IDEMIA Identity & Security

IDEMIA

‘Identity on the Edge’

Protecting Customers, Companies and Governments with Privacy-First Mobile ID

www.na.idemia.com

INTRODUCTION

The Stakes Are High in the Identity Decade

Digital transformation is affecting all parts of American life. From how we conduct finance and interact with our government, to how we work and conduct business, to how we get to school and even how we gather with our families. At the core of this widespread digital transformation is identity – how we prove who we are in online and offline spaces.

Over the last decade, new technologies like biometrics, cloud computing, mobile devices, secure encryption, and artificial intelligence helped build the basis to allow users to assert their identities online, but user privacy was left vulnerable. Massive data breaches caused by poorly implemented privacy practices and a continued reliance on Knowledge Based Authentication (KBA) led to a proliferation of personal information online, providing the basis for a new wave of synthetic identity fraud.

Thankfully, the solution to protecting identities and empowering users has emerged: IDEMIA Mobile ID, a standards-defining converged identity technology that keeps users safe, enhances their privacy, and improves their experiences as they navigate their digital and physical lives.

IDEMIA Mobile ID is an example of **Identity on the Edge**, a powerful design philosophy that puts privacy first while enabling the full potential of digital transformation to make life safe, secure, and convenient. In this paper, we will further explore the privacy implications of digital transformation and delve into the components of Identity on the Edge in order to illustrate how a robust Mobile ID technology can make strong trusted identity a defining feature of our bright future.

IDEMIA

PART 1

The Importance of Privacy in the Era of Digital Transformation

Online fraud has been a serious concern for years, as digital transformation has continued to sweep across various sectors around the world. But in the wake of the COVID-19 pandemic, alarm bells are going off louder than ever.

The pandemic pushed all kinds of organizations – from banks to government agencies to retailers – into digital channels as social distancing guidelines emerged and lockdowns were implemented. And in many cases, organizations were not fully prepared, and did not have time to implement effective cybersecurity safeguards. Meanwhile, fraudsters followed their targets into the online space, seeking to take full advantage of the relative lack of security.

The State of Play for Fraudsters

The result is a profound threat of online fraud. A TransUnion analysis found that fraudulent transactions targeting international businesses were **up 46 percent** in 2020; LexisNexis, meanwhile, estimates that in the first half of the year, **one in seven new accounts** were likely fraudulent.

The fraud threat is also evolving. Bot attacks and stolen credentials are still in play, but there are also newer, more sophisticated threats such as **synthetic identity fraud** attacks in which AI technologies are used to construct fake identities.

In addition to defrauding organizations and consumers, these identity fraud threats can also lead to serious data breaches. The past year has further illustrated the catastrophic effects of such attacks, with **the infamous SolarWinds assault** having widely compromised government databases, and SITA acknowledging the **breach of customer records** in its U.S. Passenger Service System. And these occurred after high-profile data breaches on the part of Yahoo and Equifax that resulted in massive legal settlements – $117.5 million and a whopping $700 million, respectively.

Outdated Security

Much of this carnage is facilitated by organizations' reliance on outdated security practices, particularly with respect to Knowledge-Based Authentication (KBA). The most familiar form of KBA is the password – a concise token of secret knowledge that, in theory, is known only to the authenticating party. Other popular forms of KBA include PINs, passcodes, and designated questions (e.g., "What was the name of your first pet?").

The key problem with KBA is that it simply has not kept pace with evolving approaches to online fraud. Passwords and PINs can be compromised through brute force attacks, or even guessed, while security questions can be overcome through data searches on the internet. And cracking the password of one account can quickly lead to more intrusions, such as cases in which a hacked email account is used to reset a password for digital bank account access.

Virtually all cybersecurity experts agree that KBA is irredeemably flawed as a security framework, and advocate for the use of more secure authentication factors, such as biometrics.

Post-password Solutions

Biometrics enable one of the most secure approaches to authentication. Unlike authentication based on 'something you know' – such as a password or PIN in a KBA framework – biometric authentication is based on 'something you are'. No one else has access to credentials like your fingerprint or your face, and they certainly can't be guessed or stolen the way a password can. Biometrics are also far more convenient than KBA credentials, as they can't be forgotten and are always at hand.

That having been said, there are still security vulnerabilities to consider with respect to biometrics. One of the most important is the risk of data breaches when biometric templates are stored on a server. If an organization collects end users' biometric data for the purpose of matching during subsequent authentication sessions, that data will be stored in a database that may itself be an attractive target for hackers – especially if it's stored alongside Personal Identifiable Information (PII). A successful hack attack against such a database would have devastating consequences, with sensitive data spilled into the dark web alongside biometric information that could be replicated in future spoofing attacks.

How Personal is Biometric Data?

New AI-enhanced spoofing techniques are on the rise, putting biometric security under threat. We can no longer rely on the strength of biometric authentication alone to prevent scalable hack attacks. A database containing sensitive user data and their biometrics is an enticing honey pot for bad actors. That's why a viable Mobile ID should keep biometrics and authentication on the user device, with the rest of the PII. That's why IDEMIA trusts in Identity on the Edge.

PART 2

Identity on the Edge: A Future-proof Design Philosophy

The fraud and data breach landscape of the current decade cannot be addressed on an individual solution level. Truly safe and privacy-enhancing security requires a paradigm shift that informs the conception and design of digital identity technologies. For IDEMIA, that core design philosophy is called “Identity on the Edge”.

> *Our goal in all this is to put infrastructure in place that allows the state to issue their residents, their citizens, a more modern identity credential, and to keep that data safe and protected, but respond to a request to have it verified when the citizen is the individual whose identity is associated with it is the one that is making the request. We just think that's a really impactful role for states to play, and really increases the level of trust that we can expect related to digital commerce or digital citizen delivery.*
>
> **Matt Thompson, SVP Identity Solutions, Identity & Security, N.A., IDEMIA**

On a system level, Identity on the Edge is built on three pillars that represent the foundation of a robust and user-friendly Mobile ID. These are:

The Issuer System of Record:

One of the key differentiators of IDEMIA Mobile ID is the role of the state Motor Vehicle Administration (MVA) (also known as Department of Motor Vehicles (DMV)) as the idetity issuer. IDEMIA’s decades-long relationships with state MVAs enable the Mobile ID solution to build on the highest level of identity assurance and trust available to Americans. Enrolling in Mobile ID requires an official state-issued ID, which itself is only obtained through a powerful in-person identity proofing event at the MVA. The role of the MVA system of record is to act as the signatory for the data stored on the Mobile ID. This way, when an online account asks for confirmation of a user’s identity, it can trust that the user was vetted at the highest level.

IDEMIA's Identity as a Service (IDaaS):

IDEMIA's IDaaS provides the standards-defining infrastructure that allows for Mobile ID to be deployed at scale with relative ease. The cloud platform acts as a secure throughway between the Mobile ID device holder and the system of record, ensuring that the data on the device is always trustworthy and up-to-date.

A User Device with Mobile ID:

For the end user, their mobile device with their Mobile ID is as trusted as a driver's license, but much more versatile, convenient, and private. A Mobile ID can be used offline in the same way a physical credential can, only with pseudonymous features (like age-checks). But the real game-changer is in how Mobile ID bridges the gap between the physical and online worlds during this time of digital transformation: just as a Mobile ID device can be used to verify a user's identity at a store or government office, it can also be used for secure login online.

The "Edges" in Identity on the Edge are the MVA system of record and the Mobile ID device. This is key to the privacy-forward concept that powers IDEMIA's vision of Mobile ID: a user's personally identifiable information does not need to be shared with a party outside of the identity issuer and the user. For relying parties that need to verify and authenticate users – that is, the entities between those two Edges – this means no need to store databases of valuable PII that are ripe for hacking, while still having the high-level of assurance provided by state-signed digital identity. For users, it means complete control of their identity and data, both online and offline.

At the dawn of the mobile identity wave that started with the launch of Apple's Touch ID in 2013, the initiative to replace KBA with strong authentication like biometrics bifurcated into two camps: de-centralized authentication that occurs entirely on a device and centralized authentication that takes place in the cloud. The Identity on the Edge design philosophy has the best of both worlds: the privacy and security inherent in decentralized authentication, supported by the unmatched assurance, convenience, and interoperability of a centralized system of record. IDEMIA bridges the gaps between the edges with its IDaaS cloud solution, which enables cost-effective scalability.

Mobile ID Versus KBA

As an alternative to KBA, Mobile ID is a versatile and intuitive solution that's as trustworthy as a government-issued document, only used in a digital space. KBA is the standard legacy authentication method online, and it is therefore subject to all the most common and highly evolved fraud methods and hack attacks. A password can be guessed, stolen, cracked, phished, or purchased online in easily available databases for sale on dark web marketplaces. They can also be forgotten, which not only presents a major inconvenience to the user managing KBA credentials for dozens of different accounts, but also presents another attack vector for fraudsters, who can use account recovery methods to gain access to the accounts of their victims.

Even more advanced KBA methods are susceptible. Authenticator apps and SMS passcodes are vulnerable to phishing and other social engineering attacks, while complex password generators still succumb to brute force hacks and database leaks.

Mobile ID uses a variety of different authenticators, including PIN, biometrics, and device factors, but these do not leave the device's secure element, which might allow them to be intercepted. For example, the scanning of a biometric on the Mobile ID could release a key that is used for an online portal, so none of the user's data, biometric or otherwise, leaves their device. The Mobile ID simply confirms you are who you claim to be, and the relying party with the authentication request can trust that assertion because it bears the MVA's seal of approval.

Maintaining Integrity and Interoperability with Liveness Detection

Identity on the Edge can only be achieved with the strongest identity technologies on the market, without which the use cases described in this paper would simply not be viable due to their high-risk nature. An integral aspect of maintaining the chain of trust in an Identity on the Edge system is ensuring that every time authentication is required on the user's mobile device, it is in fact the rightful user and not an impostor.

A biometric credential is naturally more secure than a password or other type of KBA, but advances in fraud methods have raised concerns about presentation attacks, or "spoofs" – hack attacks that use material and digital artefacts in order to trick a biometric system into issuing a positive identification. Fake fingerprints and 3D-printed masks are simple spoofs that can be effective against consumer grade technology, but AI-powered deepfake technologies have challenged some of the best biometric security solutions. This has led to the need for Liveness Detection.

The Full Potential of a Standardized Mobile ID

Standards are more than the frameworks that enable powerful technology like the IDEMIA Mobile ID. They also provide the basis for many integral aspects of business, finance, communication, and identity. Learn more about the standards IDEMIA is bringing to maturity through Mobile ID and IDaaS by requesting the white paper "The Importance of Standards on the Road to Mobile ID."

IDEMIA Mobile ID uses state-of-the-art liveness detection technology – lab-tested and compliant with the ISO 30107 Presentation Attack Detection standard – in order to confirm upon authentication that the credentialed user is present and not an impostor. In doing so, the high level of assurance built on the trusted foundation of the system of record is carried forward on the far edge of the system, with no risk of compromise via stolen devices.

Defining Standards and Interoperability

The ISO presentation attack detection standard is only one component that enables Mobile ID to remain trusted wherever it is used, while ensuring the safest and most private user experience. Because Mobile ID is a new technology meant to build on the long legacy of identity documents across states and eventually between countries, IDEMIA plays an active role in contributing to the international, national, and industry standards that are defining the use of mobile IDs.

By working closely with the National Institute of Standards and Technology (NIST), the FIDO Alliance, and OpenID Foundation, and through its participation in mobile ID and mobile drivers license testing events that improve the drafting of the applicable ISO Personal Identification standard (ISO 18013-5), IDEMIA is ensuring that its Mobile ID is driving forward a unified user experience for Americans online, offline, remotely, and in-person.

PART 3

Mobile ID at the Center of the Identity Decade

With its groundbreaking Identity on the Edge framework, IDEMIA Mobile ID opens the door to a wide range of possibilities for strong identity verification online and in the real world. Innovative applications and use cases will inevitably emerge as more states and jurisdictions beyond the United States embrace the Mobile ID concept. But in the immediate future, Mobile ID is already poised to make a substantial impact in a few areas of daily life, starting with the source of official ID for many Americans.

One Visit for Life

Trips to the MVA can be a serious hassle, with citizens and residents forced to wait in long lineups as overburdened administrators process routine requests. A recent survey found that 90 percent of respondents were **willing to pay** in order to renew their driver's license online and avoid such a visit, with 35 percent willing to spend as much as $20 for that convenience.

IDEMIA's Mobile ID can solve this problem. It takes only one visit to the MVA to create a virtual driver's license, and from there, license holders can perform all kinds of actions through the online channel – everything from renewing a license to registering a vehicle. For a license holder, this means that there is no need to ever return to a physical MVA location.

What's more, that one visit will be made a lot more convenient. That's because widespread use of Mobile ID would mean that the administrative burden on a given MVA is dramatically eased, since so many transactions are being done online, through the app. That will equate to shorter lines, happier civil servants, and much more efficient processing for driver's license applicants.

Curbing COVID

The convenience and administrative benefits that Mobile ID offers made perfect sense before 2020, but in the wake of the COVID-19 pandemic, it's now clear that the solution can also play an important role in mitigating the spread of the virus. This is because Mobile ID brings even more services into the mobile channel, reducing the need for the kinds of in-person interactions that can facilitate the spread of the virus.

Curbside pickup offers one illustrative use case. Mobile ID could be used to identify a consumer during an online purchase, and then can be presented by the consumer outside a store for convenient curbside pickup with no need to hand over a physical driver's license or other proof of identity, facilitating an entirely contactless process that minimizes face-to-face contact.

In a similar vein, Mobile ID could be used for an expedited, automated bag drop process at the airport; and it can be used to remotely open a bank account, bypassing the need for an in-branch identity check. These are just a few examples of how bringing identity verification into the mobile channel can reduce the need for face-to-face interactions and curb the spread of COVID-19.

These potential use cases help to illustrate the enormous promise of IDEMIA's Mobile ID. In the near term, meanwhile, a number of states are already embracing the mobile driver's license solution on the basis of its more immediate benefits. Oklahoma became the first by launching its own **Oklahoma Mobile ID** in 2019, and was followed by **Delaware, Iowa, and Arizona**. Additional deployments are in the pipeline as more states recognize the immediate benefits and massive potential of Mobile ID technology.

CONCLUSION

The Edge of Identity Innovation

Digital transformation is only accelerating, and thanks to a Mobile ID solution developed under the Identity on the Edge design philosophy, Americans across the country will be able to navigate their online and offline lives with confidence, convenience, and safety, assured that their privacy is being protected, and their identity is safe.

About IDEMIA Identity & Security:

A trusted partner to U.S. government agencies for more than 60 years.

We are a global leader in providing identity-related security services to governments and private companies. Our mission is to help people access what matters most faster, safer, and more securely in both the physical and digital worlds. We accomplish this by helping to capture, authenticate, and secure both physical and digital transactions for citizens and consumers alike.

IDEMIA Identity & Security USA LLC is administered, managed and operated by U.S. staff on U.S. soil for all services provided to U.S. government customers at the federal, state, local, and tribal levels.

For more information, visit: **www.na.idemia.com**

IDEMIA