DIGITAL IDENTITY

Building Trust in a Digital World

Our Service

February 2020

A service by

As individual lifestyles become digital-first, organizations in the digital ecosystem—financial institutions, merchants, governments, service providers, and more—recognize the need for a globally interoperable service that seamlessly, securely connects every party.

Mastercard heard these concerns and responded with a vision for digital identity grounded in collaboration and user-centric principles. This vision was outlined in our white paper, Digital Identity: Restoring Trust in a Digital World.

Now, Mastercard has introduced its digital identity service—ID—built upon those principles. ID will enable people to quickly verify their identity in every interaction, anywhere in the world. To learn how ID gives individuals more control and privacy, while enabling organizations to deliver services with less friction, more confidence, and greater trust—we present this new white paper.

Table of contents

Introduction

The problem

How do you trust someone you don't know and can't see? Traditionally, identification has been anchored in the physical world, such as presenting a passport, proof of address, or driver's license in person. But today more than five billion people conduct at least part of their lives online, where digital interactions require burdensome processes around identity verification.

The average online user must manage scores of logins, passwords, and authentication procedures

Yet online identity fraud and data breaches continue to increase

Risks multiply in the Internet of Things (IoT), as individuals may lose control over their data

At the other extreme, more than a billion people are completely absent from the identity grid, living in remote or difficult-to-reach locations. They do not interact with mainstream agencies and government institutions, limiting their access to identity services.

The challenge

How do you give individuals more control, with less friction and risk? There is clear demand for a safe, convenient way to create a verified identity that is accepted globally and across multiple digital touchpoints:

It should enable the individual to control how their data is used

It shouldn't place personal information in potentially vulnerable data stores

It should be convenient and frictionless

An adult should be able to prove they're old enough to buy age-restricted products, rent a car, travel, or take out a mortgage without having to produce a bundle of paper documents or reveal unnecessary personal information.

The solution

Imagine a world where your identity can be verified immediately and securely in both the digital and physical worlds, where access is gained without passwords, and data is exchanged only with consent. Mastercard has created **ID**—the first globally interoperable digital identity service—to make that vision a reality. ID is designed to:

Create trust with Users in digital interactions

Give individuals more control

Deliver services with less friction and more confidence

ID is convenient

ID quickly verifies the User when it matters most, so they can do the things they want and need to do—more quickly and easily with ID

ID is secure

ID uses facial biometrics to make sure only the User can access and use their data, and data is never stored in a central database that could be hacked by others

ID is smart

With ID, Users are in complete control of their data and how it is shared: Users choose what to provide and control where to share it

ID is being brought to market by Mastercard. Why? Because a workable digital identity service requires commercially focused innovation, governance, interoperability, and the trust of all stakeholders. Mastercard has built the world's leading global payments network to facilitate the secure exchange of data between financial institutions, merchants, governments, and consumers. And we're bringing those same high standards of quality, reliability, security, and privacy to the multi-party network model required for digital identity.

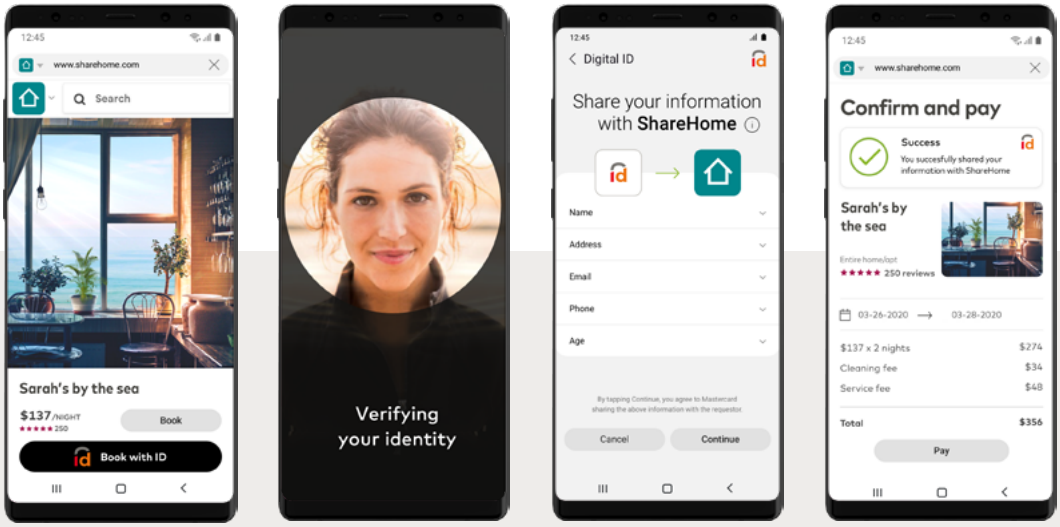
A better way

For a citizen, consumer, student, parent, gig worker, or business traveler, ID provides a better way to establish and use a digital identity across a wide range of use cases, reducing hassle and friction in everyday tasks as well as other important interactions, from arranging a family vacation to enjoying a music concert to visiting a doctor to applying for a job.

In a simple example of booking a vacation rental in the sharing economy, an individual would select the ID option when ready to proceed with the rental, unlock their ID using their facial biometrics, and agree to share the specific information requested by the vacation rental company. This three-step process replaces the lengthy and less secure experience of creating an account with a password, providing a large amount of data manually, and performing additional checks to verify the identity.

Illustration: User books vacation home with ID service on Relying Party app

Not actual screens



The User finds their desired property and taps "Book with ID"

The User unlocks their ID on their device using facial biometrics

The User reviews and decides to share their information

The User is returned to the rental app and completes the booking

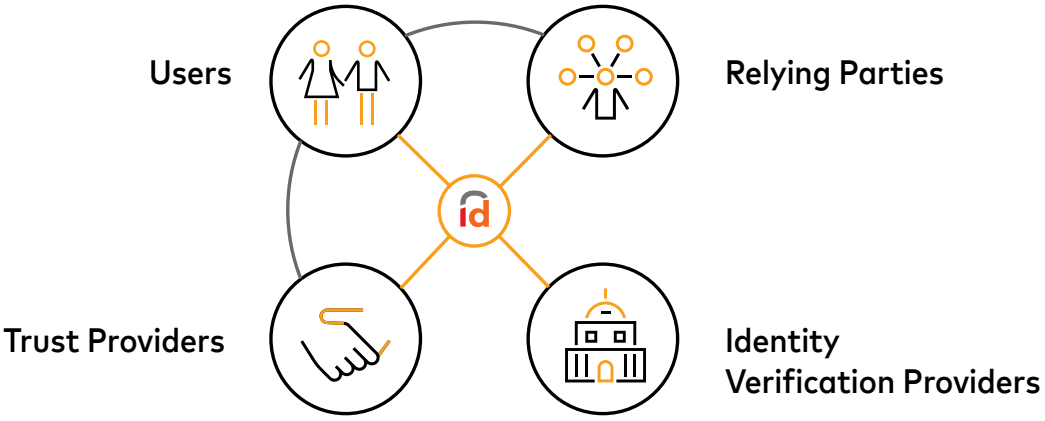
Uses of ID are far-reaching, and can range from a secure login to perform a financial services transaction to more complex use cases, such as a car or vacation rental, filing a tax return, or a credit card or mortgage application.

- Secure, verified login
- Government programs
- Financial services
- Health insurance
- Travel and transportation
- Education
- Shopping, gaming, entertainment
- Employment services
- And many more use cases

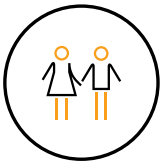
ID network

Collaborative digital identity network

Underpinning the ID service is the ID network, a collaborative digital ecosystem that enables four key participants—Users, Relying Parties, Trust Providers, and Identity Verification Providers—to achieve together what is impossible alone: convenient, secure, smart digital interactions that work better for everyone. Here's how each participant contributes to creating a robust, practical, efficient digital identity network.



Roles and value exchange in the ID network



Users are ordinary people who want their digital interactions—from buying concert tickets to applying for loans—to be easier and more secure. They enroll in ID so they can interact in a trusted way with Relying Parties, such as service providers and merchants, quickly and confidently by securely providing their identity data.

Convenient

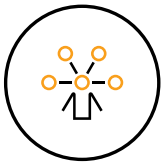
ID quickly verifies a User when interacting with Relying Parties—online, in app, and in face-to-face settings. Freed from having to remember multiple passwords or presenting physical documents, Users can do the things they want to do faster and easier with ID.

Secure

A User's data is never stored in a central database that could be hacked by others, and facial biometrics on the User's device ensure that only the User can access and share their digital identity.

Smart

ID enables Users to connect and interact, without giving up their privacy or oversharing their information. ID gives individuals complete control of their data—they decide the information they want to provide and control where they share it.



Relying Parties are entities such as airlines, hotels, banks, merchants, and service providers that need to establish a User's identity to process a digital transaction or provide access to a service. Relying Parties can define the data they need to complete different use cases.

Improve the customer experience

With ID, Relying Parties can remove or reduce the frictions common in their digital experiences: requiring Users to enter passwords, manually enter information, scan documents, or even wait to be verified. Since ID provides a reusable, verified identity, a more seamless experience can be provided.

Reduce identity fraud and losses

ID can also help Relying Parties reduce fraud and associated losses. ID verifies the User's identity data with one or more authoritative sources, based on the Relying Party's requirements, providing a level of confidence the User is who they claim to be.

Trust Providers can be organizations—such as a bank, mobile network operator, university, or postal service—that has a preexisting, trusted relationship with the User. Trust Providers connect Users to the ID service, enabling them to sign up, use, and manage their digital identity.

Increase engagement and loyalty

By providing digital identity access with ID, Trust Providers can extend and build an even deeper relationship in new ways, fortifying that relationship for years to come.

Be part of every trusted transaction

When Trust Providers embed ID into their mobile application, they become a part of each interaction the User has with their digital identity. Across all areas of life—financial, travel, health, education—the Trust Provider's brand can be a part of it, delivering even greater value and recognition.

Identity Verification Providers are authoritative sources of information—such as a driver's license authority, passport office, university, mobile network operator, bank, or employer—that can verify identity documents or data.

Provide verified information efficiently

Through a single integration with ID, Identity Verification Providers can serve the full ID network of Users and Relying Parties looking to establish trust in order to interact.

Reach new markets and use cases at scale

The ID service takes on the work of cross-border expansion and interoperability, allowing Identity Verification Providers to scale globally with minimal effort.

ID network: Mastercard's role

A global digital identity network must be carefully organized and governed for efficiency, transparency, and reliability. Mastercard is uniquely positioned to lead this effort, given our experience operating and governing global networks, responsibility to data privacy as reflected in our Data Responsibility Imperative, and commitment to investing in a global infrastructure. Over the past half century, we've built a global payments network that securely processes over a billion transactions per day for 2.5 billion cards across 210 countries and territories—quickly, securely, and reliably.

Mastercard will bring that same world-class performance to orchestrating the ID network as we assume responsibility for:

Trust framework and governance

- Establishing a collaborative governance model for all stakeholders in the ID network
- Defining the operating rules, including the responsibilities of parties in the ID network
- Developing and monitoring compliance with the ID service rules

Platform and technology

- Developing, operating, and supporting the ID platform and technology
- Enabling participants to integrate with the ID network via software development kits (SDKs), application programming interfaces (APIs), and related support

Identity verification

- Using the latest verification and authentication technologies, including liveness checks, biometric authentication, and biometric-to-document matching
- Verifying User identity, attributes, and documents with Identity Verification Providers and, with User consent, providing appropriate data to Relying Parties

Security practices and protections

- Defining a distributed security approach that protects a User's data in transit and at rest, with an architecture that respects user privacy and provides Users with control
- Protecting the ID network against data breaches and fraud

ID design components

Mastercard is committed to providing a best-in-class, user-centric, digital identity service that raises the bar on data protection and privacy, can handle millions of digital identity interactions daily, and scales globally. Our design components put the User in control; address critical issues of privacy, ownership, transparency, security, and more; and guide our choices in partners, technology, systems architecture, processes, and practices.

ID encrypts and protects identity data on the User's device, not in a central database

Device-based storage

To protect against unauthorized data access, ID stores data on the individual's own device, rather than a central server or database where it could be vulnerable to hacks. ID also leverages security tools such as biometric authentication, encryption keys, and a mobile device's secure environment to provide highly secure and efficient data protection. This approach virtually eliminates the possibility of a large-scale breach or hack, protecting the User and other participants in the ID network.

ID enables tailored data policies to satisfy unique Relying Party data needs

Needs-based policy engine

In a world of billions of unique digital interactions, a one-size digital identity does not fit all. That's why Relying Parties can define their own Assurance Policy, based on their unique use cases and needs. By establishing their own requirements for User data, as well as the strength and recency of the verification, ID will only request from the User the specific data elements needed by the Relying Party at each digital interaction. Relying Parties can modify these rules to address new use cases and security challenges.

ID verifies identity data in real time with authoritative data sources

Real-time identity verification

When an individual creates their ID, and when a Relying Party requires identity verification, the ID service connects to authoritative sources—called Identity Verification Providers—in real time. An authoritative source could be, for example, a driver's license authority, a bank that issued a credit card, or the passport office. In addition, identity data that has already been verified by an authoritative source, and that is stored on the User's device, may be used by the Relying Party if it meets their needs as stated in their Assurance Policy.

ID is designed to protect identity data and the individual's privacy

Privacy by design

Protecting User privacy is central to the ID service. In addition to complying with country and regional privacy regulations, such as the EU General Data Protection Regulation (GDPR), several privacy-enhancing features have been directly embedded into the ID service:

- **Avoids data oversharing –** A critical privacy issue with digital interactions is that individuals unintentionally share their personal information, or their data is used without their knowledge or consent. This is not the case with ID. The individual has control over their digital identity and must agree to share their data with a specific entity for a specific purpose. Requiring User consent and providing only essential data are key to ensuring data minimization and privacy. As a result, Relying Parties limit their data-handling exposure and Trust Providers can offer a valuable service without having to store new data.

- **Blinds data between network participants –** ID also protects the individual's privacy through use of "double blinding" between network participants involved in a transaction. For example, Relying Parties don't know the specific sources of data verification, Identity Verification Providers can't see who is requesting the verification, and Trust Providers aren't aware of the nature of the individual's digital interactions.

ID is the first globally interoperable digital identity system design

Globally interoperable system

A student applies for study abroad. A business person travels to meet with foreign clients. A grandparent purchases toys from an overseas retailer. Individuals need to prove their identity and share data for myriad reasons—and a university, airline, or merchant must decide whether to rely on that data. Unlike other digital identity systems, ID is designed for global interoperability to accommodate multiple use cases, whether a User is in their home country or abroad. We're building a global network of reliable Identity Verification Providers to make digital interactions simple, seamless, and secure—from any location. We're also partnering with local digital identity providers to enable cross-border interactions between Users and non-local Relying Party services.

ID is designed with speed, flexibility, and growth in mind

Fast, scalable network

ID is a scalable, extensible service capable of handling millions of digital interactions daily. We coupled proprietary systems and development with best-in-class third-party system components to create a high-speed, highly secure network that is consistent with open standards.

The foundation of the ID service is the Microsoft Azure Active Directory B2C Identity Experience Framework (IEF) platform—a highly secure and proven cloud identity platform. This base is enhanced with a rules-based identity policy management engine, a framework for multiple identity verification source decisioning, User liveness detection, document authenticity checking, biometric-to-photo ID matching, and other components. Verifications with authoritative data sources occur in real time through use of APIs. This design offers the best of both worlds: data storage on the User's device and local applications for data protection, combined with cloud-based processing for high performance.

Built on open standards, ID supports ease of integration and system interoperability

Open standards

In designing ID, Mastercard uses established standards where they exist and, where there are gaps, engages with progressive organizations and communities working to define new standards. For example, ID is based on OpenID Connect (OIDC) standards, enabling easy implementation and quick onboarding for Relying Parties. ID platform components also leverage REST APIs, and we use standards-based symmetric and asymmetric cryptography for data encryption.

Mastercard is active in community-based efforts to establish digital identity standards. In addition to maintaining interoperability with existing OIDC standards, ID will work with groups such as the Decentralized Identity Foundation, W3C, eIDAS, and others to enable emerging standards such as W3C Verifiable Credentials using Decentralized Identifiers (DIDs). These will serve as a means of supporting existing and emerging identity schemes in local markets, while enabling a global acceptance network.

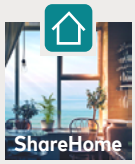
ID needs-based approach

The Relying Party Assurance Policy

The ID service is flexibly designed to support the varying needs of its Relying Parties. A needs-based Assurance Policy enables the Relying Party to define the Identity Assurance Profiles, and the identity attributes, needed for each of its use cases.

In its Assurance Policy, the Relying Party defines rules that specify:

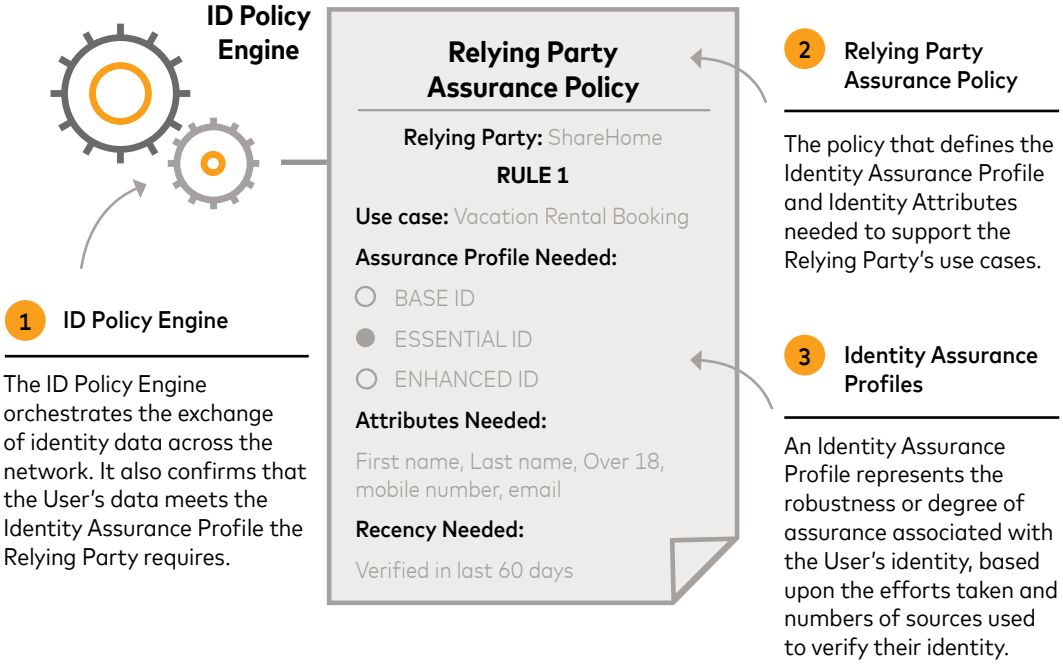
- The Identity Assurance Profile needed for the use case: Base ID, Essential ID, or Enhanced ID, explained in detail on Page 15
- The required identity attributes such as name, date of birth, age, address, etc.
- The recency with which the data has been checked



EXAMPLE

ShareHome, a vacation home sharing site, only rents properties when the lead booker is over 18. They need verified contact details to send the booking confirmation and reminders. They also need a verified name for the booking agreement. So ShareHome sets their Assurance Policy to define these needs.

Illustration: Relying Party Assurance Policy



ID Policy Engine

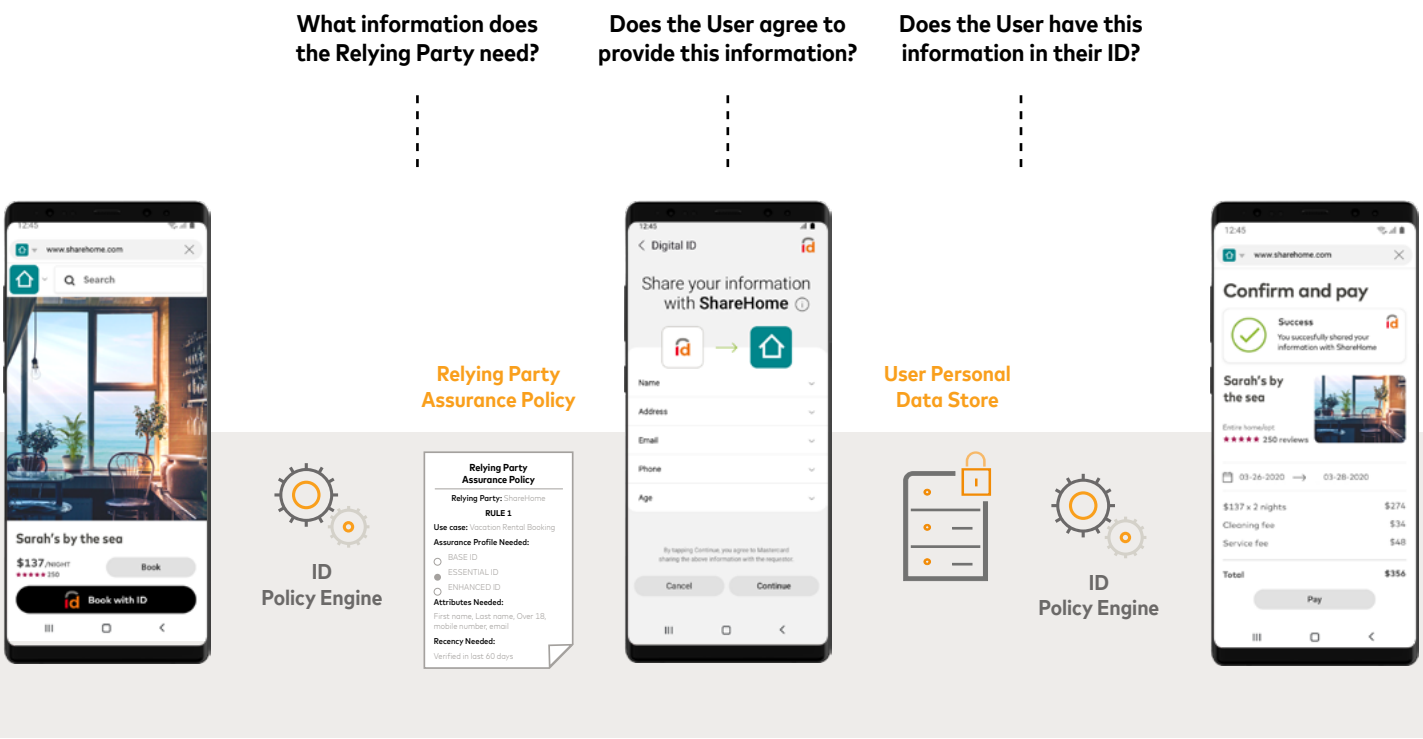
The ID Policy Engine orchestrates the exchange of identity data across the network. During an interaction between a User and a Relying Party, the ID Policy Engine checks the Relying Party's Assurance Policy and presents the needed identity attributes to the User in real time. After successful authentication, the User reviews the identity data requested and, if agreeable, provides consent to share the data with the Relying Party. This process ensures that only data needed by the Relying Party is requested from the User, and that the User provides their consent before that data is shared.

The ID Policy Engine also confirms that the User's data meets the Identity Assurance Profile the Relying Party requires. If it does not, the ID Policy Engine requests additional verifications from the IVPs and, if required, more information from the User.

The following illustrates how the ID Policy Engine determines what data the Relying Party needs, confirms that the User consents to provide it, and checks to see if the information requested is available, before completing the interaction.

Illustration: ID Policy Engine during a digital identity use case

Not actual screens



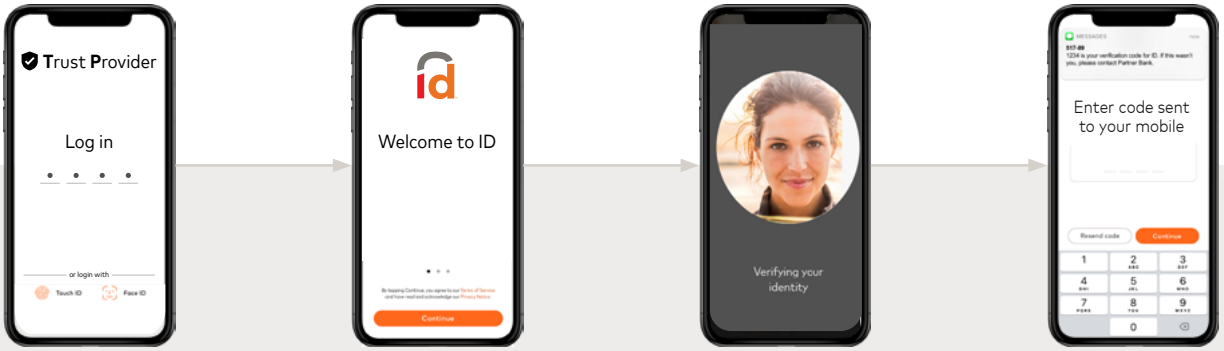
The ID experience

Creating an ID

Creating an ID begins with the User asserting information about themselves and confirming their information. The ID service processes this information and checks to ensure the individual is a live person, that their device is in their possession, that their face matches the one on their official photo identification, and that the information they have provided is valid.

Illustration: ID creation within Trust Provider app, through use of ID SDK or APIs

Not actual screens



User experience

How it works

User logs in to Trust Provider app and selects ID

Trust Provider authenticates User

User accepts terms and privacy notice

Trust Provider supplies User's name, address, DOB, etc.for the User to seamlessly establish their ID

User scans their face

Liveness detection confirms User is a real, live person

User's biometric is encrypted and stored on device

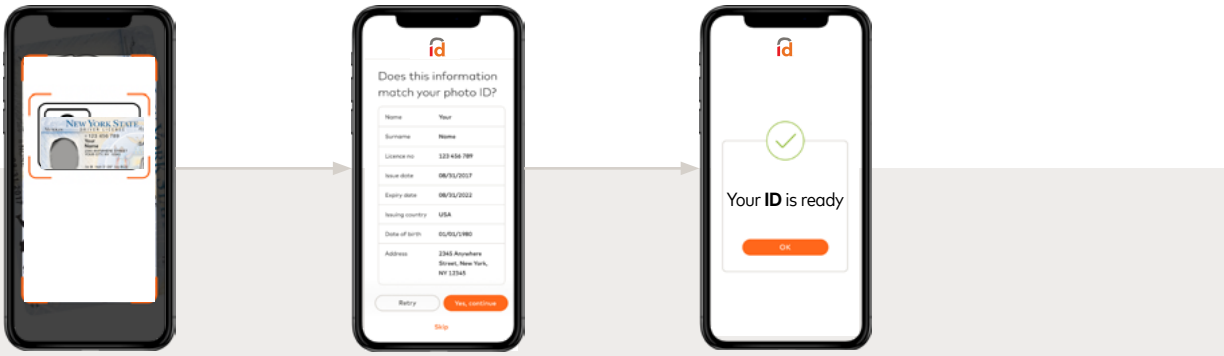
User consents to processing biometrics by the ID service

User verifies their mobile number

Trust Provider supplies mobile number or User enters it directly

ID service sends one-time password to User's mobile

Mobile number is encrypted and stored on device



User experience

How it works

User scans photo ID (optional)

ID service performs document authenticity check

ID service matches the User's biometric to photo on the photo ID

User confirms other data

ID service verifies the User's data with Identity Verification Provider(s)

User's data is encrypted and stored on the User's device

ID creation confirmed

User's digital identity is cryptographically bound to the device and protected by User's biometric

ID service stores the ID creation event in audit log and in User's activity history

Using ID

An individual's use of their ID, whether online, in apps, or in physical settings, follows a familiar sequence regardless of use case.

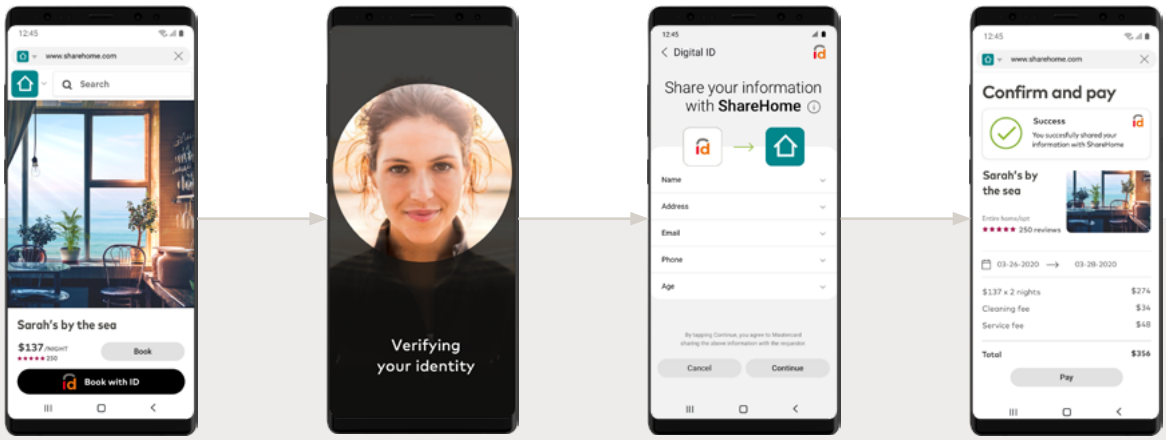
1. First, the User chooses the ID option within the Relying Party's app or website. This may appear as "Log In with ID," "Apply with ID," "Continue with ID"—or another option suited to the use case.
2. The User then unlocks their ID using facial recognition.
3. Finally, the User consents to share the data requested by the Relying Party for that use case.

Using ID in mobile apps

A representative User experience and the ID service processes are as follows:

Illustration: Use of ID within Relying Party app, through use of ID APIs

Not actual screens



	The User finds their desired property and taps "Book with ID"	The User unlocks their ID on their device using facial biometrics	The User reviews and consents to share the requested information	The User is returned to the rental app and completes the booking
User experience				
How it works	Relying Party has integrated ID into their journey for a seamless experience	Liveness detection confirms User is a real, live person ID service matches the fresh face scan to the biometric stored on device ensuring only the User can unlock their ID and share their data	ID service calls the Relying Party's Identity Verification Assurance Policy and sends appropriate prompt to the User ID service checks if User data meets Relying Party's criteria	Encrypted data is passed to the Relying Party ID service registers the event in audit log and User's activity history

Using ID on the web

The experience of using ID on a Relying Party website begins with the User selecting the ID option. The User is then presented with a QR code to scan with their mobile device. Doing so evokes the User authentication and other steps described earlier, after which the User's identity data is passed to the Relying Party, and the User can complete their experience on the website.

Using ID in face-to-face settings

The ID service will support a range of scenarios in face-to-face environments, including those at retailers, event venues, airports, restaurants, universities, medical facilities, government agencies, and more. In each case, the ID service will streamline the user experience, without compromising security or privacy. Given the differences in these environments, a range of point-of-interaction technologies will be supported. QR codes and NFC technology, for example, are optimized for certain experiences. A physical biometric reader could be appropriate for other use cases. While the ID service will initially support QR-based exchanges, other approaches will be delivered for future versions of the service.

Managing ID

With the ID service, Users have complete control over their ID—able to enhance, amend, manage, and even delete their ID. These capabilities provide transparency and peace of mind to the individual and enable them to make changes when needed. Users can:

View activity history

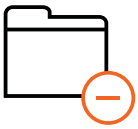
Users can view all their ID activity, including when it was created, amended, or added to; when they deleted data; as well as a log of interactions with Relying Parties. All activity is securely held on the User's mobile device, along with the User's ID data itself.

Back up and restore

Users can back up and later restore their identity data in the event they change their mobile device or migrate to a new Trust Provider application. The User's ID data, including activity history, is encrypted and saved in the User's chosen cloud storage location. This ensures that the User can restore their ID should their mobile phone be lost, stolen, or damaged.

Add data and documents

Users will be able to update and enhance their ID with an expanding set of data attributes and documents, such as updating their address, or adding an insurance card for expedited check-in at the medical clinic, or university degrees and certifications for streamlined job applications.



Delete the digital identity

Users can withdraw certain consents they have previously provided, or even delete their ID, right from the ID mobile interface. Doing so will erase the User's identity data from the User's device.

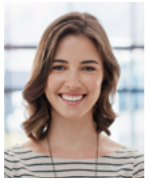
Samsung partnership

Helping people have the best possible experience in managing their digital lives. That's the goal of the Mastercard and Samsung partnership, which brings together Samsung mobile technology with the ID service to enable Users to conveniently and securely verify their digital identity with Samsung mobile devices.

This solution leverages Samsung's cutting-edge, proprietary facial biometric authentication and liveness checking capabilities. Users can access their digital identity with the same familiar facial recognition experience used across other Samsung applications. And with the ID service embedded in Samsung devices, Users will have immediate access to ID without having to download a new app, making it easier and faster to establish and use their digital identity.

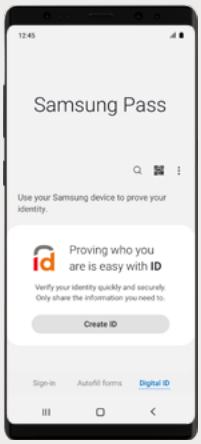
Mastercard and Samsung see particular value for the new digital identity service in a wide range of applications, from reducing card-not-present (CNP) fraud and streamlining banks' Know Your Customer (KYC) processes to enabling digital "check-in" for virtually any digital interaction and accelerating the digital sharing economy to lift emerging markets.

Looking ahead, Mastercard and Samsung will evaluate the ID service in multiple markets, continuously evolving the experience to deliver simple, seamless digital identity interactions across multiple use cases in both digital and physical settings.



EXAMPLE

Emily uses her Samsung device to help manage her digital life. Communicating with family, organizing her calendar, making daily purchases, mobile banking, or monitoring systems in her home—her device is always with her. Now with ID embedded in her Samsung phone, she has more control over her data, and can access services more quickly and securely. She uses ID on a daily basis—when accessing her financial accounts, traveling, and even signing up for classes at a local fitness center.



ID identity assurance model

Identity evidence types include official documents, accounts, or credentials, such as a driver's license, passport, bank account, and medical license

Identity evidence

How much evidence is needed to confirm an individual's identity in a digital interaction? It varies. When an individual wants to rent a car at the airport, the rental agency will typically require just a few pieces of data to be verified: a driver's license and credit card. But when that person applies for a mortgage, the evidence required and the verification process will be far more rigorous.

ID provides a robust and extensible approach to managing this verification "ladder" with defined Identity Assurance Profiles that help streamline and secure the assurance process for the individual, as well as the entities involved in the identification chain (Relying Parties, Trust Providers, and Identity Verification Providers).

An Identity Assurance Profile represents the robustness or degree of assurance associated with the User's identity, based upon the efforts taken and number and/or origin of sources used to verify their identity

Identity Assurance Profiles

Identity Assurance Profiles represent the degree of assurance in the individual's identity, based on the evidence types and the number and/or origin of sources used to verify the individual. They are designed to:

- Establish whether the User interested in the service is a real person
- Verify if the evidence to support that User's information is genuine and valid
- Use authoritative sources to verify the evidence of User's identity

For any given Identity Assurance Profile, there is more than one possible combination of evidence types (passport, driver's license, bank account data, for example) and evidence verification mechanisms (such as checking security features of the document image, authentication using bank credentials).

The ID service currently provides three Assurance Profiles for Relying Parties to leverage: Base ID, Essential ID, and Enhanced ID profiles.

1. Base ID

When a User creates their ID, a Base ID Profile is established, essentially confirming the "basics" for Relying Parties, verifying that the User:

- Has a persistent, recognizable identifier that is bound to them
- Has passed liveness checks
- Is able to respond to the contact information provided
- Has attribute information (obtained but not tested)

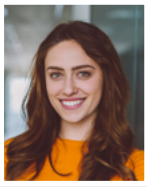
EXAMPLE

Paul needs travel insurance. In order to receive a quote, he uses his ID to log in to the website of the insurance company (the Relying Party). The insurance company wants to ensure Paul is a real, live person and has accurate contact information, so it requests his Base ID Profile, which is sufficient to provide Paul with a fast quote.

2. Essential ID

Essential ID is the next rung up the assurance ladder. Users of the ID service will have this higher profile based on how they onboarded into the ID service, or if they have added verified documents to their Base ID. The Essential ID Profile assures Relying Parties that:

- The User's asserted identity has been tested to show existence in the real world
- Name, address, and date of birth information have evidence to demonstrate association with the User
- Attribute information comes from genuine documents or sources
- Attribute information was verified by an ID service IVP within the recency specified



EXAMPLE

Esther is a graduate student and wants to rent an apartment near the campus. Using ID, she fills out an application on the website of a nearby short-term housing rental company. The rental company (the Relying Party) wants to have confidence that Esther is who she claims to be, so it requests her Essential ID to verify her information. The ID service may verify Esther's identity attributes using a combination of her university student registration information, the human resources office at Esther's part-time job, or even her mobile phone provider.

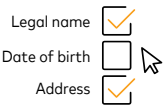
3. Enhanced ID

This Assurance Profile builds upon the Essential ID profile, and assures Relying Parties that:

- Evidence from two or more authoritative sources were used during verification
- During the verification of the User's ID data:
  - Security features of evidence presented were tested to check that the evidence was genuine
  - At least one evidence document has an image of the subject that was compared to the User presenting the evidence
  - If logon to an online account is used to verify the link between the individual and the records at the issuing source, strong customer authentication, such as multi-factor authentication, is required

EXAMPLE

Alex wants to buy a SIM card in a country that requires robust customer identification for such a purchase. Using his ID, he requests the SIM card through a mobile network operator. The mobile network operator (the Relying Party) requests Alex's Enhanced ID to meet their assurance requirements. The ID service may enable Alex's information to be verified by proving he has an active account with his financial institution. Alex would log in to his online financial account using ID in order to demonstrate that he owns the account.



The ability to request specific attributes at defined assurance levels to satisfy a specific use case (the Relying Party receives only the attributes required for the specific use case)

Attribute assurance

With ID, Relying Parties can flexibly define the specific attributes needed to support their use cases. Some will require only a few attributes rather than the User's full identity information. For example, a restaurant deciding whether to serve a patron an alcoholic beverage needs only to verify the User's age, not their full identity.

The assurance level for each attribute will vary depending on the evidence presented by the individual and the availability of validation sources. ID provides three ascending Attribute Assurance Levels:

- Level 0: The information is self-asserted by the User and has not been tested
- Level 1: The information has been validated by a single authoritative source
- Level 2: The information has been validated by two or more authoritative sources

With ID, Relying Parties will be able to define rules around the strength of the checks used to establish and maintain the User's identity, and the recency by which those checks were performed. This gives the Relying Party confidence that the associated attributes, tailored to their needs, can be trusted.

Examples of strength checks:

- A daycare hiring a new staff member requires a high degree of confidence in that person's identity. The employer would request that multiple data sources be used to verify the identity, that these sources were highly trustworthy, and that the verification process was robust.
- A website running a poll needs to know that automated bots are not influencing the voting, and also that one person is not casting an excessive number of votes. The website would require that the User pass a liveness check, supply only the Base ID, and can be verified by email or mobile phone number to authenticate their vote.

Examples of recency checks:

- In verifying the identity of a car rental customer, the rental agency would request that the validity check with the issuing authority for the driver's license be performed at the time of the transaction, rather than relying on past information.
- A mobile phone retailer shipping the latest smartphone would want to know that the address of the User was current. They would require a recent check to minimize the risk of shipping to the wrong location.

Evolution of identity assurance

Identity fraudsters are constantly evolving their methods. The ID service is designed to grow in functionality to address changing threats in the market and to provide an ever-advancing defense against identity fraud. Drawing on our collaborative partnership of Trust Providers, Identity Verification Providers, and Relying Parties, Mastercard will work to:

- Detect threats and fraud attempts to our ID network
- Engage with agencies in the public and private sector to establish good practices
- Gain insight and feedback from network partners to detect trends and predict risk
- Evaluate and incorporate innovative technology, data, and procedures as they emerge

ID service security

ID is designed to be convenient, smart, and secure. And we take that third pillar—service security—extremely seriously. That's why ID has innovative, multi-layered security that protects every digital interaction: from core platform technologies to the end points, from User enrollment to authentication and verification, from data storage to data transmission. The latest security techniques and practices are utilized, with fail-safes and redundancies in place to protect the system, Users, and the broader ID network.

Protecting access to the identity

Controlled User enrollment

ID first and foremost prevents bad actors from creating identities. From sanctions screening to a robust identity verification process with capabilities such as liveness checking and selfie-to-photo ID matching, Users are well-vetted before their ID is established.

Liveness checking

At the time of ID creation as well as each time the User accesses or shares their ID, the ID service performs a liveness check. The liveness detection technology uses the device's camera and a series of short videos to ensure the individual is a live person and not a mask, video, or robot.

Biometric authentication

ID leverages facial biometric authentication to ensure that the owner of the identity is the same person later authenticating, accessing the ID, or looking to share data with a Relying Party. And unlike standard device-based biometric authentication, the ID service further binds the User's facial biometric with photo evidence (the User's passport or driver's license, for example) in support of the claimed identity.

Protecting data at rest

Trusted application

ID is embedded within a secure Trust Provider application, such as a secure mobile banking app, that integrates with the ID service using provided SDK or APIs, according to the ID service implementation and security requirements.

Mobile application integrity

ID secures the mobile application by obfuscating the underlying code in the SDK or APIs. This works to prevent bad actors from accessing, altering, or otherwise hacking the application.

Trusted device

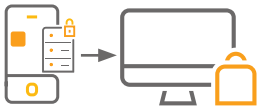
Every time the User's device interacts with ID, the system cryptographically verifies the device signature, ensuring that it can be trusted during each ID interaction. This is accomplished through use of cryptographic keys that were issued at the time of ID creation.

Secure storage

Central to ID is the User's Data Store—the encrypted record of the individual's digital identity stored on their own personal device. The User's Identity Data Store is established at the time of ID creation, contains the User's self-asserted and verified data, and is encrypted using a secure device key. The device key is stored in the Trusted Execution Environment (TEE), which is only accessible by the User via successful, on-device biometric authentication.

4-way binding

When a User creates their identity, 4-way data binding occurs, linking the User's verified identity, their device, their identity document(s), and their live presence for security. The binding is leveraged each time the User accesses the ID service—ensuring that the individual attempting access is the same User, who is owner of a verified identity document, on the same device, living and present.



Protecting data in transit

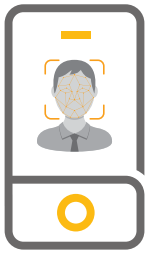
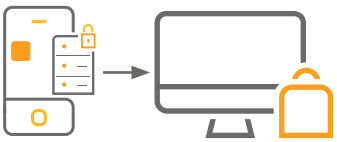
Multi-layer encryption

The ID service encrypts data when it is shared by the User with Relying Parties or when verified by Identity Verification Providers. All ingoing and outgoing messages through the service leverage message-level encryption on top of transport-layer security. This helps protect the User's data from interception or other attack during transit.

Key pairing

When data is shared by the User, those messages are digitally signed with a private key and also encrypted by the destination's public key. This private-public key pairing ensures that only the intended recipient of the data—the requesting Relying Party—receives and can unlock the User's data for the specific transaction.

Illustration: ID service security components

Protecting access to the identity	Protecting data at rest	Protecting data in transit
		
✓ Controlled enrollment	✓ Trusted application	✓ Multi-layer encryption
✓ Liveness checking	✓ Mobile app integrity	✓ Key-pairing
✓ Biometric authentication	✓ Trusted device	
	✓ Secure storage	
	✓ 4-way binding	

Conclusion

Today, people look to digital-first tools to make their lives more convenient, secure, and smart. But their digital expectations are often frustrated by the challenges of proving, and protecting, their identities. And there is no service that securely, seamlessly connects users with the banks, merchants, governments, and other organizations they need to interact with on a daily basis.

Now there is. Mastercard has created ID—a digital identity service that enables Users to quickly verify their identity in every interaction, anywhere in the world. Grounded in collaboration, the ID service is designed to meet the evolving needs and challenges faced by our partners and customers. A service that is flexible, extensible, and scalable, ID can readily grow to meet new needs and adapt to new circumstances in the years ahead.

ID provides a better way to prove identity in a digital age. Its thoughtful design gives individuals more control and privacy, while enabling businesses and organizations to deliver services with less friction and more confidence:

- **Device-based storage** – Users' data is stored on their device, not in a central database vulnerable to hackers
- **Needs-based policy engine** – The ID Policy Engine enables every Relying Party to set their own requirements for User data, as well as the strength and recency of those elements, to meet their unique use cases and needs
- **Real-time identity verification** – When an individual uses their ID, the ID service verifies their identity by connecting to authoritative sources, the Identity Verification Providers, in real time
- **Privacy by design** – The individual has complete control over their data, and only the data required is shared, while double blinding between network participants involved in a transaction protects User privacy
- **Globally interoperable system** – ID is designed for global interoperability to accommodate multiple use cases, whether a User is in their home country or abroad, to make digital interactions simple, seamless, and secure from any location
- **Fast, scalable network** – ID is built on a scalable, extensible platform capable of handling millions of digital interactions daily, enhanced with device-based User liveness detection, document authenticity checking, biometric-to-photo ID matching, and other components
- **Open standards** – ID is based on OpenID Connect (OIDC) and other open standards, REST and OIDC-based APIs, and standards-based symmetric and asymmetric cryptography—for ease of implementation

Meeting individuals' needs in this digital era requires collaboration from all parties involved. Working together, we can accomplish what is impossible alone: convenient, secure, smart digital interactions that work better for everyone. Mastercard invites all stakeholders to contribute to this collaborative model.

To learn more, visit us at www.idservice.com.

Convenient. Secure. Smart.

This document is proprietary to Mastercard and shall not be disclosed or passed on to any person or be reproduced, copied, distributed, referenced, disclosed, or published in whole or in part without the prior written consent of Mastercard. Any estimates, projections, and information contained herein have been obtained from public sources or are based upon estimates and projections and involve numerous and significant subjective determinations, and there is no assurance that such estimates and projections will be realized. No representation or warranty, express or implied, is made as to the accuracy and completeness of such information, and nothing contained herein is or shall be relied upon as a representation, whether as to the past, the present, or the future.

©2020 Mastercard. Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated.