DIGITAL IDENTITY

Restoring Trust in a Digital World

March 2019

mastercard

Table of contents

Executive Summary

This paper presents a vision of how digital interactions will evolve. It describes the role that trust will play in those interactions and explains why Mastercard views digital identity as fundamental to that trust. It proposes an efficient and inclusive model of digital identity that is collaborative in nature, and establishes clearly defined roles and values in a framework of trusted participants. It establishes Mastercard Principles of Digital Identity as key to our system model, design, and service implementation.

Here you will find key propositions that:

- Place individuals at the heart of all of their digital interactions globally
- Create an explicit framework for such interactions
- Present an overview of how an efficient digital identity system will work
- Describe Mastercard's collaborative position within a multi-stakeholder ecosystem
- Deliver best value to customers relying upon digital identity and partners supporting the system

We believe that digital interactions should be privacy-enhancing, secure, intelligent, and efficient. These digital interactions will be made possible by a user-centric digital identity that is owned, managed, and controlled by the individual and that enables the individual to interact with participating organizations. A reusable digital identity service is impossible without the clear understanding, trust, and engagement of the user. Mastercard's system model embodies privacy-by-design, is founded on user-centric principles, and requires no further aggregation of identity data or proliferation of new centralized data structures.

We envision a digital identity service that is simple, smart, and secure:

- **Simple:** Enabling a user and a third party to interact easily, confidently, and with trust
- **Smart:** Allowing digital interactions to occur with only the minimal data exchanged
- **Secure:** Safeguarding data and the use of data effectively such that the rightful owners are in control

Collaboration is at the core of our design for digital identity services. There is no single government, technology company, financial institution, or even industry sector that can effectively deliver a digital identity service by itself. Co-dependence, collaboration, partnership, and orchestration are all required. This enables us to achieve together what is impossible alone. Mastercard is forging partnerships, investing resources, and using our network expertise to make this vision a reality.

We believe that a system based upon collaboration is the best model for managing digital interactions in future. We see our role as an enabler, not unlike the way that we currently enable consumers, merchants, and financial institutions to transact and interact in a secure, convenient, and trusted manner. We already work closely with stakeholders in government, banking, telecommunications, and a range of other primary identity data holders.

Mastercard will not hold personal identity data, but will effectively serve the needs of those relying on the service and their users. Our system aligns with national standards and offers global interoperability. It will allow relying parties to distinctly define their identity verification needs.

Here we explain how.

Digital Interactions

We are helping to shape a world where people and their devices can digitally interact with one another and organizations seamlessly, without unnecessary friction and with confidence; a world where trust can be easily established, and people can be easily recognized in order to gain access to the services or experiences they desire; a world where our digital interactions will be multifaceted, from PCs and smartphones, to connected homes, cars and wearables, and by voice, touch, and presence.

A child born today will not have a bank card, hold a passport, or carry cash. Her first payment device might be her phone, a watch, or an item of clothing. Her signature might be a thumbprint, face scan, or her voice. Ultimately, her ID will be herself.

In one sense, this is a return to traditional notions of identity and trust, where an individual was recognized by sight, name, accent, or other physical trait, and, where necessary, vouched for by a trusted third party. But increasingly the interaction is digital, and our identities are used not only by ourselves, but the plethora of devices acting on our behalf.

This is because the physical and digital worlds are merging. We are never really offline. We have entered an era of hyper-connectivity, where digital services blend invisibly with people's daily lives. It has brought us huge benefits as consumers, producers, citizens, and human beings. Digital services have changed shopping, business, political engagement, health services, and communication.

This is why it is essential to establish and safeguard trust in digital interactions.

Establishing Trust

One current definition of trust is that it is "a confident relationship with the unknown."[1]

In the digital world, there is simply more of the unknown. Yet the organizations offering digital services and the people they are interacting with need to be confident in their interactions within this environment. If this leap of faith is to be rewarded, then trust has to be at the heart of the system.

Digital identity is about establishing that confidence and trust at both ends of the interaction. Each party needs to be confident that the party at the other end is who they say they are. And both require trust in the system that mediates that interaction.

Imagine a world where a person's identity and the devices operating on their behalf can be verified immediately, safely, and securely, across multiple touchpoints and in both the digital and the physical world; where access is gained without passwords and data is exchanged only with consent; as simple as saying: "Hi, this is me." This is the future we are making possible.

Enabling Trust

How do you trust someone you don't know, can't see, and isn't actually present in person?

Identifying oneself has traditionally been anchored in the mechanisms of the physical world, whether it's presenting a passport, proof of address, driver's license, or attendance in person. For the more than five billion human beings online, digital authentication is burdensome and unreliable; think of the hundreds of accounts, passwords, and memorable (or forgettable) data you've accumulated.

An average user can be faced with 150 login accounts to manage,[2] all with disparate approaches to passwords and authentication. Yet identity fraud is increasing and has become a far bigger problem online than it is offline. These risks multiply in the Internet of Things (IoT). Within a few years, there'll be 50 billion[3] connected devices and sensors, each one presenting a potential security vulnerability for the people dependent on them.

On the other hand, more than a billion people are not on the identity grid at all. They are too remote or difficult to reach and do not interact with mainstream agencies and government institutions. As a result, they are almost impossible to serve.

There is a clear need for a verified identity that is accepted globally and across multiple digital touchpoints; one that doesn't involve aggregating more information in potentially vulnerable data stores, but instead gives the individual control over the collage of data that is used to verify their identity. For example, something that allows an adult to prove they're old enough to buy age-restricted products without revealing a date of birth. Or allows them to rent a car without producing a license, travel without a passport, or take out a mortgage without a bundle of paper bank statements.

So what is holding things up? Some countries have developed their own systems of digital identity. But these are disparate, national schemes. Finding something that works for every country and across borders is a greater challenge.

Nobody today expects to use a different credit card for every shop they enter, or each country they visit. It just works. A network approach already exists to facilitate the secure exchange of data between banks, merchants, governments, and consumers. For digital identity to work, it, too, requires commercially focused innovation, standards, interoperability, and the trust of stakeholders.

Enabling Trust

Key Issues

Users

The identity we use to interact with government, access services, and pay for goods is vulnerable. Fraud and identity theft often only require the breach of a single database. Individuals have to repeatedly provide large amounts of personal information to numerous agents, and the more it is shared the greater the risk. People are juggling multiple passwords in an attempt to keep safe their identifying data, credit, and money. They lack control over their personal identity data. Where they do have rights, there is often little transparency.

Organizations

The absence of a simple, safe, and reliable way of authenticating identities digitally creates friction, increases fraud, degrades privacy, and restricts access to services.

Inclusion

A large proportion of the world's people has no trusted identity credentials to prove who they are; and they are often those most in need of it. The poorest 40% have the least access to proof of identity.[4] More than one billion people lack a basic, verifiable birth certificate—they are not on the "identity grid." The United Nations has stated that without official identification, there is no financial inclusion, health inclusion, citizen inclusion, or digital inclusion.[5]

Data Breaches and Identity Theft

In the United States alone, there were 16.7 million victims of identity fraud in 2017,[6] at a cost of $16.8 billion. In the same year, there was a 44.7% increase[7] in the number of data breaches. Most breaches were identity theft incidents[8] and $6 billion was lost to "synthetic" identity fraud in 2016, when criminals "synthesize" real-looking fake identities by combining real data from multiple individuals.[9]

Defining Digital Identity

During 2018–19, Mastercard gathered leading experts and interested parties from around the world with a view to exploring the opportunities presented by digital identity.[10] This exercise supplemented our own discussions with governments, partners, and other stakeholders—and our longstanding expertise in the fields of authentication and verification—helping us to sharpen our own definition of digital identity.

We see digital identity as being grounded in a collage of data that defines the individual. This collage of data, when bound to the individual, verified, and made securely accessible while under a user's control, is the essence of digital identity. Its primary purpose is not just to identify somebody, but more importantly to confirm their entitlement to access a service or perform a particular task.

In our view, digital identity is:

- a collage of up-to-date, high-fidelity digital data that defines an individual
- dynamic, multipurpose, and reusable
- a method of verifying information to establish entitlement to access a service, perform a task, or receive a benefit
- the consequence of a dynamic network of distributed data sources (e.g., financial institutions, mobile network providers, governments) that verifies identity as it is required

Digital identity can include:

- name, date of birth, address
- biometrics (e.g., fingerprint, face, voice)
- attributes (e.g., passport number, social security number)
- certifications (e.g., doctor, pilot, university degree)
- dynamic data from (e.g., financial institutions, retail, mobile) interactions

Digital identity is more than:

- a digitized passport, driver's license, or national ID card
- a password replacement
- an online profile

A Principled Digital Identity

Our Commitment to the Individual

People currently pay for their digital interactions with data and privacy. Each day, they are asked to provide personal information simply in order to access basic digital services. They often don't know where that data is stored, how secure it is, how it might be further traded, and who is profiting from it. This is a bad deal for the individual.

Privacy regulations such as the European Union's General Data Protection Regulation (GDPR) have helped to restore some trust and provide a welcome environment for modern identity infrastructures.

Mastercard believes that the framework for digital interactions is so important that we've drafted our own principles to guide thinking on this. They place the user in control and address issues of privacy, ownership, transparency, security, and several other areas.

It boils down to this: *The individual owns their identity and controls their identity data.*

A Principled Digital Identity

Mastercard Principles of Digital Identity

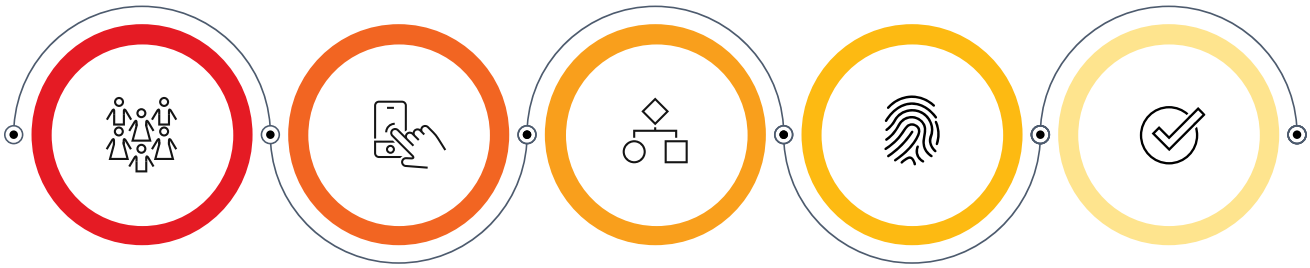
Inclusion
Everyone has a right to a digital identity

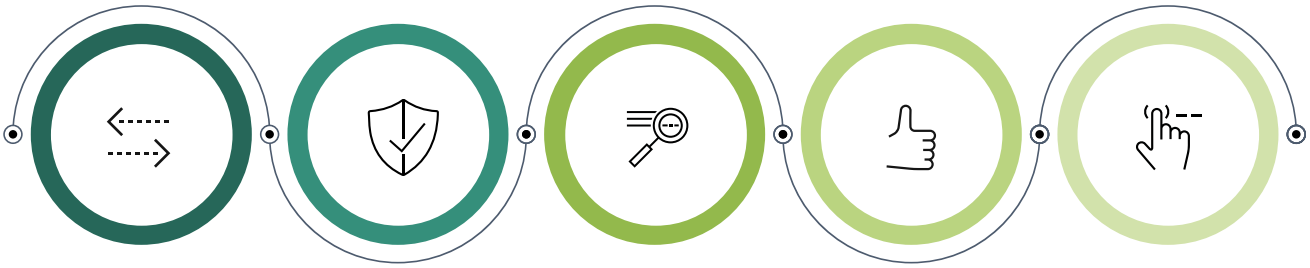
Ownership
Individuals own their identity and personal data

Simplicity
An individual's use of their digital identity should be simple and intuitive

Confidentiality
An individual has the right to keep their digital identity information private

Consent
An individual's digital identity should not be used or shared without their explicit consent, or as permitted by law





Transparency
Individuals have the right to understand how their digital identity data is used and shared

Security and Integrity
Identity data and transactions that involve an individual's digital identity should be held with the highest standards of security and integrity

Data Rights
Individuals should have the right to access, correct, and delete their identity data and the right to recourse if their rights are violated

Fair Use
An individual's identity data will be used only for legitimate, fair, and non-discriminatory purposes

Choice
Individuals should have a choice of trusted digital identity providers and the right to opt out or to change providers

A Principled Digital Identity

• User-Centric

We believe there should be no trade-off between convenience and privacy. We are focused on a digital identity service that will be global in scope, sensitive to local needs, interoperable between institutions and sectors, and ensures that people are the guardians of their data.

Digital identity is about far more than technology. It defines an individual in the digital world and, as such, needs to be underpinned by a principled framework as well as a supporting commercial service. Placing the individual at the center of digital identity ecosystems is essential. Our guiding principles promote trust and understanding while restoring control of personal data to the individual.

Access to a user-centric digital identity will unlock new and enhanced experiences for people as they interact with businesses, service providers, and communities. This includes:

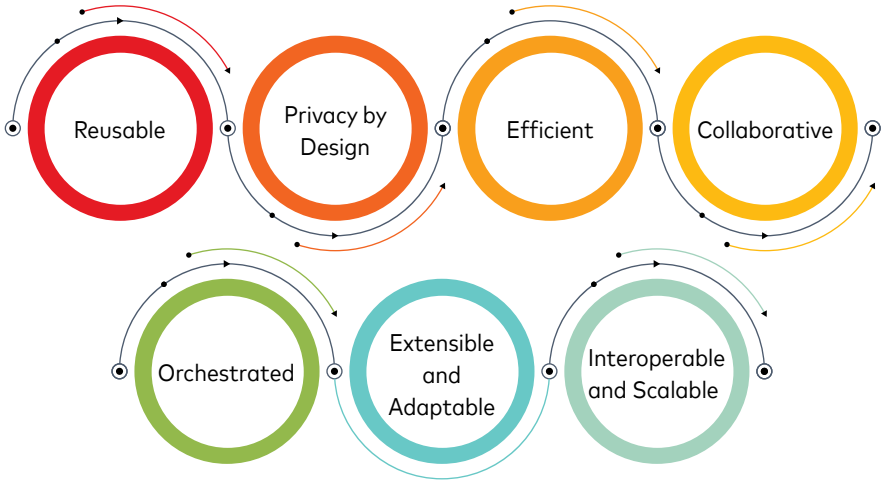
- **Financial Services:** Improve and speed-up the applicant identification process for establishing a new bank account, loan, or payment service account
- **Commerce:** Enable a more personalized and efficient shopping experience remotely and in stores, regardless of the payment type, device, or service provider
- **Government Services:** Simplify interactions with government agencies and services—such as filing taxes, applying for passports, or receiving benefits
- **State Benefits:** Verify entitlement and reduce fraud
- **Health Services:** Improve the interconnection of data services across providers while retaining user control
- **Digital Services:** Streamline and provide easier use of email, social media, movie/music-streaming services, and ride-share platforms
- **Internet of Things (IoT):** Enable devices and sensors to interact securely with and on behalf of the individual

A Principled Digital Identity

Responsible System Design

We are changing the way that people establish identity in a digital world; one that moves from:

- bespoke, niche, and closed systems to **transparent, globally interoperable services**
- over-sharing of data without transparency to data sharing **controlled by the user**
- use of static identity data to **dynamic and biometric identity data**
- hundreds of vulnerable passwords to a **reusable digital identity** that works everywhere
- a selective system excluding the poor to an **inclusive system for all**

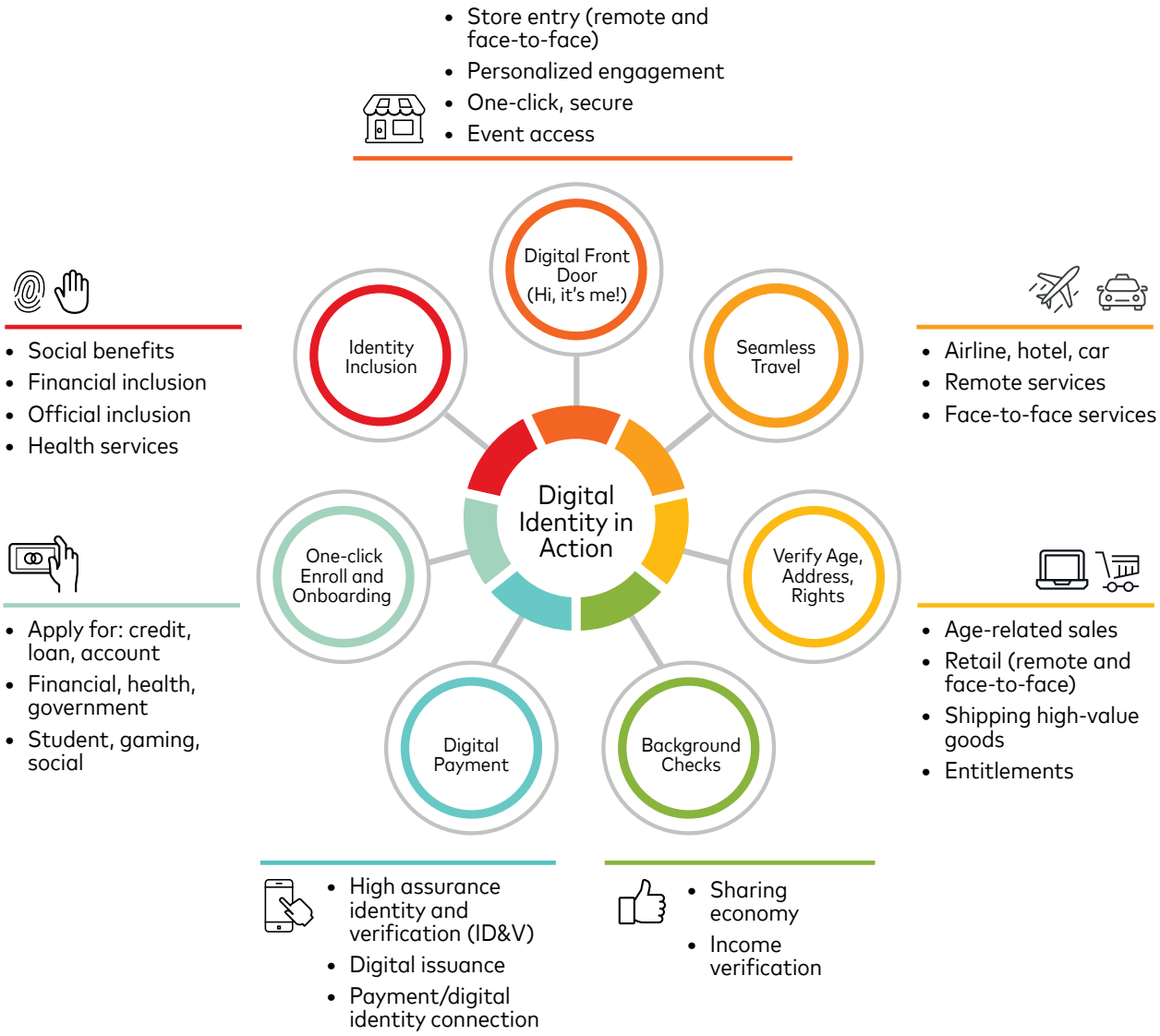


Mastercard believes this is best achieved by a responsible system design in line with our principles and core objectives:

- **Reusable Digital Identity:** Eliminating the need for multiple passwords and identity-verification procedures. A digital identity would allow people to use a single means of authenticating themselves across multiple digital services, encompassing websites, apps, devices, and more
- **Privacy by Design:** Enabling users to protect their data and experience transparency in the management of their digital lives
- **Efficient:** Helping to roll out new value-added services, improve engagement, cut friction, lower identity service costs, improve security, and meet regulatory requirements
- **Collaborative:** Working with technology and operational stakeholders to define standards and regulations
- **Orchestrated:** Replacing the aggregation of data with an orchestrated ecosystem of distributed data
- **Extensible and Adaptable:** Structured around a core that can be deployed in whole or partially, according to local country standards, regulations, and norms
- **Interoperable and Scalable:** Seamless digital interactions for the individual, enabling secure interaction between official data infrastructures and participants in the private sector, while meeting defined standards of functionality, performance, security, and other regulation that may be in local markets

Digital Identity in Action

Every hour, millions of digital interactions take place that require verification or authentication of identity. They are both simple, such as a PC login, and complex, such as a mortgage or visa application. In each case, a reusable digital identity can provide a mechanism to dramatically improve the experience for both individuals and the providers of digital services they seek.



Digital Identity in Action

Case Studies

Easing the Burden of Proof

People value speed and convenience, but expect to be kept safe. This doesn't have to be a trade-off. Digital identity accesses and presents only those credentials that are required for each task. Entering the digital front door by logging into a website or app? Do so simply with a digital identity that states "Hi, it's me." Board a plane? Use your fingerprint, rather than passport. Collecting a parcel from the post office? Do so without a driver's license.

Digital identity confirms an individual's right to access a particular service without disclosing unnecessary data. It does this by securely accessing from trusted sources only the minimum data required. Where the stakes are low, proving identity should be simple; like the face-to-face recognition that used to be good enough for your local bank manager or doctor. Digital identity applies that simplicity and recognition to the digital realm. Complex checks are reserved for interactions with higher stakes and more risks, such as proving eligibility for a mortgage or accessing medical records.

CASE STUDY

Ella employs her digital identity in different ways. At bars, she uses it to prove she's old enough to enter, without having to show a driver's license that would reveal her name, address, and date of birth. She uses her digital identity to enter her office building, instead of a staff pass, and to order her prescription medication online. But she can also use her digital identity to sign up to loyalty and rewards programs, subscribe to magazines and dating sites, create social media profiles, and share her favorite music. It is Ella's decision about where to use her digital identity, which data to make available, and to whom.

Local Solutions with Global Interoperability

Digital identity schemes are already underway in places such as India, Estonia, Canada, Belgium, and the Nordic countries. But these platforms are neither global nor interoperable, and their use outside of government interactions is often limited or non-existent. Without agreed-upon standards and interoperability, digital identity cannot scale beyond regional deployments. Mastercard believes in local solutions that can also interact with a global service. Scale is key to inclusion. We are working closely with governments to achieve this.

CASE STUDY

Michael is relocating abroad to start a new job. He needs an address in the new country in order to open a local bank account. But to rent an apartment, he needs a local bank account. With a globally recognized digital identity, he can prove who he is and provide his credit history and verified personal information from his previous posting.

Fraud Reduction

The absence of a simple, safe, and reliable way for entities to verify identity through digital channels creates friction in commerce, degrades privacy, and restricts access to services. It also creates a fertile ground for digital fraud, which is four times higher than the physical fraud rate.[11] Digital identity addresses this by embodying technological methods of identity verification, which have reached new levels of accuracy and which work across multiple devices and platforms.

CASE STUDY

Rahul was a victim of a major data breach at a credit rating agency. Fraudsters stole all the data he used to prove who he was: name, date of birth, passwords, memorable information, etc. That data was used by others to create new accounts, borrow money, and in doing so undermine his credit rating. Now he has a digital identity and the data required to assess his credit worthiness for a loan is no longer stored in a single place. Instead, with his permission, different elements are presented securely on an as-needed basis.

Improved Commercial Interactions

There are many aspects of identity involved in commercial transactions. Digital identity can dramatically reduce friction in e-commerce, facilitate one-click account creation, and significantly simplify Know Your Customer (KYC) and onboarding processes.

CASE STUDY

Jemma had so many online logins that she lost track of her usernames and passwords. With her digital identity, she can quickly and easily log into all her accounts, enjoys one-click account creation, and straightforward address and age verification. She recently started a new job and opened a new bank account and was swiftly and securely onboarded for both with minimum paperwork.

Inclusion

Identity is what makes our existence in the world official. It's how we are recognized and how we establish our entitlement to the benefits of citizenship. Yet more than one billion people lack a basic verifiable birth certificate. They are absent from the grid. In countries where large swathes of the population have no existing government identity, they are unable to access state services, open bank accounts, or register with doctors. Furthermore, there is a stark socioeconomic divide between those who are digital-enabled and those who are not. In response, United Nations Sustainability Goal 16.9 was established with the aim of providing a legal identity for all by 2030. Digital identity provides a fast, efficient, and less fraud-prone solution to inclusion. In areas where fraud is rife and records are inefficiently maintained, digital identity has a real opportunity to improve the lives of people and help combat fraud, human trafficking, and other organized crime.

CASE STUDY

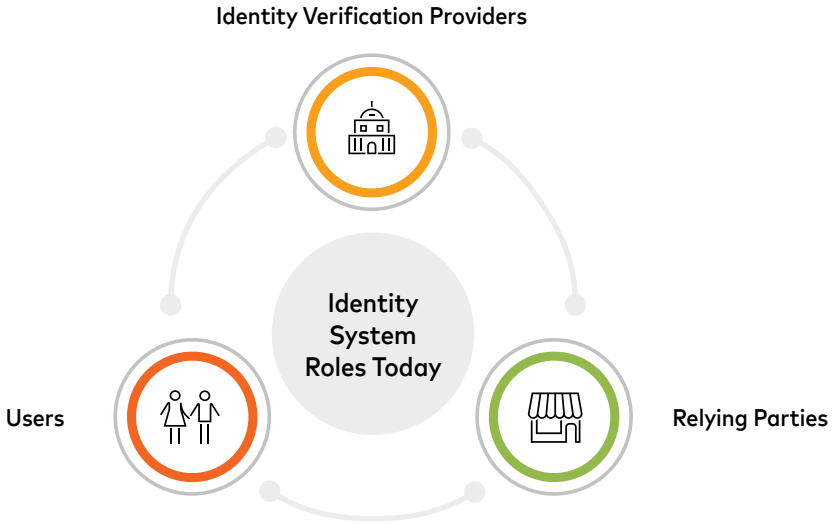
As a mother with limited income, Anya is entitled to financial assistance from the state. Previously, she was unable to access this because she didn't have an official identity recognized by state institutions. Since signing up for a digital identity, however, Anya can claim the benefits directly. The funds are applied to a prepaid debit card secured by her fingerprint. She uses the same digital identity to open her own bank account and register with a doctor.

A Collaborative System

Developing Trust in an Identity Transaction

How have we asserted and verified identity over the years?

It often works like this. Someone might say: "My name is Bob, I was born in Sydney on 29th September, 1985, and I live at this address." However, someone who doesn't know Bob needs a way of verifying that statement. They can do that through those who do know and trust Bob—one or more third parties that can back Bob's claim. In our system, we call the person who doesn't know Bob a **Relying Party** and those who do know Bob **Identity Verification Providers**.



To turn these relationships into an effective digital identity system, a **User** also needs the necessary tools to enable them to manage and present their identity data. Where there are millions of users, relying partners, and identity verification providers who need to interact with one another, those relationships require orchestration.

These challenges are met by the introduction of two other roles: **The Trust Provider** and the **Digital Identity Service Provider**. The trust provider ideally has a preexisting relationship of trust with the user—its brand acting as a bridge to a digital identity service. It might be the user's bank, for example. The trust provider also supplies the tools and service connectivity for users to register for, use, and manage their digital identities.

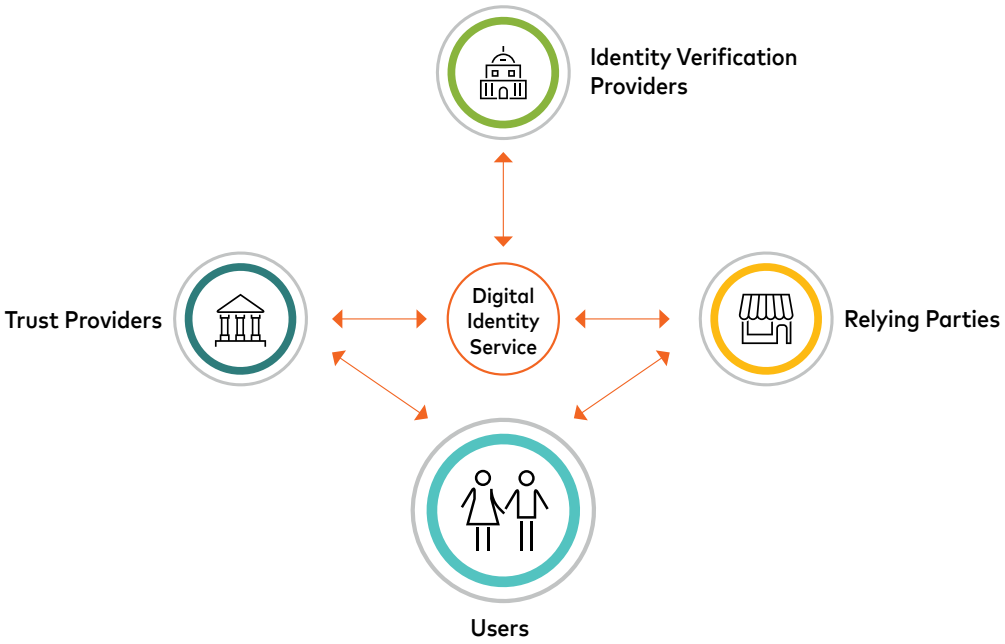
Service orchestration is performed by a **Digital Identity Service Provider**, which establishes the technical interactions, value and economic exchanges, service-level agreements, and liability allocations for this digital identity network. It also creates a commercial market for the digital identity service.

Together, the integrated operation of trust providers, identity verification providers, and the digital identity service provider creates an identity network with the kind of broad user coverage that no single body could provide alone.

A Collaborative System

Digital Identity System Roles

- **Users** who are making an identity assertion
- **Relying Parties** that rely upon the identity assertion of the User
- **Identity Verification Providers** that verify aspects of a User identity assertion
- **Trust Providers** that provide the tools and service connectivity for the User
- **Digital Identity Service Provider** responsible for service orchestration, market organization, and standards



This digital identity system is role-based, allowing existing market stakeholders to efficiently interact with and deliver value to the key participants—the user and the relying party. It is a user-centric, distributed digital identity system with the addition of a commercial framework that aligns the interests and motivations of stakeholders.

Key Features:

- Users cannot simply self-assert; they gain the confidence of the relying party through the actions of multiple identity verification providers
- The provision of a commercial framework and business roles provides incentives for identity verification providers to participate
- A user requires tools, such as an app, which a trust provider, such as a bank or mobile network operator, can provide
- A reputable digital identity service provider is necessary to give all participants the confidence and assistance they need to navigate a complex multi-stakeholder digital environment
- The relying party receives simple and trustworthy assurance about users and their data in a cost-efficient, scalable way

A Collaborative System

Delivering Value

Mastercard's objective is to bring together stakeholders to realize the collective values possible only through collaboration. The key advantages of this model are as follows:

User-centric Data: The system model establishes the user's personal data store on their mobile device along with verification and use results. This provides for a highly resilient, distributed identity infrastructure—eliminating any need for a centralized identity database.

Role-based: The model allocates function and responsibility. This allows a financial institution, mobile phone operator, government, postal service, and other stakeholders to play to their strength in a manner that minimizes entry expense and risk.

Identity Verification Providers: The identity verification providers best-suited to such a system are those that have the most authority to confirm a discrete identity attribute of a user. For example, the passport authority is best-placed to confirm the validity of passport data, the postal service to confirm the validity of an address, and the mobile network operator to confirm details of a smartphone device. Selecting those best-suited yields efficiency to the system and ensures the trust of other stakeholders. Organizations such as financial institutions, mobile network operators, postal services, educational institutions, governments, and others also have the trust of users. This qualifies them to participate and creates a substantive role for such organizations.

Trust Providers: In many geographic markets, the user's digital relationship with a retail bank represents an ideal trust provider relationship. Users of smartphone banking apps will also be those predisposed to use a digital identity. Banks have already made the security investments necessary to authenticate the user and are among the institutions most trusted with personal information. In different markets and among different users, the mobile network operator, postal service, or even a university, for example, may represent appropriate trust provider options.

Relying Party: The purpose of the system is to bridge the trust gap between relying parties and their user customers, especially in digital interactions. The relying party is the primary customer in such a system, paying for digital identity services in exchange for verified identity assertions and ongoing authentication services.

Governments: Governments set national standards for identity. By partnering with the private sector, they can create efficient, fair, and compliant digital identity services. This creates a common good for both users and organizations. Governments can also benefit by being able to provide citizens with greater accessibility to better services at lower cost.

Multiple Roles: Some system participants may play more than one role. A bank might act as a trust provider, serve as an identity verification provider (based upon account onboarding data), and conversely might rely upon a verified digital identity as a relying party. A government might act as an identity verification provider and might also be a customer for verified digital identity services as a relying party.

Varied Interaction Modes: While digital identity transactions may occur face-to-face, assisted by digital technologies, many such transactions may also be conducted remotely. In such cases, it is important to be able to confirm that the user is actually "Bob" and not a bot or fraudster.

Most Economically Efficient: With each participant performing the role most suited to it, the cost of establishing a digital identity system is minimized for all involved.

The Role of Technology and Standards

Core Technologies

While the core technologies required for an effective digital identity ecosystem exist, harnessing it in a manner that ensures efficiency, effectiveness, and sound ethics is more of a challenge. Mastercard has considerable experience applying technology in the kind of extensible, adaptable, and standards-compliant manner needed to ensure a trustworthy foundation for digital interactions.

Biometrics

As the identity verification market evolves to address the vulnerabilities of static identity data, the ethical use of biometric identity data has become more important. The verification of user biometric data, liveness detection, and associated security processing are key areas of innovation and application.

Security by Design

The use of modern cryptographic and key management methods is essential for trust in the system. This includes securing identity data through the verification process, ensuring the integrity of identity verification assertions, protecting data held by a user and the system-wide adoption of layered security technologies within devices, cloud services, distributed ledger services, and at the interfaces between parties.

Endpoint Devices

The current and future requirements of 7.5 billion people around the globe must be well-considered. Our digital interactions will encompass a diversity of devices operating as part of an intelligent digital mesh. Securing these endpoints with encryption and biometrics and ensuring the privacy-enhancing application of user identity data is central to a sound system service design.

Distributed Ledger Technology

A secure, distributed technology based upon the use of blockchain provides an immutable and transparent record of digital interactions resilient to denial-of-service attacks. The application of this technology in a manner that preserves core security and privacy principles merits further consideration.

The Role of Technology and Standards

• Standards

Framework

Current regulation around privacy and open data provides a supportive framework for effective digital identity services, as does ongoing work at national and regional levels, such as with the European Union's Electronic Identification Authentication and Trust Services (eIDAS), the National Institute of Standards and Technology (NIST) in the United States, and a number of other bodies. Regulators should ensure that they continue to accommodate the commercial involvement of an innovative private sector. Lastly, technology standards for identity services are necessary to ensure broad adoption. We welcome in particular the work of the Decentralized Identity Foundation (DIF) for distributed identifiers, the Worldwide Web Consortium (W3C) for verifiable claims and the Open ID Foundation in driving open identity standards.

Collaboration

A collaborative approach is necessary to establish the core of a commercial, operational digital identity infrastructure, and this is particularly important with regard to the technology used. Mastercard is currently collaborating with best-in-class technology partners across the industry to build and evolve world-class digital identity services.

Extensible

Our model supports the participation of existing identity data providers and national identity schemes, as well as accommodating the development of third-party identity-reliant apps in fields such as health and financial services.

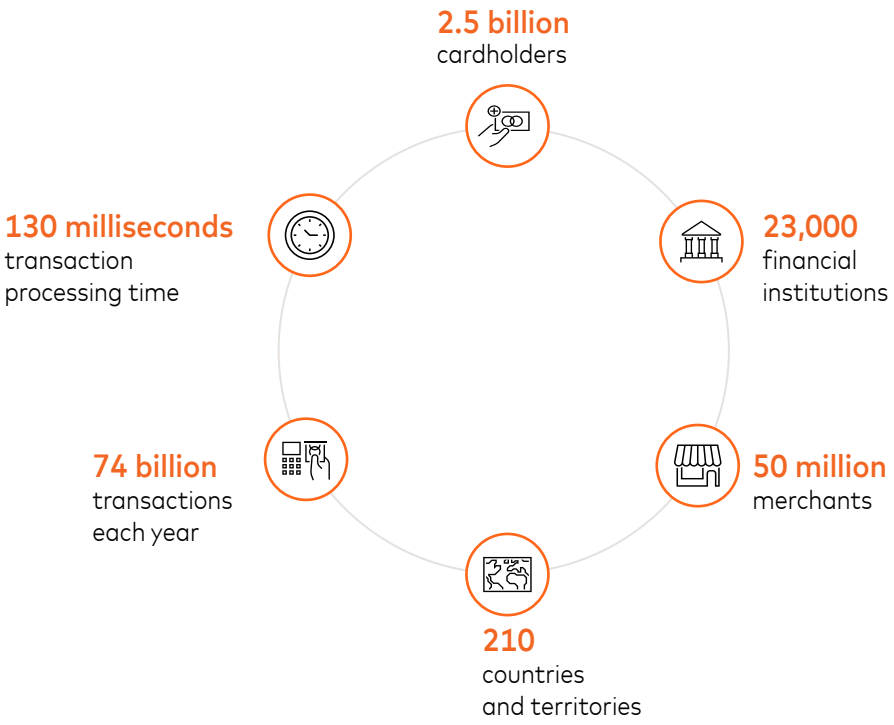
Mastercard's Role

For more than half a century, Mastercard has worked with partners to develop a model for payments that brings together consumers, merchants, financial institutions, governments, and technology providers.

There are clear parallels with the complex multi-stakeholder orchestration required by a global digital identity service. In payments, the mutual exchange of identity marks the beginning of the interaction between consumer and merchant. The framework currently underpinning financial transactions across the globe is the closest thing we have to an interoperable system of authentication and identification, according to the World Economic Forum.[12]

Mastercard is investing in an ecosystem for trusted digital interactions. We are creating a new digital identity system that works for everyone. One that is more secure, more inclusive, more convenient, and does a better job of protecting people's privacy.

What's more, we are uniquely positioned as a user champion for digital identity, given our experience in governance and operating networks, our focus on financial inclusion, our sensitivity to data privacy, and our commitment to investment in a global infrastructure. Mastercard will facilitate the service platform and network, help define the operating rules and governance, establish contracts across the network, and attract and service customers and partners.



Mastercard's Role

Mastercard Key Assets

Globally Interoperable	An identity network designed for cross-border interoperability across more than 200 countries enables a user's digital identity in one country to be recognized in another country at a desired assurance level.
Global Service Provider Acceptance	Global brands that operate in local markets seek globally recognized digital identity service providers to build scale and ubiquity.
Network Infrastructure and Governance	With proven expertise in building and operating a large global payment network, Mastercard is able to provide a scalable network service for digital identity. Defining network scheme rules, legal contracts, and governance in close collaboration with identity system stakeholders is a critical function. Mastercard leads in this field.
Efficient System Model	We have defined a highly efficient system approach by using multiple authoritative sources of identity attribute verification. By leveraging the strengths of each network stakeholder based upon their existing core business and data assets, the model minimizes the cost of delivering verified identity claims—thus accelerating market adoption.
User Choice	By enabling a network of multiple trust providers, we give users a broad choice of providers from the start.
Invested and Committed	Mastercard is investing to build and operate a commercial scheme for all network participants, which includes financial, technical, liability, security, privacy, and operational rules. This is global in scale, interoperable, and adaptable to local conditions.
Market-maker	With 50 million merchant relationships worldwide, Mastercard is in a strong position to create markets for digital identity acceptance.
International Service Provider Support	By leveraging an existing global network support infrastructure, we can support the identity network at the least cost.
Privacy and Security by Design	The Mastercard Principles of Digital Identity represents our commitment to users, customers, and partners.

Conclusion

The current pace of technological change is unprecedented. Consider the extent to which the internet, smartphone, microchip, and personal computer have transformed the world in a single lifetime. In contrast, thousands of years separate the invention of the wheel, the printing press, and the first manned flight.

In historical terms, our digital interactions have evolved in the blink of an eye. This has inevitably challenged the notions of identity, trust, and privacy with which we have traditionally anchored ourselves in the physical world.

Various concepts of digital identity often fail to meet this challenge because they are insecure, mutually incompatible, or lack the confidence of users necessary to create trust. But orchestrated and interoperable digital identity systems can provide us with safe, secure, and reliable digital interactions. Existing networks that have evolved to facilitate trusted digital financial transactions provide a model for how this will be achieved.

Furthermore, it is critical to underpin digital interactions with a set of principles that from the beginning places individuals in charge of their digital identity while providing confidence to those with whom they interact.

This is being achieved through a collective effort by both existing stakeholders and new innovators in the field of identity. No single body has the means, the infrastructure, or market position to succeed alone. Nor should it. The task is too important.

Glossary of Terms

Decentralized Identity: An identity system model that places ownership of identity with the individual.

Decentralized Identity Foundation (DIF): An organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity.

Digital Issuance: Credit/debit facilities provisioned direct-to-mobile wallets.

Digital Identity (DI): Collage of verified data that confirms the identity of a subject (user, other).

General Data Protection Regulation (GDPR): EU 2016/679 is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Electronic Identification and Trust Services (eIDAS): Commonly used abbreviation for regulation EU 910/2014. The European Parliament and the Council of the European Union's regulation on electronic identification and trust services for electronic transactions in the internal market.

Identity and Verification (ID&V): The process of verifying the identity of a user.

Identity Verification Provider: An organization that naturally is able to verify user identity data, such as a government (for passport), mobile network operator (for phone location), postal service (for address), financial institution (for core identity data from KYC actions).

Internet of Things (IoT): System of interrelated computing devices, mechanical and digital machines, objects, people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Know Your Customer (KYC): Process for banks or others to verify identity of customers, typically tied to regulatory or other business policy requirements.

Mobile Network Operator (MNO): Organizations that provide mobile phone and data services.

National Institute of Standards and Technology (NIST): United States standards body.

Relying Party (RP): The term used to describe the organization that provides user application services (e.g. a retail bank, an online pharmacy, or airline) through a digital experience and that relies upon a digital identity.

Trust Provider (TP): A provider that delivers direct users the capability to register for a digital identity, and manage the lifecycle of that digital identity and interactions.

Worldwide Web Consortium (W3C): An international community where member organizations, a full-time staff, and the public work together to develop web standards.

References

1. "Who Can You Trust?," Rachel Botsman, 2017, Portfolio Penguin.
2. "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services," Virginia Tech, 2018.
3. "The Internet of Things: Consumer, Industrial & Public Services 2018–2023," Juniper Research, 2018.
4. "Identification for Development, Africa Business Plan," World Bank Group, 2018.
5. United Nations Sustainability Goal 16.9 was established to provide legal identity for all by 2030.
6. "2018 Identity Fraud: Fraud Enters a New Era of Complexity," Javelin Strategy & Research, 2018.
7. "Better Identity in America: A Blueprint for Policy Makers," Better Identity Coalition, 2018.
8. Breach Level Index, Gemalto, 2018.
9. Synthetic Identity Fraud Working Group, Auriemma Group, 2017.
10. "Future of Digital Identity: Insights from Multiple Expert Discussions Around the World," Future Agenda in partnership with Mastercard, 2019.
11. Mastercard, January–November 2017.
12. "A Blueprint for Digital Identity," World Economic Forum, 2016.