midy™

An Introduction to Midy

A privacy-preserving way to build digital trust

Gen

Table of Contents

An Introduction to Midy

> **“Those who seek to deceive, manipulate, and defraud us do not play by the same rules as the rest of us.”**
>
> - Drummond Reed, Director of Trust Services, Gen™

In its early days, the Internet was marked by a sense of community, where everyone seemed to know everyone else–or at least knew someone who knew you. It was a time when people could trust that the person they were communicating with was who they said they were.

But as the Internet grew to connect billions of people, companies, and devices, it became increasingly easy for individuals to hide their true identities and create fake personas. This made it challenging to determine what information online was authentic and what was not. Cybercriminals could now create bots that mimic human behavior, phishing websites that are indistinguishable from genuine ones, and mobile apps that are Trojan horses for malware.

Now, with the rise of botnets, deep fakes, and artificial intelligence, we are entering an epidemic of deception and misinformation. It has become all but impossible for both individuals and organizations to verify the authenticity of online content and customer accounts, raising serious concerns about the reliability of the information we consume and share.

To address these concerns, Gen™ is pleased to introduce its latest offering: Midy™, a new product that enables individuals to prove who they are and exchange verified data with trusted brands in a safer, more secure, and more privacy-preserving manner.

This paper will address why it remains so difficult to detect bots online and how Midy uses new digital wallet and digital credential technology to solve this problem – while putting consumers back in control of their information and safeguarding personal data privacy.

Check yes or no: "I'm not a robot"

As the Internet has become more ubiquitous in our daily lives, so too have CAPTCHAs (aka "Robot Tests"). These automated Turing tests have become synonymous with bot detection–*after all, how could a bot possibly check a box or click on pictures of bicycles?*

Today, more than one-third of the 100,000 most popular websites use a CAPTCHA service.[1] As they have risen in popularity, they have also become more difficult to solve in a losing battle to keep up with increasingly advanced bots–so much so that an infamous Google study found that machine learning algorithms could solve the most distorted tests 99.8% of the time, while humans only managed 33%[2].

Despite their imperfections, CAPTCHAs have become a necessary tool on websites, mobile apps, and other digital services. These platforms must have some way to prevent bots from consuming resources, filling databases with fake accounts, compromising security, and degrading consumer trust and safety.

At the same time, most platforms also want to minimize user friction. It becomes a balancing act of putting in the right controls to detect bots while minimizing the time it takes users to complete one of these tests. The compromise has historically been the CAPTCHA—a solution that is sophisticated enough to weed out many (not all) bots while being easy enough for many (not all) humans to accurately complete in seconds.

This is, of course, despite dozens of studies showing just how badly CAPTCHAs are losing the arms race against machine learning and virtual sweatshops. Today, an entire industry has formed around 'CAPTCHA farms' with services offering to solve 1,000 of these tests for as little as $0.75[3].

The alternative is to verify users' government-issued identity documents, but this process is clunky, cumbersome, and can cause significant friction and pain for users (in addition to a host of privacy challenges if not managed properly). It is generally only used by sites and services that are required to maintain a higher level of assurance through legal requirements like the Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations that govern financial institutions and payment networks.

Until recently, there has not been any middle ground—no easy, fast way to prove that a user is a real human online that is also difficult for bots and malicious actors to circumvent.

1. American Association for the Advancement of Science. (2008). Digitizing Old Text and Fighting Spam, Too. Science.org. Retrieved from https://trends.builtwith.com/widgets/captcha 2. Goodfellow, I. J., Bulatov, Y., Ibarz, J., Arnoud, S., & Shet, V. (n.d.). Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks. Google Inc. 3. I Was a Human CAPTCHA Solver. (2021) F5 Labs, https://www.f5.com/labs/articles/cisotociso/i-was-a-human-captcha-solver

Introducing digital wallets and digital credentials

In 2015, a new era of digital identity emerged, inspired by cryptography and Web3 principles. Ironically, while the technology is available for the first time, the approach is quite familiar—it is how we have been proving our identity for centuries.

In the physical world, we rarely leave the house without our wallets or purses. Inside this container, we carry a series of paper or plastic "credentials." Some of these have to do with payments (credit and debit cards), while others have to do with identity (licenses, loyalty cards, library cards, insurance cards, etc.). If we need to prove anything about ourselves, such as that we are over 21 or we have health insurance, all we have to do is flash one of these identity cards. They are widely trusted and accepted, so we can use these cards pretty much anywhere.

The Web3 approach to digital identity is largely the same—only now, our wallets and credentials become **digital**, on our phone or other personal device. Like our paper cards, these digital credentials belong to us. We take them with us and can use them anywhere they are accepted.

At the same time, these digital documents have a few notable advantages over their physical equivalents. Most importantly, *they enable the holder to prove information about themselves without sharing the actual information.*

This is a major advance in online privacy. For example, if a user's license is stored as a digital credential, they can prove that they are over a certain age *without* exposing their birthdate. Or they can prove that they are a real human *without* sharing their name or any of the information printed on their physical license. This is known as **selective disclosure**, and it fulfills the Privacy by Design principle of **data minimization**—sharing the minimum amount of personal information necessary for any transaction.

Selective disclosure stands in sharp contrast to how data has been traditionally exchanged across the Internet—where every time someone sends a file, they are creating a copy of that file that they no longer have control or visibility over.

To put this in perspective, consider how often you have provided your email to access a website, only to find your inbox flooded with emails from unknown vendors. Your control over that personal information was lost the moment you filled out a form and checked consent for a privacy policy without fully comprehending the terms. Without your knowledge, your information could have been stored with inadequate security precautions or sold to any number of companies. If the same thing were to happen with a copy of a government-issued identity document, the consequences (including the potential for identity theft) would be severe.

The use of privacy-preserving digital wallets means that individuals no longer need to share copies of their data. They can simply share proofs *about* the data.

Without getting into the weeds, this new approach is made possible through two recent developments:

- A **standard, interoperable way** for organizations to publish credentials in a digital format
- A **digital signature** so that verifiers (people, devices, or organizations that users choose to share their data with) can use public/private key cryptography to verify that a credential is authentic and has not been tampered with or falsified in any way

The good news is that over the past four years, hundreds of organizations and technologists have collaborated to develop three global standards to address these requirements: Verifiable Credentials (W3C VCs)[4], Decentralized Identifiers (W3C DIDs)[5], and the Mobile Driver's License (ISO 18013)[6].

Today, digital wallets and credentials are becoming increasingly popular, and while work on open standards and open source code for these technologies is ongoing, adoption is gaining momentum. Notable examples of this include a new EU regulation that will enable every European to have a set of digital identity credentials that are recognized anywhere in the EU[7]; an emerging digital identity system in Bhutan based on verifiable credentials and decentralized identifiers[8]; and the launch of the OpenWallet Foundation[9], a cross-sector collaboration to promote interoperability and portability for a wide range of wallet use cases. Gen is proud to play a leading role in each of these three initiatives.

In short, the foundation is in place for digital wallets and credentials to begin delivering real solutions to real market problems.

[4] https://www.w3.org/TR/vc-data-model/ [5] https://www.w3.org/TR/did-core/ [6] https://www.iso.org/standard/69084.html [7] https://blog.avast.com/eidas-2.0-avast
[8] https://royalcentral.co.uk/asia/bhutanese-crown-prince-is-countrys-first-citizen-with-digital-identity-186659/ [9] https://openwallet.foundation/

Table stakes: Preserving personal privacy

Given the critical role we expect digital identity wallets to play in the coming years, we believe it is imperative that they are designed in a way that keeps the user safe and preserves the privacy of their personal information.

There is always a risk that digital wallet technology could lead to a "papers please" dystopia, where any website or service could start to demand that users share a government-issued identity credential—just because it is easy or it becomes commonplace. This would make the emails or phone numbers we routinely share today seem trivial: now individuals might be asked to share *everything* on their license, from their name and address to their weight and organ donor status.

The EU Commission is actively addressing this risk by building strong privacy protections into the European Digital Identity Wallet's framework to ensure consistency with their own General Data Protection Regulation (GDPR)[10]. This will mean that only organizations that have registered with the government will be allowed to request a government-issued credential from an EU citizen—and even then, only for the minimum personal data required for a very strict set of legitimate business purposes.

However, when properly implemented with the right combination of technology and governance, digital wallets can provide a major boost to online privacy. These news tools could significantly increase an individual's ability to control the use of their data, including what, how much, and with whom they share.

It begins with the understanding that **privacy is a promise**. A promise of one party to protect the private data of another.

While technology can give us the tools to help protect personal data (such as digital encryption to keep messages and documents confidential), most of the risk comes after the data is shared. Only humans can honor—and be held accountable for—their promise to protect it.

Countries express this promise in the form of **privacy regulations** that specify what data practices are and are not allowed. Companies express this promise in the form of **privacy policies** that indicate what the company will and will not do with the user's personal data.

However, both are blunt instruments. Privacy regulations have no choice but to be "one-size-fits-all" for an entire country and often take years to be updated, even as society and technology evolve. Privacy policies, for their part, are dictated by individual companies and force a "take-it-or-leave-it" proposition on their customers. If a user does not agree to a company's terms of service (often, seemingly endless pages of legalese), they are simply not able to use the service.

Once again, as was the case with proving a user is a real human, there has been no middle ground—no simple way to strike a privacy promise that feels fair and appropriate to all parties.

Here is where digital wallet technology gives us another new tool: the **privacy framework**.

Depending on your point of view, you can consider a privacy framework as either a "voluntary privacy regulation" or a "group privacy policy." Either way, here is how it works:

1. A community of organizations who collectively want to solve a digital trust problem get together and agree on the set of digital credentials they can use to do this. For example, a collection of social media sites, marketplaces, dating apps, and messaging boards could agree on the credentials they could use to solve the CAPTCHA problem.

2. The community publishes these rules as a privacy framework.

3. Organizations **issuing** their users credentials under this framework publicly commit to abide by the issuance rules.

4. Organizations **requesting** credential data from their users under this framework publicly commit to abide by the verification rules.

5. The individuals using a participating service now have a reasonable expectation that these services will uphold the privacy promises in the framework—and if they do not, the framework can include mechanisms (such as user reporting features) to hold offenders accountable.

Since privacy frameworks can now be designed for any set of digital credentials serving any online community, what has been a race-to-the-bottom in online privacy now has the potential to become a virtuous cycle of increasingly enlightened privacy frameworks.

[10] The European Digital Identity Wallet Architecture and Reference Framework. (2023). European Commission, https://doi.org/https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

How Midy Works

Returning now to the problem of proving one's identity quickly and securely online, we can now explain how Midy uses digital wallets and privacy by design to accomplish this:

Step one: Downloading Midy

Consumers can start taking back control of their data by downloading Midy, which is available in the App Store and on Google Play, starting in the United States and expanding to additional geographies in the near future.

They will be asked to secure their account with a passkey, ensuring that only they can access their Midy and the data stored within. They will also be asked to register with either an email address or phone number, which is the only personal data that Gen permanently stores outside of the user's Midy wallet. This data is required to protect and manage the user's account and is not shared with any other parties, unless the user explicitly consents to sharing that information.

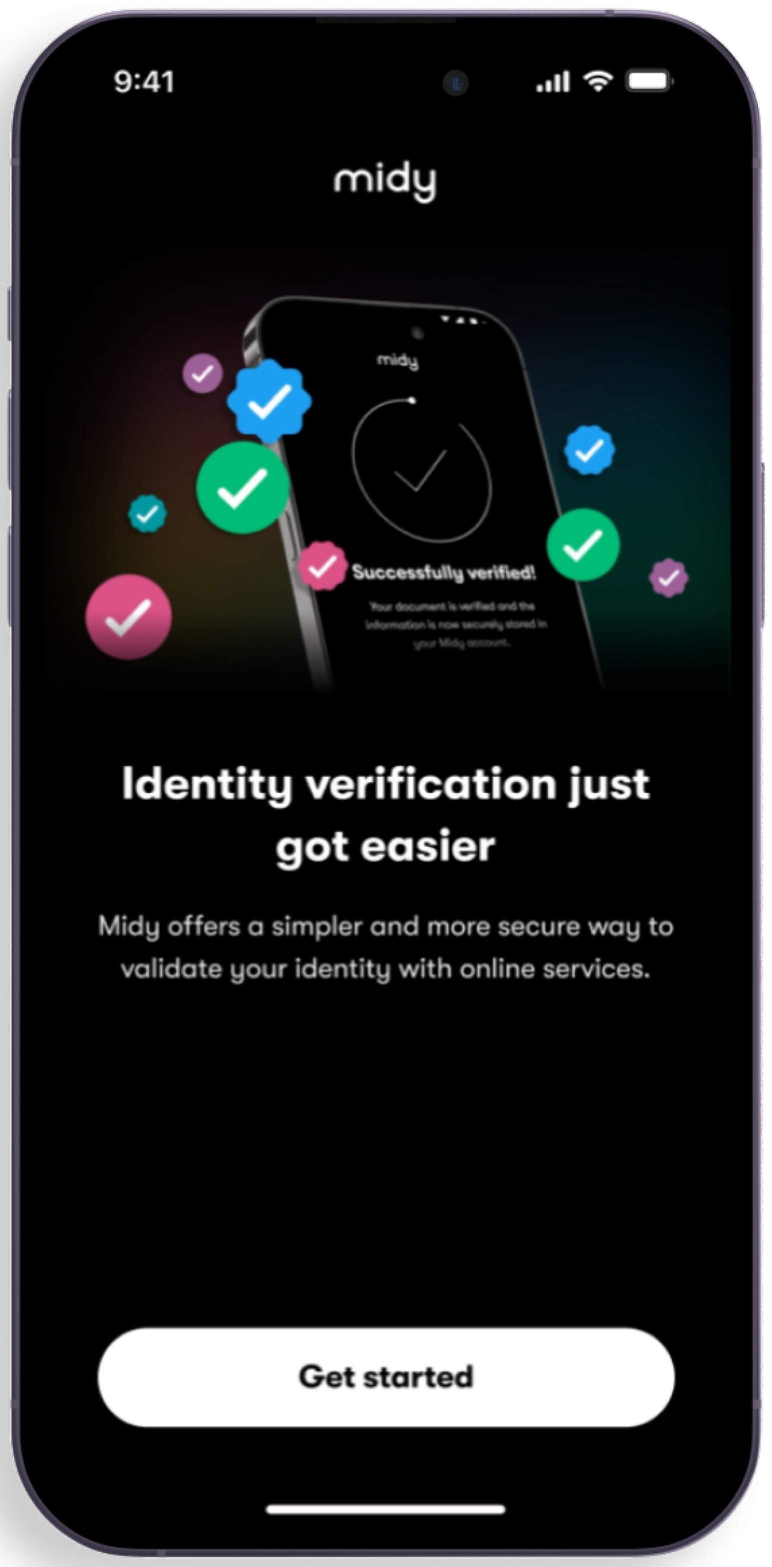
Step two: Getting an identity credential

Next, users will be able to generate their first digital credential by scanning a government-issued identity document.

Midy will guide the user through converting a passport, license, or another qualified document into a digital credential, and recording a video selfie to prove that the user is a real person and matches the photo on their identity document.

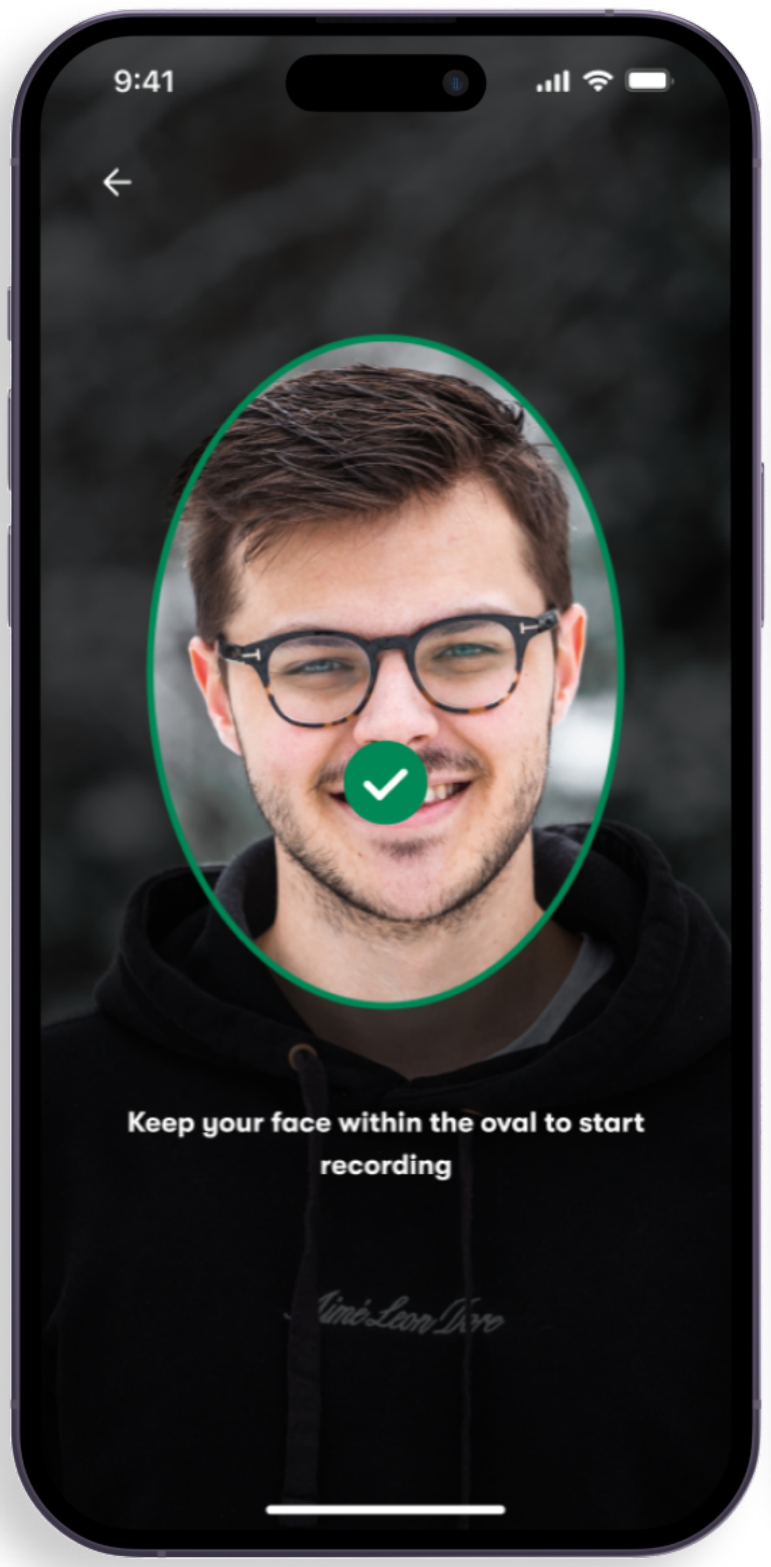
Once done, the user is now **Midy-enabled**. While proving someone is a real human is just the first of many use cases, this means that they can now instantly share this trustmark with a website or app to show authenticity.

There is no need to scan their physical credential again unless the original document expires.

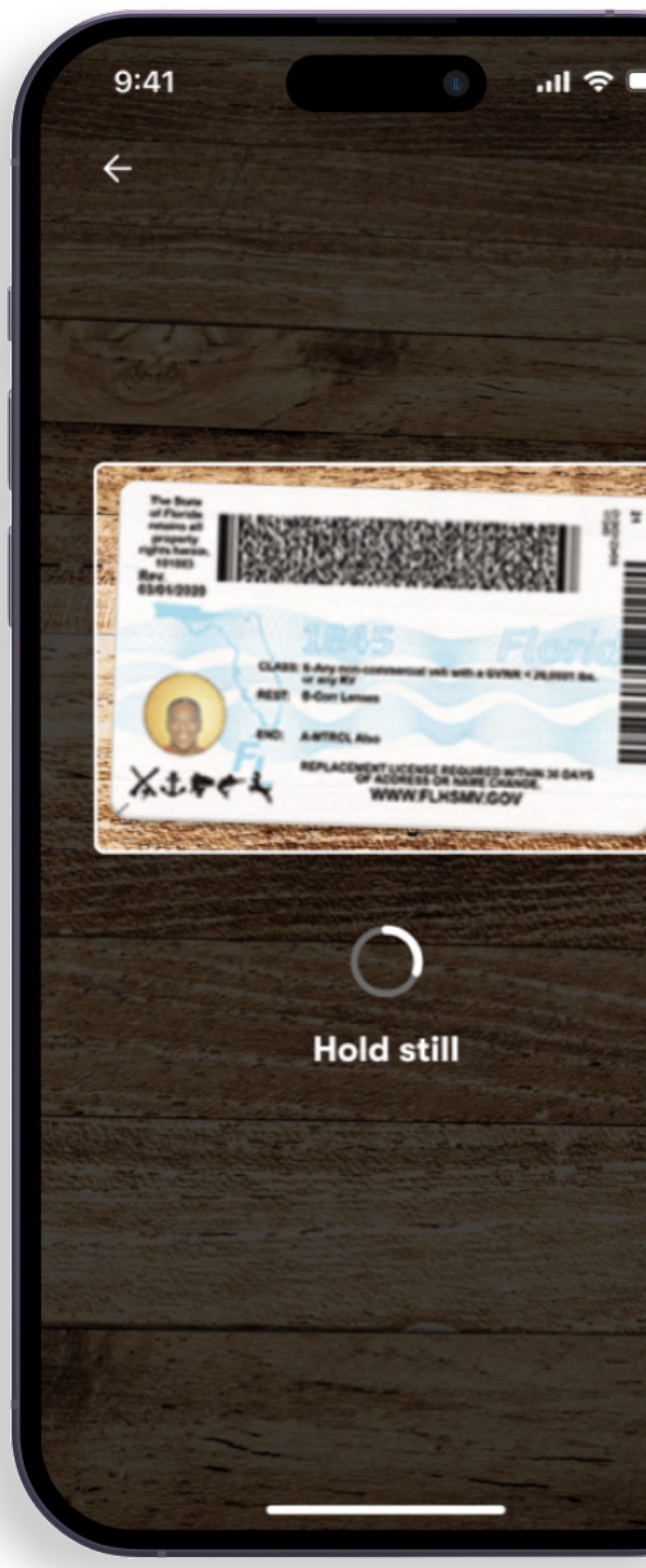


Identity verification just got easier

Midy offers a simpler and more secure way to validate your identity with online services.



Keep your face within the oval to start recording



Hold still

How Midy Works

Step three: Providing the proof

When an online service needs to ask for a user's Midy proof-of-real-human, it will display a QR code or in-app deeplink, inviting them to create a secure communication channel between Midy and the service requesting the data.

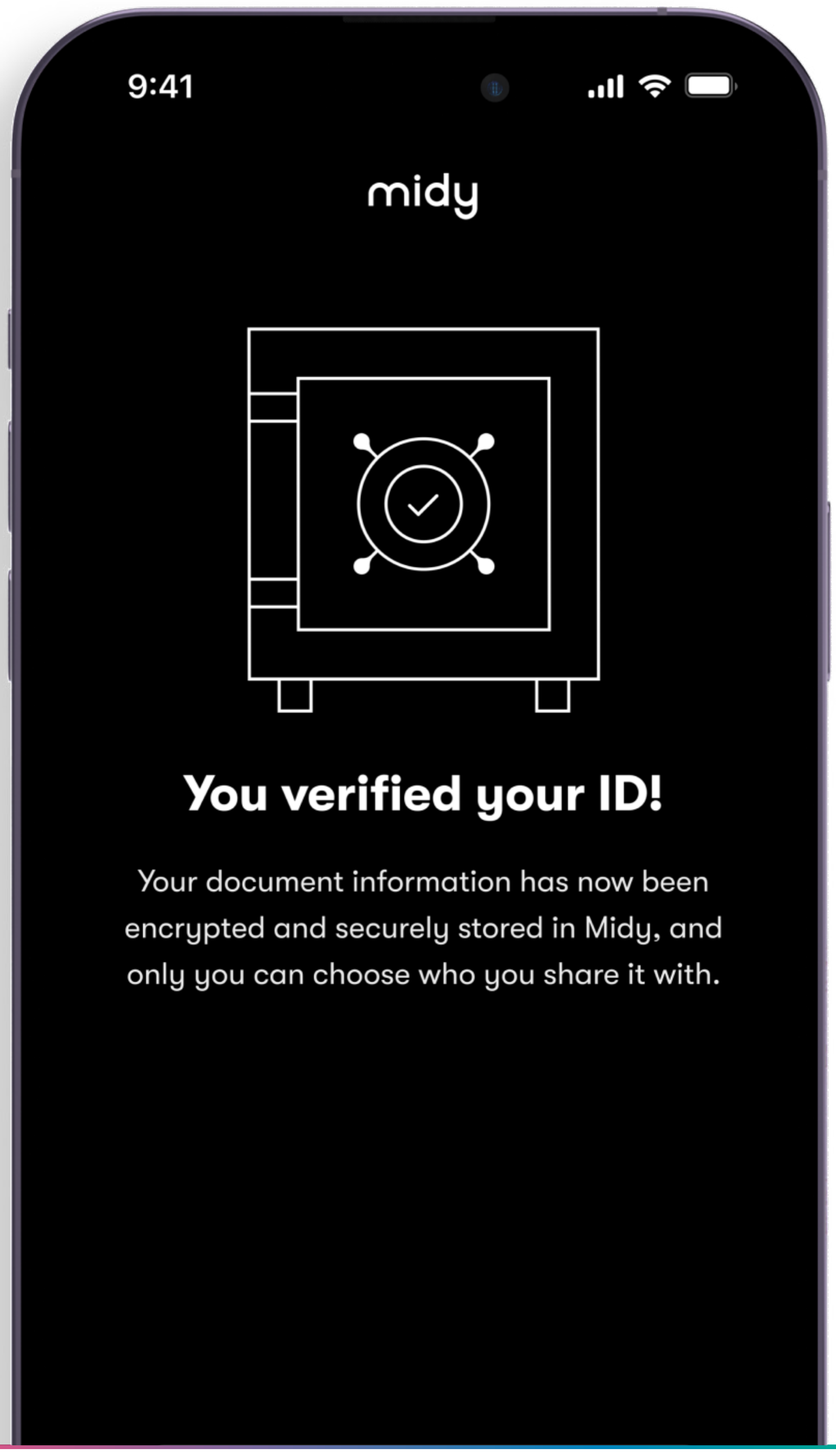
Once scanned or clicked, they will be asked to use their biometric to unlock their Midy app and provide consent to sharing a proof-of-real-human with the service. (Importantly, the user must provide explicit consent for any data that is shared from their Midy).

Once the proof is shared and verified, the user will see a success message indicating that the service has received the proof. In this use case, the proof only contains a Yes/No response to the question: "Is this user a real human?" The service will receive no additional information from their credential unless the user explicitly agrees to share it.

In some cases, organizations may configure their Midy integration to also help track down duplicate accounts or impersonation attempts, in which case the organization may request to access a count of how many times a certain document has been used to verify a unique account on their service or a Yes/No response to whether a name on a government document matches a name on an account profile.

To reiterate, this means that the user only needs to scan and verify their identity document once. They can share that proof again and again with a few quick taps of their phone. This process is easier and faster than a CAPTCHA while providing much stronger proof of a real unique human—a proof that is an order of magnitude harder to fake.

Organizations looking to integrate with Midy to request and verify customer data are encouraged to get in touch with Gen for an overview of our verification tools. These tools enable organizations to enable privacy-preserving data exchange directly with their users and prove authenticity while minimizing the amount of data collected.



You verified your ID!

Your document information has now been encrypted and securely stored in Midy, and only you can choose who you share it with.

What data is shared with organizations?

At the heart of Midy's privacy framework are the notions of explicit consent and data minimization. Users are in full control of their data, and no data can be pulled from their Midy without their explicit consent. The centerpiece of this Privacy by Design architecture is the cryptographic pseudonym generated from the user's identity credential, as explained below:

1. **This pseudonym does not share any personal data from their credential.** It is a large text string derived from the credential using a cryptographic function called hashing. The result does not reveal any data from their credential, yet uniquely identifies that credential.

2. **This pseudonym cannot be "reverse engineered" to reveal any data from their credential.** It is a "one-way mirror." The credential can produce the pseudonym, but the pseudonym cannot produce the credential.

3. **This pseudonym can only be produced by their unique credential.** Every unique digital identity credential will produce a unique pseudonym.

4. **This pseudonym is different for each website or organization the user engages with.** This feature is critical to prevent users from being tracked across multiple online services without their explicit permission. From the base pseudonym, Midy computes a second partner-specific pseudonym for each partner so that the pseudonym users share with each partner is different.

A Midy cryptographic pseudonym is the most privacy-preserving item of personal data a user can share to prove they are a real unique human being—without sharing any other data that could be used to identify them. It is true pseudonymity.

Our promise to Midy users

At Gen, we have spent the last 35 years enabling cyber-safety for our 500M users. We take security, privacy, and user experience very seriously, which means that (a) we have built Midy as a consumer-first tool, and (b) we consider Midy as an extension of our mission to create technology solutions for people to take full advantage of the digital world, safely, privately, and confidently–so together, we can build a better tomorrow.

Here are the promises we make:

1. **Midy users are always in control.** They literally have the keys—the cryptographic keys—to their Midy digital wallet. Only the user can unlock their wallet and access their digital credentials once they are stored inside. The wallet component of Midy is designed as a zero-knowledge service because Gen, as the service provider, does not have the keys. We (Gen) cannot access the data even if a user asks us to. Instead, Midy provides users with robust ways to recover their digital wallet should their device become lost, stolen, or corrupted. The only personal data we store about a user is the data we need to provide the service (which we always encrypt with our own cryptographic keys).

2. **Midy users' credentials belong to them.** These credentials can be used at any participating online service that the user wants to share information with, just like the credentials in their physical wallet. Note: some issuers or privacy frameworks may put their own restrictions on where users can use the credentials they govern. But the decision to use those credentials is up to the user, not Gen.

3. **Midy builds in Privacy by Design.** Gen is designing Midy from the ground up explicitly to help users maintain their personal privacy—for example by using the cryptographic pseudonyms described above. We will continue to develop innovative new privacy features to help users harness the power of digital wallets, credentials, and privacy frameworks.

4. **Midy builds in Security by Design.** Gen has one of the most advanced cybersecurity teams in the world. We will do everything we can to protect every Midy user's wallet from cyberthreats of all kinds, including planned integration with Gen's other cyber safety products.

Build digital trust - without sacrificing privacy

At Gen, we are making it easier for online platforms and other organizations to prove that their users and visitors are real people—not bots or impersonators. In the process, we're enabling organizations to empower their users with full control over their data with the ability to manage what, how much, and with whom it is shared.

The result is safer, more meaningful online experiences for all parties.

If you would like to learn more and explore what Midy can mean for your users, please reach out to our team at www.midy.com.

midy™

Gen