Deloitte.

Picture perfect

A blueprint for digital identity

Contents

Introduction

Dear Colleagues,

Every industry is rooted in a breakthrough technology. Frozen concentrate propelled orange juice into a worldwide commodity. The transistor became the foundation of today's electronics. Anesthesia (along with the germ theory of disease) ushered in the era of modern surgery.

And then there's digital identity.

The identity systems we have today are slowing innovation in FinTech. They're also getting in the way of delivering financial services online. Digital global transactions, so close at hand, will come about only when digital identity does.

With all this in mind, Deloitte Consulting LLP (Deloitte) and the World Economic Forum recently completed a yearlong study of digital identity, *Disruptive innovation in financial services: A blueprint for digital identity*. The goal? To understand the role that financial institutions should play in building a global standard for digital identity.

This document is a summary of the findings. It begins with an examination of identity and its importance to FinTech, financial services and societies in general. Next is a look at digital identity itself—what it is, what digital identity systems look like, some guiding principles for building them and the benefits we can expect to see. Lastly, we imagine some of the ways digital identity might apply to the business of financial services.

If you help determine the direction of financial services, this summary is for you. It should give you a general idea of the nature of identity and its broader role in how we live. We hope it also gives you a sense of urgency about building digital identity systems for financial institutions and beyond. By the time you reach the last page, you might find yourself agreeing that the time for action is right now.

Sincerely,

Bob Contri

Global Leader, Financial Services
Deloitte Touche Tohmatsu Limited
bcontri@deloitte.com

Rob Galaski

Deloitte leader for The Forum Future of FSI project
Deloitte Canada
rgalaski@deloitte.ca

Digital identity and the role of financial institutions

User identification is a vexing problem for FinTech. Today, a transaction that requires identification—whether for a payment, a loan or something else—means either collecting physical proof over a digital channel (such as by photographing a driver's license) or relying on the know-your-customer (KYC) processes of established financial institutions. Until this problem is solved, a purely digital FinTech offering will remain in the future.

The linchpin of online transactions

Customer identification is important because it's at the center of many financial services processes. Institutions need it to comply with regulations, assess risk for insurance and credit and provide a tailored customer experience. Detail and accuracy are critical. Digital identity promises to improve these while removing inefficiencies from processes that are largely manual today.

But digital identity isn't relevant to financial services only. Think about the public services that require proof of identity: old age security, unemployment insurance, education, healthcare, polling and more. Proof of identity is also necessary in many aspects of private commerce, such as buying alcohol, renting an apartment and purchasing a car. All this exposure puts people and organizations at risk. When it comes to physical identity systems, theft and fraud are seldom far from our minds.

And the need for a digital solution is becoming urgent. Transactions are growing in volume and complexity. Customers increasingly expect seamless, omni-channel service delivery and will take their business elsewhere if they don't get it. Regulators, for their part, are demanding greater insight into transactions. They'll hold firms responsible if identity information is missing or inaccurate.

Finally, the sophistication of digital attacks is rising. Hackers can exploit weak identity systems more readily than ever, wreaking financial and reputational havoc in the blink of an eye.

A multilayered problem

So where do we stand with digital identity systems? One way to understand this is to view it as a multilayered problem. At the bottom are the standards that govern system operation. These need to be developed. At the top is service delivery, which must be efficient, effective and seamless to users. In between are authorization, attribute exchange, authentication and attribute collection. Each of these has its own set of challenges.

Many efforts today address one layer but not others. For instance, authentication technology solutions tend to rely on attributes that have already been collected. These solutions provide a better experience for users and ensure that the same person is transacting each time, but it doesn't help identify who that person really is.

Other solutions address a particular type of transaction only. They might facilitate the delivery of a government service, for example, and that's all. This approach also ends up collecting "tombstone" data—things like name and date of birth—rather than data that paints a more nuanced picture of the user.

Finally, we see a lot of consensus-building around standards and processes at the expense of building a full-fledged identity solution that could be put into broad commercial use.

Identity layer	Purpose	Problems
Service delivery	Offer seamless services to users	Inefficient or unsuited delivery
Authorization	Provide the services to which users are entitled based on their attributes	Complex authorization rules and relationships
Attribute exchange	Provide ways to exchange attributes between parties	Lack of security and compromises to privacy
Authentication	Provide ways to link users to attributes	Weak or inconvenient authentication
Attribute collection	Capture and store user attributes	Inaccurate or insufficient attribute collection
Standards	Develop standards to govern system operation	Lack of coordination and consistency

The search for common ground

These gaps are the result of a crowded digital identity landscape. Technology companies, professional organizations and governments are all carving out territory. That's fine. A solution can be valuable without addressing the whole stack.

But there needs to be some way to tie solutions together so they form a strong identity system. Something that's convenient, effective, lets users control their information and protects their information where it is in use. Something that can handle large transaction volumes and makes good sense for everyone involved. That all this is obvious doesn't make it easier to carry out, of course.

That's why financial institutions should take the lead. They're exceptionally well positioned to close the gaps in digital identity.

For one thing, institutions perform many digital identity functions as a normal course of business. They store and verify user information already. Their operations span multiple jurisdictions. They have a proven ability to create new systems and standards (see: Interac). In developed economies, their coverage of people, legal entities and assets is nearly complete.

What's more, they're mature. Financial institutions' operations and use of customer data are strictly regulated. They're the intermediary of record in many transactions. Consumers trust financial institutions with their information and assets more than they do many other custodians.

The benefits of being in front

What's in it for financial institutions? Three things: efficiency (with all its cost avoidance), revenue, and transformation. Let's take a look at each.

Efficiency. A reliable, consolidated bank of user attributes can take time and the potential for human error out of the business process. It might also create new ways to serve customers and build better risk profiles.

Revenue. More customer knowledge can reveal needs for new products and services for those customers. It can also open opportunities to earn revenue from other businesses who lack access to that kind of customer information or don't wish to hold it themselves, or from people who aren't customers but must verify their identities for some other purpose.

Transformation. With digital identity, firms might look beyond their current business. They could serve as a trusted broker between parties in other industries and provide identity services to the public sector (think social services and tax filing). They could also shift the liability for wrong information back to users and eliminate third-party data mining in the evaluation of customer credit history. Customer service might extend to non-financial advisory work.

There are several ways to set up an identity system. Which way depends on the situation. We'll get into that shortly, but first, let's review the kinds of problems that identity can create for financial institutions.

The global identity challenge

Financial institutions are familiar with the difficulties of collecting the information they need to verify identity. Compliance, due diligence, KYC—none of these processes is known for its efficiency, especially in light of the obligation to protect personal information.

And these are general challenges. Consider the additional ones that retail banks, not to mention banks serving small- to medium-sized enterprises, must contend with. Lack of visibility into new customers' financial histories makes it that much harder for firms to prevent fraud and provide suitable products and services.

Then there's corporate and investment banking, which have identity-related struggles of their own. Tracking asset origination and ownership is one. Another is monitoring and tracking asset rehypothecation.

Much of this pain has a common source. It stems from a system that was designed to support face-to-face transactions. Put another way: We have a modern digital economy that still depends on physical records to establish identity.

So what's the alternative? What would a digital identity system look like?

In a digital identity system, "identity" is a set of digital records that represents a user. These records are held in a standard format by entities that provide the identity information or assurance needed to complete transactions. A digital identity also accepts and integrates new records to create a rich view of the user.

A system like this makes it easier to collect and share supporting documentation. Thanks to cutting-edge authentication and security protocols, a digital identity system also makes it harder to damage, lose, steal or tamper with identification records. Finally, digital identities offer customer-serving institutions, such as financial service institutions and many others, a better way to know and serve their customers.

Some promising technologies are bringing us closer to a digital identity system. Advancements in data storage offer improvements in storing user information, along with greater privacy, security and user control. New data transfer protocols tighten protection against interception and decryption while again putting more control in users' hands. New authentication techniques are in development as well. These link users to their digital activities in more robust and persistent ways.

The path has been bumpy, though. Amid all the new technologies in development around the world, some have failed already. Obviously if the system isn't designed well, doesn't work well or doesn't seem trustworthy, people simply won't use it. And any development effort might run out of capital. But there are subtler pitfalls as well, such as serving a too-narrow set of interests or winding up on the wrong side of public policy. This underscores the idea that digital identity must deliver a range of benefits to people, businesses and society.

A primer on digital identity

An identity is made up of many different pieces of information, also called attributes. The more attributes there are, the stronger the identity. That's true even if an attribute is unique.

For example, the state can issue someone a unique number. But the number tells you almost nothing by itself. If you also have the person's name and date of birth, you know a bit more. Add a photo, mobile number, residential address, school records and work history, and suddenly you know quite a bit more.

People aren't the only ones who have identities. So do legal entities (such as corporations and trusts) and assets (property). The attributes that go into your identity help others decide whether to engage in a transaction with you—accept your vote, open a savings account, sell you a bottle of wine and so forth. The same is true for legal entities and assets. Their identities, or rather certain attributes of them, help others decide whether to do business with the appropriate owner, representative or custodian.

Assurance is a key factor in identity transactions. It refers to the degree of certainty that the identity is real and belongs to the person using it. Some transactions, like registering on a news site or paying a parking ticket, might not be worth all the work it takes to authenticate an identity to a high degree of certainty. The opposite is true for transactions like using an online brokerage account or receiving certain government services. Those must be high assurance transactions.

Another facet of identity transactions is that they tend to form networks depending on the kind of identity. For example, government identity systems and employee management systems form around individuals. Business registries and industry identifier systems form around legal entities. Asset registries form around...well, you get the idea.

But all identity systems have some things in common. They all have **users**—the ones who get an identity in the system so they can carry out transactions. They all have **identity providers**—those who store user attributes, make sure they're real and complete transactions on the users' behalf. There are also **relying parties**, the ones who serve users after identity providers vouch for them.

In addition, all systems have a governance body that oversees the system and makes the rules. And beneath it all is some kind of platform that completes the transactions by providing all parties with what they need.

So far, none of this is new. It's the same system that people have used throughout history. Someone arrives at an employment office bearing a letter of introduction; he's a user. The letter is from someone who vouches for the user; she's an identity provider. The one to whom the letter is addressed is the relying party. The relying party decides whether to accept the letter's claims based on their own judgment and what they know about the identity provider.

A digital identity system follows this same process, but electronically. Everything happens online. But digital identity has a number of advantages. It's easier to share among all parties of a transaction. It can include much more information than a collection of physical documents. And with the proper technology, it can give users much more control over how their information is stored and used.

The landscape of digital identity systems

Digital identity systems fall into five basic categories.

The first is **internal identity management**. In this kind of system, the same party serves as identity provider and relying party. For example, a company might let employees access different services based on their attributes.

The second type of system is **external authentication**. It's similar to the first type of system, but with an extra set of identity providers to authenticate users. The advantage here is that users can use one set of credentials rather than maintaining different usernames and passwords for each service.

Centralized identity is another. In this type of system, one party (such as a government) is an identity provider that transfers user attributes to relying parties. An example is a citizen registry that lets users vote, file taxes, and so forth. A relying party can be a public entity or a private one. A private entity might access data after paying a fee and obtaining user consent.

Next are **federated authentication** systems where one identity provider uses a set of third parties to authenticate users to relying parties. These systems are similar to centralized identity systems except that a variety of private brokers issues the digital identities as a service to whomever subscribes.

Lastly, **distributed identity** systems connect many identity providers to many relying parties. This type of system sets users up with a digital "wallet" that serves as a universal login to multiple websites and applications. Generally these systems are privately held and rely on common operating standards rather than a governing body.

01 **Internal identity management**	The same entity is both identity provider and relying party	Best for managing user permissions inside a single entity based on internal information, to ensure the right individuals have access to the right resources
02 **External authentication**	Many identity providers authenticate users to a single relying party	Best for streamlining user access to a suite of services that are offered by a single entity, eliminating proprietary logins
03 **Centralized identity**	One identity provider serves many relying parties	Best for providing a complete, accurate and standardized view of non-confidential data across different users
04 **Federated authentication**	A set of identity providers authenticates users to many relying parties	Best for providing a complete, accurate and standardized view of data while allowing users to authenticate to multiple entities, eliminating proprietary logins
05 **Distributed identity**	Many identity providers serve many different relying parties	Best for user convenience, control and privacy in an online environment

Guiding principles

A successful natural identity network should be based on five principles.

The first of these is social good. That is, an identity system should provide identity to all users, serve user interests and be open to all who wish to participate. Financial institutions, with their many user relationships, can influence this inclusiveness and help drive system adoption.

Second, identity systems should protect user information. Current identity systems put users at risk. They leave user information vulnerable to privacy infringement, data leakage and overexposure. A digital identity system should ensure that relying parties see only the data they need and use it only for the purposes they disclose. For financial institutions, this means identity systems should be cyber-resilient and meet standards for data protection and storage.

This leads to the next principle, which is to give users control over the storage and transfer of their personal information in the identity system. More than one identity system has failed because users didn't trust it. Under this guidance, financial institutions will need user consent before accessing or sharing identity information.

Next is to treat an identity system as a sustainable, long-term business. Stakeholders should know that their investment will pay off. As important and trusted private entities, financial institutions have a key role to play in shaping the system's operational requirements and standards. There also may be the opportunity to monetize identity-as-a-service.

The last principle is to build identity systems on open technology and data standards. Design them to integrate new parties and serve changing user needs. The implication for firms is that this will make it easier for users to switch financial institutions.

Building a successful identity network is difficult. Who will the users be? What problem will the identity system solve? How you answer these questions will help you determine what type of system to build. Then the guiding principles for identity, along with their implications for financial institutions, will help you make the appropriate choices for everything else.

Guiding principles for digital identity

- **Social good.** The system is available to all users and delivers maximum benefit to a range of stakeholders.
- **Privacy-enhancing.** User information is exposed only to the right entities under the right circumstances.
- **User-centric.** Users have control over their information and can determine who holds and accesses it.
- **Viable and sustainable.** The system is sustainable as a business and withstands shifting political priorities.
- **Open and flexible.** The system is built on open standards to allow scaling and development; standards and guidelines are transparent to stakeholders.

Benefits

Done right, a digital identity network would benefit not only financial institutions but those they work with as well: users, identity providers, relying parties, governments and regulators.

Network stakeholders

Privacy

Users can control who has access to their attributes.

Security

User attributes are held in secure locations, while relying parties know who's legitimate.

Transparency

Users know how and when their attributes are exposed.

Convenience

Digital attribute transfer makes user transactions more efficient.

Positioning

By forging a strong relationship with users, identity providers become a critical part of the digital economy.

Closing

A streamlined user experience removes barriers to completing transactions.

Offerings

Customer details help identity providers and relying parties deliver tailored products and services.

Revenue

Relying parties make it easier to complete transactions, while identity providers can charge to process them.

Risk

Identity providers and relying parties understand their liability in the event of a data loss or breach.

Governments and regulators

Process

Governments can interact with citizens more efficiently, saving time and money.

Service delivery

It becomes easier for governments to identify and deliver services to various groups of citizens.

Assets

Regulators have a better way to trace asset origination and ownership.

Entities

Regulators gain an aggregated view of legal entities across their hierarchies.

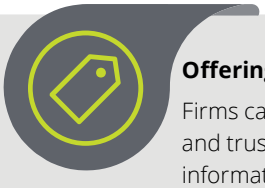
Compliance

Regulators access trusted, up-to-date user attributes, strengthening the overall compliance process.

Data

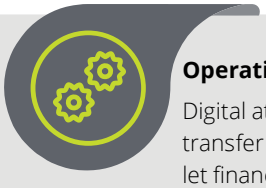
Data collection and storage are standardized across all financial institutions, removing friction from data aggregation.

Financial institutions



Offerings

Firms can use detailed and trusted customer information to provide customers with tailored services.

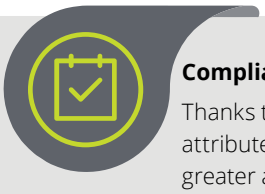


Operations

Digital attribute transfer and handling let financial institutions streamline and automate many processes, eliminating human error.

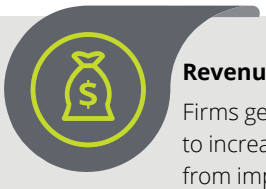
Security

The secure, digital storage of user information reduces fraud resulting from stolen information or compromised authentication.



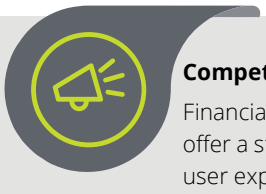
Compliance

Thanks to digital attribute handling and greater access to user identity, compliance becomes easier and more accurate.



Revenue

Firms get the chance to increase revenue from improved products and services as well as offer identity-as-a-service.



Competitiveness

Financial institutions offer a streamlined user experience and position themselves as a critical part of the digital economy.

Future applications

Beyond its inherent benefits, what would digital identity look like in the business of financial services? As usual with new technology, that depends on how it's used. Here, we explore eight potential applications.

Tailored risk profiles. Financial institutions create a risk profile from a combination of predictive algorithms and whatever information they collected about the customer. In the future, institutions might make use of the attributes already in the user's digital profile, along with a range of other attributes the user might choose to provide. With more and better-quality information becoming available, firms could create custom risk and credit products for their customers, in turn encouraging those customers to stick around.

International resettlement. Without proof of identity, anyone trying to open an account is out of luck. If they can establish identity but not financial history, the financial institution might have to move forward anyway if it wants the business. But this tedious "blank slate" situation could be avoided if users bring along a digital identity. Anywhere in the world, users could access financial and other services on the strength of attestations and attributes collected by previous institutions. And each new institution becomes another identity provider, further strengthening the user's digital credentials.

Attributes tied to payment tokens. Suppose you never again had to manually confirm your age, shipping information, or anything else at the point of sale. Digital identity could make this a reality by enabling merchants to get the information they need straight from financial institutions, with the consent of the user. The digital transfer of attributes would be free of potential for human error and help more transactions close. Add authentication to the mix, and the potential for fraud also goes away.

Digital tax filing. Right now, individuals and businesses alike must gather information from multiple sources—financial institutions, employers, schools and so forth—before they can file their taxes. But digital identity might persuade governments to accept filings from taxpayers' designated financial institutions instead. Firms would use their complete knowledge of customers' financial holdings, assets, income and personal circumstances to automatically complete returns.

Determining total risk exposure. Legal entities often have a hard time determining their total risk exposure in a transaction, thanks to complicated ownership structures and the amount of work that due diligence requires. Digital identity could provide a consolidated view of each party in a transaction, allowing companies to answer their own questions about risk in a much more convenient way.

Identifying transaction counterparties. Identifying all the participants in a brokered transaction can be next to impossible today. But with digital identity, legal entities could ask to look into the consolidated identity of a third party and the ownership history of whatever asset is involved. Knowing more about the direct customer and the end customer would lead to a more informed decision about completing the transaction.

Linking individual identity to corporate identity. Companies are not necessarily linked to all the people affiliated with them. If the identity attributes for both individuals and legal entities were digitally collected, stored and transferred in a standard way, financial institutions could get reliable insight into their relationships. The accurate, up-to-date information would serve KYC and many other purposes.

Tracking total asset rehypothecation. When assets are rehypothecated, their transaction and ownership history can become ambiguous. This creates counterparty risk and makes it hard to determine the asset's fair value. Also, the lack of an historical tracking mechanism prevents enforcement of limits on the extent of asset rehypothecation. Consolidated, standardized and digital asset information would make it possible to check such things as issuer and transaction history. This would help to prevent over-rehypothecation and make transactions less risky all around.

Conclusion

Will there be a single, global solution for identity? Don't count on it. It might not make sense anyway, so long as we have a principled basis for building and connecting identity networks.

For one thing, identity needs vary by user. Individuals need to complete transactions safely and conveniently. Legal entities need a comprehensive way to aggregate data for managing risk. Assets need a tracking system that provides transparency around ownership and value.

Another lens is privacy. Individuals must have it. Legal entities and assets can do without it; in fact, privacy might even interfere with their larger purpose. In any case, individuals have self-determination, whereas legal entities and assets have custodians who act on their behalf.

Also, identity is cultural. The people of some nations accept a national ID card. Others don't. Some governments might not be stable enough to carry out digital identity.

So there's no one-size-fits-all solution. Different groups will build their own identity networks. That's probably as it should be. Even so, at the highest level all networks do share the same basic path to development:

01. Know who you're trying to serve.
02. Understand the needs you're trying to fulfill.
03. Decide who must be involved to bring the system to fruition.
04. Figure out a way to work together—be it as a private partnership, a consortium, a utility or some other model.
05. Describe what the solution must be able to do, and translate that into technical requirements that a system developer can follow.
06. Assemble the solution, test and launch.

We encourage firms to consider a bottom-up approach to digital identity. First, test and refine the system with a critical mass of parties. Then gradually scale it to include more users, relying parties, and identity providers.

Here's another thing financial institutions can do as a group: Build the connectors between the networks. This is what allows digital identity networks to form within their natural boundaries, serving constituents in the ways that suit them best, indefinitely. They're the rails of interoperability—and among them, they allow a global blueprint for digital identity to emerge.

Contacts

Global contacts

Bob Contri

Deloitte Touche Tohmatsu Limited
Global Leader, Financial Services
New York
bcontri@deloitte.com

Rob Galaski

Deloitte Canada
Deloitte leader for The Forum Future of FSI project
Toronto
rgalaski@deloitte.ca

Neal Baumann

Deloitte Touche Tohmatsu Limited
Global Leader, Insurance
New York
nealbaumann@deloitte.com

Joe Guastella

Deloitte Touche Tohmatsu Limited
Global Leader, Financial Services Consulting
New York
jguastella@deloitte.com

Anna Celner

Deloitte Touche Tohmatsu Limited
Global Leader, Banking & Securities
Zurich
acelner@deloitte.ch

Ted DeZabala

Deloitte Touche Tohmatsu Limited
Global Leader, Cyber Risk Services,
New York
tdezabala@deloitte.com

Cary Stier

Deloitte Touche Tohmatsu Limited
Global Leader, Investment Management
New York
cstier@deloitte.com

Vikram Bhat

Deloitte United States
Global Leader, Financial Services Cyber Risk Services
New York
vbhat@deloitte.com

Regional contacts

Americas

Rohit Malhotra

Deloitte United States
rmalhotra@deloitte.com

Linda Pawczuk

Deloitte United States
lpawczuk@deloitte.com

Andre Romanovskiy

Deloitte Canada
aromanovskiy@deloitte.ca

Europe, Middle East and Africa

Michel De La Belliere

Deloitte France
mdelabelliere@deloitte.fr

Nick Seaver

Deloitte United Kingdom
nseaver@deloitte.co.uk

Chris Verdonck

Deloitte Belgium
cverdonck@deloitte.com

Asia Pacific

Trey Gannon

Deloitte Australia
tregannon@deloitte.com.au

Mitsuhiko Maruyama

Deloitte Japan
mitsuhiko.maruyama@tohmatsu.co.jp

Tse Gan Thio

Deloitte Southeast Asia
tgthio@deloitte.com

A special thank you to Christine Robson from Deloitte Canada for her help with this report.

Deloitte.