Building a global digital identity infrastructure

Received (in revised form): 18th January, 2022

Gottfried Leibbrandt*
Author and Adviser, Belgium

Daniel Goldscheider**
Chief Executive Officer, yes.com, Switzerland

Gottfried Leibbrandt

Daniel Goldscheider

***Gottfried Leibbrandt** is a former CEO of Swift, the cross-border payments network. He is currently on the board of CLS, as well as the advisory board of yes.com. He is the co-author of the book 'The Payoff: How Changing the Way We Pay Changes Everything'. He also serves as senior adviser to McKinsey & Co, where he was a partner before joining Swift.*

***Daniel Goldscheider** is the Co-founder and CEO of yes.com, a leading application programming interface ecosystem. He has previously co-founded Mediaguide with the American Society of Composers, Authors and Publishers and Aureus Private Equity in Switzerland. Daniel is currently on the board of directors of Valamar Riviera d.d., the largest hospitality company in Croatia, and the Global Footprint Network. He is a consultant and investor in numerous startups.*

Abstract

This paper lays out the need for an electronic identity infrastructure. After describing the landscape, current alternatives and hurdles to overcome, it proposes a way forward, based on the recently launched Global Assured Identity Network, which leverages existing identity and authentication mechanisms. This network uses an architecture that keeps the customer in full control of their personal data, and is based on OpenID Connect and Financial Grade API. The proposed solution is described in detail, including the way to adoption and the trade-offs and considerations that underpin it.

Keywords: GAIN, digital identity, digital infrastructure, industry initiative, open standards, OpenID, FAPI

**E-mail: gottfried@leibbrandt.com*

***yes.com,
Hafenstrasse 2,
8853 Lachen,
Switzerland
E-mail: daniel@yes.com*

Journal of Payments Strategy & Systems
Vol. 16, No. 1 2022, pp. 68–74

1750-1806

INTRODUCTION

As the number of transactions conducted online increases, so too does the need for individual and corporate entities to identify themselves remotely. The COVID-19 pandemic has accelerated the shift to transacting online, but it has also highlighted how even advanced economies lack an electronic identity (eID) infrastructure. Instead, public as well as private services have had to rely on workaround solutions, such as asking customers to show passports on video conferences, scan and then e-mail signed contracts, or use their social media accounts to log into third-party apps. These solutions are cumbersome, inefficient, and susceptible to fraud and/or the theft of personal data. There has to be a better way.

At the same time, this lack of a better solution reflects the challenges inherent in building a modern, global digital identity infrastructure. These challenges include the need for participant adoption, preventing the proliferation of sensitive data and ensuring consumers remain in charge of their own identity data, and providing interoperability so that solutions can be used across providers and countries. The need for such a digital identity infrastructure and the inadequacy of existing solutions has been widely recognised, notably by authorities such as the EU.[1]

Fortunately, recent advances in technology enable solutions that overcome these challenges. Recently, over 150 digital identity experts and financial institutions indicated their support for the proposed Global Assured Identity Network (GAIN).[2] This network offers an eID infrastructure

that leverages existing identity and authentication mechanisms, without the proliferation of data, ensuring the customer remains in full control of their own personal data. This is made possible by recent developments in technology, notably standardised application programming interfaces (APIs) and open standards like OpenID Connect and Financial Grade API (FAPI).

This paper surveys the challenges in building a global identity infrastructure and proposes a way forward. In what follows, it summarises the essentials of digital identity and the key players. It then goes on to describe the main challenges and hurdles to establishing a digital identity infrastructure. The opportunity for building a global assured identity network is then explored in more detail, followed by a discussion of the GAIN initiative, along with the trade-offs and considerations underpinning GAIN. The paper closes with a brief summary of the conclusions and some thoughts about what the future has in store.

THE DIGITAL IDENTITY LANDSCAPE

The term *identity* is used for a wide range of concepts, including 'the set of qualities and beliefs that makes an individual different from others'.[3] *Digital identity* can similarly refer to a host of things, ranging from data such as name, date of birth and address, to things like creditworthiness, medical records and reputation (for example a seller on eBay, host on Airbnb or driver on Uber), as well relationships (eg on LinkedIn or Facebook), etc. This paper sticks with a narrow definition of personal data (ie name, date of birth etc), although the proposed solution can be easily used for other types of identity data.

The identity data themselves should also be distinguished from the concept of authentication, which refers to an authority *other than the customer* confirming the veracity of the data in a verifiable way. To use the offline analogy of a passport: it contains identity data such as a person's name, date of birth and citizenship, with the passport issuer (typically a government) confirming the veracity, and features like a (tamper-proof) photo providing verification. Any digital identity infrastructure will have to offer not only the identity data, but also a level of authentication commensurate with context in which the data are used.

Opening a bank account requires much stronger authentication than, say, signing up for a newsletter. In Europe, the electronic Identity Authentication and trust Services (eIDAS) regulation provides a framework for these varying levels of data quality and authentication. It specifies several levels of trust, ranging from weak to very strong, and qualifies the different schemes accordingly. Many schemes allow for multiple eIDAS levels, depending on the specific data source and authentication mechanism used by the consumer.[4]

The present paper focuses on identity for individuals. Legal entities like corporations also have a (digital) identity, but in practice the concept is more complicated and requires identity for individuals as well. For many applications, such as signing contracts, it involves not only a unique global identifier, such as the ISO 17442 LEI code or the (domestic) VAT numbers, but also data on the individual representing the entity as well his/her authority to represent the company, including financial limits etc.

While there are many players active in the identity landscape, it is useful to focus on two main categories: identity providers and relying parties. The latter are companies that rely on the (authenticated) identities provided by the former. Consider for example the identity services offered by Google and Facebook. These services allow an individual to log in to a third party, for example a cloud application like Dropbox or a news website (acting as relying party), using their Google/Facebook name/ID and password and in conjunction with identity data

already stored at Google or Facebook (the identity provider).

Many parties of course establish their own credentials and thus serve as both relying party and provider. Using the single sign-on (SSO) service provided by, for example, Google and Facebook, allows many online players to do away with being their own customer IDs and passwords (or even second-factor authentication). In addition to big tech, there are two other important categories of eID provider: governments and financial institutions.

Governments have always been issuers of identity in the offline world, using mechanisms like passports, identity cards and driving licences. Several governments have also taken this role to the online world. In Belgium and Germany, for example, the authorities issue digital identity cards with a chip that stores a digital identity certificate that can be used online to sign into government services.[5] In the Netherlands, authorities have established DigiD, which requires a visit to the town hall or post office to set up, but after that can be used online to sign into government and other services.[6]

Financial institutions have traditionally relied on their own authentication. They typically rely on government issued IDs (such as a passport) when they first onboard a customer (often involving a physical visit to a branch), combined with their own authentication through a password and/or one-time password/token etc. As banks are obliged to comply with 'know-your-customer' (KYC) regulations and must verify the customer's identity themselves, there is a clear opportunity for them to provide identity services to others, much like Google and Facebook do, but with a higher assurance level.

KEY CHALLENGES AND HURDLES

Any initiative to establish a digital identity infrastructure faces several challenges, of which the two most important are adoption and strong authentication/assurance. To start with adoption, any initiative will have to overcome the chicken-and-egg problem of gaining traction among providers and relying parties. One can think of this landscape as a two-sided market, where adoption for a relying party is only interesting if the solution offers access to a large share of providers, and vice versa. Not surprisingly, most digital identity initiatives have started from an established base in at least one of these two groups. Google and Facebook, for example, started out by leveraging their global presence to become attractive identity providers for relying parties. Thanks to their near ubiquity, the two companies can offer a relatively broad set of data informed by access to their users' search history or social network. They do, however, face the second hurdle of strong authentication/assurance. Key data such as date of birth and user name are often self-declared and not verified (if available at all) by third-party authorities, allowing users to provide false names and dates of birth.

As mentioned earlier, banks do have both identity data and strong authentication. But as most banks have a relatively modest market share, this requires cooperation between banks in order to achieve user reach that is attractive for relying parties. In several countries, banks are indeed cooperating with each other to establish such an identity service. Examples include BankID in Sweden and Norway, as well as yes.com in Germany. In Belgium, meanwhile, banks have cooperated with telcos and the national ID scheme to offer Itsme, which is being widely adopted as a national SSO solution.[7]

Open banking regulations like the EU Revised Payments Services Directive force financial institutions to make account information freely available to regulated companies, such as certified account information service providers.[8] Banks have an opportunity to establish APIs that make additional premium data available for

aggregators as well as individual relying parties. This can provide the basis for a powerful freemium model.

In addition to schemes where banks cooperate, there are also commercial providers that provide access to multiple banks. Examples of such 'aggregators' or third-party providers (as they are often called in Europe) include Plaid and Klarna. Aggregators help developers by providing a single API integration and contract to accept. However, they also increase the attack surface and can weaken privacy as they process and/or store data.

THE OPPORTUNITY TO BUILD A GLOBAL ASSURED IDENTITY NETWORK

The bank-identity based schemes described above are often referred to as 'federated identity' requiring the cooperation of multiple parties to provide the authenticated data to the relying party. This requires the careful orchestration of information flows between the identity provider, the relying party and the consumer, who, after all, must grant permission to share his/her personal details.

Technology has evolved rapidly and now offers a set of mature tools to achieve this orchestration with minimal proliferation of data. The key ingredients here are APIs and the OpenID Connect standard, which itself rests on top of the OAuth standard. An example of an initiative based on this approach is yes.com, which facilitates direct access by a customer of a relying party to the provider (typically a bank) that holds their data. Crucially, there is no need to store any identity data along the way, leaving the customer fully in charge of their data. Figure 1 illustrates the resulting architecture.

There is a clear opportunity to use this architecture to provide a global solution, consisting of providing access to (interoperability with) existing solutions like BankId in Sweden or yes.com in Germany, while also signing on new providers and relying parties in other geographies.

As shown in Figure 1, the concept is to build a network, where every identity provider exposes a standardised API towards relying parties. This concept allows identity providers to be part of the network independent of their current architecture, technology and philosophy (eg federated or SSO). The idea is to maximise the number of existing identity solutions — and their available reach in terms of users — to take part in such a network while minimising the effort needed for integration.

The network maintains a directory of all scheme participants, which allows them to establish secure and trustworthy connections. It also provides a function for the user to select the identity provider they want to use in a certain transaction. The data are exchanged directly between providers and relying parties. This architecture will also allow third-party services providers to augment the network with value-added services, exposed via APIs and backed by identity data and consent provided by/through the identity providers.

THE GAIN INITIATIVE

On 13th September, 2021 (three days before International Identity Day) the GAIN initiative was unveiled, with the support of over 150 digital identity experts and financial institutions. The GAIN network aims to leverage the high-quality customer data and mechanisms for strong authentication that financial institutions have to build a global assured identity network, thereby addressing the shortcomings of the existing solutions.

The architecture described earlier enables GAIN to leave the customer fully in charge of their own data, while minimising the proliferation of data in multiple ways. First, there is no need for intermediary parties to store identity data, as the chosen approach

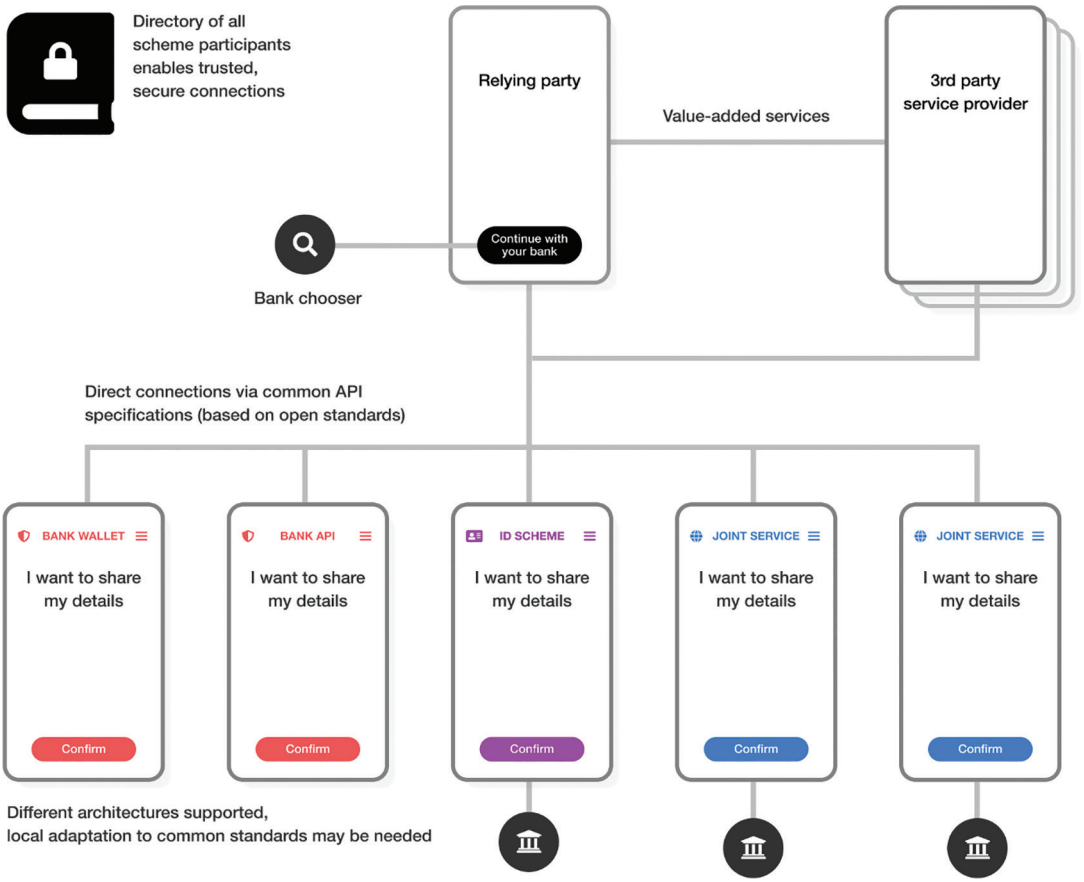

Figure 1: The identity information provider chooser allows an end user to search and pick their identity information provider at the relying party
Source: Garber, E., Haine, M., Knobloch, V., Leibbrandt, G., Lodderstedt, T., Lycklama, D., Sakimura, N. et al. (2021) 'GAIN digital trust: How financial institutions are taking a leadership role in the digital economy by establishing a Global Assured Identity Network', paper presented at the 2021 European Identity and Cloud Conference, Munich, 13th September, available at: https://gainforum.org/GAIN-WhitePaper.pdf (accessed 14th January, 2022).

makes it possible for data to be transferred directly from provider to relying party; the network and other service providers merely provide routing and other services. Secondly, any shared data can be specifically tailored and limited for the purpose at hand. If proof of a certain age is required, the provider can merely confirm that the customer was born before a certain date, rather than the full date of birth.

A key characteristic of the GAIN approach is its openness. While the focus is on financial institutions, other providers are invited to join as well. Furthermore, as mentioned earlier, GAIN provides interoperability between existing networks as well as new. To offer a truly global solution, GAIN aims to connect national schemes. Users in country A can use their local scheme to identity themselves to relying parties in country B. This is made possible, again, by the use of the technology described in previously. GAIN aims to establish an entity to facilitate such roaming. This entity will

aid relying parties to discover providers in the country of their international users, and then route the request and confirmation accordingly.

Two activities are being set up to realise the GAIN vision: a technical proof of concept (PoC) will be implemented in a community group at the OpenID Foundation. This PoC aims at connecting identity providers and relying parties across jurisdictions in a sandbox environment in order to demonstrate the technical feasibility of the approach (interested parties may reach out to gainpoc@oidf.org). Another activity is being set up at the Open Identity Exchange, and will work on the governance model and trust framework interoperability (interested parties may reach out to info@openidentityexchange.org).

CONCLUSION

As discussed, there is a real need for a modern, global digital identity infrastructure that offers strong levels of assurance while leaving customers in charge of their own data. Current solutions fall significantly short of this requirement.

The identity services offered by big tech offer ubiquity — most people have an account with the likes of Google and Facebook — as well as customer friendliness: they are embedded in consumers' mobiles and browsers and benefit from the technology skills of big tech. Big tech, however, tends not to have verified data on names, dates of birth etc. This may be a good thing, because it might be unwise to trust them with our personal data — partly because they have a history of making commercial (ab)use of it; but also because they are foreign entities, at least to their non-US users.

Digital identity schemes offered by national authorities are in many ways the reverse of big tech. The data are of gold standard quality — after all, authorities are the ultimate issuer of hard identity data like name, date of birth and citizenship, and are assumed to be highly trustworthy. On the other hand, authorities lack technical savvy and ubiquity. Pure government eID schemes, like the certificates on national Belgian ID cards suffer from poor adoption and a lack of customer-friendliness.

In addition, many current solutions rely on intermediaries like trusted third parties. These intermediaries facilitate access to providers like banks, often enriching their data with other sources. The downside is that these aggregators often store the data and act as gatekeepers.

The architecture described in this paper, and the GAIN initiative in particular, offers the best of all worlds: digital identity infrastructure that is global, and that offers high-quality data and strong authentication, all without the drawbacks of other solutions.

The GAIN initiative offers high-quality data, given the KYC requirements to which financial intermediaries such as banks are tsubject. They also enjoy trust; surveys show that customers trust their banks to handle their data, just as they trust them to keep their money. And while banks are not at the level of big tech when it comes to technology, they have come a long way and are well ahead of other sectors when it comes to, for example, mobile apps. Those same mobile apps provide ubiquity. We all carry bank authentication on our mobiles, so to speak. What is more, because there is money involved, this authentication tends to be strong (for example, payment initiation in the EU now requires two-factor authorisation).

The financial services industry has a unique opportunity to build such a network. This will not only provide the world with a much needed digital identity infrastructure, but also help banks stay relevant to their customers and become/remain key players while the world is moving online.

For this to happen, the financial services industry must embrace the approach and

put its weight behind it. While banks have the data and authentication, they must still invest in digitising their customer data — for example, many bank branches still hold physical copies of their customers' ID documents. Banks will need to cooperate at the national level to define schemes, rules and branding.

If they succeed, however, they will further contribute to building the digital infrastructure by providing a key element, and perhaps provide a key plank for their continued relevance to consumers.

References

(1) European Parliament (2021) 'Updating the European Digital Identity Framework', available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698772/EPRS_BRI(2021)698772_EN.pdf (accessed 14th January, 2022).

(2) Garber, E., Haine, M., Knobloch, V., Leibbrandt, G., Lodderstedt, T., Lycklama, D., Sakimura, N. *et al.* (2021) 'GAIN digital trust: How financial institutions are taking a leadership role in the digital economy by establishing a Global Assured Identity Network', paper presented at the 2021 European Identity and Cloud Conference, Munich, 13th September, available at: https://gainforum.org/GAINWhitePaper.pdf (accessed 14th January, 2022).

(3) Webster's Dictionary (2021) 'Identity', available at: https://www.merriam-webster.com/dictionary/identity (accessed 14th January, 2022).

(4) European Commission (2020) 'Shaping Europe's Digital Future: eIDAS Regulation', available at: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed 14th January, 2022).

(5) De Cock, D., Wolf, C. and Preneel, B. (2006) 'The Belgian Electronic Identity Card (overview)', available at: https://www.esat.kuleuven.be/cosic/publications/article-769.pdf (accessed 14th January, 2022).

(6) Dutch Government (2015) 'What is DigiD?', available at: https://www.digid.nl/en/what-is-digid/ (accessed 14th January, 2022).

(7) Echikson, W. (2020) 'Europe's digital identification opportunity', available at: https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf (accessed 14th January, 2022).

(8) European Central Bank (2018) 'The revised Payment Services Directory (PSD2) and the transition to stronger payments security', available at: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html (accessed 14th January, 2022).