***De Minimis* Assessment: Self-Certification Template**

Department for
Digital, Culture
Media & Sport

Title of regulatory proposal	*Powers for digital identity and attributes initiatives*
Stage	Final
Lead Department/Agency	DCMS
Expected date of implementation	Unknown
Date	15/09/2021
Lead Departmental Contact	Jordan Moodie 020 7211 6000
Departmental Triage Assessment	Equivalent Annual Net Direct Cost to Business (EANDCB: 2019 prices) = 0.0

Call in criteria checklist	
Significant distributional impacts (e.g. significant transfers between different businesses or sectors)	No
Disproportionate burdens on small businesses	No
Significant gross effects despite small net impacts	No
Significant wider social, environmental, financial, or economic impacts	No
Significant, novel, or contentious elements	No

BRU (CAT) signoff: ✔ Date: 17/02/2022

Chief Economist signoff (delegated): ✔ Date: 17/02/2022

Spoke Analyst: ✔ Date: 16/12/2021

SUMMARY

Rationale for government intervention

Current identity proofing methods can be expensive, inefficient, and vulnerable to fraud. Digital identities can strengthen and simplify the process.

However, the current landscape is insufficient. It lacks standards which will enable interoperability and does not yet command trust. In the 2019 Call for Evidence, respondents noted that the market required government to step in and set these standards, create mechanisms to allow organisations to prove they follow them, and to enable checks against government-held data.

The objective of this policy is to allow people to prove things about themselves as quickly and securely as possible. By enabling this, we hope to achieve the following effects:

- Unlock the economic gains associated with a functioning digital identity system, enabling the full realisation of the digital economy.
- Protect against fraud, for both businesses and people.
- Enhance privacy and enable data minimisation.
- Promote inclusive solutions and remove barriers to inclusion.

Policy options

- The status-quo option would be for Government to not seek to legislate regarding digital identity. We would still continue to develop the trust framework but there would be no mechanism for a governance function to own these requirements, and no robust route for organisations to prove they follow the requirements. Doing nothing would leave the UK with a small and poorly functioning digital identity market which leaves efficiency gains unmade and falls behind international partners.
- Option 2 is to create a statutory governance framework to oversee the trust framework. However, digital identities could still only be built on limited datasets.
- Option 3 is to enable checks against government-held data but not create a statutory governance framework. Without a visible and trusted governance, consumers would struggle to understand which organisations follow what rules and hence which they can trust.
- Option 4, the preferred option, is to combine options 2 and 3. This is the preferred option as without enabling checks the use cases will not be usable. However, without a strong governing framework to build trust in the market and support the opening of more sensitive data sets, we will not be able to fully achieve the policy objectives.

Summary of business impact /Rationale for DMA Rating

There is no direct impact on business of this legislation. All this legislation does is allow government departments the option of opening up their datasets to the private sector for use with digital identities. The only direct impact is the familiarisation cost for affected departments, which is a public sector cost and not a private sector cost.

I

Evidence Base

Problem under consideration

Current identity proofing methods can involve multiple physical documents needing to be checked at different stages of the process. Organisations have to pay for identity checks from scratch every time they interact with a new user. These labour-intensive tasks can be expensive and inefficient.

Digital identities enable people to prove something about themselves — their age, their nationality, their identity — as seamlessly as possible, simplifying this process. A digital identity is essentially 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. Under a trusted and secure digital identity framework, a person could choose to prove their identity once, then have that proof trusted throughout any process.

Use of physical documents is vulnerable to fraud, with CIFAS reporting high levels of identity fraud in the UK; there were over 180,000 cases reported in 2020[1]. Physical documents are often carried around by people to access services, and they are a legal requirement for activities such as buying alcohol or proving your right to work. However, as the ICO notes, these documents can easily be lost or stolen[2], and are fuel for organised crime.

Digital identities can be non-physical, removing the possibility of theft or loss of documents and thus potentially reducing fraud. By virtue of being digital, their use (in line with data privacy and protection law) also enables more efficient checks against fraud databases, reducing opportunities for fraudsters.

Digital identities can also help reduce other forms of fraud. For example, Authorised Push Payment (APP) scams involve tricking a person or business into transferring money to a fraudster while thinking the recipient is legitimate. In future, it may be

[1] CIFAS, 2021, Fraudscape
[2] Identity Theft, ICO

possible to make a quick and easy digital check of the recipients' identity to prevent such scams from occurring[3].

There are also privacy considerations. To prove you are over eighteen to buy alcohol, a person currently needs to show an identity credential containing information like address. This is an unnecessary disclosure of personal data. Digital identities allow a person to minimise what personal data is disclosed when accessing a service to just what is required to access that service, thus enhancing privacy.

However, the landscape of the current digital identity market is not sufficient to address these problems or to realise these benefits. It is fractured, lacking standards which will enable interoperability, and does not yet command the trust of consumers and relying parties. There is no independent way for people or businesses to know that an identity provider can be trusted or that their identity products are based on solid evidence. In turn this precludes the effective use of digital identity solutions.

In the 2019 Call for Evidence[4], respondents noted that the market required government to step in and set these standards. Alongside these standards, government also must create mechanisms to allow organisations to prove they follow them, and to monitor, oversee, and enforce the following of them. Respondents also stated clearly that, if confidence and trust is to be instilled in digital identity products, access to government-held data was required. Just as familiar forms of identification, like passports, are based on authoritative government-held data, so too must digital identities. Respondents claimed that enabling international interoperability of digital identities ought to be a key priority of government. Allowing a UK citizen to use their UK created digital identity to transact abroad and allowing the reverse would facilitate trade in addition to having the aforementioned benefits digital identities bring. However, there is no clear path to enable the UK to enter into mutual recognition agreements for either digital identities or trust services without a domestic digital identity framework.

Policy objective

The objective of this policy is to allow people to prove things about themselves as quickly and securely as possible. By enabling this, we hope to achieve the following effects:

- **Unlock the economic gains associated with a functioning digital identity system, enabling the full realisation of the digital economy.** The current lack of widespread digital identity use in the UK is preventing end-to-end digital transformation at scale. Britain's tech industry currently adds nearly £184bn a year[5] to our economy, with 74% of people in the UK saying they cannot live without the internet[6]. Individuals in the UK expect to be able to carry out their transactions online and, as services increasingly move online to meet demand, an individual's ability to provide their identity digitally has

[3] techUK, The case for digital IDs 2019
[4] Digital Identity: Call for Evidence Response
[5] Tech Nation, A bright tech future
[6] Onwards, The People's Study. (File available from GDS)

become essential. In a normal year HMPO processes around 7m passport applications, however in 2020 just over 4m people applied for a passport.

- **Protect against fraud, for both businesses and people.** Identity fraud is at a high level within the UK with just over 180,000 cases reported in 2020[7]. Digital identity can play a crucial role in reducing crime and fraud, both online and offline. The wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity to steal and use stolen documents.
- **Enhance privacy and enable data minimisation.** Use of physical identity documents often involves the oversharing of personal data which can then be misused. The wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity to steal and use stolen documents. Digital alternatives will also be able to minimise data to safeguard privacy[8], reducing the risk of data misuse.
- **Promote inclusive solutions and remove barriers to inclusion.** According to the last census in 2011, 17% of people in England and Wales do not have a passport[9] (a key document for identity proofing). Moreover, evidence from Switchback's work with young prison-leavers highlighted that 25% were released with no ID[10], making it difficult for them to access benefits or open a bank account. Digital identity presents a unique opportunity to allow people without common identity documents to use a digital alternative. A secure way to share basic identity information digitally could give excluded groups access to the services most people take for granted.

Description of options considered

Option 1: Do nothing

The status-quo option would be for Government to not seek to legislate regarding digital identity.

We would still continue to develop the UK digital identity and attributes trust framework, a set of requirements representing best practice in digital identity which organisations could choose to follow. However, without statutory powers being created, there would be no mechanism for a governance function to own these requirements and to set up an accreditation and certification framework. As such, there would be no robust route for organisations to prove they follow the requirements. Similarly, there would be no lasting oversight of these organisations so it is unlikely that trust and confidence in digital identities would increase.

The ability to share government-held data would also be very limited. This means that it would be difficult for digital identities to be built on authoritative government-held data, reducing trust in their accuracy. It is unlikely that datasets vital to building inclusive digital identities would be accessible.

---

[7] CIFAS, 2021, Fraudscape

[8] The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system

[9] Detailed country of birth and nationality analysis from the 2011 Census of England and Wales

[10] Action needed to protect prison-leavers and the public during Covid-19, Switchback

Doing nothing would leave the UK with a small and poorly functioning digital identity market which leaves efficiency gains unmade and falls behind international partners.

Option 2: Create a statutory governance framework to oversee the trust framework

This option would see statutory powers created for governance of digital identity to:

- manage the aforementioned trust framework and update its requirements to ensure they remain fit for purpose as technology evolves;
- set up and provide oversight of accreditation and certification processes so qualifying organisations can prove compliance with a trust mark;
- monitor compliance and performance of trust framework participants;
- promote consumer protection by managing enforcement, complaints, and redress;
- collaborate with stakeholders and regulators;
- maximise cybersecurity and minimise fraud; and
- promote and encourage inclusion.

This would enable organisations to prove that they follow certain requirements and can be trusted when they create digital identity solutions, both to protect users' privacy and to provide a robust service to a relying party. It would give consumers additional protection and thus promote uptake of digital identity.

However, without legislation which provides for a legal gateway which may enable checks against government-held data, digital identities could still only be built on limited datasets.

Option 3: Enable checks against government-held data but do not create a statutory governance framework

This option would see the creation of a permissive legal gateway which would enable government departments to allow checks against data they hold for digital identity, eligibility, and verification purposes. This would allow organisations to base digital identities on authoritative government-held data, which forms the basis of traditional identity checks.

However, without a governance framework, departments would need to individually set requirements for organisations to meet before allowing checks. They would also need to set up due diligence procedures to ensure organisations can be trusted to check people’s data for the purposes of verifying identity and eligibility digitally. This would inevitably add cost and could fragment the market as different departments set different standards.

Without visible and trusted governance, consumers would struggle to understand which organisations follow what rules and hence which they can trust. Individuals and organisations would have no central route to complain or seek redress. These factors are likely to hinder adoption of digital identity.

Option 4: Create a governance framework and enable checks against government-held data - preferred option

This option is a combination of options two and three and is our preferred policy option. To summarise, this intervention would:

- create a model of governance which will meet the needs of all parties while balancing proportionate rules with security, consumer protection and trust, according to the scale of digital identity use;
- provide a permissive legal power to allow digital identities in the UK to be built on a greater range of trusted datasets and for government-held attributes to be checked for eligibility, identity and validation purposes;
- build confidence in the legal validity of digital identities alongside the physical proofs of identity that businesses and individuals already trust, as part of our commitment to increase choice and confidence.

It would not be mandatory for digital identity companies to be part of this governance framework or to be certified as following the requirements set out in the trust framework. However, checks against government-held data could only be performed by trusted organisations and certification against these requirements could provide this trust.

Rationale for intervention

Ensure a functioning market

The UK Government wants to ensure that the potential of the UK digital economy is maximised. McKinsey estimates that extending full digital identity coverage in the UK could unlock economic value equivalent to between 0.5% and 3% of GDP in 2030 through the delivery of these benefits[11]. Therefore, to facilitate remote identity proofing in order to support growth of the digital economy, the UK Government wants to foster the uptake of digital identity. However, current legislation does not facilitate the creation of a fully functioning digital identity market, for example there is no legislation in place to enable the private sector to check data contained within certain government databases for identity verification purposes.

Government intervention is therefore required to overcome the current barriers faced by the market. A sustainable rule-bound environment, with a robust governance and oversight mechanism, needs to be created to allow the market to grow in a trusted and interoperable way. In order to improve trust in digital identities, the Government also needs to intervene to allow the private sector to make checks against government-held data for identity verification purposes under specific controlled circumstances

Intervention by the Government is further required to affirm the validity of digital identity solutions as methods of identity proofing. Factors such as lack of trust in the market prevent users and the relying parties from considering digital identity a

[11] McKinsey, 2019, Digital Identification: A Key to Inclusive Growth

perfect substitute to traditional ID checking, which halts a wide uptake of digital identity. Therefore, the legislation is required to build capability and trust and affirm the equal validity of digital identities and attributes relative to traditional identity documents. In turn, this is expected to foster uptake of digital identity by building confidence across guidance bodies and organisations in using the digital identity system.

Ensure a functioning international digital identity market

Currently, there is a lack of international cooperation across various digital identity markets due to a lack of mutual recognition.This creates serious barriers to both digital identity proofing of UK citizens abroad and to allowing foreign individuals to use their foreign digital identity in the UK. In turn, this limits the full realisation of the digital identity market.

For example in the case of Right to Work checks, foreign workers may particularly struggle to present the traditional identity documents required for background checks. To help with this, the Home Office has already implemented digital checks in the Right to Work and Right to Rent Schemes with the introduction of the Home Office online right to work and right to rent checking services. These services allow an individual to prove their right to work or rent digitally, by providing time limited access to the relevant information. These services can be used by individuals who have been given access to a digital version of their UK immigration status (an eVisa), or those with a valid Biometric Residence Permit or Card. However, this is still based on data held by the UK government, rather than that of the home nation of the individual.

Intervention is necessary because unless the Government creates a domestic digital identity framework, the current barriers to international cooperation and interoperability cannot be overcome. The legislation will therefore set the right landscape to facilitate the full realisation of both the domestic and international digital identity markets. In turn, this is expected to support the growth of the UK digital economy and maximise the potential economic benefits to the UK economy as a whole.

Furthermore, putting in place a domestic digital identity framework which permits international cooperation will ensure that the UK is not left behind by the mutual recognition of digital identity across other countries which could potentially harm the position of the UK as a key international player in the future. Digital identity is increasingly mentioned by potential partners in free trade agreements.

Efficiency gains to the UK economy

Currently, organisations have to pay for identity checks from scratch every time they interact with a new user. The average employer in the UK spends £3,000 and 27.5

days to hire a new worker[12] which is a clear impediment to creating and filling new jobs. We expect digital identity to allow right to work checks to take place almost instantaneously[13]. Therefore, carrying out paperless identity checks would allow the resources currently spent on manual identity proofing to be invested in other activities. These efficiency improvements will not only benefit the direct stakeholders but also society as a whole. This is because there is a positive knock on effect to society from job vacancies being filled quicker as society benefits from the products and services provided by the newly hired employee. Therefore, the legislation is necessary to bring about efficiency gains due to a better allocation of resources which in turn enhances productivity and economic growth.

Prevention of identity fraud

Digital identities may help reduce fraud, so there are potential economic benefits from having a fully functioning, trusted and interoperable market for the wider UK economy. The current, unregulated digital identity market is unable to achieve this due to a lack of suitable legislatory environment and no overarching entity in charge of controlling it. Therefore, ensuring appropriate security standards is currently a responsibility of the singular digital identity providers which may not have the incentive to ensure that fraud risks are minimised.

Furthermore, Government intervention will create the correct landscape to support fraud prevention by setting up a governance function with the powers to ensure fraud prevention best practises are followed. The governance function will collaborate with the trust framework participants to maximise cybersecurity through set standards in order to increase prevention and promote swift action in case of suspicious activity. The body will also implement an information sharing structure both between relevant bodies and the framework participants and across participants. This is expected to increase information sharing about security threats and therefore resilience within the digital identity market to identity fraud. Government intervention is therefore required to set standards to maximise cybersecurity and minimise fraud to reduce the risk of identity fraud for UK citizens, whilst fostering digital identity uptake across the UK

Coordination issue and misaligned incentives: lack of interoperability and inclusivity

Current issues across the digital identity market relate to the lack of coordination and misaligned incentives preventing the market from meeting the needs of the UK citizens. For instance, by not incentivising providers to invest in interoperable products. Therefore, Government intervention is required to ensure the market is interoperable and offers an inclusive service which considers the needs of minorities

[12] Glassdoor, (2020). cost per hire is calculated as the total of internal (e.g. wage of members of the HR team) and external costs (e.g. cost of background checks) divided by the total number of hires in a time period.

[13] The newly hired worker will have to manually complete a self-service right to work check. Afterwards, all requirements will be automatically determined and approved.

or those with protected characteristics. Specifically, the trust framework attempts to enhance interoperability by creating an environment that enables businesses to collaborate and to consider inclusivity as a key priority for the business.

The Government, by promoting a digital identity market that balances the needs of the wider public and those of the private sector, will play an important role to foster growth of the sector by ensuring a well functioning digital identity ecosystem. If the service provided meets the needs of the public, individuals will be more inclined to adopt digital identity during private sector transactions which will help the market expand and increase digital identity uptake.

Lack of interoperability

Businesses lack incentives to invest in a suitable level of coordination across the digital identity sector because businesses prioritise private benefit, such as profit, over public benefit. Therefore, the free market may not prioritise in a way that ensures that the sector is well-coordinated and that an interoperable service is provided.

Government intervention is required because without an overarching structure there will be no entity in place with the power to coordinate the market, making it difficult for players to proactively cooperate. The implementation of the trust framework attempts to tackle this issue by outlining open recommended technical standards players in the market should follow to strengthen interoperability. Government intervention should also contribute to creating the appropriate playing field for scheme creation, for instance by overseeing them. A scheme is a group of different organisations that follow a specific set of rules regarding digital identities and attributes, in addition to those set out in the trust framework. For example, there may be a scheme in the home buying and conveyancing sector which allows members to prove they provide identities with the requisite level of assurance. In turn, this is expected to increase cooperation within and across schemes and provide the opportunities to create interoperable products.

However, although we expect to see a reduction in the coordination issue, the extent of the progress is unknown because these standards will be encouraged but not enforced.

Lack of inclusivity

The choice to use digital identities would be of considerable value to those who lack traditional identity documents. For instance, evidence from Switchback's work with young prison-leavers identified that 25% were released with no ID[14], making it difficult for them to access benefits or open a bank account. A fully functioning digital identity market would support minority groups or those with protected characteristics as a much wider range of datasets could be used, rather than just the typical documents used for identity proof. This would facilitate the identity proofing process for individuals without traditional documentation, enabling them to receive the

[14] Action needed to protect prison-leavers and the public during Covid-19, Switchback

products, services and benefits they are entitled to. However, these benefits in terms of increasing inclusivity in society can only be realised if there is a widespread uptake of digital identity which will not take place without the introduction of a legislation to set the necessary rule-bound environment in place.

Furthermore, government intervention through a coordinated approach is key to ensure that digital identity is inclusive of anyone who wants one, instead of increasing the social and digital divide. Without a rule-bound market, promoting inclusion will be left in the hands of the organisations who are incentivised to develop products and services that target the market as a whole. As those at risk of being excluded from digital identities represent a minority of the UK population they would not be considered a priority for private sector businesses. Instead, businesses are focused on targeting a larger pool of potential clients when designing their digital identity service due to profit reasons.

The trust framework attempts to foster inclusivity in the digital identity market by requiring companies, and possibly schemes, to report the routes they provide to access their services and how inclusion is considered in their service development to the governance function on an annual basis However, there will not be a requirement for organisations to collect information solely for the purposes of reporting. The information included in the report will be designed to map the avenues to acquiring a digital identity, and encourage a diversity of avenues across the market.

There are many scenarios and situations where exclusion is appropriate or justified. For in the case where an organisation that focuses on scanning passport chips excludes those without a passport. Exclusion is justified in this case as it is integral to the organisation's product. However, organisations will be required to justify the reasoning behind the avenues they offer to access their service.

The governance function aims at ensuring an adequate level of inclusivity in the digital identity market by establishing inclusion principles and helping identify groups which are potentially excluded by the market using the information in the report. Furthermore, the trust framework provides indications to businesses on what approach they should take to proactively address inclusion. For instance by encouraging providers to accept a wide range of evidence of identity and / or eligibility proof including a ‘vouch’, which is a third-party declaration made by someone who knows the user. However, as it is not mandated that any specific action is taken to promote inclusion (other than completing the inclusion report) due to the difficulty around the implementation, there are no guarantees that inclusion in the digital identity market will reach the desired level.

Information asymmetry across UK citizens

Currently, there is a lack of trust and public awareness around digital identity which reduces digital identity uptake across UK citizens as consumers are rightly concerned about the privacy risks of using digital identity due to their lack of knowledge on the subject. Some citizens that may try and find out the security

standards followed by a provider often do not have the technical skills to understand what a safe digital identity or attribute looks like and may therefore opt out entirely. Due to the nature of the digital identity products and services, these justified security and privacy concerns are particularly detrimental to the uptake of digital IDs and must be tackled in order to ensure that the market fully functions.

The Government is therefore required to intervene to tackle the current asymmetric information and enhance trust in the security of the market through “signalling”. To facilitate the signalling process, the governance function will assign a trust mark to the providers that sign up to the trust framework, will maintain a list of trust-marked organisations, and will monitor the performance to ensure the standards are met. In turn, this is expected to reassure the public that those firms follow a known and approved set of standards and promote the uptake of digital identity across the UK public.

Information asymmetry across UK businesses

Although to a lesser extent, the asymmetric information is also present within the private sector as businesses are unaware of what a trusted digital identity solution looks like, meaning they cannot be sure what they produce meets existing regulatory requirements, such as anti-money laundering regulations. This lack of market structure and overarching guidance, creates uncertainty for businesses and reduces their willingness to invest in digital identity.

The UK Government is therefore required to intervene to create a landscape to facilitate better coordination of the digital identity sector, which the private sector has demonstrated to be unable to independently provide. The governance function will tackle imperfect information across UK businesses by indicating the requirements that digital identities in the UK should meet and providing a way for organisations to demonstrate they follow these requirements. Reducing asymmetric information is expected to boost confidence across businesses, increase efficiency, investment and innovation within the digital identity sector, therefore fostering the growth of the digital identity market.

Furthermore, the asymmetric information currently present in the market prevents the market from functioning in an interoperable way. Without a common set of standards there is a lack of trust across players in the market as organisations do not know the processes followed by others to provide digital identities or attributes. Therefore, an overarching governance function, which is trusted across the market players, is required to reduce the asymmetric information by “signalling” which providers within the market can be trusted. Businesses within the market will be monitored by the body, which has the responsibility to monitor compliance also post-certification, so they will be confident that they are engaging with businesses that are in line with their standards. This should facilitate interactions, transactions and information sharing within the digital identity market.

Summary of market failures

Overall, the combination of these factors prevents the digital identity market from fully developing, placing a significant constraint on the potential of the UK digital economy and the cost benefit opportunities of an international digital identity ecosystem. These cannot be overcome without Government intervention. The Government is therefore required to step in to create a rule-bound environment which supports the market growth and fosters the uptake of digital identity checks.

Evidence Base

Summary: Analysis & Evidence Policy Option 4 (preferred option)

Description:

DE MINIMIS ASSESSMENT

Price Base Year 2021	PV Base Year 2021	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Worst case estimate: 1067.5	**Best case estimate: 5394.0**	**Central case stimate: 3678.0**

COSTS (£m)	**Total Transition** (Constant Price) Years	**Average Annual** (excl. Transition) (Constant Price)	**Total Cost** (Present Value)
Low	469.6	38.4	790.6
High	1876.9	75.6	2392.8
Best Estimate	938.7	51.8	1340.3

Description and scale of key monetised costs by 'main affected groups'

We expect some public sector organisations to have direct familiarisation costs as a result of this legislation. We expect Government Departments to face indirect costs to open their databases for private sector checks if they wish to as a result of this legislation. There are also costs associated with the setting up and running the digital identity governance function until it becomes self sustainable.

We also expect some UK businesses to face indirect costs. For these businesses there are one-off costs to familiarise with their legislation and adapt to the digital verification system. We also expect UK businesses to face indirect annual costs in the form of fees levied by public sector organisations to connect to government-held datasets and to check data. These fees are intended to offset public sector costs and maintain value for money for the taxpayer.

Other key non-monetised costs by 'main affected groups'

We expect businesses to pay to sign up to the trust framework. We also expect businesses to face costs to change the way they work, for instance to set up a digital platform to carry out the checks.

BENEFITS (£m)	**Total Transition** (Constant Price) Years	**Average Annual** (excl. Transition) (Constant Price)	**Total Benefit** (Present Value)
Low	0.0	430.8	**3460.3**
High	0.0	743.6	**6,184.6**
Best Estimate	0.0	613.3	**5018.4**

Description and scale of key monetised benefits by 'main affected groups'

We analysed the benefits in relation to the four use cases we consider in this analysis. The benefits are specific to each use case but mainly focus on the monetary value of the time and resources that digital identity checks would save to businesses and individuals.

Other key non-monetised benefits by 'main affected groups'
The analysis does not consider any non-monetised benefits.

Key assumptions/sensitivities/risks	**Discount rate (%)**	3.5

We expect the market to grow throughout the 10 year appraisal period until it reaches its steady state. We assume that at that point the benefits may be fully realised and the annual number of checks may become fairly constant over time.

We also expect the costs and benefits to only impact UK medium and large businesses as we assume that small-micro UK firms will be less inclined to carry out identity checks digitally as their expected benefits are less likely to outweigh the expected costs[15].

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs: 0	**Benefits:0**	**Net: 0**	0

[15] This is an assumption we have made based on the fact that, for instance, small-micro businesses hire less staff members and therefore carry out right to work checks less frequently. Therefore, they would benefit less than medium and large businesses from adapting to digital checks. We believe that small and micro firms would have to invest similar resources to larger businesses in order to familiarise with the legislation and adapt the business to digital identity checks. Hence, their expected benefits are less likely to significantly outweigh the expected costs, making small-micro firms less inclined to use digital identity.

Monetised and non-monetised costs and benefits of each option (including administrative burden)

The digital identity uptake scenarios

Steady state:

The total number of digital identity checks we expect to take place under the steady state is detailed in table 3 at the end of this section, we have assumed all of these checks will become digital and that the proxies used to estimate the number of checks in the research project capture the majority of checks within these use cases. For the steady state to occur requires different government data sets to be opened depending on the use case. From discussion with policy colleagues we understand that the majority of use cases rely on passport data. These use cases cover DBS checks, RTW checks, travel and ticketing, home buying and, trusted financial transactions. The only use case that requires a different dataset is for the qualification checking use case. Qualification checking either needs access to professional bodies datasets or requires something simpler like a portal for uploading qualification certificates.

Central estimate:

In the central estimate scenario, public sector bodies make the necessary technical changes to allow the digital identity market to grow at different times. For instance because different departments may have different levels of willingness to promptly allow private sector checks. In this scenario, we assume that the checks that rely only on Passport data start in year 2, those that require passport data and guidance being updated start in year 3 and the remaining checks that rely on datasets other than passport data begin in year 5.

Therefore, the central scenario assumes that the digital ID checks in relation to travelling and trusted financial transactions checks and home buying are possible from year two onwards. Whereas, digital DBS, RTW and qualification checks are possible from year 2, 3 and 5 respectively.

We assume that digital identity uptake follows a linear upwards trend towards the steady state level of the digital identity market. We consider the steady state level to the point at which the estimated benefits are fully realised. This will be reached when the required datasets are open for private sector checks and necessary rule-based changes have been made. The speed at which the steady state is reached, which is reflected in the slope of the trendline, varies depending on the scenario.

In the central scenario, the estimated digital identity uptake curve predicts that it may take 7 years for the digital identity market to fully develop since the implementation of the legislation. Therefore, we assume that 100% of the estimated total annual costs to carry out checks and total benefits of using digital identity may be realised from year 7 onwards .

Best estimate:

In the best case scenario, we assume that the checks that require either passport data only or passport data and guidance being updated start one year earlier than what assumed in the central estimate, therefore in year 1 and 2 respectively. Whereas, those that rely on other datasets begin in year 3, 2 years before the central estimate scenario.

Therefore, in this scenario digital checks for DBS, travel authorisation and ticketing, home buying and trusted financial transactions begin in year one, digital RTW checks in year 2 and the qualification checks in year 3.

In this scenario, we predict that the uptake of digital identity takes place at a speed 33% higher relative to the central scenario. Therefore, in the best estimate scenario we assume that it takes 5 years for the digital identity market to be fully realised.

Worst estimate:

In this scenario, we assume that the digital checks for DBS, travel authorisation and ticketing, home buying and trusted financial transactions start in year 3, whilst digital RTW checks in year 4. One year later relative to the central scenario. Whereas, we assume that digital qualification checks, which rely on other datasets, start in year 7.

We assume that the speed of the digital identity uptake is 33% slower than in the central scenario. Therefore, in the most conservative scenario we assume it takes 10 years for the uptake of digital identity to reach 100%.

Table 1 - First year we assume the digital ID check take place

	Central case estimate	Best case estimate	Worst case estimate
DBS checks	2	1	3
RTW checks	3	2	4
Qualification checks	5	3	7
Faster employee mobility for people on short notice periods (second order indirect benefit)	2	1	3
Productivity improvements (second order indirect benefit)	2	1	3
Reduced fraudulent applications (second order indirect benefit)	5	3	7
Travel authorisation and ticketing	2	1	3
Home buying	2	1	3
Trusted financial transactions	2	1	3

Table 2 - Expected linear trend over time of the digital identity market towards the steady state

Years benefits begin:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Central case estimate	15%	30%	45%	60%	75%	90%	100%	100%	100%	100%
Best case estimate	20%	40%	60%	80%	100%	100%	100%	100%	100%	100%
Worst case estimate	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Table 3 - Total number of annual DI checks at steady state by use case	
DBS checks	7,174,588 - 9,694,574[16]
RTW checks	8,225,000
Qualification checks	1,727,250
Travel authorisation and ticketing	259,595,875
Home buying	8,882,775
Trusted financial transactions	860,772
Total	285,184,531

Monetised benefits of each scenario

Deloitte carried out a quantitative analysis of the potential economic value of the annual benefits of having a fully functioning digital identity market in four specific use cases (this report was produced in 2020 and is available upon request).[17] For the purpose of our analysis we modelled the potential indirect benefits[18] over the appraisal period based on the Deloitte calculations[19]. We assume that the annual estimations offered by Deloitte assume that the steady state market level has been reached. The monetary values used in the Deloitte analysis have been inflated to 2021 prices to ensure the estimated benefits are comparable with the estimated costs[20].

The estimated total values of the benefits over the 10 year appraisal period in the benefit analysis are undiscounted. The NPV has only been considered for the net benefits We modelled the benefits based on three potential scenarios to attempt to define what the total benefits to private organisations and individuals of having a fully functioning digital identity market may be given different assumptions. We consider the Deloitte estimates to be the value the benefits may take when the digital identity market reaches its steady state. Therefore, we assume it may take a few years to achieve the estimated size of the benefits. We assume that the total annual value of the benefits varies depending on the speed at

[16] Unlike for other DI checks, for DBS we have a forecast of the number of checks each year over the 10 year appraisal period. DBS has forecasted 7,174,588 checks in Year 1. The number of checks is expected to increase over time, and in Year 10 we expect the number of checks to be 9,694,574. See Appendix 2 for forecasted checks for each year.
[17] A full breakdown of the value of the benefits can be found in Appendix 1.
[18] All benefits to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do.
[19] *Economic analysis, Measuring the economic benefits of adopting digital identity,* Deloitte, 2020, is available upon request. Deloitte did not account for overhead costs. We have inflated the wage estimates used in the Deloitte methodology by 22% to account for overhead costs. This is a standard assumption. Furthermore, Deloitte's original estimates were based on a volume of 5,892,859 DBS checks. However, since then, DBS provided us with forecasts of checks. The estimates below are based on an average derived from the forecast (see Appendix 2).
[20] Where the costs have not changed the values have remained the same. For values for whom the year was unclear we assumed the values were in 2020 prices.

which the benefits are realised. The values we estimate increase linearly over time but at different rates depending on the scenario.

To allow the full realisation of the market, departments need to remove the barriers within their policy areas that currently prevent the market from fully developing, such as allowing private-sector checks against their databases. Therefore, we expect these benefits to arise conditional on the fact that departments make the necessary technical changes to fully unlock the development of the market. As such these are all indirect benefits.

Indirect benefits calculations

Employee mobility[21]

First order indirect benefits

According to the Deloitte analysis, a fully functioning digital identity market may positively impact employee mobility by:

- **Digitising the right to work checks process:** This process requires all employers to check the identity of the individual being hired and their right to work in the UK.
- **Allowing digital qualifications checks:** Refers to the process used by employees to verify the qualifications of professionals being hired.
- **Allowing digital employment status checks**: This is the EU Settlement scheme process run by the Home Office to allow EU citizens to remotely verify their identity through an app.

Deloitte examined the benefits of using digital identity to reduce friction in employee mobility and predicted that digital identity checks may bring monetised benefits by:

- **Improving delivery:** New hires can reduce onboarding time by proving their identity digitally for right to work (RTW checks), to carry background checks and to provide proof of qualifications in a significantly faster, self-service way and receiving a real-time response and confirmation.
- **Reducing costs:** Reduce administrative effort by minimising face-to-face and document verification for RTW, DBS and qualification checks.

DBS checks: estimation

Depending on the assumptions taken in each scenario and the slope of the digital identity uptake trendline, we estimate that the total undiscounted benefits over the appraisal period of carrying out digital DBS checks range from £107.11m to £164.79m. The central estimate is £144.19m, where we assume that the benefits are first released in year 2.

Right to work (RTW) checks: estimation

We assume that the benefits of carrying out digital RTW checks may be realised in year 2 and 4 in the best and worst case scenario respectively. Therefore, the total estimated value of the undiscounted benefits over the appraisal period ranges from £275.50m to £438.55m. In the central scenario we assume that the benefits are realised in year 3 and add up to £376.71m.

Qualification checks: estimation

[21]For this use case we separate the benefits between first order and second order indirect benefits. The first order indirect benefits arise from the growth in digital identity use within this use case and the latter arise from additional behavioural changes as a result of a fully functioning digital identity market.

The estimated year when the benefits of carrying out digital qualification checks are realised range from year 2 to year 7, with a central estimate of year 5. Therefore, the total estimated value of the undiscounted benefits over the appraisal period range from £150.27m to £327.05m, with a central estimate of £249.71m.

Table 4 - Employee mobility: first order benefits, £, millions[22]

		Central case estimate	Best case estimate	Worst case estimate
DBS checks	Annual value of the benefits	20.6		
	Estimated year the benefits begin to take place	2	1	3
	Benefits over the 10 year appraisal period (undiscounted)	144.19	164.79	107.11
RTW checks	Annual value of the benefits	56.22		
	Estimated year the benefits begin to take place	3	2	4
	Benefits over the 10 year appraisal period (undiscounted)	376.71	438.55	275.50
Qualifications check	Annual value of the benefits	44.20		
	Estimated year the benefits begin to take place	5	3	7
	Benefits over the 10 year appraisal period (undiscounted)	249.71	327.05	150.27
Total first order indirect benefits (includes DBS, RTW and qualification checks)	Annual value of the benefits	121.02		
	Estimated year the benefits begin to take place	2	1	3
	Benefits over the 10 year appraisal period (undiscounted)	770.61	930.40	532.88

Second order indirect benefits

Deloitte also expects digital identity to bring the following second order indirect benefits to employee mobility:

- **Increased efficiency in sectors with short notice periods:** Employees in industry with short notice periods or that are expected to start work immediately (e.g. hospitality) may be less likely to miss their start date due to lengthy and inefficient RTW checks.
- **Productivity improvements:** Less trips may be required to issue the necessary documentation. This may particularly benefit shift workers with unpredictable shift patterns who may struggle to get their documents verified during the typical office hours.
- **Reduce fraud:** Hiring workers with false credentials can lead to significant losses for businesses and consumers, especially in key sectors such as medical professions and aviation. Digital identity checks are more likely to detect fraudulent applications,

[22] The annual values of the benefits assume that the digital identity market has reached its steady state.

and thus reduce the number of fraudulent workers hired, relative to traditional right to work checks.

For second order benefits related to faster employee mobility for workers on short notice periods and productivity improvements we assume are gradually realised. The first proportion of these benefits that is realised equals the number of DBS checks over the total volume of employee mobility checks and is realised once DBS checks start. This is followed by the proportion of RTW checks when RTW checks begin and the remaining is realised when digital qualification checks start.

Lastly, we assume that 100% of the second order benefits related to reduced fraud are unlocked by digital qualification checks. This is because we expect that most of the savings arising from reduced fraud will arise from recognising employees with false credentials by carrying out digital qualification checks.

We assume that the indirect benefits begin to take place when digital DBS checks become available. Therefore, we estimate that the total undiscounted value of the indirect benefits of using digital identity to increase employee mobility may range from £579.47m to £1,588.44m, with a central estimate of £1,060.59m.

Table 5 - Employee mobility: second order benefits, £, millions

		Annual value of the benefits[23]	Estimated year the benefits begin to take place	Benefits over the 10 year appraisal period, £ millions (undiscounted)
Central case estimate	**Faster employee mobility for people on short notice periods**	53.06	2	362.28
	Productivity improvements	22.36	2	152.67
	Reduced fraudulent applications	96.57	5	545.64
Best case estimate	**Faster employee mobility for people on short notice periods**	53.06	1	418.35
	Productivity improvements	22.36	1	176.29
	Reduced fraudulent applications	134.30	3	993.80
Worst case estimate	**Faster employee mobility for people on short notice periods**	53.06	3	266.90
	Productivity improvements	22.36	3	112.47
	Reduced fraudulent applications	58.85	7	200.09
Central case estimate: total indirect benefits		**172.00**		**1060.59**
Best case estimate: total indirect benefits		**209.72**		**1588.44**
Worst case estimate: total indirect benefits		**134.28**		**579.47**

Total indirect benefits employee mobility

[23] The annual values of the benefits assume that the digital identity market has reached its steady state.

Overall, in the central scenario, we assume that the annual value of the undiscounted first and second order benefits for this use case may be £293.02m, which adds up to £1,831.2m over the entire appraisal period. Whereas, the lower and upper bounds of the estimated benefits over the appraisal period are £1,112.3m and £2,518.89m respectively. This value includes both the estimated benefits for private organisations and for individuals.

Benefits to private organisations and to individuals (including both first and second benefits)

We estimate that businesses may obtain the full economic value of the benefits of carrying out digital qualification checks.

We expect private organisations to gain around 30% of the total value of the benefits unlocked by digital DBS checks and around three quarters of the value of those related to digital RTW checks.

We assume that private sector organisations may receive the total value of the second order benefits related to carrying out digital ID checks within this use case.

Table 6 - Employee mobility: first and second order benefits, £, millions[24]

		Central case estimate	Best case estimate	Worst case estimate
First order benefits	Annual value of the benefits	121.02		
	Estimated year the benefits begin to take place	2	1	3
	Benefits over the 10 year appraisal period (undiscounted)	770.61	930.40	532.88
Second order benefits	Annual value of the benefits	172.00	209.72	134.28
	Estimated year the benefits begin to take place	2	1	3
	Benefits over the 10 year appraisal period (undiscounted)	1060.6	1588.4	579.5
Employee mobility, total benefits	Annual value of the benefits	293.02	330.74	255.30
	Benefits over the 10 year appraisal period (undiscounted)	1831.2	2518.8	1112.3

Travel authorisation and ticketing

According to the Deloitte analysis, a fully functioning digital identity market can streamline the travel authorisation and ticketing process by:

- **Allowing digital passport data verification when booking a flight:** Refers to the process of digital passport details collection by airlines. The airline may integrate a remote identity verification passengers may use to submit their details for real-time verification.
- **Reducing in-journey ID verification:** Refers to the process of setting up digital identity checks to potentially reduce the numerous ID verification steps an individual needs to carry throughout a journey (e.g. at check-in or when renting a car). Digital identification may be used at any step of the journey, starting from when the ticket is

[24] The annual values of the benefits assume that the digital identity market has reached its steady state.

booked to when the luggage is collected. Stakeholders which may be affected by digital in-journey ID checks include travel booking agents, airports, railway stations, port authorities, airlines, car hire service.

Therefore, using digital identity in the context of this specific use case may bring benefits through:

1. **Improved delivery:** Costs for businesses and individuals may be reduced as digital identity may allow faster and more frictionless travel. For instance, passport information could be instantaneously validated allowing real-time response and confirmation reducing wait times.
2. **Reduced costs:** Fines arising for individuals from incorrect data input may be reduced and the interactions required throughout a journey could be minimised (e.g. by providing an alternative to in-person passport controls)

In the central scenario we assume that the benefits take place for the first time in year 2. Whereas, in the best and worst case scenarios we assume year 1 and year 3 respectively.

Given the different set of assumptions and the estimated annual values of the benefits, we estimate that the total value of the undiscounted benefits of carrying out ID checks related to travel authorisation and ticketing digitally in the UK over the appraisal period may be between £1544.02m and £2375.42m. The central estimation of the benefits over the entire appraisal period of £2078.49m. These estimates are based on the assumption that the annual value of the benefits is £296.93m. These values account for both private organisations and individuals.

Benefits to private organisations and to individuals

We estimate that almost 90% of the total value of the benefits is expected to be received by private UK citizens. Therefore, individuals are expected to benefit from digital travelling authorisation and ticketing identity checks the most.

Table 7 - Travel authorisation and ticketing: indirect benefits, £, millions

	Annual value of the benefits[25]	Estimated year the benefits begin to take place	Benefits over the 10 year appraisal period (undiscounted)
Central case estimate	296.93	2	2078.49
Best case estimate		1	2375.42
Worst case estimate		3	1544.02

Home buying

The full use of digital ID throughout the home buying process is expected to reduce friction. The considered steps of the home buying process are:

- Setting up a savings account
- Searching the property
- Bidding for the chosen property
- Requesting and receiving the funding (e.g. mortgage application)
- Closing the contracts (e.g. mortgage contract)
- Moving in (e.g. having to change doctors or schools)

[25] The annual values of the benefits assume that the digital identity market has reached its steady state.

- Registering transfer of title at HM Land Registry

Specifically, Deloitte estimates that applying digital identity in the context of home buying is expected to bring monetised benefits by:

1. **Improving delivery:** Digital identity checks may streamline the home buying process and offer real-time response and confirmation of the various steps required for home ownership (e.g. when applying for a mortgage)
2. **Reducing costs:** Using digital identity may reduce administrative effort from face-to-face and document verification.

We assume that the benefits are realised for the first time between year 1 and year 3.

Given the set of assumptions of each scenario, we estimate that, over the appraisal period, the total value of the undiscounted benefits of using digital identity to carry out ID checks throughout the home buying process may be between £691.37m and £1,063.64m, with a central estimate of £930.68m.
The estimates are based on the assumption that the annual value of the benefits is £132.95m. These values include benefits for both private organisations and individuals.

Benefits to private organisations and to individuals

Through our calculations we estimate that carrying out digital ID checks for this use case will mostly benefit private UK organisations as only 15.3% of the total value of the benefits is expected to go to UK citizens.

Table 8 - Home buying: indirect benefits, £, millions

	Annual value of the benefits[26]	Estimated year the benefits begin to take place	Benefits over the 10 year appraisal period (undiscounted)
Central case estimate	132.95	2	930.68
Best case estimate		1	1063.64
Worst case estimate		3	691.37

Trusted financial transactions

According to Deloitte, a fully functioning digital identity market is expected to help ensure that financial transactions are secure by:

- **Improve customer on-boarding to financial services products (e.g. bank accounts):** Refers to the process used by financial services to check the identity of their customers during the onboarding process or when accessing a service.

- **Authenticate transactions to reduce fraud:** The use of digital identity products may allow customers to verify their identity when needed, for instance when transacting with an institution online. It may also allow organisations to prove to their customers that they offer a legitimate service, for instance by being a member of the trust framework.

[26] The annual values of the benefits assume that the digital identity market has reached its steady state.

Therefore, according to the Deloitte analysis, using digital identity within this use case is expected to bring monetised benefits by:

- **Improving delivery:** Digital identity may provide a more cost efficient alternative to in-person interaction during on-boarding identity checks (KYC checks) for businesses and individuals when opening a bank account. Digital identity gives users a self-service option for identity verification and secure transactions, which saves time by offering a real-time response.
- **Reducing costs:** Using digital identity may reduce administrative effort from face-to-face and document verification and lowers the risk of fraud through upfront ID check.

According to Deloitte's estimations, most of the value of the benefits arising from using digital ID checks to carry out trusted financial transactions arises from using digital ID checks to authenticate transactions.

In the central scenario we expect these benefits to take place from year 2 onwards. Whereas, in the best and worst case scenario we assume they begin to arise from year 1 and year 3 respectively.

Therefore, given the assumptions taken in the scenarios, we estimate that the total value of the undiscounted benefits over the appraisal period for private citizens and businesses together may be between £960.46m and £1477.63m, with a central estimate of £1292.93m. The estimates are based on the assumption that the annual value of the benefits is £184.7m.

Benefits to private organisations and to individuals

According to our estimations, we expect individuals to benefit more from using digital identity to verify financial transactions compared to the private sector as 73% of the total value of the benefits over the appraisal period is attributed to private citizens alone.

Table 9 - Trusted financial transactions: indirect benefits, £, millions

	Annual value of the benefits[27]	Estimated year the benefits begin to take place	Benefits over the 10 year appraisal period (undiscounted)
Central case estimate	184.70	2	1292.93
Best case estimate		1	1477.63
Worst case estimate		3	960.46

Total indirect benefits

Total benefits: central scenario

The central estimation of the ten year undiscounted value of the benefits unlocked by a fully realised digital identity market for the four use cases together is £5401.96m. Whereas, we estimate that the total value of the benefits worst and best case scenario may be £2996.17m and £7,385.92m respectively.

Total benefits to private organisations and to individuals

[27] The annual values of the benefits assume that the digital identity market has reached its steady state.

Given the assumptions taken, we estimate that in the context of this specific use case individuals and businesses are expected to benefit rather equally from digital identity in all three scenarios.

Table 10 - Indirect benefits: total, £, millions

	Annual value of the benefits	Benefits over the 10 year appraisal period (undiscounted)		
		Central case estimate	Best case estimate	Worst case estimate
Employee mobility (including second order)	293.02[28]	1831.2	2518.8	1112.3
Travel authorisation and ticketing	296.93	2078.49	2375.42	1544.02
Home buying	132.95	930.68	1063.64	691.37
Trusted financial transactions	184.70	1292.93	1477.63	960.46
Total	907.61	6133.3	7435.5	4308.2

Monetised and non-monetised costs to private sector organisations (including administrative burden)

We carried out a stakeholder engagement exercise to attempt to define the indirect costs[29] businesses may face to comply with the legislation, both for digital identity as a whole and in relation to the four specific use cases. We engaged with a variety of sectors. Multiple responses came from organisations that currently operate within the digital identity sector, such as identity service providers, or relying parties that would use the digital identification system. Other responses came from various different sectors. The organisations that took part ranged from micro to large businesses.

The engagement enabled us to make some qualitative and quantitative assumptions of what costs businesses may face to familiarise and adapt to the digital identity legislation. Averages of the estimated required resources and their cost provided by the engagement exercise were used to estimate the potential average familiarisation and organisational change costs per business. The engagement exercise provided us with cost estimations in 2021 prices.

The quantitative estimations were then used to model the costs under the three scenarios. Due to the early stage of the legislative planning, it was difficult to precisely estimate what costs businesses are expected to incur. Nevertheless, we expect these costs to be rather small especially for digital identity providers already established in the market as they believe they are expected to undertake limited development work to adapt to the legislation. Estimation of one-off connection fee costs and per check fee costs were provided by a piece of commissioned research. We note that these costs, levied by the public sector on the

[28] This value is based on the central estimate of the value of the annual benefits arising from productivity improvements.

[29] All costs to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do, not even when it comes to familiarisation.

private sector, are intended to offset the costs incurred by the public sector in enabling checks against data it holds, ensuring value for money for the taxpayer. Government does not intend to profit from these fees and their amounts will be kept in review to ensure this is the case.

We assume that only UK medium and large businesses face the costs to adapt to digital identity because their incentive from the potential cost savings allowed by digital identity are expected to outweigh the costs to adapt to the new technology[30]. Therefore, the estimated costs per business were multiplied by the number of medium-large UK businesses to estimate what the costs may be for all businesses as a whole.

We assume that the size of the total per check fees costs follows the estimated trend of the digital identity market towards the steady state. This is because we expect the number of digital identity checks carried out in the UK to be proportional to the size of the market.

One-off familiarisation costs for businesses:

Per business:

Although it is difficult to precisely estimate the potential familiarisation costs at this early stage, we have attempted to model the costs businesses expect to face to familiarise with the potential digital identity legislation based on the estimations provided by the stakeholder engagement exercise. We assume that these costs do not depend on the scenario as we consider these one-off costs that take place in year one independently of when the remaining benefits and costs are realised. All of these costs are indirect as the legislation itself only gives government departments the option to open up their datasets. Therefore any familiarisation by businesses is contingent on governments opting to open their datasets.

We expect that businesses may have to pay members of the legal team to review the legislation. We predict that,on average, it may cost businesses £1,018 for a member of their legal team to understand and review the digital identity legislation. Furthermore, businesses may have to pay for other staff members to spend some time familiarising with the legislation. Given our estimations it may cost on average to businesses around £1,532.8 for non-legal employees to understand the legislation. Potential staff members which may be involved in these tasks include the CEO of the company, product managers and operation directors. Lastly, some businesses may require certain employees, such as a Security Officer, to carry out a technical/security review as part of the familiarisation process. On average, firms estimate that this task may lead to a one-off cost of £1,736.2.

Businesses may also have to invest in resources to train the remaining stakeholders. For instance, businesses may have to pay a member of the legal team and a general counsel to explain the impact of the legislation both internally and to external stakeholders.We expect that for businesses already involved in digital identity, familiarisation costs will be limited as they only need to evaluate how the business is affected by the new legislation, rather than familiarise with digital identity completely.

For instance, we expect that relying parties may have to pay to train the staff members as they are less familiar with the digital identity technology relative to identity providers already established in the market. We also expect that using digital identity in the context of the use cases will bring further costs to familiarise with the legislation within the specific context. However, we expect these further costs to be far less significant.

[30] Data regarding the Number of UK medium and large businesses was collected from the ONS data release: UK "BUSINESS: ACTIVITY, SIZE AND LOCATION - 2020", table 3.

Overall, we estimate that, on average, familiarisation costs may add up to £4,287 for a business. A full breakdown of the costs familiarisation costs different businesses expect to face split by task can be found below:

Table 11 - One-off familiarisation costs to each private sector organisation

Tasks required	Average No. employees required x Median No. of hours required	Gross wage per hour, £ (including 22% overhead costs)	Total cost of the resource committed, per business, £[31]
Legal review to familiarise and evaluate the legislation	18.5	55.0	1018.0
Technical / security review	37.2	46.7	1736.2
Review to familiarise and evaluate the legislation by staff members	25.8	59.4	1532.8
Total cost per business, £			4287.0

The values of the estimated familiarisation costs over the 10 year appraisal period in each scenario have not been discounted.

Central estimate

Multiplying the estimated familiarisation costs per business by the number of UK medium-large businesses leads to a total familiarisation cost of £227.7m for all businesses as a whole.

Best estimate

We assume that the lower bound for the familiarisation costs is 50% of the central estimate. Therefore, in the most optimistic scenario we assume that familiarisation costs may add up to £113.85m for all UK medium and large firms together.

Worst estimate

We assume that the upper bound of the one-off familiarisation costs is twice the central estimate. Therefore, the upper bound for the one-off familiarisation costs is £455.4m for all UK medium and large firms together.

Table 12 - One-off familiarisation costs for private sector organisations

	Estimated one-off familiarisation costs per company, £	Number of UK medium-large businesses	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)

[31] The calculations may not perfectly add up due to rounding errors. The numbers displayed in the table have been rounded to one decimal place but the full numbers were used to calculate the estimated total cost of the resources.

Central case estimate	4287.0	53,115	227.70
Best case estimate	2143.5		113.9
Worst case estimate	8573.9		455.40

One-off organisational change costs for businesses:

Per business:

Organisational change costs consider the costs businesses face to adapt the structure of the organisation, both in terms of how it functions and the staff employed. Examples include the cost to implement a digital identity solution, the cost to hire new staff, or the costs to purchase or change technology platforms. Due to the uncertainty regarding the context of the legislation, it is difficult to make precise cost estimations and define what the impact of legislation for the organisational structure may be at this early stage.

We carried out a stakeholder engagement exercise to gather data on the resources which may be required by an average business to adapt to digital identity. We assume that, on average, each business related to digital identity may take 40 hours to carry out the expected tasks. This is the median number of hours estimated by the respondents to the stakeholder engagement exercise for all their expected tasks. We expect businesses already within the digital identity sector to face little to no organisational change costs. This is because their service is already in place so we predict they may not have to significantly adapt their firm structure to comply with the legislation.

In the central scenario we estimate that, on average, UK private sector organisations related to digital identity will face one-off organisations change costs of £13,370.6 to adapt to digital identity. For each use case, the organisational change costs are estimated by multiplying the estimated cost per business times the estimated number of medium and large businesses related to the specific use case[32]. We estimate the worst and best estimate to be half and double the central scenario respectively.

These are one-off costs for businesses that are expected to take place the year that the benefits for each specific use case are unlocked. Therefore, the exact year these costs take place varies for each use case depending on the specific scenarios assumptions. On average, we assume businesses invest £6,306.9 to allow the chief procurement officer (CPO) or other members of the management team to adapt their process to the legislation. We also predict that developers or the chief technical officer (CTO) may have to adapt their technology and user experience to digital identity. Given the available information, the expected cost of this task to be £5,045.5. Whereas, the costs to comply and implement the legislation are estimated to add up to £2,018.2 and involve either a compliance manager or another member of the senior management team.

A full breakdown of the estimated costs can be found below:

[32] For employee mobility we used all UK medium-large firms. For travelling authorisation and ticketing we summed the number of UK firms in the following sectors: “Land transport and transport via pipelines,” “Water transport”, “Air transport” and “Travel agency; tour operator and other reservation services and related activities”. For home buying we included the medium-large UK firms in the “Real estate activities” sector. For the trusted financial transaction use case we included all medium-large firms in “Financial service activities; except insurance and pension funding”, “Insurance; reinsurance and pension funding; except compulsory social security” and “Activities auxiliary to financial services and insurance activities”. Data Source: UK business: activity, size and location, 2020

Table 13 - One-off organisational change costs to each private sector organisation			
Tasks required	**Average No. employees required x Median No. of hours required**	**Gross wage per hour, £ (including 22% overhead costs)**	**Total cost of the resource committed, per business, £[33]**
Change the required technology	80	63.1	5045.5
Adapt the process to digital identity	80	78.8	6306.9
Comply with the legislation	40	50.5	2018.2
Total cost per business, £			13370.6

We expect that only the minority of companies will hire workers to comply with the digital identity legislation. Examples of staff members that may be hired include developers[34] to adapt their process to the digital identity technology, new governance staff to comply with the legislation and external audits to ratify any developed solutions.

The values of the estimated organisational change costs over the 10 year appraisal period in each scenario have not been discounted.

Central estimate

Given the estimated costs per business to adapt the organisation to digital identity, in the central scenario we estimate that the one-off organisational change costs for all UK medium-large businesses together may add up to £710.18m over the 10 year appraisal period. This value is undiscounted.

In the central estimate all medium-large businesses face organisational change costs in year 2 when digital DBS checks begin to take place as we assume all medium-large businesses will want to use digital identity to carry out DBS checks. The total estimated value of the organisation change costs in year

Best estimate

Given the assumption that some digital ID checks, for instance digital DBS checks, start in year 1, all medium and large UK businesses face the organisational change costs at the same time in the first year of the appraisal period. We estimate that these one-off costs add up to £355.09m.

Worst estimate

[33] The calculations may not perfectly add up due to rounding errors. The numbers displayed in the table have been rounded to one decimal place but the full numbers were used to calculate the estimated total cost of the resources.

[34] One survey respondent stated it may need to hire 5 full-time developers, each with a gross annual wage of £105,000.

The organisational change costs are assumed to add up to £1420.35m in the most conservative scenario and take place in year 3 for all medium and large UK businesses, when we assume some of the digital ID checks may start.

Table 14 - One-off organisational change costs for private sector organisations

	Estimated one-off organisational change costs per company, £	Estimated year the one-off organisational change costs may take place	Number of UK medium-large businesses	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	13370.6	2	53,115	710.18
Best case estimate	6685.3	1		355.09
Worst case estimate*	26741.1	3		1420.35

One-off connection fee for service providers

Per business:

We assume that organisations wishing to perform checks against government-controlled data may have to pay a one-off fee upfront. Based on research outsourced by DCMS, which used industry engagement to estimate the expected number of checks which may be performed, and the fee charged by the Document Checking Service pilot, we assume that the value of the fee may range from £3,900 to £7,400 with a central estimate of £5,650. These estimations remain constant over time.

We assume that 100 identity service providers may pay this fee and does not vary over time. This is a standard assumption taken to calculate the potential total costs. The number of firms that may pay this connection fee is constant in all scenarios. This is a one-off cost which is expected to be paid the year that the technical changes are applied and digital identity checks can therefore be extensively used. Consequently, the year these costs take place varies depending on the scenario.

Total:

The total value of the connection fee costs is calculated as the estimated connection fee price times the number of service providers we expect will pay it.

Based on the assumptions we have taken, the undiscounted value of the total connection fee costs over the 10 year appraisal period for service providers may be between £0.39m and £0.74m.

The central estimate is £0.57m and it is calculated based on the assumption that the fee per company is £5,650.

Table 15 - One-off connection fee costs for service providers over the 10 year appraisal period

	Estimated one-off connection fee costs per company, £	Estimated year the one-off connection fee costs may take place	Estimated number of service providers	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	5650.0	2	100	0.57
Best case estimate	3900.0	1		0.39
Worst case estimate	7400.0	3		0.74

Certification fee for service providers

Per business:

We expect service providers to pay a certification fee to be certified against some given standards. We estimate the certification fee per business to range from £5,700 to £14,250, with a central estimate of £9,975. These estimations are based on the costs of the ISO 27001 certification which is similar in size and effort as we expect digital identity certification scheme to be. The cost of the fee varies depending on the number of employees. Therefore, larger providers will face higher certification fees.

Despite the certification fee being one-off, providers are expected to also pay on-going certification costs. We assume that providers may have to pay for recertification every 18 months, which we estimate may lead to a repeat cost the same as the connection fee. This is based on the advice of policy colleagues and we believe it to be a conservative estimate that is likely an overestimate.

Total:

Overall, assuming that there are 100 service providers, we estimate that the certification fee for all service providers over the appraisal period may add up to between £3.4 and £3.6m. This fee is paid the year the digital identity checks begin.

Given the assumptions taken in the best case estimate, where the digital identity checks begin in year 1, the overall estimated cost is actually higher than in the worst case estimate. This is because the lower one-off certification fee is outweighed by the higher total value of the annual costs over the 10 years as the recertification costs kick in sooner compared to in the most pessimistic scenario.

Table 16 - Estimated certification fee costs for service providers over the 10 year appraisal period

	Estimated certification fee per company in yr 1, £	Estimated certification fee per company to recertify, £	Estimated year the one-off certification fee costs may take place	No. of times recertified over the appraisal period[35]	Estimated number of service providers	Estimated total certification fee cost over the appraisal period for all businesses, including recertification costs, £, millions
Central case estimate	9975	5000	2	5	100	3.5
Best case estimate	5700	5000	1	6		3.6
Worst case estimate	14250	5000	3	4		3.4

Annual membership fee for service providers

We expect certified service providers to pay the governance function an annual membership fee.

Per business:

We assume that organisations wishing to perform checks against government-controlled data may have to pay an annual fee. Research outsourced by DCMS assumes that the annual value of the fee may range from £4,625 to £6,425 with a central estimate of £5,525 and is constant over time.

We expect this annual cost to start taking place the year that digital identity checks begin and to then take place every year. Therefore, the year it starts being paid varies depending on the scenario.

Total:

The total value per year of the membership fee costs is calculated as the estimated connection fee price times the number of service providers we expect will pay it.

Based on the assumptions we have taken, the undiscounted value of the total connection fee costs over the 10 year appraisal period for service providers may be between £4.63m and £5.14m. Whereas, the central estimate is £4.97m.

[35] Excluding year 1

Table 17 - Annual membership fee costs over the 10 year appraisal period				
	Estimated annual membership fee per company, £	Estimated year the annual membership fee costs may begin to take place	Estimated number of service providers	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	5525.0	2	100	4.97
Best case estimate	4625.0	1		4.63
Worst case estimate	6425.0	3		5.14

Costs to carry out digital ID checks for each use case: Annual cost of per check fees for businesses

We assume that UK businesses wishing to make digital identity checks against government-held databases may have to pay a fee in order to carry out each check. These costs may start to be incurred when the responsible Government bodies allow the private sector to access their databases to make the ID verifications. We calculate this annual cost as the annual total expected number of checks times the expected price per check.

We estimate the per check fee may range from 15p to 50p, with a central estimate of 25p per check. The central estimate is based on advice from policy teams after having reviewed the current Document Checking Service pilot with HMPO and GDS. Whereas, the lower estimate is a 50% reduction on the central estimate and the higher estimate uses directly the current charge from the pilot.

It should be noted that these are estimates and not commitments to any particular price point. In addition, certain data is likely to cost more than the central estimate as the cost of providing it is higher. For example, a yes/no passport check supplied through the Data Verification Application (DVA) is currently priced at 35p and that price may remain, with any wider attribute provision likely being priced higher. All prices will be subject to periodic review to ensure best value for money for the taxpayer.

We expect the number of digital ID checks to increase over time until the digital identity market reaches its steady state. This is because we assume that there may be a positive correlation between size of the digital identity market and annual total number of digital ID checks. Therefore, we estimate that the total estimated costs to carry out the checks increase over time depending on the size of the digital identity market, which in turn follows the estimated trend of the market towards its steady state. The rate of change of this trend varies on the chosen scenario.

To calculate the annual cost of carrying out checks we multiplied the annual volume of checks related to each use case estimate by Deloitte by the estimated price per check

Table 18 - Annual volume of checks estimated by Deloitte, millions	
DBS checks	7.17 - 9.69*
RTW checks	8.23
Qualification checks	1.73
Travel authorisation and ticketing	259.60
Home buying	8.88
Trusted financial transactions	0.86

***** *The volume of DBS checks used in the appraisal was provided by DBS, not Deloitte. See Appendix 2 for more detail.*

This annual cost also varies depending on the year that the required datasets become available for digital identity checks[36]. The estimated years are displayed below. These are the same years we assume the benefits may begin to occur.

The total costs over the 10 year appraisal period do not equal the annual costs multiplied by 10 because we assume that it takes a few years for the market to reach its steady state. The estimated total value of these costs over the 10 year appraisal period have not been discounted.

DBS checks: total per-check fees costs

Based on the assumptions we have taken in each scenario, we estimate that the total cost over the appraisal period of per-check fees to carry out DBS checks digitally may be between £10.36m, in the most optimistic scenario, and £23.15m, in the most conservative scenario.

The central estimate for the annual cost is £2.42m[37], assuming the steady state level of the market, which leads to a total estimated value of £15.31m over the 10 year appraisal period.

RTW checks: total per-check fees costs

Based on the set of assumptions we have taken in each scenario, the estimated total cost of the fees to carry out RTW checks over the appraisal period may be £9.62m and £20.15m.

Whereas, in the central scenario the total estimated annual value is £2.06m once the digital identity market reaches its steady state, which results in a total value over the appraisal period of £13.78m.

Qualification checks: total per-check fees costs

Given the various assumptions taken in the most optimistic scenario, the total cost of the per-check fees over the appraisal period may be £1.92m. In the most conversative scenario the estimated value is £2.96m.

[36] The years we assume that digital identity checks begin in the scenarios for the four use cases are displayed in table 1.
[37] This annual cost figure is based on the number of DBS checks forecasted for year 10 (see Appendix 2 for more detail).

The central estimate scenario assumes that the annual cost once the market has reached its steady state is £0.43m for all businesses together. Whereas, the estimated total value over the appraisal period is £2.44m.

Employee mobility: total per-check fees costs

Adding together the three different ID checks related to this use case, the central estimate of the total cost of per check fees over the appraisal period is £31.53m.

We estimate that, over the appraisal period, this value may range from £21.90m to £46.23m depending on the scenario.

Table 19 - Employee mobility: per-check fees costs[38]

		Central case estimate	Best case estimate	Worst case estimate[39]
per-check fee, £		0.25	0.15	0.50
DBS checks	Annual estimated number of checks, millions	7.17 - 9.70		
	Annual estimated costs, £, millions[40]	2.42	1.45	4.85
	Estimated year the digital ID checks begin to take place	2	1	3
	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)	15.31	10.36	23.15
RTW checks	Annual estimated number of checks, millions	8.23		
	Annual estimated costs, £, millions	2.06	1.23	4.11
	Estimated year the digital ID checks begin to take place	3	2	4
	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)	13.78	9.62	20.15
Qualifications checks	Annual estimated number of checks, millions	1.73		
	Annual estimated costs, £, millions	0.43	0.26	0.86
	Estimated year the digital ID checks begin to take place	5	3	7
	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)	2.44 1.92	1.92	2.94

[38] The displayed annual costs and annual volume of checks assume that the steady state market level is reached.
[39] Total value of worst case is lower than the central because far fewer checks are carried out (this also mean fewer benefits)
[40] Based on Year 10 forecast of the number of DBS checks (see Appendix 2 for more detail).

Employee mobility, total	Annual estimated number of checks, millions	~18.33[41]		
	Annual estimated costs, £, millions	4.91	2.95	9.82
	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)	31.53	21.90	46.23

Travel authorisation and ticketing: total per-check fees costs

Given the set of assumptions we have taken in each scenario, the total costs of per-check fees over the 10 years is £311.52m in the best case scenario and £674.95[42]m in the worst case scenario.

Whereas, the annual estimate in the central scenario, assuming the steady state market level, is £64.90m. Therefore, the central estimate of the total cost of per-check fees over the appraisal period of £454.29m.

Table 20 - Travel authorisation and ticketing: per-check fees costs[43]

	Per-check fee, £	Annual estimated number of checks, millions	Annual estimated costs, £, millions	Estimated year the digital ID checks begin to take place	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	0.25	259.60	64.90	2	454.29
Best case estimate	0.15		38.94	1	311.52
Worst case estimate	0.5		129.80	3	674.95

Home buying: total per-check fees costs

Based on the assumptions in each scenario, we estimate that the cost of the per-check fees to digitally carry out the ID checks over the appraisal period may range from £10.66m in the best case scenario to £23.10m in the worst case scenario.

Assuming that the digital identity market reaches the steady state, the central estimate of this annual cost is £2.22m. This translates into an estimated total cost over the 10 years of £15.54m.

Table 21 - Home buying: per-check fees costs[44]

[41] The average of the forecasted DBS checks was used to arrive at this number (in actuality it will vary with the number of DBS checks).
[42] This is lower than the central due to the far fewer checks in this scenario. The per check cost is higher.
[43] The displayed annual costs and annual volume of checks assume that the steady state market level is reached.
[44] The displayed annual costs and annual volume of checks assume that the steady state market level is reached.

	Per-check fee, £	Annual estimated number of checks, millions	Annual estimated costs, £, millions	Estimated year the digital ID checks begin to take place	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	0.25	8.88	2.22	2	15.54
Best case estimate	0.15		1.33	1	10.66
Worst case estimate	0.5		4.44	3	23.10

Trusted financial transactions: total per-check fees costs

The cost over the 10 year appraisal period to carry out the expected volume of digital ID checks related to financial transactions may range from £1.03m in the most optimistic scenario to £2.24m in the most pessimistic scenario.

The central estimate for the total annual cost to carry out the checks, given that the steady state market level is reached, is £0.22m. This leads to a central estimate of the total cost of the per check fees of £1.51m over the appraisal period.

Table 22 - Trusted financial transactions: per-check fees costs[45]

	Per-check fee, £	Annual estimated number of checks, millions	Annual estimated costs, £, millions	Estimated year the digital ID checks begin to take place	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	0.25	0.86	0.22	2	1.51
Best case estimate	0.15		0.13	1	1.03
Worst case estimate	0.5		0.43	3	2.24

Total indirect costs to private sector organisations

The estimated total costs include the estimated total cost of the per check fee for all four use cases, one-off familiarisation costs, one-off organisational change costs for the relying parties and one-off total connection fees and membership fees for service providers. The central estimate of the undiscounted costs to UK private sector organisations is £1,449.78m over the 10 year appraisal period. We estimate that the lower and upper bound of the total

[45] The displayed annual costs and annual volume of checks assume that the steady state market level is reached.

undiscounted costs all medium and large businesses together may face over the appraisal period are £822.63m and £2,631.58m respectively.

Table 23 - Private sector costs: total over the 10 year appraisal period, £, millions

£, millions	Central estimate		Best estimate		Worst estimate	
	Annual estimated costs, £, millions	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)	Annual estimated costs, £, millions	Estimated costs over the 10 year appraisal period, £, millions,(undiscounted)	Annual estimated costs, £, millions	Estimated costs over the 10 year appraisal period, £, millions,(undiscounted)
Employee mobility: per check fee costs	4.91	31.53	2.95	21.90	9.82	46.23
Travel authorisation and ticketing: per-check fee costs	64.90	454.29	38.94	311.52	129.80	674.95
Home buying: per-check fee costs	2.22	15.54	1.33	10.66	4.44	23.10
Trusted financial transactions: per-check fee costs	0.22	1.51	0.13	1.03	0.43	2.24
One-off familiarisation costs		227.70		113.85		455.40
One-off organisational change costs		710.18		355.09		1420.35
One-off connection fees costs for service providers		0.57		0.39		0.74
Certification fees cost for service providers		3.5		3.6		3.4
Annual membership fee for service providers	0.6	4.97	0.5	4.6	0.6	5.1
Total, £, millions		1449.78		822.63		2631.58

Costs for public sector organisations

We engaged with three public bodies to try and estimate the costs[46] public organisations may pay to adapt to the potential digital identity legislation and thus allow the digital identity market to fully develop. For instance, we gathered some information on the potential costs public sector bodies may face to understand the legislation or make the organisational changes required to allow the private sector to check the databases they hold. We expect

[46] All costs to Government bodies are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for public sector organisations to do.

public sector organisations to face some rather significant costs to adapt to the legislation, especially to allow the private sector to make checks against the Government-held datasets.

We define the worst case estimate as the scenario based on the assumptions that lead to the highest expected costs. We predict high costs for all public sector bodies in a high digital identity uptake scenario where more Departments invest resources to familiarise and adapt to the digital identity system. In order for digital identity to fully develop a high uptake across public sector bodies is required. Therefore, the worst case cost estimate is not necessarily unwelcomed.

For the worst case scenario we have assumed that all departments that may hold significant identity or eligibility data, 9 in total[47], will face these costs. For the central and best case scenario we have assumed that only Home Office, DVLA, DWP, HMRC, and DfE[48] in line with the four digital identity use cases analysed.

Familiarisation costs for public sector organisations

Based on our assumptions we estimate that, on average, public sector bodies may face a one-off cost of £43,637 to ensure that members of the policy teams familiarise with the legislation. However, these are rough estimates based on a small sample size so should be considered indicative only.
We expect public sector bodies to involve both members of the policy and legal teams in the familiarisation process. For instance, according to HMPO one member of the Bills and Legislation team may spend roughly 150 hours researching the policy whilst another member of the same team may spend a similar number of hours on policy approval and governance.

A full breakdown of the potentially required tasks and their estimated costs can be found below:

Table 24 - One-off familiarisation costs to each Government Department

Tasks required	Average No. employees required x No. of hours required	Gross wage per hour, £ (including 22% overhead costs)	Total cost of the resource committed, £
Familiarise with the legislation (various employee)	127.5	38.8	4943.4
Familiarise with the legislation (policy team)	123	38.6	4746.0
Familiarise with the legislation (legal team)	150	38.8	5815.8
Training	811	34.7	28131.8
Total cost, £			43637

[47] The 9 Departments are: Home Office, DWP, HMRC, DVLA, DfE, HM Land Registry, DHSC, Companies' house, and MoJ.
[48] These are the Departments that are required to open their databases in order for digital identity checks to be carried out in the four use cases.

Depending on the set of assumptions we take, we assume that the one-off familiarisation costs for public sector bodies may range from £0.22m to £0.47m, with a central estimate of £0.22m.

Table 25 - One-off public sector familiarisation costs

	Estimated one-off familiarisation costs per Department, £	Number of Government Department	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	43,637	5	0.22
Best case estimate	43,637	5	0.22
Worst case estimate	43,637	9	0.39

Indirect costs to public sector organisations

Cost to allow private sector access to Government-held datasets for public sector organisations

We expect Government Departments to face costs both to allow the private sector to make checks against their data and to maintain the system in place. The costs estimated are baseline and in practice will be subject to iteration.

Table 26 - One-off organisational change costs to each Government Department

Tasks required	Job role	No. employees	No. hours required	Total cost of the resources committed, including 22% overhead costs, £
Build and expose external facing API portal	Software engineer, Product owner, User researcher, Business analysts, QA engineer, DevOps, Agile Delivery Manager	14	975	c. £469.7K
Provide additional capacity and protection on source systems	Software engineer, User researcher, Business analysts, QA engineer, DevOps	30	975	c. £1006.5K
Provide additional monitoring and alerting and support	Software engineer, User researcher, Business analysts, QA engineer, DevOps	12	1950	c. £805.2K

Development of edge services (API's) to allow 3rd party request relating to ID Access Management operation	At least one Agile squad with the required resources	10	978	c. £512.4K + £0.5M[49] (contingency)
Total cost, £				c. £3.3M

According to DWP the costs arise mainly from creating the external facing API portal and arranging a suitable level of protection and monitoring, alerting and support systems. Employers that may be involved in completing these tasks include software engineers, user researchers and business analysts. The Department expects to face a one-off cost of c. £3.3m to set up the system for private sector checks. Therefore, it expects the costs to be rather substantial.

Just like for the public sector familiarisation costs, we have assumed that the organisational change costs are faced by 5 departments in the central and best cases and 9 Departments in the worst case estimates. Due to uncertainty around the figures and given the GDS technical work ongoing on the 'one login for government' we have adjusted how much of these costs can be allocated to our intervention. For the worst case scenario we have chosen to be conservative and assume 100% of the proposed organisational change costs will accrue to our intervention. For the central and best case scenarios we assume that half of the costs can be allocated to our intervention.

Given the set of assumptions we have taken, we estimate that over the appraisal period, the public sector may have to invest between £8.25m and £29.70m to allow the private sector to make checks against their databases.

Table 27 - One-off public sector organisational change costs

	Estimated one-off organisational change costs per Department, £, millions	Number of Government Department	Estimated one-off costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	1.7	5	8.25
Best case estimate	1.7	5	8.25
Worst case estimate	3.3	9	29.70

Costs to Government departments to maintain the system for private sector checks

Table 28 - Cost per Government Department to maintain the digital identity system

Tasks required	**Job role**	**No. employees**	**No. hours required**	**Total cost of the resources committed,**

[49] This value does not include overhead costs.

				including 22% overhead costs, £
Build and expose external facing API portal	Software engineer, Product owner, User researcher, Business analysts, QA engineer, DevOps, Agile Delivery Manager	14	1950	c. £939.4K
Provide performance capacity reviews on source systems	Architects, Software engineers, Business analysts, Service designers	30	1950	c. £549K
Provide additional monitoring and alerting and support	Software engineer, User researcher, Business analysts, QA engineer, DevOps	8	1950	c. £4099.2K
Transaction processing	Members of the technical / service management team	Unknown	Unknown	Likely to be transaction based
Additional infrastructure and hosting costs	Unknown	Unknown	Unknown	£200K[50]
Total cost				c. £5.79M

DWP estimates the recurring costs it may face to maintain an adequate system, most of which are similar to those required to set up the system in the first place.

According to their estimations the costs to maintain this system in place may add up to roughly £5.79m a year.

An example of a recurring task which may be required is investing in additional monitoring, alerting and support. This task may require the full time commitment of 8 employees (e.g. software engineers, user researchers) and is likely to cost roughly £4.1m per annum to the department.

DWP estimates that on top of recurring staffing requirements to allow the private sector to make checks against their data, it may face costs to maintain a suitable infrastructure. This is estimated to cost c. £0.2m per year. Due to uncertainty we have taken the same approach as the one-off organisational change costs, that is that the worst case scenario has full cost, and both the central and best cases have half cost..

Given the assumptions we have taken, we estimate that maintaining the system may cost the public sector between £14.48m and £52.11m every year. With a central estimate of £14.48m.

Table 29 - Public sector annual costs to maintain the system over the 10 year appraisal period

[50] This value does not include overhead costs.

	Estimated annual maintenance costs per Department, £, millions	Number of Government Department	Estimated total annual costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	2.9	5	14.48
Best case estimate	2.9	5	14.48
Worst case estimate	5.8	9	52.11

Therefore, adding together the one-off and annual organisational change costs for the public sector leads to an estimated value over the appraisal period of between £138.53m and £374.0m. The central estimate is £138.53m.

Table 30 - Public sector costs to build and maintain the system over the 10 year appraisal period

	Number of Government Department	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)
Central case estimate	5	138.53
Best case estimate	5	138.53
Worst case estimate	9	498.69

Cost to set up and run a governance function

The digital identity market may function in a trusted and interoperable way conditional on the fact that there is an effective governance function overseeing the market. For instance, we expect the governance function to ensure trust in the market by checking that the members of the Trust Framework meet the required standards. Therefore, we assume that without functioning governance the benefits of a fully functioning digital identity market may not be realised.

The governance function may require one-off costs to be set up (though these are expected to be marginal) and will require annual costs in order to be maintained. At this early stage it is difficult to estimate what these costs may add up to. We will aim over time for governance to move towards a self-funding model.

As set out in the response to the digital identity and attributes consultation, we have decided to establish an interim governance function within DCMS while we actively seek a permanent location for the governance function as the market develops and we gather data on the challenges associated with its operations. Our estimates for the central and low funding scenarios for the cost of governance come from FTE requirements which DCMS will incur as part of this, with the difference between the scenarios reflecting potential reductions in FTE for some functions. The high funding scenario is based on costs submitted by the ICO to DCMS as the ICO's estimated cost of fulfilling the governance function.

The cost of these scenarios in year three, when we expect the function to be fully set up and functioning, are laid out below:

Table 31 - Governance function costs over the 10 year appraisal period[51]

Scenario:	Estimated annual governance function cost, £, millions, (undiscounted)	FTE	Estimated total costs over the 10 year appraisal period, £, millions, (undiscounted)[52]
Medium Funding (Central case estimate)	1.2	17.0	11.1
Maximum Funding (Best case estimate)	3.9	33.0	35.6
Low Funding (Worst case estimate)	0.7	9.5	6.2

Total indirect costs to public sector organisations

We estimate that, based on our assumptions, the costs public sector bodies may face over the appraisal period to fully realise the digital identity market may range from £149.87m to £505.28m. The central case estimate for the estimated public sector costs is £149.87m.

Table 32 - Public sector costs: total over the 10 year appraisal period, £, millions

	Central case estimate	Best case estimate	Worst case estimate
	Estimated costs over the 10 year appraisal period, £, millions, (undiscounted)		
One-off familiarisation costs	0.22	0.22	0.39
Organisational change costs	138.53	138.53	498.69
Governance function funding costs	11.13	35.60	6.2
Total, £, millions	149.87	174.35	505.28

Total indirect costs to private and public sector organisations

The central estimate of the undiscounted costs to UK private and public sector organisations is £1456.16m over the 10 year appraisal period. We estimate that the lower and upper bounds of the total undiscounted costs all organisations together may face over the appraisal period are £853.82m and £2631.97m respectively.

The per check fees and the one off connection fee which are both indirect private sector costs are intended to recover public sector costs to ensure value for money for the taxpayer. Therefore, when calculating the total cost in Table 33, we must deduct per check fees and the one off connection fee from the public sector cost by up to but not exceeding the cost

[51] The best case estimate predicts higher costs relative to the other scenarios because we assume maximum funding for the governance function which, in turn, leads to higher funding costs for governance.
[52] Until year 3 the costs are not fully realised as we do not expect full funding to take place at first.

that is incurred. We do not deduct these fees such that the public sector cost becomes negative because the government does not intend to make a profit. In reality, these fees will be determined with thought by the respective organisations and they will be under constant review to ensure the fees are for cost recovery purposes. Similarly, the annual membership fee is intended to offset the governance function funding cost.

Table 33 - Total costs over the 10 year appraisal period, £, millions

	Central case estimate	Best case estimate	Worst case estimate
Private sector costs	1449.78	822.63	2631.58
Public sector costs	149.87	174.35	505.3
Total per check fees	(502.87)	(345.10)	(746.5)
One off connection fee	(0.57)	(0.39)	(0.74)
Annual membership fee for service providers	(4.97)	(4.63)	(5.14)
Total, £, millions	1456.16	853.82	2633.03

*Note: Total per check fees and the one off connection fee has been deducted **up to** the amount equivalent to the public sector costs set out in table 30, and **by no more** because the government does not intend to profit from these fees. Therefore, the total in the table will not equal the sum of the costs with the exception of the best case estimate.*

Value for money

We expect digital identity to bring value to the UK economy under best, worst and central assumptions and the NPV of the benefits unlocked by a fully functioning digital identity market over the appraisal period is positive under these scenarios.

Overall, given the assumptions we have taken, we assume digital identity to add value to the UK economy as the estimated benefits outweigh the estimated costs for public and private sector organisations.

Table 34 - Value for Money

		Estimated year digital ID checks start	Estimated net benefits value over the 10 year appraisal period, £, millions (undiscounted)	**NPV benefits over the 10 year appraisal period, £, millions,**
Digital identity	**Central case estimate**	2	4677.15	**3678.0**
	Best case estimate	1	6581.71	**5394.0**
	Worst case estimate	3	1675.17	**1067.5**

Central case estimate

In the central scenario the value of the discounted net benefits of using digital identity is £3678.0m. Therefore, the expected benefits outweigh the expected costs over the appraisal period. The breakeven point is reached in year 5. This means that, although we assume that some benefits begin to realise in year 2, it takes 3 extra years for the total estimated benefits to fully cover the total estimated digital identity costs.

Best case estimate

The estimated upper bound for the value of the NPV of the benefits is £5394.0m. According to our estimations, the breakeven point takes place in year 3. This means that in the most optimistic scenario public and private sector organisations may recover their costs within three years from when digital identity checks against Government-held data may begin.

Worst case estimate

In the worst case estimate, we estimate that the NPV over the appraisal period to be £1067.5m.

Based on the estimates, the value of the annual undiscounted net benefits is positive from year 4 onwards, the year after we assume digital identity checks against Government-held data may begin.

Whereas, we estimate that the breakeven point may be reached in year 10. Therefore, in the worst case estimate we assume that it may take 8 years from when private-sector checks against Government-held data start for the total estimated benefits to begin to fully cover the total estimated costs.

Non-monetised costs to businesses

Employee mobility

We expect businesses to face some costs to adapt their organisation in order to carry out real-time digital verification for DBS, RTW and employability checks. For instance, businesses may be required to set in place a platform which determines the requirements based on nationality and work location. Consequently, new hires may be invited to complete a self-service right to work check and may be able to provide the necessary attributes through a digital identity service to complete the checks. We expect businesses wishing to use digital ID checks to carry out these checks to have to pay for the required platform. The payment will most likely be on a subscription basis but were unable to estimate these ongoing costs at this early stage.

Travel authorisation and ticketing

Verifying passport data when booking a flight and reducing in-journey ID verification

We expect businesses to shoulder costs to use digital identity to reduce in-journey ID verification. For instance, businesses may need to integrate a remote identity verification solution through a platform that passengers may use to submit their passport details for real-time verification. We expect businesses to outsource the required platform and pay it on a subscription basis, therefore creating an ongoing cost for the business. However, we are unable to estimate what these costs may add up to at this early stage.

Costs to align with industry initiatives on passenger identification (e.g. ICAO's OneID)

We also expect businesses to take actions to align with industry initiatives on passenger identification to streamline the journey of passengers by creating an interoperable system between airports, airlines and governments. We are currently unable to estimate what these costs may add up to.

Home buying

Cost to extended ID verification to witnesses

We assume businesses may have to take actions to extend remote ID verification to witnesses to facilitate identity proof throughout the home buying process, where necessary. Currently, the real estate market relies significantly on witness proofing, which in turn may require the identity verification of the involved witnesses. Unless the steps taken to digitise the identity verification system of the home buyers is extended to witnesses, the market will be unable to fully function digitally and the benefits of using digital identity will not be maximised. We are unable to predict such costs at this early stage.

It is also possible that the requirements for witnessing of certain deeds may change in future. In particular the use of Qualified Electronic Signatures, in conjunction with the digital identity trust framework, is something which can be explored further as a means of replacing existing requirements for witnessing.

Reducing friction in the home value chain

We assume that businesses may have to adapt the ID checking process required throughout the entire house buying process to the digital identity verification system. We believe that these steps are essential in order to use digital identity across the multiple identity verification process required throughout the home buying process. Unless all identification steps are digitised, the real estate market will not be able to fully function using digital identity.

We considered the following steps:

- Setting up a savings account
- Searching the property
- Bidding for the chosen property
- Requesting and receiving the funding (e.g. mortgage application)
- Closing the contracts (e.g. mortgage contract)
- Moving in (e.g. change doctors or schools)
- Registering transfer of title at HM Land Registry

Businesses are expected to face costs to create and maintain the system for any potential platform required to remove the friction in the home value chain. Businesses may incur costs to adapt to closing contracts digitally. However, due to the level of uncertainty we are unable to estimate these costs.

Trusted financial transactions

Businesses may pay to adapt their organisation in order to digitally prove the identity of customers throughout financial transactions. Businesses may either outsource or build and maintain the platform in-house. However we are currently unable to estimate what these costs may add up to.

Further potential costs to public sector organisations (not included in the quantitative analysis)

Digitisation costs for public sector organisations

We consider the digitisation of most Government-held datasets to be considered business as usual. This is because the vast majority of personal data which may be used as part of attribute checking is already held in a digital form by Government Departments. On rare occasions we expect some Government Departments to incur some digitisation costs of personal data in a paper-only format. For instance, the General Register Office for England and Wales (part of HMPO) would have to digitise birth records dated from 1937 to 2009, marriage records dated from 1946 to 2011 and death records dated from 1970 to 2009 to use them as part of the attribute checking process. These are currently not available in digitised form.

According to the HMPO, the digitisation is expected to be carried out through a blended service, both outsourced and carried out in house. HMPO estimates that the outsourced service to digitise all outstanding personal data held in a paper-only format may cost c. £18m. We expect this to be a multi-year process involving external resources to complete tasks, such as scanning and image improvement, and internal resources to carry out tasks such as data assurance and the development of storage.

A full breakdown of the estimated number of IDs to digitise and the expected costs are shown below:

Table 35 - Paper-only civil registration to digitise

Tasks required	Estimated number of documents to digitise	Estimated external supplier cost
Birth Records 1937-2009	45,000,000	c. £9m
Marriage Records 1946-2011	13,500,000	c. £3m
Death Records 1970-2009	20,000,000	c. £6m
Total estimated cost		c. £18m

Risks and assumptions

Table 36 - Assumptions

CENTRAL ESTIMATE SCENARIO	BEST ESTIMATE SCENARIO	WORST ESTIMATE SCENARIO	RISK ASSESSMENT
Wage estimation			
Wage data used in both the cost and benefit estimated has been inflated by 22% to adjust for overhead costs.			No sensitivity analysis has been undertaken.

We assume that a Grade 7 public sector employee earns £75,000 including overhead costs. This is a standard DCMS assumption.			No sensitivity analysis has been undertaken.
Estimated cost values			
The hard-coded values used to calculate the estimated costs have been gathered from an engagement exercise with stakeholders.			There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
Averages of the inputs gathered throughout the engagement exercise were used to estimate the potential average cost of each task for a business.			
The cost estimations provided by the engagement exercise are in 2021 value.			
Wage per hour has been calculated by dividing the gross annual wage by the number of weeks in a year (52) by the ONS' 2019 average number of working hours in a week. We took the 2019 value as the 2020 value has been significantly affected by Covid 19 and would not have been representative of the usual working patterns.			No sensitivity analysis has been undertaken.
Costs over the 10 year appraisal period are undiscounted.			
Number of businesses			
We assume that only medium and large UK businesses will take up digital identity as their benefits will significantly outweigh the transition costs. Data regarding the Number of UK medium and large businesses was collected from the ONS data release: UK "BUSINESS: ACTIVITY, SIZE AND LOCATION - 2020", table 3.			No sensitivity analysis has been undertaken.
Familiarisation costs			
The values from the engagement exercise have been used to calculate the central estimate of the potential average familiarisation costs per business.	We reduced the central estimate by 50%.	We inflated the central estimate by 100%.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
For each task the estimated costs have been calculated as: average resources required (employees and time) * average wage per hour (including 22% overhead costs). The estimated cost of each task was then summed together to calculate the estimated cost per business.			
To calculate the total estimated familiarisation costs we multiplied the familiarisation costs per business by the 2020 number of UK medium and large businesses.			
The familiarisation costs are one-off costs.			
We assume all businesses face familiarisation costs in year one independently of the use case.			

Organisational change costs(private sector)			
The values from the engagement exercise have been used to calculate the central estimate of the potential average organisational costs per business.	We reduced the central estimate by 50%.	We inflated the central estimate by 100%.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
We estimated the organisational costs per business and multiplied the value by the 2020 number of UK medium and large businesses to calculate the total estimated familiarisation costs.			
Due to the limited number of responses and the presence of outliers we have used the median number of hours gathered from the engagement exercise to calculate the expected costs per business.			
The organisational change costs are one-off costs.			
For each task the estimated costs have been calculated as: average resources required (employees and time) times average wage per hour (including 22% overhead costs). The estimated cost of each task was then summed together to calculate the estimated cost per business.			
We estimated the organisational change costs per businesses and multiplied the value by the 2020 number of UK medium and large businesses.			
Businesses in the sector related to each of the use cases face the organisational change costs the year that the digital ID checks take place for the first time. (E.g. real estate businesses face the organisational change costs when the checks related to the home buying process begin). If businesses are affected by multiple use cases they face the organisational change costs only once in the year that the first check is expected to take place.			
All medium and large UK businesses face organisational change costs to adapt to carrying employee mobility checks digitally.			
One-off connection fee			
We assume that the one-off connection fee may be £5650. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We assume that the one-off connection fee may be £3900. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We assume that the one-off connection fee may be £7400. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We set different connection fee costs in each scenario to attempt to mitigate the risk of under or overestimating the connection fee costs.
The number of identity providers that may pay the connection fee has been estimated by the private sector on behalf of DCMS. This number (100) does not vary across scenarios.			No sensitivity analysis has been undertaken.
Certification fee and annual membership fee			
The number of identity providers that may pay the connection fee has been estimated by the private sector on behalf of DCMS. This number (100) does not vary across scenarios.			No sensitivity analysis has been undertaken.

Linear trend over time of the digital identity market towards the steady state			
We assume that the digital identity uptake grows over time following a linear trend. For instance, in the central scenario we assume that only 15% of the total potential number of checks and expected benefits estimated by Deloitte takes place in year 1. In the central scenario 100% of digital identity uptake is reached by year 7 of the appraisal period.	The trend in the best case scenarios is 33% higher than the central scenario.The estimated percentage in year 1 is 20%.	The trend in the worst case scenarios is 33% lower than in the central scenario. The estimated percentage in year 1 is 15%.	There is a risk that the estimated trend lines may be incorrect. We have set three different scenarios to attempt to mitigate this risk.
The trend has been estimated through conversations with the policy team based on their knowledge of the digital identity sector.			
Cost per check			
We assume that the per-check fee may be 25p .The assumption has been set in agreement with the policy team based on their market knowledge and with input from the Home Office.	We assume that the per-check fee may be 15p .The assumption has been set in agreement with the policy team based on their market knowledge and with input from the Home Office.	We assume that the per-check fee is 50p. The estimate comes from the Home Office Passport Pilot Scheme.	There is a risk that these costs may not be true to reality. To mitigate this risk we have taken one of the cost scenarios from the Home Office Passport Pilot Scheme and we have set three different scenarios.
Number of checks			
The annual number of checks (assuming the steady state market level) for each use case has been estimated by a research project carried out by Deloitte (except for DBS checks - see Appendix 2). The values are constant across scenarios.			There is a risk that the full number of annual checks estimated by Deloitte may not be realised as soon as checks begin. To mitigate this risk we have multiplied the annual volume of checks by the estimated trendline.
The number of digital ID checks grows over time following the estimated trendline. The trendline varies depending on the scenario.			
Total annual cost of per check fees			
We calculate this estimate by multiplying the estimated annual number of checks (adjusted to the trend) by the estimated per check fee.			No sensitivity analysis has been undertaken.
Year the costs and benefits take place			

The assumptions regarding the year the digital ID checks may begin for each use case and scenario are based on information provided by the policy team based on their knowledge of the sector.			There is a risk that these assumptions may be incorrect. To mitigate this risk we have set different years in each of the three scenarios.
The years assumed in the best and worst scenarios are variations of what estimated in the central scenario.			
Scenarios			
In the central scenario we assume that the checks that rely only on passport data may start taking place from year 2 onwards. Whereas, it may take 3 years for those that rely on passport data and guidance being updated. Lastly, it may take 5 years for the checks that rely on datasets other than passport data.	In the best case scenario we assume early uptake, low costs and high benefits.	In the worst case scenario we assume later uptake, high costs and low benefits.	There is a risk that these assumptions may be incorrect. To mitigate this risk we have set different years in each of the three scenarios.
Benefits			
The estimated benefits over the 10 year appraisal period have not been discounted.			
The values used in the Deloitte methodology to calculate the benefits have been modified to align with the cost estimations. Estimated wage values have been inflated by 22% to account for overhead costs and monetary values have been inflated to 2021 prices. Where the year was unclear we assumed the values were in 2020 prices.			
Any benefits that consider time value are multiplied by 24 to decimalise time in order to correctly multiply it by wage.			
First order indirect benefits			
The estimated annual economic value for the UK of carrying out digital ID checks has been estimated by Deloitte (however, we used DBS forecasts for DBS checks to update benefits associated with undertaking DBS checks).			No sensitivity analysis has been undertaken.
The estimated values assume that the steady state level of the market is reached. Therefore, we adjusted the estimated values of the benefits by the estimated digital identity market trend over time.			
The total value of the benefits are split by the value we expect private citizens to experience and the value we expect businesses to experience.			
Second order indirect benefits			

We assume that one proportion of the value of benefits related to faster employee mobility for people on short notice periods begins to take place when digital DBS checks are realised, the second part when digital RWT checks begin to take place and the remaining value when digital qualification checks begin to happen. Each percentage is proportional to the annual number of checks estimated for DBS, RWT and qualification checks.	No sensitivity analysis has been undertaken.
The assumption above is set for productivity improvement as well.	
The total value of the benefits related to reduced fraudulent applications arises when digital qualification checks begin to take place as we assume the current costs are related to hiring workers with false credentials.	
Non-monetised costs to private sector businesses	
We expect businesses to have to pay to adapt the way they carry out ID verification to digital identity. For instance, by setting up a platform to perform digital ID checks.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.
Non-monetised costs to businesses: Costs to join the Trust Framework	
Although being signed up to the trust framework will not be compulsory to operate in the market, we assume that private-sector access of government-held databases is only granted to the businesses signed up to the trust framework. Therefore, businesses will have to sign up to it in order to effectively operate in the market.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.
Cost for public sector bodies	
We assume that public sector bodies face familiarisation costs, costs to digitise any IDs in paper-only form (e.g. birth certificates before a certain year), costs to allow private sector access to their databases and costs to set up and run the governance function. All costs except digitisation costs have been included in the net benefits calculations.	No sensitivity analysis has been undertaken.
In the central and best scenarios we assume that 5 departments adapt to digital identity, whereas in the most pessimistic scenario we assume 9 departments adapt to digital identity.	Sensitivity analysis has been undertaken by varying the number of Departments across scenarios.
Net benefits	
The net benefits have been discounted so they are presented in NPV.	

Impact on small and micro businesses

Small and micro businesses are not exempt from this legislation. However, we do not expect the legislation to significantly impact small-micro relying parties as we assume they will be less likely to adopt digital identity. Regarding service providers, we do not expect a

significant disproportionate impact as these businesses are already established in the market so we expect their cost to understand and adapt to the legislation to be minimal..

Relying parties[53]:

We expect the legislation to not significantly impact small and micro businesses as we assume that small-micro relying parties will be significantly less likely than bigger ones to adopt digital identity because their expected benefits are less likely to outweigh the costs. For instance, businesses are considered small-micro if they employ less than 50 staff members. Therefore, we assume they are less likely to be interested in digital RTW checks as their gains from digital checks will not be significant compared to the cost of familiarising and adapting to digital identity.

According to ONS data, the average turnover of small micro businesses in 2020 was £606,501. We estimated that the one-off familiarisation costs plus the one-off organisational change costs for a business wishing to adopt digital identity may add up to £17,657.5. Therefore, these estimated costs add up to roughly 2.9% of the average revenue of a small-micro business in 2020. Whereas, the equivalent calculation for medium-large businesses adds up to 0.08%. This suggests that the estimated costs of adapting to the legislation may create a greater burden for small-micro businesses relative to larger ones. However, this legislation is not designed to substitute traditional identification checking. Therefore, we expect small and micro relying parties that may experience a significant burden to adopt digital identity to continue to only use traditional identification systems. Therefore, overall we do not believe that small-micro businesses will be disproportionately affected by the legislation in a significant way.

Service providers[54]:

Small-micro identity and attribute service providers have a greater risk of being disproportionately impacted by the legislation. We expect these businesses to face familiarisation costs and organisational. As demonstrated above, these costs may generate a greater burden for small micro firms relative to medium-large businesses. However, we do not believe this disproportionate impact will be significant as small and micro identity and attribute service providers are already established in the market so we expect that their costs to understand and adapt to the legislation to be minimal.

The legislation aims at providing the right legislatory environment to promote the adoption of digital identity. Therefore, we expect the small-micro providers to experience a growth in demand on the back of the legislation. We believe that the resulting increase in revenue will cover some, if not all, the costs businesses may experience due to the legislation.

Costs if SME's did decide to use digital identity

We have expanded the model to include small and micro businesses. This has given us an upper end of the indirect costs that could come to fruition. However, due to the use cases being examined and given that most SME's employ so few people we believe that not many SME's will take advantage of DI.

---

[53] We define relying parties as organisations that get (or 'consume') digital identity products or services.

[54] We define service providers as organisations that prove and verify users' identities and/or attributes. They might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process.

We estimate that the central estimate of the total undiscounted indirect costs over the appraisal period, assuming that digital identity is taken up by small, medium and large UK businesses, is £5,520.4m. This estimation is almost 3 times the total cost value estimated in the case where digital identity is adopted only by medium and large firms.

Wider impacts (consider the impacts of your proposals)

Equalities Impact Assessment

Although a digital identity market already exists, it is not developed to its full potential and it presents some key flaws which may exclude minorities or those with protected characteristics. For example:

- When setting up a digital identity, individuals have highlighted that the process usually requires a sequencing of tasks which are considered difficult for people that are, for instance, digitally excluded or neuro-diverse[55].
- The digital identity system tends to be rather rigid, therefore excluding people whose circumstances differ from the expected social structure, such as those wishing to manage two bank accounts at the same bank from one mobile phone[56].

The digital identity legislation, by promoting the growth of the digital identity market in an inclusive way, provides the opportunity to use a digital alternative, giving to excluded individuals an easier option for proving their identity or eligibility. For example, those who cannot afford a passport may instead opt for a digital identity product based on their data or a 'vouch'[57].

Inclusion is explicitly mentioned in the UK digital identity and attributes trust framework. Although signing up to the Trust Framework is not compulsory, organisations will need to be certified against it to prove that their products or services meet the UK Government requirements for checking government-held records of identity-related data.

The Framework aims at improving inclusivity by:
- Stating that all identity service providers should ensure no one is excluded due to their *'protected characteristics"*. There are exemptions to this, for instance restricting the availability of a product or service to an individual due to their age (e.g. businesses cannot sell alcohol to underage individuals).
- Giving examples of ways organisations can increase inclusivity. For instance, when choosing a system for facial recognition, digital identity and attribute providers should ensure that the chosen system is built in an inclusive way. A system which was tested with a small sample of white men risks excluding users of other genders and ethnicities, therefore excluding minorities or those with protected characteristics from being able to use the service.
- Requesting both public and private sector organisations to meet appropriate accessibility standards. For instance, those that operate in Wales offer products and services available in Welsh.
- Requiring organisations that sign up to the framework to submit an annual inclusion report.

The inclusion report

[55] Digital Identity: Ground-up Perspectives Report Summary
[56] Digital Identity: Ground-up Perspectives Report Summary
[57] A vouch is a declaration from someone that knows the user which can be used as evidence for identity proof.

The inclusion report aims to provide information on the routes service providers offer users for acquiring a digital identity. The report will also allow organisations to provide evidence of their efforts to improve their level of inclusivity. This information will give the governance function an overview of all of the avenues available across the market, so that it can determine whether any intervention is needed to encourage a diversity of avenues across the market. The government will not mandate that organisations collect information solely for the purposes of reporting.

Public sector equality duty

Section 149 of the Equality Act 2010 imposes a legal duty, known as the Public Sector Duty (Equality Duty), on all public bodies, to consider the impact on equalities in all policy and decision making.

The Equality Duty requires a public authority, in the exercise of its functions, to:

- consider the need to eliminate unlawful (direct or indirect) discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010;
- advance equality of opportunity between people who share a protected characteristic and those who do not share it; and
- foster good relations between people with a protected characteristic and those who do not share it.

The relevant protected characteristics are: age, disability, gender reassignment, Marriage and Civil Partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

The Digital identity and digital attribute measures provide people with an additional choice of how to prove things about themselves but do not remove any current methods or mandate a new approach. These measures have no identifiable adverse or negative impacts in relation to the first limb of the Equality Duty.

Instead, these measures ought to have a positive impact on promoting equality. As discussed above, without intervention it is likely that a digital identity market may develop which negatively impacts those with protected characteristics. The trust framework aims to tackle this by setting rules for trust-marked private sector organisations (who are not themselves necessarily bound by the public sector equality duty).

These initiatives can help advance equality of opportunity between people who share a protected characteristic and those who do not share it. For example, the fact that a digital identity can be based on a wider range of attributes could help someone with a disability prove something about that disability more seamlessly than is currently possible. Further iterations of the trust framework will contain information around sex and gender to give guidance on information sharing for people who have undergone, intend to undergo or are currently undergoing gender reassignment so they can limit excessive or unnecessary disclosure.

Innovation test

Relying parties:

We expect the legislation to behave as a catalyst for innovation for relying parties for whom digital identity is a core part of their function (e.g. airlines that frequently carry out passport checks). The legislation will enable the standards required for the market to develop in a trusted and interoperable way, which aims at making relying parties more willing to adopt digital identity. This means that, in future, services which were previously provided in person may be provided remotely, giving relying parties the opportunity to provide new innovative services. We expect to see the increase in innovation in the short-term[58] and to have a medium to high impact due to the potential scale of the uptake of digital identity across numerous sectors of the UK economy.

Service providers:

We expect the legislation to foster the growth of the market by enhancing trust and interoperability, which we expect will drive an increase in demand. We believe that the greater demand will lower verification costs due to economies of scale driven by the larger size of the market. In turn, this should contribute to providing identity providers with the required financial resources to invest in innovation.

These factors should all provide new opportunities for businesses already established, and increase the number of businesses entering the market, which will increase the level of competition within the market.

We expect that the greater demand and market size, the lower costs and increased competition will all boost the willingness of identity and attribute providers to innovate to a medium to high extent. Already established businesses will benefit from a first-mover advantage, therefore we predict that their innovation will particularly benefit from the legislation. Although signing up to the trust framework will not be compulsory for any size or type of organisation, it will be strongly encouraged. If the framework is too prescriptive it risks constraining the ability of providers to innovate. Therefore, firms signed up to the framework will need to be aligned with the required standards which give them less freedom to innovate and develop as they wish.

Moreover, companies on low liquidity might struggle to adhere to the set standards, potentially driving them out of the market or increasing barriers to enter the market. Both of these factors may harm innovation of service providers. The framework is currently being tested out to achieve the right balance between prescription and freedom to innovate to ensure trust in the market. This should minimise the risk of the trust frameworking behaving as a stumbling block for innovation.

Even if at first the trust framework does create some obstacles to innovation, we expect that overall in the long term the potential benefits to innovation brought by a larger, interoperable and trusted market outweigh these potential costs.

A summary of the potential trade implications of measure

This legislation may indirectly support international trade by setting the powers to permit international cooperation in the future. Therefore, it is the first step towards creating a statutory environment that can foster the growth of a trusted and international interoperable digital identity market.

All policy options, other than the “do nothing” option, should indirectly support international trade of goods and services. However, we expect the preferred option to provide the most

[58] We consider an impact short-term if it takes place within 2 years from the implementation of the legislation.

significant support, relative to the other options. This is because we expect that creating a trusted and interoperable market overseen by a governance function will support the growth of the digital identity market the most, which in turn should have the greatest impact on trade.

We may expect this to bring beneficial impacts to international trade, reducing friction by facilitating remote ID verification checks, which is very commonly required whilst trading internationally.

The legislation will ensure the UK is not left behind from the mutual recognition of digital identity across borders, and supports the position of the UK as a key international player.

Without government intervention through digital identity legislation the UK will not have a fully realised digital identity market in the future. This risks leaving the UK behind and excluding it from international trade if other countries begin to widely use digital IDs to carry out identity verification checks whilst trading between each other.

A summary of the potential environmental implications of measure

We expect that the legislation, by fostering the uptake of digital identity checks, will have a positive effect on the environment. This is because less trips will be required during the identity verification process and to allow the individuals to obtain the required physical identities.

Furthermore, a greater uptake of digital IDs may lead to less people choosing traditional IDs over digital alternatives which in turn may lead to a lower quantity of IDs produced and disposed every year. This could be beneficial to the environment.

However, despite the fact that digital identity should benefit the environment, these benefits are expected to be very small and possibly insignificant. For instance, the total number of trips related to identity verifications carried out every year, although substantial, is not large enough to significantly impact the environment.

Monitoring the policy

We will aim to monitor the policy over time. As the legislation itself will permit and not require OGDs to open their data we have no concrete plans for how this will be done especially as different departments may wish to use different metrics to measure the impact of this legislation. However, some practical metrics by which to measure this policy are things like the number of organisations certified, the number of checks made, the number of people signed up to the trust framework and the growth in numbers of service providers. Of course there are likely many other potential ways to measure the impact of this policy and this will be thought through further down the line when we know whether any departments are opening up their data.

Appendix 1:

Monetised benefits of using digital identity in the four use cases: Deloitte calculations

Deloitte identified the potential savings on the back of using digital identity in the four use cases and estimated the annual economic benefits for the UK to add up to £743m - £938m. However, the calculations in the Deloitte report do not account for overhead costs. Therefore we inflated the wage values estimated by Deloitte by 22% to account for them.
In all scenarios, digital identity users benefit from time and cost savings, relative to a situation where no digital alternative is available, as digital identity proofing is faster and cheaper than traditional identity checks. Therefore, in all scenarios the benefits have been monetised by looking at the costs currently faced by businesses and individuals to carry out physical identity checks, and multiplying them by the number or businesses and/or individuals currently affected.

A breakdown of the variables, assumptions and calculations that fed into the variables outlined can be found in appendix 2.

Total estimated first order indirect benefits for Employee Mobility:

The economic value of the predicted benefits arising from reducing friction for employee mobility by using remote ID verification is expected to add up to:

Table 37 - Employee Mobility (first order indirect benefits): Total calculations

Variable number	Benefits	Value
15	Business costs saved per RTW check per new employee	
16	Individual costs saved per RTW check per new employee	
	Savings associated with RTW checks	£56,224,730
17	Business costs saved per DBS check per new employee	
18	Individual costs saved per DBS check per new employee	
19	Business costs saved due switch to new Status Notification system	
	Savings associated with DBS checks	£20,598,963
22	Business costs saved per RTW qualification check per new employee	
	Savings associated with Qualification checks	£44,196,009
Total estimated first order indirect benefits for Employee Mobility:		**£121,019,7021**

Whereas, the estimated value of the second order indirect benefits may consist in the following benefits:

Table 38 - Employee Mobility (second order indirect benefits): Total calculations

Variable number	Benefits	Value
17	Total cost of fraudulent applications going undetected	
16	Total resource wasted in onboarding costs of fraudulent applications	
	Total savings resulting from reduced fraudulent applications	£58,850,914 - £134,297,194
18	Total cost for re-issuing documents for background checks (trips + cost of re-issuance)	
19	Total cost of time value taken to produce ID documents for reference checks	
	Total benefit from productivity improvements	£22,361,439
20	Time value for all employees whose start date is delayed per year	
	Total saving due to faster employee mobility for people on short notice periods	£53,064,461
Total estimated second order indirect benefits for Employee Mobility:		**£134,276,814 - £209,723,094**

Total estimated indirect benefits for Travelling Authorisation and Ticketing:

The economic value of the benefits for individuals and businesses on the back of using digital identity in this use case may add up to:

Table 39 - Travel Authorisation and Ticketing: Total calculations

Variable number	Benefits	Value
19	Business costs saved through seamless check-in, boarding and passport control	
20	Individual costs saved through seamless check-in, boarding and passport control	
20	**Costs saved through seamless check-in, boarding and passport control (individuals)**	£295,051,576
21	Individual costs saved on correcting identity errors	
21	**Costs saved on correcting identity errors**	£1,875,889
Total estimated indirect benefits for Travel Authorisation and Ticketing:		**£296,927,465**

Total estimated indirect benefits for Home buying:

According these calculations the economic value of the benefits for businesses and individuals using digital identity throughout the home buying process may add up to:

Table 40 - Home buying: Total calculations

Variable number	Benefits	Value
22	Business costs saved on KYC	
23	Individual costs saved on KYC	
	Costs associated with KYC	£109,021,259
25	Costs associated with mortgage application fraud cases borne by Businesses	
26	Costs associated with mortgage application fraud cases borne by Individuals	
	Costs associated with mortgage application fraud cases	£23,933,680
Total estimated indirect benefits for Home buying:		**£132,954,939**

Total estimated indirect benefits for Trusted Financial Transactions:

The savings to businesses and individuals by using digital IDs to safely carry out financial transactions may add up to:

Table 41 - Trusted Financial Transactions: Total calculations		
Variable number	Benefits	Value
18	Business costs saved because of KYC checks	
19	Individual costs saved because of KYC checks	
	Costs associated with KYC	£9,038,426
20	Savings on card fraud incidents	
21	Savings on online fraud incidents	
	Savings on fraud incidents	£175,665,913
Total estimated indirect benefits for Trusted Financial Transactions:		**£184,704,339**

Appendix 2:

Table 42 - Employee Mobility (first order indirect benefits): Assumptions and calculations			
	Variable	**Formula**	**Value**
1	Number of jobs		32,900,000
2	Job turnover rate		25%
3	Time taken by government worker to perform an RTW check		00:15
4	Time value of employee performing an RTW check		£20.47
5	Time taken for the average worker to complete an RTW check		00:10
6	Time value of average person		£10.31
7	Annual volume of DBS checks (nationals vs non nationals)		8,379,239
8	Time taken by government worker to perform a DBS check		00:00
9	Cost per DBS status notification - current		£0.74
10	Cost per DBS status notification - with Digital ID		£0.00
11	Time taken for the average worker to complete a DBS check		00:10
12	Proportion of jobs classified as 'professional' by ONS		21%
13	Time taken by government worker to perform an RTW qualification check		01:15
14	Base: Annual volume of RTW checks	1 x 2	8,225,000
15	Business costs saved per RTW check per new employee	14 x 3 x 4	£42,091,438
16	Individual costs saved per RTW check per new employee	14 x 5 x 6	£14,133,292
17	Business costs saved per DBS check per new employee	4 x 7 x 8	£0
18	Individual costs saved per DBS check per new employee	6 x 7 x 11	£14,398,326
19	Business costs saved due switch to new Status Notification system	7 x (9-10)	£6,200,637
20	Number of jobs classified 'professional' by ONS	1 x 12	6,909,000
21	Annual volume of qualification checks	20 x 2	1,727,250
22	Business costs saved per RTW qualification check per new employee	21 x 4 x 13	£44,196,009

Table 43 - Employee Mobility (second order indirect benefits): Assumptions and calculations			
	Variable	**Formula**	**Value**
1	Number of employees changing jobs		2,993,900

2	% of onboarding checks that result to false positives (i.e. application is fraudulent but not detected)		2.5%
3	Calibration factor to take into consideration that not all economic output is lost		30% (low) - 70% (high)
4	Hours in employment before fraudulent application is identified		160
5	Average UK hourly salary		£15.75
6	Business Cost of onboarding checks (identified from primary impact)		£92,488,084
7	% of applicants that may require to take a trip to gather the necessary evidence		7%
8	Average cost per trip		£4.80
9	Average cost per certificate (passport re-issuance)		£85.00
10	Average hourly salary lost (due to time taken to produce ID documents)		£8.45
11	Average time taken away from the office to reissue documents		2
12	Number of jobs that are expected to be filled immediately		1,339,200
13	% of employees who miss their start date due to delay in background checks		30%
14	Average delay on employment start date due to background checks delay (in hours)		16
15	Average hourly salary lost (due to delay in employment start date)		£16.51
16	Total resource wasted in onboarding costs of fraudulent applications	6 x 2	£2,312,202.09
17	Total cost of fraudulent applications going undetected	1 x 2 x 3 x 4 x 5	£56,584,710 - £132,030,990
18	Total cost for re-issuing documents for background checks (trips + cost of re-issuance)	3 x 7 x (8 + 9)	£18,819,655
19	Total cost of time value taken to produce ID documents for reference checks	10 x 11 x 1 x 7	£3,541,784
20	Time value for all employees whose start date is delayed per year	12 x 13 x 14 x 15	£106,128,922

Table 44 - Travel Authorisation and Ticketing: Assumptions and calculations

	Variable	Formula	Value
1	Base: Total number of travellers		296,681,000
2	Proportion of Total Travellers who are UK nationals		63%
3	Estimated volume of identity checks at airport		1.4

4	Time Taken to check in		00:01
5	Time value (airline service staff)		£14.75
6	Time value (border control staff)		£17.05
7	Total time value (average staff)		£15.90
8	Number of flight take offs in the UK		1,100,000
9	Estimated saving from moving to 1 gate agent for c. 900k domestic flights in US		£28,299,999
10	Time Taken by average individual to check in		00:05
11	Time value (business passengers)		£54.55
12	Time value (average passenger)		£12.14
13	Proportion of passengers who need to correct errors		1%
14	Time Taken by average individual to correct errors		00:05
15	Airline booking process time		01:00
16	Accrued fines per passenger		£0.44
17	Proportion of errors solved		50%
18	Total number of travellers (UK nationals only)	1 x 2	185,425,625
19	Business costs saved through seamless check-in, boarding and passport control	9 x (1.1/0.96)	£32,427,082
20	Individual costs saved through seamless check-in, boarding and passport control	18 x 3 x 10 x 12	£262,624,494
21	Individual costs saved on correcting identity errors	18 x 12 x 13 x 14	£1,875,889

Table 45 - Home buying: Assumptions and calculations			
	Variable	**Formula**	**Value**
1	First time buyer mortgages - No. of transactions		351,450
2	Other mortgages (home movers and buy to let) - No. of transactions		413,770
3	Remortgage (with new contract) - No. of transactions		622,960
4	Remortgage (product transfer) - No. of transactions		1,195,200
5	First-time buyer mortgages - No. of checks		5
6	Other mortgages - home movers and buy-to-let - No. of checks		5
7	Re-mortgage with new contract (singles vs couples) - No. of checks		2.5
8	Re-mortgage product transfer (singles vs couples) - No. of checks		0
9	Average number of adults involved in transaction		1.65
10	Time spent by Business on KYC		00:20
11	Average employees' time value		£30.75
12	Time taken for Individual to complete KYC process		00:10
13	Time value of average person		£12.14
14	Number of mortgage application fraud cases		2,386
15	Total losses from mortgage fraud - from National Fraud Agency		£1,231,899,304
16	Average UK house price		£250,772
17	Fraudulent mortgage size relative to house price		80%
18	Average fraud losses		£200,618
19	Proportion of frauds avoided due to Digital ID		5%
20	Proportion of Fraud Costs borne by Businesses		90%
21	Base: Total number of checks for all type of transactions	((1 x 5) + (2 x 6) + (3 x 7) + (4 x 8)) x 9	8,882,775
22	Business costs saved on KYC	21 x 10 x 11	£91,048,444
23	Individual costs saved on KYC	21 x 12 x 13	£17,972,815
24	Costs associated with mortgage application fraud cases	14 x 18 x 19	£23,933,680
25	Costs associated with mortgage application fraud cases borne by Businesses	24 x 20	£21,540,312
26	Costs associated with mortgage application fraud cases borne by Individuals	24 - 25	£2,393,368

Table 46 - Trusted Financial Transactions: Assumptions and calculations			
	Variable	**Formula**	**Value**
1	Base: Total number fraudulent card transactions		2,745,539
2	Total value of fraudulent transactions (losses)		£663,666,642
3	Total number of KYC checks		860,772
4	Average cost of KYC check		£56
5	% of business account KYC checks		7.14%
6	% of individual account KYC checks		93%
7	Time taken for businesses to undertake KYC		01:00:00
8	Time value (business)		£41.63
9	Time taken for individuals to undertake KYC checks		00:40:00
10	Time value (individual)		£12.14
11	Value of currently protected transactions		£1,068,539,652
12	Total value of card transactions		£886,528,594,725
13	Average cost saved per transaction		£242
14	Reduction in fraudulent mortgage transactions		12%
15	Total online card transactions		2,848,000,000
16	Time		00:00:10
17	Value of time saved		£0.02
18	Business costs saved because of KYC checks	3 x 5 x 8 x 7	£2,559,567
19	Individual costs saved because of KYC checks	3 x 6 x 10 x 9	£6,478,859
20	Savings on card fraud incidents	13 x 14 x 1	£79,625,024
21	Savings on online fraud incidents	10 x 15 x 16 x 24	£96,040,889

Table 47 - Forecasted DBS Checks										
Year	1	2	3	4	5	6	7	8	9	10
No. of checks	7,174,588	7,325,180	7,585,739	7,924,946	8,260,652	8,485,789	8,815,301	9,120,475	9,405,145	9,694,574

DBS provided us with a forecast for the first 5 years. Using this forecast, we projected the expected number of checks over the next 5 years (years 6-10). The costs were modelled using the forecasted/projected number of checks in Table 47. The average expected number of checks over the 10 years is 8,379,239 and the benefits were modelled using this figure.