Digital Identity:

Relying Party Views on Adoption Readiness

Daon®

OIX
OPEN IDENTITY
EXCHANGE

Digital Identity:
Relying Party Views on Adoption Readiness

TABLE OF CONTENTS

Digital Identity:
Relying Party Views on Adoption Readiness

photo credit – Richard Thompson

INTRODUCTION

This report is based on qualitative research exploring the depth of understanding of digital identity within solution buyers in relying parties. The following insights are built from hour-long interviews about what people think of digital identity, its value, and its prospective adoption.

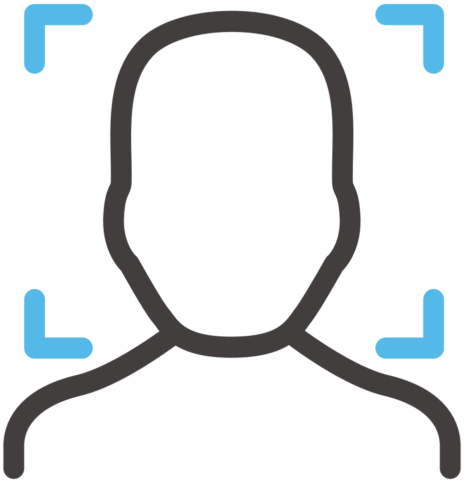
The research gathered responses from a mix of respondents in seven distinct business sectors. Each respondent has a different level of exposure to digital identity.

KEY FINDINGS

The following findings offer the opportunity for industry, government, and regulators to be informed, to evaluate, and to respond accordingly.

- **Value** – Many relying parties see the value of digital identity through cost saving and efficiencies, improved conversion, better throughput, improved customer engagement, and overall increase in user satisfaction.
- **Education** – There is still work to be done to educate organisations about digital identity solutions and their inherent benefits. 'What's in it for me?' remains an outstanding question, prompting the need for more real-life examples of digital identity use cases and benefits/values. This is especially true when it comes to educating stakeholders about reusable identity.
- **Purpose** – Relying parties are motivated by solutions that solve problems. Digital identity is a component of making digital journeys more effective, convenient, and reliable for customers and businesses. The identity industry must improve its communications surrounding how data enablement and customer experience work in parallel when solving problems.
- **Disconnected** – Eligibility data enablement must also power joined-up digital experience and digital transformation. The value of digital identity also lies in the surrounding attribute data and how it can be used to automate decisions in a way that creates more consistent, efficient outcomes, improves defences, and creates economic value (e.g., share codes).

- **Technobabble** - Alongside education, use of plain language is critical. To increase the depth of understanding of digital identity, clear, concise, and non-technical language that leaves relying parties feeling certain and engaged, rather than confused and disengaged, is needed. The whole ecosystem has to become more explainable and relevant.
- **Customised** - Messaging surrounding digital identity cannot be one-size-fits-all. This includes everything from the personas being engaged to the sectors and use cases and the 'jobs to be done.'
- **Inclusion** - Relying parties want a focus on inclusion. A one-size-fits-all approach to digital identity is perceived as a dangerous concept. Availability of public data is needed to unlock market potential, drive inclusion, and create relevant experiences that ensure ongoing engagement.
- **Accessibility** - Relying parties consider digital poverty as a concern. They want to ensure that benefits reach those that neither have the tools nor the profiles to complete digital actions. They want to ensure that society has the tooling to access services whatever their situation. (It's simpler for their processes, ESG compliance, and cultural goals).
- **Security** - Relying parties are very aware of the need for security and privacy. They are looking for cross-industry thinking and cooperation, especially as propositions are developed alongside changing regulations and user expectations.
- **Alignment** - Relying parties mention the need for certainty and for a clear understanding and alignment of digital identity standards and regulation. There is a feeling of disjointed standards and of a lack of confidence in what digital identity achieves. For some regulated respondents, reliance on other parties' identity checks is considered a hard red line. This highlights the need for regulator guidance and 'approval.'
- **Divergence** - Interoperability needs to be as expansive as possible, covering not only global and sectoral identity trust, but also covering payment, privacy, ethics, vulnerability, and wider framework thinking. This is to ensure that gaps between principles and practices do not widen.
- **Regulator Guidance** - Relying parties want regulator, industry body, and government 'permission.' There is a feeling that regulatory approval is needed to accept and trust identity innovations. More work is required to drive trust through messaging, collaboration, and 'approval.'
- **Suitability** - Relying parties get little value out of the current UK DVS register (aka, how to find an identity provider and easily see their value). They feel it's confusing, poorly laid out, and lacking relevancy. They could not determine which provider did what or which would provide the best outcomes for them; relying parties felt there was a lack of independent feedback and validation on the execution of a provider's service(s).
- **Standardization** - Relying parties are looking for assessment and contracting efficiencies as a way of standardising policies, terms, and solution suitability assessments to simplify the contracting, solution diligence, and organisational assurance processes.
- **Proof of Concept** - Relying parties are waiting for a tangible working framework, an ecosystem, and explainable, specific use case initiatives. Perception is still of theory, not of reality.
- **Sense of Urgency** - There is a feeling of stagnation and lack of pace. Many respondents talked of theory and not of a pressing need to change systems to react to any reusable identity opportunity, to market demand, or to regulation. There was nothing to trigger a sense of urgency. Certified use cases are piecemeal; interoperability, a concern and value, is yet to be persuasive. It feels like a hiatus on the path to value-add reusable identity.



DIFFERENCES IN TAXONOMY AND DEFINITION

All the participants described digital identity differently, using various terms in their responses.

Significant differences in language existed between technicians and operational stakeholders within the relying parties.

- Lack of language alignment showcases that education and common taxonomy are critical to storytelling and explainer documentation.
- The more technical the language and nuanced the delivery of messages, the greater the risk that operational users and key participants may get lost and disconnect.

DEFINITIONS OF DIGITAL IDENTITY

(Definitions are phrased/grouped for simplicity)

Many of the respondents had a very clear definition of what they felt digital identity was. However, in many cases, they went on to use multiple, overlapping descriptions based on digital use cases and need.

Some were far more technically aware and able to describe digital identity in multiple ways. Others simply articulated how they were able to move from trusting 'paper' documents in person to trusting 'paper' documents online.

Definitions of digital identity:

1. A way of checking someone's identity remotely (usually using IDV technologies that enable digital checking of documentation)
2. A single URN identifier that unifies all digital information held across a disparate data landscape.
3. A portable authentication system for somebody to expediently confirm they are who they claim to be.
4. A reusable identity where all the data to evidence the person is held centrally or where all the data is controlled by the individual and is potentially distributed.
5. The ability for organisations to be able to utilise a singular identity, meeting AML/KYC regulations, allowing them to onboard across financial services.
6. An official identity <token> backed by a 'qualifying authority' in a digital format.
7. A digital wallet, rather than hard copy identity documents, to prove who you are.
8. Receiving verified attributes relating to an individual's identity that would be digitally signed in some way and from a party who you know could attest to its authenticity.
9. A zero-knowledge token that simply passes a confirmation of trust from one party to another.
10. The digital persona and collection of data that represents you online.
11. The identifiers used by a company to allow you access and manage your online services.

Education and value storytelling are important as proponents of digital identity build messages. Simple, non-technical language and explainers are critical, alongside real-world use case examples that educate, inform, and standardise terminology.

MIX OF ATTITUDES TOWARDS VALUE AND URGENCY

To combat bias, invitees with a different mix of digital identity knowledge were encouraged to give their views. Invites were issued through the OIX (the relying party working group membership), through governing and industry bodies, and from direct 'cold call' approaches.

Responses to the research invites were, therefore, mixed. As expected, those with a higher degree of awareness and interest in digital identity participated, whilst those without the same understanding or interest were harder to engage.

NON-RESPONDENTS

The insight from non-respondents provides a set of relying party engagement signals in its own right. The reasons for not participating and the language used by non-respondents is interesting to try and interpret. Paraphrasing the decline feedback, the most consistent themes of non-responder declines were:

- 'Non-participation due to organisational policies.'
- 'Complexity getting through internal compliance sign-off.'
- 'Not having the time.'
- 'Not being interested.'
- 'Did not feel they knew enough.'

This may point to several potential non-engagement factors which include lack of awareness (of both OIX and the subject), a lack of interest or pressing need, and, maybe, concerns about revealing too much.

One example was of a large, cross-border organisation (which is digitally enabled and holds an obligation to ensure robust identity assurance) declining because the organisation 'had not and was not planning on adopting digital ID.'

This suggests pockets of low relying party engagement where better awareness and a need to engage exist. Undoubtedly, the unengaged need to understand the potential benefits available to their organisation: 'What's in it for me?'

Relevance and value are critical to engagement. Without a market driver (mandated) or a clear statement of benefits over incumbent solutions, it's hard to win over the priorities of non-participants.

HOME RENTAL | LETTINGS

Digitalising compliance in lettings

- Moving landlord/tenant KYC from in-person to remote.
- Getting properties on the market faster, removing admin delays, and demonstrating auditable compliance.
- Improving security and control by automating away from points of manual risk.
- Combating fraud.
- Ensuring competitive process advantage.
- Dual processes, covering both landlords and tenants.

On the move to digital:

- 'On lettings, we risk assess a number of events, money laundering, right to rent checks, even right to work and so on.'
- 'Digital identification is speeding up our onboarding and diligence processes and that has a lot of knock-on effects, meaning we can get the properties to the market quickly.'
- 'When it comes to security checks, the unscrupulous will pinpoint the agents who they perceive to be easier to get through. The fraudsters will go to those agents who aren't embracing it.'
- 'The agents who don't embrace it will be left behind and will then probably lose out because everybody wants to do things for speed. Once everybody becomes aware of it, it's an education piece.'
- 'We get quite nice feedback from our estate agents who go out to value properties, whether that's for both sales and for lettings. The reception from clients when they see that we are making an effort to be technologically forward-thinking is a lot more positive than it would be if we were to be going entirely down a very manual, archaic route. There have been occasions where that has helped us win business, which is a good thing.'
- 'If you are just able to go out and rely on digital identity providers (IDPs) to provide a digital sort of verification of a customer for you, but without a set of standards or a framework, or without them being, let's say, government-approved or approved by a body which is government-approved, then that carries a high risk of inaccuracy and that is not necessarily an advantage for the business.'

On the idea of reusable identity:

- 'I would liken it in the same way as we used to just use cash. Now a lot of people use digital wallets rather than just using hard copy documents to prove who you are.'
- 'It's an ongoing transaction. From an AML standpoint we have an obligation to continue to monitor the clients that we work with.'
- 'Updating checks in ongoing monitoring is something that I think could be mitigated by a more universally accepted, government-run digital ID system. For example, ensuring that sanctions checks were streamlined. If it is the government issuing those sanctions through the OFSI, theoretically, a government-run digital ID system would tie into that automatically.'
- 'We won't rely on other people's checks at the moment.'

- 'I think the digital passport, the reusable one, I think it needs to get to a stage where the government say that it is acceptable to use it. If HMRC say it's okay to do it, we will do it. If they don't, then we won't.'
- 'The only way that you can get anything with government is by lobbying them and getting them on board with it.'
- 'We've got 2 industry bodies, RICS and Property Mark. If they were to say that this is acceptable to use, then I think that then we would look at it seriously.'
- 'It would be an absolute dream to be able to have complete digital identity checks for somebody living in Dubai or Singapore or somewhere like that you know <anywhere else>.'

Respondents considered processes as antiquated. The move to digital identity was seen as an accelerant to better controls, costs, and UX. Reusable identity, although seen as beneficial, comes with concerns: respondents need to know that regulators and governing bodies approved adopted solutions.

RECRUITMENT | HEALTHCARE, SOCIAL CARE, AGENCY

Digitalising recruitment

Moving candidate ID checks from in-person to remote:

- Combating significant health & social care resource gaps.
- Reducing the risk of contract workforce moving to other sectors and job types or being lost to the employment pool.
- Placing candidates in employment faster and preventing candidate deselection because of admin/onboarding process delays.
- Automating processes; improving experience with remote, anytime processing to replace face-to-face interviews, reducing costs for all.
- Checking supporting claims, e.g. Right to Work, in parallel. Dual processes.

On the move to digital:

- 'From the user perspective, we can proceed with their checks a lot more conveniently for them. We were doing face to face appointments, often meaning that we had to wait days if not weeks for somebody to come in.'
- 'It was inconvenient for them, including travel to us. They now can't believe they don't need to take that day off. This is a big game changer for our applicants. When we do our satisfaction surveys at the end, this comes up quite often.'
- 'In terms of business benefits, we can do things faster because we've sped up the process. We've shifted the action to the applicant. Face to face appointments used to take us half an hour. The current process is 7 minutes. So, for 20,000 applicants, that's a huge saving (667 days saved).'
- 'I believe that technology is better equipped to compare the face matching and actually look at all the details on the photo and match it against the person who's in front of them.'

- 'If somebody onboards, taking 12 weeks, on zero-hour contract, I've no obligation to give them work in that period. By the time they're onboarded, if the job has been filled, they've been onboarded, and I've now got no work for them. They have to start that all over again for roles with different organisations.'
- 'It could be that they started work a week earlier. We're earning money a week earlier, paying taxes to Treasury a week earlier, reducing waiting lists and workloads or whatever work they were doing a week earlier than they would have done.'
- 'In terms of legislation, the government is still requiring for that person to be seen in person or via video call. They're not actually recognizing the security & benefits of face recognition for the purposes of the online checks.'
- 'They're powered by digital identity, but still have some really old-fashioned rules, like you can't use online documents, and yet they need still the extra proofs of identity in many cases, like a gas bill, but you can't use an online document.'
- 'I think there's the problem of attracting people who are expectant of getting a job digitally (which grows constantly) and balancing those 20% of people in digital poverty.'

On the idea of reusable identity:

- 'To give a care worker, somebody coming into social care, an identity that they can build, own, and share into a marketplace where 50% of the employees are on zero-hour contracts, exposes capacity.'
- 'They will be able to build, own, and share a single identity that we know is trusted. They can be retained within the sector and that eases the pressure on the market.'
- 'There's no standardisation across organisations. Implementing a way that standardises workforce recognition is only ever going to bring great benefits. It will expose who really is in the market and who really wants to work. We will know their availability soon as they leave an organisation. Currently we don't know.'
- 'It revolutionises the model because suddenly you can base yourself in Cornwall and be able to register workers anywhere in the UK and supply them anywhere in the UK. The same for home-working roles.'
- 'We do need to get to the stage where all 16-year-olds have a digital identity that's got their school record on it as well as their identity and their right to work.'

Respondents believe the sector is behind the digital curve. Digital identity is seen as an accelerant to recruitment innovation, with financial benefits to candidates, employers, agencies, and the wider economy (just consider an extra 6-12 weeks of income, taxes, and spend per candidate in the economy).

Efficiency, the commercial benefit of getting people into work faster/keeping them employed, and security, are key drivers of adoption. Modernisation of the approach to data enablement is seen as the next move. Respondents did not always feel that regulators are in-step.

Digital Identity: Relying Party Views on Adoption Readiness

FINANCIAL SERVICES | ONBOARDING

Non-banking FS digital compliance

- Creating streamlined processes.
- Ensuring that the real-time identification processes use AML/KYC-grade identity mechanisms.
- Being able to provide an audit trail demonstrating that regulatory obligations have been met.
- Minimising the volume of identifications that are handled manually, reducing poor UX, costs, and risk of losing the customer or business.

On the move to digital:

- 'We take away a chunk of something we already do and just have an accepted, singular process which is perfectly simplified, but with all the benefits and upside of everything you're required to pass, you know, security, regulation, and any other obligations we have as well.'
- 'You are part of mass adoption and meeting customer expectation that you do have it. Over time it's a hygiene factor, something that all services will offer to benefit the customer.'
- 'So, for me, there is a throughput and business benefit from services that are more modern and more inclusive.'
- 'AML digitization is different from digital ID. I always refer to that as a portable identity across the sectors for financial services.'
- 'I suppose for us, in our usage of digital identity solutions, we're trying to get to a place where we can very much increase security without making a big sacrifice with the user experience.'
- 'We're open to integrating all sorts of different partner integrations, depending on the particular kind of use case and user journey that we need (e.g., how to enrich the outcome).'

On the idea of reusable identity:

- 'We're looking at the value of a reusable ID across an ecosystem as opposed to a one-off verification.'
- 'The ability for customers to be able to utilise a singular identity, meeting AML KYC regulations, allowing them to onboard across financial services.'
- 'The benefit of being able to support an identity across the financial services sector as well as the customer benefit of just a simplified onboarding journey.'
- 'My hope is that eventually we'll get to a place where we can have a very high level of assurance with verified attributes, but with a kind of easy, seamless user journey.'
- 'Some digital identity attributes are about us being able to reduce risk and increase security, in a more seamless fashion. Another benefit is being able to offer additional services based on financial behaviours.'
- 'If you don't use digital identity solutions, if you go back to manual, call centre, paper-based approaches, or just your own homegrown digital identity system, then that's potentially going to be quite costly, going to introduce friction for end users, and maybe also not be that effective.'

- 'From a strategic, business, and technical perspective, we are in favour of digital identity. But one blocker is the fact that, in the UK, we don't have a national digital ID system like other European countries, and that lack of a standard scheme is potentially a hindrance. A well-organised, well-run, and potentially well-recognized scheme would really help.'

Respondents were positive about the opportunity for security and experience and service enablement.

However, an overriding feeling that the digital identity vision remains just a vision, along with interoperability concerns, still need to be addressed.

FINANCIAL SERVICES | EMBEDDED FINANCE | UNSECURED CREDIT

Immediate compliant access to credit

- Offering unsecured credit lines in commerce journeys.
- Enabling faster activation where credit is required at a point in time and then ongoing reuse.
- Adhering to financial crime identity and risk obligations.
- Managing the risk of funding high-value physical items and virtual goods (and the different loss timescales).
- Ensuring key demographics with immediate need can be serviced (defending the risk of them going elsewhere, often outside the immediate buying process).
- Reducing poor UX, costs, and risk of losing the customer or business.

On the move to digital:

- 'Speed is a key driver of digital identity. If we don't get in there first on the lend, they'll go to the next lender on the list. You will lose competitive advantage, the timing to make a sale, and run a risk that the only ones you'll end up getting to come through your doors are the ones that, for whatever reason, are perhaps a little bit more desperate and have failed all the other lenders.'
- 'Anybody can tell you a subject's name, address, etc., and often credit file data, but the trick with the digital ID piece and some of the tools that we use is it will allow us to comfortably do that authorization check, that verification check, which we must do on the money laundering regs before we lend any money. It delivers safe identification mechanisms.'
- 'It allows a quicker, seamless product to marketplace; time to product and 1st sale with good online purchase experience in sub six or seven minutes.'
- 'I have a suite of authentication tools which depends upon which product is being purchased or which demographic a sector is using.'
- 'We need to have information that is right for the journey.'

On the idea of reusable identity:

- 'If we just went solely digital identity, we may cut off, potentially, the route to some of our older demographics and high net worth individuals that prefer physical credit and journeys. Identity tools must dovetail with activation strategies.'

Respondents focused on secure, compliant onboarding practices, allowing access to credit in real-time. Speed, certainty, and inclusivity were considered critical.

The fear of technology excluding certain demographics shone through with the feeling that digital identity must empower the end results based on demographic and situational need. This includes unintentional digital exclusion.

There is, again, a feeling here that the true potential of digital identity remains a vision.

GAMBLING

Digitalising compliance in gambling

- Registering users for use of online gambling services.
- Ensuring that regulatory, vulnerability, and wider risk assessments are seamless and fast, allowing real-time participation.
- Adhering to financial crime identity and risk obligations across territories in as consistent a manner as possible.

On the move to digital:

- 'Our primary goal is about identifying users fast. In a lot of jurisdictions, the customer can't transact with us until we verify that individual. The gaming sector is all about speed and compliance.'
- 'Tools that digitise identity documents, like credit and other data, educational certificates, qualifications, bank statements, records, stuff of that kind; anything that can be used to form or present something in a digital way, digitise the information to present it in a way that the individual can then represent themselves and present themselves as the true and proper person accelerates compliance processes.'
- 'In terms of regulatory requirements, unless the Gambling Commission puts more of a focus and has more of a steer on digital identity and forces it down, then I don't suppose regulation (moving very, very slowly) will immediately pressure change.'
- 'In the space that we're in, it's about looking at risk versus reward. Verification versus fraud risk mitigation – that space is the world that's being looked at closely. Getting customers in versus the friction that we must put in place to make sure we stop the bad actors coming in.'

On the idea of reusable identity:

- 'I don't think internally it's a topic that we're discussing at great measures. We discuss what's in front of us in terms of what's current regulation, what's current requirements, how do we pass, how do we get to meet gaming, gambling, AML regulation. The concept of digital ID is probably not something that's widely discussed or probably understood.'
- 'I guess the individual having full confidence in the sharing of that data that presents them, represents them, confirms who they are. They need confidence that wherever they send that data, it'll be secure (like to the US). We've got to be confident that the commercial enterprise or government or whoever is using it knows the individual sharing data wants the digital ID and the mechanisms to transport that information to be secure, robust, and non-penetrable.'
- 'Each country, each regulated jurisdiction, has its own requirements for customer verification both at gambling regulation level and at AML level and so, even in the US – and you think of the US as, what, 52 states – they've got an AML, a federal AML law, but at local levels the gambling and how a customer can be verified are all different.'
- 'I think in a nirvana of digital ID, somehow that space would look to add consistency and a common framework.'

Respondents wanted to ensure the evolution of digital tools that simplified and accelerated compliance processes. Client 'time-to-play' is critical.

Internationally, organisations wanted ways of protecting shared data and having identity and KYC systems that interoperated seamlessly across territories.

The feeling is that knowledge of digital identity and its potential is not widespread.

INDIVIDUALISING EXPERIENCE

- Creating hyper-individualisation, down to tailored, single-person experiences.
- Being able to receive healthcare data and other user preference information to ensure the optimised recommendations in the promotion of beauty products.
- Putting data and trust in the hands of the user and allowing them to control their dataflow and subsequent journeys.
- Providing the right data at the right time for the right experience.

On the move to digital:

- 'User engagement and loyalty are our goals. We don't need the rigour of identity assurance that a financial services company would need; we do need tools that allow transmission of data that enhance loyalty outcomes.'
- 'The opportunity for the right data at the right time is key to individualisation and service excellence. It's often seen as a contradiction when weighing up data privacy, security, and data minimisation regulation.'
- 'We expect digitalisation of identity to resolve these perceptions of security exposure. The market needs standards of security, encryption, and tokenisation, married to an ethos of security and privacy by design.'
- 'Data compliance and digital thinking is often built for the 20th Century. We need to move past this and provide enriched experiences built on the right data.'

On the idea of reusable identity:

- 'Reusable identity has the potential to liberate users.'
- 'FMCG goods may be bought in different ways, needing different data points, secured in different data silos. Within the sharing mechanism, loyalty wallets need to understand whether loyalty applies to the transaction, the distribution brand, a specific scheme (e.g., through employer benefits) or the underlying brand of the item. Users must be able to exercise a choice in which loyalty journey they want.'
- 'User control is critical and drives the individuality of the experience someone receives.'
- 'The possibility of a decentralised model with user-controlled data, in a wallet, and using open standards with proper encryption and signature is key. A centralisation of data primed for hacking must be avoided.'

Respondents want digital identity to be a vehicle to transport and share just enough information at just the right time to individualise experiences, in turn improving relevancy and driving loyalty.

Security and data standards are expected to marry those of digital identity. Innovation looks forward to the user being the owner and permitter of the data they hold, to benefit their experience, creating loyalty.

RETAIL | DRIVING OPPORTUNITY AND SALES EXECUTION

Maximise conversion and revenue

- Drive conversion of sales opportunities.
- Ensuring that payment, delivery, and preference data combine to deliver simpler checkout experiences enabled by an adaptive digital identity.
- Seeking to unify data transit to ensure maximum commercial value between retailer and partners.

On the move to digital:

- 'If we take digital identity as a 100%, then each channel does not use 100% of that digital identity. Usage in different steps of a customer experience requires only a particular part. If we have this one whole digital identity as a platform or as thing, then it's just sliced during each session to apply the right user experience. That way it is more secure and easier for the business to interact with the customer without violating their privacy.'
- 'Digital Identity is needed, basically, to not lose the conversion of orders – the conversion of sales.'
- 'Sometimes, in the payment checkout on the online flow, you just don't have enough authentication data points for that customer to check out. So that's why you don't know that customer, basically, but they would probably want to pay.'
- 'There are a lot of digital inequalities of digital data in this current world. That's why it's beneficial for us to have standardised data.'
- 'It has a direct commercial financial impact in terms of having more customers and the loyalty as well.'
- 'Digital identity should be part of the larger foundational strategy of any company.'

On the idea of reusable identity:

- 'It should be fully sovereign and there shouldn't be any interference, basically, from the real life to the virtual internet life. Both worlds should be equal, sovereign to each other, and transferable.'
- 'There are certain standards you must follow to not compromise the customer data and we can talk about CRM, CDPs, and customer data frameworks. But I think there should be an industry standard. I think when it comes to digital identity there should be a convergence of all those standards at one point that's part of the larger digital identity framework or policy.'
- 'Different silos of the business are seeking a unified view. There needs to be synchronicity of internal customer data, and one that encompasses the external service providers as well.'
- 'There are discussions internally to cover different use cases in different departments and a recognition of the need to utilise it in a more commercially viable way.'

Respondents see the value of digital identity to improve key performance metrics in commerce transactions. There was a desire to understand how to create an all-encompassing digital ID that was ready to balance data minimisation with improved payment execution. Standards and interoperability were important considerations but needed to be interoperable with other, wider data standards and frameworks (including, but not limited to, privacy and payments).

UNIFYING ENTITY DATA

- Drive to serve information needed at the right time and the right place to ensure optimum efficiency, accuracy, and quality of service.
- Unification of data from over 1,000 different systems. 300 providing critical information (pieces of the service jigsaw) across disparate channel access points (physical, phone, and online), and partner services.
- Creation of one electronic record that facilitates communication between digital information and operational management.

On the move to digital:

- 'Within my world there's two digital areas to consider, there's our citizens identifier and how we record citizen information, which varies on all the different systems. Then there is our colleague information. The people that work with those systems navigate them to compile the right information. They have to navigate the log in credentials for all those different systems that we have.'
- 'I watched a consultant the other day use eight different systems to do 1 action for a citizen. Each with its own log-in.'
- 'There is an awful lot of very, very sensitive information including health, demographic, and financial information. It's not joined up and both citizens and colleagues have to repeat themselves as they access different parts of service rather than it all being in one place.'
- 'I think it's the fact that organisations have too many systems and people's data and digital IDs spread across all of those. There is a risk for how we manage the people's data.'

- 'More importantly for the citizen, with their digital ID being in one place, it will mean people can spot information, take action earlier, which improves service response and safety.'
- 'We still have paper records in parts of the organisation. The ability to audit what's happening in citizen interactions is severely limited, as is the way that we share information with other organisations when needed.'
- 'The vision we are working towards is a single Identity, immediate access to data, reduced operational overheads, and links to national scheme identifiers.'

On the idea of reusable identity:

- 'We've got to make decisions on how the information is made accessible to the citizen, so they can have a portal with all their relevant and contextualised information on their phones.'
- 'Privacy and ability to act independently are key considerations. What age does a child take control of their records; what age does parental access get cut; what does consent, and culpability, look like? And repeat that question for other vulnerable populations.'
- 'We must really think about what our data security is and looks like. There's a huge level of confidentiality concern. We know we hold incredibly sensitive data that even their closest family members may not know.'

Respondents see digital identity as much about the surrounding information held about the citizen as the way of proving an identity itself.

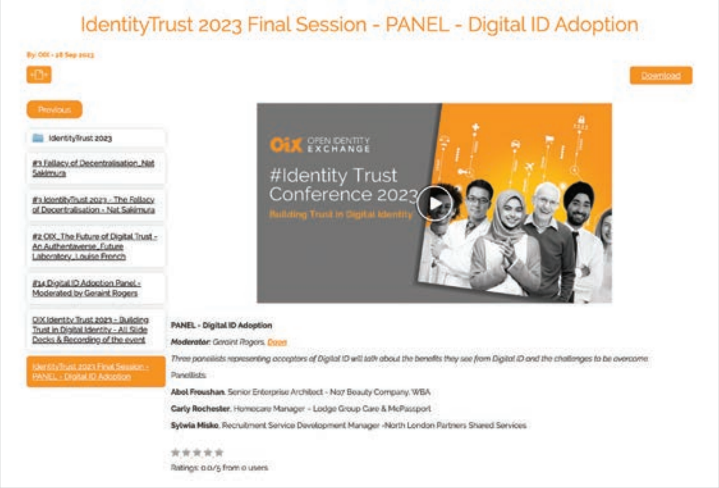
Unification of data and appropriate access (including consent and culpability) needs careful consideration.

Data security is vital, as is the implementation of common identifiers to unify and map data to a single identity. Transformation must use the right data at the right time to deliver enhanced service responses.

This also means a focus on access to vital information and simplified controls for that is critical.

IDENTITYTRUST CONFERENCE 2023 – BUILDING TRUST IN DIGITAL IDENTITY

During the OIX IdentityTrust Conference 2023, a panel of sector stakeholders brought to life some of the challenges and thinking voiced in this research. Click on a link or image to view the session recording.



IdentityTrust 2023 Final Session - PANEL - Digital ID Adoption

By: OIX - 28 Sep 2023

Download
Previous
IdentityTrust 2023
#1 Fallacy of Decentralisation_Nat Sakimura
#1 IdentityTrust 2023 - The Fallacy of Decentralisation - Nat Sakimura
#2 OIX_The Future of Digital Trust - An Authentaverse_Future Laboratory_Louise French
#14 Digital ID Adoption Panel - Moderated by Geraint Rogers
OIX Identity Trust 2023 - Building Trust in Digital Identity - All Slide Decks & Recording of the event
IdentityTrust 2023 Final Session - PANEL - Digital ID Adoption
OIX OPEN IDENTITY EXCHANGE
#Identity Trust Conference 2023
Building Trust in Digital Identity

PANEL - Digital ID Adoption

Moderator: *Geraint Rogers,* Daon

Three panelists representing acceptors of Digital ID will talk about the benefits they see from Digital ID and the challenges to be overcome

Panellists:

Abol Froushan, Senior Enterprise Architect - No7 Beauty Company, WBA

Carly Rochester, Homecare Manager - Lodge Group Care & McPassport

Sylwia Misko, Recruitment Service Development Manager -North London Partners Shared Services

★★★★★

Ratings: 0.0/5 from 0 users

https://openidentityexchange.org/networks/87/item.html?id=710

photo credits – Richard Thompson

Abol Froushan of No7/Boots (part of the Walgreen's Boots Alliance) talks of individualised user experience driving loyalty.

Carly Rochester of MEPassport and Sylwia Misko of North London Partners Shared Services talk about the benefits to employers, candidates, and society of having immediate resource onboarding; being able to keep resources retained in the Social and Healthcare employment sector.

Geraint Rogers of Daon® facilitates conversation, drawing out the real-life challenges seen by relying parties and adding value to their digital propositions.

CONSIDERING ADOPTION

Decision makers and influencers

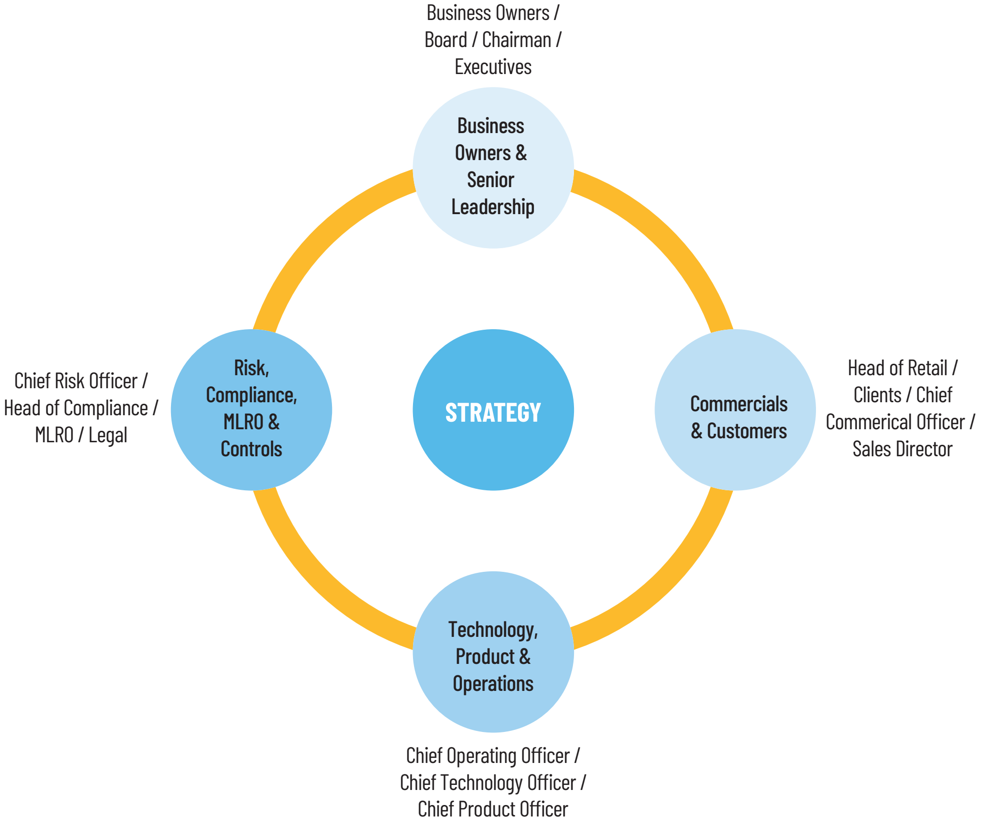
A goal of this research was to explore who makes investment decisions regarding digital identity within organisations – and who supports these leaders in decision making.

There was no clear, consistent answer amongst the respondents. In simple terms: it depends on the sector, the use case, the organisation's size and maturity, and the personalities within an organisation. The dominance of any one sponsor or decision maker seemed dependent on individual company culture and design.

In broader terms, many respondents did reflect on collective decision making.

They also talked consistently of value as investment was considered: What's in it for the organisation?

- Meeting organisational & leadership strategy
- Achieving commercial & customer value (revenue and satisfaction)
- Driving operational, technological or product value (revenue, cost, modernisation, and delivery)
- Mitigating business and customer risk (e.g., compliance and security)


Business Owners / Board / Chairman / Executives
Business Owners & Senior Leadership
Chief Risk Officer / Head of Compliance / MLRO / Legal
Risk, Compliance, MLRO & Controls
STRATEGY
Commercials & Customers
Head of Retail / Clients / Chief Commerical Officer / Sales Director
Technology, Product & Operations
Chief Operating Officer / Chief Technology Officer / Chief Product Officer

Most organisations reflected that middle and senior management had played a role in educating and evaluating digital identity opportunities and in bringing a case to the decision makers. This varies based on sector and organisational culture with Compliance (including those with SMF17 obligations), CX, Product & Proposition, Commercial, Security, Operational, Technology and Transformation potentially playing influencing and gatekeeper roles.

SEARCHING FOR THE RIGHT PARTNER

The research was keen to understand how relying parties chose their IDSP/identity partner. Whilst several respondents were not close to assessment processes, many reflected on a standard procurement template that 'undoubtedly existed' for their organisation. Others talked of leveraging recommendations or acting on previous life experience.

The following were common threads demonstrating the need for consistent points of information and marks of trust.

The need for confidence

Respondents looked to existing, trusted relationships, opinions from a network of like-minded operational partners, proven track records, and trust provided by accreditations.

Evidence of expertise in the sector was also important (knowing the job to be done).

'The first thing we were looking for was approval or endorsement. We looked at what work they've done with the regulators to ensure that they were well accredited.'

'We wanted that trusted, credible provider. They've ticked all the boxes in terms of the certification and supplying to government.'

'All of our partners were already using the provider. It made sense to us as well.'

The need for information

Respondents across the board admitted that their level of understanding of digital identity, including what it means, what value it has, how safe and secure it is, what solution providers exist, and the providers' benefits, are hard to understand. Navigation and 'discovery' work is a barrier to adoption for some organisations.

Key explainer and filtering resources should exist; what's available today lacks maturity, is not democratised, or is not always valuable.

'You probably know this already, but the average Relying Party doesn't understand about certification.'

'I think the Gov UK site with information on IDSPs is just really poor. I feel sorry for the IDSPs that are called XYZ identity or registered last, because they're just at the bottom of the list. Relying Parties scrolling through all these potential providers is just crazy. There should be a web platform that Relying Parties can go to that is democratised.'

'The current one doesn't promote the ABC IDSP versus XYZ because the A one's at the top. Relying Parties should be able to search for IDSPs by keywords or by other types of identifiers, even by volume or by feedback and reviews. It's just not clear and Relying Parties don't understand or value the site.'

The need for simplicity

The thirst for knowledge extends into the buying cycle. Relying parties are searching for quicker ways of comparing solutions and ensuring they do the intended job.

A simple outline of key information, from how the solution works, to where its data is accessed, to how the technologies achieve the objectives being sought, to understanding the security and privacy implications to finally what it means to user interaction, is critical.

A lot of effort is expended in this area, which means there is opportunity for both standardisation and service differentiation.

'We won't bring anything in that we don't understand.'

'My colleagues in procurement — simply put, they'll be interested in cost.'

'You want to understand their pricing model and what is it based on.'

'We were looking at pass rates, accuracy, efficiency, the user journey experience.'

'We didn't want to suddenly find that 10% of all these checks were suddenly then going to a service centre in India.'

'We need to understand the security of the technology, how checks are set up, how the data's passed, where the data's held, how the service and support model works.'

The need for a trusted partnership

Whilst not universal, several respondents were keen to see supplier expertise and engagement extend to consultation and a partnership model.

They wanted to see IDSPs care about the outcomes and go on a journey with them. This showcases the desire by relying parties to be more informed and to have the option of leaning on 3rd party expertise.

Some of the feedback also showed that there is not always a one-size-fits-all model and that adaptation needs to be available to match business risk appetite.

'Making sure that we had strong customer support and looking for an identity partner that demonstrates a desire to continue to improve and develop their product and service.'

'We have all sorts of customer experience principles in mind. We want flexibility and tailorability. We weren't buying something that was just 'out-of-the-box'. We wanted a technology partner with a road map that could also develop things with us.'

PROCUREMENT AND CONTRACTING

Another goal of this research was to explore what relying parties thought of contracting implications.

Most of the candidates felt unable to explore that area in any great depth, so it remains an opportunity for more robust research within relying party organisations with respondents who can give a legal view.

That said, the few respondents that did offer an opinion revealed some interesting insights as to what their interpretation of digital identity means to them.

Liability

For some, liability boundaries remain an unclear position.

For others, the same expectations are not held. Does this mean that the expectations of what digital identity is are mismatched to liability conversations in industry circles, or that the issue truly is less significant than it appears?

'I've got my general counsel's voice in my head, you know, it would just be where the responsibility and liability boundaries lie.'

'I think in the context of digital identity, liability on what happens if attributes are incorrect, is a really important issue.'

'I remember at the time there was quite a lot of commotion from within what is now DSIT about contracts being really difficult to flow down liability. But I haven't found that's the case. I don't know if it's one of these things that people worried about more than was actually necessary, but we didn't find it particularly an issue. It's all in the contractual layer and to equitable parties working it out rather than putting a framework across everything. It's far easier.'

Common Clauses

For those who attempted to answer, the responses gave the impression that most organisations were interested in similar things: security, privacy, data transfer, price, operational model, sub-contracting, and SLAs. However, each organisation likely has different risk thresholds and tolerances.

SOLUTION DILIGENCE

Daon™ and OIX wanted to explore what made a relying party sure that their chosen IDSP/solution provider was right for them. Several of the sectors, especially where organisational size is typically smaller, lean heavily on accreditation.

A key part of their consideration was not only knowing certification was in place, but that their industry body/regulator approved of its use.

In terms of technical testing, the depth of confidence testing varied from organisation to organisation:

- Some rely on the accreditation combined with evidence on performance from trusted 3rd parties already using the solution (as reference model).
- Others want to look at the actual solution performance. This varies from dip-testing, to planned break-testing (trying to spoof the solution outcomes), to volume testing and retrospectives.
- Others consider A/B testing (multi-provider included), Proof of Concepts, MvP studies, and, eventually, a progressive roll-out across their journeys and brands as best practice.
- Others also felt that live performance reporting and periodic situational analysis was healthy best practice.

'What we did is we got confirmation from DCMS that all of our final stage partners were going through the certification process. So, in many respects (and this is quite unusual), it's the trust framework, the certification, that kind of did that job for us, if I'm honest.'

'We'd want to be thorough. Prototyping, a proof of concept. We've got access to a load of data and demographics. We'd want to sign all the necessary nondisclosures to test and get the service right. We would start with, 'Can we run some samples?' and then move to 3 to 4 weeks of running tests. 'Can we try and break it?"

'We would be looking at the customer journey, how they actually experience using the product, and the quality of results.'

'As we piloted them, we put through some dud documents. We would put through, for example, a passport, and then we would manually put through a very different name, a random address that we knew would not correlate to see whether or not the system would pick that up. We did various different experiments to ensure a level of accuracy.'

'That doesn't mean you're looking for 100% pass rate at the onset, which would imply there's a problem. You're looking for a system that can pick up on red flags as opposed to pass everything that runs through it.'

PRIVACY

When it came to privacy, a research question was put in place to understand relying parties' attitudes towards user preferences and consent and how this needed to be considered within digital identity.

Of the three broad levels of response that led to the question, two themes formed the majority of relying party feedback:

1. The mechanics of informing the user about what was happening in the process and consenting to the use of information and biometrics. Of a real adherence to GDPR and data protection.
2. An empowerment mechanism permitting the sharing of information (especially amongst those considering sharing identity across a networked process or in thinking about reusable identity).

Though mentioned as the survey was being built, there was little talk of whether preferences and consent management inside a digital identity proposition could create either a commercial or value-add consumer proposition. Only in Retail Loyalty use cases did marketing consent processes outside of a single digital interaction get referenced.

OTHER REFLECTIONS

The final part of this research involved asking for any other thoughts relying parties had about digital identity.

There was some feeling of emerging clarity, but still plenty of uncertainty. A real interest in seeing technical implementation, understanding reusable digital identity in more detail, and seeing real-life working examples.

A desire to see a tangible roadmap of public sector data powering digital identity and the surrounding processes that it could support. Data needs to be considered as part of what's needed to automate 'the whole activity.' Identity should not be in a silo.

Government process and regulations are considered disjointed by respondents. Obligations to provide digital checks exist, yet permissions to use digital technologies that automate the full process are missing. The Share Code is the prime example.

Other respondents reflected on the use of public sector data in process automations. There was a feeling that inclusion, financial crime defences, vulnerability, and credit assessment could all be enhanced with standard, shared signals provided alongside digital identity processes.

From a privacy standpoint, Zero Knowledge trust was considered key but in need of more collaboration in standards activity.

Overall, there is a feeling of a hiatus before the UK government leads further framework evolution.

'We feel confident that frameworks being established at the moment give the level of surety that we would seek to adopt. Anything that is beyond that is unknown.'

'I've got one concern I suppose, which is the need for additional data for use cases when it comes to international and reporting obligations alongside identification.'

'Identities providing us with tax identification numbers would be a very good enabler.'

'When it comes to applicants with online rights to work share codes, in my opinion it's not aligned because it calls itself an online right to work check, but it's accessed and checked manually – not the same as a digital check.'

'Having a provider check the face with recognition software and on the government's online page as well is logical and it's difficult to understand why the steps are so different at the moment.'

'The government is still requiring for that person to be seen in person or via video call. So, basically, they're not actually recognizing the security and benefits of face recognition for the purposes of the online checks.'

'If it is the government issuing those sanctions through the OFSI, then in my head a government-run digital ID system would tie into that automatically.'

'Privacy and the choice to act with Zero Knowledge is important. Overall, whilst theory is evolving, implementation is just not there.'

'The challenges around the system is not something that providers can resolve themselves, but once the government legislation is aligned, it will make it easier for others to use it.'

ABOUT THE RESEARCH

Digital identity – a buyer organisation viewpoint

Ever wondered what real-world buying organisations think of digital identity? That's the challenge that the Open Identity Exchange (OIX), its Relying Party Working Group, and Daon sought to understand together, undertaking facilitated qualitative research to drive insights into perceptions, value, and adoption.

Research background

The OIX and identity communities have long seen the vision of a connected digital identity ecosystem – one where all participants help to evolve thinking and solve problems together.

In late 2022, to support this vision, the OIX completed quantitative research that looked at how relying parties viewed digital identity.

Its findings led to a continuation of a wider debate on how relying party organisations could be engaged and how their opinions could be used to inform solutions, standards, positioning, and many other linked subjects. Key questions still needed to be addressed; specialists still needed to complete a temperature check of the level of understanding and engagement present in the market (with the hypothesis being that there was a mix of experience on which messages were landing).

It led to the commissioning by Daon of discreet qualitative research that supported this mission. The idea was to bring the depth of understanding of digital identity by relying parties to life by using verbatim quotes, delivering direct insights that can help the digital identity industry engage relying parties in a more informed way.

The research plan seeks to ensure that relying parties have an ongoing voice, supported by research findings and continual engagement.

Research design

Research was conducted over the summer of 2023 and involved 14 participating organisations that were interviewed in hour-long research sessions. Those interviewed responded to 12 specific questions, crafted to gain insights on:

- What relying parties understood about the phrase 'digital identity'
- What value relying parties see in digital identity
- What challenges to adoption they envisage

The research sought to deliberately interview respondents with different experiences in terms of organisational size, roles and responsibilities, depth of potential exposure, and subject matter expertise. They were asked to give honest answers based on what they knew. Seven different sectors were represented in the research: Employment (Health and Social Care plus agency workforce solutions), Financial Services, Gambling, Property Rental, Retail, and Transformation.

Discussion was free-flowing, with planned questions acting as a framework to collect insights. Responses were not mandatory. All verbatim is anonymised.

RESEARCH QUESTIONS

Exploring... definition of digital identity

[Q1] Thinking about digital ID, what is your understanding of the term?

[Q2] Considering both user engagement and business security, what do you think digital ID does?

[Q3] Thinking about innovative marketplaces, what do you think are the benefits of digital ID to your organisation? (Why do they need it?)

Exploring... perception of value

[Q4] Considering digital trends and ways of doing business, what do you think happens if you don't implement digital ID?

[Q5] Considering your current organisational strategy, what do you think would drive your organisation to implement digital ID?

[Q6] Considering your current roadmap, are you considering implementing a digital identity solution? (Which one? Why)?

Exploring... attitudes to adoption

[Q7] Who in your organisation would sponsor a move to digital ID (and who are the key stakeholders supporting them)?

[Q8] When considering your procurement process, what questions would you seek to address in any RFI, RFP, or SOW?

[Q9] When considering the legal contracting process, what are the key clauses and terms you would seek to see covered?

[Q10] When considering implementing digital ID, what solution suitability evidence would you seek (and why)?

[Q11] When considering privacy, what are your organisation's thoughts on user preferences and consents, and how would you consider them for digital ID?

[Q12] When considering any other technical, security, or operational matters, do you have any concerns or questions that you feel need to be addressed?

CONSULTANT INFORMATION

Geraint Rogers
Market SME: Identity, Fraud, and Financial Crime
Daon
grogers@daon.com
+44 7432 707707

Geraint is Daon's Market SME, with over ten years' experience analysing and responding to Identity, Fraud, and Financial Crime needs across a number of sectors and use cases. He's led identity thinking in a number of data providers and IDSPs.

Geraint has over 25 years of experience working for financial services companies in Product Management, Change, Operational, and Transformation roles.

Geraint has a passion for solving problems and believes that the voice of the customer is critical to understanding a challenge and being able to respond accordingly.

He also believes that education must be accompanied by real world insights, context, and an understanding of market drivers to mount an intelligent and effective response to challenges.