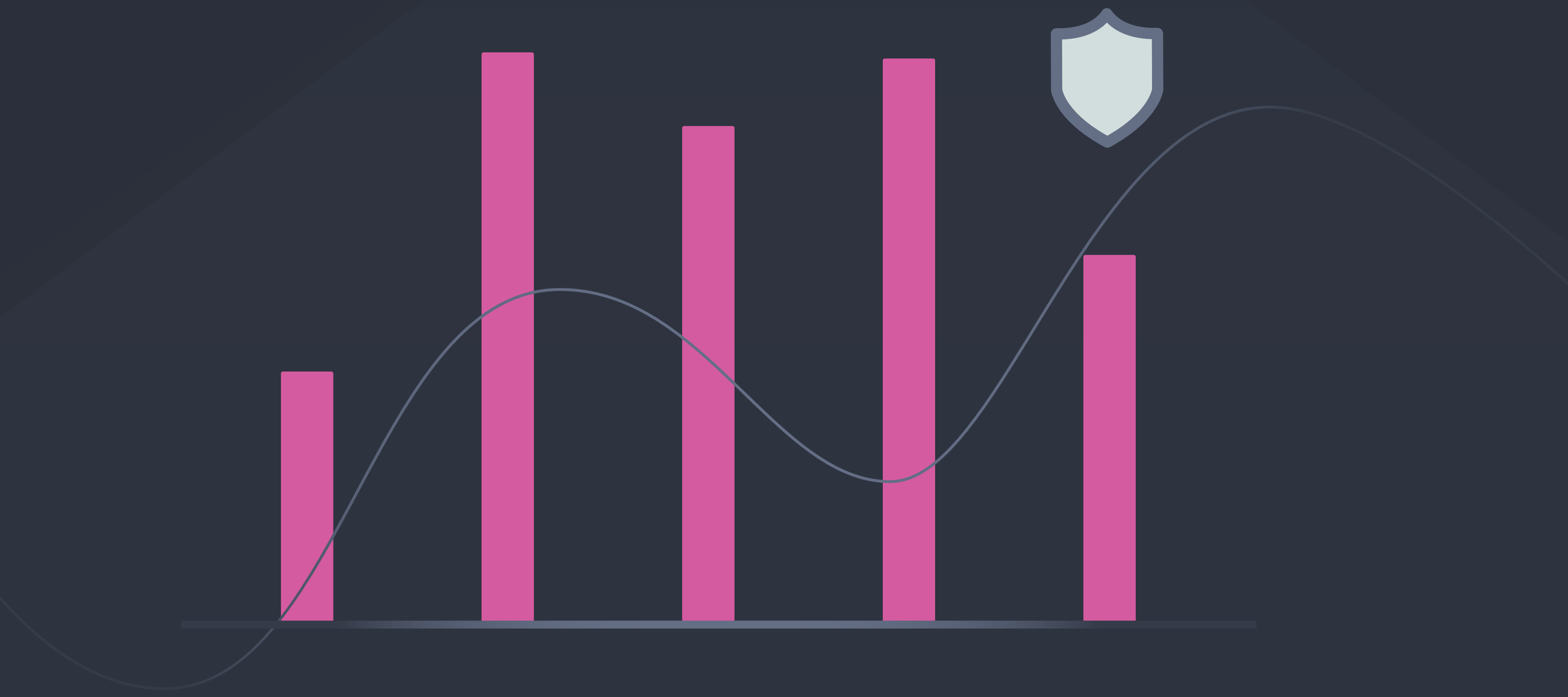
Plotting the Roadmap for Digital Identity

Can evolving identity technology match expectations of users, consumers, and citizens?



CURITY

Executive Summary

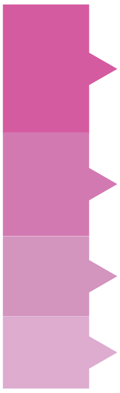
This report, commissioned by **Curity,** researched 200 IT decision makers and 1000 consumers in the UK and US, to understand the current attitudes towards digital identity, adoption levels of digital wallets, challenges to established security practices, and the future landscape of digital identity. In addition we asked organizations about their understanding of the concepts around decentralized identity, and how this may influence their business decisions in the future.

Familiarity with Digital Identity

Around half **(57%)** of IT decision makers (ITDMs) are very familiar with the concept of digital identity and how it works, while those working for larger organizations are twice as likely to be very familiar with digital identity as those in smaller organizations (80% vs 38%).

Security Challenges

Among individuals that agree that digital identity will transform the organization they work for and enhance security practices, the greatest security challenges for incorporation and adoption include:



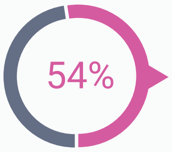
39% Hacker sophistication

33% Lack of appropriate infrastructure

27% Lack of team knowledge

19% Lack of organizational buy-in

Decentralized Identity



Over half of ITDMs are likely or definitely planning to incorporate decentralized identity into their organization in the future.

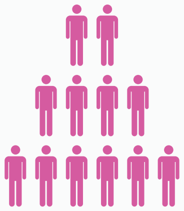
Organization Size Comparison

Larger Organizations 84%*

Smaller Organizations 41%*

ITDM Level Comparison

Results suggest a lack of awareness of this issue at Board Level.



30%* Board Level

68%* Director Level

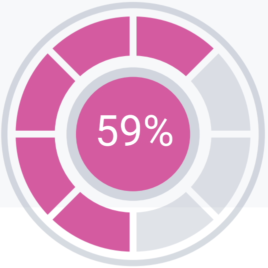
67%* Senior/Mid Manager

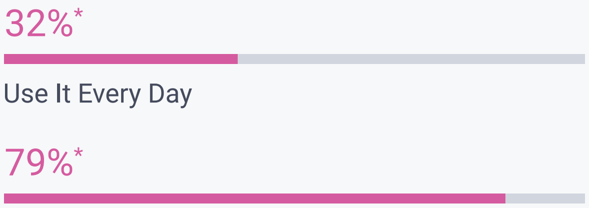
* Of those surveyed who are likely or definitely planning to incorporate Decentralized Identity into their organization in the future.

From a consumer perspective, we spoke with people across the UK and US to understand their attitudes towards digital wallets, any concerns they may have with securely storing information in a digital wallet, and which industries they trusted the most with this information.

Digital Wallets

Consumers Who Currently Use a Digital Wallet

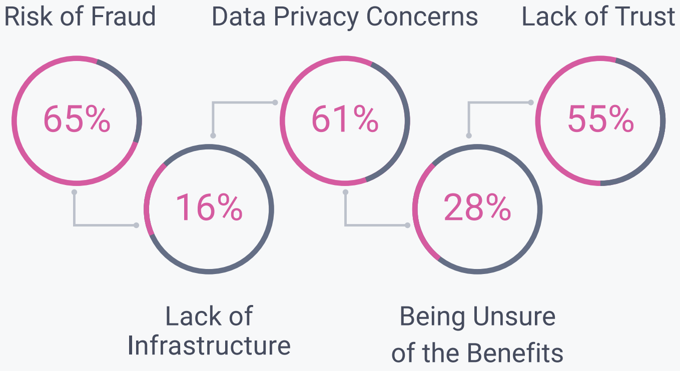




* Of those who use a digital wallet

Personal Information in Digital Wallets

Less than one in five **(18%)** consumers feel uncomfortable storing personal information in digital wallets. Of those consumers that are not comfortable using a digital wallet to store online purchases or personal information, their top deterrents include:



Digital Identity Wallet Management

Type of Organizations Consumers Trust

38% Financial Institutions

35% Medical Providers

34% Technology Companies

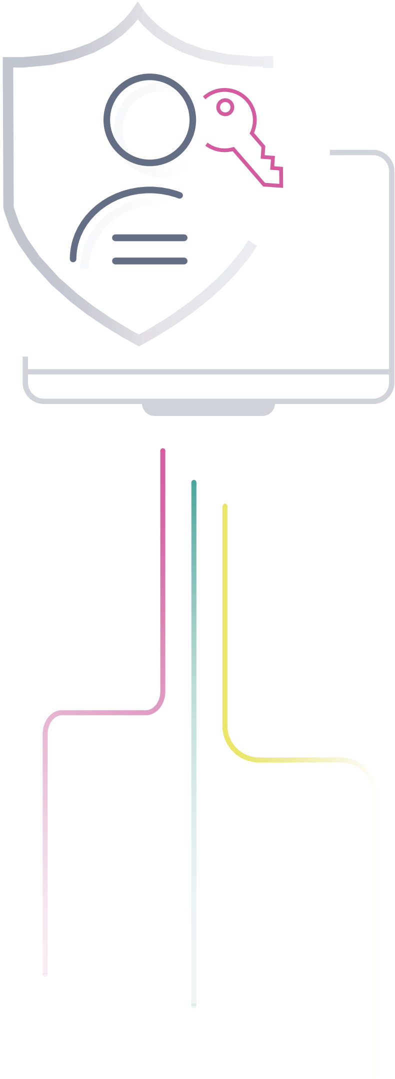
31% Software Companies

22% Government

17% Transport Providers

29% No-One

Introduction: Why Digital Identity and Why Now?



Digital identity goes right to the heart of how we interact with the digital world of today. It has the potential to revolutionize how we prove that we are who or what we say we are during digital transactions and interactions.

The term digital identity is not new, it is a term that can refer to different concepts often with considerable overlap. Our definition for this report is that digital identity is information used by computers to verify and allow access to online services by a person, organizations, applications or devices.

The recent drive to deliver large scale digital transformation projects and the rapid increase in online services has triggered a shift in how we think about digital identity. Understanding consumer and business attitudes better is crucial. By looking at how consumers engage with their digital identity and at how businesses plan to move away from traditional identity management systems, we can get a clearer picture of the effect it will have on our digital lives.

Secure digital identities are a critical component in this ongoing digital transformation. Businesses rely on technology to enhance and improve their services and competitive edge. Usernames and passwords will wane in popularity and methods such as biometric authenticators and Passkeys will help deliver these new services and thwart the hackers.

The developments we are now seeing in digital identity signal a move away from disparate methods and pieces of information to verify identities. Many of these are inconvenient and some are even insecure. As digital identity develops, the authentication tools that organizations have available to them are set to become some of the defining features of this next stage of digital transformation.

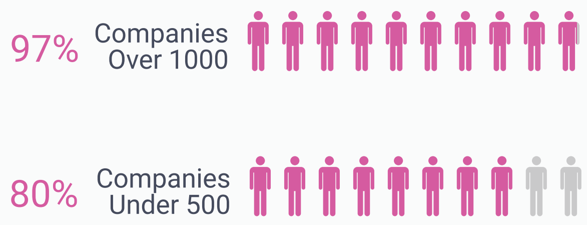
How digital identities are managed - and by whom - is one of the key questions to ask. We expect to see a battleground between governments, financial institutions, and tech companies jostling to control how this question is answered.

The Current Digital Identity Landscape

As technology evolves, so do expectations and understanding. Users want convenience and hassle free experiences, and organizations want to be among the first to deliver them.
Our research shows that managers hoping to, or currently working with, digital identity are well-informed, and confident with the technology. Our data also reveals that organizations use digital identity to transform their organizations and the industries they work in.

There's strong industry knowledge around the concept of digital identity and how it works with **the vast majority (87%)** of ITDMs saying they are familiar with it and **over half (54%)** saying they are very familiar.

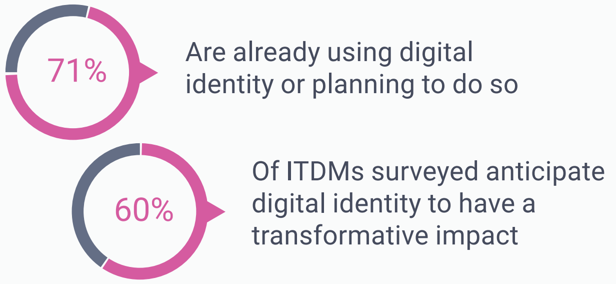
ITDM Familiarity and Confidence*



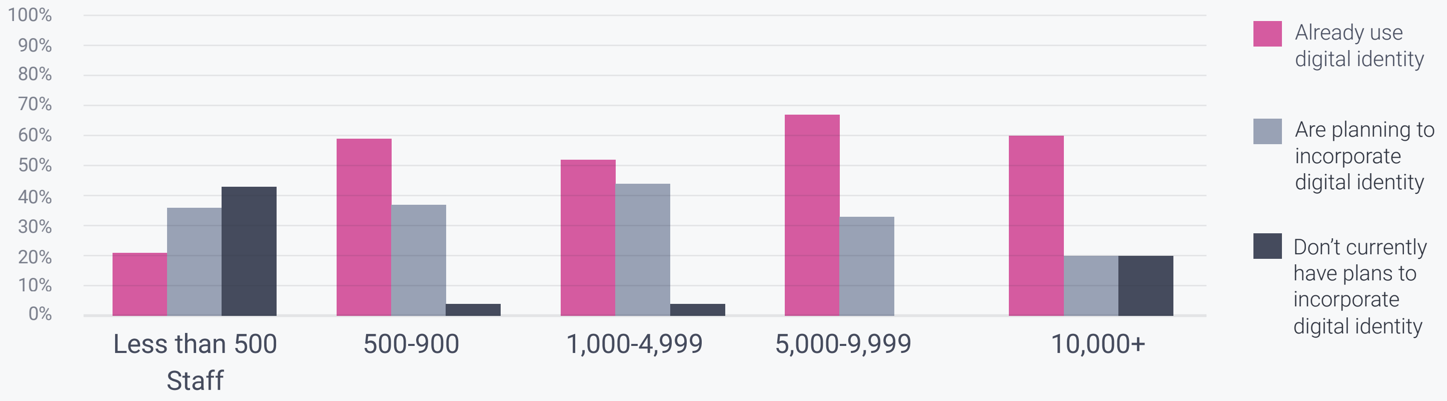
*with Digital Identity

However, there is still an element of sector education needed: **13% of ITDMs** in our survey admitted they have limited familiarity with digital identity. Considering its growing importance, this minority does pose a concern.

Industry Knowledge



Digital Identity Adoption by Organizational Size



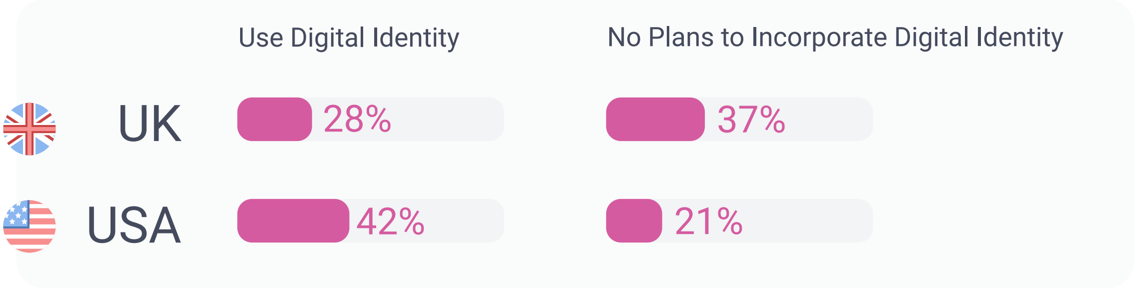
As the concept of digital identity becomes more embedded into day-to-day business operations in many industries, a lack of knowledge could have negative consequences for business performance and end user experience.

Larger organizations lead the way when it comes to businesses who are already seeing the benefits and opportunities of digital identity. ITDMs in larger organizations are around three times as likely to already be using digital identity as their counterparts in smaller organizations.

There's also a stark difference between **UK** and **US** adoption. However, there is still time for the UK to catch up, particularly as more regulation is passed to protect digital identities.

A third (36%) of organizations are planning to incorporate digital identity within their organization and this change is imminent. Among those, **over two-thirds (71%)** are planning to do so within one year and **almost all (97%)** are planning to do so within the next two years.

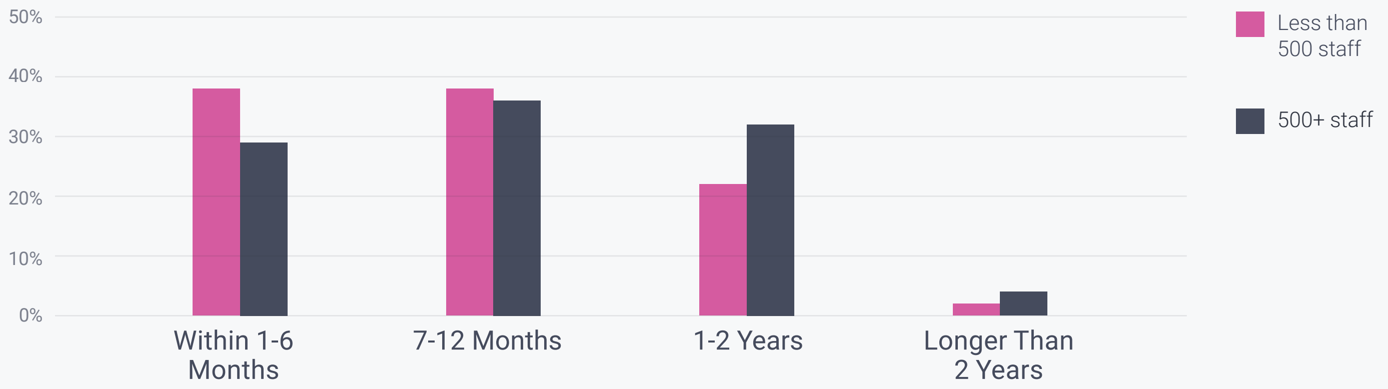
There are still some organizations who are not embracing digital identity. Almost **3 in 10 (29%) of ITDMs** don't currently have any plans to incorporate digital identity within their organization with UK organizations displaying much more reluctance: **37% don't have any plans**, compared to **21% of US organizations**.



Given the pace of change, smaller organizations will need to become more familiar with the opportunities modern digital identity solutions can provide.

While smaller organizations often lack the budgets and resources to be early adopters of innovation, their size can also work in their favor. Often more nimble and agile than their larger counterparts, they may be able to react more quickly to the changes we can expect to see in digital identity in the coming years. Our research highlighted this trend, with **76% of smaller organizations** planning to introduce digital identity solutions in the next year.

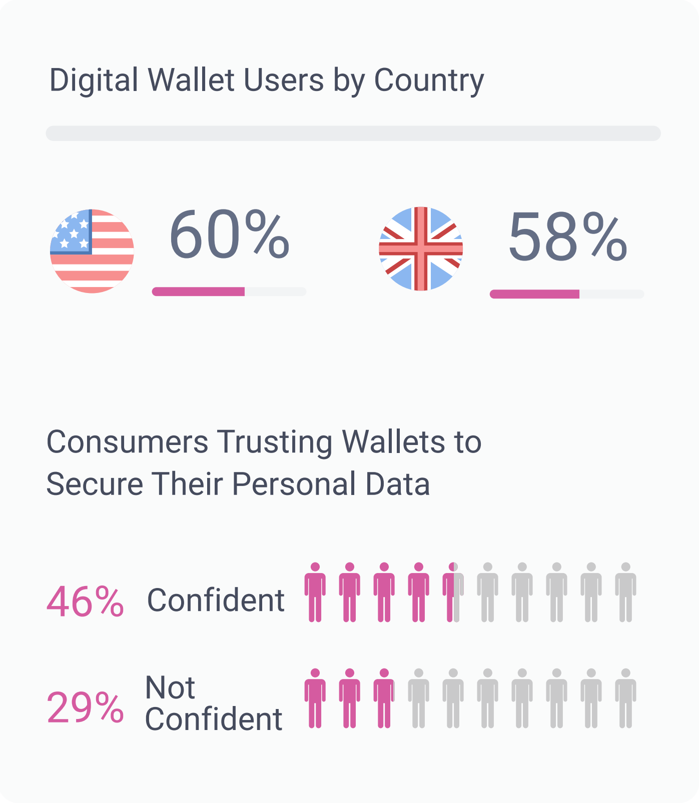
Plans to Incorporate Digital Identity by Organizational Size *



*out of those who are planning to incorporate Digital Identity

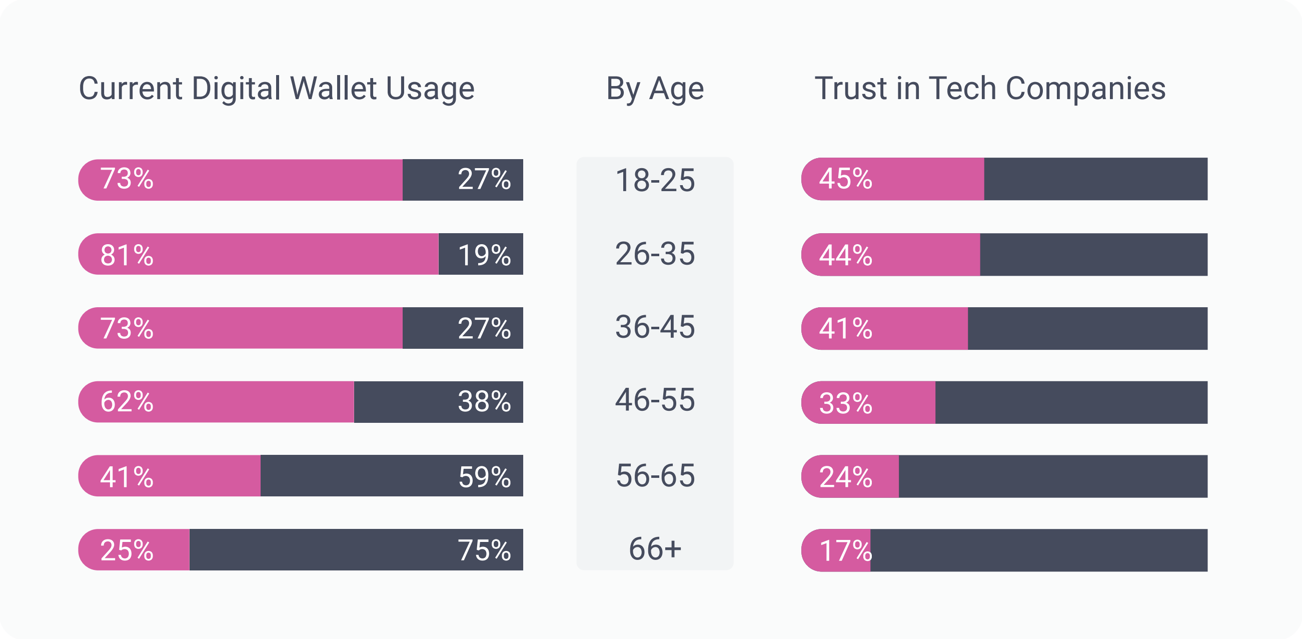
Consumers Embrace Digital Identity

Curity's consumer research found that consumer behaviors and attitudes encourage the growth and development of digital identity, embracing new solutions. **6 in 10 (59%)** of consumers currently use a digital wallet and consistency is global, as UK and US usage is similar **(58% for UK consumers and 60% for US)**. Encouragingly, consumers are also showing strong levels of confidence in new solutions such as digital identity wallets to protect their personal information.



Age is definitely a factor for adoption. People aged 18-45 are more likely to use digital wallets than those aged 46 and above. Crucially, of those aged 26-35, **81%** currently use a digital wallet, compared to **73%** aged 18-25 and 36-45.

Beyond 46, digital wallet usage declines with age. Those aged 26-35 and 36-45 have been raised with these new technologies. Similarly, trust in technology companies to hold and manage their data is highest among younger participants. Therefore it comes as no surprise that they are most likely to embrace digital wallets, and these figures can be key motivators for businesses planning new investments.



There's also room for growth among the different age groups. Although **41%** of consumers currently don't use a digital wallet, **48%** of those would definitely or probably consider using one in the future, with 1 in 10 definitely considering using one. Interest extends across the age groups - though 36-45 year-olds were the most likely to consider using a digital wallet in the future **(71%), 40%** of 56-65 year olds and **37%** of those aged 66 and above would consider doing so.

Among consumers that currently use a digital wallet, the most-used services include: financial services **(62%)** shopping, **(61%)** travel, **(46%)** event passes, **(34%)** healthcare, **(26%)** and automotive **(21%)**. Something all these apps have in common is the personal data required to build a digital identity within them.

Most Used Services by Customers Who Have a Digital Wallet

62%	Finance (e.g. Payments)
61%	Retail (e.g. Loyalty Cards)
46%	Travel (e.g. Boarding Passes)
34%	Events (e.g. Tickets)
22%	Health (e.g. COVID Passport)
21%	Automotive (e.g. Car Keys)
5%	Other

As our data shows, the current and future popularity of digital wallets mirrors ITDMs' optimism for digital identity and the transformative impact it is set to have on many sectors.

Curity's survey of consumers has interesting implications for IT professionals, as **84% of ITDMs** believe financial services will reap moderate or large benefits from incorporating digital identities. However, there's even bigger belief in the potential for the health industry with **87% of ITDMs** believing the health industry would experience moderate or large benefits from digital identities. Both financial services and the health industry are verticals comfortable with data security and privacy regulation. The experience and know-how within the sectors will put them in an excellent position to reap the benefits that digital identity can bring.

Financial institutions are current leaders in public trust **(38%)**, likely because they already manage a lot of our sensitive data. They are followed by medical providers **(35%)**, **34%** trust technology companies (such as Apple, Samsung, HTC) and **31%** trust software companies (Microsoft, Google, Android). Trust drops to **22%** for government, as the second least trusted industry for managing data and information in a digital identity wallet, with transport providers bringing up the rear **(17%)**.

Consumer Trust across Industries to Handle Data and Info in a Digital Wallet

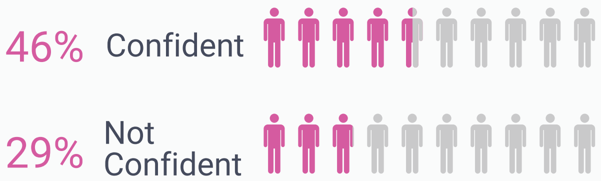
Financial Institutions	Medical Providers	Tech Companies	Software Companies	Government	Transport Providers	
42%	36%	36%	36%	18%	19%	USA
35%	34%	31%	25%	26%	15%	UK

US consumers display greater trust than UK consumers across every industry except government.

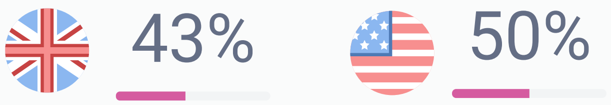
29% of consumers would not trust any of the industries listed to manage their data and information in a digital identity wallet. It is interesting to reflect that despite privacy concerns across social media platforms, consumers continue to use them on a daily basis, indicating that the service on offer is more valuable than the perceived privacy issues. Americans are also more likely to display confidence: **49%** of US consumers feel confident that personal data held in a digital identity wallet would be secure, compared to **43%** of UK consumers.

Consumer behavior shows encouraging signs that uptake of new applications for digital identity could well sky-rocket. Consumer buy-in, and business willingness to get that consumer buy-in will be key to delivering on these expectations. Ultimately, consumers will use digital identities if they are convenient and easy to use.

Privacy-Focused Consumers Trust in Digital Identity Wallets for Data Control



Trust in Digital Identity Wallets by Country



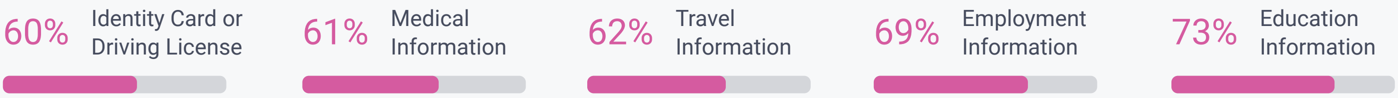
Securing Digital Identity

Moving Away from Siloed Identity Management Systems

The innovation in digital identity is turbo-charging a new wave of digital transformation initiatives, offering customers access to new online services, improved user experience and providing organizations with more efficiencies. The survey results reflect this; we asked ITDMs what their top business motivation was for introducing new methods for authenticating digital identities. Improving the customer experience **(36%)**, and the ability to innovate and provide new services **(33%)** came in first and second.

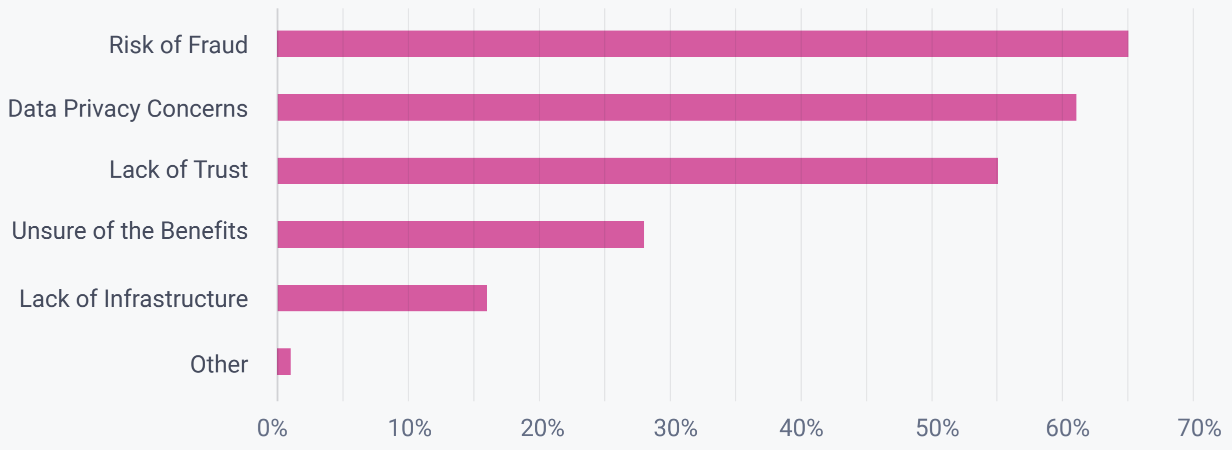
However, technological innovation may, in the mind of consumers, come with an increased security risk. When asking consumers what would deter them from storing personally identifiable information (PII) in a digital identity wallet, the top responses were fraud **(65%)** and data privacy concerns **(61%)**. Greater awareness of the digital trail they leave behind only adds to consumer concern.

Consumer Hesitancy Levels in Storing Certain PII in a Digital Wallet



We have already seen governments, financial institutions and tech companies using digital identities or planning to do so. However, our research also reveals a significant number of organizations in industries such as Retail **(76%)**, Hospitality **(66%)** and Health **(87%)** are considering using digital identities within their organization. All are industries that have seen increased threats from hackers and an increasing number of breaches in recent years.

Top Reasons Consumers Avoid Storing PII in Digital Wallets



For organizations, the disparate pieces of information relied upon to authenticate users is also a significant headache, with legacy systems often siloed, creating significant challenges when storing and protecting user data. Organizations that can manage and work with best-of-breed products from a range of vendors can build a network of solutions as part of their security infrastructure that will be able to keep up with the pace of innovation.

Organizations with global user bases will have an even bigger challenge. We're seeing governments across the globe begin to bring in their own regulations and industry standards for digital identity. So, interoperability between systems using recognized security standards will be crucial to delivering on business and consumer expectations.

Top Security Challenges Faced by ITDMs *

39%
Hacker Sophistication

27%
Lack of Team Knowledge

33%
Lack of Appropriate Infrastructure

19%
Lack of Organization Buy In

*of ITDMs who agree digital identity will transform the organization highlighting this as a top concern.

ITDMs acknowledge that there are security challenges that come with digital identity. We did find that less senior ITDMs were more conscious of security challenges, which indicates they are more likely to be dealing with the issues on a more regular basis.

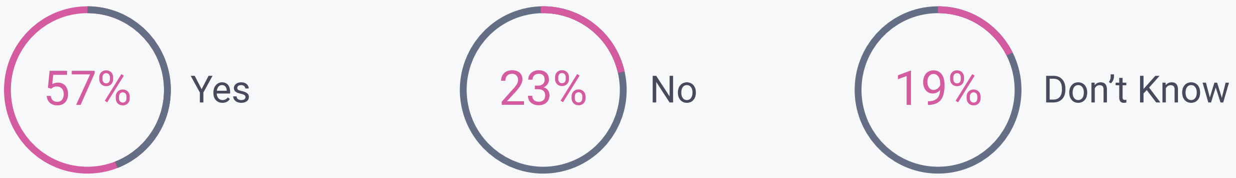
Additionally, smaller organizations cited a lack of team knowledge as a greater issue than large organizations at **24%** compared to **19%**. It is also important to call out the security benefits that the advancements in digital identity will bring. Passkeys and decentralized identity for example offer organizations huge opportunities to enhance authentication processes, mitigate risk and bolster security practices. Some of these new innovations will greatly reduce the amount of PII organizations process and significantly diminish consumers' exposure to risk.

Decentralized Identity - On the Horizon

Another key area for our research was the concept of decentralized identity. It has the potential to transform the verified identity landscape over the next few years. Decentralized identity, also referred to as Self-Sovereign Identity (SSI) or Web5, will fundamentally change how identity professionals and security teams manage identities.

Decentralized identity allows users to control their online identity and choose which information they provide to authenticate their login when accessing digital services. Through methods of identity management, decentralized identifiers (DIDs) and verifiable credentials (VCs) form a self-controlled identity.

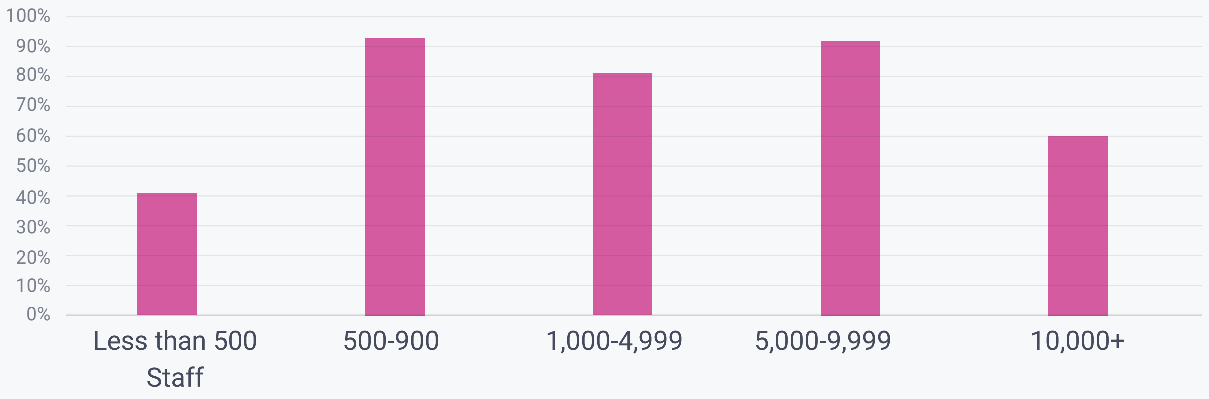
ITDMs Planning to Implement Decentralized Identity



Both DIDs and VCs are now defined by global standards governed by non-profit organizations, and vendor adoption is rapidly increasing as a result. It has the potential to greatly reduce the amount of personally identifiable information that organizations process, significantly reducing exposure to risk.

Larger organizations are more confidently pursuing decentralized identity: ITDMs in organizations with more than 500 employees are almost four times as likely to be definitely planning to incorporate decentralized identity within their organization as those in organizations with less than 500 employees (37% vs 9%).

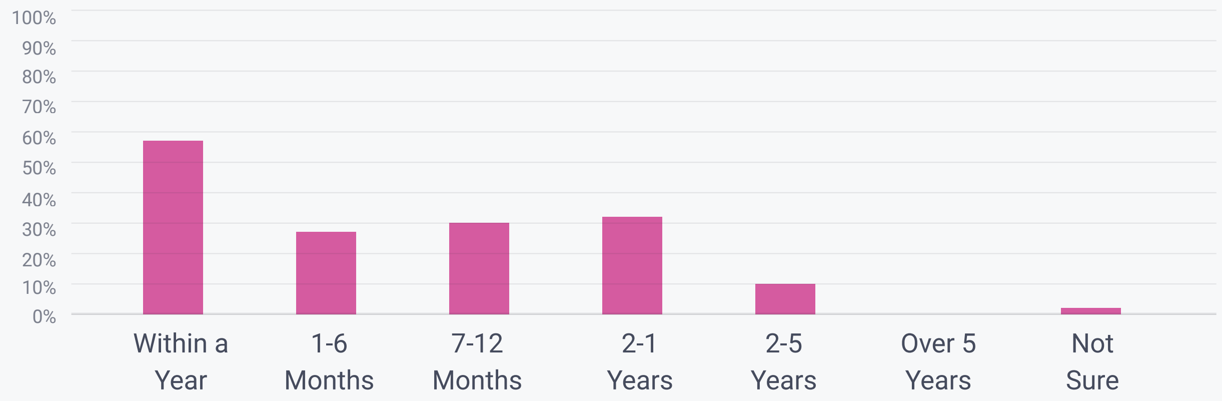
ITDMS Adoption of Decentralized Identity Solutions by Organizational Size



It’s possible that smaller organizations could be at an advantage here as their size may enable them to move more swiftly. While larger organizations often have longer lead times and larger infrastructures, which include more legacy systems and integration challenges than small organizations.

Among ITDMs that are planning to incorporate decentralized identity, those in the US are looking to move significantly more quickly than those in the UK. US ITDMs are more than twice as likely to incorporate it within one year than UK ITDMs **(74% vs 36%)** with the most popular time frame being in 1-6 months **(39%)** in the US, compared to 3-5 years in the UK. If these plans translate to action, the US market is set to develop markedly faster than in the UK.

The Expected Timeframe for ITDMS Planning Decentralized Identity Adoption



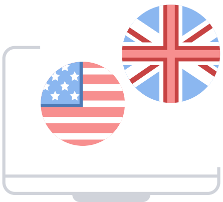
ITDMS Planning Decentralized Identity - Smaller Organisations Change Faster

50% Of Larger Organizations Plan to Do so within a Year

62% Of Smaller Organizations Plan to Do so within a Year

Conclusion

Curity's research finds both business and consumers ready to usher in a new era of digital identity. There's already an understanding and familiarity with digital identity among ITDMs, with the majority of organizations either already using it within their organization or planning to do so. We can expect quick changes and developments as adoption rises, with business early adopters wanting more advanced technology and consumers expecting better control over their digital identity.



UK organizations and particularly smaller businesses will need support and encouragement to tap into the power of digital identity. Both are less likely than their respective US and larger counterparts to be already using digital identity **(42% of US ITDMs vs 28% of UK ITDMs)** and more likely to not have plans to do so.

Organizations that shy away from this digital future are putting themselves at a distinct disadvantage. Consumers are showing a great appetite for digital identity solutions. Though demand is being driven by younger generations there is a desire for digital wallets across the board.

Securing digital identity is crucial. Organizations have many security challenges including threats, hacks and other security breaches both internal and external. Overcoming these challenges is seen to be worth it: **60%** of ITDMs believe digital identity will transform the organization they work for and **79%** believe it will enhance security practices.

60% Of ITDMs Believe Digital Identity Will Tranform the Organization They Work For

79% Of ITDMs Believe Digital Identity Will Enhance Security Practices

Ease of use and seamless user experience will also have a key role in the adoption of digital identity and reducing the risk of digital exclusion in some groups. It is encouraging to find that amongst ITDMs the top motivation for introducing new digital identity solutions into their organizations was improved customer experience.

It will be interesting to watch which players become the dominant drivers of digital identity, with government institutions, financial institutions and tech companies all vying for this role. Financial institutions are off to a strong start with consumers expressing trust in them to manage their digital identity wallet, with government institutions trailing far behind. Though governments can dictate consumer behavior by issuing mandates, if they wish to compete with the popularity of private companies they need to address consumer trust.

2023 is set to be a crucial year for digital identity as organizations start to consider implementing decentralized identity plans. For this new era of digital identity and decentralized identity to become the new normal, collaboration will be required to make digital wallets as accessible as possible. Work is already happening to ensure that user data is secure and protected. Strong industry knowledge, proactivity, consumer enthusiasm and countless potential applications create the ideal conditions for better user experiences and greater security. Businesses should act now to reap the benefits and follow the roadmap to success.

Methodology

This report draws on research conducted by Curity in January 2023.

Curity carried out an online survey of 201 IT Security decision makers in the UK and US, including 101 in the UK and 101 in the US, and an online survey of 1,003 adults with bank accounts in the UK and US, including 502 people in the UK and 501 people in the US.

CURITY

Address
Curity AB
S:t Göransgatan 66
112 33 Stockholm
Sweden

Website
curity.io

Twitter
@curityio

Email
info@curity.io

Linkedin
curity