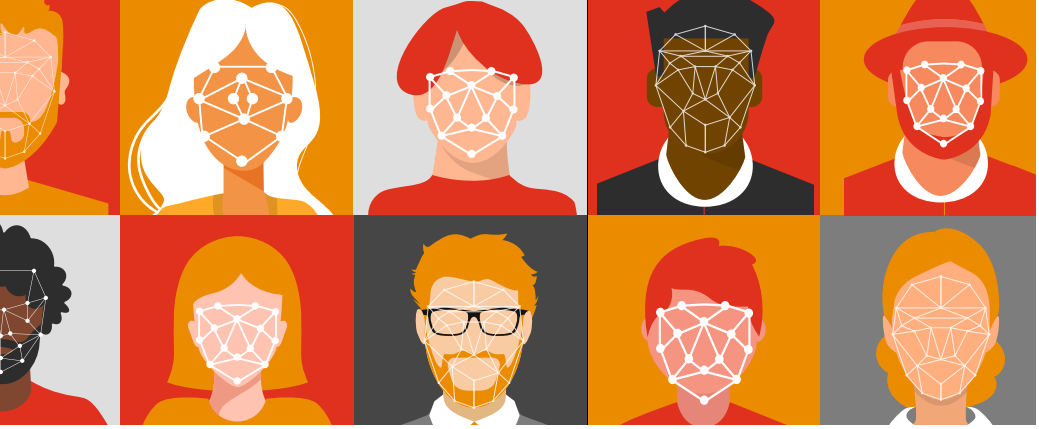


Digital identity

Unlock digital services and trust digital life

"EU citizens not only expect a high level of security but also convenience (…). The European Digital Identity wallets offer a new possibility to store and use data for all sorts of services, from checking in at the airport to renting a car. It is about giving a choice to consumers, a European choice. Our European companies, large and small, will also benefit from this digital identity, as they will be able to offer a wide range of new services since the proposal offers a solution for secure and trusted identification services."

Thierry Breton, EU Commissioner for Internal Market, about the European Digital Identity initiative

pwc

We've never been so close to bringing true digital identity to citizens and corporate life – secure, easy and consent-based.

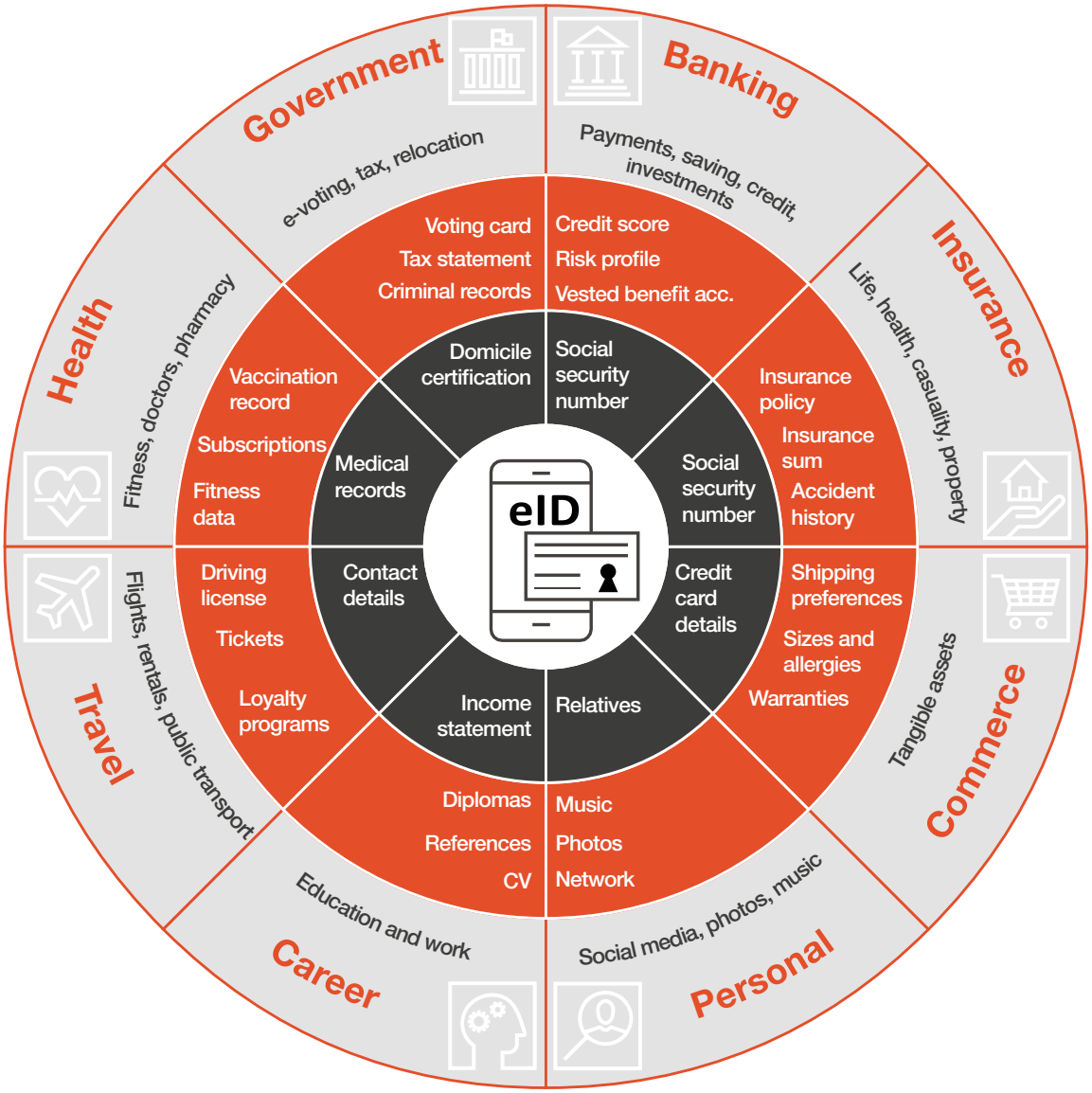
The reward? Speed, convenience, trust and privacy.

Contents

1 A growing need for a digital identity

Identity is a precondition for participating in society by facilitating access to health and welfare systems, education, and financial and government services. With the accelerating digital transformation, a rapidly growing number of transactions is conducted online, creating an ever-more-urgent need for a digital identity.

Based on verified personal information, a digital identity can be defined as a set of digitally captured and stored attributes such as name, date of birth or gender coupled with credentials that are linked to a unique identifier to identify a person and thereby facilitate transactions in the digital world. Core digital identity attributes can be complemented with additional attributes and documents from all areas of life such as social security number, medical records or school diplomas, catalysing the digital transformation for countless use- cases ranging from opening a bank account and taking out an insurance policy to filing a tax return.



eID Verified core identity: Name, first name, gender, nationality, place of birth, facial image, reg. nr.

Use-case area

General data

Industry-specific data

Before we were aware of how extensively the internet would proliferate and works its way into our everyday lives, the internet was built without a native identity layer. In the absence of a standardised way to identify people or entities, every website started to create its own digital identity solution with its own local accounts and passwords. As a result, in their digital interactions, people amass a multitude of digital identities ranging from different e-mail accounts and social media profiles to e-banking accounts.

The ability to use the internet without revealing your real identity is not necessarily bad. When using certain digital services, like sharing content on social media, a pseudonym is more than enough. In some instances, such as exercising the right to freedom of expression in an authoritarian state, remaining anonymous is key. In many other cases, for example when opening a bank account or taking out an insurance policy, companies are required to know the identity of their counterparty by law.

Today's fragmented digital identity landscape, with its large number of accounts and passwords, comes at a cost. For users, having an unmanageable number of accounts and passwords is time-consuming and inconvenient, as they have to register their identity data repeatedly with every new counterparty and often lose access to their accounts.

From a security perspective, today's fragmented digital identity landscape is unregulated and characterised by a daunting number of heterogeneous and unregulated security levels. Faced with this complexity, many users neglect security concerns and use the same simple pass- word across many different services.

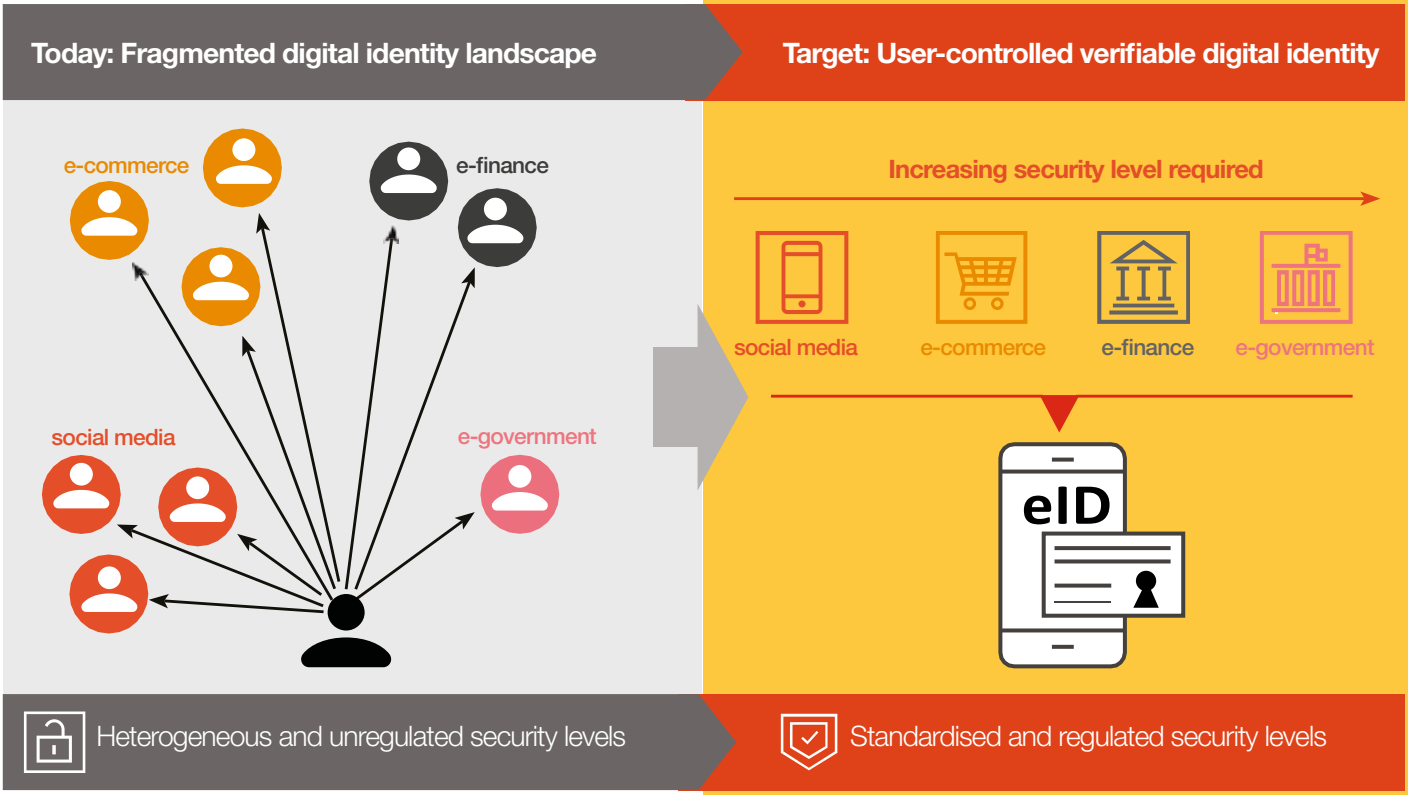
These issues arise because of the current paradigm around digital identity which has evolved organically over the years: there are almost as many issuers of digital identity as there are verifiers, as organisations trust the data they have collected and believe they benefit from owning it.

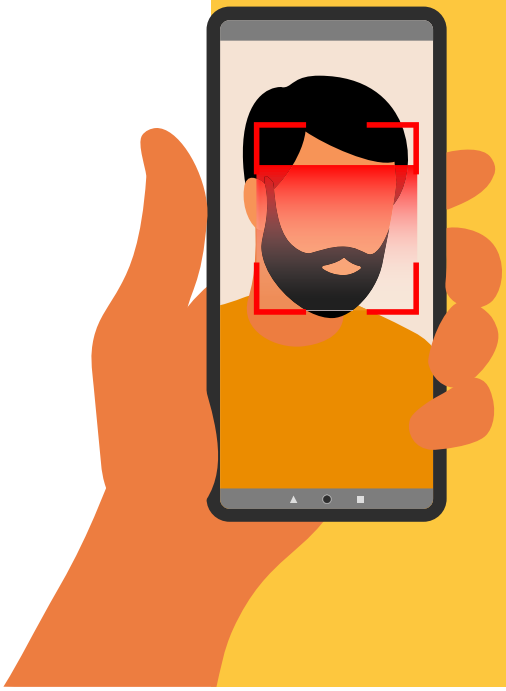
Thankfully, this paradigm is about to change. Technological advances such as Distributed Identifiers and Verifiable Credentials enable a multitude of identity verifiers to trust a set issuer, thereby dramatically reducing the number of required digital identities.

By reducing the amount of identities, and putting them in control of the end used, there is the potential to significantly improve both user experience and convenience by making a wide range of digital services accessible in a seamless fashion and rendering repeated registration obsolete. In addition, users will be able to regain control over their digital identity by being able to manage which attributes they want to share with which counterparty.

From a business point of view, the identification of the same customer is redundantly replicated with every company a customer has a business relationship with. This means every company must develop and maintain their own costly and often largely paper-based identification processes for onboarding new clients as well as authenticating existing clients in order to provide services to them. In addition, every business must periodically review and update the customer data to reflect any changes.

With this in mind, verifiable digital identities represent an opportunity for public organisations and private companies to reduce risks and realise considerable cost savings by increasing process efficiency and de-facto outsourcing customer identification. Businesses can increase their conversion rates by lowering the threshold to conclude a transaction, and by launching new products and services with a superior user experience to help them gain a competitive edge. Public organisations can more effectively render accessible their services to the citizens and the private sector at a lower cost to them.


Today: Fragmented digital identity landscape
Target: User-controlled verifiable digital identity
e-commerce
e-finance
social media
e-government
Increasing security level required
social media
e-commerce
e-finance
e-government
eID
Heterogeneous and unregulated security levels
Standardised and regulated security levels



2 Understanding digital identity

2.1 Digital identity ecosystem

The provision and usage of digital identity involves a number of interdependent actors, who collectively form a digital identity ecosystem. Confronted with increasing complexity due to growing transaction volumes and increasing customer expectations, any successfully digital identity ecosystem requires a collaborative effort across organisations and industries.

Across all stages of the digital identity lifecycle, every player takes on certain tasks or operations that are associated with their role. But digital identity systems can come in many different forms. The number of defined roles and the scope of their activities largely depend on the specific requirements of a country's legal framework and the players involved.

Hence, a set of archetypical roles in a digital identity ecosystem will be introduced. The first three core roles Identity Owner, Identity Provider and Relying Party represent the minimum for any digital identity ecosystem. The three roles Broker, Attribute Provider and Service Provider are labelled as ecosystem- dependent roles, as they can be incorporated in a digital identity ecosystem as needed. It is important to note that these generic roles can be further subdivided to accommodate different circumstances and requirements.

In practice, the key question when designing a digital identity ecosystem is whether to adopt a model that is broker centric or Identity Provider centric.

Identity Owner (IO)	• Owner and controller of a digital identity • Uses their digital identity to conveniently and securely identify themselves in digital transactions • Natural person (e.g. Alice or Bob)
Identity provider (IdP)	• Responsible for the provision of a digital identity • Verifies an individual's identity and issues the corresponding digital credentials to ascertain their digital identity • Government agency (e.g. passport office) or government-recognised organisation (e.g. bank)
Relying Party (RP)	• Relies on a digital identity for onboarding of new customers and authentication of existing customers • Integrates digital identity in its operating model to improve the user experience and increase efficiency • Industry-agnostic role including businesses (e.g. online shops) and government agencies (e.g. tax offices)
Broker	• Ensures interoperability in the ecosystem and enhances privacy by preventing tracking actions across different roles • Intermediates the data flow between the Identity Provider and the Relying Party • Neutral organisation (e.g. infrastructure provider)
Attribute Provider (AP)	• Offers additional attributes that are not collected by the Identity Provider during registration • Additional attributes allow Relying Parties to accelerate their digital processes and offer more tailored services • Government agency (e.g. fedpol), state-affiliated company (e.g. Post) or private company (e.g. Telco)
Service provider	• Offers electronic trust services such as digital signatures • Electronic trust services allow providers to enhance and expand the interactions and services within the ecosystem • Private company (e.g. Telco)

Core roles Ecosystem-dependent roles

Identity Provider centric

In an Identity Provider-centric model, the data flows directly from the Identity Provider to the Relying Party, and vice-versa. Hence, the actions of the Identity Owner can be traced across the ecosystem. For example,

the Identity Provider could track how often the Identity Owner logs into an online casino, while the casino might register which institution the Identity Owner has registered their digital identity with.

Broker centric

In a broker-centric model, an Identity Broker intermediates the data flow between the Identity Provider and the Relying Party to ensure interoperability and enhances the system's overall privacy by "blinding" the Identity Provider and Relying Party from one another. This means the Identity Owner's actions cannot be traced.

However, channelling the entire data flow through the broker as a central authority introduces a single point of failure and creates a honeypot with a vast quantity of valuable data. Implementing a broker based on a private blockchain, as in the case of the Canadian digital identity solution (developed by SecureKey), could offer a solution to this issue and meet the so-called triple-blindness requirement.

2.2 Digital identity lifecycle model

The provision and usage of digital identity is not a single, one-time event, but rather a sequence of (recurring) events, which can be conceptualised in a lifecycle model. In the following, a generic end-to-end digital identity life- cycle will be introduced based on a broker-centric digital identity ecosystem.

Registration

The registration stage initiates the digital identity life- cycle and can be further subdivided into claiming and verifying digital identity. (1) In a first step, the Identity Owner registers their digital identity by entering a set of required identity attributes in the Identity Provider's web or mobile application. The attributes can be categorised as biographical data such as name, gender, address, biometrical information (e.g. fingerprint, iris scan) and/or additional data formats such as behavioural data. (2) Depending on the chosen security level, the Identity Owner has to set up an appropriate authentication method. In the case of 2 Factor Authentication (2FA), this includes a first as well as a second factor of their choice. (3) The completed application is then submitted to the Identity Provider.

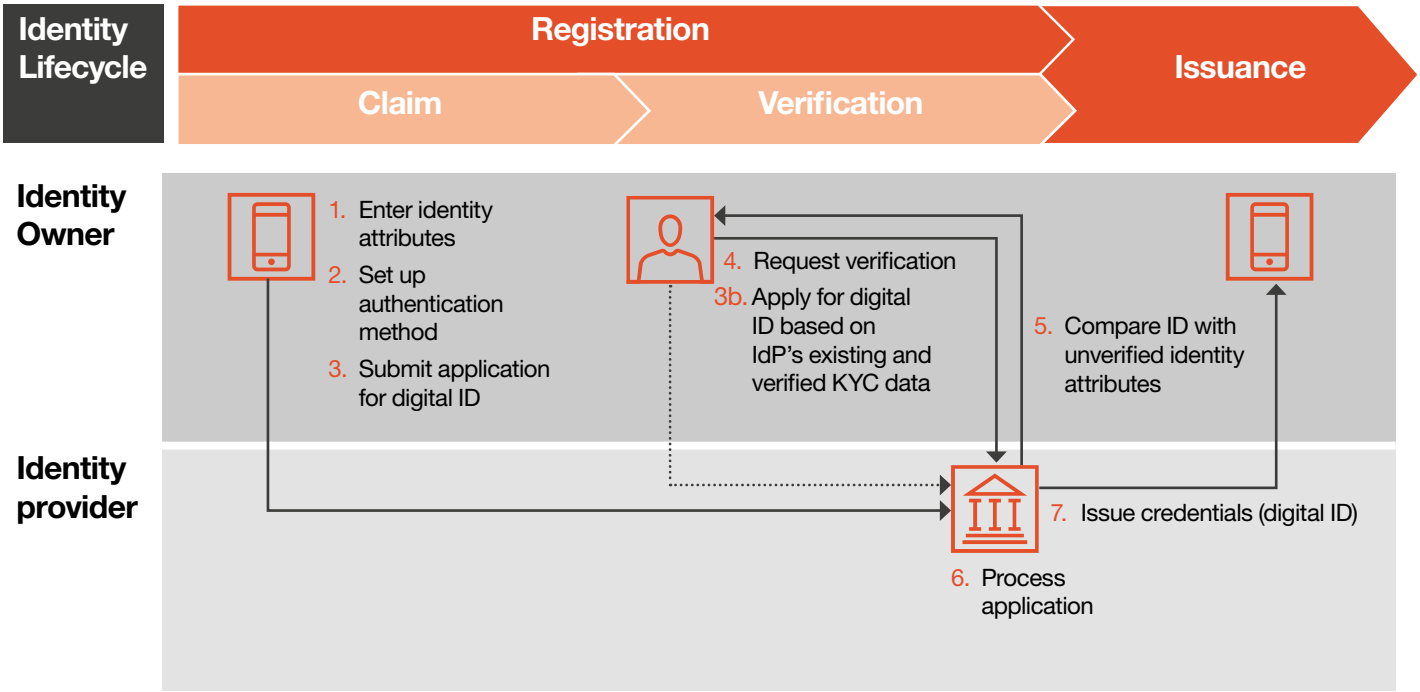
Verification

In a next step, (4) the Identity Owner requests verification of their identity data. In response, (5) the Identity Provider verifies the claimed identity against existing data. This is necessary to ascertain whether the claimed identity exists and is unique (deduplication). In most cases, the verification is based on at least one official government ID. Depending on the desired security level, this step is executed as face-to-face verification at the Identity Provider's premises or through an equivalent online presence such as a video identification (see also FINMA Circular 2016/7 Video and online identification).

Depending on the design of the digital identity ecosystem, (3b) the Identity Owner can shorten the registration process and leverage an existing business relationship. Identity Providers (i.e. banks) can reuse the verified identity data they have already collected to meet their Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) obligations.

Issuance

Once the Identity Owner's identity is successfully verified, (6) the Identity Provider processes the Identity Owner's application and (7) issues the credentials in the form of a digital identity. With the issuance of credentials, the Identity Provider ascertains the Identity Owner's identity by authoritatively linking the digital identity via a unique identifier to at least one authenticator. Credentials can be categorised as something you know (e.g. password or PIN), something you are (e.g. biometrical information such as a fingerprint) or something you have (e.g. ID card or security token).

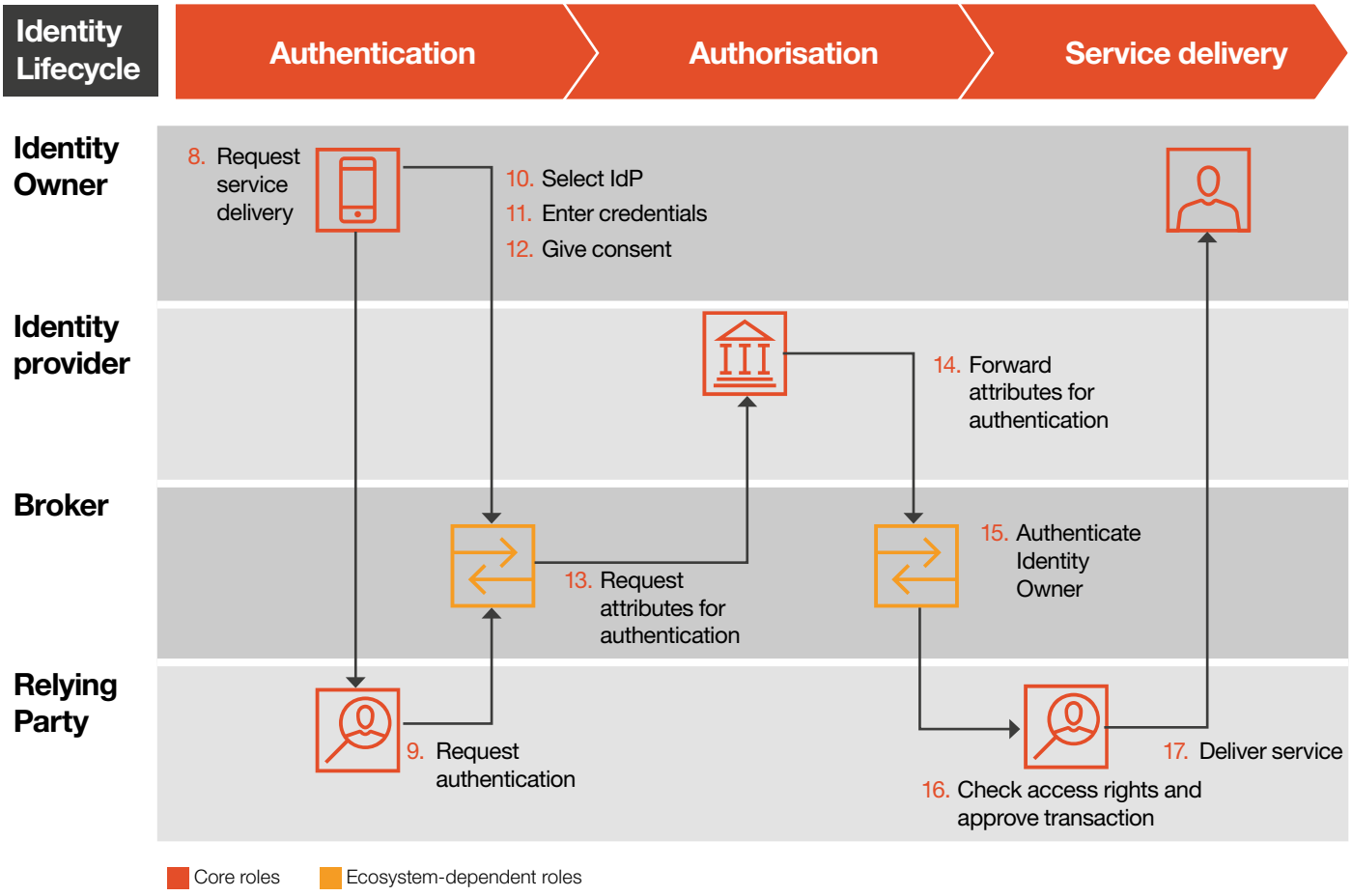


Authentication

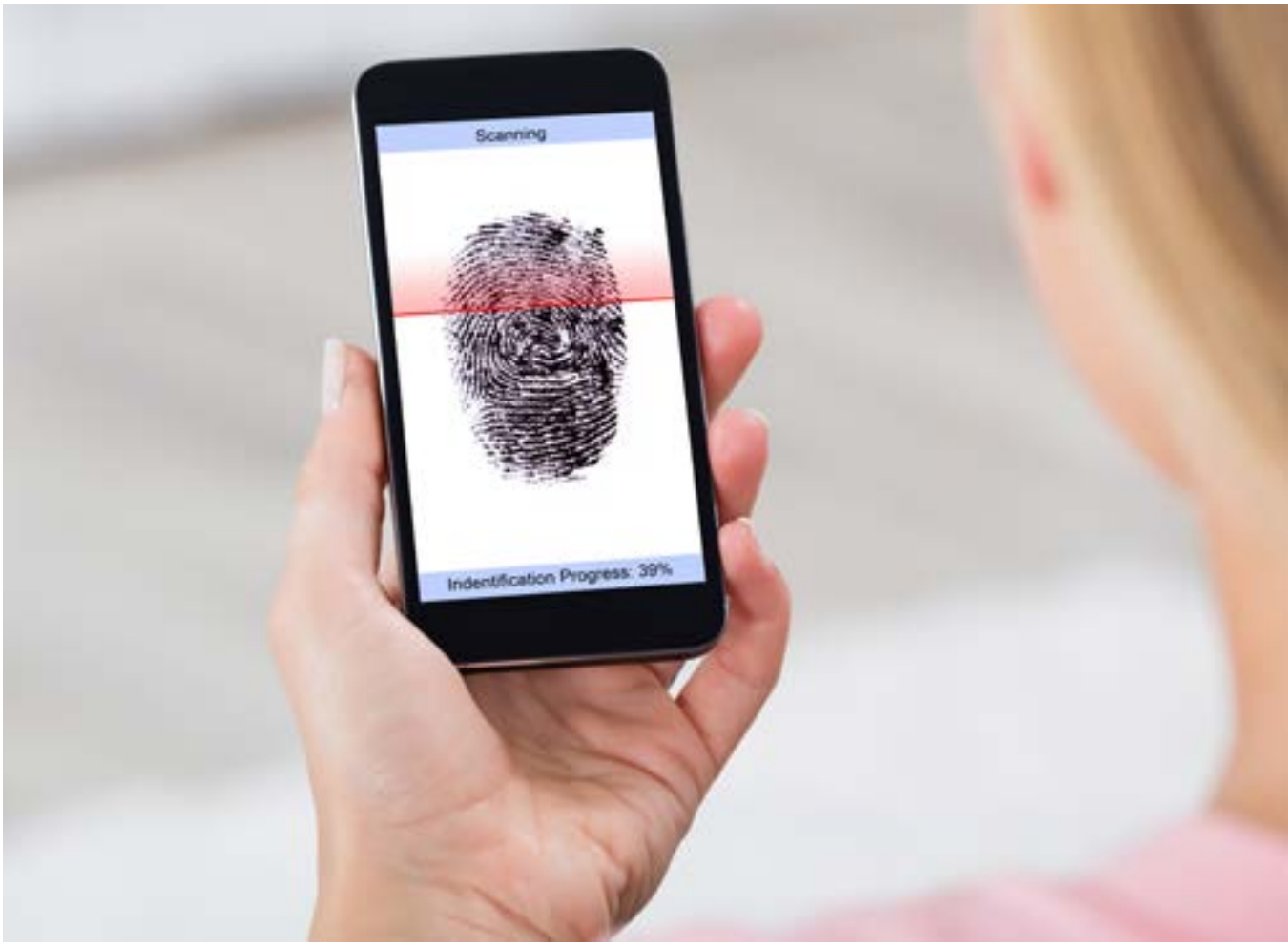
(8) The Identity Owner can now use their digital identity to access and request digital services, such as signing into the web portal of an airline to purchase a flight ticket. (9) In order to provide the required service, the Relying Party needs to authenticate the requestor. In a broker-centric digital identity ecosystem, the Identity Owner is redirected for the purpose of authentication to the broker's mobile or web portal. At this point, the Identity Owner is asked to (10) select their preferred Identity Provider for this transaction, (11) present one or more (digital) credentials to prove their identity and (12) give consent to share the requested identity attributes with the Relying Party on a one-time or time-bound basis. As soon as the authentication request is fully approved by the Identity Owner, (13) the broker requests the desired identity attributes from the chosen Identity Provider and (14) transmits the received data to the requesting Relying Party for authentication of the Identity Owner.

Authorisation and service delivery

(15) After having authenticated the requestor, (16) as part of the authorisation process the Relying Party checks which rights are associated with the user's digital identity. If the result of the authorisation is positive, the transaction can be approved and (17) the requested service is delivered to the Identity Owner.



3 What is at stake?



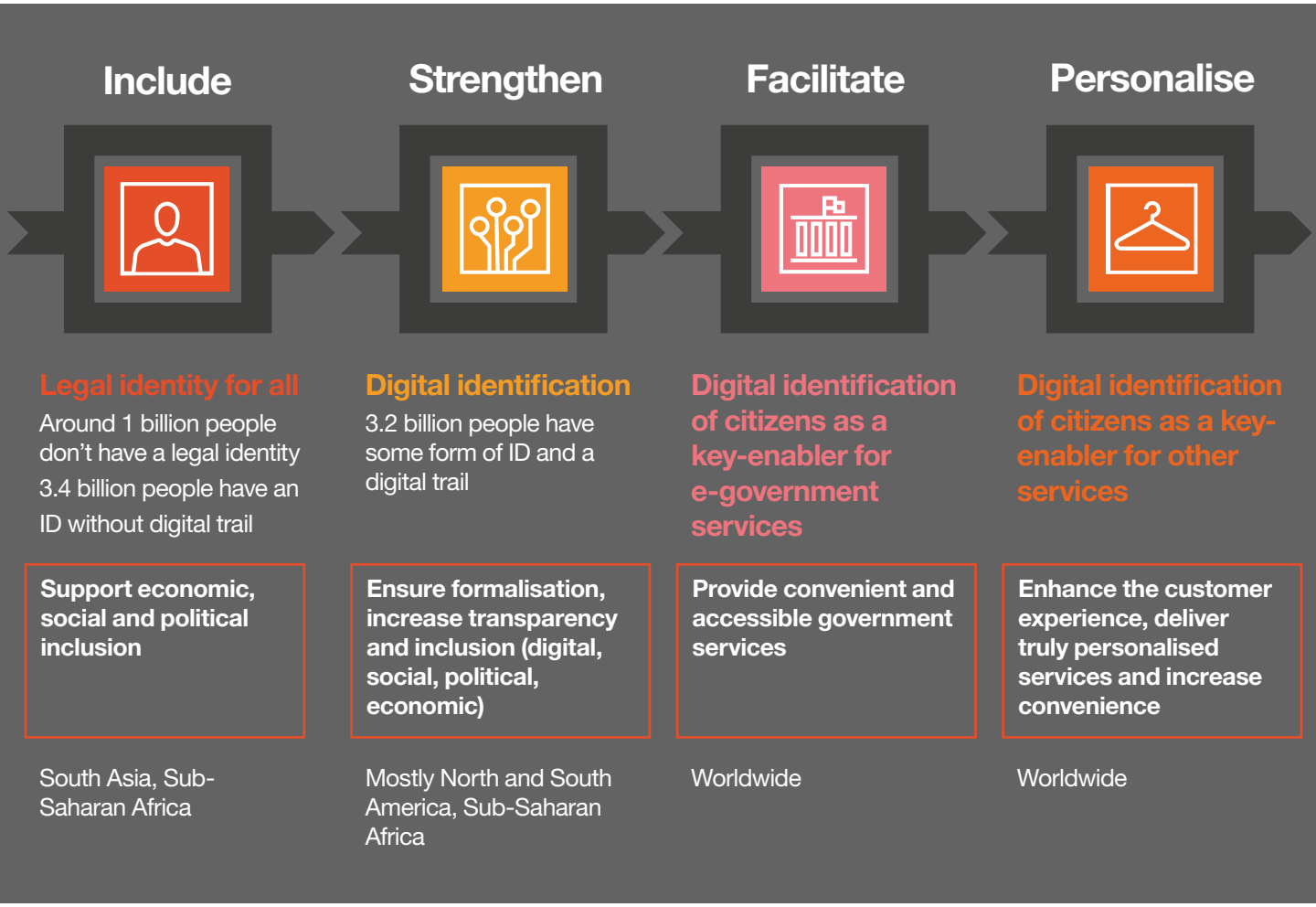
4%
of the World's GDP by 2030, in excess of 5,000 billion USD.

While the previous years have been the years of the blockchain and Artificial Intelligence, there is much to indicate that the next decade will be the decade of Digital Identity. Indeed, while our world has digitised tremendously, we are still lacking the essential trusted link between citizens, businesses and service providers, including governments.

First things first: Digital Identity is expected to unlock around **4% of the World's GDP by 2030,**[1] **in excess of 5,000 billion USD.** Both highly developed countries such as European Union countries and emerging countries have to gain from the emergence of a strong Digital Identity ecosystem.

We can roughly split country maturity when it comes to Digital Identity into 4 different stages, with each subsequent stage bringing multiplying the benefits obtained in the previous stages:

1. *Digital Identification: A Key to Inclusive Growth January 2019. McKinsey Global Institute*



The benefits are tremendous at each stage of maturity, as they support most societal activities, including:

1. Efficient administration
2. Better targeting and inclusion of people
3. Improved delivery of social schemes
4. Reduced fraud, identity theft
5. Enhanced development planning
6. Reduced cost of national initiatives
7. Enhanced tax collection
8. Better border control and facilitated mobility
9. Improved e-services
10. Facilitated participation in the economy

4 A highly favourable environment in Europe

A perfect opportunity to develop Digital Identity in Europe

The context for deploying Digital Identity is particularly favourable. The EU has recently pushed forward several important regulations and initiatives and has committed to strategies that encourage and support a strong Digital Ecosystem. We highlight a few of them:

The European Digital Identity **initiative by the European Commission:** Announced in June 2021, the European Digital Identity will be a EU-backed embodiment of the principles outlined earlier in this whitepaper, and a fantastic opportunity to open the world of safe, secure and convenient digital identities to citizens and customers. Using wallets and credentials to put the person in control of their own data, it will facilitate deployment of cross-border identity initiatives for governments and companies alike. It will also act as a strong catalyst for making Digital Identity the new normal in every home and business.

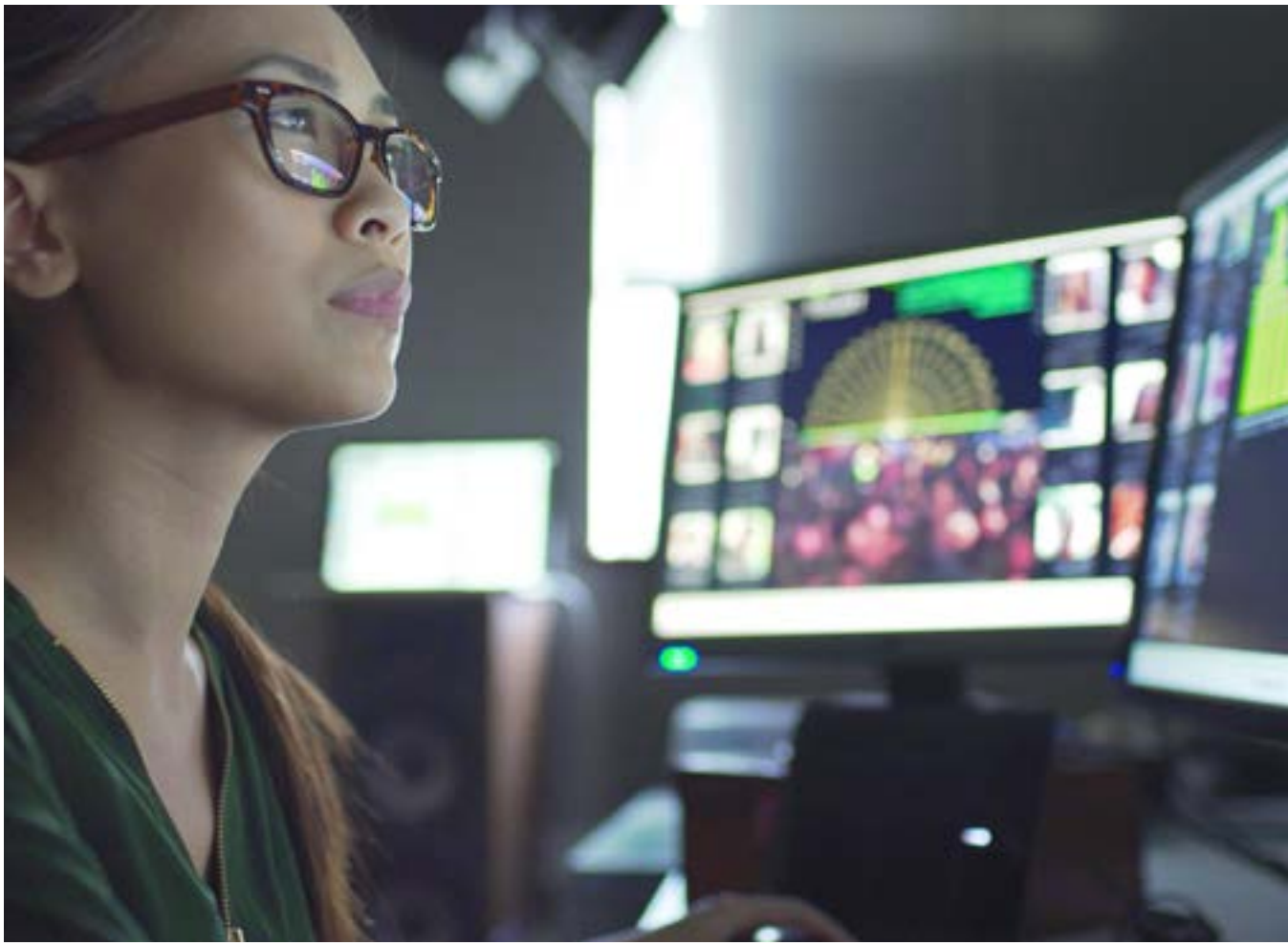
eIDAS:
The Regulation on Electronic Identification and Trust Services for Electronic Transactions (eIDAS), applicable since 2014, is one of the cornerstones of the digital transaction ecosystem. It provides a framework and an infrastructure to provide legal validity for electronic identification in all Member States. Together with the eIDAS bridge which enables trusted and qualified digital signatures to enhance the trust in digital credentials attached to a digital identity, eIDAS is a solid framework upon which a Digital Identity ecosystem can safely be built. Its current revision even brings hope for a universal public digital identity model.

GDPR:
The GDPR applicable since 2018, also fully supports a Digital Identity ecosystem, thanks to its clarification of the ruleset that applies for processing and storage of personal information. It thus greatly reduces uncertainty when it comes to developing Digital Identity programmes. While it may be challenging to navigate, the benefits of doing so are many, including reduced impact in case of cybersecurity incidents and a higher level of trust by users.

Digital Services Act:
The Digital Services Act promises to solve one of the main challenges in enabling pan-European Digital Identity: the lack of harmonisation of rules when it comes to providing Digital Services. Concretely, this means much more certainty for Digital Identity providers about what services they can provide and a larger coverage and targetable user base than ever before under the same rules.

The regulation of 20 June 2019 on strengthening the security of national identity cards of EU citizens, which accelerates the digitalisation of information storage and transmission, including biometric data.

5 Conclusion and outlook



Digital identity has the potential to become a catalyst for the end-to-end digital transformation of a wide range of business and government processes and thereby to increase efficiency, facilitate new products and create enhanced digital client interactions. In its absence, cumbersome and costly in-person identification is necessary in many cases, with existing digital identities inconveniently scattered across a multitude of different platforms.

From a technology perspective, emerging technologies have the potential to take centre stage in superseding today's scattered and outdated legacy identity systems. While biometrics could be used for capturing identity attributes and for authentication, verifiable credentials enable trusted claims to be stored by users, and blockchain technology has the potential to perform essential functions in the overall identity system and thereby mitigate the challenges associated with centralised systems.

In a rapidly evolving technological and legislative environment, it is essential for any organisation to have a clear strategy and positioning with regards to identity management. The privacy, reputational, cybersecurity risks attached with the status quo of storing digital identities in a centralized way are far too great to ignore, and citizens and customers expect their personal data to be protected, or they will bring their business – and trust – elsewhere.

How can we help you?

As a multi-disciplinary practice, we are uniquely positioned to help our clients adjust to the new environment. Our digital identity team includes strategists, consultants, lawyers, digital experts, cybersecurity specialists and technologists. Our global team of experienced business, technology and regulatory leaders can help you identify how digital identity can benefit your organisation and what you need to do to move your initiatives forward and achieve success.

Thanks to our extensive expertise in client onboarding, digitalisation and regulatory matters, we can help you design and implement the best solution for your business, from strategy to execution. Starting with an assessment of your current situation, we determine how your organisation can leverage digital identity to increase efficiency, enhance customer experience, and design and deliver a solution that is tailored to your businesses needs and in line with the relevant regulatory provisions.

1

Assessing the impact of digital identity on your business

Market and company assessment:

Understand your role in the in the digital identity ecosystem and how digital identity impacts your overall strategy (e.g. market positioning, product portfolio and roadmap as well as distribution model).

2

Designing your digital identity operating model

2.1 Mandate for digital identity:

Establish a board level mandate with clear purpose through a common strategy and secure sufficient funding.

2.2 Integrated digital identity solution:

Identify your priorities and align the operating model with your firm's strategy and commercial objectives across the four foundational layers:

- **Strategy:** Go-to-market approach, product portfolio and distribution model
- **Experience:** User journey and flow across all channels (mobile, online, PoS)
- **Process:** On-boarding (incl. compliance checks), authentication and authorisation
- **Technology:** Front end (GUIs, CRM), back end (logic, data) and interfaces
- **Compliance:** Regulations, governance and contractual framework

3

Delivering your digital identity programme

Implementation:

Deploy your change-the-business capabilities to ensure transformation excellence through proven programme management methodologies to deliver your digital identity solution at speed.

4

Handing over to business as usual

Continuous performance:

Complete the transition of your digital identity programme to your Business as Usual organisation and ensure your staff is fully trained and capable to run the delivered operating model.

For more information please contact our experts

Advisory

Serge Hanssens

Partner
+352 621 33 2189
serge.hanssens@pwc.com

Advisory

Frédéric Vonner

Partner
+352 621 33 4173
frederic.vonner@pwc.com

Technology

Xavier Lisoir

Managing Director
+352 621 33 4114
xavier.lisoir@pwc.com