rates.



Passkey identified at checkout

Consumer verifies using biometrics

Note: The above is intended for illustrative purposes only. It contains depictions of a product currently in the process of deployment, and should be understood as a representation of the potential features of the fully-deployed product. The final version of this product may not contain all of the features described in this paper.

It works on existing open standards and leverages the same tokenisation currently used at Visa via three simple steps:

1. User enrols once using device biometric capabilities and accepts terms and conditions.
2. Visa creates two keys: a private key that sits on the device and a public key that sits on the server.
3. This securely binds their identity to payment credentials without the need to worry about passcodes or authenticator apps for each checkout experience.

✓ The credentials are ready to use in checkouts that have incorporated this functionality.



© 2024 Visa. All Rights Reserved

What are Passkeys?

Passkeys, also known as digital keys or cryptographic keys, are a set of standards developed by the FIDO Alliance that are poised to transform the way we authenticate and sign in to websites, apps and other digital services.

By leveraging passkeys, both consumers and businesses can enjoy a more seamless and secure online experience, reducing the risk of fraud and identity theft and improving overall user satisfaction.





Key features

Public Key Cryptography
Passkeys use public key cryptography to provide a secure way to authenticate online. Private keys are never shared, and public keys are used to verify the user's identity.

WebAuthn Protocol
Protocol to provide a standardised way of authenticating online which is supported by most modern browsers and devices.

Device-Based Authentication
Passkeys are stored on the user's device, which provides an additional layer of security and convenience.

Phishing-Resistant
The user's device is required to sign the challenge from the server, which makes it much harder for attackers to intercept or steal the user's credentials.

Key benefits

Improved Security
Secure way to authenticate online, reduced risk of phishing attacks and identity theft.

Convenience
Eliminates the need for users to remember multiple passwords.

Privacy
Helps protect user data and reduce the risk of data breaches.

Control
Easily revoked or updated, giving users more control over their digital identity.

© 2024 Visa. All Rights Reserved

Visa Data Tokens

Visa Data Tokens allow merchants and acquirers to get customer spend insights, while providing customers with a consent-based interaction of the data they would like to share.

These can be grouped into three categories:

1. **Persona insights** (based on behaviour)
2. **Spend Insights** (based on category/ segment aggregation)
3. **Predictive signals** (likely next actions)

Spend and spend-derived insights will be tied to the consumer and beneficial to multiple players across the payment transaction:

Merchants

Will be able to access customer spend data in the shape of Data Tokens and leverage it to create customised services and experiences.

Customers

Will have a consent-based ability to choose the level of privacy they want. They get a customised shopping experience by choosing to use data tokens, but can withdraw permissions anytime.

Issuers

Will be able to improve customer engagement leading to higher active rates, higher spend per card, and therefore revenue.



© 2024 Visa. All Rights Reserved

How financial institutions and merchants can prepare and benefit



As eID initiatives and technologies evolve across Europe, businesses and financial institutions will encounter new opportunities to improve key areas like customer acquisition, conversion, user experience and security, but they must also be aware of the related compliance and technical requirements.

Core strategic considerations to participate and benefit from the new wave of eID developments

01
Get familiar with digital identity

02
Take stock and audit

03
Comply with regulations

04
Innovate to lead

05
Strengthen and secure infrastructure

06
Train and communicate

© 2024 Visa. All Rights Reserved

01

Get familiar with digital identity

Ensure that your organisation is up to speed with the eID landscape, players and regulatory expectations.

As we have discussed, the eID landscape is evolving and nascent, so key players and roles are still in flux. Research and form your own opinion:

- **Understand**
  eID attributes, verification methods, and authentication channels.
- **Follow**
  The latest trends, developments and regulatory developments.
- **Attend**
  Relevant events, webinars, workshops and courses to deepen your institution's understanding and meet potential partners.

Identify the best use cases and solutions for your organisation, considering factors such as customer needs, market potential, competitive advantage, cost efficiencies and risk mitigation. You may also want to identify potential trusted partners and reliable providers of eID services.





02

Take stock and audit

Work through all your existing customer journey flows, digital onboarding processes and data sharing touchpoints, to understand where new eID requirements – and opportunities – may impact your business and its goals.

As you assess these flows, processes, and touchpoints, focus on any areas where the integration of eID technology could streamline and enhance the user experience – as well as any risks and opportunities for improvement.

Be sure to analyse the needs and preferences of your customers and stakeholders to ensure the eID solutions you implement align with their expectations and comfort levels. Also, benchmark your current performance and levels of customer satisfaction against industry best practices and standards for eID, and use this comparison to identify gaps in your current approach and opportunities.

© 2024 Visa. All Rights Reserved

03

Comply

Ensure you are prepared for new regulatory requirements – such as eIDAS 2.0 – applicable to the jurisdictions in which you operate.

As early as 2026, financial institutions in the EU will be legally required to accept the EU Digital Identity Wallet (EUDIW) as a means of identification. You should therefore map out the right workflows and requests that leverage EUDIW for customer onboarding, new product applications and SCA.[37]

To verify incoming requests and ensure outgoing statements can be validated by relying parties and wallets, financial institutions are required to attain Qualified Trust Service Providers (QTSP) status under the eIDAS 2.0 regulation.[38] This means, for example, they will need to be independently accredited, and able to create, verify and validate electronic signatures, timestamps, and seals, as well as certificates related to these services, complying with the requirements established by the eIDAS Regulation.[39]

Any merchants operating in the EU that are legally obliged to request identification, will also be required to accept the EUDIW, and will be subject to a raft of related regulatory requirements. Importantly, businesses must be prepared to accept eIDs from any EU member state. This means they must also understand and comply with the legal and technical requirements for accepting international eIDs, ensuring their systems are equipped to handle eIDs from various jurisdictions.

Both banks and merchants should therefore work with legal and compliance experts to ensure all aspects of their eID strategy are compliant.

37. The Paypers, What is the impact of EU digital ID wallets on banks and financial institutions?, 2022: https://thepaypers.com/thought-leader-insights/what-is-the-impact-of-eu-digital id-wallets-on-banks-and-financial-institutions--1255579
38. Ubiqu, Why eIDAS 2.0 is a major opportunity for banks, 2024: https://ubiqu.com/why-eidas-2-0-is-a-major-opportunity-for-banks/
39. Ultimaco, What is a Qualified Trust Service Provider?: https://utimaco.com/service/knowledge-base/digital-signing/what-qualified-trust-service-provider-qtsp



04

Innovate to lead

Because the ecosystem is nascent, there is an opportunity to move well beyond regulatory requirements, assert a leadership position and introduce new products. This can take shape in different ways. For example:

- Explore opportunities for new products or services that leverage eID technologies.
- Always keep the customer experience at the forefront of innovation efforts, and focus on how eIDs could streamline processes, increase security, and create seamless, personalised customer journeys.
- Stay ahead of the curve by investing in research and development in the field of eID.

Remember that, for financial institutions, eIDs and KYC eSealed documents can help make manual checks obsolete. This not only streamlines the authentication process, reducing customer dropouts at onboarding, but also enhances the payment experience by facilitating smoother transactions, reducing risk, and lowering fraud rates. Any business can even consider joining government-backed and/or pan-regional initiatives to stay at the forefront of the eID landscape.

© 2024 Visa. All Rights Reserved

05

Strengthen and secure infrastructure

Ensure that your technology platforms are flexible and capable enough for you to take full advantage of the eID opportunity.

Infrastructure enhancement

Evaluate and upgrade your existing infrastructure to adequately support and manage eID, which could involve investing in new hardware and updating software.

Data protection

Implement robust data protection measures to ensure the security and privacy of eID data.

Cybersecurity

Strengthen cybersecurity frameworks to protect against potential threats.





06

Train and communicate

Ensuring staff, partners and customers are well informed about the benefits and potential risks related to eID helps build trust, improves user experience, and facilitates smoother adoption of the technology.

Training programmes

Create comprehensive training programmes for staff to understand the nuances of eID technologies. This includes technical training for IT staff and awareness training for other employees.

Regular updates

Keep staff and stakeholders informed about developments in the eID landscape. This could include changes in regulations, advancements in technology, or shifts in industry trends.

Outbound communications

Educate customers about the benefits and potential risks of eIDs, and provide clear instructions on how to use eID technologies safely and effectively.

© 2024 Visa. All Rights Reserved

Visa can help you with eID planning and implementation

Our global team of experts can help with understanding eID, planning a use case roadmap, and delivering implementation support. We have a comprehensive portfolio of services to support clients with their eID journey – from supporting discovery and planning all the way through to use cases and implementation. Visa Consulting & Analytics also helps clients design and develop their foundational capabilities, including strategy and data governance.

Foundational

- eID capability assessment
- eID support
- Data, content, and insight provision

Discovery and planning

- Understand eID
- Design and develop eID use cases
- Audit internal processes
- Identify best practices and opportunities

Implementation

- Design and deliver test and learn programmes
- Support on the development and launch of Minimum Viable Product (MVP)
- Establish the approach to scaling and execution
- Identify and evaluate partners and vendors



About Visa Consulting & Analytics

We are a global team of hundreds of payments consultants, digital marketing specialists, data scientists and economists across six continents. The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that help drive business decisions.

Experts

Our consultants are experts in strategy, product, portfolio management, risk, digital and more, with decades of experience in the payments industry.

VisaNet

Our data scientists are experts in statistics, analytics, and machine learning, with exclusive access to insights from VisaNet, one of the largest payment networks in the world.

Unique

Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends.

Get in touch

For help addressing any of the ideas or imperatives in this whitepaper, please reach out to your Visa Account Executive to schedule time with our Visa Consulting & Analytics team

Email our team

Visit our webpage

Follow us on LinkedIn

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

© 2024 Visa. All Rights Reserved