September 2020

Business trends report - Bring Your Own Identity

CEF eID SMO

Version 1.0

European Commission

This study was carried out for the European Commission by Deloitte.

Authors: George O'Neill, Massimo Pedroli, Arianna Fravolini, Leonardo Marcon

Picture on the first page from Gregor Cresnar for Flaticon.

Internal identification

Framework Contract DI/07624 - ABC IV Lot 3

ABC IV-000358-6000184687-REQ-01

CONTENTS

Introduction

01

"Bring Your Own Identity" (BYOI) is a growing trend in the world of access management and user identification. Under this trend a single digital identity is re-used to provide access to multiple different services from different providers either in the public or private sector.

As presented in this report, government eIDs can themselves be seen as a type of BYOI solution as they typically provide access and are reused across multiple different public sector organisations and types of public services, and to a lesser extent in the private sector as well. The following report focusses primarily, however, on the private sector counterparts to these government BYOI solutions, presenting the different uses and requirements that they respond to. This is done in an effort to learn about what makes such schemes attractive to the general public and what lessons could be drawn for government eID schemes.

Chapter 2 of this report considers the nature of the BYOI trend and the drivers behind it, chief among them being the explosion of digital services for which some type of identification is required and the inconvenience for a user of having to remember and provide different credentials for each.

The following chapter dives into the different types of providers of these BYOI identities – from social media organisations to dedicated digital identity companies. Bearing in mind the particularly high level of take up of identities provided by social media companies, it zooms in on these solutions while also providing a comparison of the characteristics of the solutions deployed by other BYOI providers.

The third and final chapter considers in greater depth how and for what these BYOI solutions are used. It presents:

- BYOI functionalities – what the solution practically enables the user to do (e.g. create an account);
- BYOI use-cases- what services the solution enables the user to access (e.g. review of their healthcare data, streamlined payment for online purchases);
- BYOI industries – those domains in which BYOI solutions are most likely to be used.

The research reviewed in this report suggests a high level of use of privately issued BYOI solutions, as well as considerable opportunity for their providers going forward. In light of this, this report aims to prompt government digital identity providers to consider what this might mean for their own solutions and approaches. On the one hand, this could entail adopting practices from the private sector intended to improve user experience and convenience. On the other hand it could entail considering how such private-sector identities could be used to enable access to public services.

What is "Bring Your Own Identity"

02

The Bring Your Own Identity (BYOI) concept

Managing multiple digital identities to access online services has become a considerable burden. Users, when surfing the web, are commonly asked to create a digital identity for each service they want to access, forcing them to manage multiple accounts/passwords/tokens. This situation exposes them to various risks and, since most of these identities are not interoperable and their number will constantly increase due to the digitalization of organizations, it is clear that this model is not sustainable in the long-term.

People want to be able to create a digital identity securely and easily, with the opportunity to reuse it in multiple domains. Similarly, with the digitalization of the economy, private organizations are moving their business to the web, and want a way to securely identify users.

A response to these demands is offered by the Bring Your Own Identity (BYOI) concept, an "approach to digital identification that allows users to select and use digital ID that is self-managed or managed by a third party and external to the service where it is used"[1]. Examples include social media identities (such as Facebook, Google or LinkedIn) and higher-assurance identities (such as a BankID or government eID) that, once recognized by the service provider, enable the user to access the services provided. This allows users to exploit the same digital identity to access services provided by different entities, without having to create each time a new digital identity.

The rise of Bring Your Own Identity

But what are the origins of BYOI? The concept is closely linked to Identity and Asset Management (IAM). This can be defined as "a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities"[2], which has evolved after the spread of cloud, mobile and IoT technologies. These trends have shifted the focus of security leaders from "where" the data/resources are, to "who" has access to them.

These technologies on the one hand have brought great benefits to organizations, while on the other hand opening the door to more sophisticated and targeted cyberattacks, forcing organizations to prevent or at least reduce this risk.

In recent years, we have witnessed the development of a more general trend that has inspired BYOI. This is the *Bring*

[1] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[2] TechTarget: Identity and Access Management (IAM) (2019)

Your Own "X" movement, which responds to the need of organisations for agility and flexibility. It provides the possibility for people (staff) to use their personal tools to access specific services or perform particular tasks.

Following this trend, organizations realise that restricting people regarding the type of technology they use can lead to a negative impact on business performance, while providing a certain amount of freedom and putting people's needs first can positively impact productivity[3]. In this regard, one of the first initiatives was Bring Your Own Device (BYOD) – a methodology which allows employees to use their personal devices in the workplace to carry out their tasks. Following this, then many other BYO-X trends have been pursued. In particular, these include:

- Bring your own device (BYOD);
- Bring your own attribute (BYOA);
- Bring your own apps (BYOA);
- Bring your own encryption (BYOE);
- Bring your own identity (BYOI);
- Bring your own technology (BYOT);
- Bring your own network (BYON);
- Bring your own wearables (BYOW);
- Bring your own cloud (BYOC)[4].

Each trend represents a solution for a specific problem. BYOI offers a solution addressing the risk for security providers of losing users if the Identification and Access Management (IAM) process is not made simple, transparent and secure. Organisations and users want to minimise redundancy when it comes to identification and authentication. In this regard, BYOI can make a contribution, relieving users from the burden of setting up and remembering multiple usernames and passwords.

DRIVERS

There are a number of drivers that have allowed BYOI to become a widespread practice. In particular, the most significant are the following:

- The proliferation of digital services requiring specific identification procedures;
- IT consumerisation - the blending of personal and business use of technology devices and applications. BYOI can be considered a "consumerization of electronic identity";
- Growing acceptance of cloud-based services and reduced importance of where the solutions and data are hosted, provided that security is ensured;
- Rise of the "as a service" model;
- Growing need for an interoperable and universal authentication framework;
- Users' "identity fatigue" in memorizing too many accounts, too many usernames and too many passwords;
- Growth of the big internet platforms –huge proportion of people have an account which could be used for authentication purposes;
- Desire to embrace the growing use of social media;
- Global regulations around data security and privacy;

However, although these drivers have contributed to the adoption of BYOI among users and have simplified online transactions, another side should be considered. While transferring the management of users credentials to third parties can simplify access procedures it may also create privacy concerns and raise doubts about the effective security of the digital identity itself, which could be compromised or stolen. Nonetheless, the ease of use, and the time-saving aspects of BYOI have in many cases outweighed these concerns for users[5]. .

[3] https://www.condecosoftware.com/blog/byox-bring-your-own-x/

[4] https://www.condecosoftware.com/blog/byox-bring-your-own-x/

[5] https://proofid.com/blog/advantages-byoi-businesses/

THE BYOI ECOSYSTEM

03

THE BYOI STAKEHOLDERS

The BYOI ecosystem comprises three main groups of stakeholders:

1. Identity providers
2. Users
3. Service providers

Identity providers – also known as "third party identity providers" in the BYOI model - are the entities responsible for the issuance, storage and maintenance of the digital identity. The different types of identity providers are described in the next sections. The users can choose which identity to use for which service. Finally, there are service providers, which, instead of requiring users to create an ad-hoc client account for their services, can allow them access by simply recognising the identity provided by the third party identity providers. The more such service providers exist, the more users have the possibility to use the same digital identity to access different services, without the burden of creating each time a new account.

This can actually be a huge advantage not only for users but also for service providers. According to research conducted by the Ponemon Institute, nearly 50% of consumers have been unable to execute an online transaction due to forgetting their password[6], while according to a Gigya survey, more than 80% of consumers admit to having quit an online registration form because they were uncomfortable with the amount or type of information requested[7].

As a consequence, by implementing BYOI solutions, service providers have the possibility to attract new customers, while at the same time avoiding the cost of issuing, storing and managing multiple digital identities. Identity providers, on their side, have the possibility either to expand the use of their solutions (if identity provision is their main business) or to enhance customers' loyalty and gather further information on them (if identity provision is only an ancillary service in their portfolio).

DIGITAL IDENTITY PROVIDERS FOR BYOI

Having seen the stakeholders involved in the BYOI ecosystem, it is now useful to consider in greater depth the different types of digital identity providers operating in this market. The solutions presented by each type of provider tend to exhibit different characteristics in terms of trust, user experience, frequency of use, but they all provide the possibility of accessing online services without creating each time a new digital identity. The competitive landscape of BYOI is made up of the following six actors[8]:

[6] Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

[7] Gigya: Gigya 2014 Privacy & Personalization Survey (2014)

[8] Gartner: Innovation Insight for Bring Your Own Identity (2019)

1. Social Media providers
2. Governments
3. Financial Institutions or banks
4. Mobile network operators
5. Digital identity companies
6. Digital Identity networks

Social Media Providers

A quick and easy way to create a digital identity is through a social media account, since this is self-asserted and does not require further authentication processes. For this reason, it is embraced by many users who, thanks to it, can access multiple organisations' websites without having to create every time a new digital identity providing each time their personal information. The sheer number of users with social media accounts support this trend. Facebook, Instagram, Twitter and LinkedIn between them have 4 billion monthly active users[9].

This approach is called "social login" and is a form of single sign-on (SSO) which serves to authenticate to a third party platform through existing information stored by a social networking service, such as Facebook, Google or LinkedIn. Through this approach, the details related to the users are provided by the social platform chosen for the login., and, the associated data can also be used to improve the user experience by displaying tailored content. The customer identity management platform Gigya claims that the top three reasons users decide to login via social media identities are:

1. They don't want to spend time on registration forms;
2. They don't want to create another username and password ;
3. They want to easily share content with friends on social networks[10].

In general, online services providers offering a social log-in option continue to offer the possibility of registering through other methods, to avoid excluding those without a social media account.

In terms of players, the market share is dominated by the following organizations:

- **Facebook**: Facebook Login provides users with the possibility of creating an account and logging in into a company app or website in a fast and secure way. It enables two different scenarios: authentication on one side and requesting permission to access people's data, on the other. Service providers can implement Facebook Login simply for users authentication or for both authentication and data access. While websites and apps have control over the information they request from the users, Facebook has a review process for developers that require a high number of permissions, preventing them from misusing user data. Despite that, in 2018 Facebook was involved in the Cambridge Analytica scandal, where 87 million users' identities were compromised and accessed without authorization[11]. When using Facebook Login, users can customise "permissions and privacy" as they have control over what they approve or share, with an option to select the type of information they would like to be shared. Moreover, Facebook claims that providing users with the possibility of signing in using their already existing Facebook account leads to higher conversion rates and at the same time higher retention thanks to the personalisation of content that companies can put in place[12].
- **Google Sign-In**: Google Sign-In is an authentication system that allows users to securely sign in into websites and apps with their existing Google accounts, reducing the burden of creating a new account. By

[9] https://dustinstout.com/social-media-statistics/

[10] Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

[11] https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

[12] https://developers.facebook.com/docs/facebook-login/overview

implementing the Google Sign-In solution, websites and apps can access users' information such as the public profile, age range, and friends list, and at the same time ask permission for email addresses and contacts. On the other hand, users have the possibility of controlling the information they share during authorisation and perform a series of tasks such as save a file to Drive, pay with Google Pay, add an event to Calendar, and share with their Google-wide contacts. However a disadvantage is the inability to alter an app's permission after the initial authentication — except without completely disconnecting it and re-authenticating from the app itself[13].

- **Instagram**: Similarly to Facebook, logging in with Instagram is a means for people to access a company app or website. Two use-cases are supported: authentication and asking for permission to access people's data[14].
- **LinkedIn**: With LinkedIn being the largest and most trusted source of professional identities, LinkedIn Login is an authentication solution for websites and apps that want to allow users to sign in with their professional identity. By implementing the LinkedIn Login solution, websites and apps can access the basic profile, location, and positions of the users. For additional information such as the user's contact information, full profile, education or recommendations, developers must request an approval to the LinkedIn program. However, the end users cannot control permissions and can therefore not see what type of information the apps have access to[15].
- **Twitter**: Signing in with Twitter allows users to access a website or app with their already existing Twitter account. By implementing the Sign in with Twitter solution, websites and apps are provided with permissions to see who users follow, whose tweets they read, if they access direct messages and get profile updates. However, as Twitter makes public all content, this means that anyone with a Twitter account can access the information linked to another user's account. – unless the user restricts his/her view permissions[16].
- **Amazon**: Login with Amazon is a solution that allows users to sign in into websites or apps using their already existing Amazon account, in a faster and more secure way than creating every time a new account for each service. Thanks to the Login with Amazon solution, websites or apps can leverage data including name, email address, and zip code to build a more personalised experience for the users and at the same time give them the opportunity of re-using already entered payment credentials to perform a transaction. In addition to the typical advantages related to social login, when websites or apps add Amazon Pay, they enable Amazon buyers to log in and pay with the information already stored in their Amazon account.

GOVERNMENTS

Government digital IDs include both a digital identity and, in some cases, a physical ID, and are provided to citizens who typically use them to access online public services. These identities, backed up by identity proofing, provide a higher level of assurance compared to social media identities but at the same time require a longer process to be issued.

The fact that these types of identities have a higher level of assurance makes them more relevant for use cases that

[13] https://developers.google.com/identity

[14] https://www.instagram.com/developer/

[15] https://docs.microsoft.com/en-us/linkedin/consumer/integrations/self-serve/sign-in-with-linkedin

[16] https://medium.com/@siftery/top-social-login-tools-compared-b350eae26118

require a high level of trust or for identity proofing (for example in e-Government situations). However, in less sensitive cases the complexity of the registration process may deter users.

In addition, the extent to which government IDs are available for use to access private services differs according to the country.

Financial Institutions or banks

Financial institutions and banks offer a type of eID that is often based on a federated approach, where issuers of eID and relying parties are connected through an identity federation. In this scenario, user data is controlled by multiple management systems and when a user accesses the services of one of them, he/she is automatically authenticated also on the platforms of the other federated systems.

The competitive advantage of these eID is that consumers use them regularly to perform financial transactions, and that financial institutions and banks are usually regarded as trustworthy organisations, providing secure online services.

However, use cases for such identities are still limited, as many bank digital identity remain closed off to external service providers and digital services in the private sector[17]. Examples of this type of digital ID include:

- **Verified.me**: a network of major Canadian banks and other service providers which provides users with a federated identity across a permissioned Hyperledger Fabric blockchain[18]. Verification is based on information users have already shared with institutions they trust and which belong to the Verified.me network. In particular, this latter is made of seven of the major financial institutions in Canada: National Bank of Canada, BMO, CIBC, RBC, Scotiabank, TD and Desjardins[19], with many more planning to join.
- **Swedish BankID**: a user identification solution that allows companies, banks and government organisations providing public services to authenticate and conclude agreements with individuals over the Internet, and that is provided in 3 different options:
  1. mobile BankID: an app on the user's smartphone or tablet;
  2. BankID on a card: a physical smartcard;
  3. BankID in a file: computer software[20].
- **Norway BankID**: similarly to the Swedish version, Norway BankID is a personal electronic ID for secure identification. It is used by all the country's banks, public digital services and an increasing number of enterprises in a wide range of sectors for identifying easily and securely users online[21].

Mobile Network Operators

The digital identity provided by mobile network operators (MNOs) is another way through which BYOI can be implemented. MNOs are "telecommunications service providers that deliver wireless voice and data communication for their subscribed mobile users"[22]. MNOs provide users with a SIM card that allows them to be identified within their specific mobile network. Here the level of security depends on the identity verification processes imposed in the countries considered. Some countries require a minimal identity verification, while others require a government ID in order to issue the SIM card.

However, since every MNO has its own data management

[17] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[18] https://www.hyperledger.org/use/fabric

[19] https://verified.me/

[20] https://www.bankid.com/en/

[21] https://www.bankid.no/en/company/

[22] https://www.techopedia.com/definition/27804/mobile-network-operator-mno

system, in order to allow service providers to enable BYOI it is necessary to create a standardised infrastructure able to connect them all. In this regards, GSMA Mobile Connect, enables people to identify and authenticate using their mobile phone[23] without a username and password, representing a possible solution to address this issue, since it provides a globally interoperable solution made available from mobile network operators worldwide.

The advantage of MNO's operators' eID is based on their established reach and their customer relationship management experience[24]. As of August 2020, 23 MNO's[25] around the globe, have made the Mobile Connect authentication service available for users, while a further 11 are piloting it. Major EU telecommunictions providers already providing the Mobile Connect solution include Telefonica, Orange, Deutsche Telekom, Vodafone Germany, Telia, T-mobile, and KPN.

In some countries, such as Moldova, MNO's have worked with the government in order to provide an eID that is used to access online public services. In Moldova, the technical infrastructure for the Mobile eID solution is provided by two national mobile network operators who work together with the e-Governance agency and Center for Special Telecommunications to provide the country's eID scheme[26].

DIGITAL IDENTITY COMPANIES

Another opportunity in the BYOI market has been seized by dedicated "digital identity companies", which have been set up with the main purpose of providing digital identity to users, as opposed to banks or social media which provide these identities as an offshoot of their other activities. These companies offer users the opportunity of creating a digital identity by following a registration process backed up by already existing ID documents (e.g. driving license, passport), social media identity, or other certificates, and at the same time increasing the security of these identities with biometric tools such as facial recognition.

These BYOI solutions are appreciated by users in particular for their portability and the fact that they employ advanced technologies such as biometrics to better protect the identity. Some of the solutions currently available in the market are presented below (the services accessible with these solutions are presented in Chapter 4):

- **Yoti**: allows users to add their phone number, setting a 5 digit PIN to protect their phone, take a quick scan of their face to prove they are a real person, and finally add an ID document. The company states that the details of the user are encrypted. As of today, seven million people have downloaded Yoti[27].
- **SisuID**: an authentication and digital identity platform, hosted and governed by the SisuID community. It provides a strong level of authentication to service providers which can rely on the platform since it requires users to verify their identity by adding either their bank credentials or ID documents. Once the identity is confirmed, users can access the online services that support the SisuID platform[28]. SisuID additionally exploits biometric technologies such as facial recognition to increase the security of users' digital identities[29].
- **GlobalID**: gives users the opportunity to create a

[23] https://www.gsma.com/identity/developer-portal

[24] Yasmina McCarty, Head of Mobile for Development, GSMA, cited on https://news.itu.int/mobile-operators-digital-identity-system/

[25] See https://developer.mobileconnect.io/operators?title=&name_list=All&field_mobile_connect_status_value=2

[26] ID4D (2019), Practitioner's Guide Version 1.0. Available at http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

[27] https://www.yoti.com/

[28] https://sisuid.com/index.html

[29] https://www.biometricupdate.com/201912/finnish-ministry-tests-sisuid-biometrics-nixu-restructures-amsterdam-team

digital identity backed-up by multiple "verifications" that can be obtained through mobile number, government ID, social media account, college degree verification or bank account[30].

- **Onfido**: by exploiting biometric and machine learning technologies, it allows users to create a digital identity by scanning their face and their ID document. The company states that the document verification process catches up to 98.7% of ID fraud attempts[31].
- **Chekk**: a mobile data wallet that allows users to create a digital identity by scanning, storing and managing their personal information (e.g. passport, ID card, driving license, bank and insurance details)[32].
- **Janrain** is an software provider that offers various customer identity and asset management (CIAM) solutions, allowing the sharing of profiles among websites or single sign-on across websites. It claims more than 1000 customers[33] (businesses accepting its ID as an authentication means). Among these customers are the main social media such as Facebook, Google, LinkedIn, Twitter. It uses profile data, such as a user's age, gender, interests, and location, allowing marketers to target advertising messages. It has been taken over by Akamai in January 2019.
- **Gigya** offers a customer identity management platform that businesses can use to identify customers, aggregate data & personalize campaigns. Similarly to Janrain, the platform offers products for customized registration, social login, and user profiles. It claims to have more than 1400 customers[34], among which are large corporations such Fox, Forbes, Repsol, Toyota, and Bose. Gigya has been acquired by SAP in September 2017.

DIGITAL IDENTITY NETWORKS

Digital identity networks differ from the solutions mentioned above since, although they serve BYOI purposes, they are not identity providers, but are instead a sort of facilitator between identity providers and service providers[35].

These solutions are considered a trusted, safe and secure way to verify users identity online, as their business model consists in providing the network participants (identity and service providers) with an infrastructure where they can exchange identity information of users. Consequently, a main advantage is represented by the fact that digital identity networks create an ecosystem where multiple identity and service providers can easily and securely exchange identity information depending on the use cases. Included within this category are "derived identity" providers, which draw on existing digital identities to create a new, more user-friendly one. Examples of this type of solution are provided by MasterCard, Verimi and Yes.

- **MasterCard:** provides users with a secure network that is backed by trust agreements between identity and service providers, where identity providers such as banks or financial services establish partnerships with MasterCard to provide users with payment credentials. On the other hand, service providers can allow consumers to directly use these payment credentials to pay for their goods and services[36].
- **Verimi**: an identity platform that combines all functions around the digital identity, related to secure login, online identification and digital signature, allowing easy access to digital services across all types of industries. Within Verimi users can store personal data coming from documents such as driving licence, or other identity providers such as banks in a

[30] https://www.global.id/
[31] https://onfido.com/
[32] https://www.chekk.me/
[33] https://stack.g2.com/janrain
[34] https://stack.g2.com/gigya
[35] Gartner: Innovation Insight for Bring Your Own Identity (2019)
[36] https://idservice.com/~/media/digital-identity-our-service.ashx

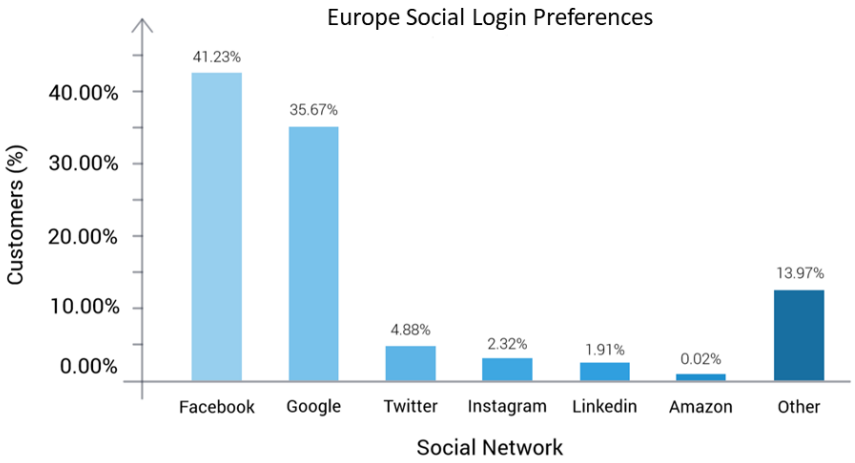
secure way[37].

- **Yes**: an organisation with the goal of enabling the user to use their identity data, collected digitally at their bank, for other service providers, creating an infrastructure that allows the user to transfer his/her data from the banking system to the requesting company, once the customer's approval has been provided[38].

FOCUS: THE SOCIAL LOGIN MARKET

Focusing on social media, there are over 30 social media identities with which users can log in into other websites or apps. The six major players mentioned in Chapter 3 cover more than 90% of the market share of social login in North America and the APAC region, 87% in Europe and 80% in the rest of the world[39].

Out of these six, the leading role is played by Facebook and Google. In Europe, these are the most popular social networks for social login, with Facebook preferred by 41.23% of users, and Google by 35.67%.



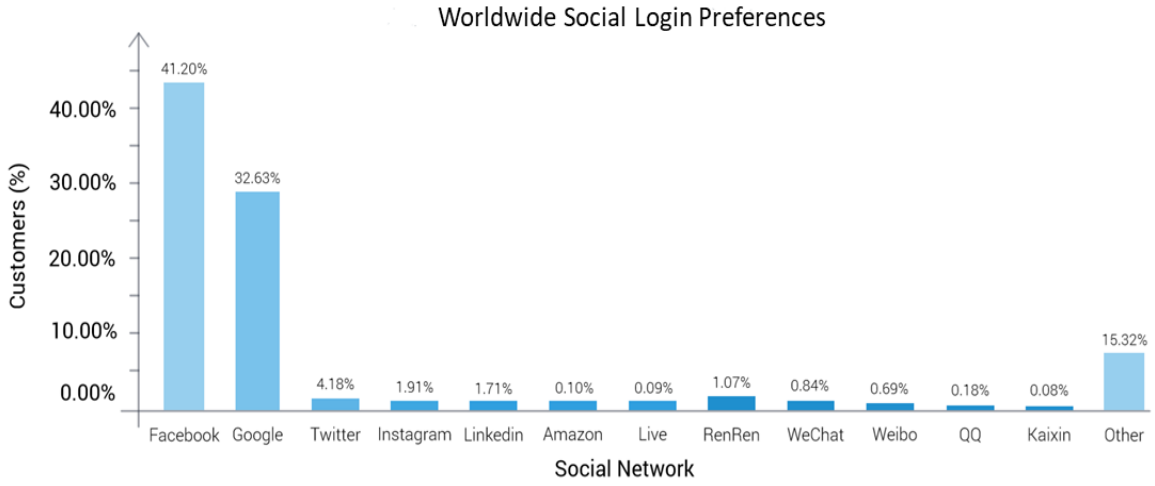
Source: LoginRadius: Digital Identity Trends (2019)

The same trend appears at the global level, where Facebook and Google are again clearly dominant, preferred respectively by 41.20% and 32.63% of users.

[37] https://verimi.de/en/

[38] https://www.yes.com

[39] LoginRadius: Digital Identity Trends (2019)



From: LoginRadius: Digital Identity Trends (2019)

The above graphs demonstrate that Facebook and Google are the most used solutions for social logins. One of the main reasons is the level of data that such identity providers store and can share about their users (e.g. name, email address, birthday, gender, city, education) as well as the number of their active users. Facebook's 2.4 billion monthly active users[40] and Google+'s 395 million monthly active users[41] can be said to play a large role in their leadership in the social login market. Together, these two solutions account for at least 75% of the market share of social login.

Following these two leaders are Twitter, Instagram and LinkedIn. Although these platforms havesignificant bases of monthly active users (respectively 330 million, 1 billion and 303 million[42]) they lag far behind the two main players in terms of preferences for social login (Instagram is positioned behind Twitter and only slightly above Linkedin despite having three times the number of active users of the other two).

Finally, Amazon is emerging as the main identity provider across eCommerce websites thanks to its capacity to streamline the checkout process[43].

The remaining 10% to 20% of the market share for social login is fragmented across a number of competitors:

- Microsoft
- Aol
- WeChat
- Instagram
- Vkontakte
- Renrem
- Foursquare
- Kaixin
- Yahoo Japan
- Tencent
- Odnoklassniki
- RenRen
- Netlog
- Sina Weibo
- Wordpress

[40] Dustin W. Stout: Social Media Statistics 2020: Top Networks By the Numbers (2020)

[41] Ibidem

[42] https://dustinstout.com/social-media-statistics/

[43] Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

- Weibo
- VZnet
- Mixi
- Typepad
- Livejournal
- Skyrock
- Xing

The market for social login is therefore very concentrated. From a service provider's perspective, it is likely to be more convenient to implement already existing solutions such as the Facebook Login and Google+ Sign In, covering more than a third of the of the world's population (2.8 billion monthly active users combined), unless other solutions offer significant competitive advantages against other dimensions.

Comparison Between Digital Identities

Having described the actors providing digital identities for BYOI purposes, these will now be compared according to the different dimensions that service providers take into account when deciding what type of BYOI solution, if any, to integrate for identification purposes[44]: Level of trust and assurance, Convenience and user experience, Frequency of credential use, Link to a physical credential.

Level of trust and assurance: *how secure the digital identity is perceived by the service providers and the users.*

For this first dimension, the solutions mentioned above are perceived as secure by both users and service providers, with the exception of those provided by social media. Service providers and users differ according to the reasons that they give for judging that social media identities are less reliable. For service providers, the first drawback is related to the fact that social media identities are self-asserted and not backed by identity proofing, meaning that they can provide false information about the user. People do not always provide accurate information about themselves when setting up their social media account, either due to mistakes or because they do not want to share too much personal information.

Another reason why service providers may be less trusting of social media identities is that they make the service provider dependent on the correct and adequate functioning of the social media platform linked to those identities. If the social media platform crashes, users trying to access the service provider's website with their social media account will not be able to do this, thereby damaging the service provider.

Meanwhile, on the users' side, the first concern relates to privacy. Even though digitalisation enables a lot of opportunities, it also increases the risk of cyber-attacks. Third-party identifiers, such as Facebook or Google+, still use basic password authentication methods, potentially exposing users to the risk of identity theft. If one of these social media identities is hacked, all people using that solution to log in are affected as well. This may be even worse if the whole system is attacked, risking the loss of billions of credentials (and their related data).

Moreover, users know that social networks monetise their data by sharing and analysing it. Given this, it is understandable that some users are reluctant to share certain information with these platforms (for example information that can be leveraged to define their tastes or political preferences). This distrust is further fuelled by recent data breach scandals, the most famous of which is the Facebook-Cambridge Analytica, scandal, which led to 87 million user identities being compromised and accessed without authorization[45].

Other types of BYOI solutions are backed by identity

[44] Gartner (2019), Innovation insight for Bring Your Own Identity.

[45] https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

proofing, and consequently viewed as having a higher level of assurance by both users and service providers. However, even if social media identities are viewed as less reliable by service providers, this does not seem to have substantially damaged their user numbers. Social media login represents the most implemented type of identity solution, followed by mobile login[46].

Convenience and user experience: *the ease with which users access the identity and consequently the service*.

BYOI offers portable solutions which can reduce friction and increase adoption, security numbers and overall user satisfaction. From the user perspective, the first benefit that can be identified is the fact that BYOI offers a simplified, quick and easy registration process. Relying on BYOI authentication means no longer having to memorise dozens of passwords and manage multiple different user accounts.

It is necessary also to distinguish between the different BYOI solutions previously described. Social media identities generally represent the most convenient solutions; users are able to create accounts with just a few clicks (and limited information) and access the websites/services that it supports. However this same convenience and low level of identity proofing means that such accounts are not used for more sensitive services such as banking, which have more strict onboarding requirements. If a user wants to carry out a payment or transaction when logged in with a social media account, they will need to fill in additional information like billing details and payment method, with the possibility that this will degrade the user experience.

Other BYOI solutions generally have a lower level of convenience than the social media ones, reflected in measures such as the amount of time to create a digital identities. These BYOI solution providers require users to go physically to a dedicated place to create his/her digital identity, whether directly as with MNOs or Government eIDs, or indirectly with bank digital identities and other digital identity providers (i.e. the solutions provided by digital identity companies). The more time spent and the more documentation required to create such a digital identity, the more inconvenient it will be for users to use such identities compared to social media identities. In addition, these (non-social media) BYOI solutions generally require a second authentication method such as tokens (bank digital identity), SMS (MNOs), or card reader (Government eID). This results in a longer procedure in order to authenticate, although it is should be emphasised that this is paid off in terms of higher levels of trust and security for both users and service providers.

Overall, BYOI solutions provide users with a more customised experience compared to traditional account creation. This is because organisations, by giving users the option to log in using their existing digital identities, can request access to specific data, which in turn can be used to build an authentic relationship with the customer. In other words, BYOI solutions can act as an "informal" agreement between customers and organisations, where the former knowingly grant access to requested data in return for a more significant user experience. Reflecting this, customers logging in with a BYOI solution spend more time navigating an organisation's website compared to anonymously logged in customers[47], consequently increasing the chances of concluding a transaction or deeper collection of data.

Another factor that should be considered is that, when starting a new registration process, users may provide incorrect information about themselves, for example because they do not trust the website they are trying to access. Giving users the option of signing in through a BYOI solution can build trust in the user's mind and increase the

[46] LoginRadius: Digital Identity Trends (2019)

[47] Gigya: Social Login 101: Everything You Need to Know About Social Login and the Future of Customer Identity (2015)

likelihood the use the service.

Frequency of credential use: *how frequently the digital identities are used.*

In terms of frequency of use, Gartner reports that among the BYOI solutions, social media identities and MNOs are the most exploited ones, with a usage rate that goes from daily to weekly[48] - one of the main reasons being the "convenience and user experience" dimension previously described. Another reason may for social media identities leadership here may be the sheer number of websites where these BYOI solutions can be used to log-in. Data from G2 – a peer-to-peer review website with more than 1,079,300 software products and professional services reviews from users – indicates that Facebook Login, Google Sign-in, Twitter Sign-in, Instagram Login and LinkedIn Login are employed by over 50 thousand companies as solutions to allow users signing in into their websites[49].

On the other hand, the usage made by Government eID's tends to be much more limited[50]. One of the main reasons may the fact that these types of identities are typically employed for accessing public services and must satisfy more strict identification requirements in order to be processed. Moreover, the demand for digital public services is still relatively low. In 2018, only 64% of EU citizens used public services online[51].

Finally, concerning the frequency of use of bank digital identities, this remains higher than government eIDs (at least once per quarter[52]). The gap may be linked to the fact that this type of identity can be exploited in multiple situations, including both public and private services (which will be described in the next chapter).

Link to a physical credential: *whether the digital identity is backed up by a physical ID such as passport, national ID or driving license.*

This dimension is linked to the "level of trust" dimension. Social media identities, which tend to be less trusted, are not backed up by a physical ID. MNOs are sometimes backed up by physical IDs, however the most prominent example – Mobile Connect – is not linked to any physical credential. Users will require access to their mobile phone but not to any other physical device[53]. On the other hand, biometric credentials may be used in combination with Mobile Connect. Government eIDs, and BankIDs are meanwhile highly likely to be backed up by some form of physical credential, whether that is some form of smart card, payment card or other certificate.

Market Opportunities

According to web analytics firm StatCounter, in October 2016 the level of mobile browsing surpassed desktop web browsing for the first time in the internet's history[54]. Going forward, businesses face an imperative to ensure their web presence is as mobile-friendly as possible. A quick and easy BYOI sign-on can facilitate the use of web platforms from mobile devices, helping businesses securing the growing mobile browser market. This may indicate a positive future for such BYOI solutions.

Forecasters also appear to agree that the future of BYOI is bright. Organisations including Grand View Research, Fortune Business Insights and Global Market Insights predict that the Identity and Access Management market

[48] https://www.gartner.com/document/3978687?ref=solrAll&refval=254995734

[49] https://stack.g2.com/

[50] Gartner (2019), Innovation insight for Bring Your Own Identity.

[51] Digital Economy and Society Index Report 2019 - Digital Public Services

[52] https://www.gartner.com/document/3978687?ref=solrAll&refval=254995734

[53] GSMA (2016), Mobile Connect: Mobile high-security authentication. Available at https://www.gsma.com/identity/wp-content/uploads/2016/10/MC_high-security-authentication_Sep-16.pdf

[54] The Guardian: Mobile web browsing overtakes desktop for the first time (2016)

will grow to at least 20 billion U.S[55] dollars by 2026. Meanwhile, Gartner predicts that by 2022, BYOI will be recognized as a common practice in 70% of consumer Identity and Access Management (IAM) programs, up from less than 40% today. It predicts that by 2023, BYOI will be a multi-billion-dollar industry[56].

MARKET POSITION OF BYOI PROVIDERS

Even if the overall prospects of the BYOI sector are strong, those of the different types of providers described previously may differ significantly, as they start from quite different positions.

As mentioned previously, in this regard, social media identity platforms with their four billion *monthly active* users[57] may have a significant advantage.. Furthermore survey data indicates that 77% of internet users believe that social login is a good registration solution[58].

As concerns MNOs instead, there are 5.9 billion people with access to mobile telephony (70% of which are smartphones) and 7.9 billion SIMs in the world[59]. Moreover, according to a paper from Juniper Research, the growth in mobile digital identity solutions could exceed 800% over the next five years, with unique mobile identifier services likely to become the primary source of identification for over 3 billion people by 2024[60].

Considering bank digital identity solutions – these have a high level of penetration within very specific markets – namely the Scandinavian countries of Sweden, Norway, Denmark and Finland. In these countries, digital identity solutions provided by financial institutions or banks account for 21,4 million users.

To take Sweden as an example, in 2018 the preferred online identification method was dominated by BankID, with a market share of 70% against 30% of classic username and password or other multi-factor authentication procedures[61]. Meanwhile, in Norway 96% of BankID customers (4,1 million who account for 77% of the population), perceive it as a "simple and easy to use solution, making their life simpler"[62].

Looking at government digital identity solutions, there are more than 185 million eIDs issued in the European Union, while for what concerns the solutions provided by digital identity companies, the number of users differs from company to company and there is not a holistic market overview. Some examples include Yoti, which has been downloaded by more than seven millions people[63], while Yes.com is expected to reach 35 million users within the next few years[64].

IDENTITY-AS-A-SERVICE: A COMPETITOR TO BYOI?

One competitor, to BYOI, is Identity-as-a-service (IDaaS) companies providing cloud-based authentication or identity management systems. Such solutions free organisations from the development and monitoring costs associated with managing their own internal access management solutions.

Under the "X-as-a-service" model features are delivered

---

[55] https://www.fortunebusinessinsights.com/industry-reports/identity-and-access-management-market-100373

[56] Gartner: Innovation Insight for Bring Your Own Identity (2019)

[57] https://dustinstout.com/social-media-statistics/

[58] https://www.annexcloud.com/thankyou/social-login-ebook

[59] https://www.primaonline.it/2020/03/04/302418/nel-mondo-ci-sono-59-miliardi-di-persone-e-79-miliardi-di-sim-il-70-dei-telefonini-in-circolazione-e-uno-smartphone/

[60] https://www.gsma.com/identity/news-flash-7-billion-opportunity-in-digital-identity-for-operators-by-2024-as-world-turns-to-mobile

[61] https://www.statista.com/statistics/873932/users-preferred-identification-method-for-online-services-in-sweden/

[62] https://www.cashlessfuture.cz/assets/files/5_%C5%A0irok%C3%A9%20vyu%C5%BEit%C3%AD%20bankovn%C3%AD%20identity%20v%20Norsku.pdf

[63] https://www.yoti.com/

[64] https://www.finextra.com/pressarticle/78648/signicat-and-yescom-collaborate-on-digital-identity-service-in-germany

or served to a company through a remote connection from a third-party provider, as opposed to the feature being managed on site and by in-house personnel alone. Solutions provided by such cloud service providers may be more reliable and robust than in-house security and authentication systems.

Solutions available on the market are provided by operators including[65]:

- Atos (Evidian)
- Auth0
- Broadcom (CA Technologies)
- ForgeRock
- IBM
- Idaptive
- Micro Focus
- Microsoft
- Okta
- OneLogin
- Optimal IdM
- Oracle
- Ping Identity
- SecureAuth

Although representing an alternative to BYOI, IDaaS may also reinforce the trend whereby service providers increasingly seek identity solutions other than in-house ones and rely upon third parties for sign-on purposes.

[65] https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management

04

BYOI USE CASES

BYOI FUNCTIONALITIES

The solutions provided by different types of BYOI providers may best apply to different use cases. This depends on the specific functionalities of each solution. There are a range of functionalities that are supported by BYOI solutions[66] . The most relevant functionalities which may support the spread of the BYOI model are described in the following paragraphs.

CONVENIENT LOGIN SOLUTIONS FOR ACCOUNT CREATION

By leveraging third-party identity providers, users are facilitated in creating a new account using an already existing digital identity.

This functionality is particular typical of social media IDs, and mobile network IDs[67], which are considered the most convenient solutions for logging in to websites and creating a new account.

Social media identities, generally include information on name, surname, email address, age, gender, profile photo, and city[68]. Using this information, service providers are able to set up an account for the user, who, in turn, is relieved from the burden of starting a new registration process. Users are furthermore generally able to carry out basic tasks such as accessing the free content of a service provider platform/websites, subscribe to a newsletter, create a wish list for future purchases and share content on social media platforms.

However, more sensitive services such as carrying out an economic transaction generally require the user to provide additional information and cannot be automatically carried out based on the social media identity.

Mobile network IDs such as Mobile Connect also allow users to quickly share personal data, whether this is required to set-up a new account or for other use-cases (e.g. sharing contact details to facilitate delivery services)[69]. Users can consent to share particular attributes or core information revealing their identity.

PRIVACY CONTROL

BYOI solutions can offer users the opportunity to control their identity and their related attributes when dealing with a service provider,

The digital identities that most allow the user to have

[66] Gartner (2019), Innovation Insight for Bring Your Own Identity
[67] Gartner (2019), Innovation Insight for Bring Your Own Identity
[68] https://www.slideshare.net/Gigya/social-login-101-free-ebook
[69] https://mobileconnect.io/identity/

control over the information shared with the service provider are represented by those issued by digital identity companies and digital identity networks[70].

An even greater level of control can be offered by "decentralised identities", which aim to provide complete control to users of the use that is made out of their identity information[71]. Such solutions enable the user to decide what identity information is shared with who[72]. Such features are less likely to be provided by other BYOI solutions

SECURE LOGIN

This last functionality of secure login involves situations where a high level of assurance is required that the user is who they say they are. This functionality is more typical of Government eID, Bank IDs, mobile network IDs[73] and digital identity companies, which draws on physical identity credentials to provide a higher level of assurance for the digital identity. These types of providers usually require a second authentication method such as tokens (bank digital identities), SMS (MNOs), or card reader (Government eID), therefore making the login procedure more secure.

Such procedures are necessarily more time-consuming compared, for example, to the creation of a social media identity. However the higher level of assurance enables the user to carry out a wider range of activities, including more sensitive activities.

Secure login with Bank IDs

To take *Bank IDs* as an example, these digital identities appear to be primarily used in the eGovernment and eBanking domains. Norway BankID, for example, enables its users to log into practically any public sector website and perform tasks such as checking and/or amending tax information or signing loan agreements.[74] The use cases enabled extend beyond typical eBanking situations to aspects such as buying and selling fund units for example[75].

Many other use cases are enabled by BankID (in Norway alone there are 409 use cases)[76]. A common service is enabling access to secure digital mailboxes – allowing users to report a change of address for example – or granting access to eLearning portals, where student records, score cards and other sensitive information is stored.

Meanwhile in other private sector contexts, BankID can be used to verify age for purchases of restricted products (such as tobacco), for secure identification and acquisition of insurance when a user decides to rent out his/her car, or to verify payments or login to customer pages.

Secure login with digital identity companies

The secure authentication enabled by digital identity companies also provide users with a large range of use cases. The digital identities provided by these dedicated companies tend to be backed up by already existing ID documents (e.g. driving license, passport) or other certificates, but at the same time provide the user with strong security measures through biometric technologies such as facial recognition.

In general, such identities cannot yet be utilised in eGovernment scenarios. Available use cases do however

---

[70] Gartner (2019), Innovation Insight for Bring Your Own Identity

[71] See https://www.gsma.com/identity/decentralised-identity#:~:text=Decentralised%20identity%20is%20an%20emerging,(such%20as%20the%20Government).

[72] https://www.citi.com/ventures/perspectives/opinion/digital-identity.html

[73] Gartner (2019), Innovation Insight for Bring Your Own Identity

[74] https://www.cashlessfuture.cz/assets/files/5_%C5%A0irok%C3%A9%20vyu%C5%BEit%C3%AD%20bankovn%C3%AD%20identity%20v%20Norsku.pdf

[75] https://www.bankid.no/en/private/areas-of-use/

[76] Ibidem

include eBanking situations where an account needs to be set up[77] or to the user identity needs to be verified prior to an economic transaction[78] (e.g. purchasing cryptocurrencies with a credit card). In eCommerce situations, these digital identities can allow customers to simply and securely prove their age when using their debit card to buy from online shops[79].

In other industries, including entertainment, travel and telecommunications, these digital identities are used to rapidly verify the user's identity online in a fast and secure way. Onfido for example, is a solution adopted by companies such as BlaBlaCar (transport), Yallo (telecommunication) and Dribble (entertainment) to on-board new verified users[80].

Secure login with MNOs

As concerns *mobile network IDs*, these also have been used to provide access to both public and private services.

In the eBanking industry, such identities can be used when users attempt to access their bank account from a new device, when sending a payment to a contact that is not on the user's pay list or when the user needs to authorise a payment when he/she is abroad[81].

In the eCommerce industry, mobile network IDs are used for faster registrations, to streamline check outs and authentication of pre-stored credit card details. An example of a mobile network ID deployment in eCommerce is the FIDO implementation of PayPal which allows consumers to authorize payment transactions at online-shops using the FIDO authentication on the supported devices[82].

Mobile network IDs can in some cases also be exploited also in the eGovernment area, with users able to log in to portals and perform tasks such as checking a tax return, apply for a driving license, register a new company and vote in local, regional and national elections[83].

In the healthcare industry, mobile network IDs are changing the way healthcare is delivered to patients by enabling them to access and manage their own health data via their mobile phone. In such scenarios, it is critical to reliably identify both patients and healthcare providers. Mobile identity allow just that, enabling patients, practitioners and providers to prove who they are online in a secure and convenient way. In this way, patients can access, manage and share their personal data with healthcare professionals who can quickly and accurately make diagnosis.

Finally, mobile network IDs find application also in the education sector, allow students access to restricted educational content anywhere and anytime they want it.[84]

Secure login with digital identity networks

Digital identity networks enable similar use cases to those described previously for digital identity companies, In the eBanking industry, solutions such as Yes.com allow the user to login, pay, sign documents and verify his/her identity with the bank[85] or even create a new bank account[86].

The digital identity network provided by MasterCard, also provides the possibility for a user to conclude an economic

---

[77] https://onfido.com/industries/telecommunications/

[78] https://www.yoti.com/blog/buy-cryptocurrencies-in-under-60-seconds-with-safello-and-yoti/

[79] https://www.yoti.com/blog/using-yoti-to-buy-jagermeister/

[80] https://stack.g2.com/onfido

[81] https://mobileconnect.io/about/

[82] http://www.securitydocumentworld.com/creo_files/upload/article-files/GlobalPlatform_White_Paper_MobileID.pdf

[83] https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf

[84] https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf

[85] https://www.yes.com/

[86] https://verimi.de/en/

transaction where an account was previously created thanks to a social media identity.

Secure login with Government eIDs

Finally, considering *government eIDs,* the secure authentication solutions they provide make them more relevant for use cases that require a high level of trust. They tend to be used for eGovernment tasks, and to have relatively limited application outside of the public sector. The public services accessible using such identities include those in the following domains:

- Agriculture
- Business
- Civil registry
- Culture
- Defense
- Disaster Management
- Education
- Energy
- Environment
- Health
- Local / regional planning
- Marine
- Property / land administration
- Smart cities
- Tax policy
- Transport
- Work and retirement

BYOI AND INDUSTRIES

Based on the previous analysis, and bearing in mind the main functionalities and use-cases supported by the different types of digital identity providers, we can now also consider the industries in which BYOI solutions are mostly employed.

For what concerns *social media identities* the industries making use of such solutions include:

- Consumer brands
- eCommerce
- Education
- Entertainment
- Media/Publishing
- Transport/Hospitality[87]

Meanwhile, the use of *BankIDs* is not restricted to just financial areas, (such as eBanking and eCommerce), but covers also sectors including:

- Education
- eGovernment
- Telecommunication
- Transport/Hospitality[88]

For what concerns *digital identity companies* instead, the industries in which their solutions are seen include:

- eBanking
- eCommerce
- Entertainment
- Healthcare
- Telecommunications
- Transport/Hospitality[89]

The mobile digital identity services provided by *MNOs* can provide the gateway to a vast range of public and private services, related in particular to:

- eBanking
- eCommerce

[87] https://blog.hubspot.com/marketing/most-popular-social-logins-infographic

[88] https://www.bankid.no/en/private/areas-of-use/

[89] See footnotes 26, 27, 29, 30

- Education
- eGovernment
- Healthcare[90][91]

Government eIDs are predominantly used to access online public services, which can vary depending on the country, and are used to a lesser extent to access private services.

Finally, taking into account the *digital identity networks*, which, as mentioned previously, are not identity providers, but a facilitator between identity and service providers, these have been used in the following industries:

- eBanking
- eCommerce
- eGovernment
- Entertainment
- Media/Publishing
- Telecommunication
- Transport/Hospitality[92][93]

[90] https://www.mobileid.ch/en

[91] https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf

[92] https://verimi.de/en

[93] https://ec.europa.eu/futurium/en/content/electronic-payments-enabler-egovernment

THE USE OF DECENTRALISED IDENTITY IN THE BYOI MODEL

05

DECENTRALISED IDENTITY IN THE BYOI ENVIRONMENT

Most of the digital identity providers analysed so far base their model on a centralised ID or federated ID. The centralised model consists in a system where users' credentials are stored and controlled by a single central authority, typically in a single database. The classic example is that of a user creating a digital identity through a username and password procedure every time he/she intends to access a service provider website/platform. This results in inconvenience for users as they must remember a large number of credentials that can easily be forgotten or lost. The main issue related to this model, however, is that it provides a low level of portability, as the identities used are limited to the domains were they were initially created. Moreover, this solution is neither secure nor efficient for service providers who are targeted by hackers and must invest resources every time a user needs to reset his/her account.

These drawbacks led to the implementation of the federated model, which links a person's digital/electronic identity, storing and recognizing it across multiple identity management systems. In other words, this solution allows a user's digital identity to be recognized by multiple service providers, therefore solving the problem of portability and meaning that individual service providers' websites/platforms, do not need to build their own identity management infrastructure.

Examples of this federated model are provided by the eIDs of banks or financial institutions[94] as well as those of social media companies. A drawback of this federated model, which is also experienced by the centralised model, consists in the fact that these digital identities are not in the hands of the owner. The user is consequently not in full control of the use that is made of the information/data related to his/her identity, leading inevitably to privacy issues.

One possible way to address such issues is represented by a new model for digital identity called "decentralised identity", which aims to provide users with an identity that

[94] See Error! Reference source not found., page 12.

is[95]:

- *Case centric*: showing only data necessary to a specific situation.
- *User centric*: allowing users to decide whom to give data to and in which measures.
- *Trusted, portable and verifiable*: bringing the trust of centralized identities to the digital world and at the same time ensuring an overall portability.

Among the different types of BYOI providers analysed so far, some are already pursuing a decentralised approach, while others are undergoing a technological transformation which will allow them to do so.

A key set of underlying technologies enabling user control over their identities are *distributed ledger technologies*[96] (such as blockchain). These allow the users to encrypt their personal information into private keys and store them in identity wallets that can be installed on mobile devices or PCs. These private keys remain under the users' exclusive control, who in turn can decide whether to grant third parties access to them or not. Users not only have control over their personal information, but can decide what information to include when sharing identity data, and with whom to share it, changing completely the digital identity landscape.

The information that users share with the service providers must be verified by someone. Such verification can come from all kind of trustworthy sources including governments, insurers, banks, MNOs or any organization which belongs to the decentralised identity providers' network.

For a concrete example of how this technology works, consider the process involved in a request for a home loan. The bank requires a lot of personal information to complete the user's application, asking him/her to provide his/her legal name, current address, employment history, credit score, etc. In this situation, using a decentralised identity the user can ensure the bank is provided with only the information required for the application, without having to disclose additional information that is not relevant, thus preventing the misuse of data by the bank.

PROVIDERS OF DECENTRALISED DIGITAL IDENTITY FOR BYOI

In this new environment, the digital identity providers analysed until now include:

- Providers of decentralised digital identities;
- Digital identity providers exploring providing decentralised digital identities;
- Digital identity providers partnering with providers of decentralised digital identities.

These groups crosscut the types of identity providers described in chapter 3.

We find examples of the first group – providers of decentralised identity - among bank and financial institutions eIDs (Verified.me[97]) and digital identity companies (SisuID[98] and GlobalID[99]), with all of them providing users with the possibility of directly managing their identity thanks to the exploitation of distributed ledger technologies. Other solutions of this kind available on the market, include Sovrin[100], uPort[101], IBM[102], Microsoft[103], and SecureKey[104]. The city of Zug in Switzerland has leveraged the uPort solution to carry out a

[95] Forrester (2019), Decentralized Digital Identity: A Primer For B2C Marketers

[96] See https://www.gsma.com/identity/decentralised-identity

[97] https://verified.me/wp-content/uploads/2019/05/DIACC_Phase2_SK-2019-FINAL.pdf

[98] https://sisuid.com/rulebook/SisuID-Governance-Rulebook-v1.0.pdf

[99] https://medium.com/@myglobal_id/globalid-partners-with-coti-a-blockchain-based-payments-network-b241d4a40d18

[100] https://sovrin.org/

[101] https://www.uport.me/

[102] https://www.ibm.com/blockchain/solutions/identity

[103] https://www.microsoft.com/en/security/business/identity/own-your-identity?market=af

[104] https://securekey.com/

pilot project with the aim of creating the world's first decentralised government-issued identity[105]. There are few government initiatives moving in this direction, however one other example, is provided by the IdentiCAT project in Catalonia, which is expected to soon provide its citizens with a decentralised digital identity[106].

Identity providers exploring decentralised identity include Verimi[107], MasterCard[108] (both digital identity networks), SK Telecom and Deutsche Telekom[109] (both Mobile Network Operators). These providers are planning to undergo a technological transformation that will allow them to provide users with a decentralised digital identity.

The final group is made up of digital identity providers partnering with providers of decentralised digital identities. This group includes the digital identity company such as Onfido, which partners with providers of decentralised digital identity to equip them with forefront technologies in order to strengthen the identification process.

There is therefore no one type of identity provider (of the types described in Chapter 3 which is exclusively or predominantly associated with decentralised identity. The extent to which these different types of identity providers are exploring or providing decentralised identities is visualised in Figure 1.

Figure 1: Types of BYOI Identity providers' association with decentralised identity

The use cases associated with the digital identity providers described in chapter 4 apply also to the providers of decentralised digital identities. An additional functionality often associated with decentralised digital identities is the ability to sign and verify electronic transactions or documents. This is possible thanks to the private keys

[105] https://consensys.net/blockchain-use-cases/government-and-the-public-sector/zug/

[106] https://www.catalannews.com/tech-science/item/catalan-government-presents-identicat-decentralised-digital-identity-project#:~:text=According%20to%20Torra%2C%20IdentiCAT%20would,of%20their%20identity%20and%20data.%E2%80%9D

[107] https://www.gi-de.com/en/it/g-d-group/press/press-releases/detail/press-detail/the-green-button-is-online-verimi-is-gradually-launching-its-id-and-data-platform/

[108] https://www.wired.com/story/mastercard-digital-id/

[109] https://www.gsma.com/identity/news-flash-mobile-operators-progress-blockchain-based-identity

encrypting information within the identity wallet of the user.

ADVANTAGES AND CHALLENGES

A primary advantage associated with decentralised identities is privacy. The distributed ledger technologies (DLT) underlying such identities put users in the position to decide what use is made of their identity data, protecting themselves from the risk of identity theft common of centralized systems where identity is stored in a single database.

Another advantage linked to privacy is that thanks to distributed ledger technologies, the trusted party issuing the digital certificate will not know that a proof or an attestation was requested by the user. This means that the identity provider and service provider are blinded from one another, preventing user tracking.

In terms of security, one of the most significant advantages is that distributing users' data on the blockchain makes it possible to disintermediate existing centralized data storage systems, while still maintaining trust and data integrity. This limits the risk of hackers gaining unauthorized data access, as there is no centralised system comprising thousands or even million users identities for them to attack.

However, there are also some challenges that should be addressed in order to get the best out of this model. First, reaping the benefits mentioned above depends on how well populated the ecosystem is, both in terms of users willing to use such solutions and service providers willing to accept them. This requires the implementation of a large number of new infrastructures, including new blockchain registries for decentralised identities, user wallets, and cloud services able to connect everyone in the ecosystem.

Moreover, the fact that the decentralised model doesn't rely on third parties creates a considerable problem if a user loses his/her identity wallet with the private keys enabling his/her personal information. A satisfactory solution enabling users to recover their identity without diminishing the privacy and security features at the heart of this model has not yet been found.

An additional challenge is associated with the "honesty" of the user. Although putting identity in users' hands can enhance privacy and security, it also represent a threat when necessary information should be disclosed. Users might be tempted to disclose only the information strictly requested by the relying party to conceal other information that may negatively impact their digital reputation as a whole.

Overall however, the potential benefits linked to the exploitation of decentralised digital identities seem to exceed the challenges that need to be addressed, which are typical of a model which still requires further development.

Conclusions

05

In this report, five types of private providers of BYOI solutions have been considered – social media, banks, mobile network identities, digital identity companies, and digital identity networks – alongside government providers of such identities.

Especially for social media BYOI options there is a high level of availability and use of these identity solutions. However, it is also clear that such social media identities are not currently used for certain types of tasks, in particularly those which require a high level of assurance. Currently these social media identities, largely provided by Facebook and Google, have prioritised low hassle use and user experience ahead of provision of the more rigorous authentication that would be required in order for their identity solutions to be used in more sensitive situations.

Other BYOI solution providers, have stepped into this gap, and provide identities that satisfy these demands for higher level of assurance. However, such solutions also come with a lower level of user convenience, suggesting that there continues to be some kind of trade-off between these two dimensions. In addition, these other BYOI identities have a lower level of take-up. Given this context, with multiple different types of identity providers offering BYOI identity solutions appropriate for different types of use-cases, the future of digital identification may be fragmented.

In light of this, there are at least three strategies that governments could adopt when considering BYOI identity providers. Firstly, they could assess the service these BYOI providers offer their users, consider how their practices could be translated to the government eID scenario, and assess the significance of any effect on security.

Secondly, as users of BYOI solutions increase, governments might reassess the extent to which their own online public services can be accessed using these solutions. A number of EU countries have of course already taken this route, particularly with eID solutions provided by banks. However this could be extended to additional countries or to additional types of digital identities.

Finally, government identity providers could consider how their own solutions could be used in a complementary manner to increase the level of assurance associated with low assurance (but convenient and widespread) BYOI solutions such as those provided by social media. One option could be to work with these companies to link the social media account to the government eID. This could entail the creation of a derived identity account or simply the re-use of verified attributes issued by governments.

Whether or not these strategies are pursued, it seems likely that BYOI identities are here to stay. Government providers of digital identity solutions will have to grapple with the drivers and context that led to their adoption. Whether through competition, or collaboration, they will have to find a way to coexist with the BYOI trend and the private solution providers linked to it.

European Commission

Business trends report - Bring Your Own Identity

2020 – 26 pages