ABE EBA

EURO BANKING ASSOCIATION

Opinion Paper on Digital Identity: 'From check-out to check-in'

EBA Working Group on Electronic Alternative Payments

Version 1.0

13th May 2014

CONTENTS

The information contained in this document is provided for information purposes only and should not be construed as professional advice. The views expressed are those of the members of the EBA Working Group on Electronic Alternative Payments and not necessarily the views of the EBA. EBA or its affiliates do not accept any liability whatsoever arising from any alleged consequences or damages arising from the use or application of the information and give no warranties of any kind in relation to the information provided.

layout: www.quadratpunkt.de
photo credit: © fotolia.com / scusi

I. PREFACE

The internet has irreversibly changed the way we look at commerce. Separation of time and location between buyers and merchants is the new normal, introducing a whole array of new digital players, risks and opportunities also in the banking world. One ‘basic ingredient’ for the future growth of online business (both in the private and public domain) is a reliable digital identity of buyers and merchants, offering tremendous opportunities for both incumbents and new players.

Businesses and public services look for comprehensive solutions that enable ordinary people to authenticate themselves towards merchants and towards each other. The sharing of personal data in a private, controlled, secure and convenient way without having it spread all over the internet, is another crucial pocket of value to be unlocked. Offering such services to enable commerce with minimal loss of customer conversion rates at merchants is of great value and defines a whole new market.

This paper expresses an opinion about the value of digital identity services to banks, the contenders in this new market, why this is the right time to seize this opportunity and finally why the collective European banks are so well positioned to offer this service to their customers and monetise this opportunity.

In the first section, the value of digital identity solutions for consumers and businesses is explained. In the second section, we look at the opportunity of digital identity from the perspective of the service providers. In the third section, the arising economy around digital identity is explored: the players that are active and the business models that apply. In section 4, we will argue that banks are well positioned to claim a role in the emerging digital identity market place, ending in section 5 with recommendations for action by banks.

II. MANAGEMENT SUMMARY

The market for digital identity[1] is one of enormous growth driven by accelerating demand from consumers and businesses for digital services and further fuelled by an array of security, privacy and KYC driven European regulation (PSD2, General Data Protection, SecuRe Pay, eIDAS, AML4).

This market is a typical example of a two-sided network, where two categories of actors have different needs: a user (typically 'the buyer', a consumer, business or government) wants to use the service of the relying party ('merchant or government'), whereas the relying party wants to know whom it is dealing with. The relying party is the website or application that wants verification of the identifier of its user. Cross-sided network effects (more users stimulate more relying parties) can ignite this market, but for the years to come the classic chicken and egg problem has to be overcome. Will the number of users drive the demand of relying parties or vice versa?

As relying parties had to solve this problem on their own, three solution generations have emerged over the years. The first generation is the direct model where the relying party issues its own authentication method and keeps it for proprietary use. Banks are a well-known example of the first generation where they have built their own credential infrastructure for their (mobile) internet channel. The second generation is a three-party model where parties with large user bases (e.g. social media players) open up and make their authentication method available for other parties. In the third generation, authentication is organised through a trust framework: a four-corner model, similar to that of payments (e.g. schemes). In this model users and relying parties can choose their own service provider and they are able to interact with each other in a consistent and secure fashion because of the underlying set of agreements.

Within the different models, the value of authentication services depends on the 'breadth' and 'depth' as displayed in **Figure 1**. The more attributes (pieces of personal information) the services provide, the breadth, the more value the service generates. The depth concerns the trustworthiness ('level of assurance') of single attributes.

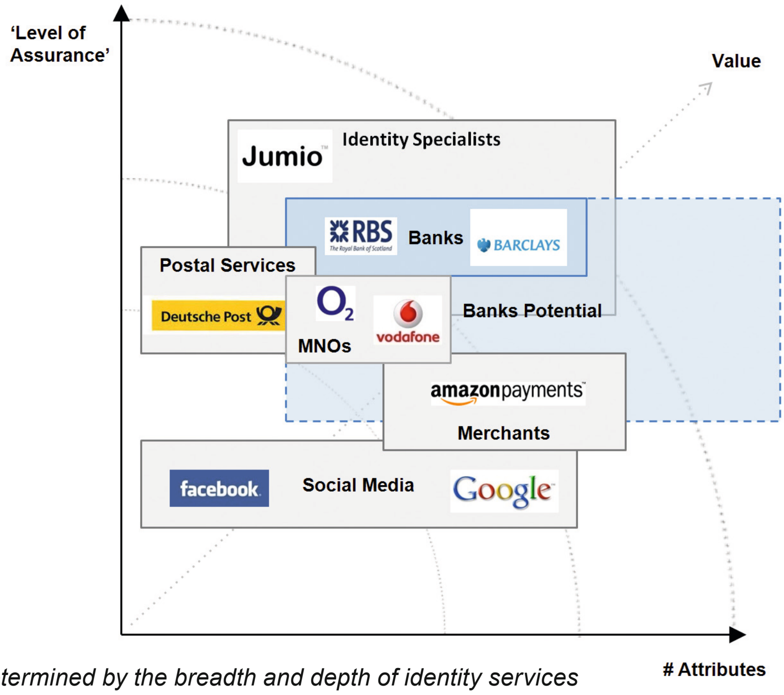


Figure 1: *Value determined by the breadth and depth of identity services*

[1] The definition of digital identity can be found in Annex A – Glossary of terms

There is tremendous value in knowing your customers, just as there is value for consumers in controlled ways of sharing (parts of) their identity. To reveal your identity online, there are a lot of fields to be manually inserted. The demand for applications to simplify this process is increasing, accelerated by the mobile revolution, as mobile phones allow for less manual interaction. 'One click' becomes the norm. A powerful example is where the traditional check-out in any commercial context, is being replaced by a check-in. This way, the buyer is identified when he enters (e.g. when he logs in his phone or tablet), instead of when he leaves (i.e. when he pays). Users can benefit from a higher, more personal service whereas the merchant can increase the relevance of his service and, last but not least, has the lowest barriers for conversion from visitors into buyers.

Traditionally, authentication is part of a payment transaction. With the authentication and payment diverging, part of the value that is currently in payment transactions is shifting towards the separate authentication ('digital identity'). As such 'unbundling' is taking place, the check-in becomes the pivotal moment in the customer journey instead of the check-out. The actual size of this market is expected to be larger than payments by an order of magnitude: digital identity transactions only involve payments a fraction of the time. In the Nordic area a few successful digital identity services already exist, illustrating the potential of this market.

With the momentum building around this category of services, an ecosystem of players and business models is gradually emerging and we can see the first outlines of how this market is likely to evolve. Various types of players are all chasing their piece of the pie, such as postal services, identity specialists, merchants, social media businesses and telecom providers.

Banks are particularly well positioned to claim a position in this ecosystem, as the market is far from mature. They can benefit from at least three assets they have invested in heavily in the past:

- Their regulated position has earned banks the **trust** of consumers, businesses and the public sector.
- Their experience with cooperation in two-sided markets provides the **network**.
- For reasons of compliance and otherwise, banks have a rich set of verified data about their customers: Know Your Customer (**KYC**).

This does not mean that the battle for the market for digital identity services is already won, given other contenders. There are various categories of service providers that are also aiming for this position. The time is right for banks to take action and monetise this significant opportunity by:

1. The unbundling of the bank's valuable authentication services from payments;
2. Enabling controlled (by customers) availability of valuable information;
3. Setting up and positioning digital identity services towards the market.

Controlling one's digital identity is the tool through which true customer centricity can be realised. Banks have a unique opportunity to become the tool of customer choice.

1. FROM CHECK-OUT TO CHECK-IN

Digital identity services have the potential to provide real value for consumers and businesses as will be illustrated in this first section. Firstly, it is important to understand what the term (digital) identity exactly means:

- Identity is **what I say about myself** (self-declaration)

- Identity is **what others say about me** (assertions)

A trusted identity is what a trusted third party says about me, e.g. passport, driver's license, etc. It is important to realise that a digital identity is not an equivalent of identity. Digital identity describes an ecosystem to use 'real life' identities in online transactions. Separate aspects of a person or organisation's identity are used for the identification process as is shown in **Figure 2**. It is not necessary for online identification to disclose all the attributes at once. The identification process has three (often related) purposes: identification, authentication and authorisation.

One example of where rich identity services could provide the value mentioned above is in shopping contexts where checking in could replace the traditional check-out to smoothen the shopping process for consumers and provide additional revenue for merchants.

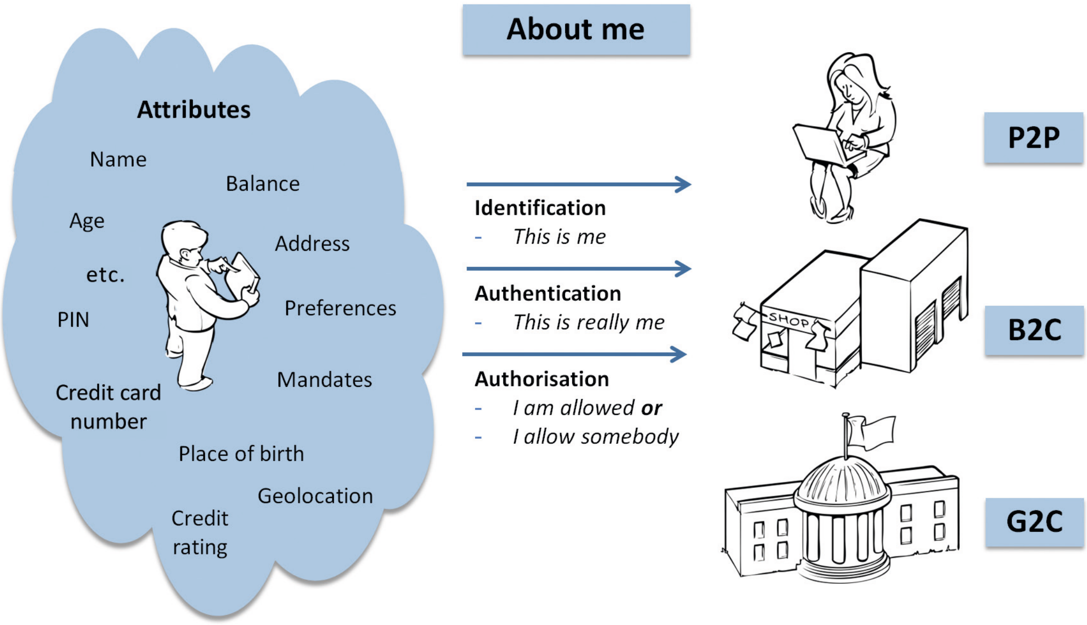


Figure 2: *Attributes are used for identification, authentication and authorisation*

1.1 Driven by the mobile revolution: check-in will replace check-out

The internet has turned almost all concepts in retail upside down, but both in brick-and-mortar and in many web shops, the check-out remains an important step in the shopping process and it is placed at the end of the process. Commonly, the shopping process starts off with an anonymous buyer who browses for the item of choice. Finally, in the last step of the shopping process the buyer is asked to identify himself. If this is a recurring customer, billing address and preferred payment method are often stored and pre-filled to enhance the shopping experience.

The user experience (more and more on smaller screens) and therefore the conversion rate are primarily defined by the authentication method, which currently is often bundled with the payment. If one imagines that the authentication, with consent of the buyer, would take place **before** browsing, shopping and selecting items, then personalised offers can be made based on not only this shopping session, but also on previous visits and even visits to other stores. Buyers would actively choose to share their information (consent!) and enjoy an enhanced proposition and shopping experience. Moreover, personal data such as gender, age and personal preferences could further personalise the offers. Finally, when the buyer has finished and is done shopping, the payment can be executed with only a (one click) confirmation.

More and more (mobile) retailers understand the power of removing the check-out barriers often created by the authentication process. The advantage is two-fold:

- A more detailed understanding of the client's needs can lead to a more rewarding shopping experience;
- Removal of the check-out barriers (due to authentication steps) will lead to major improvement of conversion rates.

Moving the check-in to an earlier moment in the process is illustrated in a shopping context, but the same advantages apply for all kinds of service contexts in the private and public domains. Schematically, the effect of positioning the check-in more early in the process can be illustrated as in **Figure 3**.

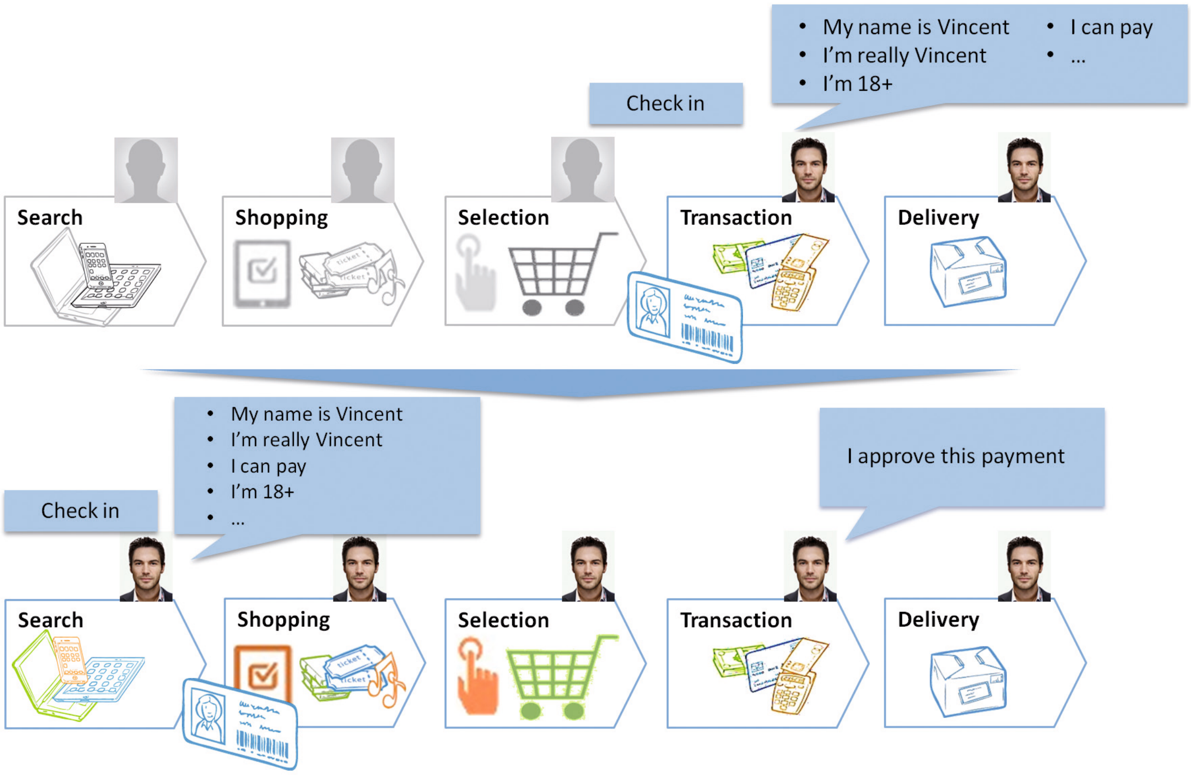


Figure 3: *Positioning the check-out earlier in the (shopping) process*

3D Secure: Paying with your credit card

Paying with a credit card with 3D Secure (3DS) is an example of a classic 'check-out' experience in online retail. Traditional card payments are extended with a dedicated authentication process. The details are entered at the end of the shopping process and the authentication (3DS) is paired with the payment. Often the authentication credentials are specific for the card, which leads to a high drop-out rate, since customers do not always recall their credentials. In practice many online merchants leave out this authentication step in order to preserve their conversion rates and manage the associated risks themselves.

1.2 The unbundling of payments

"If you solve the authentication problem ... everything else is just accounting."
Ross Anderson, Federal Reserve Bank, Kansas City

Retail payments consist of two processes: the **authentication/authorisation** and the actual **transfer of funds**. Traditionally, these two processes occur instantaneously. Unbundling is the process in which the authentication and payment diverge. Authentication is an important part of all kinds of services. Payments have been the application for which authentication has been addressed most extensively. With cards and other devices, people were able to authenticate themselves securely and conveniently. In recent years, the solutions for people to authenticate themselves have been evolving to suit new channels (e.g. internet contexts).

Deutsche Bahn: log in with your national identity card

An example of the use of 'third party authentication methods' in a payment context is the portal of Deutsche Bahn. In this portal, users can initiate, revoke or change the mandate that is used to debit their accounts (for subscriptions and other services). Users can do this without using any credentials. This is possible, because logging on to DB's portal is only possible with the 'Neue Personalausweis' the digital identity card, which assures the authenticity of the operation.

We are now witnessing the application of authentication methods that were once invented for payments in non-payment contexts. For example, credit transfers for a nominal one cent value are being transacted in certain service propositions as an authentication method to validate consumer name and address data to be used, for example, as an e-mandate. Alternatively, new authentication methods that are not associated with payments are applied to payment contexts. The effect of these developments is that authentication and payments are diverging, as is illustrated in **Figure 4**.

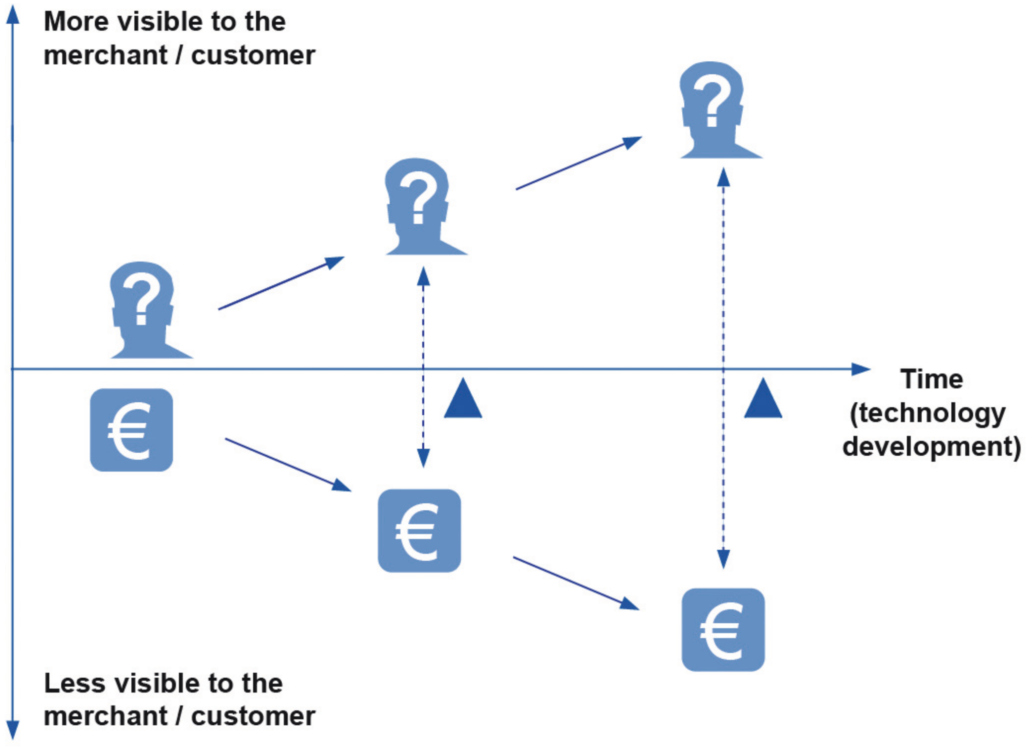

More visible to the merchant / customer
?
?
?
€
€
€
Time (technology development)
Less visible to the merchant / customer

Figure 4: *The unbundling of payments and authentication*

As mentioned in the previous paragraph, a far higher value is placed on authentication services that provide information on users than the value ascribed to traditional payment transaction services. At the same time, this value can be captured by the provider of the authentication and not by the party taking care of the 'administrative' payment element of the process. Today, those two providers of authentication and payments services are usually the same entities, but this is likely to change in the near future (see **section 4**).

Amazon.com: the merchant's proprietary authentication method

Amazon.com is an example where the merchant has developed an authentication method of its own. Using this authentication method that is depending on derived identification in the onboarding process, Amazon can rely on payment methods that would otherwise be 'insecure' (e.g. direct debit, non 3DS card transactions): they can rely on their own authentication to make sure the consumer is trustworthy.

In this first section we have seen the potential of the movement from check-out to check-in and that of the unbundling of payments and authentications. It used to be enough for a buyer to make himself known when the payment was happening. Now the authentication not only becomes more important, it no longer needs to happen simultaneously with the payment transaction. With this unbundling new opportunities arise to tailor the shopping experience to individual buyer preferences or, for example, combine multiple sessions.

PayPal: seamless check-out, thanks to check-in

When a merchant is certain that a consumer is who he claims to be, he will be able to assess the risk better which leads to less transaction barriers. PayPal promoted this concept and introduced a seamless shopping experience for the customer and a secure authentication method for the merchant. After opting for PayPal, the consumer is redirected to the PayPal website for a secure log in. After being redirected back to the merchant, the consumer can proceed shopping and does not have to enter any personal data since these (e.g. name, payment details, delivery address) are provided by PayPal 'under water'. All the consumer needs to do is confirm, which includes consent towards PayPal for sharing the personal details with the merchant.

In the next section, we will take a look at how this value is likely to evolve and where it provides opportunities for service providers in the digital identity domain.

2. LARGER MARKET BEYOND PAYMENTS

The digital transaction market is one of great size and potential growth. The number of users keeps increasing as is the number of transactions per person. This chapter describes this growth as well as the factors driving digital identity and thus the market value. The value of the market is not only determined by the size, the value of digital identity is just as important. The last part of this chapter explains how regulation further stimulates the growth.

2.1 Growing market because of larger user base and more transactions per user

The number of transactions executed online is increasing since more business is handled online. Those transactions demand certain solutions for authentication and authorisations. Digital services are no longer considered a special feature of an analogous process. It is the other way around: digital is the 'new normal'. Consumers expect those services from both public and private organisations. This growth, facilitated by the digitalisation of our society, is composed of two drivers:

- **More users of digital transactions**
- **More digital transactions per user**

This double effect is a proven recipe for exponential growth.

More users of digital transactions

The use of internet by individuals keeps increasing steadily in the European Union as is shown in **Figure 5**.

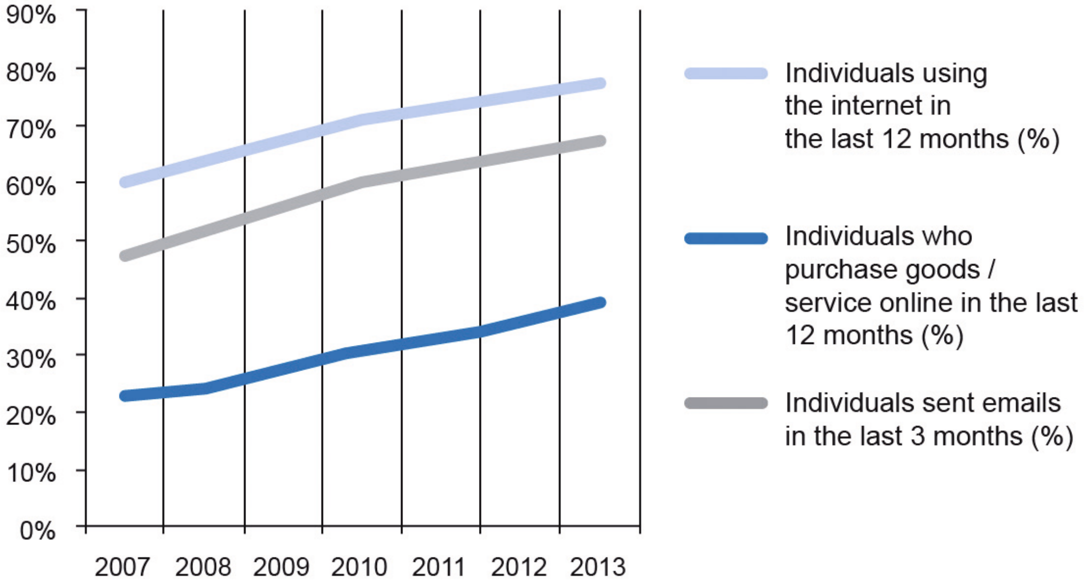


Figure 5: *Internet use of individuals in the European Union (28 countries)*

Source: Eurostat, Innopay analysis

Not only is the level of growth quite steady, there is still a lot to be gained. Merely 50 percent of the European individuals who use the internet purchased services or goods online in 2013. The growth potential of additional users for digital services and thus digital transactions is expected to be of significant size over the next five years. Research by Forrester forecasts a compound annual growth rate of online retail sales in Europe of 11 percent until 2017[2]. More and more individuals start consuming digital services, driving the demand. The supply side, however, is still fragmented as will be discussed in **section 3.**

[2] Forrester (2013): European Online Retail Forecast, 2012 to 2017

More digital transactions per user

The nature of digital transactions may differ enormously. The traditional payment market depicts only a part of the broader market for ‘digital identity transactions’.

A rough and conservative estimate is that the amount of digital transactions is a factor 4-6 times larger than payments, since each successful payment is part of other increasingly digital processes such as contracting, ordering, invoicing, delivery and taxing.

Table 1 shows the estimated number of transactions in the European Union in 2013 for several digital identity services.

Individuals in the EU in 2013 using …	Millions	Year-on-Year growth	Number of authentication transactions per year (Billions)
eGovernmental services	*207*	*-7%*	*0.5*
Social Media	*217*	*+14%*	*79*
Internet Banking	*212*	*+5%*	*14*
eCommerce	*238*	*+7%*	*5*
Email	*339*	*+3%*	*125*

Table 1: *Information society statistics of the European Union*[3]

Digital services are provided by both governments and private parties. Even though the absolute number of people interacting online with governmental organisations is substantial (207 million in 2013), the percentage of the population of the European Union using these services is at the same level in 2013 as it was in 2010. As can be expected, the real growth is to be found in the private sector.

The significant increase of both users and number of transactions per user show how attractive this market is to enter. The following section describes how the regulation stimulates the digital identity market to grow even further. Section 3 depicts how the market developed thus far and identifies the opportunities in this industry.

2.2 EU Regulation drives digital identity

Governments are increasingly aware of digital fraud, privacy and security. On a European level several regulations are in effect or in preparation. Although not all of this regulation is always well coordinated, it all points into the direction that digital identities are becoming pivotal for the further growth of the digital economy.

The five most relevant European regulations for banks, directives and recommendations are listed below. Digital identity transactions present a whole new canvas for the banks to add value and sustainably claim the positions closest to the end-users.

[3] *Source: Innopay analysis, Eurostat, Ecommerce Europe*. European Union: 28 countries as defined by the Eurostat. Note that the year-on-year growth of social media is from 2011-2013 instead of 2012-2013 like the others.

1. SecuRe Pay recommendations

The SecuRe Pay Forum is a forum of the national supervisors from the European Economic Area with support of the ECB. In January 2013, this forum published recommendations on the security of online payments. The keystone is that all internet transactions have to have 'strong authentication'. Without a clear definition of 'strong', this implies a thorough credential issuing process and secure transaction infrastructure.

2. Access to the Account (PSD2)

Access to the Account (XS2A) is a chapter in the draft PSD2 regulation, which is to be in place in 2017. Access to the account does not only offer Third Party Providers (TPPs) a lot of opportunities but also incumbent players. The amendment of November 2013 proposes that "*The new rules should therefore address all those challenges appropriately and ensure that TPPs operating in the Union are licensed or registered and supervised as payment institutions.*" The need for authentication methods compliant to the EU regulation will thus increase as challenges arise in safeguarding the personal data provided to them by the consumers. Authentication is defined as a procedure that permits the 'Account servicing PSP' (bank) to verify the identity of the consumer. That does also include the use of the personalised security features or the checking of personalised identity documents.

3. Fourth AML Directive

In April 2014, the European Parliament voted in favour of the proposal of the Fourth AML Directive. The Directive will be processed further after the European elections. Customer Due Diligence (CDD) is required when a consumer is not physically present at a transaction and account opening. An important CDD measure to be taken is "*identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.*" Online financial services (incl. money remittances, mobile banks and lending) are in great need for online CDD solutions.

4. General Data Protection Regulation

The General Data Protection Regulation aims for more effective control of a person over his personal data. Furthermore, harmonisation of legislation will make it easier for non-EU companies to enter the European market and comply with all countries at once. This increased competition should lead to more innovation. However, a failure to comply with this legislation could result in severe penalties up to five percent of the worldwide turnover. It is still unclear when exactly this regulation will come into effect.

5. eIDAS Regulation

The Regulation on 'e-identity and signature' (eIDAS) is expected to be in place by July 2014. The aim is to ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries and to create a European internal market for public electronic trust services. Although it is confined to the public sector eIDAS is driving the awareness and roll-out of secure credentials, offering also opportunities for private digital identity service providers including banks, Mobile Network Operators (MNOs) and postal operators.

3. EMERGING DIGITAL IDENTITY MARKET

In the previous sections we have seen the opportunities of the emerging market for digital identity services for consumers and businesses and, as a consequence, for all private and public parties that provide online services. In recent years, an ecosystem has slowly been developing and service providers, users and relying parties are exploring how this all fits together. In this third section, we will illustrate the current state of play: the market structure, economics shaping the business, the categories of players that are active and the size of the market.

3.1 A two-sided market similar to payments

Digital transformation is taking place in both the private and the public sector and many opportunities and solutions have emerged to cater for this revolution.

Today, the digital identity market shows all characteristics of a two-sided market: cross-sided network effects (more users attract more relying parties and vice versa) and the classical 'chicken and egg' problem in building up customers on both sides of the market.

As a result today we see the three paradigms existing next to each other: the direct model, the three-party model and the four-corner model. We know all models from the payment industry (**Figure 6**). In the last mature market model users and relying parties (payers and payees in the payment industry) can choose their own service provider and market fragmentation is solved by interoperability agreements or schemes (e.g. Visa and Maestro).

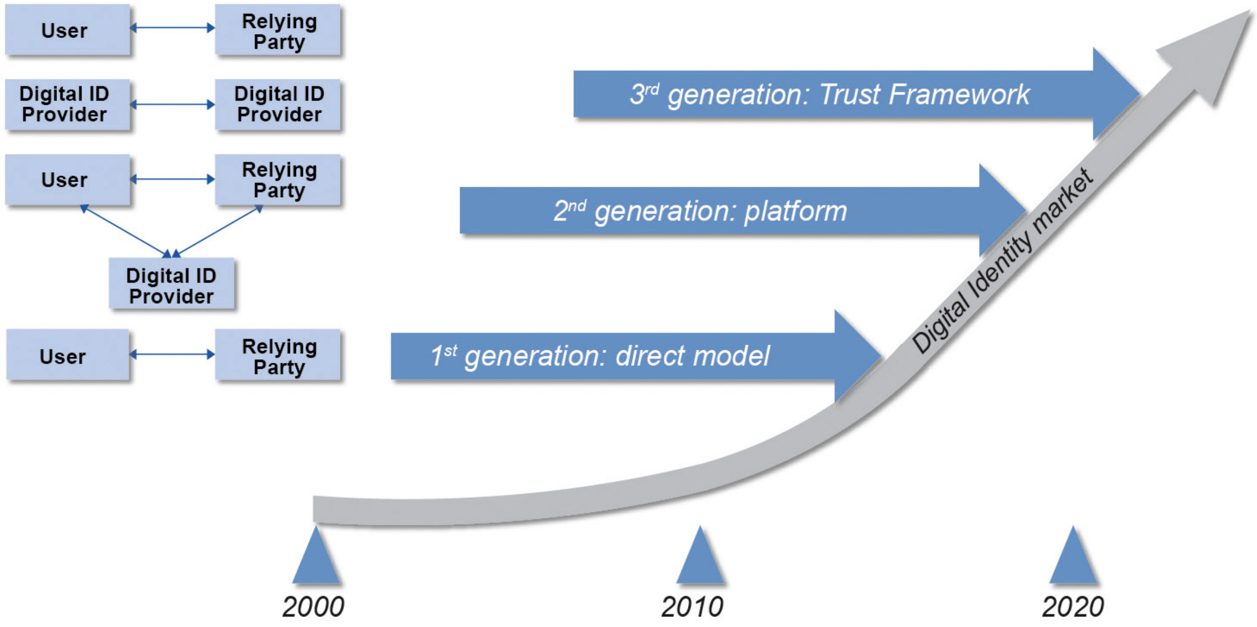


Figure 6: *Evolution of digital identity solutions paradigms*

The direct model of the first generation was set up because market actors (including banks) needed to solve their own business problem. This resulted in users that ended up with multiple passwords and relying parties suffered from the costs of building their own authentication system. Having a growing 'digital keychain' is more and more regarded as a societal (security) risk since many users re-use their password for different websites. A data breach in one website can compromise many other websites as well.

Parties with large user bases (e.g. social media players) made their services available and became identity service providers in the second generation. The third generation of identity services is based on a four-corner model where different roles emerged in the digital identity business: brokers, identity providers, authentication service providers and mandate registries for authenticating legal entities. In a growing number of jurisdictions (including UK, US, the Nordics, NL) we see a further appreciation of the two-sided nature of digital identity and the need for trust frameworks as the scalable paradigm for going forward. The reduced risk of market dominance by a single set of players is also regarded (by public authorities, users and relying parties) as a strategic advantage of the four-corner model.

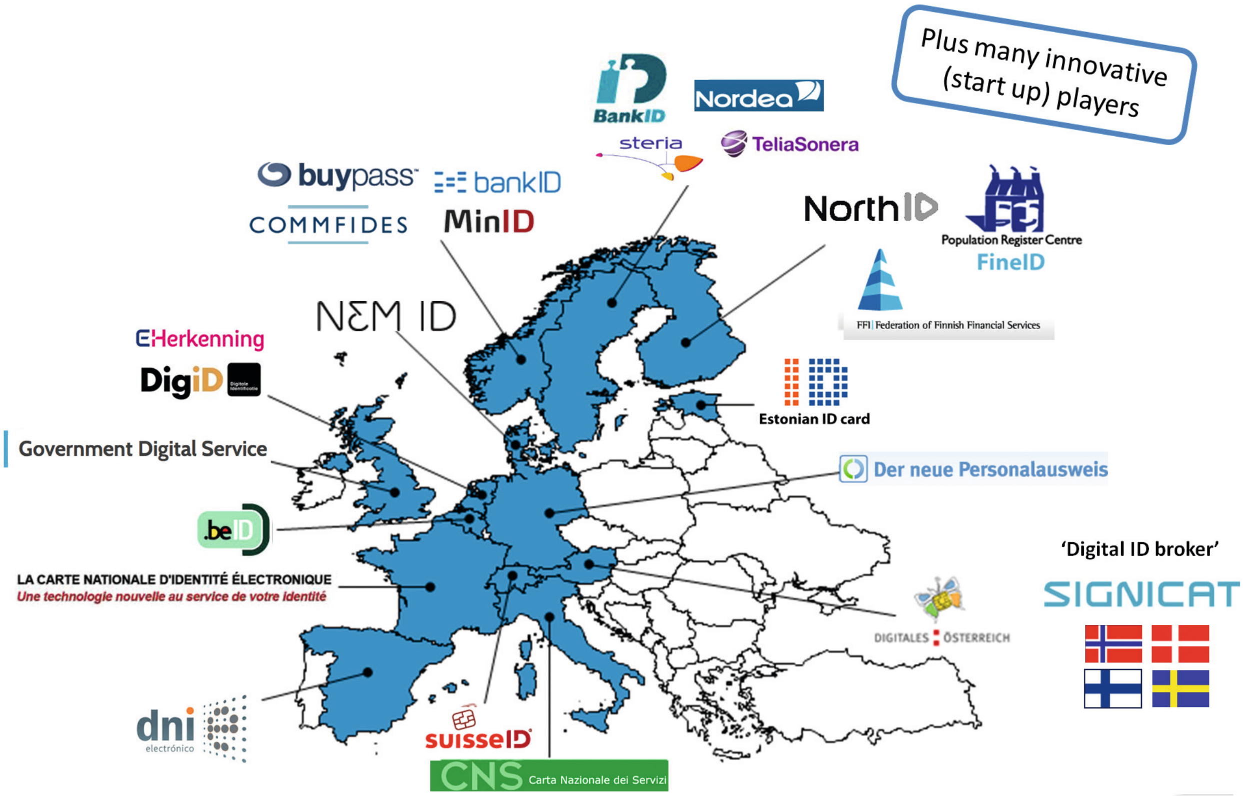

Plus many innovative (start up) players
BankID
Nordea
steria
TeliaSonera
buypass
bankID
COMMFIDES
MinID
NorthID
Population Register Centre
FineID
FFI Federation of Finnish Financial Services
NEM ID
EHerkenning
DigiD
Estonian ID card
Government Digital Service
Der neue Personalausweis
.beID
'Digital ID broker'
SIGNICAT
LA CARTE NATIONALE D'IDENTITÉ ÉLECTRONIQUE
Une technologie nouvelle au service de votre identité
DIGITALES ÖSTERREICH
dni electrónico
suisseID
CNS Carta Nazionale dei Servizi

Figure 7: *Digital identity solutions across Europe*

All three models and the roles within these models are currently applied widely. As **Figure 7** shows, the digital identity market shows a very diverse picture.

For service providers to step in, the concept of trust frameworks provides the opportunity to leverage solutions across industries, provide buyers and merchants with a trusted and uniform user experience and to realise the scale that is needed for a viable business case. As the industry evolved from the first two generations, the economics in the third generation have, until now, mostly been based on both sides of the ecosystem 'paying their own fare'. In a starting two-sided market, the 'chicken and egg' problem has to be overcome since the 'willingness to pay' is not equally divided over the two sides of the market. At this stage of the market, typically the merchant (relying party) has a larger benefit than the buyer (user). Therefore, a stimulus towards the buyer side of the ecosystem makes sense, in order to offset the imbalance of benefits.

This evolution of the business model will be proven crucial for the ignition of the identity market in a similar way, as this has been conditional for the fast growth of the electronic payment market.

3.2 The value of a digital identity transaction

The value (and costs) of digital identity depends both on the level of security offered ('level of assurance', depth) and the types of information offered ('attributes', breadth) to merchants and other digital service providers. The highest levels of assurance (LOA) involve also a (more expensive) physical identity checking during the issuing process of authentication credentials.

eHerkenning: a trust framework for B2B and B2G digital identity

eHerkenning (eRecognition in English) is a trust framework, which allows market parties to issue a digital key for businesses to interact with eGovernment services. By the end of 2013, 92,202 businesses could interact with 75 public bodies resulting in 125,000 transactions per month. The identity providers all have different ways to charge their customers for the products, which all comply with the eHerkenning standards (most of them use a combination of one-off and annual fees). eHerkenning defined the one-off and recurring pricing structure as is shown in **Figure 8**: one-off costs for verification of identities (issuing process) and recurring costs for the on-going service provision. Also the price distinction is shown in 'levels of assurance' (depth). The pricing as shown still has a strong potential for decrease when volumes increase.

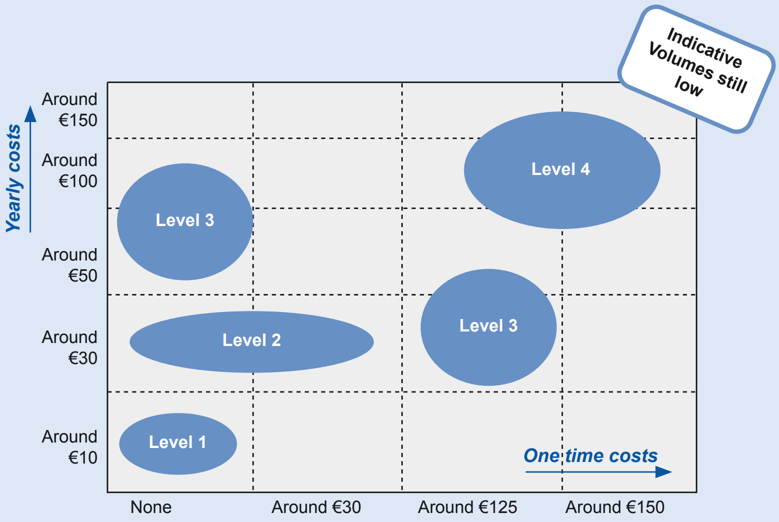


Figure 8: *price points of authentication tokens*

The trust framework that is currently live in the Netherlands enables representatives of a business to sign in a website of a government organisation or another business. This can be done with the e-identity credential issued by the e-identity service provider of their choice. Tokens include user name/password, phone, one-time password (OTP), or public key certificate, effectively supporting all four LOAs. An accredited e-Recognition broker has access to an authentication service and an authorisation register where the check is done if the representative may act on behalf of his business. After logging on successfully, the representative can submit his/her application, and the relying party can be sure it is genuine.

The registrations of reliable attributes (such as a verified address or minimum age) are valuable activities for which merchants are prepared to pay higher amounts than for a payment transaction. The number of third parties that offer these expensive and highly regulated services is increasing every day.

To scope the field of digital identity services, a framework to assess the breadth and the depth of these services can be useful. The breadth of an identity transaction refers to the richness of data, the number of attributes (pieces of information such as an address) that can be provided or shared. The term 'depth' is used for the certainty around these attributes, the level of assurance as described above. One can imagine that in certain contexts, e.g. in many commercial contexts, a rich image of (potential) customers is useful for merchants to apply filters and show the most relevant items. Whether or not all of the attributes are 100 percent certain is not the most important, a specific combination of attributes can increase certainty (e.g. device finger print and location). Social media profiles, for example, provide lots of detail about a person's demographic information, preferences, earlier behaviour, social surrounding, etc. This is a sharp contrast with the validation of a person's passport at the desk of the local post office. Here, the detail and richness of the data is limited, but the certainty to which relying parties can assume that the name, date of birth, etc. are correct is much higher. This is shown in **Figure 9**. If an authentication service validates one's age with certainty, the LOA is high and one attribute is clear; the age verification service is thus placed in the left top of the graph.

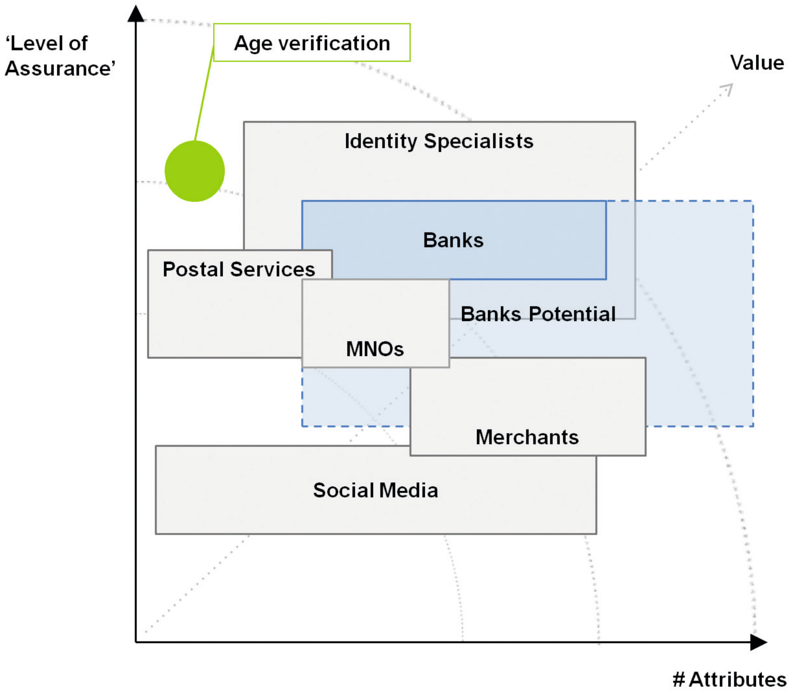


Figure 9: *Authentication services sorted by quality and quantity*

To sum up, the value of an identity transaction is determined by the breadth (number of attributes) and the depth (level of assurance) of the information provided/shared. Relying parties, based on the context, determine their needs on both axes.

3.3 Value turned into a business model

As familiar as the four-corner model is to financial institutions, it is important to realise the difference of digital identity transactions compared to payments. An important consideration is that the value of a digital identity transaction is difficult to determine because of the context sensitivity: the value depends on what you can do with it. Common business models in payments apply a fixed and/or ad valorum fee to transactions. In this way, these business models apply some sort of value based pricing as merchants (or consumers) are likely to accept a higher price for a transaction, as the amount transferred is higher. With digital identity the pricing might be dependent on the value the user and relying parties perceive.

Use case for customers

John had so many passwords and tokens that he decided to subscribe to a digital identity service provider. This provider issues a token which stores his credentials in a secure manner. These credentials may be based on a smart card or any other authentication token (One-Time Password, pass, username/password, SMS etc.). John makes sure that when he joins, the service of his choice can be used across all channels and devices. Assuming that John's service providers (relying parties) are connected to his identity service provider, John is able to:

- Transfer money in his online bank environment;
- Access his online government tax services to change his personal information;
- Buy a book at an online retail shop;
- Check the results of the recent blood test in his personal health record;
- Send a message on his employer's intranet portal to his fellow co-workers;
- ...

He has one secure token to authenticate himself and to authorise transactions online. He has paid a one-off fee of €20 to the identity service provider for the enhanced level of security and convenience. He no longer has to enter his information and obtain a separate account for each service. He is in control over his own personal information.

Validated identities and personal information can be of substantial value to relying parties, because they reduce operational back office costs for checking and risks while doing business online, hereby some indicative values:

- Validated email or physical address: € 2-4
- Financial check: € 4-6
- Qualified addresses (preferences): € 4-8

Use case for merchants

A small Italian caterer wants to expand its offline services with an online shop. The online shop will, among other products, sell wine. The legislation in his country requires a certain 'Level of Assurance' for authentication when selling alcohol online to verify that the buying customer is over 18 years old.

The shop chooses to take on a digital identity provider affiliated with a trusted network (third generation) for the authentication service.

Because the seller is now connected to a network, all buyers using an authentication service within the network that are compliant with the rules, are now able to order at the shop without opening an account. Only the buyers using providers in the network offering services compliant with the requirements imposed on the level of security are able to buy wine online.

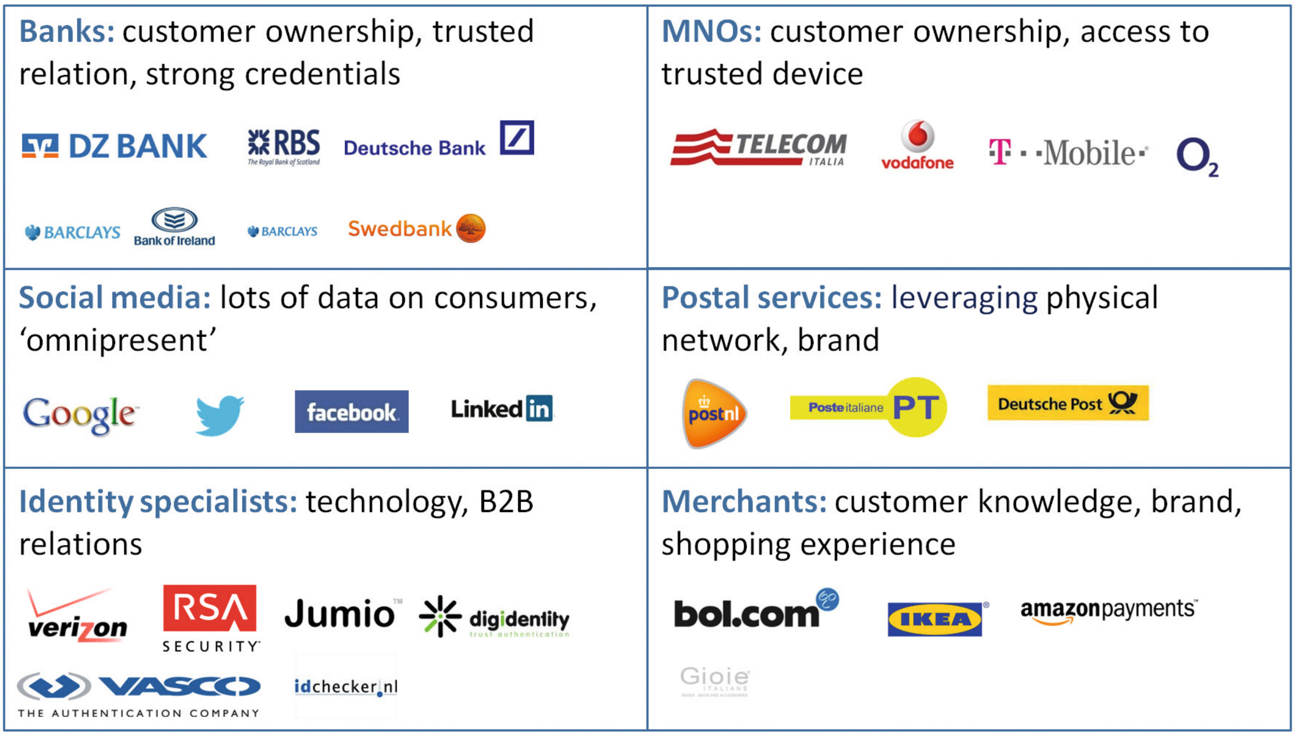
Since buyers are no longer required to open an account at the webshop and they can use an authentication service they have chosen themselves, the conversion rate is likely to be significantly higher.

The merchant will pay a transaction fee to his identity provider for its services. Moreover, the identity provider of the merchant also pays a transaction fee to the identity provider of the customer. That provider may or may not charge his customers for the offered services.

For transactions that concern personal attributes or pieces of information, it is also likely that end-users are willing to pay a price that is relative to the broader context of the transaction. The value to be paid by merchants and the public sector is a function of the op-erational cost reductions and the increase in on-line conversion. The business model in the Nordics will be further explained in **section 4**.

4. BANKS WELL POSITIONED, BUT FAR FOR FROM SAFE

This fourth section will discuss that banks are not alone in the digital identity space, but that they have several key assets that they can exploit when moving into the digital identity space. In **Figure 10** categories of service providers are identified that in some way already play a role today in the emerging digital identity market.



Banks: customer ownership, trusted relation, strong credentials

MNOs: customer ownership, access to trusted device

Social media: lots of data on consumers, 'omnipresent'

Postal services: leveraging physical network, brand

Identity specialists: technology, B2B relations

Merchants: customer knowledge, brand, shopping experience

Figure 10: *Different categories of service providers aiming for a role in digital identity*

The first section below will focus on the assets that banks have: trust, network and KYC. In the second section below, competitors are identified that could claim the same position the banks should be aiming for.

4.1 Banks are well positioned ...

Banks in general have several assets that are key to establishing a trustworthy position in the digital identity space. The banks have:

1. **Trust**:
   the image and history of being a trusted partner

2. **Network**:
   a trusted and secure (cross-border) network among them as well as the experience to build services on top of the network

3. **KYC**:
   rich and reliable information about their customers

SEPA Direct Debit e-Mandates: re-using digital identities

e-Mandates are a great example of the application of digital identity in a four-corner model by banks. With the bank's authentication token, the debtor signs the mandate digitally, giving his consent to his creditor to debit his account at the issuing bank via a (SEPA) direct debit. When the authentication service is successfully performed by the issuing bank, the e-Mandate is sent via the acquirer to the creditor. Finally, the creditor sends a confirmation to the debtor.

The MyBank initiative is using this principle because it is designed as a pan-European e-authorisation scheme to be applied on top of online banking infrastructures. Initially positioned for authorisation of payments (SCT, SDD and cards) this scheme can be expanded for use with non-payment use cases. The MyBank Mandate Pilot has been finalised in February 2014.

Because banks could not build on an existing (pan-European) infrastructure for authentication at the time they were creating online banking, they invested heavily to create this service for their customers. They have been cautious when entering the internet era and although incidents have been reported, no major breach has significantly hurt the banks trusted image in this space.

As a result banks enabled global, trusted and governed networks to send and receive funds securely and conveniently. Banks have been investing a lot in knowing and verifying a large set of data points (attributes) of their customers, partly forced by KYC-rules.

Altogether, banks have a secure and high-level credential infrastructure in place that is geared towards payment-related use cases, but could well be broadened to serve other contexts at both public and private parties other than banks.

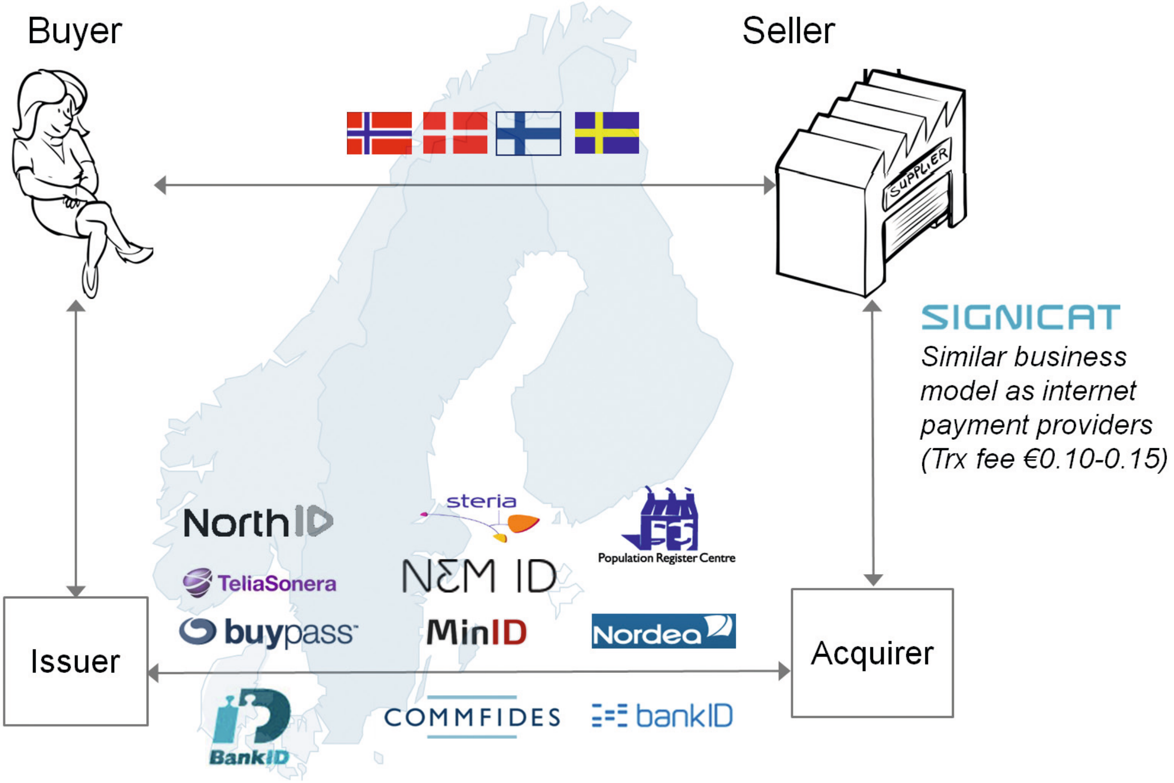


Figure 11: *Merchants are connected to all the trust networks via Signicat*

The opportunity for banks lies exactly in expanding the capabilities of this authentication infrastructure and in the provisioning of generic digital identity services. This has already been done in the Scandinavian region, where banks collaborated in order to re-use their credential infrastructure for authentication purposes. Well-known examples are BankID (both in Norway and Sweden), NemID (Denmark) and Tupas (Finland). To connect the merchants to all the different digital service providers, Signicat serves similar to an internet payment provider in the payment four-corner model (**Figure 11**).

BankID: an e-authentication and e-signing solution in the Nordics

BankID is an e-authentication and e-signing solution provided by Nordic banks. It is being sold to relying parties from the public and private sector. The number of e-identification transactions has been growing in recent years. E-signing is at the start of a similar development as the insurance sector is discovering the solution for the signing of contracts.

The business model of this solution is a per transaction fee, sold directly by the banks to corporates or through resellers that develop tailor-made solutions to fit smaller businesses.

The introduction of a mobile version called ‘Mobile BankID’ has fuelled growth considerably as it made it very easy for consumers to e-identify themselves in a number of different e-services.

It is clear that digital identity services provide a huge opportunity and banks are not the only players aiming at a position in this field, as we will see in the following section. First of all, we see that the issuing and acquiring domains are under pressure and secondly we notice that other categories of service providers also have strong cases.

4.2 ... but far from safe

This section describes two key reasons why banks are far from safe:

- **The issuing and acquiring domain are under pressure**
- **Other market players are warming up**

Issuing and acquiring domains are under pressure

With the unbundling of payments and authentication, third party providers are challenging the business model for banks in the issuing domain. For example, non-bank mobile wallets will intermediate between the issuing bank and its customers. This disintermediation may be even stronger with the advance of ‘access to the payment account’ as proposed in the revised PSD2 (see above). The most valuable part of the transaction, the user experience of authentication, will no longer be exclusively part of the issuer’s service. Of course, banks can respond by seizing the opportunity to develop standalone authentication capabilities, which they can then leverage in other domains. Existing schemes like MyBank could be used as a possible starting point.

On the side of the acquirers, a comparable movement can be observed. Challengers like non-bank (internet) payment service providers (PSPs) are already putting the position of traditional acquirers to the test. Moreover, the PSD2 Regulation aims to ‘reset’ the acquiring domain of payment services, by allowing ‘every party compliant with regulation’ to access the issuing domain of payment accounts. Part of scheme agreements (such as contracting and technical access) is brought into legislation, creating a level playing field for regulated entities. Many kinds of regulated parties can now be part of the acquiring domain: incumbent acquirers and payment service providers, newcomer Third Party Providers (TPPs) and also merchants. This picture is summarised in **Figure 12**.

Furthermore, interchange fees will be capped in the near future. The payment transaction business is changing throughout the entire four-corner model. Banks must act in the area of digital identity (which is out of scope of the PSD2 Regulation) in order to retain control over this valuable part of the transaction in e-commerce.

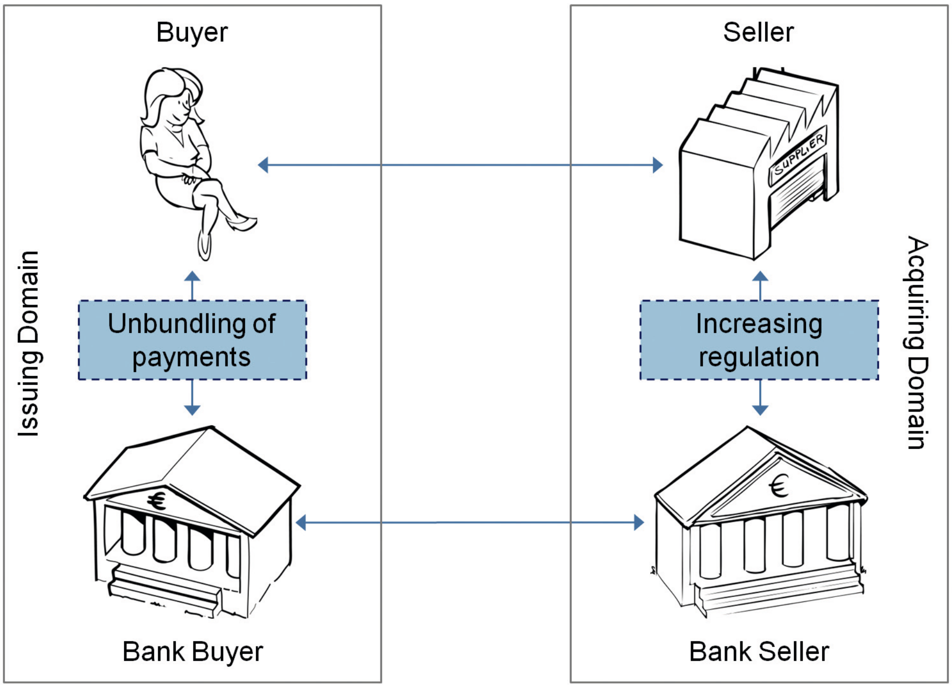


Figure 12: *Issuing and acquiring side under pressure*

Other market players are warming up

Identity services are a new market and to be successful will take a new combination of assets and capabilities. As indicated in the previous section, banks are well positioned as they have several of these assets and capabilities. Other industries however, have different starting points that also might provide them with a competitive edge. We will assess five of these industries with their respective strong suits, which are summarised in **Table 2** and positioned in **Figure 13**.

1. Identity service providers have been the early pioneers in this market and some of them have already been active in the market for digital identity services for more than a decade. Most of these services are created by a 'technology push', where entrepreneurs had a state-of-the-art technology, which they exploit in the market. RSA and Jumio are two frontiers in this market where RSA, focuses on Public Key Infrastructure and Jumio uses Optical Character Recognition to scan physical identity documents. These companies do not often have a direct relation with the customer, but sell to service providers who sell to consumers online.

2. Large merchants are solving the authentication issues for themselves, since they perceive a need to identify their own clients. They have created their own proprietary infrastructure and might bring these capabilities to the market. One of the leading examples is Amazon, who has pioneered the 'one click buy' already at the end of the 1990s. In effect this is a wallet storing payment, shopping and other personal credentials. This wallet (Amazon Payment Services) can be re-used with other merchants starting in Amazon's own ecosystem.

For the professional IT services market Amazon has created its own Identity and Access Management (IAM) which enables you to securely control access to Amazon Web Services (AWS) and resources for users.

3. Postal services are looking for new markets to replace their traditional ones by leveraging their physical networks. As discussed earlier in digital identity two aspects play a role: issuing of the credential and the authentication transaction. Since postal services have a direct relation with the customer, they can use their physical network to issue credentials to end-users. On the other hand, the online presence

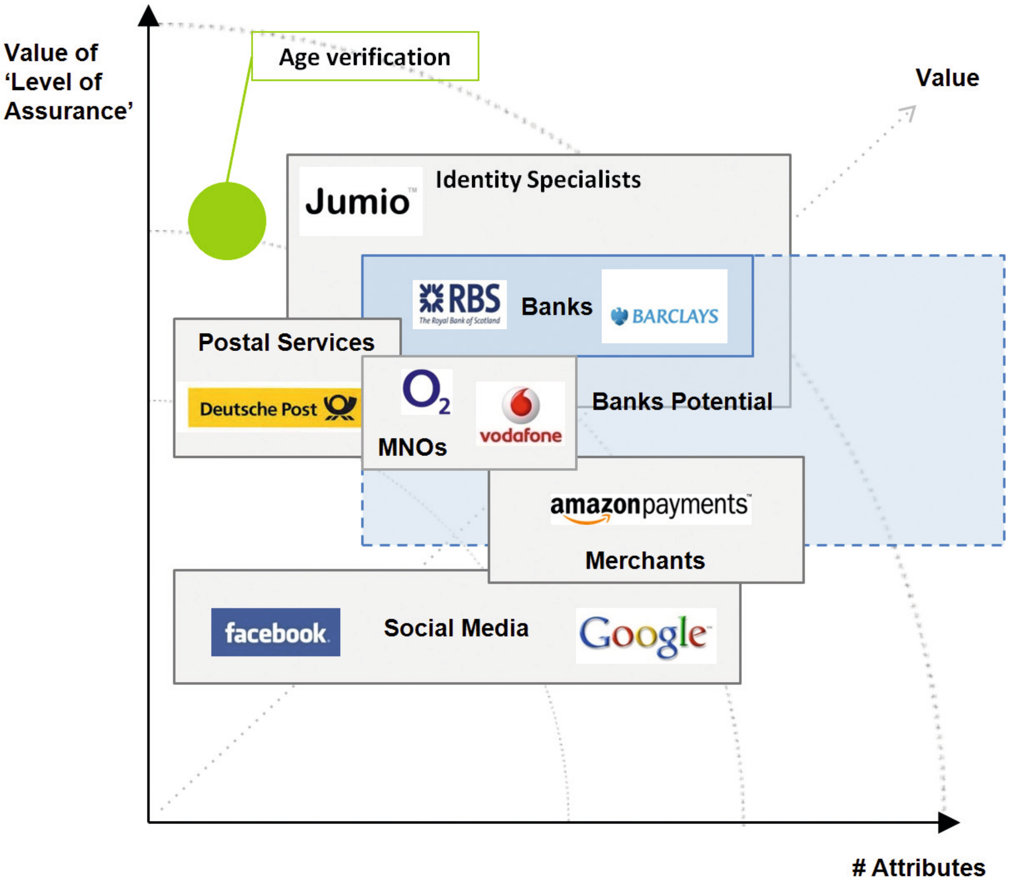


Figure 13: *The positioning of the various players by depth and breadth*

is limited given the nature of the business. In Europe there are many initiatives from postal services that are currently working to develop digital identity propositions. Postal organisations are eagerly exploring what role they can play in the e-commerce field, since the internet is a serious threat to their current business models. Leading examples are PostItaliane and PostIdent (Germany).

4. Social networks have proven to be able to scale quickly. They are extremely aware of the value, which lies in users' credentials. Besides the often-used credential infrastructure, companies like Facebook and Google exploit the customer data for their advertisement revenues. As part of the ´Application Programming Interface (API) economy´ these parties offer their authentication services to other web-players. On more and more websites one can login using one's social media credentials. Although the depth (level of assurance) is limited, many applications benefit, since not all applications require absolute certainty about the user. Recognising users is often just as important as to know who they are. The downside is the high level of concentration, which gives rise to serious concerns regarding privacy and competitiveness.

5. Mobile Network Operators (MNOs) or Telecom Providers are also players in the digital identity domain. They are the ones that have an exclusive control over the devices that will prove critical for the success of this new service domain: the mobile phone and in particular the SIM card. Companies like T-Mobile and Vodafone often issue mobile phone subscription in a (partly regulated) face-to-face setting, where the SIM card is directly linked towards an end-user. This SIM card and telephone can then be used as a secure authentication device. Orange has planned the launch of Mobile Connect, a secure SIM card based authentication solution for accessing digital services from mobile devices.

Service provider	Examples	Positive	Challenges
Identity service providers	*RSA* *Jumio*	*Technology focused* *B2B focused*	*No direct relation with the user*
Large merchants	*Amazon* *IKEA*	*Customer knowledge & brand* *Shopping experience*	*Expensive to create proprietary credential infrastructure*
Postal services	*PostIdent* *PostItaliane*	*Brand* *Leveraging physical network*	*Not much online experience*
Social networks	*Facebook* *Google*	*Customer data* *Many customer interaction moments*	*Low level credential infrastructure*
MNOs	*T-Mobile* *Vodafone*	*Customer ownership* *Access to a trusted device*	*Limited KYC requirements*

Table 2: *Different categories of potential competitors*

These companies all have capabilities very suitable for the digital identity market. All of these players have digital identity on their ´radar´ as a serious play for the near future. It will not be a matter of ´one winner´, but merely an ecosystem will have to emerge in which both users and relying parties can obtain services from a range or service providers, including banks.

5. THE TIME TO ACT IS NOW

As illustrated in **section 1**, the check-in is becoming more valuable than the check-out, in a world which is rapidly digitalising and 'doing business across a distance' becomes the new normal. This is clearly different compared to ten years ago, where we already did have the internet, but the mass adoption of digital services was still in an early stage. The mobile revolution is clearly accelerating this.

With the payment and the authentication becoming separated, the value and the user interaction will remain with the authentication, reducing the payment to a mere administrative operation. The market for digital identity services will eclipse the market for payments in the long run.

To seize the opportunity of digital identity, banks will have to get into action as well: other players certainly are already taking action. Multiple external factors have been discussed in this paper that demand immediate action (**Figure 14**).

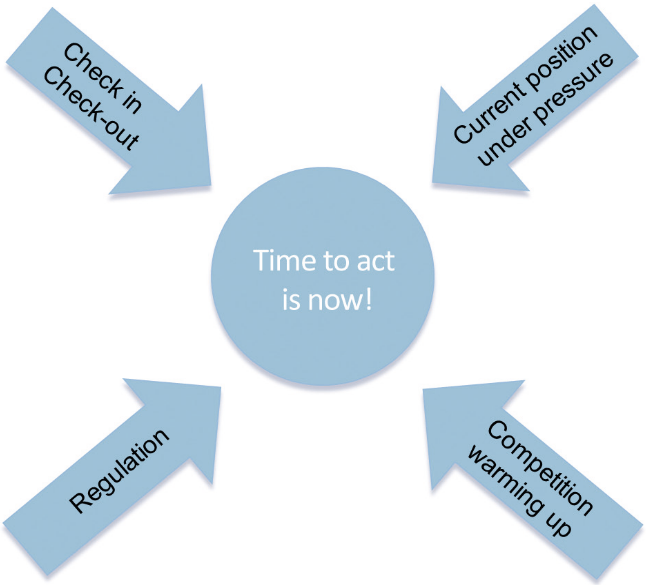


Figure 14: *Four external factors demand action*

1. Check-in rather than check-out

Authentication becomes more important than the payments, driving the mobile revolution. The unbundling of payments offers vast benefits to both the consumers and the merchant.

2. Regulation

General data protection regulation, PSD2, SecuRe Pay and AML4 are all about increasing certainty of users. Therefore, these drive the need for digital identity solution of significant level of assurance.

3. Current position of banks under pressure

The market for the current services of banks is becoming more and more open for other service providers: with wallets on the issuing side and the non-bank PSPs on the acquiring side.

4. Competition is warming up

Digital identity is a topic bordering multiple industries: players from other industries are exploring possibilities.

Banks have it all, but need to move fast by prioritising this important development. Digital identity is at the heart of customer centricity and works both ways: for the user a banking identity is relevant in all of his digital life while for the merchant the banking identity provides tangible process improvement, cost reductions and less revenue barriers (conversion).

Given its strong impact on retail and wholesale customers, digital identity concerns various silos in the bank including payment, operations, marketing, customer intelligence and security. The management needs to recognise and address this, when entering the digital identity business.

A distinct way of moving forward is leveraging the vast experience in operating in a four-corner model. The third generation of digital identity has taken up the same form as the payment market. Banks are well equipped to thrive in such a collaborative trust network, because banks know this way of working better than any other industry.

Banks possess the potential to become the most important player in the field of digital identity services due to their current qualities. High-end authentication tokens are not only proven to be safe, they are also trusted by consumers, businesses and governmental organisations. Furthermore, banks have a rich and trustworthy set of information about their customers, which is an asset of tremendous value to the relying party (**Figure 15**).

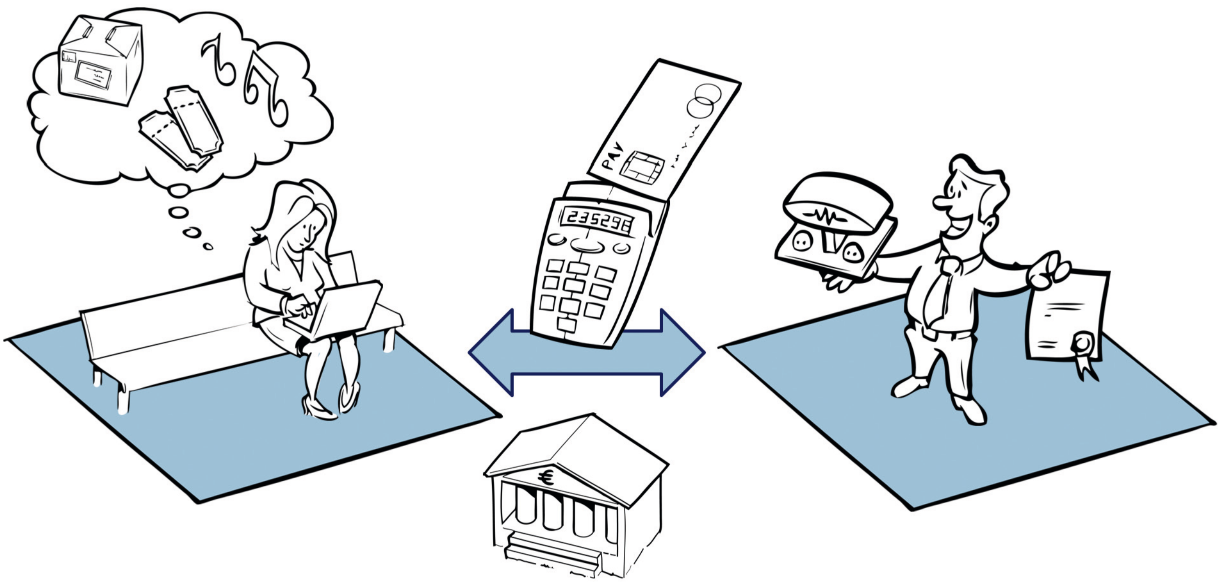


Figure 15: *The bank's services have the potential to enhance the experience of both the customer and the merchant*

The external conditions combined with the internal assets listed above, lead to the following three recommendations for banks who want to become a leading player in the digital identity market:

1. Unbundle the bank's valuable authentication services from payments;

2. Enable controlled availability of valuable information;

3. Set up and position digital identity services towards users and relying parties.

The first recommendation addresses that banks should decouple their authentication infrastructure from their current payment capabilities. Secondly, banks should enable customers to control their valuable information, which can be monetised to the market. Finally, these services should be offered as propositions in the market, which also requires market and new business development capabilities. Although banks are very well positioned, the time to act is now, since other market players are warming up.

ANNEX A – GLOSSARY OF TERMS

3D Secure

3D Secure (3DS) was developed by VISA to provide enhanced security for online credit and debit card transactions. 3DS is an XML-based protocol. VISA offered 3DS under the name of Verified by Visa. The protocol is also adopted by Master Card as MasterCard SecureCode, and American Express as American Express SafeKey.

API

An API (Application Programming Interface) defines how several software components should interact with each other and is most often used as a connection point to online services. The API defines the access to the software behind it. For example, a website can find the authentication services of a third party via the API provided to him. The API defines how to use the authentication services.

Attributes

Properties of an individual, also known as Personal Data.

Authentication

Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:

- *Something you know, such as a password or passphrase*
- *Something you have, such as a token device or smart card*
- *Something you are, such as a biometric features*

Authorisation

In the context of access control, authorisation is the granting of access or other rights to a user, program, or process. Authorisation defines what an individual or program can do after successful authentication.

CDD

Customer Due Diligence. The AML directives dictate parties executing financial transactions to apply Customer Due Diligence in some cases. A variety of methods can be used for the online verification of the identity of the customer to comply with the AML directive.

Digital Identity

A digital identity describes a subject (person, organisation or system) via its properties (attributes), in the online/mobile world, in a consistent and verifiable way.

Identification

Identification is the process whereby a user makes himself known (via one or more attributes to the relying party in order to establish a connection or to gain access to the system/website/web service etc.).

Level of Assurance

Level of Assurance for authentication services defines the reliability of the identifier. The level of assurance is defined as:

1) *the degree of certainty that the individual using the credential is in fact the individual to whom the credential was issued;*
2) *the level of confidence in the manner of establishing the identity of the individual to whom the credential was issued.*

Relying party

Party that wants to identify the user.

TPP

Definition according to the ECB:

“Service providers offering internet-based account information services and/or payment initiation services for payment accounts for which they are not the account servicing PSP are qualified as third-party service providers (TPs). The report focuses on the legal entity offering the account information services and/or payment initiation services which enters into an agreement with the account owner. Outsourcing agreements are considered to be under the outsourcer’s responsibility and are therefore not covered in this report. Both licensed PSPs and non-licensed service providers can offer services as a Third Party Provider.”

User

Individual or a person acting on behalf of a business or government who wants to identity himself towards a relying party.

ANNEX B – LIST OF ACRONYMS

(See Annex A for explanation)

3DS	*3D Secure*
AML4	*Fourth Anti-Money Laundering Directive*
API	*Application Programming Interface*
CDD	*Customer Due Diligence*
eIDAS	*Draft Regulation “on electronic identification and trusted services for electronic transactions in the internal market”*
IAM	*Identity and Access Management*
KYC	*Know Your Customer*
LOA	*Level of Assurance*
MNO	*Mobile Network Operator (Telecom Providers)*
PSD2	*Payments Services Directive 2*
PSP	*(Internet) Payment Service Provider*
SCT	*SEPA Credit Transfers*
SDD	*SEPA Direct Debits*
TPP	*Third Party Providers*

Contact details

For any additional information, please contact:

Daniel Szmukler
Director
d.szmukler@abe-eba.eu

Euro Banking Association (EBA)
40 rue de Courcelles
F - 75008 Paris
TVA (VAT) n°: FR 12337899694