EFFECTIVE DIGITAL IDENTITY AND THE NEED TO ORCHESTRATE

Whitepaper

THALES
Building a future we can all trust

JUNIPER RESEARCH

Contents

Top 3 Digital Identity Key Takeaways

1. Orchestration Critical to Success

Given the complexity of the digital identity space, ensuring that digital identity solutions can effectively orchestrate all the different verification methods and data sources is critical to success.

2. Government, Financial Services and Mobile Network Operators Just as Important

Digital identity implementation can have significant benefits in all these areas. There is a network effect: successful deployments in one area potentially benefit all the areas through improved data sources.

3. Digital Identity Can Transform Business Models

The pandemic has accelerated the transition to digital, meaning that there has been rapid change. Businesses are now moving from their reactive strategies to more proactive ones, and are realising that digital identity can be a major creator of value.

To find out more about effective digital identity orchestration, contact Thales:

www.thalesgroup.com/en/markets/digital-identity-and-security

THALES

JUNIPER RESEARCH

1. Drivers for Digital Identity Adoption

1.1 Introduction

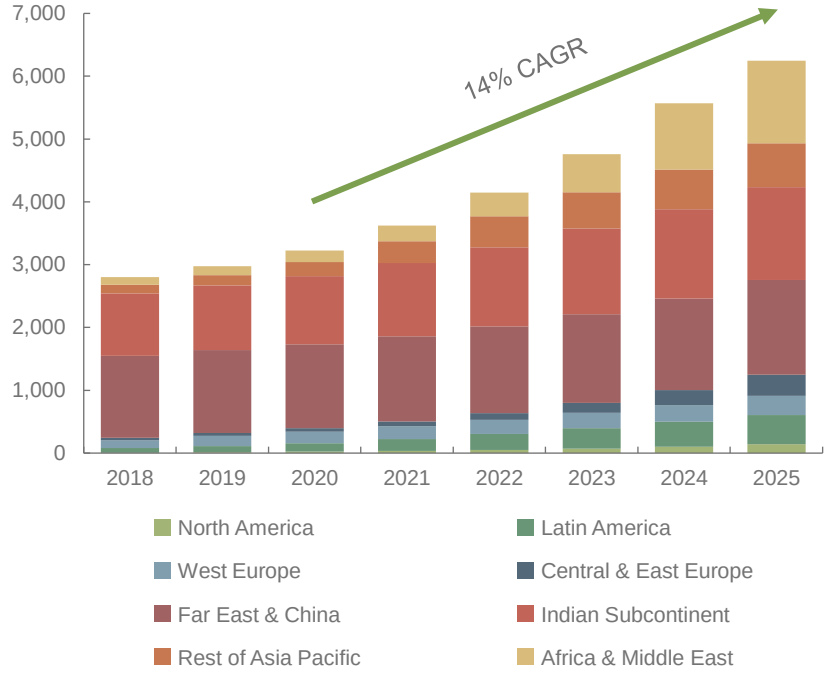
The last few years have seen much innovation around digital identity, to the point where it is crystallizing as a highly important market. A digital identity is a technological link between a real entity, such as a person, and its digital equivalent entities. It includes a collection of electronically captured and stored identity attributes, including biographic and biometric data.

People own many digital identities that consist of an email address and a password to access different online services. In this case, they are not verified and, therefore, not trusted. It is critical that user identity is verified and trusted when it comes to security sensitive services such as government, MNOs (Mobile Network Operators) and financial services

As Figure 1.1 demonstrates, the number of people with digital identity documents has been rising rapidly, and is expected to continue to do so.

Government use and issuing of digital identity has been of critical importance, and is a major driver of digital identity roll-outs. However, the digital identity market is also important in the banking & payments and mobile network operator spaces, reflecting the increasing widening of the market over time.

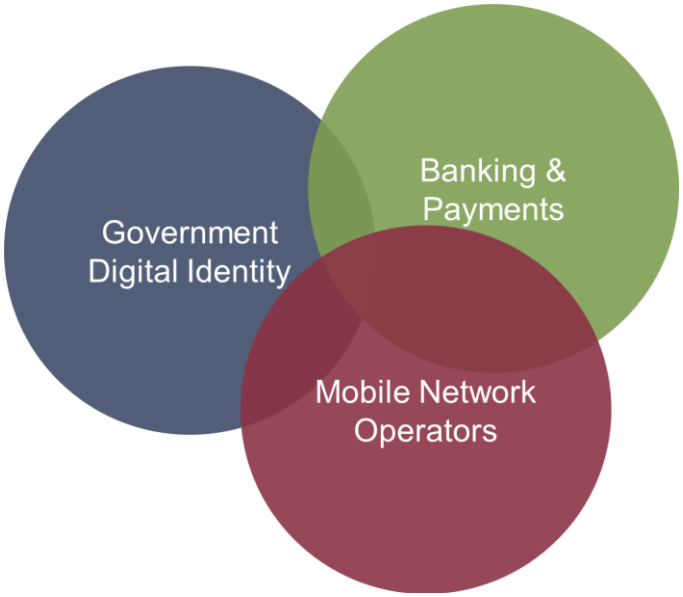
Figure 1.1: Number of People with Digital Identity Documents (m), Split by 8 Key Regions, 2020-2025



Source: Juniper Research

Ultimately, the best outcomes for users will be when government-issued digital identity becomes a contributor to a wider digital identity orchestration system, where onboarding in banking and mobile identity are added in to create an overall secure and accessible user experience.

Figure 1.2: Different Areas of Identity



Source: Juniper Research

This section will explore the important drivers for digital identity use, and how these are evolving over time, leading to a varied set of market requirements.

1.1.1 Onboarding During the Pandemic & Beyond

Onboarding has become highly topical during the pandemic, which is understandable, given the circumstances involved; however, this reflects a long-term acceleration of the digital uptake of the service.

i. The Context

The COVID-19 pandemic has forced changes in every corner of society. In Europe for example, measures taken to contain its spread during the peak of the virus have included lockdowns in Germany, France, Spain and the UK, which has been strengthened and relaxed at various points.

The popularity of digital services has also been on the rise for several years, meaning that the pandemic has accelerated the existing direction of travel, rather than creating a brand-new market dynamic.

ii. The Development of Onboarding

What is clear from these developments is that the COVID-19 pandemic has caused significant disruption to processes in a variety of areas, including banking & financial services, eCommerce, access to government services and others.

This has had the effect of bringing the need for digital access to services into sharp focus. Given the lack of digital access to many services, digital onboarding, which was beneficial but not necessarily essential, has become critically important to the new way of operating.

The difficultly here is in facilitating these transactions. By enabling accounts, such as bank accounts or mobile phone contracts, to be opened online, stakeholders need a new set of skills. Digital identity verification, being able to not only use digital credentials, but also to analyse their validity, is critical to this journey.

During the pandemic, many businesses have adapted processes to support digital onboarding, but these have not taken full advantage of the capabilities in the digital identity space.

The so-called 'selfie onboarding' has been a popular way to do so, but it has required manual review of photos and videos by staff, where automated solutions have not yet been deployed. Scanning and sending documents has also been widely used, but this is a highly manual process.

iii. The Future of Onboarding

The onboarding market will shift to a future which is much more seamless and much less reliant on manual input. By leveraging biometric capabilities and analytical systems, onboarding will move from its reactive position during the pandemic to a proactive one that makes the most of automation capabilities.

Orchestration is critically important to this future. Digital identity is made up of so many different elements, including the following:

- Government-issued digital and mobile identities.
- Mobile identity from MNOs, including identifiers such as phone numbers.
- Biometric information, including face, voice, fingerprint and other elements.
- Transaction history at various merchants (credit checks).
- Data from online presence (social media activity, etc).

Only by incorporating all these elements and more, businesses will build the optimal onboarding experience that reduces manual intervention, while increasing the quality of the user experience. Orchestrating these different areas requires a rich variety of capabilities and a strong identity network, making choosing the right digital identity technology vendor a highly important decision. It also requires a robust ability to handle data in a way that respects data protection regulations, as well as ensuring that only the authorised parties access information. We ultimately believe that authentication will move from selfie videos with government-issued identity documents, to authentication using biometrics and behavioural analytics, which will provide a better experience for both businesses and users, so technology vendors that support this will reap advantages in the market.

1.1.2 Digital Identity as Digital Transformation

To date, digital transformation has been widely discussed as a topic across a variety of industries, but it has not been the simplest of processes. Digital transformation broadly involves making the heart of business models digital, but this has different ramifications in different verticals:

- Digital Transformation in Banking: Perhaps most associated with banking, digital transformation has involved expanding services available via apps, while reducing branch footprints to increase efficiency. New digital features have included areas such as financial insights, chatbots or in-app onboarding.
- Shift to eGovernment: Digital transformation in government has meant better delivery of public services with a clear shift to digital access to public services, such as for tax, social security and registering for elections. To accompany this move and protect citizens from ID theft and online fraud, governments started to deploy digital identities, first taking the form of an eID card (in Estonia, Portugal, Belgium) and now

moving to a civic mobile ID for more convenience (MitID in Denmark, Chave Móvel Digital in Portugal, Alicem in France, UAE Mobile Pass, etc)

- Changes in Retail: In retail, digital transformation has meant offering an omnichannel experience that is personalised to users, as a reaction to the rise of eCommerce and the many struggles that traditional retailers have had.
- Changes for MNOs: In this sector, regulations are adding pressure to ensure that strong identity verification is in place for users for all channels (in store and online). Digital identity services are also being boosted in this area due to the rise of digital telecom operators, who are very focused around a digital brand, and want to offer mobile-centric experiences to their users. MNOs have also faced challenges with work-from-home conditions, in ensuring that networks are resilient enough to cope with changes in usage.

In all these cases, the pandemic has accelerated these digital transformation journeys, but it did not create them. There has been a longstanding transition to digital services in many areas, driven by the increasing dominance of the app and improvements in service delivery. However, ultimately, digital identity is a key capability of digital transformation.

Why is this? At a basic level, a digital identity is a digital representation of a person in the online world, and understanding this digital representation is critical to better serving the user. Digital transformation means building a business model that is data driven, and using digital identity is an important way to switch to this model. With a plethora of data sources currently available, building a digital representation which can be analysed to build a reliable picture of customer behaviours and can then inform business strategies, is more feasible than ever.

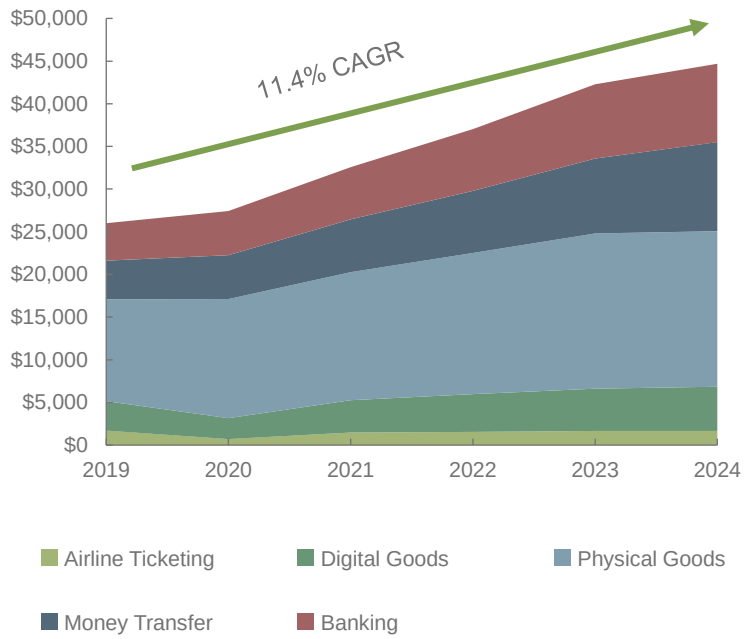
Armed with these accurate views, stakeholders can make their digital transformation journeys much more effective, by focusing on the areas which cause friction, and delivering the greatest value. We regard streamlined digital onboarding as a basic requirement for digital transformation, and its use for ongoing authentication and personalisation, backed by analytics capabilities, as the best way to reach digital transformation goals.

However, there are several challenges to overcome in achieving these goals. Data that can be used to build accurate digital identities is often siloed at businesses, with different departments using different systems that do not interact. The other challenge here is that processes are disconnected, with very little interaction between them. These challenges need resolving to get the best business outcomes. In banking, for example, updating core banking systems to use modular design is one way to build a system that can take advantage of digital identity. Stakeholders must review their digital transformation roadmaps and ensure that they have the capabilities necessary to take advantage of digital identity innovation.

1.1.3 Fraud in the Pandemic & Digital Identity's Role

The pandemic has had a dramatic effect on many areas, including the fraud area. Figure 2.3 shows the increase in fraud in 2020, and its expected rise for the coming years.

Figure 1.3: Total Transaction Value of eCommerce Fraud ($m), Split by Channel, 2019-2024



Source: Juniper Research

The increase in 2020 is understandable, given that the pandemic has seen growth in digital services use, with many users new to the channel. It has also seen many merchants who had previously only worked in the offline space launch digital services for the first time, as well as governments starting to make essential public services available online, meaning that the area is exposed to fraud. It additionally saw many COVID-19-focused phishing attempts.

The other side of this increase in fraud is the high level of data breaches which continue to occur across the world. High-profile data breaches in 2020 include a middleware security failure at Estée Lauder exposing 440 million internal records, a breach at EasyJet resulting in 9 million customer records being exposed, and a breach at app Freepik impacting 8.3 million users. The healthcare sector was also badly hit, with breach reports up 35.6% in the second half of 2020 compared to the first half, according to a CI Security report. Every data breach adds more compromised credentials that can be used to create synthetic identities for fuelling account takeover fraud, which has become difficult for stakeholders across all online verticals to manage.

Advancements in fraud require advancements in fraud detection and prevention, and digital identity is a major step in this direction. Leveraging digital identity verification is a key requirement here to combat these advances in fraud. Only by using a well-orchestrated system of digital identity verification methods, with different methods utilised for appropriate scenarios, will stakeholders be able to combat an increasing range of online payment, ID theft or social benefits fraud attempts.

1.1.4 The Increasing Role of Government Digital Identity

Digital identity as a concept has become vitally important to government use cases, with several trends driving the greater use of digital identity for eGovernment purposes. These trends include the following:

- Shift to eGovernment: Regardless of the pandemic, there has been an overall shift to eGovernment over time, with digital processes becoming ingrained due to the benefits that this can bring to both users and the government themselves. The Estonian model is often lauded as an example, and today, governments around the world are expanding their

eGovernment initiatives with the launch of a mobile ID for citizens. This requires a structured approach to identity, ensuring that access to services is seamless but also highly secure.

- eDocument Reading via NFC: NFC is built into the vast majority of smartphones sold today, making this a key enabling technology for digital identity use. Android smartphones have always had open NFC access, and in late 2019, iOS 13 opened up NFC for purposes outside of making payments on iPhones. This has enabled the reading of NFC-electronic identity documents by smartphones, and is being used in areas such as visa applications. Combined with biometric face recognition, this is such a user-friendly way to identify citizens remotely that governments that have already deployed contactless eDoc are using it to offer citizens a smooth remote onboarding to civic mobile identity. With so many NFC-equipped identity documents available, we anticipate that this will become widespread as a remote identification use case.

- Identity in New Use Cases: Governments moving to digital identity use means that use cases outside of traditional law enforcement and border control are now increasingly possible and being explored. By moving to identity documents with digital credentials and combining this with new, national biometric databases, these elements together can be leveraged to enable new sources of remote identification and authentication. Critically, this can then be leveraged to meet public and private sector needs as they arise.

- The Use of Wallet-style Digital Identities: Governments are starting to add a mobile companion to the official ID documents they issue, taking the form of a wallet-style digital identity. Digital ID wallets issued by public authorities can aggregate multiple digitalised and encrypted identities (mobile identity, driver license, digital travel credential, health credentials, proof of vaccination, etc) into a single app.

With the citizen having the ability to prove who they are online and authenticate themselves wherever they are, ease of access to eGovernment services is streamlined, and person-to-person identification in the physical world, with the possibility to run online checks versus government data sources, brings the trust needed to address new market needs and best support the sharing economy. This is a natural expansion that will allow for government-issued identity to become much more widely used in third-party processes.

It is clear to see that government-issued digital identity has a significant role to play going forward, but will require countries to develop adaptable platforms that can be leveraged by third parties easily to gain the most.

2. Effective Digital Identity Strategies

2.1 Key Capabilities for Digital Identity

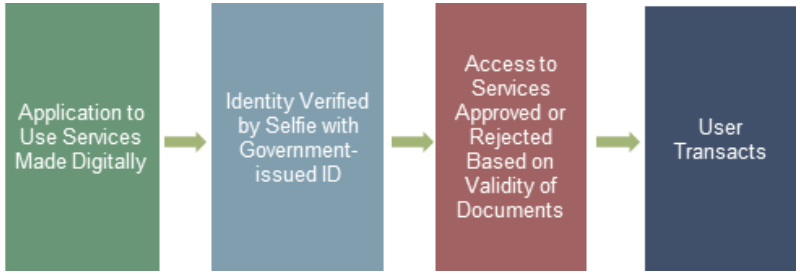
This section will analyse the most effective digital identity strategies and what areas key stakeholders must consider when designing their models.

2.1.1 Analysing the Customer Journey & Orchestration

One of the key topics surrounding the use of digital identity is how to integrate it within the overall customer journey, and to orchestrate the different verification methods to achieve the best outcomes.

Figure 2.1 shows how the traditional onboarding process, where a customer applies for access to certain services, is validated, and can then transact.

Figure 2.1: Traditional Digital Identify Verification Process



Source: Juniper Research

This process is purely transactional, in that an application starts the process, then the transaction is completed, with the access being granted or denied. There is no continuous element under this model.

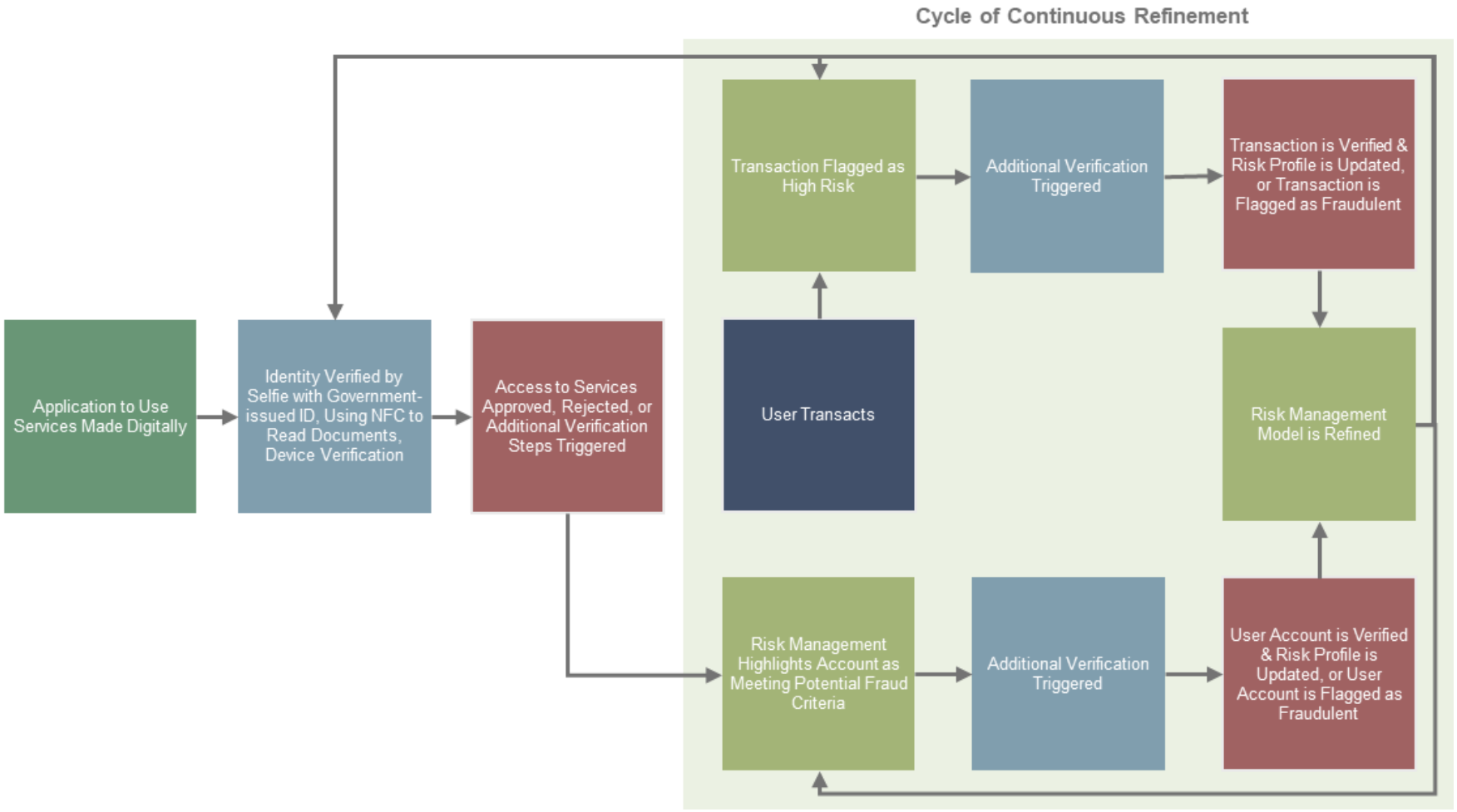
This model, however basic, has definitely been useful during the pandemic. By enabling previously in-person onboarding processes to go digital, it has enabled business to continue despite challenges brought by lockdowns or customers minimising their travel. It has also added a level of verification in terms of selfie onboarding, which will have helped to reduce fraud risks.

However, it is not the optimal way of approaching the introduction of digital identity at scale within organisations. While onboarding is an important use case, digital identity as a concept is not limited to this. Digital identity can be introduced throughout the customer lifecycle to ensure the best outcomes:

- Onboarding: This will always be a critical use case and needs to move to be more fully automated over time, increasing the benefits to businesses of deploying verification tools.
- High-risk Transactions: When transactions that are high risk are carried out, a digital identity verification system should trigger an additional authentication, to ensure that not only does the customer start as genuine, but also remains genuine.
- Risk Management: These capabilities should be backed up with risk management strategies which identify high-risk events and categorise these, setting the policy for checks throughout the system. This needs to be data driven based on fraud outcomes, in order to see the best results.

Figure 2.2 outlines our vision of the ideally orchestrated customer lifecycle supported by digital identity.

Figure 2.2: Digital Identity Orchestration Process and the Customer Lifecycle



Source: Juniper Research

By following this model, stakeholders can radically improve their fraud outcomes, by offering both a continuous identity verification, and a continuous improvement in terms of detection rates. By employing the most advanced verification methods possible, the system will create fewer problems for the user.

With a system this complex, however, orchestration will be completely critical. Knowing which verification method to use at which point will be highly challenging, and ensuring that all these solutions work together effectively requires a lot of coordination. These systems will need to be orchestrated by APIs, ensuring that implementation is not onerous.

2.1.2 Risk Management & Digital Identity

An extremely important element of any digital identity system, or indeed any security system, is ensuring that the right risk management strategies are in place to mitigate against the threat of breaches and fraud.

Effective risk management strategies need to deliver the following capabilities:

- Effective Reporting & Strong Communication: Risk management should be capable of reporting what is happening in the business, how systems are performing, and communicating these outcomes in an easy to understand manner.
- Continuous Improvement: Risk management systems must be able to deliver continuous improvements. By monitoring the overall system performance, iterative changes should be made to systems to allow constant refinement.
- Contingency Planning: All risk management solutions must be able to ensure resilience in the face of unexpected events, with redundancies in place and reporting advanced enough to show problems as they arise.

Within the digital identity space, these risk management strategies are highly important. Digital identity is a highly effective and valuable anti-fraud tool if it is implemented in the correct way, and ensuring that these pillars of risk management are met is critical to this. This requires several technological capabilities:

- Highly Configurable Dashboards: In order to understand risk performance, solutions need to offer dashboards that outline how the orchestration systems are working, what rate of approvals/declines the systems are generating and identify any particular fraud challenges. This allows decision makers to change criteria or rules as situations evolve.
- AI Analytics: Onboarding and verification processes generate an enormous amount of data, which can be difficult to distil into actionable insights. Systems need to leverage AI to cope with the scale of data. By building well-trained AI models, systems can provide insights into critical areas, such as surges in particular types of attempted fraud and geographic trends of transactions. This data can then be used to refine onboarding criteria or adjust the user experience.
- Human Intelligence: While AI analytics are an important area, human intelligence, and the role of manual reviewers should not be understated. It is highly important that any system continues to include human intelligence and that this is used to refine the operation of the whole system.

AI analytics, including the human intelligence aspect, is particularly critical to this market – if continuous insights can be created that are actionable, then ongoing improvement in strategies can be achieved. This ability to improve constantly is one of the major benefits of using an effectively orchestrated, analytics-driven digital identity platform.

2.2 The Importance of Different Identity Capabilities

Digital identity is an extremely broad ecosystem, which contains capabilities across several key areas, those of government, financial services and MNOs. This section will examine these areas in greater depth, including developments to date, the most important use cases and what capabilities are a priority.

2.2.1 Government

Government-issued identity is at the heart of any digital identity initiative. This is for a number of reasons. Firstly, because to be trusted, a mobile ID must be based on solid onboarding protocols with high identification assurance level, based on government-issued foundational identity. Secondly, government use cases are highly critical (access to essential government services such as unemployment benefits, social security, travel and visas, etc) and require strong identification. Thirdly, because government digital identity schemes can be a starting point for a wider digital identity transformation within society, with third parties using it as a validation source. In this section, we will analyse the most important areas in government digital identity and what capabilities are particularly important.

i. Passports/Driving Licences & Access to Wider Services

At its most basic level, providing access to a robust digital identity system requires digital identity documents to be issued to start with. Ensuring that identity documents are in a standardised format makes them machine readable. Recent efforts have focused on upgrading identity documents with biometric data and digital features such as NFC, to increase their usability. Passports are a perfect example as they feature NFC chips, which store digital copies of the identity credentials of the party involved. This unlocks the ability for devices to read this data and validate against it. It also unlocks the potential for users to scan this data with their smartphone, for onboarding processes or to access government systems. In the US, states' motor and vehicle departments have started bringing a mobile companion app to driver licence cards to enable a wider range of online identity-related services (mobile identification, ID attribute sharing, authentication).

Ultimately, how they are integrated into a wider system is just as important as the documents themselves. If a government creates a database against which identity details can be validated, that opens up a widespread use of credentials both for access to government services and identity verification for third-party services. These third-party services can include banking and payments vendors who need to perform KYC checks, or it could even refer to healthcare providers, who need to validate identity to ensure access rights to healthcare. The potential use cases unlocked by this approach are numerous.

The important challenges, which identity vendors can assist with, is how governments create systems that allow access and validation, but do not share too much data with third parties and create additional risks. This will require governments to deploy systems that can validate with yes/no

answers against databases, rather than sharing the raw data for third parties to compare.

In emerging markets, there has been a mobile-first trend in digital identity, with many government identity schemes having digital features as a starting point. However, in developed markets, where systems have already developed along different lines, there will need to be initiatives to restructure existing processes to better achieve the potential of digital identity.

ii. Border & Visa Management

Another important use of identity has been identifying individuals and establishing their right to travel, to stay in and work in countries. The transition to digital identities can make this process easier to handle.

By associating identity documents with digital identity systems, governments can quickly establish what rights the individual has, which can make border operations simpler.

Visa applications can also be greatly simplified using digital identity capabilities. Document reading via NFC is a key capability here. Governments can deploy apps that read NFC ePassport documents to simplify visa applications and move the whole operation to a completely remote footing. This was partially seen with the app deployed by the UK government to enable EU citizens to apply for permanent residency prior to Brexit, but this will see more widespread usage over time, with advanced functionalities once the ICAO (International Civil Aviation Organisation) releases the full specification of the mobile Digital Travel Credential. This will enable officially issued digital identity to become part of the mobile ecosystem, unlocking new use cases.

iii. Biometrics for Government

Biometrics are a clear part of the digital identity ecosystem, primarily being used to securely verify identity credentials, they are critical for law enforcement and other areas. Governments also tend to embark biometrics in their mobile ID schemes to provide citizens with smooth and secure access to digital services. Biometric verification as a layer is also essential to ensure that government digital identity can be a platform for further identity innovation.

iv. Conclusion

Government use cases are critically important to the use of digital identity, and they are a basis to deploying digital identity solutions and eServices throughout society. Choosing the correct vendor to support government mobile and digital identity roll-outs, and realise these benefits is highly important, and will require a vendor with a wide range of capabilities.

2.2.2 Financial Services

The concept of digital identity has been linked to financial services for some time, for a number of reasons. As a highly regulated industry, financial services have a number of requirements that do not exist to the same extent as in other industries. These are the following:

- KYC (Know Your Customer): This requirement is for financial institutions to verify that the customer is who they say they are, and that transactions are genuine. KYC checks are a requirement in nearly all banking regulations, for example.
- EDD (Enhanced Due Diligence): This is a requirement where the customer and product combination are considered to represent a greater

risk, such as the risk of fraud or money laundering. Enhanced measures can include additional verification steps, identifying sources of income or adverse media checks. EDD is a requirement of the 5MLD (Fifth Money Laundering Directive).

- AML (Anti-money Laundering): This is an obligation to ascertain the source of funds and verify identity, in order to ensure that funds are not being laundered for criminal activity or to fund terrorism. The US PATRIOT Act and the EU's 5MLD both contain this as a requirement, and it is a basic requirement of most regulatory frameworks.
- Anti-fraud: Various regulations require financial institutions to take steps to minimise fraud in transactions, but this is as much a reputational risk as a regulatory one.

These requirements together mean that the concept of identity in financial services is of great importance. Robust digital identity systems can play a large role in meeting all these requirements. As the digital identity market evolves, we are seeing an ever-greater alignment between payment security, anti-fraud and digital identity systems.

i. Account Onboarding

The first element that will be critical to financial services delivery is onboarding. Onboarding is important, as identity must be verified at the start of the process. If fraud can be eliminated at the initial stage, then it is much easier to protect the overall environment.

Onboarding technologies have evolved rapidly in recent years, with selfie onboarding becoming popular. Digital-only banks were the first to adopt such solutions, looking to offer easy access to services that are not supported by extensive branch networks. Due to the pandemic, these solutions have been adopted by many traditional banks as well.

However, there is progress to be made in this area. Digital onboarding needs to be highly robust in order to work effectively. This requires a few key capabilities:

- Robust Biometric Verification: In order to secure the process, robust biometrics are needed. This can include using fingerprints or other biometric types to verify identity, or using features such as liveness detection to ensure that selfie onboarding is accurate.
- Additional Verification Services: While securing the onboarding process, biometrics by itself is not sufficient. Models around verification must include a scoring system, leveraging reputational scores and fraud prevention scoring. This can help to ensure that biometrics are not being spoofed.
- Clear Business Rules around Onboarding: Each financial services business offering a digital onboarding service must have very clear rules around what constitutes a pass, a fail, or what additional verification checks are triggered at each stage. This will allow the system to be transparent and will offer a proper user experience.
- Regulatory Compliance: All systems must be fully transparent for regulatory purposes, in terms of being able to explain why a decision has been made, given that it is a highly regulated industry where decisions may need to be explained at any time.

If all these requirements can be satisfied, then financial services technology vendors can create a robust onboarding process that provides security, but also continues to provide a good user experience.

ii. Continuous Verification

While verification at the onboarding stage is important, verification must not cease there. Continuous verification is a critical requirement for ensuring that digital identity is used to verify at key stages in the user journey. Additional verification should be triggered for high-risk transactions, or when an unusual behaviour is detected, meaning that ongoing monitoring and identity integration with fraud tools is critically important.

iii. Conclusion

It is clear when examining the financial services market that it is a priority area for digital identity use. If identity can be verified and leveraged in a secure way, then financial services players will be able to offer a superior user experience. Picking the right vendor with the correct capabilities and the ability to orchestrate these abilities will be critical.

2.2.3 Mobile Network Operators

When examining the digital identity landscape, it is clear that telecommunications companies, primarily MNOs, have an important role to play in the area. Key capabilities are examined below.

i. Account Onboarding & Ongoing Verification

In a similar way to financial services, MNOs have had to adapt to digital onboarding. Many MNOs have had to close shops during lockdowns, which has accelerated the existing trend of digital transformation, placing greater emphasis on the challenge of adopting purely digital onboarding. MNOs have suffered heavily with fraud around shipments of devices and access to services, and they are highly susceptible to identity fraud. As such, MNOs need to employ robust onboarding procedures to ensure that fraud is minimal.

Getting the identity verification challenge right is also particularly important, given that MNOs can act as guarantors of digital identity throughout the digital ecosystem under the identity networks model, as a source of trusted identity. If MNOs want to pursue their role in that model, they need to ensure their own processes are extremely robust.

ii. Supporting Subscriber Identity

The concept of subscriber identity is not new, but integrating it within processes has been an ongoing challenge in multiple areas. The standard from the GSMA is Mobile Connect, but there have been multiple services from vendors such as Thales which offer capabilities beyond this. Mobile identity introduction by MNOs allows them to become a trusted digital identity provider to the wider market, as part of a wider consortium of identity verification partners.

Figure 2.3: Key Mobile Network Operators Using Mobile Connect

Source: Juniper Research

By leveraging details, such as the mobile number attached to a particular subscriber, MNOs can act as an additional source of identity data. This can then be used to verify access to wider ecosystems, such as government or financial services.

This approach is even more important in markets where banking penetration is lower than mobile penetration, meaning that in many cases, mobile is the best way to identify and verify a user (phone number).

iii. Identity & IoT

The concept of identity is also important in the IoT area, referring to the identity and access rights of devices, rather than people. The identity of connected objects must be trusted, with the object and cloud elements clearly identified. This is two-way – objects need to be communicating with legitimate cloud services, and cloud services need to be communicating with legitimate objects. In order to support this, MNOs and other connectivity players must ensure that they have secure systems in place to ensure that their IoT platforms are protected by design.

iv. Conclusion

MNOs clearly have an important role to play, both in creating trusted identity to secure their own operations, as well as operating as a trusted identity broker in the wider digital identity verification market. As such, MNOs must create effective digital transformation strategies that ensure that they are making the most of digital identity throughout their operations.

This is particularly true in the cellular IoT market. MNOs are well positioned to address this market. They manage billions of SIMs that are deployed globally, meaning they have the necessary experience and set of skills to manage this. Combined with this, they are already experienced in identity, having to verify subscriber identity at enrolment. This means that MNOs can manage identity services for IoT devices as well, which combined with their global reach, will be important in securing the IoT ecosystem.

2.2.4 Key Capabilities - Conclusion

Throughout this section, we have examined the capabilities required across our three important digital identity use cases, in order to support the best introduction and use of digital identity at scale.

What can be seen here is that digital identity is universal; it is just as critical to governments as it is to banks and to MNOs. The other element here is that when the overall adoption and technology use is better within the identity space and numerous players form effective identity networks, this has a network effect on how useful digital identity is, as the ecosystem grows and verification methods multiply. When trusted digital identity is shared, it must be recognised by all parties in the ecosystem to be truly effective.

We ultimately believe that the concept of identity networks is critical to the future of digital identity – the system as a whole is better when more participants are submitting more data. The performance in anti-fraud then rises significantly as a result.

The difficulty is in orchestrating these different scenarios, verification methods and data sources. Vendors in the digital identity space must be able to arbitrate these complications, make implementations and usage simple for the business and ultimately, the end user, and ensuring that it is improved, rather than degraded by digital identity use, will be critical to ensuring success.

3. Thales – Company Profile & Digital Identity Capabilities

3.1 Thales Profile

THALES
Building a future we can all trust

i. Corporate

Thales is a French multinational designer, builder, and supplier of technology to the aerospace, defence, transportation, and digital identity & security sectors. Thales Digital Identity Security sells its digital identity solutions in over 180 countries. Over 30,000 companies have Thales digital identity solutions deployed for their employees, and they are involved in over 200 government programmes.

Table 3.1: Thales DIS Financial Snapshot, (€m), 2019-2020 (FYE 31st December) – Digital Identity and Security Segment Only

	2019	2020
Order intake (€m)	€3,315	€3,023
Sales (€m)	€3,202	€2,992
EBIT	€274	€324
In % of sales	8.6%	10.8%

In April 2019, Thales acquired Gemalto for €4.8 billion ($5.4 billion). The unification of the specialisms of both Thales and Gemalto created a new group that offers a wide portfolio of digital identity and security solutions. These solutions utilise technologies such as biometrics, data protection and cybersecurity. Research and development are a core capability of the new Group, which employs 3,000 researchers and 28,000 engineers solely working in these two areas. The Group has also been allocated a budget of around €1 billion ($1.14 billion) per year to advance innovation in key areas such as IoT, Big Data, AI and cybersecurity.

Thales currently holds a portfolio of over 23,000 patents. In 2019, Thales was voted one of the '100 Global Innovators' for the most innovative companies in the world. Patrice Caine is the Chairman & CEO of Thales; Philippe Keryer is the Executive Vice-President, Strategy, Research and Technology; Philippe Vallée is Executive Vice-President, Digital Identity and Security.

ii. Geographic Spread

Thales is headquartered in Paris, Île-de-France, France. The company employs 83,000 people in 68 countries. The company generated sales of €17 billion in 2020.

iii. Key Clients & Strategic Partnerships

Thales' identity solutions are primarily used in the public sector, as well as in banking and payments, enterprise and cybersecurity.

iv. High-level View of Offerings

Thales presents their offering as covering the entire lifecycle of identity, from its creation and management, down to its revocation, through a wide and rich range of products and solutions referred to as 'techno-bricks.' Thales' solutions cover face-to-face, as well as remote identity verification, document verification, online authentication, digital signature, selective ID attribute sharing, biometrics, mobile ID and digital ID wallets, digital identity services management platform, broker orchestration (hubs), and all the pieces that enable the ecosystem to generate trusted ID Networks.

One example of a solution that crosses industry borders is the Thales remote ID Verification solution, which enables government bodies, banks, mobile operators and any type of public or private entity to check a person is who they claim to be when registering to new online service providers (eg opening a bank account with KYC processes, purchasing a new SIM card, or registering to new online public services).

a) Digital ID Wallet

The Thales Digital ID wallet is a next-generation mobile ID solution which can be used for face-to-face with mobile-to-mobile identification, as well as for online authentication, to address the latest market needs for both in-person and remote identification. It provides the necessary portability and the ability to securely store ID credentials and aggregate all the user's digitalised and encrypted identity documents in one single secure ID vault. This wallet is centralised but the release of the data is under user control, with the user able to share only what is necessary to verify a transaction. The details are also ring-fenced between issuers, with the issuer of a digital driving licence unable to access a digital health card in the same wallet, for example. The wallet provides self-sovereign identity without the need for a back-end blockchain.

The phone uses a secure mobile-to-mobile communication protocol to confirm age, prove identity, residency, entitlement to drive, right to vote, etc. It can also be used for real-time government-citizen communications through notifications received in the wallet.

Figure 3.2: Thales Digital ID

Source: Thales

b) KYC and Other Verifications

The Thales IdCloud platform offers identity verification and genuine user confirmation during the entire client life cycle. KYC checks include document verification, face recognition, and AML (Anti-money Laundering) checks. The use of adaptive onboarding can ensure that KYC is only performed when anti-fraud checks have passed to help reduce fraud and cost.

c) ID Network

In 2020, Thales released their ID Network. The ID Network creates new networks and allows existing networks to strengthen their existing position in their ecosystem.

The ID Network acts as a broker of identity attributes, user consent and user authentication. Securely connecting information supply of, and demand for, identity credentials between identity providers and relying parties. It leverages familiar and smooth, strong customer authentication processes from banks to retrieve data from a variety of participating data sources, such as government databases, MNOs and credit bureaus.

By calling on its IdCloud and orchestration functionality, Thales can deliver wide-ranging identity ecosystems to provide seamless and assured retail consumer services. Systems built on the backbone of orchestration and identity verification can be applied across industry sectors and consumer use cases.

d) Thales Trusted Digital ID

Thales' Trusted Digital Identity Platform is a one-stop services platform to digitalise mobile subscriber enrolment and authentication in store and online, and protects businesses and customers from subscription fraud.

It orchestrates everything needed by telecom operators to digitalise customer enrolment, including the capture, verification, and authentication of customer credentials and biometrics.

Drawing on Thales' in-depth experience and expertise in these fields, the platform complies with government regulations such as KYC, AML, registration for prepaid, and eIDAS. The system provides seamless & secure biometric authentication for service access, as well as integrating easily with eSIM Management platforms for a full trusted digital subscription journey.

As a result, telecom operators, OEMs, and other enterprises can accelerate their digitalisation strategies, launch new services, fight fraud, and meet regulations.