CITY OF LONDON

THE GLOBAL CITY

In collaboration with

EY

Shape the future with confidence

Securing growth:
the digital verification opportunity

THE GLOBAL CITY

Contents

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

Forewords

Christopher Hayward
Policy Chairman,
City of London Corporation

At the City of London Corporation, we are committed to empowering the financial and professional services ecosystem - from start-ups to established multinationals, and from large technology firms to the government and regulators. By accelerating the adoption and development of cutting-edge technologies, we aim to secure the UK's position as a globally competitive financial centre.

A critical aspect of this mission is the advancement of digital verification technologies, which are essential for ensuring that individuals and companies can securely prove their identities and credentials in the digital age. This initiative not only addresses the immediate need for identity verification but also enhances the integrity and efficiency of financial transactions, contributing to the overall growth of the UK economy.

Digital verification is not merely about confirming identities but also about facilitating a seamless and secure digital economy. The UK is at a tipping point in public support. With the UK poised at the forefront of digital innovation, the implementation of a comprehensive digital verification framework is timely. This urgency is backed by increasing public support for digital IDs and the momentum provided by legislative advancements like the *Data (Use and Access)* Bill.

Our efforts to scale digital verification are outlined in this report, which reflects extensive engagement with industry leaders, government officials, and regulators. These discussions have helped shape a scalable model that prioritises user privacy, data security, and trust, fostering wide-scale adoption and stimulating economic growth.

The recommendations detailed in this report are designed to propel the UK forward, ensuring that we remain leaders in the global digital economy. They are based on rigorous analysis, including international benchmarks, and are aimed at driving both technological innovation and economic benefits. We have articulated the need for digital infrastructure in finance to dovetail with the government's AI strategy.

The path to implementing a robust digital verification infrastructure may be complex and will require time, but the foundations we lay today will define our economic landscape tomorrow. I am confident in our collective capacity to drive this change, ensuring the UK continues to benefit from leading-edge technologies that safeguard and streamline digital interactions.

We thank all contributors, especially Ernst & Young LLP, for their insights and support in developing this pivotal initiative. Together, we are setting the stage for a more secure, efficient, and prosperous digital future for the UK.

Axe Ali, Partner
Private Equity and Venture Capital,
Ernst & Young LLP (EY)

The recent momentum built around Digital Verification (DV) services in the United Kingdom represents a significant opportunity to drive economic growth and enhance operational efficiency across multiple sectors. With projections indicating a £4.8 billion increase in economic output by 2031 through fraud loss mitigation and the modernisation of digital services,[1] the strategic adoption of DV is crucial for consumers, businesses and the overall economic landscape.

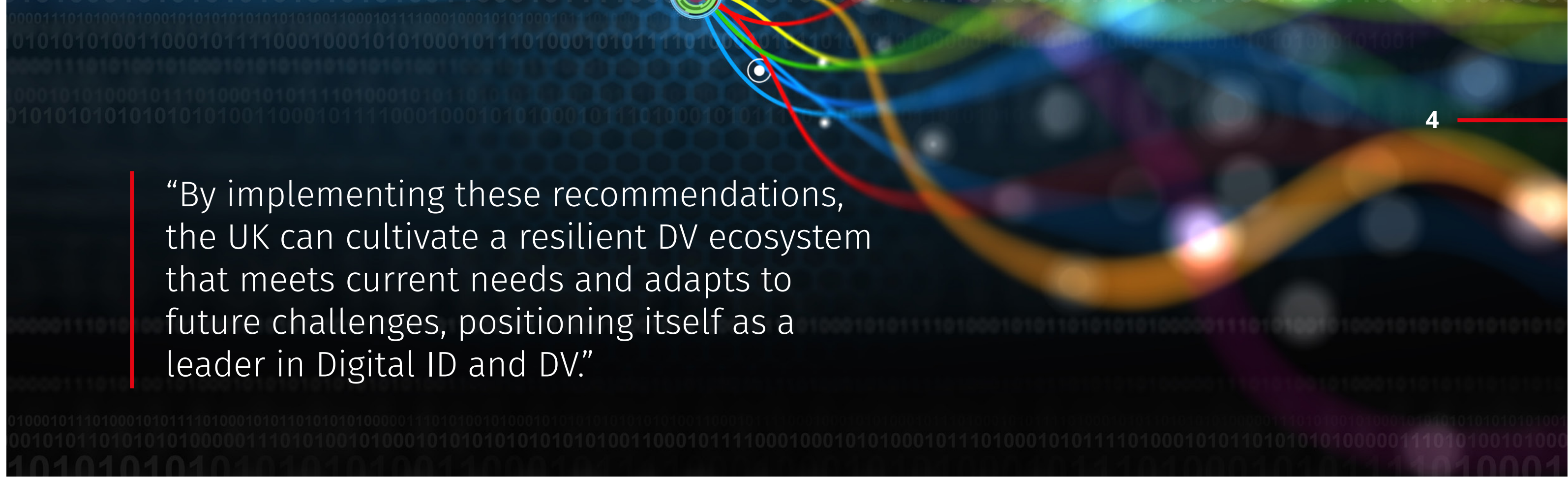
Legislative efforts, such as the *Data (Use and Access)* Bill, are laying the groundwork for a robust digital verification framework. Underpinned by these regulatory directives, a new, widely accepted Digital Verification Service (DVS) could enable quick access to services, allowing users to complete processes in minutes while fostering trust. This system is poised to safeguard against identity theft, ensuring that only verified individuals can access sensitive services.

This increased efficiency and trust in digital systems can create a ripple effect, driving greater adoption of innovative technologies and stimulating investment, ultimately reinforcing the UK's position as a leader in the global digital arena. Furthermore, in creating an innovative DVS, the UK has the opportunity to set the foundation for international adoption of common DV standards. However, realising the full benefits of DV will require a collaborative approach involving government bodies, regulatory agencies, and industry leaders to create a cohesive and effective ecosystem.

As a firm dedicated to promoting growth and innovation, EY is proud to contribute to this report, which highlights why the time is now to advance this conversation on DV in the UK. The proposed model and recommendations derived by the City of London Corporation from this work emphasise user privacy and data security, fostering trust while promoting adoption and growth. We look forward to witnessing the positive impact of this initiative, as it stands to empower businesses with essential tools for success and contribute to the UK's ongoing journey of economic growth and technological leadership.

[1] City of London Corporation (2023). *Vision for Economic Growth – a roadmap to prosperity.*

Executive Summary



"By implementing these recommendations, the UK can cultivate a resilient DV ecosystem that meets current needs and adapts to future challenges, positioning itself as a leader in Digital ID and DV."

The need for Digital Verification in the UK

A widely accepted Digital Verification Service (DVS) across the UK has become essential as consumers increasingly demand secure identity verification for both routine transactions and significant life events. A robust, government-supported DVS is crucial for processes such as opening bank accounts and conducting Know Your Customer (KYC) checks, as it enhances efficiency and mitigates fraud risks. Recent public support for digital ID - with over 50% favouring its introduction[2] - along with the momentum from the *Data (Use and Access)* Bill, highlights the urgency for establishing a unified DVS. The Office for Digital Identities and Attributes (OfDIA) has laid the groundwork with its *UK digital identity and attributes trust framework*, paving the way for a certified and trusted DVS.

Successful adoption of this service will require clear regulatory standards, stringent data security measures, and viable commercial opportunities. Building public trust and demonstrating user value are critical for widespread participation, ensuring confidence in the security and reliability of the DVS, and driving widespread adoption.

A principles-led DV model for the UK

This report presents a principles-led approach to choosing an effective DV model tailored to the UK context. By analysing three international DV models - Centralised, Federated, and Decentralised - we propose a conceptual, hybrid model that integrates elements from both federated and decentralised approaches. Key principles include interoperability, liability, data security, inclusivity, and a sustainable commercial structure.

At the core of this model is the 'orchestrator,' an independent entity that facilitates secure information exchange among users, Relying Parties (RPs), and Identity Data Providers (IDPs). The orchestrator sets common data-sharing standards, enables the encrypted transfer of high quality data, while prioritising user privacy through consent-based sharing. It also manages legal agreements, ensuring compliance with regulations and fostering trust. Governance considerations may involve the Financial Conduct Authority (FCA) and Information Commissioner's Office (ICO) to ensure oversight and compliance with financial regulations and UK General Data Protection Regulation (GDPR).

Key aspects of the model include the ability for users to select from a variety of certified and trusted IDPs, enhancing flexibility in identity verification. With user consent, RPs will have access to high quality datasets, designed specifically for their use case. While RPs remain ultimately accountable for the data they use and must make informed, risk-based decisions regarding the DVS, IDPs are held to high standards of data quality and verification. Additionally, the model incorporates a self-sustaining commercial structure. Fees collected from RPs fund the orchestrator and compensate IDPs, thereby incentivising the maintenance of high standards of data quality and compliance, underpinned by a robust trust framework aligned to OfDIA rules.

Whilst no DVS will be free of risks, the proposed model in this report addresses key risks associated with implementing a DVS in the UK and aims to learn from lessons of the past. Central to the proposed model are security, trust and user centricity, to promote widespread adoption. These have all been stumbling blocks previously. The proposed model aims to address these risks, and more, and this is demonstrated through our outline of a conceptual model and a complex use case later in the report. This is not intended to be the end of the conversation, and the City of London Corporation aims, with this report, to advance the debate and then continue to play a full part in the ongoing discussions.

High impact use cases for DV and the need for widespread participation

The adoption of DV in the UK will depend on identifying high-impact use cases that drive adoption, such as streamlining KYC compliance and enhancing fraud prevention. Demonstrating tangible benefits, akin to successful implementations in Estonia and Finland, will be vital. Interoperability with international services and regulatory regimes, including alignment with the EU's eIDAS regulation, will facilitate cross-border transactions, enhance user trust and ensure interoperability with services already implemented in other jurisdictions. Collaborating with initiatives such as that launched by the Centre for Finance, Innovation and Technology (CFIT) to create a secure reusable Digital Company ID framework can standardise technology and regulations across consumer and company DV. While the DVS may start with an initiative from government and the Financial Sector, a cross-industry solution is needed to gain maximum benefit.

Recommendations to progress a DVS for the UK

The report recommends establishing a comprehensive legal and regulatory framework as outlined in the *Data (Use and Access)* Bill. This framework should clarify responsibilities for stakeholders, particularly in the Financial and Professional Services (FPS) sector, and designate a regulatory authority to oversee the DV service. Defining technical standards will promote interoperability and enhance data security. Prioritising accessibility and inclusivity within the DV model is essential to drive adoption. By implementing these recommendations, the UK can cultivate a resilient DV ecosystem that meets current needs and adapts to future challenges, positioning itself as a leader in Digital ID and DV.

Definitions explained

The following definitions are based on those provided in the *UK digital identity and attributes trust framework*.

Digital ID
A digital representation of who a user is. It lets them prove who they are during interactions and transactions. They can use it online or in person.

Digital Verification Service (DVS)
Services that enable people to digitally prove who they are, information about themselves or their eligibility to do something.

Relying Parties
An organisation that relies on (or 'consumes') certified products or services.

Trust Framework
A set of government-approved rules, which draws mainly on existing standards, guidance, best practice and legislation, that organisations agree to follow to have their service certified as a trustworthy digital verification service.

User
A person who uses digital verification services.

Identity Data Providers (IDPs)
Organisations that hold identity data attributes for users, including name, date of birth, address details, unique identifiers such as national insurance number.

[2] More in Common survey for The Times and Justice Commission - *More than half of public support digital ID cards.*

Introduction and objectives

This report aims to explore how, and why, the United Kingdom could implement a widely accepted and highly trusted DVS. DV is defined in this report as services that enable people to digitally prove who they are, information about themselves or their eligibility to do something. DV is the mechanism through which individuals, and companies, could be verified with a range of institutions, organisations or with other individuals (peer to peer) using verified identity data. This is different to, but complemented by, Digital ID which is a digital representation of who a user is, and which can be used to prove who they are during interactions and transactions. When discussing the participants in a DVS, the report leverages the definitions from the *UK digital identity and attributes trust framework gamma (0.4) pre-release* (Published 25 November 2024)[3], with additional definitions or context provided where required.

The City of London Corporation's Vision for Economic Growth (published in October 2023) highlighted the substantial economic potential of DV, projecting a £4.8 billion boost to the UK economy by 2030 through fraud loss mitigation and the transformation of digital services and infrastructure. As the world's leading international finance centre for five consecutive years, the UK financial services (FS) industry contributes 13% of the UK's economic output, equating to £294 billion in 2023.[4] Recent City of London research found that London ranks second globally in terms of innovation in financial services ecosystems, closely following New York, while the UK excels in cross-border banking, positioning itself as a leading market for the movement of capital and people.[5] A DVS is essential for safeguarding and enabling the future of cross-border trade and innovation in the UK.

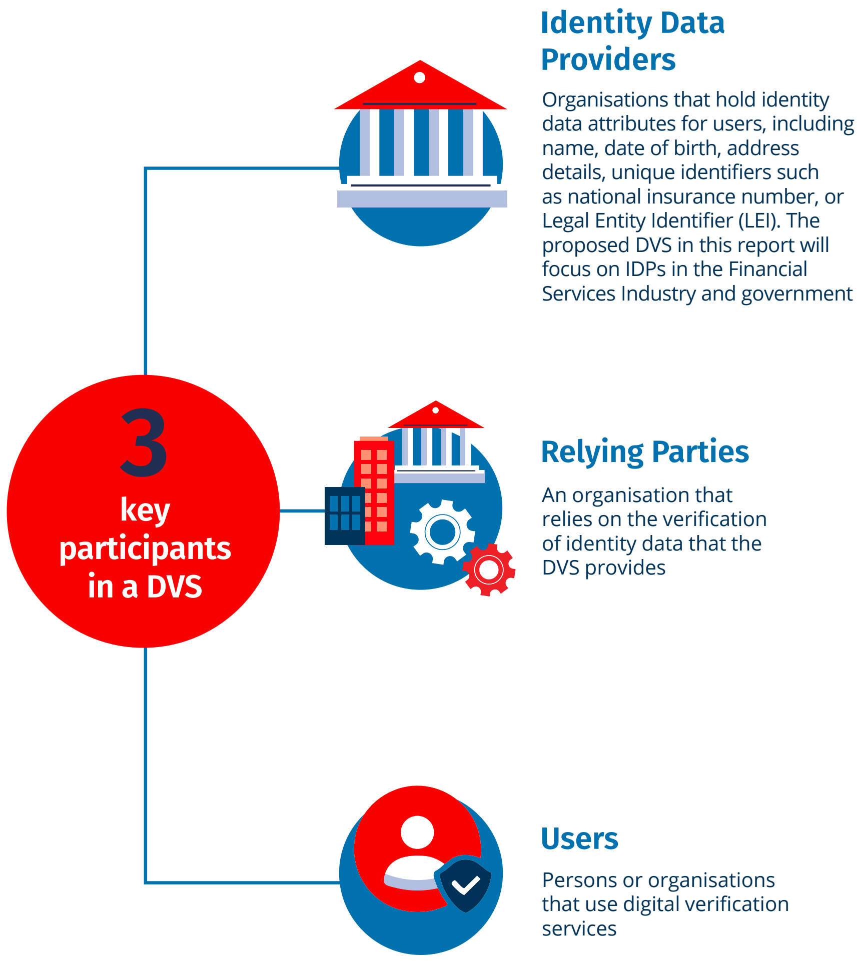
From a legislative perspective, the passage of the *Data (Use and Access)* Bill will lay the foundation for DV. However, there is more to do.

As individuals share and transact more digitally and as the prevalence and impact of economic fraud increases, the need for a robust DVS becomes clearer. So too does individuals' willingness to use a DVS, as we have all become more used to sharing sensitive data online. Individuals are more inclined to adopt DV services that enhance data protection and reduce fraud risk, thereby fostering the growth of digital transactions and the economy.

The adoption of DV is set to streamline processes across the FPS sector and beyond. In financial services, DV can reduce manual verification time, lower compliance and KYC costs, combat fraud, and enhance customer experience by expediting onboarding and transactions. However, the benefits extend to adjacent sectors such as property, retail, telecommunications, and utilities, all of which can gain from improved efficiency and increased access to high quality customer data.

Implementing DV in the UK presents complexities that require careful consideration. The current landscape features numerous private Digital ID and DV providers offering diverse solutions for various use cases, from age verification to access to government services (e.g., GOV.uk One Login). Harmonising these existing solutions with a unified service will be challenging but essential for achieving consistency and expanding DV applications for individuals and institutions.
This report provides a conceptual view of how an industry-wide, government-supported DVS might work in the UK for consumers, proposing a model for adoption and actionable recommendations for government, regulators and industry stakeholders. While it does not serve as a definitive guide to DV implementation, it offers a high-level approach based on consultations with industry experts, regulators, and relevant bodies, with a focus on DV usage within the FPS sector in the UK.

Over the course of a year, alongside international and quantitative analysis, the City of London Corporation has undertaken qualitative research interviews with experts across the financial services industry. The views, suggestions and comments made by these experts have been reflected in both the design of the suggested approach and the considerations and recommendations for industry. Key themes of these considerations include support for a public-private model, the need for regulatory certainty and clearly defined roles, establishment of high standards for data security and verification and fostering a fair value exchange among participants to incentivise engagement. These themes have been reflected throughout the report and have informed the recommendations and considerations within the report. Detail on these can be found in Appendix 3.



Identity Data Providers

Organisations that hold identity data attributes for users, including name, date of birth, address details, unique identifiers such as national insurance number, or Legal Entity Identifier (LEI). The proposed DVS in this report will focus on IDPs in the Financial Services Industry and government

Relying Parties

An organisation that relies on the verification of identity data that the DVS provides

Users

Persons or organisations that use digital verification services

[3] Department for Science, Innovation & Technology (2024). *UK digital identity and attributes trust framework gamma (0.4) pre-release.*
[4] City of London Corporation (2025). *Our global offer to business 2025.*
[5] See reference 4

1. DV in the UK - where are we today?

Digital ID and DV in the UK has evolved significantly since the mid-2000s, marked by initiatives like the Identity Cards Act and the launch of Gov.UK Verify, which aimed to enhance security and access to public services. Recent developments, including Gov.UK OneLogin and the *Data (Use and Access)* Bill, alongside growing private sector and public adoption of Digital ID and DV services, indicate a shift towards a cohesive digital identity strategy that could drive economic growth and innovation in the UK.

The journey of Digital ID and DV in the UK has been marked by significant advances and a growing recognition of its potential benefits. Since the mid-2000s, there has been a concerted effort to explore potential Digital ID or DV services, beginning with the attempted introduction of identity cards. The introduction of the Identity Cards Act in 2006 aimed to establish a National Identity Register, enhance security and facilitate access to public services. Although the scheme was ultimately abolished in 2010, this period laid the groundwork for future innovations.

The launch of Gov.UK Verify in 2014 was a pivotal moment, providing a DV service for individuals accessing government services. However, it faced low adoption rates among government service providers, users and industry participants. Privacy and security concerns were also raised on the design of the service.[6] The service has been decommissioned as of 2023.

Recent developments, such as the creation of Gov.UK OneLogin and the introduction of the *Data (Use and Access)* Bill, signal a commitment to creating a cohesive Digital ID and DV strategy in the UK. This formalisation coincides with increasing private sector adoption of Digital ID and DV services for various transactions, from purchasing age-restricted products to streamlining customer experiences in retail and hospitality. Private sector DV services are enhancing privacy by minimising the sharing of sensitive information, reducing wait times, and mitigating the risk of lost personal documents.

With over 50 certified Digital ID and attribute service providers registered with the Department of Science, Innovation and Technology, the UK has a thriving Digital ID and DV sector. Consumers are increasingly familiar with DV methods, such as using technology providers for age-restricted purchases, which is expanding to include alcohol purchases without physical ID. The growth in adoption of related technology solutions from the private sector such as digital wallets has also laid the groundwork for increased public support. Similar concepts underpin many DV services and much of the public is now familiar with verifying themselves during day-to-day transactions. The UK is at a tipping point in public support and recognition for the need for DV services to enhance trust, streamline processes, and reduce fraud-related concerns.

The sector's growth is further evidenced by UK start-ups raising over £35 million in 2024, showcasing strong private sector momentum despite the lack of a centralised digital ID strategy. The potential for DV to drive economic growth and investment is substantial, comparable to the transformative impact of Open Banking. By unlocking innovation and attracting investment, DV can empower new businesses and enhance the overall digital landscape in the UK. Moving forward, clarity on data standards and sharing mechanisms will streamline existing solutions, fostering an environment where DV services can thrive and deliver their full benefits.

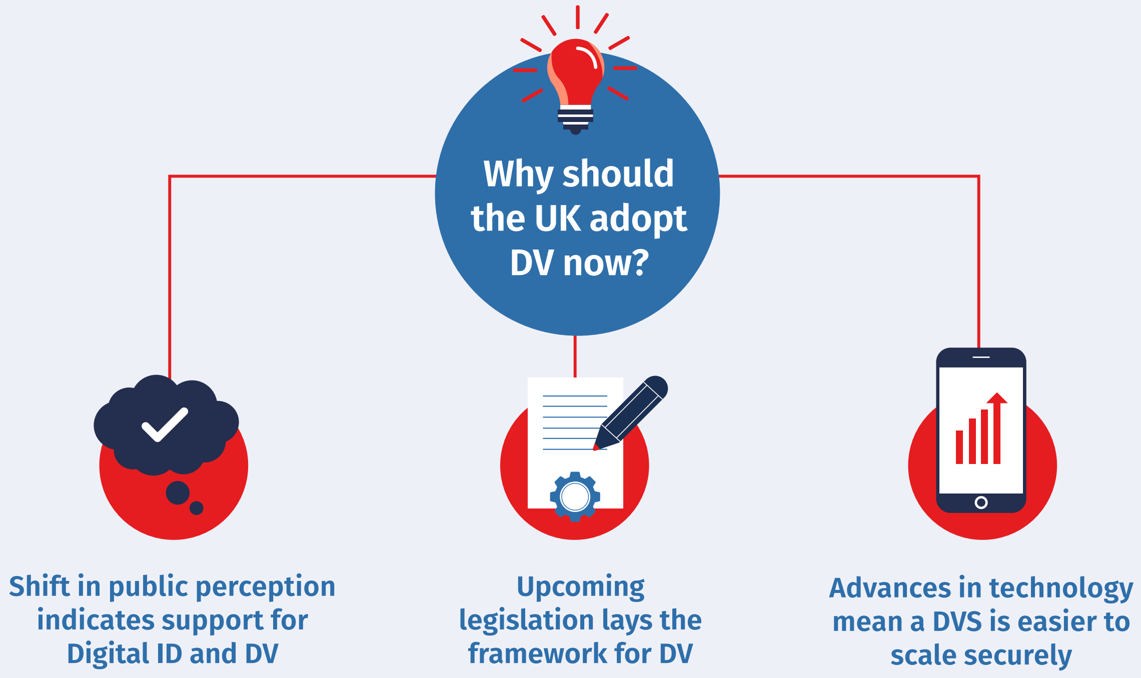
> "The UK is at a tipping point in public support and recognition for the need of DV services to enhance trust, streamline processes, and reduce fraud-related concerns."

[6] Brandão, L. T. A. N., Christin, N., Danezis, G., & Anonymous (2015). *Toward Mending Two Nation-Scale Brokered Identification Systems.*

2. The opportunity for a UK DVS

The UK is at a pivotal moment for adopting DV, with strong public support and increasing familiarity with Digital ID and DV services among consumers. Legislative advancements, technological improvements, and government backing create a conducive environment for implementing a national DV service, which could enhance security, streamline processes, and support key government initiatives.

The adoption of DV is projected to contribute more than £4.8 billion to the UK economy in economic output by 2031 through fraud loss mitigation and the modernisation of digital services. With growing public interest, a supportive political environment, and a focus on combating fraud, implementing a DVS presents numerous benefits, including fostering consumer trust and improving global competitiveness. As the UK navigates the complexities of the digital age, engaging with these technologies could lead to a more secure, efficient, and innovative approach to identity verification, ultimately positioning the country as a leader in the evolving digital economy.



Why should the UK adopt DV now?

Shift in public perception indicates support for Digital ID and DV

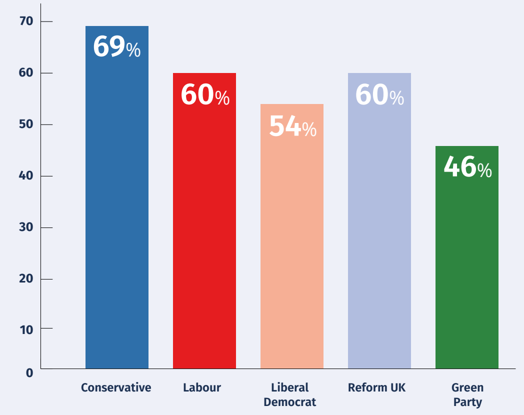
Upcoming legislation lays the framework for DV

Advances in technology mean a DVS is easier to scale securely

Shift in public perception indicates support for Digital ID and DV[7]

Over **53%** of respondents favour a universal Digital ID

Support for Digital ID cuts across voting preferences with the survey finding:



Why should the UK adopt DV now?

Shift in public perception indicates support for Digital ID and DV

Recent polling indicates strong public support for digital ID, with over 53% of respondents favouring a universal digital ID.[7] Support cuts across voting preferences, with the survey finding that 69% of Conservative voters support Digital ID cards, whilst 60% of Labour voters, 54% of Liberal Democrat voters, 60% of Reform UK voters and 46% of Green Party voters also supportive.

Consumers are becoming increasingly familiar with Digital ID and DV. They are currently able to use private sector DV services to prove their age when purchasing cigarettes, energy drinks and lottery tickets. Later in 2025, consumers will also have the ability to prove their age digitally for alcohol purchases. This is likely to increase adoption of DV and increase customer familiarity with these services and their benefits.[8] The growth in usage and adoption of DV among customers indicates that the UK has arrived at a 'tipping point' for Digital ID and DV after historically cautious public sentiment. The shift in perception and increased support for these services makes now a more appropriate time to consider a national DVS.

Upcoming legislation lays the framework for DV

There is growing sentiment among government and regulators that DV could drive benefits across the UK, with legislation set to enable DV in the UK currently progressing through parliament and regulators expressing their support for DV. The progression of the *Data (Use and Access)* Bill (DUA) reflects a significant political commitment to reforming the UK's identity verification landscape and government commitment to progressing Smart Data schemes. In a recent letter, the Financial Conduct Authority (FCA) highlights the importance of adopting DVS to enhance security and trust in financial services. The letter emphasises the need for regulatory frameworks that facilitate innovation while ensuring consumer protection, aligning with the UK's National Payments Vision which calls for secure and efficient payment systems reliant on robust identity verification. Startup Coalition and the Tony Blair Institute have also highlighted the need to pass the DUA Bill and implement sector-specific Smart Data schemes, including in FPS, to expedite Open Finance and improve data sharing.[9] Together, these elements create a timely opportunity for stakeholders to implement a DVS that aligns with these emerging legislative standards and the broader goals of the UK's financial ecosystem.

DV technologies could also support recent government announcements of more stringent 2-step systems to be made mandatory for all retailers selling knives online.[10] These requirements could be enabled by a robust DVS, reducing the need for individuals to share personal data online and in person with delivery staff. Under the new measures a person may need to submit a copy of a photo ID such as a driving licence

[7] See reference 2

[8] GOV.UK (2024). *Pubgoers given choice to prove age with phones next year in boost for high street and hospitality sectors.*

[9] Startup Coalition & Tony Blair Institute (2025). *Making Smart Data Happen.*

[10] GOV.UK (2025). *Stricter age-verification checks for all knife retailers.*

or passport, as well as proof of address such as a utility bill, before showing ID again when the package is delivered. This could also include a person submitting a current photo or video of themselves to an online retailer alongside their ID. This proposed service, which would involve customers directly sharing personal information with retailers, could be improved or streamlined through the implementation of a DVS available for use by retailers.

Stronger government support and a legislative framework that facilitates the creation of a DVS across the UK demonstrates a significant shift in support for DV initiatives, creating an environment that makes implementation possible, which is markedly different from previous attempts.

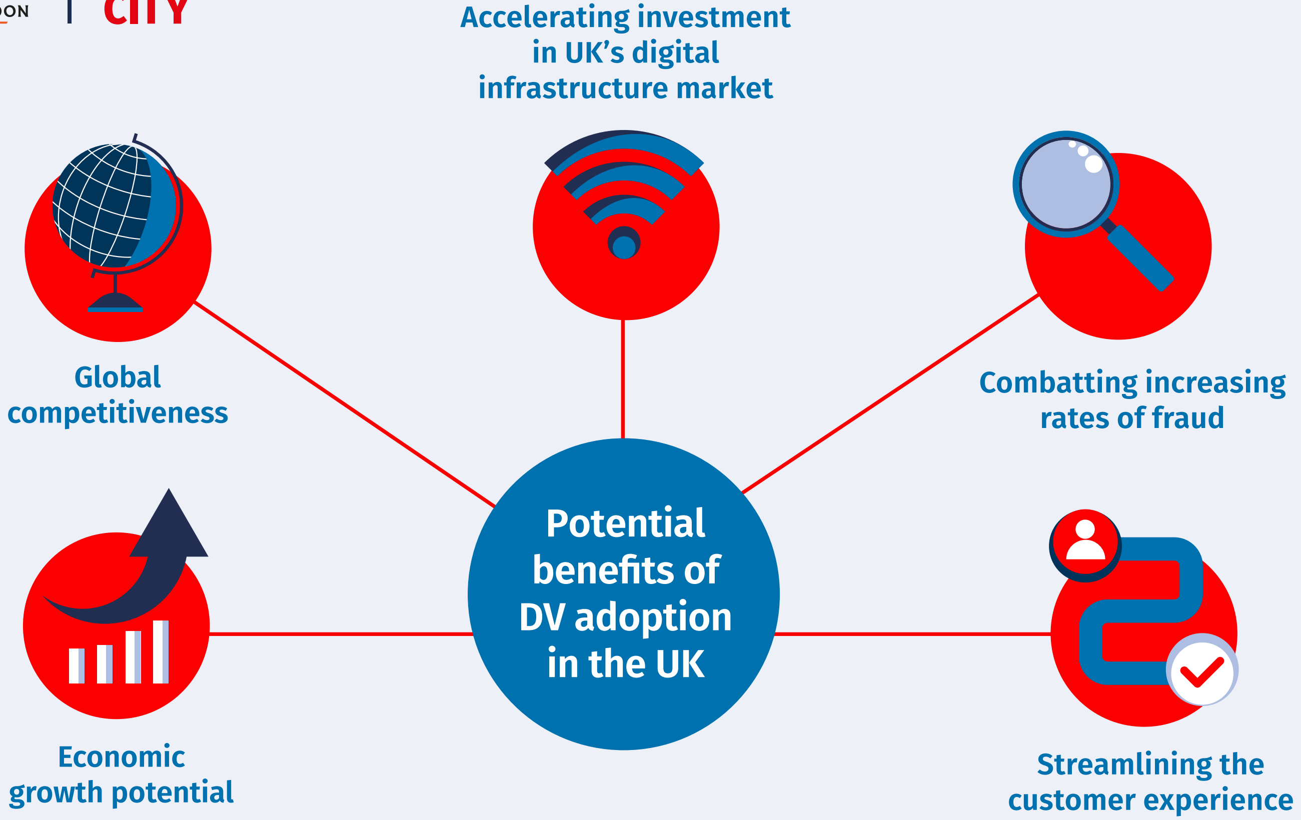
Advances in technology mean a DVS is easier to scale securely

The successful implementation and adoption of a national DVS hinges on several advances in adoption of technology. The infrastructure for a DVS relies on supporting elements such as widespread and reliable internet access and smartphone penetration. The UK meets these preconditions, with 84% of UK adults (aged 16 and over) using a smartphone,[11] according to the ONS, and 96% of UK households having internet access in 2020.[12] Moreover, the integration of privacy by design principles into the development of these services is crucial. By prioritising user privacy from the outset, advances in technology can ensure that sensitive personal information is handled securely and transparently. Additional use cases, such as age verification, may require further technological enhancements, including biometric authentication (e.g., facial recognition).

The advent of 'privacy by design' solutions and the ability to integrate the principles of privacy by design into DV services ensures that sensitive personal information is handled securely and transparently. This approach, and the advances in technology that enable it, not only protects user data but also creates increased trust in the service, something that is crucial for the widespread acceptance and adoption of DV. Integration of technology such as blockchain and digital wallets can further enhance the security and usability of DVS, allowing users to control their personal information while ensuring that verification processes remain efficient and tamper-proof. These technological capabilities can now ensure that DV services are able to verify sensitive data in a secure manner, increasing the ability to build a safe, trusted DVS.

> "The shift in perception and increased support for these services makes now a more appropriate time to consider a national DVS."

[11] Office for National Statistics (2020). *Percentage of homes and individuals with technological equipment.*
[12] Office for National Statistics (2020). *Internet access – households and individuals, Great Britain.*


Accelerating investment in UK's digital infrastructure market
Global competitiveness
Combatting increasing rates of fraud
Potential benefits of DV adoption in the UK
Economic growth potential
Streamlining the customer experience

Potential benefits of DV adoption in the UK

Economic growth potential
The adoption of DV is projected to contribute more than £4.8 billion to the UK economy in economic output by 2031 through fraud loss mitigation and the modernisation of digital services. This growth aligns with the UK government's commitment to fostering a "Smart Data Economy," which aims to unlock £149 billion in organisational efficiency and £66 billion in new business opportunities,[13] ultimately driving innovation and competitiveness. In addition to the economic benefits that can be quantified, there is a wider trust dividend which can be unlocked. A widely accepted, highly trusted DVS, with the ability to scale across the economy and society more broadly, can enable a level of trust in commercial transactions currently hindered by distrust of users in current DV services in many parts of the UK economy. In areas from e-commerce and online marketplaces to property and real estate, the number of economic decisions that can be enabled by such a service could count in the millions.

Global competitiveness
Many countries are advancing their DV frameworks, and the UK risks falling behind if it does not follow a similar approach. Embracing DV can position the UK as a leader in the global digital economy, attracting investment and talent while ensuring that UK businesses remain competitive in international markets. Additionally, in enhancing trust in cross-border transactions, DV enables increased trade with the UK internationally, increasing investment and growth of the UK economy.

Accelerating investment in UK's digital infrastructure market
The Global DV market is experiencing a surge in investor interest, with funding from Venture Capital (VC) and Private Equity (PE) reaching £2.5 billion in 2023—an impressive leap from just £90.7 million in 2014, marking a 2656% increase over the decade. Average deal sizes have also risen significantly, at upwards of £2 million per deal in 3 of the last 5 years, up from £270k per deal in 2015, indicating a more mature industry.

Capital invested in the UK in the DV market is also surging, from £7.72 million in 2014 to £114.7 million in 2023, a 1386% increase. While investment trends do fluctuate year-to-year, total capital invested has averaged almost £69 million per year between 2020 – 2024.

However, when compared to countries with established national DV frameworks such as Sweden (where investment in DV made up 0.36% of total PE and VC investment in 2024), the UK has work to do, with just 0.047% of PE and VC investment targeted at DV in 2024.[14]

These trends suggest that a robust national DVS can drive innovation and investment in a technology ecosystem, while serving as a foundation for an array of trust enabled services (e.g., e-health services, verified payments, smart contracts). Therefore, whilst it is positive that companies based in the UK are able to attract significant investment, there is further potential for increased investment into DV infrastructure and the services that rely on it, as a result of a more developed system.

Combatting increasing rates of fraud
Identity fraud is a growing concern worldwide, including in the UK. Reports indicate that, in the UK alone, fraud losses could exceed £3 billion annually.[15] Implementing a widely accepted and trusted DVS can provide secure methods for identity confirmation, thereby reducing these losses and protecting consumers and businesses from financial harm. As consumers increasingly engage in online transactions, there is a heightened demand for secure and efficient identity verification methods. Many individuals are concerned about the risks of data breaches and identity theft, which have been widely reported in the media and have affected numerous high-profile companies. This has led to a significant lack of confidence in digital services, with consumers often hesitant to share personal information online. DV can address these concerns by providing reliable methods for identity confirmation, enhancing consumer trust in digital services. By implementing effective DVS, organisations can reassure users that their personal data is protected, ultimately leading to increased adoption and usage of digital services, which is vital for the overall health of the financial system.

Streamlining the customer experience
DV can significantly reduce the time and effort required for identity checks during transactions. For example, users can quickly verify their identities for online banking or loan applications without lengthy processes, such as submitting multiple forms of identification. This reduction in friction enhances the overall customer experience, leading to higher satisfaction and retention rates, as customers appreciate the convenience and speed of service. Additionally, the estimated spend on KYC operations in the UK is in the order of billions of pounds, indicating that there is considerable scope for cost savings through more efficient DV processes.

Uses for DVS

There are already a number of firms and organisations active in the space of Digital ID and DV services in the UK. In order to spur adoption and growth, there is a widely held recognition of the need to realise scale and tap into network effects across users, IDPs and RPs. Efforts to create these networks have begun, both in the UK and globally, bringing industry participants together. The aim of our report is to further these efforts, highlight key principles we believe should be considered in the creation of a DVS in the UK, suggest a model we believe is suitable for the UK, and call for a wide participation in the effort by the financial services industry and government.

Key to driving adoption and realising these network effects will be penetrating use cases for DV in the UK. Initial use cases centre around making it easier for customers to identify and verify themselves when registering with a financial services provider, streamlining KYC processes. Additionally, initial use of

[13] Parris, Stuart, Anton Spisak, Louise Lepetit, Sonja Marjanovic, Salil Gunashekar, and Molly Morgan Jones (2015). *The Digital Catapult and Productivity: A Framework for Productivity Growth from Sharing Closed Data.* Santa Monica, CA: RAND Corporation.
[14] Pitchbook data (2025). Accessed 19th Feb 2025.
[15] UK Finance (2024). *Annual Fraud Report 2024.*

the DVS will aim to reduce identity fraud, mitigating fraud losses for both customers and banks. The below sections detail some of the immediate use cases for DV and potential pools of customers impacted so as to demonstrate the potential widespread uptake of DV.

Example use cases in FPS

Within FPS, a DVS has potential use cases in any scenario where a user's identity must be provided, verified or trusted. Some key FPS use cases are included below; however the list is non-exhaustive, and our proposed model intends to enable flexibility and scale in the use cases to which it could be applied in FPS. Use cases outside of FPS are not in scope of this report, however wide adoption across industry and government unlocks many more use cases and potential for economic growth.

Account opening & KYC: One in eight (13%) of UK adults have switched bank accounts in the previous three years[16] and four in ten (42%) UK consumers have opened a new personal or joint current account in the last six months.[17] Of those who had opened a new account, 40% of accounts opened were additional accounts, meaning customers would have already verified their identity with a financial services provider. These customers could benefit from streamlined yet secure KYC, leveraging DVS.

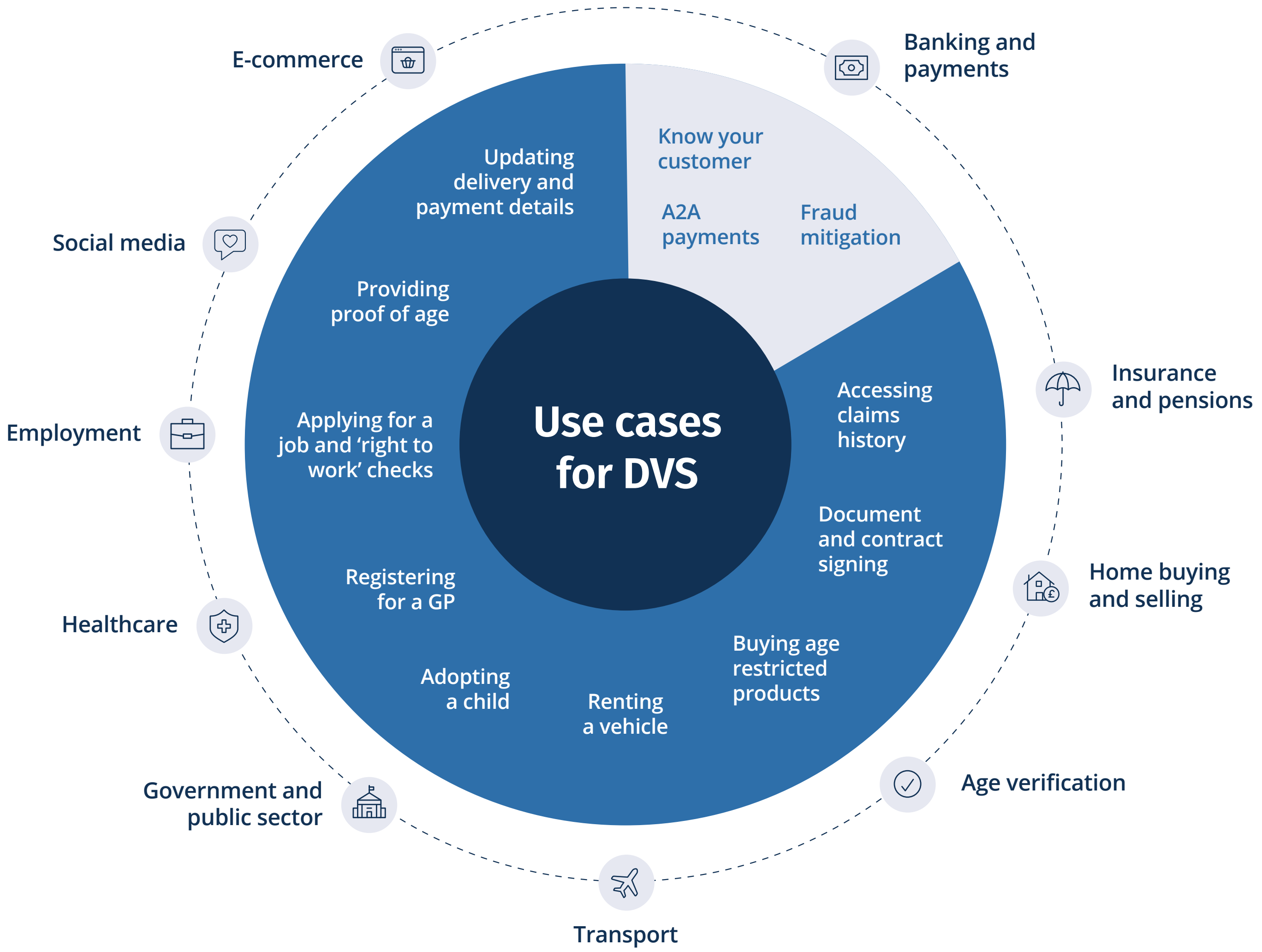
Combatting fraud: 9 million adults in the UK were victims of a financial scam in the year to October 2024.[18] Losses associated with payment fraud in the UK amounted to nearly £1.2bn in 2024 according to UK Finance[19] and, more broadly, fraud costs the UK economy £190bn annually.[20] DV mechanisms offer an opportunity to combat fraud, with a particular focus on impersonation fraud or identity theft, reducing the impact on millions of UK adults. Enabling an ecosystem with a strong level of verification for all individuals and organisations applying for financial products can help to close one entry point to the financial system for criminals. Such an ecosystem can prevent those who use synthetic or stolen identity information to create mule accounts or apply for financial products illegitimately. In the proposed model and use case set out in this report, we outline a service that can help to build such an ecosystem.

Age verification: Millions of UK adults will be impacted by enhanced UK regulation ensuring those purchasing age-restricted products online have their age confirmed at the point of purchase and again at the point of delivery. Whilst digital IDs such as the digital driving licence, due to be introduced in 2025, could have a positive impact on the customer experience in age-restricted online transactions, a DVS with multiple verification points (including government and privately held identity data) enables secure and highly trusted online verification, with limited data sharing.

Account to account (A2A) payments: A2A payments refer to real-time or near real-time transactions that occur directly between two bank accounts without the need for intermediaries, such as payment processors or card networks. While currently offered in the UK and worldwide, they are primarily used for peer-to-peer transactions[21] and have not seen the same level of adoption for consumer purchases – in the UK, c.7% of e-commerce transactions used A2A payments in 2022.[22]

A robust DVS has the potential to address issues of trust in the A2A payment sphere, by providing a validated identity credential alongside account and payment details. Any implementation as part of a consumer purchase process would need to ensure no additional friction is introduced in the payment journey. International examples such as the A2A / mobile payment service Swish in Sweden evidences where a digital ID enables trust in the A2A payment system, allows Financial Institutions to capture payments on a platform managed by them, while ensuring the service remains free to, and widely adopted by customers.[23]

Document / Contract Signing: Contract management is a key high-frequency use case for digital ID and verification services globally. Provision of a highly trusted, authenticated signature enhances trust in the process. A widely accepted service increases the efficiency and speed of signing, and a DVS could strengthen the enforceability of the contract signed through use of non-repudiation features.



[16] YouGov (2025). *Three in five Brits have had the same current account for over ten years.*
[17] Savanta Europe (2025). *Why UK consumers are opening new bank accounts – and what banks can do to keep them.*
[18] Citizens Advice (2024). *9 million people caught out by financial scams in the past year.*
[19] See reference 15
[20] Crowe Clark Whitehill, Experian, & Centre for Counter Fraud Studies at the University of Portsmouth. (2017) *The Annual Fraud Indicator - UK foots £190bn annual fraud bill.*
[21] FIS Global (2023, March 23). *Account-to-Account Payments Set to Revolutionize Shopping, with E-commerce Payments Reaching $525 Billion Globally: Worldpay from FIS 2023 Global Payments Report.*
[22] Simon-Kucher & Partners (2025). *Accelerating Instant Payments in the UK: Why Ecosystem Incentives Are Key to Success.*
[23] Banking Gateway (2019). *What is Swish? The mobile payments system used by more than two-thirds of Swedes.*

3. What model of DV should the UK adopt?

In defining a DV model for the UK, we adopted a principles-led approach that established key principles to guide model selection and ensure alignment with industry expectations. Our methodology involved identifying global DV models, defining critical principles for successful implementation, evaluating models against these principles, and ultimately defining a UK-specific model that incorporates the most suitable features of the global models.

The selected DV model is underpinned by four essential pillars: Adoption and Growth, Privacy and Security, Public Trust, and Legal and Regulatory Compliance, each supported by specific principles to foster user engagement, protect sensitive information, build trust, and ensure adherence to legal standards. This structured approach aims to create a robust and widely accepted DVS that meets the needs of both consumers and businesses while enhancing the UK's position in the evolving digital economy.

3.1 Taking a principles-led approach to DV model selection

In our work to propose a DV model for the UK, we have followed a principles-led approach whereby we established principles that served as guardrails for the choice of model and ensured that the outcomes remained aligned with the UK's expectations as expressed by industry experts.

Our methodology consisted of four key stages:

1. Identification of DV models globally: We reviewed and defined possible model options in existence in the global DV market that could inform the choice of a UK model. This analysis involved examining international DV models and conducting review and discussion sessions with experts, and a review of available academic and research content (see Bibliography). The detailed outcomes of this stage are included in the appendix.

2. Identification of DV model principles: Next we established a set of four pillars critical to the successful implementation of a DV model in the UK. Under each pillar, we have detailed principles to guide the choice of the DV model. These principles, which reflect the UK's expectations as well as international best practice, were derived from discussions with CoLC, EY Subject Matter Resources (SMRs), academia*, and other expert interviews.

3. Evaluation of DV models against principles: We then evaluated the identified DV models against our principles to determine areas of alignment and divergence to principles. In this activity we focused on a set of core principles which significantly influenced our choice of model.

4. Definition of the UK model: Based on the evaluation conducted between the global DV models and principles analysis, we defined a UK model by leveraging the most suitable features from each of the models analysed. The outcome of this stage is presented in the following section.

Our principles-led approach has enabled us to develop a DV model that aligns with the UK's expectations. By following a structured methodology, we aim to contribute to the dialogue with a clear rationale and point of view, supporting progress and contributing to the development of the public and private sectors' ambition to establish a robust DVS for the UK.

3.2 Evaluating principles against existing DV models

DV model types

Models for DV are generally considered on a scale from more centralised to more decentralised.[24] The model types we outline in this report are in broad terms commonly accepted as the three primary model types, however there can be considerable overlap of features between them as we explore in this report.

1. Centralised model
2. Federated model
3. Decentralised model

Centralised model: In this model, a central authority (e.g., a government or organisation) manages and controls the entire identity verification process. The central authority will also maintain the authoritative source register, such as a national ID or population source register. The ID is generally recognised by the government as providing proof of legal identity. All user data is generally stored in a central database. In cases where no foundational ID system exists, the official digital ID may be offered by an entity that relies on multiple functional and lower-tiered government ID systems as authoritative sources, exemplified by systems like myGovID in Australia. The Indian and Singaporean models align closely to a centralised model.

Federated model: This model involves multiple authorities (organisations or entities) collaborating to manage identity verification, and often providing a government-recognised digital ID. The model is generally coordinated or accredited through a trust framework or federation authority. Identity providers can include both public and private entities that can leverage a foundational ID system as their authoritative source. User data may be stored across different entities, but each entity retains control over its own data. Participants agree on common standards and protocols for identity verification. Users can in some cases choose which entity to trust for verification. The federated approach allows for a diverse range of IDPs while maintaining a level of oversight and trust. Examples include DigiD in the Netherlands, BankID in the Nordics and and the Estonian Digital ID scheme.

Decentralised model: This model operates without a central authority and relies on a distributed network of participants. Participants interact directly with each other for verification of identity. Users have control over their own data and can choose how and when to share it. Participants can use different protocols and standards, leading to flexibility. This model allows for identity portability across different enterprises, enabling users to manage their identity without relying on a central authority. It emphasises privacy as users retain ownership of their data, and security through high levels of encryption and by eliminating single points of failure. Examples of this model include Verified.me in Canada and the European Digital ID Wallet, which empower users to maintain control over their personal information.

In the following section, we will explore the principles that we believe should underpin our choice of model, and align these models to our principles. The aim is to assess the strengths and weaknesses of each model in relation to the specific needs and context of the UK.

[24] Mole, C., Chalstrey, E., Foster, P., & Hobson, T. (2023). *Digital identity architectures: comparing goals and vulnerabilities.*
*Millo, Y., Panourgias, N., & Zachariadis, M. (2021). *Identification Infrastructures and the Capitalization of Data in the Development of Data-Driven Regulation: The Case of the Global Legal Entity Identifier System.* In B. Unger, L. Rossel, & J. Ferwerda (Eds.), *Combating Fiscal Fraud and Empowering Regulators: Bringing tax money back into the COFFERS (pp. 158-179).* Oxford: Oxford University Press.

Principles guiding our DV model choice

In our effort to create an effective, widely accepted and trusted DV model for the UK, we identified four key pillars that are critical to its successful development and implementation:

1. Adoption and Growth
2. Privacy and Security
3. Public Trust
4. Legal and Regulatory Compliance

Adoption and growth - the effectiveness of a DV model relies on its ability to attract and retain users. A model that delivers meaningful value to all stakeholders - be it individuals, businesses and organisations, or government entities - will encourage widespread participation. Prioritising user-centric design, scalability, accessibility and adaptability to evolving needs are key strategies for fostering high adoption rates and ensuring the model's long-term success.

Privacy and security are paramount in safeguarding sensitive identity-related information. In an era where data breaches and privacy concerns are prevalent, it is essential that the DV model incorporates robust security measures to protect user data. Implementing best practices for data confidentiality and compliance with privacy regulations not only secures user information but also enhances public trust and facilitates greater adoption. Use of international best practice standards in identity, authentication and data security will be key to strengthen privacy and security and will also increase interoperability of the service with international peers.

Public trust is the foundation upon which a successful DVS is built. Users must have confidence that their identities will be securely verified and that their interactions with the service are protected. Establishing a strong trust framework, ensuring transparency in processes, and maintaining accountability are vital for cultivating this trust among individuals and organisations.

Lastly but vitally, **legal and regulatory compliance** provides the necessary framework for the DV model to operate. Adhering to and enabling relevant laws and regulations, for example within data protection and anti-money laundering, is essential for establishing a trustworthy and legally sound service. Ongoing regulatory oversight ensures that the model remains compliant and responsive to changing legal landscapes.

Together, these four pillars form the key elements of a successful DV model. Each pillar is supported by a range of principles that provide a comprehensive foundation that guides the choice of a model that meets user needs while promoting trust, security, and compliance. The full set of principles, aligned to our pillars, can be found in Appendix 3. In this report, we highlight five key principles that will significantly influence our choice of model. By highlighting these five principles, we do not intend to minimise the importance of other principles we have listed in Appendix 3, particularly in the design and implementation of a DV model. However, we believe these to be the key principles in influencing a choice of model.

Pillar	Principle	
Adoption and growth	Commercial model	It is crucial to balance the commercial interests of all stakeholders, including IDPs, RPs, and government, while maintaining a free service for users. This is critical to fostering collaboration and ensuring that all parties are motivated to contribute to the service's growth. Key considerations include ensuring adequate commercial incentives for all participants and evaluating both initial setup and ongoing operational costs to maintain financial sustainability. By prioritising these elements, we can create a sustainable model that not only meets the needs of stakeholders but also delivers a valuable, free service to users.
Adoption and growth	Interoperability	The model should allow the establishment of common standards for technical integration, enabling seamless collaboration among participants and with international counterparts. By implementing standardised semantics, we can ensure that all parties involved have a shared understanding of the data and processes, which is crucial for effective communication and interoperability. Furthermore, the development of a unified legal and organisational framework is essential to govern and enhance participation and to enable a robust commercial and liability model.
Privacy and security	Data Security	At the core of the model must be a focus on safeguarding highly sensitive information against potential attacks or breaches. This focus on security is not only a legal and regulatory requirement; it is essential for building trust and confidence among users. Furthermore, it is vital to empower users with control over their personal data, allowing them to manage access and permissions effectively. This user-centric approach not only enhances security but also fosters a sense of ownership and responsibility among users, encouraging greater participation in the service.
Adoption and growth & public trust	Inclusivity	The service must be accessible to as wide a range of users as possible, both individuals and organisations, thereby enhancing the overall impact. Choosing a model with inherent scalability and flexibility will maximize inclusivity in both the medium and long term. Flexibility to adapt to the evolving needs of users and scalability to accommodate growth as demand increases. This inclusivity will be instrumental in driving widespread adoption and establishing the DVS as a trusted and essential component of the digital landscape.
Public trust & legal and regulatory compliance	Liability	The chosen model must allow for clear lines of responsibility and accountability among all participants. This clarity is essential for fostering trust and confidence in the service, as it delineates roles and expectations for each stakeholder involved. To further enhance trust, the model should incorporate robust mechanisms for redress in the event of negligence, illegality, standards violations or misuse. These mechanisms not only provide a pathway for addressing grievances but also demonstrate a commitment to transparency and ethical governance, and ensure regulatory and legal compliance.

Analysis of common Digital ID and DV models against key principles

In the table we have set out some considerations of each of the global DV model types against our key principles for model selection. To aid understanding we have highlighted in blue where elements of the model type align with or support our principles or are favourable in a UK context. Our findings show that no one model fully satisfies our principles, or that there are elements of multiple model types which should be considered in the choice of a model for the UK.

Pillar	Core principle	Digital ID and DV model type			Conclusion for the UK
		Centralised model	Federated model	Decentralised model	
Adoption and growth	Commercial model - incentives	Can commercialise service by charging RPs for access to verification services, however this benefit is largely realised by the central authority.	Both models can enable a commercial model by extending participation to a range of IDPs and RPs, while a federated model emphasises setting common standards on interoperability to ensure a level playing field. Both models allow for a multitude of use cases, from the simpler (e.g. age verification) to the more complex (e.g. KYC and onboarding). Thus they enable a sophisticated commercial model with incentives matching the complexity level of identity assurance required of the specific use case. Wide adoption by IDPs, RPs and users will be key to unlock network effects and grow the size of the potential market.		Both the federated and decentralised model reward IDPs and incentivise them to uphold high standards of data quality to continue participating in the service. A model for the UK should have a focus on mutual benefit for all participants, reducing initial cost for setup, and a mechanism to sustain the service commercially, or provide returns over time. We believe this is a model that is particularly well-suited to the cost-constrained environment in the UK.
	Commercial model - costs	Requires upfront investment by a single entity, which can impose a substantial financial burden. However, it can benefit from reduced complexity due to having a single point of control. Ongoing maintenance costs can be significant to mitigate risks related to data security and privacy.	Federated model allows for budget control and cost-effectiveness through use of existing technology infrasturcture and storage, and collective contributions from multiple entities for integration build and ongoing maintenance. Costs can be incurred establishing and maintaining common standards and a legal framework across participants.	The decentralised model, often leveraging blockchain technology, can incur higher initial setup costs but can also lead to operational cost savings over time by eliminating the need for a central authority. However, it may encounter challenges such as high initial costs and potential complexity of managing multiple providers and ensuring data security.	
	Interoperability	A centralised model relies on standardised protocols and formats, which simplifies integration and communication with the central authority. However, organisations may face challenges if they become overly dependent on a single provider whose ability to innovate may be limited, potentially hindering flexibility and scale.	The federated model fosters collaboration among multiple identity providers, enhancing data exchange and interoperability. This model excels in facilitating data sharing among different organisations, making it a more robust choice for ensuring seamless integration.	The decentralised model supports self-sovereign identity, empowering users to control their own data and share it selectively. While it promotes user autonomy and data privacy, it can create challenges if there is an absence of strong central standards, which may impede interoperability.	The federated model provides a practical approach to standard setting and interoperability across IDPs and RPs. In the UK context, self-sovereign identity may be the preferred option due to its focus on user control over data, which empowers users and builds trust. The chosen model should combine the establishment of standards with the adoption of self-sovereign identity principles.

Pillar	Core principle	DV model type			Conclusion for the UK
		Centralised model	Federated model	Decentralised model	
Privacy and security	**Data security**	In centralised models, all user data is stored in a single repository managed by the central authority, which streamlines data management. However,risks of data breach or leaks are significant and focused on a single point of failure.	The federated model distributes data management responsibilities among multiple providers, with standards set centrally on security and privacy, including data minimisation. This model relies on IDPs to implement identity theft protection measures, or re-use existing measures. Strong standards on security of data in tranmission are key.	The decentralised model, leveraging blockchain technology, offers inherent security features such as immutability and transparency. By distributing data across a network, it reduces the risk of a single point of failure and enhances data integrity. Global examples of decentralised models emphasise their advantages in terms of data security – including use of a triple-blind framework to ensure data, identity and process blindness.	Both the federated and decentralised models bring benefits over a centralised model in terms of data security. A model for the UK should enshrine security throughout the process, in data at rest, by including encryption during transmission, data minimsation as a principle and the possibility to enforce triple-blind exchange when the use case allows (e.g. age verification). The model should have legal, technical and semantic standards set centrally to enforce data security. Additionally, the model should empower users to manage their data sharing by granting granular consent options to provide consent only for specific purposes.
Public trust	**Inclusivity**	Centralised models, such as government-issued identity systems, can provide widespread access to identity services, particularly when implemented at a national level. They are often mandated for participation for certain use cases, particularly access to government benefits or services.	The federated model enhances inclusivity by allowing users to choose their identity provider, enabling individuals to select providers that best meet their needs and circumstances. This model can also incorporate multiple points of verification, including government data, to increase inclusion.	The decentralised model empowers users with control over their own identities, fostering self-sovereign identity management and enhancing privacy. This approach allows individuals to manage their information independently, reducing reliance on a central authority.	The mandatory nature of service usage often associated with centralised models is likely to meet resistance in a UK context. A model for the UK should promote inclusivity and lower barriers to adoption. In a highly-banked economy such as the UK, a model with a choice between multiple financial institutions and/or government as IDP can be highly inclusive.
Legal and regulatory compliance	**Liability**	In centralised models, the central authority assumes responsibility for the integrity, accuracy and relevance of data, providing a clear point of accountability.	A federated model generally employs a shared liability model, defined through contractual agreements between IDPs and RPs. Liability is limited and only arises in cases where standards have been broken, or in cases of mis-use. This model necessitates strong governance and oversight to ensure compliance and manage risks effectively.	In a decentralised model, standarised agreements are key to regulate liability. In the Canadian model, IDPs provide data on an 'as is' basis, and RPs are presumed to use additional sources outside of the scheme to provide additional verification where required. Liability for errors or other breaches is limited, with exceptions for a party's breach of applicable law or confidentiality or its negligence.	A limited liability model, enforced through agreed, standardised contractual arrangements is preferable for the UK. Liability agreements will vary by use case, providing flexibility for highly regulated environments. Liability is explored at some length in *Section 3.3 A DV model for the UK*.

3.3 A DV model for the UK

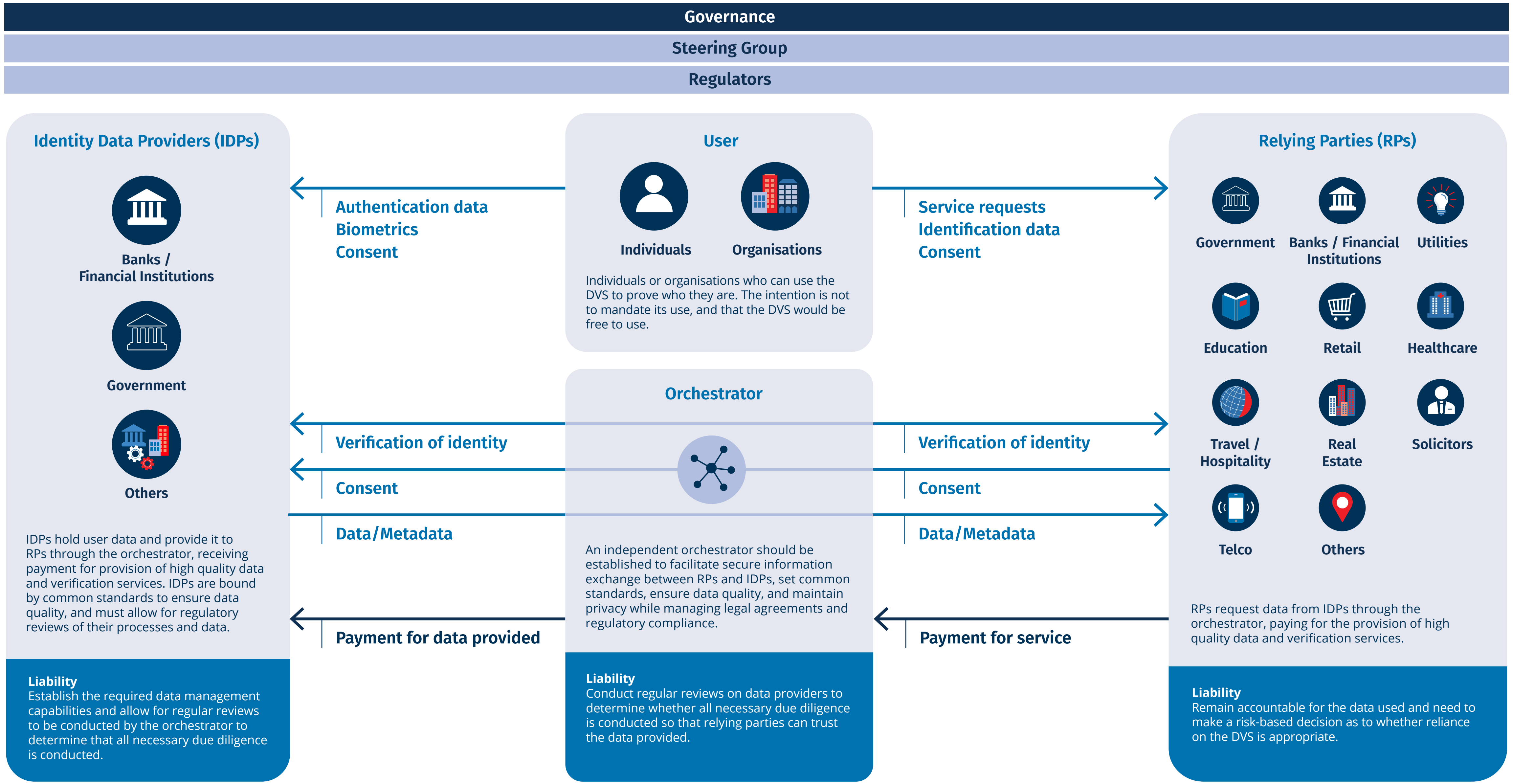
Drawing on the principles outlined in the previous section, The City of London Corporation have developed a conceptual model for a DVS tailored to the UK. This model does not strictly adhere to any single existing framework; instead, it represents a hybrid approach that integrates key elements from both federated and decentralised models while addressing the unique needs of the UK context.

The conceptual model was designed to facilitate a secure and efficient exchange of information between three key players: the RPs, Users (individuals or organisations), and IDPs.

To the right is the visual high-level design of the model. This model is intended to be illustrative and to summarise our principles-based analysis. It intends to further the discussion on adoption of a DVS in the UK. The conceptual model does not provide a definitive answer to how DV should be implemented in the UK.

A conceptual model for DV in the UK

Key: → Exchange and verification of data → Commercials



Governance

Steering Group

Regulators

Identity Data Providers (IDPs)

IDPs hold user data and provide it to RPs through the orchestrator, receiving payment for provision of high quality data and verification services. IDPs are bound by common standards to ensure data quality, and must allow for regulatory reviews of their processes and data.

Liability
Establish the required data management capabilities and allow for regular reviews to be conducted by the orchestrator to determine that all necessary due diligence is conducted.

User

Individuals or organisations who can use the DVS to prove who they are. The intention is not to mandate its use, and that the DVS would be free to use.

Orchestrator

An independent orchestrator should be established to facilitate secure information exchange between RPs and IDPs, set common standards, ensure data quality, and maintain privacy while managing legal agreements and regulatory compliance.

Liability
Conduct regular reviews on data providers to determine whether all necessary due diligence is conducted so that relying parties can trust the data provided.

Relying Parties (RPs)

RPs request data from IDPs through the orchestrator, paying for the provision of high quality data and verification services.

Liability
Remain accountable for the data used and need to make a risk-based decision as to whether reliance on the DVS is appropriate.

The conceptual model for the UK involves four key players:

Entity	Role description
Orchestrator	An independent entity, the orchestrator, should be established to facilitate information exchange. The orchestrator's role is to enable interactions between RPs and IDPs, set and enforce integration standards, ensure data quality, secure transmissions, and maintain privacy as agreed with users. This entity supports growth and adoption by additional IDPs and RPs over time, provided they meet the orchestrator's standards and requirements, as informed by regulatory bodies such as the FCA and ICO. The orchestrator's role proposed in this model extends beyond that of the orchestration service provider in the *UK digital identity and attributes trust framework*. The orchestrator in this model not only facilitates secure data exchange. It also sets common standards to ensure integration and interoperability, manages legal agreements between IDPs and RPs, conducts data quality reviews in IDPs, and provides dispute and resolution services. Organisations including financial institutions can act as both IDPs and RPs, and also have a role in the orchestrator, as outlined in more detail in this and subsequent sections.
	Further details below on the role of the orchestrator, including key points for further clarification after the publication of this report: • The orchestrator should be established as an independent entity by a public-private partnership. Its ownership must be structured in a manner that avoids conflicts of interest and does not discourage participation from RPs or IDPs due to competition. • The orchestrator will require investment for setup but should be funded on an ongoing basis by charges collected from RPs requesting ID verification or datasets. • The orchestrator will define the data requirements and semantics for information exchange between the IDPs and the RPs. This will allow for scalability and integration of new IDPs and RPs over time, by setting and enforcing common standards. • The orchestrator will conduct regular reviews on IDPs to determine that all necessary due diligence is conducted, and data management capabilities are in place so that RPs can trust the data provided. Additional oversight and reviews to be conducted by independent regulatory bodies such as the FCA and ICO. • The orchestrator will establish processes to conduct checks on RPs willing to integrate, to confirm that the firm is who they claim to be and do what they say they do. It will also conduct ongoing reviews of RPs' processes to ensure compliance with agreed standards and prevent misuse of data. • The orchestrator will maintain the scope and definition of use cases for which the DVS can be used, including the level of identity assurance and verification required for each. In some more complex use cases, multiple identity providers, including government (e.g. HMRC, OneLogin, Companies House), may be required. The set of valid use cases will expand over time and can vary in terms of complexity and level of verification required. • The orchestrator will establish a process for identifying and addressing operational issues raised by RPs and IDPs and maintain an effective process for resolving them. • **The orchestrator will not store data.** • Redundancy in infrastructure and processes will be key to avoid the orchestrator becoming a single point of failure in the DVS. • The orchestrator itself is not an IDP however there may be IDPs with an investment or governance stake in the orchestrator. • The orchestrator ensures that data sharing with RPs is subject to users' consent and common data privacy standards. • Given its role as a standard setter, managing legal agreements and commercial arrangements for participants, and acting as an infrastructure operator, a robust governance structure is required. This includes exploring the potential involvement of the FCA to ensure robust oversight and compliance with financial regulations, and the potential involvement of the ICO to regulate and enforce data protection laws such as the UK GDPR and the *Data Protection Act 2018*.

Entity	Role description
Relying Parties (RPs)	Entities that request data or verification from IDPs through the orchestrator. They pay to use the service and must obtain user consent for each use. RPs play a key part in promoting usability as users interact directly with the relying parties' interfaces, which in turn exchanges data with the orchestrator to enable the operation of the DVS. • RPs remain ultimately accountable for the data used and need to make a risk-based decision as to whether reliance on the DVS provided by the orchestrator is appropriate. Reliance is governed by common standards and contractual agreements to which all RPs and IDPs must adopt. • RPs, informed by relevant legal and regulatory requirements, will define upfront their data requirements for each use case and agree on them with the orchestrator so they can be configured and provided by the orchestrator on an ongoing basis. • RPs have the option to maintain their own identity verification processes, should they decide not to utilise the service provided. Adoption will depend on the level of maturity and quality of the service offered by the orchestrator.
Identity Data Providers (IDPs)	IDPs hold user data and can provide verification of the data, or the data itself, to RPs through the orchestrator. IDPs will be paid by the orchestrator when providing data in response to the requests of RPs. They will also have the following specific obligations: • Make the necessary modifications to integrate with the orchestrator, ensuring alignment with the data requirements and semantics of the service. • Confirm the identity of the user against their own data when requested. Provide the required dataset to the RP if the user has given consent and it does not conflict with the privacy terms agreed between the user and the data provider. • To maintain integration with the orchestrator, data providers must uphold an adequate level of data quality and due diligence processes. They must allow for regular reviews to be conducted by the orchestrator to ensure that all necessary due diligence is performed. • Address data quality issues raised by the orchestrator, and provide copies of verification data, documents or CDD information when required. • Big tech firms continue to develop technology to improve accuracy in identity verification, which will benefit institutions that act as IDPs in this model. By adopting improved technology, data providers will be able to offer a more secure service to RPs and users. This will elevate the entry criteria for integrating into the DVS, preserving or enhancing its level of trust across all participant entities and users. • While the focus of this report is on the FPS sector, IDPs are not restricted to financial institutions. Telcos are examples of organisations that could act as both IDP and RP. IDPs such as streaming services and food delivery providers are examples of IDPs that might not be sufficient on their own to verify a user. However their presence in a user's profile of IDPs can increase the level of assurance in the user's authenticity, and this could be used to combat mule accounts being verified by the DVS, for example.

Entity	Role description
User	To use the DVS in this model, users should have successfully completed identity verification with at least one IDP. For some use cases, verification against multiple IDPs may be required, including government data. Once registered, users have the autonomy to select the IDP for each request (if they meet the standards required by the orchestrator), ensuring self-sovereignty. Data sharing with RPs requires user consent on a case-by-case basis. Stronger authentication of the users will be enabled via the use of biometrics. Whilst using the DVS wouldn't be mandated for users, a set of use cases that deliver sufficient value and ease of use need to be developed to drive user adoption and contribute to surpassing the tipping point of critical mass adoption.

Spotlight on structure of orchestrator

When considering the structure of the orchestrator, we have analysed the advantages and potential risks associated with two options in the table below. In either approach to the orchestrator, there remains a commercial incentive to participate as an IDP or RP – i.e. fees will still be charged for provision of high quality, regulatory-compliant data. Additionally, a role as an IDP or RP does not exclude an organisation from becoming stakeholders of the orchestrator in either model. In both models, the service remains free for users.

Whilst these possibilities have been analysed and the potential risks and advantages documented, determining which option should be adopted is a key next step that potential stakeholders will need to consider to ensure the decision aligns with their purposes, policies, and objectives.

The structure of the orchestrator should be guided by the principles for the DVS outlined in this report. To achieve widespread adoption of the DVS, it is essential to promote growth and build public trust, with a focus on security, privacy, and compliance. Government involvement will be crucial to catalyse adoption and encourage use of the DVS. We believe a public-private partnership to be the preferred approach. It is important to note that potential investors in the orchestrator may also serve as IDPs, RPs, or fulfil a combination of these roles. Additionally, the investment requirements for establishing and maintaining the orchestrator should be clearly defined. The role and mandate of government-owned investment vehicles, such as the National Wealth Fund (NWF), should be considered in light of the pressing need for the UK to invest in digital infrastructure.

Option	Option description	Advantages	Potential risks
Return for stakeholders*	Revenue earned by the orchestrator generates a return for stakeholders / investors, in addition to covering the costs of infrastructure and ongoing maintenance.	A commercial incentive that generates return on investment can spur investment in the orchestrator and create incentives for innovation. There is also an incentive to enforce strong standards in security, interoperability and user experience, to further adoption.	A balance must be struck between financial incentives, quality of service and wide adoption of the service by RPs. Fees must be set at a level that allows for adoption and growth of the service.
Self-sustaining*	Revenue generated by the orchestrator is intended to return initial investment, plus cover the costs of infrastructure and ongoing maintenance. There is no ongoing return to stakeholders.	Stakeholders can recoup their initial capital investment. Non-profit focus can increase level of trust amongst some users who may have concerns.	Incentives for investment, innovation and growth are less obvious and will require a mandate for participants to reinvest ongoing revenue into innovation, service quality and growth. Accountability for ongoing maintenance and performance is more diffuse.

Spotlight on liability

Liability within this DV model is intended to be limited and applies only under specific conditions related to the IDP or RP. Liability considerations will emerge in instances such as standards violations, misuse, and negligence, with the extent of liability calibrated to the identity assurance level pertinent to each use case or dataset - differentiating, for example, between age verification and KYC use cases. In use cases where a dataset is exchanged for consumption by the RP (e.g. KYC use case), the RP remains accountable for the data used and must make a risk-based judgment regarding reliance on the DVS. This process is bolstered by verifiable or audited evidence of IDP operations and processes, which are prerequisites for IDP certification. The orchestrator and regulatory bodies are tasked with conducting regular assessments of IDPs to confirm comprehensive due diligence, thereby enhancing RPs' confidence in the data quality provided. RPs are also mandated to implement robust and verifiable measures to safeguard user data shared via the DVS, alongside establishing reporting protocols for any data breaches. Furthermore, clear recourse mechanisms must be available to users in cases of data misuse.

International models for DV offer valuable insights into liability regimes. For instance, the Canadian Verified.me service limits liability for damages that can be incurred by IDPs arising from incorrect or outdated data, unless the IDP has acted illegally or negligently. In this model, all identity data is presented 'as is,' compelling RPs to employ supplementary methods for data acquisition, validation, or verification beyond the Verified.me service.[25] The overarching objective of the DV model articulated in this report is to reduce compliance costs and overhead, and thus limit additional checks that may be required outside of the DVS. Instead, such checks are envisioned to occur within the DVS, using electronic verification against multiple data sources to ensure a high level of identity assurance.

A critical next step in the design and implementation of a DVS involves an in-depth exploration of the proposed liability regime and strategies for limiting liability through the provision of enhanced identity assurance levels regarding data sourced from IDPs.

Spotlight on data protection

The role of the proposed orchestrator aligns with the UK GDPR, safeguarding privacy and adhering to requirements to protect against data breaches and misuse. A comprehensive analysis and ongoing alignment with the UK GDPR are required throughout the design and implementation of the orchestrator. Under the proposed model, it is considered a data processor as it processes personal data on behalf of the data controllers, which are the RPs and IDPs. The orchestrator does not decide the purposes and means of processing the data on a case-by-case basis; these decisions are made by the data controllers. Instead, the orchestrator's role is to facilitate secure information exchange, establish common standards for data sharing, and ensure compliance with regulatory requirements.

Parallels with existing examples in the UK

The proposed orchestrator draws parallels with existing and relevant services already operational in the UK, such as Pay.UK and the API Gateway in Open Banking. Each of these entities plays an important role in managing the infrastructure, governance, standards and legal agreements required for effective collaboration between different financial institutions on payments and financial data sharing.

This section examines the shared elements of the orchestrator, Pay.UK, and the API Gateway to clarify the orchestrator's role in the proposed model.

Similar to Pay.UK and the API Gateway, the orchestrator serves as an intermediary between participating entities. Operating in the background, it facilitates interactions between diverse entities, enhancing the user experience in their daily interactions with service providers.

[25] Digital ID & Authentication Council of Canada (2020). *DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment.*

* Based on City of London Corporation analysis of international markets, under a commercial option, we could expect a customer adoption rate of between 40 and 90%.

** No developed economy uses a non-profit orchestrator - instead preferring a government or commercial approach. The MOSIP model is deployed in some developing economies.

- While Pay.UK coordinates the integration of various payment schemes, including Bacs, Faster Payments, and Cheque and Credit Clearing, by establishing rules and standards to ensure compliance with regulatory requirements, the orchestrator performs a similar role but for data providers. Pay.UK enables users to access multiple payment options through a single interface, and the orchestrator allows users to choose from various data providers for identity verification and data sharing via RPs' user interfaces.
- The API Gateway in Open Banking facilitates the sharing of financial information such as transactions and balances, between financial providers. The orchestrator allows transfer of identification data and allows DV of users. By incorporating verification, the orchestrator will enable the development of new use cases based on trust, including comprehensive KYC onboarding, document signing, account-to-account payments, and pave the way to integrate other sectors, such as telecommunications, healthcare, and education.

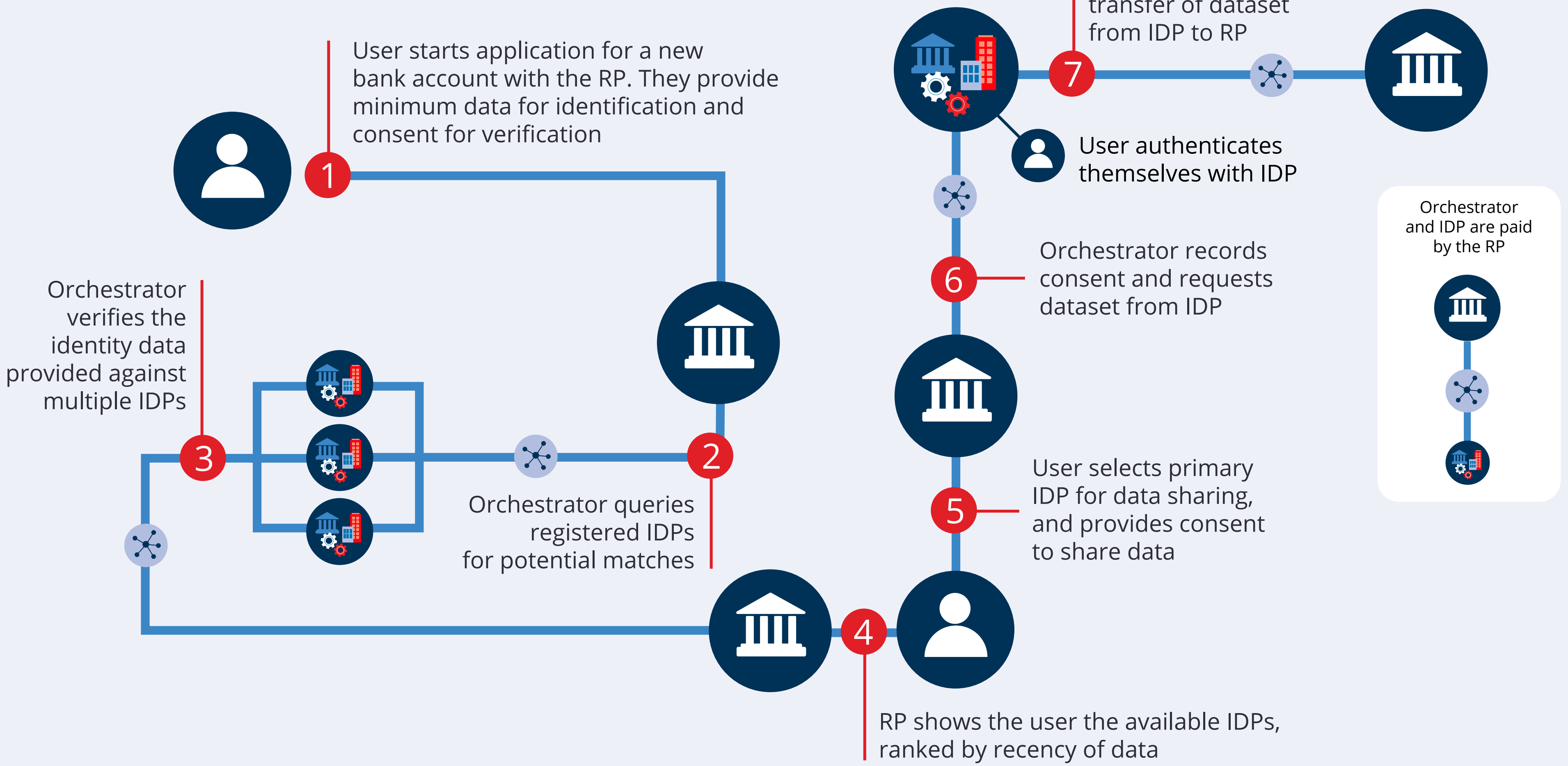
Bringing the model to life – KYC use case

Building on the conceptual model, we now explore its practical application through a use case: customer onboarding and KYC in financial institutions. This example demonstrates how the model's principles are implemented in a real-world scenario, highlighting the roles and interactions of the orchestrator, users, RPs, and IDPs. The benefits of using a DVS in KYC and onboarding include enhanced efficiency, reduced fraud risk, compliance with regulatory requirements, and improved customer experience by streamlining the verification process. Additionally, there is a commercial incentive for both IDPs and RPs. IDPs can be paid for provision of high-quality data, while RPs can reduce the cost of onboarding new customers as they have pre-verified KYC data provided to them.

The process involves identity verification, dataset transfer, and payment, showing how information exchange will occur.

Key: Orchestrator | Users: Individual | Relying Party (RP): Bank / Financial Institution | Identity Data Providers (IDP): Banks / Financial Institutions

Enhancing KYC processes using the Digital Verification Service



1 User starts application for a new bank account with the RP. They provide minimum data for identification and consent for verification

2 Orchestrator queries registered IDPs for potential matches

3 Orchestrator verifies the identity data provided against multiple IDPs

4 RP shows the user the available IDPs, ranked by recency of data

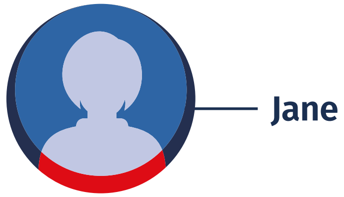
5 User selects primary IDP for data sharing, and provides consent to share data

6 Orchestrator records consent and requests dataset from IDP

User authenticates themselves with IDP

7 Orchestrator facilitates transfer of dataset from IDP to RP

Orchestrator and IDP are paid by the RP


Jane

The sequence of steps show Jane opening a new bank account with Future Bank. This is a fictitious visualisation of the use case on the previous page.

Step 1: Jane is opening a new bank account with Future Bank, a RP registered with the DVS. Jane has no prior relationship with Future Bank or the DVS.

Step 2: Jane can choose to onboard manually by entering details and uploading documents, or she can connect to an existing provider to onboard using the DVS.

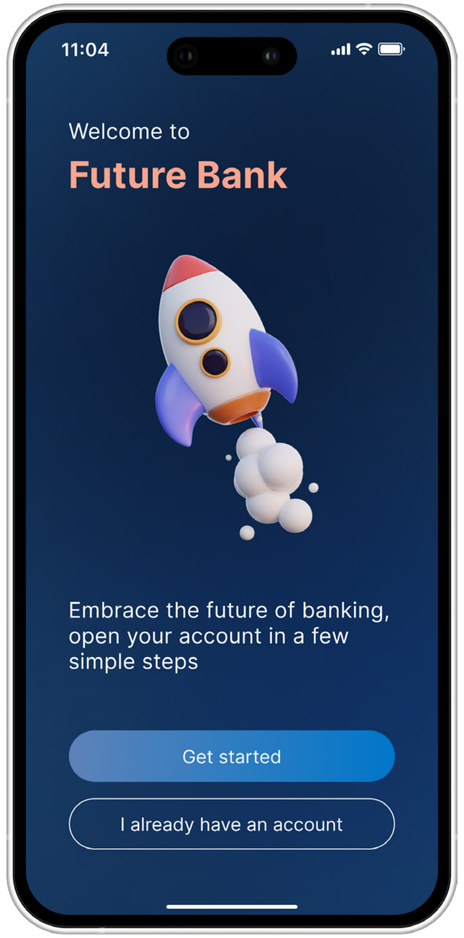
Step 3: Jane inputs basic identity information for the orchestrator to search her profile. For organisations, similar data points like Full Legal Name and Legal Entity Identifier are used. Verification with multiple IDPs may be required at this point, based on the identity assurance level needed.

Step 4: The orchestrator queries IDPs certified to provide KYC data, using the data Jane provided. Potential matches are displayed, ranked by recency. Jane selects One Bank as the most recent source, with an additional authentication step still required.

Step 5: Jane reviews the data points that she is consenting to share, without seeing values until authenticated with One Bank. Consent is provided by Jane for sharing, and this is recorded by the orchestrator.

Step 6: Once consent is received to share the data, the orchestrator informs One Bank, which must independently authenticate Jane to confirm the legitimacy of the data-sharing request. A notification is sent via the One Bank app for authentication.

1


11:04

Welcome to

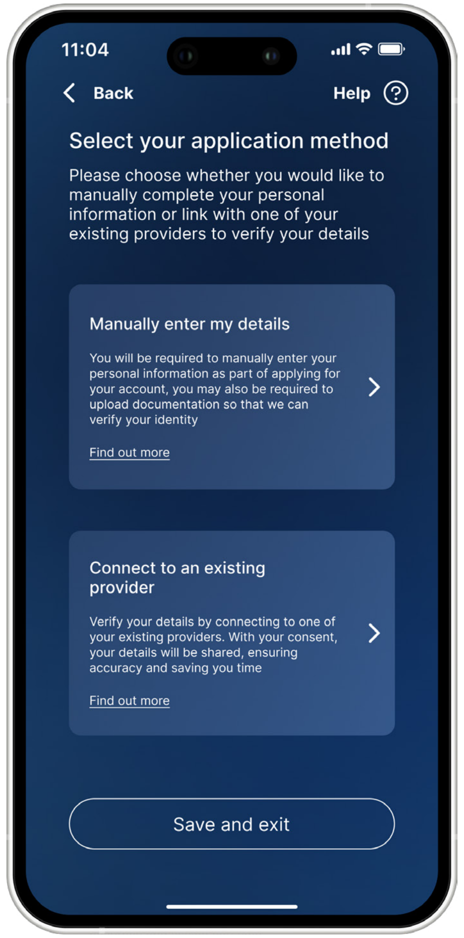
Future Bank

Embrace the future of banking, open your account in a few simple steps

Get started

I already have an account

2


11:04

Back Help ?

Select your application method

Please choose whether you would like to manually complete your personal information or link with one of your existing providers to verify your details

Manually enter my details

You will be required to manually enter your personal information as part of applying for your account, you may also be required to upload documentation so that we can verify your identity

Find out more

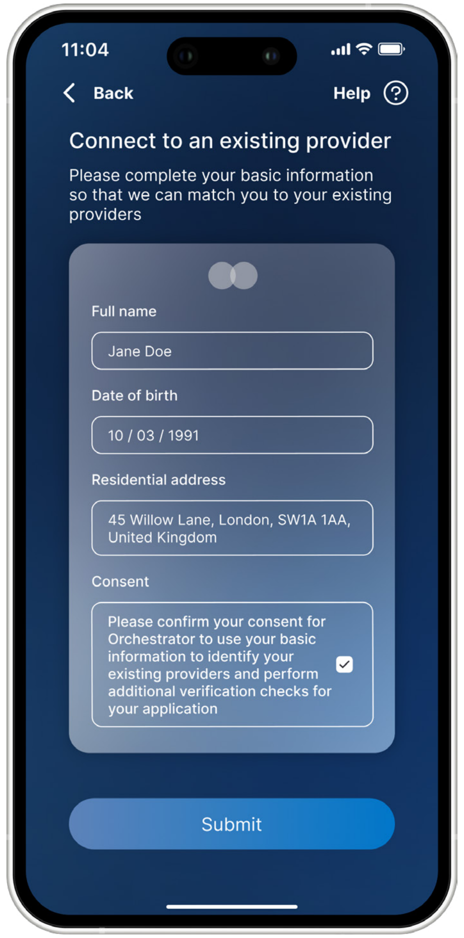
Connect to an existing provider

Verify your details by connecting to one of your existing providers. With your consent, your details will be shared, ensuring accuracy and saving you time

Find out more

Save and exit

3


11:04

Back Help ?

Connect to an existing provider

Please complete your basic information so that we can match you to your existing providers

Full name: Jane Doe

Date of birth: 10 / 03 / 1991

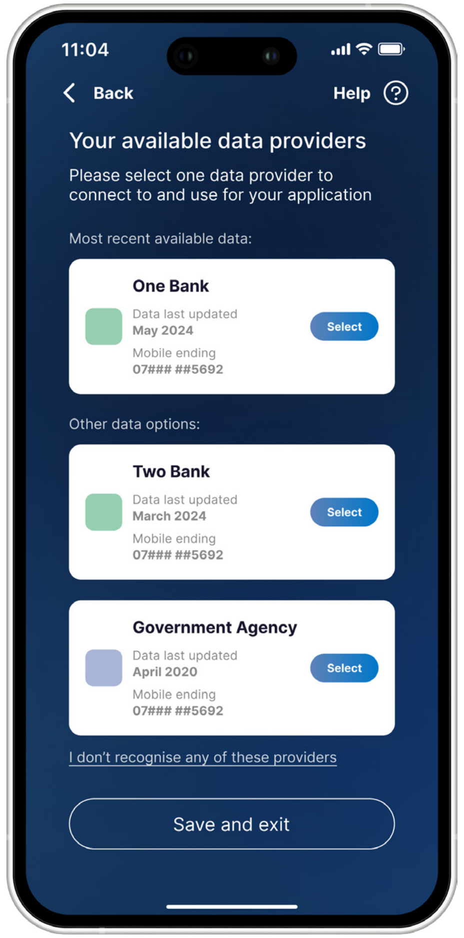
Residential address: 45 Willow Lane, London, SW1A 1AA, United Kingdom

Consent

Please confirm your consent for Orchestrator to use your basic information to identify your existing providers and perform additional verification checks for your application ☑

Submit

4


11:04

Back Help ?

Your available data providers

Please select one data provider to connect to and use for your application

Most recent available data:

One Bank
Data last updated May 2024
Mobile ending 07### ##5692
Select

Other data options:

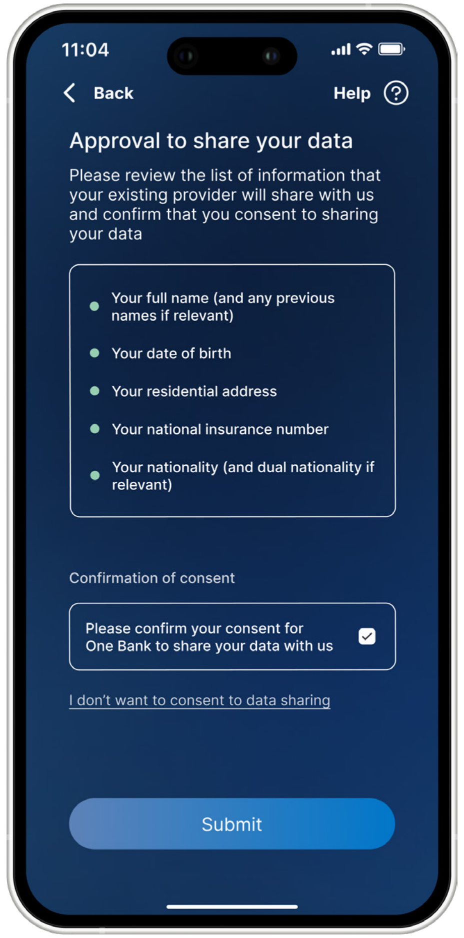
Two Bank
Data last updated March 2024
Mobile ending 07### ##5692
Select

Government Agency
Data last updated April 2020
Mobile ending 07### ##5692
Select

I don't recognise any of these providers

Save and exit

5


11:04

Back Help ?

Approval to share your data

Please review the list of information that your existing provider will share with us and confirm that you consent to sharing your data

- Your full name (and any previous names if relevant)
- Your date of birth
- Your residential address
- Your national insurance number
- Your nationality (and dual nationality if relevant)

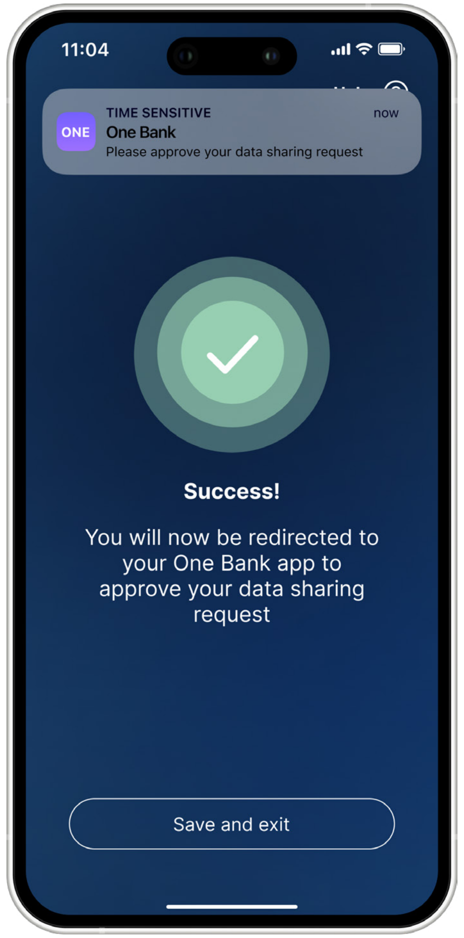
Confirmation of consent

Please confirm your consent for One Bank to share your data with us ☑

I don't want to consent to data sharing

Submit

6


11:04

TIME SENSITIVE now
ONE One Bank
Please approve your data sharing request

Success!

You will now be redirected to your One Bank app to approve your data sharing request

Save and exit

Step 7: Jane authenticates through the One Bank app using biometrics or a PIN. Biometric data is not stored by the orchestrator. One Bank confirms authentication to the orchestrator.

Step 8: Jane reviews the data that she is about to share, and provides explicit consent to share. If the data is incorrect or out of date, Jane can update it with One Bank before sharing. This allows for ongoing due diligence on KYC data via the DVS. Consent for data sharing is case-by-case. Future sharing will require explicit consent from Jane.

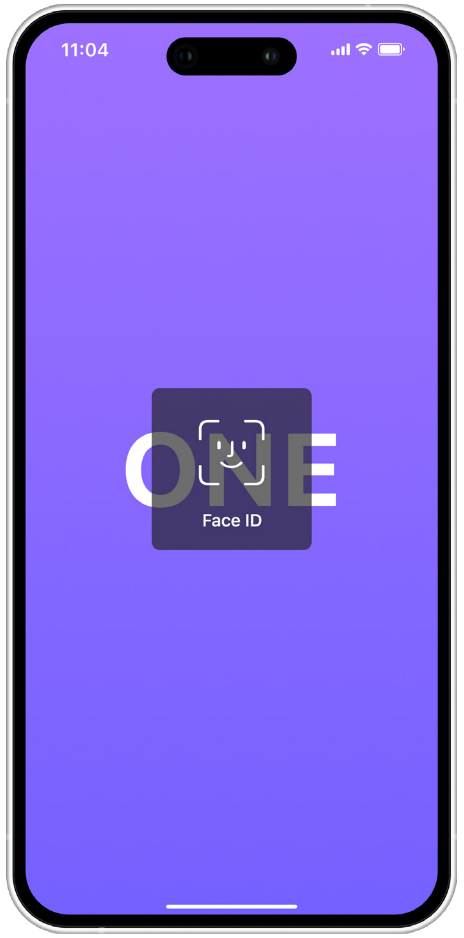
Step 9: After successful authentication and verification with One Bank, Jane is now registered with the DVS and data sharing has been approved. A fee is paid by Future Bank (RP) to the orchestrator and One Bank (IDP). Jane is re-directed back to Future Bank.

Step 10: Jane is now onboarded to Future Bank, without the need to provide detailed KYC data or documentation.

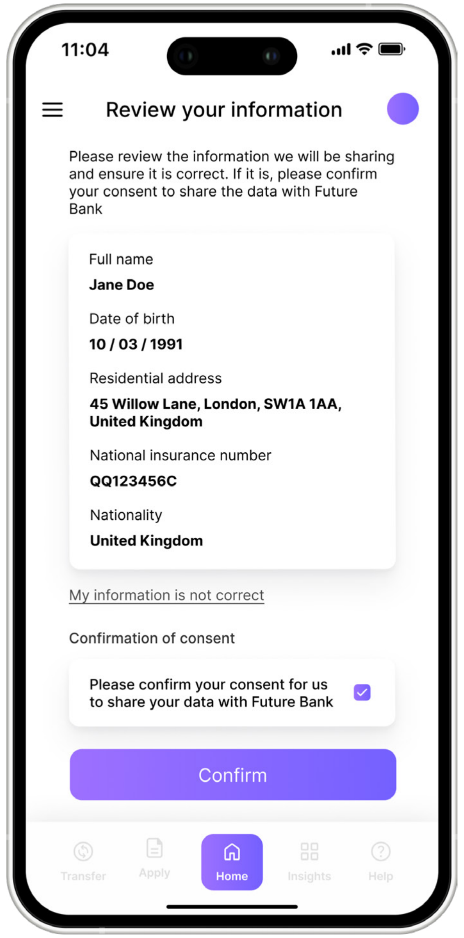
All data exchanges described above would be conducted in encrypted form. The orchestrator would not have access to the data being exchanged, as it would remain encrypted in transmission. The RP will have access to the data if the use case requires it. In this use case, the bank receiving the information needs to access the dataset to complete the KYC profile of the new customer.

All data exchanges described in this use case will include metadata to ensure transparency and accountability. Metadata provides context about data records, including their characteristics, origin, structure, usage, as well as the consent and privacy terms agreed with users. It helps manage data exchange and consumption by providing origin details for records, which may be required for regulated entities like banks. It also includes privacy preferences and user consent, ensuring compliance and contributing to the building of trust in the service.

7



8



Review your information

Please review the information we will be sharing and ensure it is correct. If it is, please confirm your consent to share the data with Future Bank

Full name
Jane Doe

Date of birth
10 / 03 / 1991

Residential address
45 Willow Lane, London, SW1A 1AA, United Kingdom

National insurance number
QQ123456C

Nationality
United Kingdom

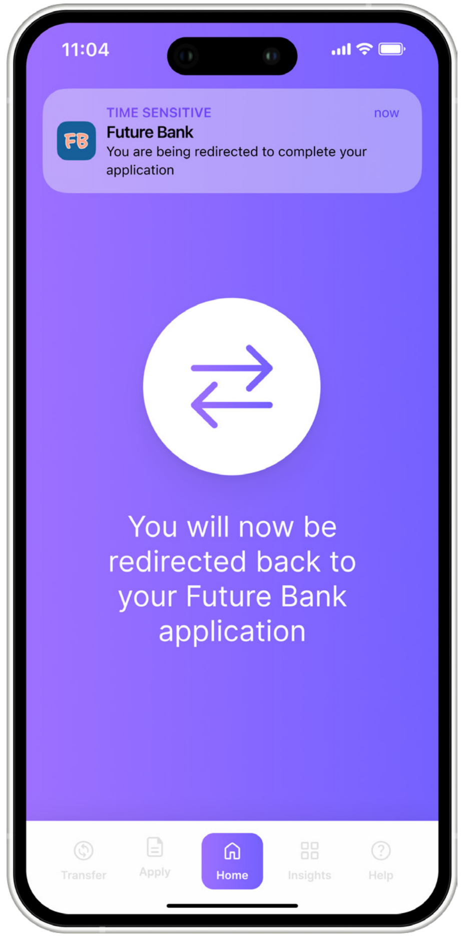
My information is not correct

Confirmation of consent

Please confirm your consent for us to share your data with Future Bank ☑

Confirm

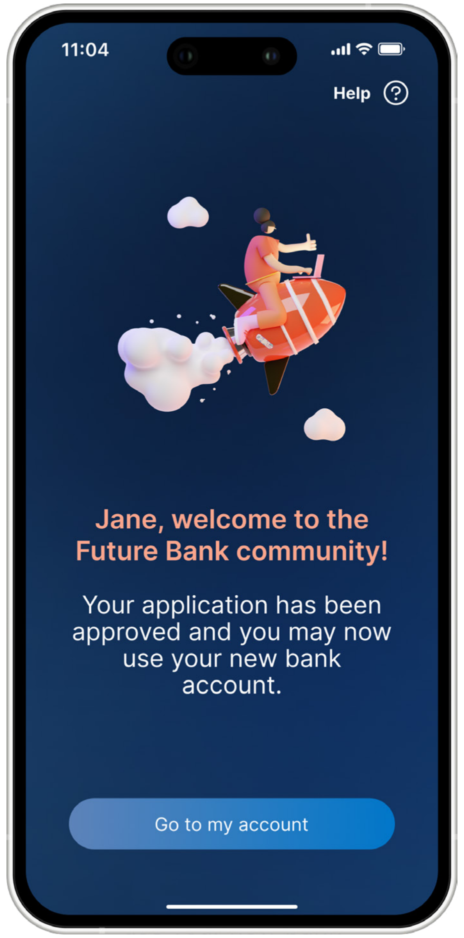
9



Future Bank
You are being redirected to complete your application

You will now be redirected back to your Future Bank application

10



Jane, welcome to the Future Bank community!

Your application has been approved and you may now use your new bank account.

Go to my account

Model definition conclusion

To conclude, we've defined a conceptual model, outlined roles and responsibilities, and presented a use case along with its benefits to bring the model to life. This model aims to advance the conversation on establishing a DVS for the UK by leveraging industry knowledge, research, and engagement with stakeholders in the area. It was developed based on a principle-driven approach that focuses on public trust, legal and regulatory compliance, privacy and security, and adoption and growth. By implementing this model, users, RPs, and IDPs will benefit from more streamlined processes across financial institutions and other sectors, ultimately driving economic growth and supporting innovation.

4. Considerations and recommendations

To advance work on the proposed DV model for the UK, the City of London Corporation has outlined below our considerations and recommendations that we believe will progress this effort across government and the financial and professional services industry.

4.1 Considerations for adopting and scaling DVS

Choose penetrating use cases which will drive adoption and power growth

The successful adoption of DVS requires a critical mass of users, often driven by high-quality use cases that drive users to utilise the service frequently. Giving the population a clear reason to use the service – and regularly – will drive adoption. As one expert noted, "we need a system built for multiple use cases. if not public-private from the get-go, it won't work. We need the involvement of multiple stakeholders to get to bigger use cases." Prioritising high value use cases which make a process easier or quicker for users will highlight the benefits of DV to the general public. Placing customer experience at the heart of use case selection will catalyse adoption.

In countries that have adopted DV, we see clear examples of use cases which have driven adoption and those that have been less successful. For example, in Estonia, which has 84% adoption rate[26] use cases range from voting, access to healthcare, banking related use cases and authentication of digital signatures. Similarly, Finland's eID proposition, which has 98% adoption rate,[27] is used frequently as it is woven into day-to-day interactions with use cases spanning banking (including mortgage renewals and account opening), age verification and e-government services. In particular, the Finnish system is known for its user friendliness, which has driven high adoption levels due to its convenience and ease of use. A recent report by the Finnish Transport and Communications Agency found that 88% of consumers prefer logging into a service using the strong eID as they find it to be a safer and more user-friendly option.[28] Key use cases to drive adoption in the FPS sector in the United Kingdom focus on fraud prevention and reducing the time and inconvenience of customer verification (e.g. KYC) within the banking sector. Both of these areas currently cost the FPS sector and broader UK economy significant amounts each year, with fraud costing the UK economy £190bn annually.[29] Within Financial Services, fraud cost UK banks £1.2bn in 2022[30] and UK banks spent £34.2 billion each year on financial crime compliance to tackle fraud related issues.[31] Even a small reduction in the costs associated with fraud, financial crime and identity checking would be beneficial for banks. For consumers, avoiding delays when registering with a new financial services provider, transacting online or even purchasing age restricted products would quickly prove benefit, in addition to the enhanced security when transacting online.

In the longer-term, DVS could be expanded into other industries and enhance the efficiency of transactions that currently take significant amounts of time and result in inefficiencies. For example, DV has the potential to significantly improve housing transactions within

[26] Signicat (2024). *The State of Digital Identity in Europe 2024-2025.*
[27] See reference 26
[28] Signicat (2021). *Digital eIDs in the Nordics.*
[29] See reference 20
[30] UK Finance (2023). *Annual Fraud Report 2023.*
[31] LexisNexis Risk Solutions (2024). *The True Cost of Financial Crime Compliance 2024.*

> “Scalability is equally important; the service must be designed to accommodate growing user bases and increased transaction volumes without sacrificing performance or security.”

the UK, both for the purchase and rental of properties. By implementing these services, buyers and renters could streamline the verification process associated with all property transactions, reducing the time and complexity associated with traditional methods. For home purchases, DV could facilitate quicker and more reliable checks on a buyer’s financial status, credit history and identity, expediting both mortgage approvals and anti-money laundering checks required by solicitors and conveyancers as well as improving security during the homebuying process by reducing the need to share sensitive documents with multiple parties.

Recent government initiatives announced to improve the home purchasing journey, including enhanced digitisation,[32] could link to DVS, paving the way for their adoption beyond FPS. Additionally, in the rental market, DV can simplify right-to-rent checks, allowing landlords and letting agents to swiftly confirm a tenant’s eligibility to reside in the UK, while also protecting against identity fraud. Additionally, DVS could act as an enabler to increased entrepreneurship in the UK, streamlining the processes of identity validation, credit assessment, and compliance checks, which are often barriers for new business ventures. For example, current business current account onboarding and business credit or loans require confirmation of individual directors’ identities and creditworthiness, a process that can range from weeks to months under the current manual system depending on the number of directors and their financial situation. In quickly verifying business directors’ identities, entrepreneurs are able to access capital more quickly and are able to spend more time building their business, rather than on bureaucracy. This benefits both individual companies as well as the broader economy by allowing more businesses to flourish and create jobs.

Ensuring interoperability and alignment with other DVS

Interoperability with international Digital ID and DV services is crucial for the success of a UK DV, as it facilitates seamless cross-border interactions and enhances the overall user experience. In an increasingly globalised world, individuals and businesses frequently engage in transactions and communications that span multiple jurisdictions. By ensuring international interoperability, the UK can promote greater accessibility, security, and trust in digital services. This interoperability not only supports international travel, trade, and commerce but also fosters collaboration in combating identity fraud and enhancing cybersecurity. Additionally, the long-term sustainability of the DVS hinges on its ability to adapt to evolving technologies and user needs, ensuring that it remains relevant and effective over time. Scalability is equally important; the service must be designed to accommodate growing user bases and increased transaction volumes without sacrificing performance or security. Ultimately, a robust and interconnected DV ecosystem will empower citizens and organisations to navigate the digital landscape with confidence, while positioning the UK as a leader in innovative verification services on the global stage.

Interoperability with international services and regulatory frameworks

The European Union’s eIDAS regulation establishes a common EU-wide framework for Digital ID and DV, with the aim of facilitating cross-border transactions. Within the EU regulation, regulations set out uniform standards, specifications and procedures for technical implementation of the Digital ID wallets. These standards include data formats required for cross-border use and measures to ensure the reliability and security of the wallets. This allows each Member State to develop their wallets in a way that is interoperable and accepted across the EU, whilst protecting personal data and identity. In the EU system, data is stored locally on the wallet, with users controlling what information they share and with zero tracking or profiling built into the wallets. Wallets are also designed to have a built-in privacy dashboard, giving complete transparency to users on what data is shared with whom and how.

Any DVS implemented in the UK should align to international best practice and standards to promote interoperability, and to enable a higher level of trust in international trade and cross-border payments.

Company and SME DV

The City of London Corporation, as a response to the Kalifa Review of UK FinTech, co-founded (with HM Treasury) the Centre for Finance, Innovation and Technology in 2023. CFIT’s coalition model brings together key industry players – including innovative technology firms and incumbent financial services firms – to develop solutions to shared challenges. CFIT have recently brought together a coalition of over 70 organisations across industry, policymakers, academia and consumer groups to consider how corporations might be more effectively verified to combat economic crime. As part of their work, CFIT’s coalition has defined and mapped datasets to create a framework for a secure reusable Digital Company ID for bank onboarding; developed a proof-of-concept on Digital Company ID, validated by SMEs and financial institutions; identified safeguards for emerging risks and generated a set of actionable insights for industry, government and regulatory stakeholders.

As UK consumer DV develops, it should be ensured that the technology, standards, mechanisms and legal and regulatory frameworks are as similar as possible to those used for any Digital Company ID.

[32] GOV.UK (2025). *Home buying and selling to become quicker and cheaper.*

4.2 Recommendations for establishing DVS in the UK

Providing legal and regulatory clarity

The *Data (Use and Access)* Bill, currently progressing through Parliament, establishes a comprehensive legal framework for digital verification in the UK, governing the use, sharing, and access to personal data. This legislation mandates the publication of a 'trust framework' and the creation of a registry and trust mark for accredited Digital ID and attribute services, including DVS. It also facilitates information sharing between public authorities and registered organisations to conduct identity and eligibility checks for the public. While the Bill is foundational for DV, further clarity is essential for the public sector, particularly the FPS sector, to fully adopt DV.

A well-defined regulatory framework outlining specific guidelines and requirements for organisations involved in DV is crucial. As one expert emphasised "there is a need for a strong, well defined regulatory framework that details uniform data standards to drive consistency". Under the *Data (Use and Access)* Bill, key terms such as Data Holder, Data Subject, Data Points, Data Standards/ Trust Framework, Authorised Third Parties, Implementation Timelines, and Regulator must be clearly specified before DV can be realised. Industry stakeholders are unlikely to invest in developing DVS without clarity on these terms and their associated roles and responsibilities. Moreover, the establishment of detailed technical standards in collaboration with industry stakeholders will enhance clarity regarding the requirements for services developed by financial institutions, ensuring that services are interoperable, secure, and user-friendly.

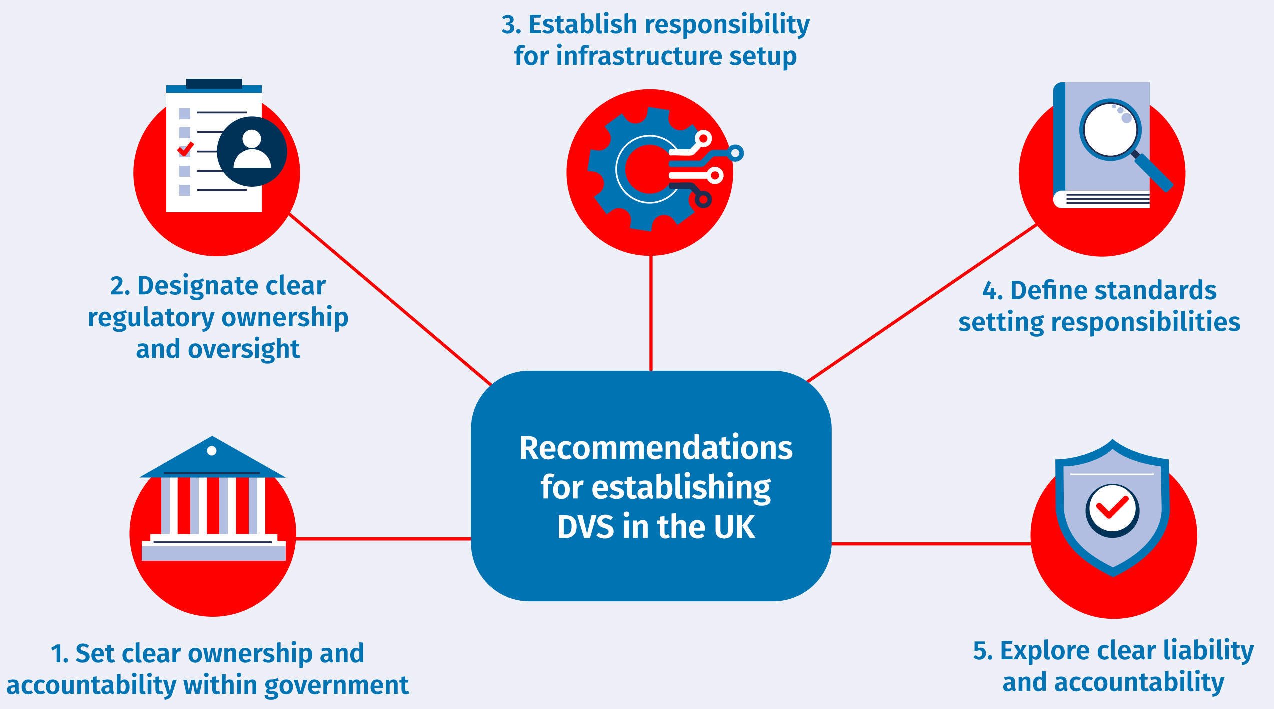
Advancing the DV model

To advance the proposed DV model in this paper, key areas underpinning the proposed orchestrator, which plays a central role in the model, need to be further developed. This involves establishing clear regulatory ownership and oversight, defining responsibilities for infrastructure setup and standards, and ensuring clear liability and accountability for its operation, as outlined in the following recommendations:

1. Set clear ownership and accountability within government: The adoption of DV in the UK has previously been impeded by the absence of a cohesive strategy and a designated owner within government. A successful implementation requires a comprehensive strategy and steering group that promotes inter-agency collaboration and stakeholder engagement across government, regulators, and industry, along with a flexible roadmap that adapts to technological and policy changes. One government department should be tasked with coordinating the implementation of DV in the UK to provide a clear owner. The Office for Digital Identities and Attributes (OfDIA) could offer guidance and support on DV implementation alongside its current work, while maintaining a robust trust framework and standards. A steering group should support the design and implementation, consisting of other relevant government departments, alongside support from the private sector. From government, the Cabinet Office (CO), The Department for Science, Innovation and Technology (DSIT) and HM Treasury (HMT) could all take on a role in the Steering Group.

2. Designate clear regulatory ownership and oversight: While the *Data (Use and Access)* Bill lays the groundwork for DVS in the UK, further actions are necessary to translate the Bill's provisions into a functional DVS. This will primarily occur through regulatory requirements derived from the legislation. An expert highlighted the importance of clear roles and responsibilities for regulators. He mentioned that "regulators should focus on ensuring a balanced approach to challenges and providing clarity on oversight and liability early on".

Clear regulatory responsibility should be designated to oversee the proposed DVS in the UK. Given the initial focus on the FPS sector as a primary use case and the role of banks as IDPs, the FCA may be a suitable candidate for this role. The FCA has indicated that Digital ID authentication and verification could unlock significant economic benefits, positioning it well to oversee a DVS, particularly as it pertains to financial institutions and financial data. Additionally, the ICO could play a role in ensuring the security, resilience, and data protection aspects of DV, especially as it expands beyond the FPS sector.



Recommendations for establishing DVS in the UK

1. Set clear ownership and accountability within government

2. Designate clear regulatory ownership and oversight

3. Establish responsibility for infrastructure setup

4. Define standards setting responsibilities

5. Explore clear liability and accountability

3. Establish responsibility for infrastructure setup: The establishment of infrastructure within the proposed service will likely be completed through a public-private partnership between a government entity and industry. However, a clear owner is needed for the central infrastructure. Responsibilities may include operating the required applications and infrastructure to facilitate data exchange between participants across financial services and beyond, maintaining this infrastructure, and providing technical support.

4. Define standards setting responsibilities: It is essential to define the technical and semantic standards that must be adhered to within any proposed DV model. It is recommended that an independent body representing a consortium of financial industry participants (IDPs and RPs) be tasked with defining data formats and standards for technical integration among different participants. Given the speed of change in the area, there will be an ongoing need to review and update technical and semantic standards, they ensure they remain fit for purpose and aligned to the strategic outlook of the DVS. Initially funded by industry and a government entity, this body could become self-sustaining as revenue is generated from information sharing.

5. Explore clear liability and accountability: A critical next step in the design and implementation of a DVS involves an in-depth exploration of the proposed liability regime. Strategies for limiting liability through the provision of enhanced identity assurance levels on data sourced from IDPs will be key. Liability calibrated to use cases is recommended. The liability regime proposed in this report must be expanded upon, tested with regulators and industry participants and explicitly defined in any further DV regulations.

> “Participation in the DVS enables banks to utilise the investments made in Open Banking technology including APIs.”

Incentives to get involved

There should be a clear incentive for financial institutions to participate in a DVS. As one expert emphasised “Banks would want to see a clear compensation model to be incentivised to be a part of the verification system”. These could include the opportunity to commercialise the data currently held by financial institutions by providing it, only with user consent, to RPs in exchange for a fee. This enables banks to utilise the investments made in Open Banking technology including APIs. Additionally, savings on KYC spending and reduced fraud losses should be fully quantified so banks can understand the financial and/ or efficiency benefits associated with DV.

The structure and responsibilities of the orchestrator will be key to fostering an incentive for participation. Under any structure of the orchestrator proposed in this report, there is a commercial incentive for financial institutions to participate as IDPs. Consideration should be given to an orchestrator that is government-led, with oversight from regulatory bodies, and with sufficient investment from both public and private sector to ensure adoption, growth and innovation. It follows that the role and mandate of government-owned investment vehicles, such as the NWF, be considered.

Education

As the DVS evolves, educating all key participants - including RPs, data providers, and users - about their roles and responsibilities within the proposed framework is essential. Once the model is further defined, participating data providers and RPs should be informed about the data sharing protocols, the liability model, and other integration requirements. Similarly, users should be educated on the benefits of using the DVS and how it operates, particularly regarding their interactions with relying parties.

It is essential to emphasise that information will only be shared with their consent, in accordance with the privacy agreements established with data providers. This education is vital as the concept evolves and becomes more specific during the subsequent development and implementation phases, where comprehensive content should be delivered to ensure that all key players understand their roles and responsibilities.

Accessibility

In developing the DVS for the UK, it is imperative to prioritise accessibility and ensure no individuals or groups are excluded from participating in essential services. This is particularly important for vulnerable customers, who may face challenges in using digital technologies and would perhaps be disproportionately negatively impacted should DV become the only option for individuals to interact with essential services. Whilst the service proposed in this report is designed to enable a digital-first approach to identity verification it will be crucial to maintain a commitment to inclusivity by ensuring alternative options are provided for those who cannot or prefer not to engage with digital platforms. This approach aligns with the principles of Consumer Duty, ensuring that all customers, regardless of their circumstances, have equitable access to verification processes. By integrating multiple pathways for verification, the service will not only enhance customer experience but will also uphold the rights and needs of all individuals, fostering a more inclusive digital landscape.

Recommendations conclusion

In conclusion, the establishment of a comprehensive legal and regulatory framework for DV in the UK, as outlined in the *Data (Use and Access)* Bill, is a critical step towards enabling secure and efficient identity verification processes. However, for the successful implementation of this framework, it is essential to provide further clarity on key terms and responsibilities, ensuring that all stakeholders, particularly those in the financial and professional services sector, understand their roles within the service. Clear ownership and accountability, both within government and the private sector, will foster collaboration and support for DV initiatives.

Moreover, the proposed model must prioritise accessibility, ensuring that vulnerable customers are not excluded from essential services and that alternative verification options remain available alongside digital services. By addressing these considerations, the UK can create a robust DV ecosystem that not only meets current demands but also adapts to future challenges. Ultimately, a well-defined, inclusive, and collaborative approach will position the UK as a leader in DVS, benefiting both individuals and organisations while promoting trust and security in the digital landscape.

5. Conclusion

The UK is at a critical juncture, where adopting a widely accepted DVS is essential for reinforcing its position in the global digital landscape. This report presents a model for a DVS that illustrates how a strong framework can enhance economic growth and operational efficiency across various sectors, benefiting consumers, businesses, and citizens alike. Successful implementation will require renewed partnerships among government, regulators, and industry stakeholders to drive innovation and increase investment.

The successful implementation of DVS in the UK may take some time as an approach is created and standards are set. Whilst the approach set out in this paper is by no means definitive; by focusing on the principles outlined in this report, the UK can advance towards the creation of a cohesive ecosystem that streamlines identity verification processes while building trust and security.

The time for action is now; embracing DV will empower individuals and businesses, paving the way for secure growth and a prosperous future for the UK.

Appendix

The following appendices provide additional insights and further information and context relevant to the discussion of DV and identity services throughout this paper. **Appendix 1** presents key definitions aligned with the *UK digital identity and attributes trust framework*, clarifying important terms and concepts.

Appendix 2 outlines the guiding principles for selecting a proposed DV model for the UK. These principles emphasise the importance of public trust, user value, operational resilience, and legal compliance, among others. By establishing a clear framework for evaluation of DV models, this appendix aims to ensure that the chosen model effectively meets the needs of all stakeholders while fostering a secure and inclusive digital environment.

Appendix 3 summarises market sentiment regarding DV, highlighting stakeholder perspectives on the importance of a public-private framework, the need for regulatory certainty, high standards in security and data quality, and the establishment of a fair value exchange. Together, these appendices serve as a resource for stakeholders involved in developing and implementing DVS.

Appendix 1: Definitions

The definitions provided in this section align at a minimum with those in the *UK digital identity and attributes trust framework gamma (0.4) pre-release* (Published 25 November 2024).[33] Where the definitions have been elaborated or further developed for the purposes of this report, that is detailed in the table below.

Term	Definition in *UK digital identity and attributes trust framework*	Additional context or definition
Digital Identity or Digital ID	A digital representation of who a user is. It lets them prove who they are during interactions and transactions. They can use it online or in person.	• **Components:** Digital identities can include personal information such as name, national insurance number, date of birth, and addresses, but can also include other identifiers like a digital certificate or biometric data • **Purpose:** The primary purpose of a Digital ID is to provide a secure and reliable way to prove one's identity online. It can be used for accessing various digital services and can also be used offline. • **Examples** include government-issued digital IDs like Aadhaar in India, eID in Estonia, and digital driver's licences
Digital verification service (DVS)	Services that enable people to digitally prove who they are, information about themselves or their eligibility to do something.	In this report, our DVS is further defined as a service that enables the secure and efficient verification of an individual's identity or attributes through digital means. • **Components:** These schemes involve various technologies and methods such as biometric verification, multi-factor authentication (MFA), digital signatures, and blockchain technology • **Purpose:** DV schemes ensure that the person or entity presenting the digital identity data or ID is who they claim to be, and/or that the attributes such as DOB are correct. The primary purpose of DV schemes is to enhance security by preventing fraud and unauthorised access. They can also be used to verify a person's age or their eligibility to do something. • **Examples:** Gov.uk Verify was an attempt at a digital verification scheme (now closed). Digital ID schemes do also have an element of digital verification as part of the security framework of the scheme.
Biometric information	Measurements of a biological or behavioural attribute, like an iris or fingerprint	
Certified service	A digital verification service that has been certified against the trust framework	
Digital wallet	An electronic device, online service or software programme that allows one party to make electronic transactions with another party for goods and services.	
Identifier	A piece of information that can be used to make a connection between an attribute and a person or organisation.	In literature on Digital ID and DVS, also referred to as "identity attributes"

[33] See reference 3

Term	Definition in *UK digital identity and attributes trust framework*	Additional context or definition
Identity data providers	**Not defined**	Organisations that hold identity data attributes for users, including name, date of birth, address details, unique identifiers such as national insurance number. There is overlap in literature on Digital ID and DVS with the term "identity service provider".
Identity service provider	An organisation providing a service that proves and verifies a user's identity for one-off use at a single point in time. It can do this using online or offline channels, or a combination of both.	In literature on Digital ID and DVS, multiple terms can also refer to ISPs: "Identity issuers" - governments and banks / consortiums that are responsible for issuance of identification and mandating eID solution providers through mandates. "Platform owners" – often a group of identity providers (e.g. financial institutions) who own and manage the eID platform infrastructure, and/or control access to the platform.
Orchestration service provider	An organisation providing a service that makes sure data can be securely shared between participants in the trust framework through the provision of their technology infrastructure.	In literature on Digital ID and DVS, also referred to as "Service Providers"
Relying party	An organisation that relies on (or 'consumes') certified products or services.	In literature on Digital ID and DVS, also referred to as "Service Providers".
Trust framework	A set of government-approved rules, which draws mainly on existing standards, guidance, best practice and legislation, that organisations agree to follow to have their service certified as a trustworthy digital verification service.	
User	A person who uses digital verification services.	In literature on Digital ID and DVS, also referred to as "Subjects"

Appendix 2: Digital Verification model principles

The principles guiding our selection of a proposed DV model for the UK are outlined below. Five key principles have been elaborated upon in the body of the report. Many of these principles will continue to guide the chosen model during development and implementation phases.

Pillar	Principle	Description	Considerations for UK
Public trust	Governance	A structured set of policies, standards, and practices governing identity verification and trust establishment must be in place and agreed to by all participants.	The framework must support robust verification for both organisations and individuals, including checks against government held data.
	Transparency	Clear and open communication about system operations, data collection, and usage.	Must provide transparency on system workings and data sources. Complexity can hinder transparency. Transparency regarding the trade-offs between models engenders public trust; simplicity of the chosen model can enhance understanding.
	Inclusivity	Ensuring wide participation while allowing users to opt out.	Should allow maximum participation, including those without technology access or disabilities. A non-mandatory service which provides benefits for users but can be opted out of will be preferable in terms of inclusivity
	Assurance	Robust auditable assurance processes to monitor and detect fraud.	Must enable strong central assurance processes agreed upon by all parties. Model may require a central authority for regulation and assurance of processes and quality.
Adoption and growth	User value	Meaningful value for stakeholders must exceed the status quo.	Different models provide varying types and levels of value. A set of strong, penetrating use cases that have user value at their heart will drive adoption. Value can be understood as time saving, cost saving or provision of new services not previously available.
	Scalability and flexibility	Ability to scale and adapt to changes in technology and user needs.	Constraints on scale must be compared across models – international interoperability, standards on integration and use of best class protocols on security, authentication and privacy. Strong standards in integration and governance are key to drive scalability.

Pillar	Principle	Description	Considerations for UK
Adoption and growth	User centricity and experience	Prioritising user needs to enhance experience and engagement.	Model should be accessible, easy to register for, and inclusive. Initial registration should be made as simple as possible, with minimal data entry from user and ideally little or no provision of documentation if possible. Clear communication to the user on what data is being shared and to what purpose.
	Operational resilience and high level of support	High technical support and operational resilience are essential.	A central body for support and regulation of value-added services is key. Previous experience in Open Banking and Gov.UK Verify shows the importance of high level of availability and high success rates for verification, with excellent support provided for exceptions.
Commercial model	Commercial model	A billing and liability management model that incentivises participation.	See body of report for detailed considerations.
	Interoperability	Ability of different systems to work together seamlessly.	
	Cost effectiveness	Initial capital investment and ongoing maintenance costs.	
Privacy and security	Data confidentiality and security	Protecting sensitive information from unauthorised access.	See body of report for detailed considerations.
	Data integrity	Ensuring accuracy and reliability of data throughout its lifecycle.	Must enable data integrity and align with UK GDPR and other laws. Initial attestation by IDPs to the quality of data, backed up by ongoing monitoring of data quality levels, verification success rates. Allowing an easy way for users to update their data across multiple IDPs can incrementally improve data quality and integrity over time.
	Data minimisation and purpose limitation	Limiting data collection to what is necessary for specific purposes.	See proposed model and body of report for detailed considerations.
Privacy and security	User agency and consent	Individuals should have control over their personal data.	Consider data sharing levels required for use cases; consent must be revocable. User education and empowerment are key.
	Data decentralisation	Distribution of data across multiple locations rather than a central repository, ideally without creation of new data stores that could become targets for attack.	See body of report for detailed considerations.
Legal and regulatory compliance	Legal foundation for acceptance of DVS	Legal foundation defining acceptable use cases for DVS.	Initial use cases should have a pre-existing legal foundation. Existing regulated sectors such as KYC / AML may provide a good basis, with existing regulatory basis and active involvement from regulatory bodies likely.
	Ongoing regulation of DV activity	Continuous regulation and monitoring of digital verification activities.	See body of report for detailed considerations on the role of orchestrator.
	Liability	Legal requirements and liability in the event of misuse or breaches.	See body of report for detailed considerations.
	Compliance with AML and CTF legislation	Adherence to anti-money laundering and counter-terrorist financing regulations.	Existing regulated sectors such as KYC / AML may provide a good basis, with existing regulatory basis and active involvement from regulatory bodies likely.
	Compliance with Digital ID and verification legislation	Adherence to laws governing digital ID and verification.	Must comply with existing and upcoming identity verification laws and regulations. government involvement in the orchestrator in proposed model is key.
	Compliance with consumer duty	Enhancing consumer protection in financial services.	Key considerations must be built into the design and implementation to ensure ongoing compliance with Consumer Duty.

Appendix 3: Market sentiment

Theme 1: Market sentiment strongly favours public-private framework for DV

Market sentiment as gauged through City of London Corporation Roundtables and discussion with a wide range of industry participants, is weighted in favour of a shared DVS. Many industry stakeholders have asserted that a public-private framework is the most viable method for implementing DV in the UK.

A successful DVS relies on a robust partnership between the government and the private sector, particularly financial institutions that possess large volumes of verified identity data. As one expert noted, "Banks have a 250-year relationship of trust with the people of the UK," emphasising the importance of leveraging this trust in the initiative. Additionally, survey data highlights that financial institutions are amongst the most trusted organisations to hold users' data in the UK, ahead of both central and local government.[34]

However, a government-dominant model may pose risks, such as creating centralised "honey pots" of data that could attract cyberattacks. Therefore, the government's role in establishing a regulatory framework is essential to balance innovation with security. This oversight not only helps build public trust but also enhances the validation of private sector information.

Recent developments in the legislative framework for data sharing enables this public/private partnership approach. The *Data (Use and Access)* Bill will give the Science and Technology Secretary and HMT the power to introduce new Smart Data schemes through regulations. The regulations will allow the creation of models such as that proposed in this report, allowing consumers and businesses who want to safely share information about them with regulated and authorised third parties.

Theme 2: Need for regulatory and legal certainty in DV

The establishment of a DVS requires clear legal and regulatory frameworks to ensure its success. Stakeholders emphasised that without defined roles, responsibilities, and liability standards, the implementation of DVS may encounter significant challenges. "Three items that always come up - liability, reliance, and commercials," one participant remarked, highlighting the complexities involved in navigating these issues. A well-defined regulatory framework will foster trust among participants and facilitate smoother collaboration between public and private sectors. Furthermore, an interoperable DVS that aligns with international standards will be crucial for boosting cross-border digital trade and enhancing the UK's GDP. As one expert pointed out, "Having regulators in the room during the discussion is key," emphasising the importance of early engagement with regulatory bodies to ensure a balanced approach to the challenges ahead. This proactive stance will help create a legal environment that supports innovation while safeguarding public interests.

Studies on the impact of regulation on digital platforms, including identity platforms, offer useful case studies of how such platforms can become shared "industry infrastructure", the value that participants can gain from such a platform, and also highlight the value of standardised contractual agreements for all participants within the platform.[35]

Theme 3: Establishing high standards in security, data quality, and verification

The credibility and effectiveness of any DVS are fundamentally linked to the technology that underpins it, particularly regarding data quality, security, and privacy. Stakeholders agree that the service should incorporate industry best practices, such as encryption and multi-factor authentication, while also addressing privacy concerns through data minimisation principles. As one participant stressed, "Each data point should have a rule for its currency and strength of verification," highlighting the need for a standardised approach to data quality.

Moreover, prioritising user agency and consent is essential to ensure that data sharing aligns with user needs. The standardisation of data and verification processes will enable interoperability across different firms and sectors. As another expert noted, "We are exceptionally poor at measuring data quality, legitimacy, verification standards, etc.," indicating a need for improvement in these areas. Establishing high standards around security and data quality will not only enhance the effectiveness of DVS but also build the necessary trust among users and stakeholders.

The focus on agreed standards in data security, authentication and verification are shared across international and national guidance on Digital ID and DVS. Internationally, these standards have been collated in Appendix D of the *"Guidance on Digital Identity"* report published by FATF.[36] Nationally, the *UK digital identity and attributes trust framework* (v0.4) also includes a comprehensive table of standards, guidance and legislation which are followed and referenced throughout the framework.[37]

Theme 4: Fair value exchange to incentivise participation in DV

The development of a DVS presents a significant opportunity for growth within the FPS sector, particularly in creating a fair value exchange between parties. Banks, which hold extensive amounts of high-quality customer data, can leverage this information for verification purposes, enhancing their value proposition to customers and third-party service providers. As one expert mentioned, "A fair value exchange will incentivise participation in the ecosystem," suggesting that a balanced approach to data utilisation is essential.

Typically, commercial models for DVS involve charging RPs per verification, often with tiered pricing to encourage high-volume usage. This model ensures that verification remains free for end customers while compensating data suppliers for their services. Additionally, a clear liability regime must be established from the outset to incentivise the provision of high-quality identity data. As one participant noted, "Basic attributes should be shared for free," indicating that premium attributes could be offered through a paid API, thus allowing for monetisation with customer consent. This commercial model needs to support and incentivise participation and investment, ensuring that all stakeholders benefit from the DV ecosystem.

[34] Cited in McKinsey Global Institute (2019). *Digital identification: A key to inclusive growth.*

[35] Bazarhanova, A., Yli-Huumo, J., & Smolander, K. (2019). *From platform dominance to weakened ownership: how external regulation changed Finnish e-identification.* Electronic Markets, 30, 525–538.

[36] Financial Action Task Force (FATF). (2020). *Guidance on Digital Identity.*

[37] See reference 3

Acronyms

A2A	Account to Account
AML	Anti-Money Laundering
API	Artificial programming interface
CFIT	Centre for Finance, Innovation and Technology
CO	Cabinet Office
DV	Digital Verification
DVS	Digital Verification Service
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FPS	Financial and Professional Services
FS	Financial Services
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HMT	HM Treasury
ID	Identity
ICO	Information Commissioner's Office
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
NCA	National Crime Agency
OfDIA	Office for Digital Identities and Attributes
PE	Private Equity
SME	Small and medium-sized enterprises
VC	Venture Capital

Contacts

EY Contacts

Axe Ali
Partner, Private Equity and Venture Capital
axe.ali@parthenon.ey.com

Thomas Bull
Partner, UK FinTech Growth Leader
tbull1@uk.ey.com

Robyn Easton-Fei
Director, UK Financial Crime Consulting
REaston@uk.ey.com

Support provided by:
Cormac Mealey, Senior Manager
Rafael Pontes, Senior Manager
Ellie Marsh, Manager
Annabel Buxton, Manager
Bhavya Kapur, Consultant

City of London Corporation Contacts

Leighton Hughes
Senior Adviser (FinTech, Digital Infrastructure)
Leighton.Hughes@cityoflondon.gov.uk

Adam Summerfield
Head of FPS Technology (Interim)
Adam.Summerfield@cityoflondon.gov.uk

Additional support provided by:
Markos Zachariadis,
Professor and Chair in Financial Technology (FinTech) & Information Systems, Alliance Manchester Business School

Bibliography

1 City of London Corporation (2023). *Vision for Economic Growth — a roadmap to prosperity.*

2 More in Common survey for The Times and Justice Commission. *More than half of public support digital ID cards.*

3 Department for Science, Innovation & Technology (2024). *UK digital identity and attributes trust framework gamma (0.4) pre-release.*

4 City of London Corporation. (2025). *Our global offer to business 2025.*

5 See reference 4

6 Brandão, L. T. A. N., Christin, N., Danezis, G., & Anonymous (2015). *Toward Mending Two Nation-Scale Brokered Identification Systems.*

7 See reference 2

8 GOV.UK (2024). *Pubgoers given choice to prove age with phones next year in boost for high street and hospitality sectors.*

9 Startup Coalition & Tony Blair Institute (2025). *Making Smart Data Happen.*

10 GOV.UK (2025). *Stricter age-verification checks for all knife retailers.*

11 Office for National Statistics (2020). *Percentage of homes and individuals with technological equipment.*

12 Office for National Statistics (2020). *Internet access – households and individuals, Great Britain.*

13 Parris, Stuart, Anton Spisak, Louise Lepetit, Sonja Marjanovic, Salil Gunashekar, and Molly Morgan Jones (2015). *The Digital Catapult and Productivity: A Framework for Productivity Growth from Sharing Closed Data*. Santa Monica, CA: RAND Corporation.

14 Pitchbook data (2025). Accessed 19th Feb 2025.

15 UK Finance (2024). *Annual Fraud Report 2024.*

16 YouGov (2025). *Three in five Brits have had the same current account for over ten years.*

17 Savanta Europe (2025). *Why UK consumers are opening new bank accounts – and what banks can do to keep them.*

18 Citizens Advice (2024). *9 million people caught out by financial scams in the past year.*

19 See reference 15

20 Crowe Clark Whitehill, Experian, & Centre for Counter Fraud Studies at the University of Portsmouth. (2017) *The Annual Fraud Indicator - UK foots £190bn annual fraud bill.*

21 FIS Global (2023, March 23). *Account-to-Account Payments Set to Revolutionize Shopping, with E-commerce Payments Reaching $525 Billion Globally: Worldpay from FIS 2023 Global Payments Report.*

22 Simon-Kucher & Partners (2025). *Accelerating Instant Payments in the UK: Why Ecosystem Incentives Are Key to Success.*

23 Banking Gateway (2019). *What is Swish? The mobile payments system used by more than two-thirds of Swedes.*

24 Mole, C., Chalstrey, E., Foster, P., & Hobson, T. (2023). *Digital identity architectures: comparing goals and vulnerabilities.*

25 Digital ID & Authentication Council of Canada (2020). *DIACC Identity Networks Paper Verified.Me by SecureKey Technologies Inc., Self-Assessment.*

26 Signicat (2024). *The State of Digital Identity in Europe 2024-2025.*

27 See reference 26

28 Signicat (2021). *Digital eIDs in the Nordics.*

29 See reference 20

30 UK Finance (2023). *Annual Fraud Report 2023.*

31 LexisNexis Risk Solutions (2024). *The True Cost of Financial Crime Compliance 2024.*

32 GOV.UK (2025). *Home buying and selling to become quicker and cheaper.*

33 See reference 3

34 Cited in McKinsey Global Institute (2019). *Digital identification: A key to inclusive growth.*

35 Bazarhanova, A., Yli-Huumo, J., & Smolander, K. (2019). *From platform dominance to weakened ownership: how external regulation changed Finnish e-identification.* Electronic Markets, 30, 525–538.

36 Financial Action Task Force (FATF). (2020). *Guidance on Digital Identity.*

37 See reference 3

Bibliography

Additional papers and research which contributed to our thinking in this report.

a Soltani, S., & Rasouli, A. (2021). *Proposing a digital identity management framework: A mixed-method approach. Concurrency and Computation: Practice and Experience.*

b Segovia Domingo, A. I., & Martín Enríquez, Á. (2022). *Digital identity: the current state of affairs.*

c Li, J., & Jing, Y. (2022). *Establishing an International Engagement Model of Digital Identity Based on Blockchain*.

d Cheesman, M. (2022). *Self-Sovereignty for Refugees: The Contested Horizons of Digital Identity.*

e Rasouli, A., & Soltani, S. (2021). *A Survey of Self-Sovereign Identity Ecosystem.*

f Alizadeh, M., Andersson, K., & Schelén, O. (2022). *Comparative Analysis of Decentralized Identity Approaches.*

g Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2023). *Comparative Analysis of Technical and Legal Frameworks of Various National Digital Identity Solutions.*

h Alizadeh, M., Andersson, K., & Schelén, O. (2022). *Comparative Analysis of Decentralized Identity Approaches.*

i Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2023). *Comparative Analysis of Technical and Legal Frameworks of Various National Digital Identity Solutions.*

j Goel, A. & Rahulamathavan, Y. (2025). *A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility.*

k Office for Digital Identities & Attributes, Department for Science, Innovation & Technology (2024). *Digital Identity Sectoral Analysis 2024: Interim Findings.*

l Visa (2024). *Digital Identity: What to know and how to prepare.*

m World Bank (2022). *National Digital Identity and government Data Sharing in Singapore: A Case Study of Singpass and APEX.*

n Pradhan, P., & Kumar, V. (2016). *Trust Management Models for Digital Identities.* International Journal of Virtual Communities and Social Networking 8(4), 1-24.

o Ferdous, M. S., & Poet, R. (2012). *A Comparative Analysis of Identity Management Systems.* Proceedings of the International Conference on High Performance Computing and Simulation (HPCS).

p World Bank. (2018). *Guidelines for ID4D Diagnostics*

q Millo, Y., Panourgias, N., & Zachariadis, M. (2021). *Identification Infrastructures and the Capitalization of Data in the Development of Data-Driven Regulation: The Case of the Global Legal Entity Identifier System.* In B. Unger, L. Rossel, & J. Ferwerda (Eds.), *Combating Fiscal Fraud and Empowering Regulators: Bringing tax money back into the COFFERS* (pp. 158-179). Oxford: Oxford University Press.

THE GLOBAL CITY

About the Global City campaign

The Global City campaign is the City of London Corporation's overarching initiative to promote the UK as a world-leading international financial centre. It showcases the UK as a great place for financial and professional services firms to invest, locate and grow.

theglobalcity.uk

About the City of London Corporation

The City of London Corporation is the governing body of the Square Mile dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally successful UK.

We aim to:

– Contibute to a flourishing society
– Support a thriving economy
– Shape outstanding environments

By strengthening the connections, capacity and character of the City, London and the UK for the benefit of people who live, work and visit here.

cityoflondon.gov.uk

The publisher of this report is the City of London Corporation. This report is intended as a basis for discussion only. Whilst every effort has been made to ensure the accuracy and completeness of the material in this report, the City of London Corporation give no warranty in that regard and accept no liability for any loss or damage incurred through the use of, or reliance upon, this report or the information contained herein.