The public dialogue on Trust in Digital Identity Services

A findings report

Hopkins Van Mil

February 2024

Department for Science, Innovation & Technology

sciencewise

UK Research and Innovation

www.hopkinsvanmil.co.uk

Contents

Foreword

Trusted digital identities are a vital building block for the future. They give people a way to prove things about themselves, such as their age, address or qualifications, without the need for physical documents. They help make people's lives easier by enabling smoother, cheaper, and more secure online transactions.

However, before businesses and individuals will use these technologies, they need to know they can be trusted. The Department for Science, Innovation and Technology (DSIT) is working to build this trust by setting standards in the form of the UK digital identity and attributes trust framework, which includes rules on privacy and data protection, fraud management, cyber and information security, and ensuring that products and services are inclusive. The trust framework will be underpinned by legislation and managed by a governing body to ensure it is kept up to date.

Last year, we commissioned a public dialogue to seek in-depth views from members of the public on building trust in digital identity solutions. We asked participants for views on the rules in the trust framework, the role of the governing body, and public-facing communications. We also sought participant views on the potential opportunities and risks of the use of digital identities, as they become more widespread across the UK economy. I am excited to see the publication of this report, which summarises the findings of the dialogue and provides evidence on public perceptions on areas like usability, transparency, accountability and inclusivity in digital identities.

In the coming year, we will be setting up the governance arrangements and processes which make real the rules and legislation we're putting in place. The findings from the public dialogue will inform this work at every stage. Already, we are refining the UK digital identity and attributes trust framework to respond to what we've heard.

We are immensely grateful to all those who contributed to this project. I would like to thank UK Research and Innovation's Sciencewise programme and Hopkins van Mil for designing and delivering the public dialogue. Thanks are also due to the project's independent oversight group and their chair – Professor Lizzie Coles-Kemp of Royal Holloway, University of London. The oversight group generously contributed their expertise and ensured the impartiality of the project. Most importantly, I would like to thank each of the members of the public who participated in the dialogue and engaged in such a range of rich and in-depth discussions.

Saqib Bhatti MP

Minister for Tech and the Digital Economy
Department for Science, Innovation and Technology

Executive Summary

The Public Dialogue on Trust in Digital Identity Services was commissioned in March 2023 by the Department for Science, Innovation and Technology (DSIT) in partnership with UK Research and Innovation's Sciencewise programme. It was designed and delivered by the deliberative engagement specialists Hopkins Van Mil and independently evaluated by Navigator Consulting with Graphic Science.

Background to the dialogue

Digital identity and attribute services allow individuals to prove who they are or things about themselves, such as their age, easily and securely without relying on physical documents. They can enable people to access services more easily, safeguard privacy, giving people better control on how their data is handled by others.

The government is working to enable the use of trusted digital identities in the UK. To ensure that these services can be adopted confidently and securely, DSIT is developing a trust framework of rules and standards, alongside supporting governance and legislative measures.

The UK digital identity and attributes trust framework[1] is a set of rules and standards that digital identity providers can follow to demonstrate that they meet robust requirements surrounding cyber security, fraud and inclusion to build trust in their services. The framework is being developed iteratively, with its second prototype ('beta') version published in June 2022.

In this report we describe what participants involved in this public dialogue considered important when deliberating on trust in digital identity services. The purpose of the dialogue was to inform:

- The rules that providers of digital identities must follow in order to become certified against the UK digital identity and attributes trust framework
- The functions, oversight structure and interaction with the public of the governing body for digital identities (the Office for Digital Identities and Attributes - OfDIA)
- Planning for public communications initiatives.

About the dialogue

Public dialogues guide participants through an independently facilitated process which is given time and allows for interaction with specialists and peers. As a result, participants explore their hopes and concerns and the values and principles that underpin them.

In this dialogue participants engaged in a series of five online workshops and in an online space in which they could give the topic further consideration in their own time. To inform dialogue deliberations, participants heard from subject matter specialists, including data scientists, legal and human rights specialists, academics, and industry experts. People who had specific experience of a challenge in proving

[1] The UK digital identity and attributes trust framework beta version

something about themselves or their identity were interviewed for the project. These interviews were shared with participants as short films or audio clips describing barriers to verifying identities as a result of living with a disability, leaving prison, seeking asylum, and identity theft.

From April to June 2023 the dialogue engaged 96 members of the public recruited for the purpose. The sample of digitally excluded people was boosted for: people from communities experiencing racial inequalities; disabled people; those living with long-term chronic health conditions and younger people. The process was intended to be as inclusive as possible. The facilitation and technical team ensured that participants were supported at all points to take a full and active part in the deliberation. Workshops were scheduled to give people time to consider the issues.

The findings

Section A: Attitudes, benefits and concerns

Participants' attitudes towards identification and digital identity services shifted during the course of the dialogue. Many participants began the dialogue believing that having identity documents is purely practical. As participants' discussions developed, many began to think of identity documentation as a basic human right.

Three key findings related to attitudes, benefits and concerns on **trustworthy digital identity services are:**

1. Trust in digital identity service cannot be seen in isolation

Participants contextualise their views on trust within broader considerations of trust in government and business. They draw on their examples of how government and others have managed challenging social, economic and political situations such as exiting the European Union (Brexit), the Covid-19 pandemic and the cost of living crisis. Trust in this context is seen as a challenging and complex issue to discuss.

2. Taking care of digital identity service users

The data collected, used, stored and shared by digital identity service providers is significant. Participants perceive it to be an articulation of being human and a demonstration that they have a recognised role in society. Participants believe the importance of identity data is not simply practical but also instrumental in people having control over their lives and life chances.

This has ethical implications. It means participants want to know that service providers will look after them and their data and protect and support the vulnerable and disadvantaged in society. This is important so that everyone can accrue benefits from digital identity services.

3. Benefits to society

Participants want to know that digital identity service providers are motivated by more than generating income. They call for the trust framework to make it clear that public benefit is a core value for those being certified to deliver digital identity services, and the government and OfDIA as overseers of the programme.

To demonstrate to people across society that this public benefit value is being upheld, participants want to ensure that the trust framework is published in ways

which will be visible and accessible to them.

Participants do not see convenience on its own as a compelling enough reason for increased use of digital identities. They want to know how digital identity services are going to benefit society by making proving identity more inclusive.

Section B: Policy expectations, solutions and implications

Two key findings relate to expectations, solutions and implications for **trustworthy digital identity services are:**

1. Accountability and transparency

Participants place accountability and transparency at the core of trustworthy digital identity services. To enable this, they call for a clear route map in the trust framework outlining actions to take now to minimise long term risks. They argue for longer term assurances, articulated in the trust framework, that their data will be held carefully and protected. Participants feel that the system of oversight through government and OfDIA should make it clear who is responsible when things go wrong and what recourse users have when it does. Being accountable, honest and transparent throughout the digital identity services ecosystem is vital for building and retaining trust.

2. Accessibility, agency and involvement

Participants want to know that these services are accessible to those that want and need to use them. Having options that work for everyone is seen as part of an inclusive system, one which enables people to verify their identity or attributes in the way which works for them, whatever their background, level of skills and experience.

Having control over their data is important to participants. They want assurances within the digital identity services trust framework that they have choice about who they share data with and why.

They call for the public voice to be centred as the primary stakeholder of digital identity services. They describe people should be involved in all aspects of the design, delivery and ongoing decision making on digital identity services. This includes involving people who have experienced barriers to verifying their identity such as prison leavers, asylum seekers and people who do not have a fixed address in the design of digital identity services. If those who have been most excluded from society are included in this process it will be considered more trustworthy.

Amendments and additions to the trust framework

Participants propose specific amendments and additions to the trust framework:

The benefits of digital identity services

Clearly articulate the benefits of digital identity. This means going beyond convenience and efficiency to inclusion.

Embedding simplicity in the trust framework

Providing templates for the terms and conditions for using digital identity services so that people can clearly understand what happens to their data and how potential risks are mitigated.

The importance to participants of having control over their data

Participants believe the trust framework should provide a clear statement on how users 'own' and 'control' their data, including being able to update it and protect personal data they do not wish to share.

A rigorous, effective and human centred complaints procedure

There is a strong feeling amongst participants that the trust framework needs to be explicit about what is expected of service providers in relation to their complaints procedures.

Future proofing digital identity services

Participants call for the trust framework to demonstrate that consideration has been given to future proofing both service provision and its oversight, for example, putting protections in place to make sure digital identities do not, either by design or default, become mandatory.

Ensuring there are protections against system over-reach

Participants want assurances within the trust framework that the data (now and in the future) can only be used for the purposes of verifying identity and nothing else.

The importance of inclusion

Participants like the examples given in the trust framework on inclusion but consider that there could be more examples and more detail to ensure this is specific enough and does not leave, what they consider to be an important aspect of digital identity service provision, to chance.

Principles of trust

Participants agreed on principles of trust for digital identity service providers:

Act with **transparency**, using clear communications and with the expectation of openness in all relationships.

Define, and act within, high **ethical standards** meeting expectations for what good looks like. Look after users' data, protect them from harm, protect the vulnerable in society from harm and bring them into an inclusive system.

Be **reliable** and **proactive**: say what you are going to do, do it, and tell people that you have done it. This extends to complaints, recourse and responding to those who need guidance to use the technology.

Be **genuine, authentic and human**: show that service providers care and put people at the heart of the service. This includes using clear, honest communications which does not over-promise.

Secure the data: data shared with digital identity service provider should not be shared with others without express user permission.

Put **safety** first. Do nothing to harm people or knowingly put them at risk and have safeguards in place for when things do go wrong.

Demonstrate that **public benefit** comes before financial motivations

Part 1
Setting the Scene

1. Introduction

1.1 Background

Digital identity and attribute services allow individuals to prove who they are or things about themselves, such as their age, easily and securely without relying on physical documents. They can enable people to access services more easily, safeguard privacy by enabling people to better control how their data is handled by others and grow the economy by enabling digital transformation that saves people and businesses time and money.

The government is working to enable the use of trusted digital identities in the UK. To ensure that these services can be adopted confidently and securely, DSIT is developing a trust framework of rules and standards, alongside supporting governance and legislative measures.

The UK digital identity and attributes trust framework is a set of rules and standards that digital identity providers can follow to demonstrate that they meet robust requirements surrounding cyber security, fraud and inclusion to build trust in their services. The framework is being developed iteratively, with its second prototype ('beta') version published in June 2022.

To show they follow the framework's rules, organisations need to get certified by independent certification bodies. There are already over 40 organisations using this certification process to prove they meet the right standards to do pre-employment, pre-rental and criminal record checks for British and Irish citizens as part of right to work, right to rent and Disclosure and Barring Service programmes.

DSIT is working to put in place governance structures by establishing the Office for Digital Identities and Attributes (OfDIA), the new governing body for the digital identity market which will support the development of the market by helping develop trust and enable access to digital identities across the UK economy.

1.2 Dialogue aims

DSIT's digital identity programme is at a pivotal phase of work, focused on designing the structure of the new governing body (OfDIA) and testing the beta version of the trust framework. In order to inform further policy making, DSIT commissioned this public dialogue on trust in digital identity services. The public dialogue was commissioned to engage members of the public in a conversation about the shift to greater use of digital identities, what future opportunities and problems this might present, and how certification, governance, and other mechanisms could be used to ensure digital identity services are trustworthy. As the beta version of the trust framework had been developed the dialogue was not intended to test whether digital identity services should be developed.

The focus of the dialogue has been on public trust in digital identities, resolving trade-offs related to digital identity policy, identifying specific issues that need to be

addressed, and proposing policy solutions. Previous research[2] focused on wider principles that the public expected from digital identities and on issues of inclusion but did not include deliberation on detailed interventions, rules to be followed or governance design. It suggests that the public is particularly interested in the ease of use, strong governance, transparency and inclusivity of digital identities. The dialogue has explored each of these areas while focusing on trust in digital identities.

The findings of the dialogue will inform the rules that providers of digital identities can follow in order to become certified against the UK digital identities and attributes trust framework, the functions of the governing body and how it interacts with the public and planning for public communications initiatives. Findings could also impact potential new initiatives, such as new pilots related to use cases or target users and engagement with the market, civil society and regulators.

DSIT has also separately engaged with industry and other stakeholders in testing using sandbox-style methods, testing policy questions by observing how digital identity service providers handle synthetic identity data in different test scenarios. The public dialogue was conducted in parallel with this programme to ensure people's views are considered alongside the private sector testing strand of the policy development.

1.3 Programme objectives

The objectives of the trust in digital identity services public dialogue are to:

- Engage a diverse selection of the public to determine what further policy would be needed to ensure digital identity providers and services are trusted by the public
- Inform the rules in the UK Digital identity and attributes trust framework
- Inform the functions, oversight structure and interaction with the public of the governing body for digital identities (OfDIA)
- Inform planning for public communications initiatives
- Test a new engagement strategy combining a public dialogue and sandbox-style testing with industry.

1.4. Dialogue scope

The research questions the dialogue has sought to address are:

- What rules should be put on digital identity and attribute providers regarding user control of data, transparency, privacy and inclusion?
- What does the public think providers should and should not be allowed to do with users' data?
- What does the public expect from the use of technologies, including biometric technologies, in digital identities?
- How should digital identity and attribute services be monetised?
- What does a digital identity governing body need to have in order to be trustworthy?

[2] Britainthinks: Insight & Strategy, Public perceptions of digital identities and attributes: transparency, trust and data, CDEI, DCMS, March 2022.

- What risks does the public see in digital identities that must be mitigated?
- What should the general public know about digital identities?

The dialogue was designed and delivered with a 'participant-led' approach in mind. This means that we dedicated one of the workshops to explore these research questions with participants, to see if participants wanted to amend or build on any of the questions or reframe the dialogue scope.

HVM convened a dialogue design workshop to review the scope of the dialogue. During this workshop we discussed hopes and expectations for the dialogue; things to bear in mind as we design the dialogue; the range of perspectives to include in the dialogue and 'thorny issues' relevant to a dialogue on trust in digital identities.

Further scoping exercises were conducted through one-to-one interviews with members of the design group, the oversight group and others with a stake in the process. We also conducted lived experience interviews to understand the challenges people face in this context, for example the experience of an asylum seeker, a recent prison leaver, a person with a learning disability and someone who had experienced identity theft. Each of these interviews informed the scope of what was discussed.

1.5 The dialogue context

The context in which the public dialogue took place in the spring of 2023 may have had a bearing on the findings of a public dialogue related to trust. Generally low levels of trust in the UK government were apparent among participants. Ongoing coverage at this time of the UK Covid-19 Inquiry and the House of Commons Committee of Privileges about the legality of activities in 10 Downing Street and the Cabinet Office under Covid regulations, provided evidence for many participants of a lack of transparency and/ or competence by some in government. Participants said that this informed their perceptions of who could be trusted to provide oversight of digital identity services.

1.6 A note on this report

This report is divided into two parts:

Part A: Scene setting

Describes how the public dialogue process was designed and delivered. It explains the participant-led approach and what evidence and information participants received to inform their deliberations. It will be of particular interest to those wishing to understand the detail of the public dialogue methodology.

Part B: Findings

Sets out the dialogue findings. These are divided into two sections:

- Section A: In which participant attitudes towards, benefits of and concerns about, digital identity services are described
- Section B. Policy expectations, solutions and implications in relation to the role of digital identity service providers, government and OfDIA. In this section we set out participant solutions to some of the challenges they have identified, including involving people in society in the design, development and oversight

of digital identity services.

This section will be of particular interest to those with an interest in how trust in digital identity services can be developed and fostered.

Postcode Films created a public dialogue film which shares the experiences of three participants in the process.

2. Methodology

The Public Dialogue on Trust in Digital Identity Services was commissioned on 1st March 2023. Fieldwork took the form of a webinar and five workshops, 20-hours of deliberation, including a pilot process, from 23rd April to 7th June. The dialogue was therefore designed, delivered and reported on in a five-month process.

The Department for Science, Innovation and Technology (DSIT) in partnership with Sciencewise and UK Research and Innovation commissioned the dialogue. It was designed and delivered by the deliberative engagement specialists Hopkins Van Mil (HVM) and independently evaluated by Navigator Consulting with Graphic Science.

2.2 Project governance

A project team was set up to manage the process led by Hopkins Van Mil working with DSIT, Sciencewise and the independent evaluators Navigator Consulting with Graphic Science. See the Acknowledgements chapter for details of who was involved in project governance.

DSIT is a government department. Its mission is to drive innovation that will deliver improved public services, create new better-paid jobs and grow the economy. DSIT's responsibilities are:

- Positioning the UK at the forefront of global scientific and technological advancement
- Driving innovations that change lives and sustain economic growth
- Delivering talent programmes, physical and digital infrastructure and regulation to support the UK's economy, security and public services
- Research and development funding.

Sciencewise is an internationally recognised public engagement programme which enables policy makers to develop socially informed policy with a particular emphasis on science and technology. Sciencewise helps to ensure that policy is informed by the views and aspirations of the public. The programme is led and funded by UK Research and Innovation (UKRI).

HVM is an independent social research agency which creates safe, impartial and productive spaces to gain an understanding of people's views on what matters to society. HVM has extensive experience in preparing for, designing and facilitating effective deliberative processes. HVM's work involves hold a lens up to issues which are contentious, emotionally engaging and on which a broad range of viewpoints need to be heard.

This public dialogue was conducted in line with Sciencewise Guiding Principles and Quality Framework[3] and considerations for online dialogues. The work was supported by a Sciencewise dialogue and engagement specialist. An independent evaluation was commissioned at the beginning of the project providing a formative and summative evaluation of the process.

As with all Sciencewise public dialogues an Oversight Group was established for the

[3] https://sciencewise.org.uk/about-sciencewise/our-guiding-principles/

project. Members of the Oversight Group included experts from industry, academia and civil society. This group was convened by DSIT four times and provided challenge, guidance and advice on the dialogue scope, design and delivery.

2.3 Participant involvement

96 participants from across the UK took part in the dialogue. All participants were recruited using purposive sampling against a specification agreed by the project team. This method of sampling was used to ensure that the group reflected a broad demographic of the UK population. Sampling ensured a balanced spread across factors including age, gender, geographic location, life stage and multiple socio-economic indicators. We set minimum recruitment numbers for some factors to achieve the required levels of participation among people aged 18-25, people experiencing racial inequalities, disabled people, people with long-term health conditions, and people in vulnerable financial circumstances. All participants received a payment in recognition of the time commitment made in taking part over 20-hours of deliberation. More detail on the recruitment process and specification is provided in Appendix A.

Digital inclusion is an essential part of recruitment for an online dialogue. No one who wished to participate in the dialogues was excluded because they did not have the hardware, software or technical knowledge to attend an online workshop. Near the beginning of the process, HVM ran a 'tech support' session to guide people through the online tools used for the dialogue. Some participants were also loaned equipment such as headphones or a webcam in order to take part online.

Participants were supported throughout by the facilitation team, ensuring that participants less confident in sharing their views were given a range of ways of tools to do so, including using the chat and having one-to-one conversations with the facilitators. Workshops were spaced over a four-week period to ensure they were not overwhelming and gave participants time to think and consider the issues outside of the scheduled workshops. Workshops were designed using Plain English materials and with frequent summaries of what had been shared and discussed previously to keep participants focused on the dialogue scope, and to enable the discussions to develop based on what had previously been discussed.

2.4 What is a public dialogue?

Public dialogue is a process during which members of the public interact with academics, industry, civil society, stakeholders and policy makers to deliberate on issues relevant to future decisions.

Public dialogue enables constructive conversations amongst diverse groups of citizens on topics which are often complex or controversial. Not only does it provide an in-depth insight into public opinion, it also offers a window into understanding people's reasoning. The HVM team has extensive experience in designing, delivering public dialogue and reporting on the outcomes.

Public dialogue was chosen as the deliberative method to ensure that participants were given time and a level playing field to discuss the issues that matter to individuals, to communities and to society. Public dialogue is:

- Informed: evidence is provided on key themes in relation to the topic so that participants can give their opinions where public input adds most value; access is given to specialists in their field
- Two-way: participants, policy makers and experts all give something to and take something away from the process
- Facilitated: – the process is carefully structured to ensure that participants receive the right amount and detail of information, a diverse range of views are heard and taken into account and the discussion is not dominated by particular individuals or issues
- Deliberative: – participants develop their views on an issue through conversation with other participants, policy makers and experts.

2.5 The dialogue process

This dialogue was informed by evidence provided by 16 speakers including from DSIT, digital identity providers, wider organisations in industry, academics and research institutes, civil society and regulatory bodies. HVM conducted desk research to create a stakeholder map to identify a longlist of potential speakers. This list formed the basis of those invited to participate in the dialogue design workshop. The list was reviewed by the project team and a shortlist agreed of people who would bring a range of perspectives and evidence to the public dialogue deliberations. HVM also asked the Oversight Group for their view on who should provide input into the dialogue. The final list of speakers was agreed after HVM conducted interviews with each person on the shortlist. As a result of this work agreement was reached on what should be presented to the group by whom.

Professional perspectives were complemented by the perspectives of people with lived experience. HVM conducted desk research to create a longlist of organisations that could give routes to people with the relevant experience such as charities, networks and support groups. Four people were interviewed and filmed describing the following specific experiences:

- Proving an identity whilst seeking asylum
- Identity theft and its impacts
- The experience of digital exclusion for a disabled person
- Proving an identity as a prison leaver.

Material was also produced by HVM to explain key terms and concepts. The dialogue process plans, narrative flow and stimulus were tested and refined in pilot workshops held in April 2023, with 9 recruited participants. Following the pilot process, the 96 recruited participants took part in the following workshops:

A webinar:

To understand the purpose of the dialogue, who is involved and the regulatory context for digital identity services.

A question and scope review workshop:

In which participants continued to develop their understanding of the topic. Whilst doing so they had opportunities to review the dialogue scope and the research questions. They were able to add to and amend the questions and share what they thought should be in scope for their discussions, ensuring the process remained participant led.

Exploratory workshop 1:
Participants were given evidence on the context, history and development of identity and digital identity services in the UK, as well as hearing about the current regulatory framework. They discussed their priorities for identity services given that context.

Exploratory workshop 2:
Gave participants the opportunity to explore identity theft, identity fraud and measures to prevent these within digital identity service provision

Exploratory workshop 3:
Based on an exploration of digital inclusion and data privacy, participants considered issues of human rights and social justice.

The concluding workshop:
Participants took part in activities about and discussion on the trust framework, trust more broadly and communications about digital identity services.

At each stage of the dialogue the facilitation team reminded participants of the materials that they had seen, giving information on digital identity services and attributes. This helped to keep the evidence and contextual information at the front of participants minds as they deliberated on the topic. Reminders were also given as to how participants had responded to these materials at various points in the process. This enabled participants to decide what they wanted their discussions to focus on, which informed the scope of the dialogue process.

In addition, throughout the process participants engaged in deliberation in workshops and in the online space, guided by a design process plan. A range of tools were used including:

- In workshops, time was taken at the beginning and end of each workshop to review what had been seen and discussed. A range of dialogue techniques were used including open questioning and activities to draw out people's thoughts, views and experiences. These included:
    - Mentimeter.com an online polling tool in which we could ask questions such as 'when I say 'identity' what comes to mind?' to understand and track shifts in thinking on key dialogue points
    - Lead facilitator presentations to summarise the key points that had been made in previous workshops for participants to build on in the discussions
    - Q&A sessions with speakers and additional questions answered by DSIT outside of the workshops, with responses shared in the online space.
- In the online space called Recollective[4] a range of online activities were used to give people time outside of workshops discussions to reflect on the issues. These included:
    - A 'digital identity services journal' where participants could reflect on how the subject comes into their daily lives: in the news; on social

[4] Recollective – an online qualitative research tool tailored by HVM for participants to reflect on the topic outside of the workshops, via activities, stimulus review and discussion threads.

media; in their interactions with friends and family
    - Repeated ranking and sorting exercises where the issues that participants had discussed and topics they had raised were summarised into a set of cards which participants could rank in order of importance to them
    - A discussion area where participants could raise topics that they wanted the opinion of others on.
- Posing questions for the sandbox project, a concurrent DSIT project being used to test policy questions by observing how digital identity service providers handle synthetic identity data in different test scenarios.

More information on the stimulus materials is set out in Appendix B. For a sample of the process materials followed in the workshops see Appendix C.

2.6 Analysis and reporting

The HVM analysis and reporting team met regularly to reflect on emerging themes and to develop our thematic analysis approach. After each participant session, facilitators reflected on emerging views from their group discussions. Emerging findings from participant discussions were explored and validated with participants in later workshops to test and refine our understanding.

All qualitative data was thematically coded using the qualitative analysis software NVivo. Early findings were shared in the fifth workshop with participants in order for them to develop their recommendations based on what they had considered important at earlier stages in the process.

Public dialogue is a qualitative methodology. We have used qualitative research methods to review what participants told us, specifically grounded theory, where the findings come from a thorough reading of the transcripts. Transcripts were created from each of the deliberative methods used. We collated what was said into key themes and used those themes to draw out meaning from the discussions. We chose this approach to ensure the findings are rooted in what participants said, rather than looking for confirmation of preconceived ideas. The transcripts used were anonymised so that no one can be traced back to comments included in this report. For a full review of the analysis and reporting process please see Appendix D.

Interpreting and extrapolating findings

Public dialogue is a well-respected, robust approach for engaging the public with complex policy issues in a meaningful and informed way. As with any research method, it is important to consider what the approach means for interpreting or extrapolating findings.

- People interested in a topic are more likely to sign up and attend. While our recruitment process was designed to reduce potential bias, participants may have been more interested in questions around trust in digital identities than might be seen across the general public.
- This report is a snapshot in time, people's views may change in the future

The dialogue was a qualitative exercise, which did not aim to be representative of the UK population. As such, findings are not intended to be statistically representative or generalisable across the wider public.

2.8 About this report

Qualitative research reports, including this one, do not report on the number of times something was said, but rather the strength of feeling expressed. As such we use the following quantifiers in the report:

- 'Many' or 'most' when it is clear that all or almost all participants shared a similar view
- 'Some' when a reasonable number of participants shared a similar view
- 'A few' when a small number of participants shared a similar view

Bullet points are used to summarise key points made. These mostly reflect areas of agreement and where points were made by many participants across many groups.

Anonymised quotations are used to highlight points made by a number of participants and to underline points made by a range of people. They also highlight points of particular significance to participants.

Reading this report

Those reading this report will find:

"**Quotes** set out like this. Quotes are used throughout the report to illustrate points, not replace narrative. These are provided verbatim in participants' own words, we remove filler words, but do not make changes to spelling or grammar so as not to distort the participants' meaning".

Summary icons such as this illustrating a key topic or theme.

Extracts from the UK digital identity and attributes trust framework

Relevant extracts from the trust framework are presented in a greyed-out box with a coloured frame such as this one.

Summary findings

Presented at the beginning of each chapter in text boxes with a coloured frame like this one. They set out the main findings to be discovered in the chapter.

The dialogue findings are set out from the next page onwards.

Part 2
The findings

Section A. Attitudes, benefits and concerns

Section B. Policy expectations, solutions and implications

A. Attitudes, Benefits and Concerns

3. Attitudes towards digital identity services

Summary findings

We begin this chapter by describing participants' everyday experiences in proving something about themselves or verifying their identity. Many participants began the dialogue believing that **having identity documents, and ways of proving something about themselves, such as their age, is purely practical.** Participants see **passports and driving licenses as vital gateway documents.**

As the dialogue developed, because of what they heard in presentations and films, or as a result of conversations with other participants, many began to think beyond their own experiences to that of people who have less secure means of verifying their identity or attributes. From this point in the dialogue **many participants began to think that being able to access identity documentation easily is essential for being able to play a full part in society. As such it should be considered a basic human right.**

A few participants were consistent throughout the dialogue in saying that **they will not trade-off their privacy for convenience.** For these participants, unless data privacy is thoroughly and effectively managed, and security systems are seen to be trusted, uptake of digital identity services is likely to be limited. This is not true for everyone as we see in chapter 4.

For some participants **trust in digital identity services is difficult to accept, particularly if they consider the data shared with identity service providers to be an articulation of their humanity.** Seen through this lens, data is considered precious and significant and as such **needs high levels of protection.**

3.1. The frequency of proving an identity

Table 1 summarises the ways in which participants describe verifying their identity or something about themselves. Participant experiences range from:

1. Accepting the need to verify their identity, or demonstrate attributes, for large and small tasks, and having a process which they already trust for doing that; to
2. Having had a challenging experience when trying to verify their identity or demonstrate attributes, they do not take it for granted that they will have the right process, document or description available when they need it.

A common thread for many participants is just how frequently they need to verify something about themselves.

> "It suddenly dawned on me how often we prove our ID without a second thought. (It happens) every day when we open our phones using face, fingerprint, or a four digit code; open various accounts for shopping online;

government apps such as HMRC; or online banking." Participant, Recollective – online digital identity journal

Table 1: A selection of ways[5] participants verify their identity or something about themselves

Everyday verification	Verification for life shifts	Renewable longer-term needs
A simple process – one form of proof e.g. age/ address	A more complex process requiring several different documents/ forms of proof	
Shopping: • Online shopping • Collecting parcels • Buying alcohol • Buying some equipment e.g. cooking knives	Applying for a job	Getting or renewing a passport
Leisure facilities/ apps • Joining a gym • Joining a library • Gambling • Dating • Social media	Professional accreditation/ registration	Getting or renewing a driving licence
Travel • Renting a car • Proof of travel ticket purchase • Boarding pass • Covid pass	Housing: • Renting • Buying • Acting as guarantor for a child renting a property	Getting or renewing travel passes

Finances
• Bank account access
• Checking your credit score
	Financial services
	• Opening a bank account
	• Applying for a
	  ○ Loan
	  ○ Mortgage
	  ○ Credit card
		Applying or renewing residency permits/ Visas

Voting in local elections	Registering: • A birth • A marriage • A death – being an executor for a will	Government gateway e.g. for HMRC self-assessment
Office entry cards/ eligibility for working on site	Being a company director	Work security clearance and DBS checks

[5] Much of what participants describe here is included in the Government Digital Service's One Login programme. Participants did not make a distinction between One Login and digital identity services.

Redeeming energy bill vouchers	Health • Registering with a GP/ dentist • Setting up the NHS app • Accessing emergency health services	Blue badge application or renewal

Participants describe their passports and driving licences as gateway documents which they use most frequently to verify their identity or an aspect of it. Other documents which are helpful are utility bills; birth certificates; NHS and National Insurance numbers; and work and education certificates.

> "My UK passport is quite a powerful thing it seems" Participant, Recollective – online digital identity journal

> "If, God forbid, there was ever a fire where I live, I'll be jumping out of the window holding my passport. For me, that's the most important thing. I'll protect my passport." Participant, England group

3.2 A verifiable identity: both practical and significant

Participants describe the importance of having a verifiable identity as a practical tool for accessing work and services. They see identity proofs as a means of achieving everyday tasks like buying a bottle of wine in a local shop and proving who they are when collecting a parcel. These tasks are seen by participants as easy, every day and only of consequence when they do not have the right ID with them at the right time. Early in the dialogue when participants discussed identity services in this practical sense, some questioned the need to discuss digital identity services at all.

> "I honestly don't know why we are discussing this. If it isn't broke don't fix it. We've got ways of proving who we are, or our age or whatever without a big hoo-ha about what format that proof comes in." Participant, Scotland, Wales & Northern Ireland group

Participants see identification for consequential transactions such as renting or buying a property; proving you have the right to work in the UK or to get or renew a passport or driving license as more complex. It moves identification beyond the practical to instrumental in achieving life shifts such as demonstrating something significant and personal to them, including gender transition.

> "If my birth documents need changing because I want to live my life as a man, then that's a big deal. It has consequences if I can't do that." Participant, Scotland, Wales & Northern Ireland group

The more participants thought about identification, the more they considered it a route to demonstrating that they are part of and contribute to society. Many participants feel that not being able to demonstrate something about themselves could have a significant impact on their lives, including having a meaningful role in society.

> "Being able to prove your identity allows you to take an active role in society." Participant, Scotland, Wales & Northern Ireland group

Having a verifiable identity is seen by participants as important in having control over

their lives and destiny.

> "To be able to prove who you are means you are in control, you can move forward. It's a positive thing." Participant, England group

3.3 Moving from a 'me' into an 'us' position

Many participants said that the most significant shift in their thinking during the process was initially starting from a 'me' and moving into an 'us', and 'society' position. These participants feel themselves to be privileged because they have the security of being able to prove who they are or something about themselves easily. As such their principal concern early in the dialogue was data privacy.

In the third of our three exploratory workshops, discussions focused on digital inclusion and data privacy, issues which participants said were important to consider in their deliberations. At the beginning of the workshop participants heard from speakers with a focus on inclusion and human rights, the experience of young prison leavers and on data privacy and its importance.

Participants also heard from our lived experience interviewees (figure 1)[6] with experience of vulnerable IDs in a range of contexts. These presentations and the evidence they provided on the importance of being able to prove an identity, or verify an attribute, were a significant moment for many participants. As a result of these films participants said they could see that having a secure, verifiable, identity is for some people a struggle to achieve.

Figure 1: Videos and audio clips filmed by Postcode Films to provide the lived experience perspective

The discussion on human rights led many participants to think that being able to access identity documentation easily is what is needed to play a full part in society. As such it should be a basic human right.

[6] The following lived experience interviews can be viewed online at: Janet & Siôn; Comfort; Tyrone (see appendix B also).

For some, discussions on human rights and privilege shifted their perception of what identity documentation is: from something practical to something with much more significance and a core part of how we establish who we are. This gave rise to a greater depth of discussion on why trustworthiness in this sphere is complex. If identity is seen as an articulation of who participants are as human beings, then it is much harder for them to trust those who hold sensitive identity proof data and those who oversee the system.

> "I've learnt this can be a sensitive subject for a lot of people. Identity is the core of who we are and a lack of trust of the government/ authority is key to understanding the use of digital identity." Participant, Recollective – online digital identity journal

Many participants, those who had not had the experience of challenges of proving their identity, continued into exploratory workshop 3 and the final deliberations with a conviction that the dialogue topic is more significant than they originally assumed. The layers of complexity were now obvious and worth the depth of deliberation provided in this public dialogue.

> "Not having a safe way of identifying yourself could make you feel as though you don't count." Participant, Scotland, Wales & Northern Ireland group

For some participants one thing did not shift in their thinking as they moved through the dialogue. They will not trade-off their privacy for convenience. For many, unless data privacy is thoroughly and effectively managed and security systems are trusted, take up of the service is likely to be limited to those who do not think about the consequences of prioritising convenience.

> "I think me and others in this dialogue conclude that security is our top priority. It doesn't matter what benefits a system could bring to my life, if I was not comfortable with the management of my data I would not sign up." Participant, Recollective – online digital journal

4. Benefits and concerns

4.1 What participants see as desirable in DI services

Summary findings

Participants **welcome that convenience is a benefit to users highlighted in the trust framework**. Some participants said **convenience might convince them to use digital identity services, even if they don't entirely trust the system**. This is not true for all participants who believe that **convenience, although useful, is not significant enough to outweigh potential risks related to privacy, data theft, and the risk of digital identity services putting profit before the needs of users**.

Participants add potential benefits of trusted digital identity services as being:

- **Universality and simplicity:** being able to use a UK digital identity across country borders; and the same digital identity app or software in many different shops or services
- Having **control** over their data
- Offering **a system for those who currently do not have secure identity documentation**

Concerns about digital identity services are important to participants when discussing trust in the system. They raise issues such as being careful not to become overly **dependent on the technology**, which risks lack of access when the technology fails. They want to be reassured that there is an offline mode as a backup for the system.

Accessibility is a key concern for many. They want to ensure that service providers consider the needs of people without the equipment, confidence or experience to access the technology. Participants believe digital identity services should not become mandatory by default, and that paper alternatives should always be available.

Other key concerns set out in this chapter include:

- Monetisation of the system, with **a concern about data being sold on to organisations unrelated to identity verification**
- A human centred approach to complaints and customer service is called for by participants; they are **concerned that service providers will be more focused on getting the technology right than they are with developing a service that will take care of users and their data**
- **Systemic challenges** e.g. institutional racism potentially being built into the system, or the cost of living crisis affecting people's ability to pay for identity services.

Section 8 of the UK digital identity and attributes trust framework, beta version[7], sets out the benefits for users of digital identity services. In reviewing these, participants could see four main benefits had been listed within the current version of the framework (figure 2):

- Convenience
- Speedier verification
- Safer interactions
- An aim for universality and mutual recognition.

> Being able to share their digital identities and attributes with different organisations, and between users, will make it easier for users when they choose to complete interactions and transactions digitally. This is because it will be much quicker and safer to prove their identity and eligibility when they interact with a new organisation. The UK government plans to make it possible for this to happen across different industries, sectors and countries where it's safe and legal to do so.

Figure 2: The benefits to users stated in section 8 of the beta version of the trust framework.

Many participants welcome the fact that benefits to users have been identified in the framework. They express the view that there would be no motivation for anyone to make use of digital identity services unless the benefits go beyond those for government, businesses, employers or others who need to verify user identification documentation.

Convenience

Participants agree that convenience is a valuable benefit to accessing digital identity services. During the dialogue, they shared everyday frustrations of forgetting, or not being able to find, a critical document at the right time. Being able to refer to documents that were already securely held for a range of reasons was also seen as part of a 'convenience' benefit.

For participants who said, "my whole life is on my phone" using digital identity services is a convenient option for many tasks. Participants believe that convenience and making people's lives easier is important. They refer to the pace of life now and the expectation that using digital services will ensure that identities and attributes can be verified quickly, even instantly. Some participants express the hope that digital identity services will help them to organise their lives more efficiently and reduce the need for paperwork, which they lose or misfile.

Even those who feel resistant to the idea of digital identity services generally, express the view that convenience could be the thing that sways them into acceptance.

> "I've got a bit of a battle going on in my head, because I'm kind of anti the whole idea. But the convenience of it is really appealing. That might be starting to outweigh my concerns." Participant, England group

Speed was also seen as an important benefit with many saying that having quick access to the services they need is important, for example paying for something using your phone or opening a bank account.

[7] UK digital identity and attributes trust framework beta version (0.3), updated January 2023, referred to in the rest of this report as 'the trust framework'.

> “My husband opened an online only bank account. (It) took ten minutes to complete and at the end he had a virtual bank card ready to use. Far easier than opening a high street account where he needed proof of income and residence.” Participant, Recollective – online digital identity journal

However, for some participants convenience, although useful, is not significant enough or a proportionate enough benefit in relation to potential risks to privacy, data theft and private sector profiteering. These participants say they have found ways to prove their identity or something about themselves which work well, and they don’t need a complex system of digital identity services to function in the world.

> “I can't really see the benefit of this other than ‘convenience’. It takes minutes to create a folder of personal documents and store them safely on my own. Why would I trust a third party to retain those documents for me? (This) is unnecessary, pointless and invasive.” Participant, Recollective – online digital identity journal

Potential for safer interactions

Participants do see the potential for safer interactions within digital identity service provision. This relates most closely to the protection of personal data. People’s experiences of data loss inform these discussions.

> “Yesterday my laptop received an update. I lost my search history and several of the apps I use were corrupted so that they no longer recognise my passwords. I’m still not sure what I’m going to do but I did think to myself how nice it would have been if I had one universal ID to access all my sites and apps.” Participant, Recollective – online digital identity journal

Being able to prove one aspect of themselves, and no other, is seen as a clear benefit to participants, and important in building trust. They welcomed the fact that a digital identity provider would have verified that a person is over-18 with checks through appropriate documentation. Then when that person goes to a club, buys alcohol or accesses any service which needs proof of being over-18, all that the shop, club or service provider sees is that this person is over 18. They don’t need to see the full documentation that would share more data than is necessary such as address or driving licence/ passport number. This feels more secure to participants and a more appropriate limit on who can see what from their personal data.

> “The digital identity would need to respect the individual’s permission so that they can control what information gets shared with who. So if I said Tesco’s could see that I am over-18 but couldn’t see where I live that would be of benefit.” Participant, England group

> “I’m currently doing job applications. They ask so many details, including about whether you are gay, straight, bi-sexual. A benefit would be absolutely that I can make sure no one sees my gender identity, they just see the bits they need.” Participant, Scotland, Wales & Northern Ireland group

Participants gave several scenarios of when they have been asked to share information verbally in a public place, for example at their GP’s reception being asked why they want an appointment; at a police station trying to report a crime but being asked to share details about where they live, or who they live with. Participants feel that relevant elements of a digital identity could be shown, rather than shared

verbally in those situations, which would be a benefit in terms of protecting sensitive information and their privacy.

Universality and simplicity

Some participants had personal connections to asylum seeking or immigration, either via direct experience or from family members or people in their community. These participants believe that an important benefit for digital identity services would be recognition of an identity across country borders, in effect a global digital identity.

Reciprocal arrangements between countries are seen by many as something that would be beneficial for the system. However, of more immediate concern to many is that one digital identity service is recognised by all those organisations that need to check something about someone or verify their identity. Participants view a system which doesn't provide universal acceptance as being ineffective, but one that does as hugely beneficial. For example, participants speak of being able to prove your age using the app of one digital identity provider across many different shops, or leisure services.

> "I think it has to be universal and that means being accepted everywhere, and it has to be universal because otherwise you know, there is no benefit, you are just running more and more apps to do the same thing." Participant, Scotland, Wales & Northern Ireland group

Keeping things as simple as possible is seen as vital.

> "But what I'd like is a single app. It's my passport, driving licence, everything." Participant, England group

Participants list a series of benefits around the concept of simplicity, at the top of which is making life simpler, given all the administrative pressures people experience every day. Whilst participants understand that digital identity services alone cannot result in all these benefits being achieved, they believe that the following benefits could be in some ways supported by the adoption of these services:

- A simplification of digital identity service terms and conditions, with digital identity service providers agreeing to a common form of terms and conditions which are simple, clear, visual, easy to read and short
- Making it easier to travel without having to remember paper documents
- Keeping an individual's proof of identity/ attribute data in one secure place, getting rid of multiple apps and documents
- A simplification of right to work/ qualification verification checks
- Being able to simply update documents e.g. a change of name, marital status, address, gender identity.

Control over 'my' data

Participants consider that the data held by digital identity service providers to verify their identity or prove something about themselves should be 'owned' by them and within their own control. Participants consider that they should be able to:

- Update and correct incorrect data about themselves as and when they need to e.g. if they have new information on a credit score, or if they no longer identify with their birth gender
- Exercise their right to be forgotten, with swift responses from digital identity

service providers when they have made such a request
- Protect personal information that they don't wish to share e.g. specific details within medical or criminal records unless completely relevant and specific
- Ensure privacy for views, opinions and protected characteristics e.g. political views, marital status, gender identity, ethnicity, disability – all as protected under the Equality Act 2010[8]
- Verify that there really is a need for data to be checked, stored and shared for the purposes of digital identity including putting limits on the amount of data that can be collected for the purpose of identity/ attribute verification
- Set out within the digital identity services trust framework the parameters for who data is shared with and why
- Make sure family members can remove the data of a family member who has died.

> "I think it's about whether people have choice on the important things. We should always have the choice to keep our own data or, or not, but to basically still be the owner or keeper of our own data. I think that and how much data we share should be our choice." Participant, Scotland, Wales & Northern Ireland group

Verification for people with vulnerable identities

Many participants believe there is a clear benefit in digital identity services for those with vulnerable identities. They see this as an opportunity to enable people to prove who they are or something about themselves with support to use the digital identity services. They hope that provision can be made for people without identity documents to be enabled to use digital identity services.

Participants also suggest that the government, or the digital identity oversight body, could play a role in ensuring that people have appropriate documentation to prove their identity. For example, giving everyone who leaves prison a recognised document which gives a previous address, states what training has been completed and gives them an identity number or a form of verification which could enable them to open a bank account.

> "If the government wants them to play a constructive role in society, they can be given some sort of ID through which they can get a job, get paid, find a home and play a positive role in society." Participant, England group

Concern was also expressed for young people who have been estranged from their families, or people trying to leave abusive and controlling situations. They feel there could be a role for digital identity providers to support people in these situations and offer them a digital identity which would help them move forward with their lives because they can simply and easily prove things about themselves, for example to get a job or find accommodation. They wonder if it is possible to include an element of the trust framework which highlights this as an important role for the digital identity service providers and one that the government would support.

One participant summed up the views of many in saying,

[8] https://www.gov.uk/discrimination-your-rights

> “A good benchmark to know whether digital identities will work is if they include those marginalised groups, and it works for them. If they work for them, then they really can work for everyone.” Participant, England group

4.2. Concerns

Dependence on technology

Concern was expressed by participants about a dependency on the technology, and the issues that might cause when something goes wrong, such as if their phone is lost or stolen. This concern extends to significant power cuts, floods, or other emergency situations when their devices can’t be recharged or accessed.

> “My biggest worry is what about if there’s a power cut? What if all the systems go down and your whole life is online? What if there’s a flood or something like that? You can’t access anything. How are you going to prove that you own that house? Or car, or whatever?” Participant, England group

Many participants thought about the experience of losing their phone, or phone charger, or experiencing phone theft at a critical moment. They wonder what the repercussions of losing access to the main way they have of verifying attributes or identity would be.

> “You lose your phone, it gets stolen, that’s your whole life gone, because all that information is in that phone.” Participant, England group

Our dependence on technology is only seen as a benefit for participants if the technology can be relied upon. This causes concern about:

- What happens when the technology fails, “Today the airport e-gates went down. What would happen if this happened to the digital identity system?” Participant, Scotland, Wales & Northern Ireland group
- Or if there is a system-wide hack - with geo-political implications, “If (another country) decides to hack everything and close everything down, we can see what will happen. It’s a great way to destabilise society.” Participant, Recollective – online digital identity journal
- Or if just, as frequently happens, signal to the phone is lost, or battery charge runs out?

Participants suggest that some sort of ‘off-line’ mode should be part of the trusted system. They believe that ensuring users can access their digital identity, even when they don’t have access to Wi-Fi or a device, is essential.

Accessibility

A recurring concern was about how accessible digital identity services can be for people across society. Participants refer to people who may not have the confidence, the skills or the knowledge to use the technology on offer. In this context they speak about biometric technologies not working for everyone, for example fingerprint recognition being impossible for some disabled or elderly people. This means that the technology needs to offer a range of options, fingerprint or facial recognition technology for those that want it, but also a pin or password access for those who would prefer to use that. It is essential for participants that the technology does not over-turn the possible convenience of the system.

Participants like the fact that there is a rule on inclusion in the trust framework (figure 3). However, they consider that the rule should extend beyond monitoring and allowing the user to retake an identity or attributes check. More information in their view could be included on how to make the service accessible, and measures to ensure the technology works for everyone in society, whatever their circumstances.

Some participants have specific experience of supporting parents, or working with people whose first language is not English, or with people with learning disabilities. They highlight that some people will need support to be able to use a digital identity tool. They suggest that services should invest in ensuring that the terms and conditions, the technology and the support provided are all in accessible formats such as Easy Read and the guidance is clear to those challenged with lower levels of literacy.

Participants want to make sure that identity verification is not digital by default and that it is always possible to use paper documents. They see this as particularly important for people who are not confident or familiar with technological solutions, but also for those who perhaps because they are unsure of the security measures in place choose not to use digital identities. They want no suggestion that this is a situation where,

> Making your products and services inclusive means as many people as possible can use them no matter who they are or where they're from. This includes people who do not have traditional identity documents such as passports, or who may find it difficult verifying their identity to access services online. However, there are reasons why someone might be legitimately excluded - it is fair to restrict service access on account of someone's age e.g. you cannot buy certain products until you are 18.
>
> Organisations must follow the Equality Act 2010 when considering how to make sure no one is excluded because of their 'protected characteristics'. This applies to all organisations offering services. Public sector organisations or non-public sector organisations carrying out public functions will also need to meet the public sector equality duty (PSED) detailed in the Equality Act 2010.

Figure 3: The rule on inclusion in the trust framework.

> "They might feel kind of forced, like there is no option. You don't want to be forced to give your information even if you don't feel comfortable." Participant, England group

Participants propose that there are a range of mediums for users to prove their identity: physical documents, scans of documents and digital identity. Because people across society have a range of needs and the system needs to work flexibly to encompass those.

> "We are living in a digital age, but not all the population is digitally literate. So unless you are going to make it mandatory that every citizen has to have a certain level of digital literacy, then I don't see how everything can be done digitally." Participant, Scotland, Wales & Northern Ireland group

Having these options is seen as part of an inclusive system, one which enables people to verify their identity or attributes in the way which works for them, whatever their level of skills and experience. Having paper documents also provides assurance and backup if the technology fails.

Knowing that bias, discrimination and exclusion will not be embedded in digital

identity services or perpetuated by those that run them is important for some participants. Many participants said a redline for them was a service which, either by design or default, allowed discriminatory practices to take place.

> "What are the redlines? Well clearly that providers should not be allowed to discriminate based on people's personal data." Participant, England group

The use of biometric technologies was discussed in this context, with participants concerned about the way that the AI learns. There is a perception that biometric technologies have been frequently developed using white male faces to train and test them, a practice which is seen to be inherently discriminatory.

> "Training data sets look like me. White, male, middle aged. So really good at identifying me but not if you're not my kind of gender or ethnicity." Participant, England group

In the context of bias, discrimination and exclusion participants refer to:

- Only using biometric technologies if they can be assured as non-discriminatory and non-biased
- Ensuring that the trust framework sets out ways for digital identity services to make life easier for everyone, not just those who can afford to pay, or who have the 'right' profile
- Uphold what is in the framework currently about monitoring what is happening to make services inclusive, and regularly evaluate service provision to ensure this is the case
- Ensure the framework embeds support for the digitally excluded so that it is possible for them to use these services if they wish to
- Embed values of inclusivity in all approaches so that bias and discriminatory practices can be removed and addressed.

> " It feels as though the system will just replicate existing inequalities and it's always the same groups that are involved. This will lead to ongoing problems." Participant, Recollective – online digital identity journal

Many participants are fearful that disabled people and the elderly could be left by the wayside if they can't become technologically or digitally literate. They see this as unacceptable. Other concerns are about what access to devices or digital tools people have. They are concerned for people who do not have, and cannot afford, a smartphone, a tablet, a computer or the broadband to access the Internet. They are also worried about those who do not have English as their first language and will be excluded if they can't understand basic instructions.

Some participants see the development of the trust framework as an ideal opportunity to address these fears. They suggest that the section on inclusion in the framework could be developed, working in co-production with those who have experienced these barriers, to make sure the technology, the language used, and the knowledge required to access the services are all appropriate to a diverse system which values inclusion.

> "If I want this to work then it has to be possible for everyone. So if everyone is not able to get the ID in the way that they want are we creating an underclass within society? It would make me and others here very angry if that's the case." Participant, Scotland, Wales & Northern Ireland group

Monetisation and digital identity services

For a few participants monetisation of digital identity services is not a concern. This is because they:

- Consider it to be normal that a company needs to make money, and would expect to be able to profit from running its business
- Would expect to pay for a service which makes life easier and identity proofs more convenient
- Assume that users will be charged, but in a clear and transparent way with published pricing structures, no hidden costs and at rates which are affordable
- Assume that the service will be provided at no charge to the user but that the company will have other ways of making money from the service such as advertising.

However, for many more participants monetisation of the system causes concern, particularly when they think about digital identity service providers charging other organisations to access user data. This is acceptable to participants when it is part of the digital identity ecosystem, for example, charging a bank to be able to use the system to verify their customers' identities. It becomes unacceptable to many participants when users' data is sold on to external organisations parties. It is particularly unacceptable to participants when:

- Data is sold on to external organisations, for example for marketing purposes, without an informed and transparent consent process – a circumstance which occurs when a user might quickly accept terms and conditions which they have not read because they are long and complicated
- Data is shared with a series of organisations, making it less and less secure with each transaction, exposing the digital identity service user to risk of identity theft or fraud.

  "The more you give access to third parties, then the model of income generation becomes a model for data breach." Participant, Scotland, Wales & Northern Ireland group

Concerns about the monetisation of the digital identity services include that:

- Charging users to supply digital identity services could exclude those in society who are likely to find a digital identity most valuable, such as those with vulnerable identities due to asylum seeking, homelessness, disability, gender transitioning or being most at risk of identity theft
- Services might offer free services initially, but gradually add in charges for the user which are accepted because they are subtly and incrementally introduced. For example, a subscription model, or a tiered payment structure where some documents can be included for nothing, but a paid for premium service releases more user benefits. Both options are seen to exclude people without the means to pay and have potential to lead to divisions in society
- Company motivations are centred on profit-making, not on people's needs, or safety and support for individuals who are using the service

  "I get a bit fed up of seeing the same cycle of behaviour thinly disguised as being for the good of the people when it is always about money and never for the people, especially the less profitable people who of course are in the

disadvantaged groups." Participant, Recollective – online digital identity journal

- People will be charged twice, once to renew a passport, for example, and again to include it within the digital identity system
- The system in the long-term is not viable because it doesn't generate enough income for the companies, resulting in companies folding with inherent risks to the data held by them.

A risk participants consider possible is that digital identities become commodities and perceived as a product rather than as an essential proof of their identity or an attribute. Participants see this as negative and damaging.

> "This is identity, this isn't a consumer product, this isn't just a service, this is your everything, this is the sum of your parts. Trying to commercialise this is wrong." Participant, Scotland, Wales & Northern Ireland group

The multi-provider model

Participants were told that more than forty companies are already certified for some aspects of digital identity service provision. For some, this was a challenge for data protection. They believe that this means that many different organisations could be managing a separate aspect of their identity, making it less secure.

> "If all of these 40 different identity providers have my data stored in slightly different ways. That feels a bit more vulnerable than at the moment where my driving licence lives in my wallet as a physical piece of plastic, rather than 40 different copies." Participant, Scotland, Wales & Northern Ireland group

4.3. Concerns – globally and at home

Participants identify four specific concerns that make it hard for them to entirely give their trust to the system.

1. The potential to undermine democracy

Some participants are concerned that the trade-off for convenience is exposure to identity fraud and theft. They are fearful that large corporations and technology companies are not solely owned and run within the UK. This has the potential, in their view, to expose people to the risk of fraud and identity theft on a global scale across country borders.

There is an additional fear that, through this global system, countries that wish to undermine geo-political systems will harvest data to gain information and influence change.

> "That's the greatest risk to society. Not that somebody finds out my date of birth or where I live, but voting, financial systems and our society will be undermined by the availability of that data." Participant, Scotland, Wales & Northern Ireland group

2. Perpetuating existing systemic inequalities

In the UK participants see a significant risk in digital identity services which perpetuate inequalities in society. For some, trying to develop a trusted system for digital identity services is near impossible because of the existing flaws in our social

and economic environments. They feel that building a system which exists within an already flawed society will increase harm to those people who are marginalised by society.

They point to examples they have already seen where unfairness and discrimination seem to be embedded in our systems, for example,

- Racism within policing and the criminal justice system with examples of stop and search and the Stephen Lawrence case being cited
- The disproportionately negative impacts of Covid on people from communities experiencing racial inequalities

  "We have to understand how deep racism is. There are figures out recently, saying that 70-80% of the Covid fines went to Black and Asian people[9]. If they had digital IDs and knowing the system is biased against them. That's going to make literally every Black and Asian person completely more scared of having an ID." Participant, England group

- The cost of living crisis having a substantial impact on those who live in disadvantaged communities.

  "If you aren't in an upmarket town, uptown society, you are discriminated against all the time." Participant England group

3. System over-reach

The risk some participants articulate is that the system will over-reach. They suggest that this may not happen immediately, within the purview of the current trust framework, but may do so over time. As a result, they want the trust framework to give assurances that the data (now and in the future) can only be used for the purposes of verifying identity and nothing else. They specify that they do not want to see at any point government departments having access to data for reasons beyond identity and attribute verification, for example, as a check against benefit fraud.

> "What if in the future these public bodies gain open access to our information and at any point can use and possibly share this, perhaps without consent." Participant, Recollective – online digital identity journal

4. Future proofing the system

Participants call for the system to be future proofed, concerned that if it isn't the measures set out in the trust framework about how to operate with trustworthiness will be undermined and ineffective. Five key areas are covered within this 'future-proofed' system.

Table 2: Key aspects of future proofing the policy and the framework

Mandatory over time

Participants were told and understood that there is no intention within the current policy plans for digital identities to become mandatory. Some are not convinced that, even if not the intention now, this would

[9] www.parliament.uk Is there unlawful discrimination in the use of FPNs?

be the reality in the future. They are sceptical of government motivations for investing resources in establishing a digital identity services model and framework which is only motivated by convenience. This is a significant factor in the dialogue for people – it was mentioned frequently as something that could undermine trust in the system.

"I do wonder how long it is going to be until they make it mandatory. I think it might be a bit of a slippery slope." Participant, England group

It is also seen as something that could happen inadvertently, for example if more and more businesses and service providers *only* accept identities verified digitally. It will not be government policy, but it will be in effect mandatory.

The business model

There is an expectation expressed by participants that digital identity services and those overseeing them keep up with potential changes in the business model, making sure aspects, such as how the system is funded, cannot change dramatically without the consent of people across society. Participants believe that if significant changes can happen without consultation trust will be undermined.

"We want some sort of measure in place to prevent a universal paradigm shift in the business model. So if they decide to change how they are going to operate we should have a say in how that works." Participant England group

Technological advances

Keep up with technological advances to ensure that the policy, the legislation and the trust framework reflects the protections that are in place in the context of new developments. For example, participants mention rapid developments in AI which were on the news during the period of the dialogue fieldwork. They heard that policies regulating these technologies are not keeping pace with the technology.

"On the radio they had somebody on from one of the AI companies. He says it is moving so fast that even one year down the line (everything) will be unrecognisable from now. How do we protect the digital identity side from being unrecognisable, so that none of the policies work?" Participant, Wales, Scotland & Northern Ireland group

Government policy

Use the trust framework to set out how the principles within it are protected with shifts in government, in policy and in the social and economic landscape.

"If there is a new government and new policies we still need to know that the trust framework is protecting the system, that it won't be

thrown out and we go to the wild west." Participant, England group

Protections for other policy areas

Participants are concerned that developing digital identity services does not undermine work in other policy areas. For example, they speak of the potential impact on the environment of large-scale data storage; and geo-politics being affected by the protections needed against data being hacked by a foreign power.

"All this data is being stored, and that will increase. This could cause a massive environmental issues in the world because all the servers are actually storing this data. That's a huge amount of CO2." Participant, England group

Throughout the dialogue participants feel that the main benefit cannot only be convenience. This doesn't seem substantial enough for the effort that government, services providers, third sector organisations and people across society as stakeholders need to make in establishing the programme. They feel there should be other benefits, for example, enabling more people to be able to prove their identity than currently can with paper documents. They feel there is a potential risk in trust in the system being undermined by a lack of foresight in terms of technological advances and policy protections.

B. Expectations, solutions and implications

5. Expectations of digital identity service providers

Summary findings

We begin this chapter by describing participants' expectations in relation to data protection and security. Central to participants' thinking is that **the systems put in place are robust and effective**. They want to be reassured that **data protection is a higher priority for service providers than profit making.** Suggestions are made for monitoring systems, including employing 'ethical hackers' as a constant check that data security is working, and risks of data breach are minimised.

A sense of unease came from the range of software and data storage methods used by service providers. **They want assurance that the trust framework will set out the standards for how to store data and where data is stored.**

Participants expect service providers to **operate within a trustworthy corporate culture which invests in staff, trains them properly and employs people with the appropriate skills and experience** to deliver the service.

Effective communications and transparency are important to participants. They want to be reassured that there are no **hidden agendas** and that **people across society are made aware of digital identity services** and are **clear what they do.**

Service providers **acting with transparency is a key expectation**. Participants propose that **service providers should publish key information** about their work, such as how they protect data and who has access to stored data. It is suggested that expectations of this published information are set out clearly in the trust framework. Participants expect **clear and accessible communications at all times with jargon-free, Plain English and visual summaries that people can readily access and understand**.

This chapter ends with an analysis of what participants expect in relation to trust. We describe what and who participants consider trustworthy which highlights the **importance of building relationships over time**. Principles of trust are required by participants when considering how trustworthy digital identity services are. **These include high standards, being reliable and genuine, acting with discretion and putting safety first.**

In this second section of the report the focus is on the expectations of, solutions for, and implications of trusted digital identity services. The section has a policy focus. We begin with expectations of digital identity service providers.

5.1 Data protection and security

A key expectation of digital identity services is that the data they hold about identities and attributes is protected and security measures are in place and robust.

Participants noted that at least four parts of the trust framework cover the rules for data protection and security, including standards, information management and security.

Given what participants feel about the very personal nature of the data that would be shared with digital identity service providers, they expect that data protection and security measures set out in the framework, and delivered by service providers, are robust and effective. Key considerations for participants in relation to data protection and security are:

- Making sure their own device is appropriate/ up to date to handle the data protection measures set up by the digital identity providers
- Having two-factor authentication as standard
- Retaining the encryption methods in the trust framework, making sure these are always up to date and in line with technological advances
- Using authentication methods which are hard to break through, biometric technologies such as fingerprints and facial recognition are considered more secure than passwords by many
- Ensuring the technologies used for digital identities keep pace with the fast-moving technological environment
- Working to high data protection standards because this data is so important, and its theft or misuse has serious and long-term consequences

  "(Quality) standards need to be high for this project which is about who we are as people." Participant, England group

- Having a service level agreement between digital identity service providers and relying parties to ensure that how data is shared, transferred and used is secure.

  "If, for example, a bank is paying the digital ID provider, I think a service level agreement from the lawyers of how the data is used would be an extra step of protection. I think that would be reassuring for me." Participant, Scotland, Wales & Northern Ireland group

Prevention of hacking, theft and fraud

For some participants, protecting users' data is not front of mind for digital identity services providers. They believe that the profit motive is a barrier to putting users' interests first. They wonder what can be embedded in the trust framework to change this, to guarantee that providers will do everything they can to help users feel safe about the data held within digital identity systems. For these participants data security lies at the heart of a trusted digital identity service, but they fear for service providers it is currently not a priority.

> "This highlights my issue about data security with digital identity service providers. I have little trust that they really care about our data. When the end goal is generating income, I feel that organisations will always put profit over and above security of our data." Participant Recollective – online digital identity journal

They expect the framework to ensure that digital identity service providers:

- Monitor the effectiveness of their systems and address any issues before they

become a problem for users
- Employ all available methods for testing their systems. Several participants suggested employing 'ethical hackers' - people who can try their hardest to find every way in which the system could be hacked so that service providers can mitigate against the risks

  "It's like putting the hacker's head on your shoulders isn't it? Because you need to understand the extent of the potential damage to then understand how you can rectify that." Participant, England group

- Ensure that service providers have a data security plan, policy or strategy which is adopted by all staff and is clearly communicated to users.

For service providers to have a plan for when things go wrong is important to participants and critical for a trusted system. Participants are realistic. They do not expect digital identity services to provide a system which is 100% guaranteed to protect against theft or fraud, but they do expect to see a clear statement on what service providers will do when things go wrong. In addition, participants expect there to be compensation and other measures in place which recognise the harm caused to individuals if there is a data breach, or data is lost, stolen or hacked. They also call for:

- A system for individuals to block their own accounts if they feel their data is at risk, e.g. in the case of someone experiencing coercive control, or if a phone is lost or stolen
- Companies to act with transparency, to tell users if there has been a data breach, or any other event which could put their digital identity data at risk
- Support provided to users whose data has been compromised, support from a trained member of staff who can guide the user on next steps to protect themselves and aim to reclaim their identity data
- Guidance and advice for users so that they can take steps to protect their data – but without putting too much responsibility on users to protect data within the system
- Guidance on what the service provider is responsible for and what steps they will take in each potential circumstance.

  "What I have been informed (by HooYu, during a workshop) is that my data (when I use the service provided by HooYu) will not be stored in a database. It will be on my device. And this indicates that I am responsible for protecting my own device and account. So what I feel is that the providers bypass a big share of the responsibility." Participant, Scotland, Wales & Northern Ireland

How and where data is stored

How and where data is stored is important to participants as a consideration for protection against hacking, theft and data loss. The fact that there isn't a common system for data storage: some use of databases, some use of cloud storage (in the UK and internationally), was confusing for many dialogue participants and contributed to a sense of unease. Participants could not identify anywhere in the trust framework which sets the standards for data storage, but they hope that the next iteration of the framework provides more consistent rules on this subject.

"The thing about the fraud is that there is nothing in the trust framework of

> where the data will be stored. (I think) it should be stored in UK clouds because (I understand that if) data is stored in international clouds, the chance of fraud is immediately heightened, because of the way servers are maintained." Participant, England group

Concerns about the diversity of data storage mechanisms and places gave a sense to participants that their data is 'everywhere', distributed across storage systems with little regard to the protections needed. They expect that this will change and assurances given by service providers on what measures are in place.

Expectations also focus on making sure that how data is stored, even if this changes over time, comes with due consideration for short, medium and long-term protections for their data. A user may consider that they trust a service provider with the information they have been given when they signed up, but five or ten years later they may feel differently. Having assurances that service providers have given thought to the longer-term security of data storage and use is an important participant expectation.

> "There might be short term benefits. But if I can't trust them to give me long term protection I'm not going anywhere near it." Participant, Scotland, Wales & Northern Ireland

5.2 A trustworthy corporate culture

Participants expect that a trustworthy system will include within it organisations with a trustworthy corporate culture. They characterise this as one which is inclusive and does not only recognise people with easy access to verifiable identity documentation.

Participants also want to know that service providers invest in their staff, train them properly, employ people with trusted skills and experience and create a working culture which is inclusive, supportive and meets clear values and expectations. For some, trustworthiness of an organisation is closely related to how they treat their employees. Participants feel there is a risk to data and the system as a whole if this is not articulated effectively as a trust framework rule and service providers are monitored for their compliance with the rule.

> Training of staff needs to be monitored to make sure it is robust on things like GDPR. OfDIA should surely have a role in making sure service providers have the funds and the commitment to employ trained, experienced, good staff." Participant, Scotland, Wales & Northern Ireland group

OfDIA, participants believe, should be working with government and through the trust framework to articulate the employment, training and skills development standards they expect digital identity service providers to have in place.

A human-centred approach to complaints and customer service

In thinking about corporate culture, participants repeatedly returned to how digital identity service providers handle complaints and give redress, for example, in the case of identity theft and fraud. In reviewing section 15.3 of the trust framework participants were pleased to see the inclusion of a rule about responding to

complaints and disputes[10]. They want to know that rule is specific and detailed. They feel that the framework needs to set out quite clearly model complaints and redress procedures.

> "For something as important as our identities we have to have that ability to point to something which says, 'you are responsible, you are going to fix it'." Participant, England group

Participants state that a clear complaints procedure would increase confidence in individual service providers, and the overall system. They ask for transparency about how the process would work in practice, and a statement in the trust framework on what is expected including:

- What should happen when things go wrong in a range of scenarios expressed in a visual format such as a flow chart or decision tree
- Each company having a dedicated complaints resource – a named team or department with contact details made obvious and clear
- What to expect in terms of speed of resolving issues and complaints
- How companies ensure that complaints are really heard, not just registered, and action is taken
- That the system is responsive and listens and responds to people's needs.

Participants want the trust framework to ensure that services cannot automate their complaints process with a Chatbot or equivalent tool. They want to be assured that a 'real person' will address the issue they have. This is particularly the case in a hacking, fraud or theft issue.

> "I heard on the news about generative AI today and the possibilities that is allowing. I am increasingly concerned that the penchant for non-human contact based services will mean that mistakes will never be sorted out. Because there is not a trained, sympathetic, understanding human being at the other end." Participant, Recollective – online digital identity journal

This human-centred approach is requested throughout the system, not just for complaints. Participants describe someone who is not used to technology or unfamiliar with apps, someone who is older. People referred to their parents or others that they care for who they help to use technology now. They said that these people would need help and support to use digital identity services and that support should come from a trained member of staff, not an automated system.

This points to a broader, more philosophical point that is a thread throughout the dialogue. Participants are concerned that digital identity service providers will be more focused on the technical aspects of the service, than they are with developing a service that will take care of users and provide them with the support they need to use the service, and to ensure their data is safe and secure. Participants believe their confidence and trust in services will develop and increase if they see evidence, through the trust framework and in the actions of service providers, that they support people and put user needs and experiences at the centre of service design and delivery.

[10] Trust framework section 15.3

> “I think it’s really important that there are people to help people. People to talk it through. You always need a human element to this.” Participant, England group

5.3 Effective communications and transparency

An expectation for the future of digital identity services is that people across society become more aware of digital identity services than they currently are.

What a digital identity / digital identity service is

Participants highlight the importance of making it clear to society exactly what a digital identity is, given many people will be unfamiliar with the concept, and what types of identity it includes.

> “I think people are misunderstanding what digital identity really, truly means. Maybe because information about what digital identity is not clear. I think there needs to be a better understanding of what it means” Participant, England group

Some participants express the view that they were previously unaware that digital identity services exist before engaging in this public dialogue. They believe there is a need for information to be provided regarding the different digital identity services and products that are available, as well as how these services can be used by the public.

The rationale for digital identity services

Participants argue that it is important to clearly articulate the reasons why people might choose digital identity services over traditional identity verification techniques. Some reflect that people may be hesitant to use digital identity services because they:

- Believe the current system functions adequately
- May not be familiar with issues associated with physical identity proof
- May be apprehensive about using new technologies.

They emphasise the need to explain to the public what the rationale is for offering digital identity services and the problems they aim to address.

> “Whenever these services are coming up, the issues must be explained. Like what problem are we tackling? So there should be a background and a rationale.” Participant, Scotland, Wales & Northern Ireland group

How to set up a digital identity account

A few participants call for clear and simple instructions on how to get a digital identity account. At this stage, people will need to be informed how much the service will cost. Some participants call for digital identity services to be free or provided to the public at very low cost.

> “I'd say, clear instructions on how to do it first. How do you start off and get your digital identity in place?” Participant, Scotland, Wales & Northern Ireland group

Other information about digital identity service providers

Participants talk about a range of things people will need to know about digital identity service providers and how they operate. This includes information on:

- Which companies provide digital identity services/ hold digital identity data
- The measures in place to protect people's data
- What digital identity services providers can and cannot do with sensitive and personal data.

Participants expect digital identity service providers to live up to expectations for inclusivity and reflect this commitment in the services that they provide.

> "Diversity and inclusivity have become such hollow words. We need to see (inclusion) lived out properly." Participant, Scotland, Wales & Northern Ireland group

They argue that companies that genuinely are doing something about diversity and inclusion should publish information and statistics that evidence the diversity of their users, their workforce, and initiatives they are rolling out to be inclusive.

How to protect your identity

Some participants talk of the importance of providing general guidelines for the public on how to protect their data. They see this as particularly important for those who are inexperienced in the digital sphere.

> "Like educating the general public, how you have to look after your digital identity. Don't fall for scams or like phishing attacks, scams, not just click on any link that comes in your email or on your phone. Make sure you're checking the link, need to educate people. So I guess that comes under awareness and education." Participant, England group

They reflect that many people are still unaware of how to protect their digital data and how accessible an individual's digital footprint is when people use social media for example.

5.4 Solutions for transparency and communications

Transparency

Participants in the dialogue frequently put 'trust' and 'transparency' together in the same sentence, they see one being contingent upon the other.

> "Trust is transparency as well. It's sort of this mission statement and that ethos. Transparency is so important. It means when we see their books we can see if they match up to their core ethos." Participant, England group

Service providers acting with transparency will publish key information about their work, according to participants. It is suggested that expectations of this published information should be set out clearly in the trust framework. Participants did not prioritise these transparency actions, they are set out below in alphabetical order so as not to indicate a hierarchy.

- Evidence on who has been supported to use the service
- Evidence on who within society has been supported to gain a digital identity

- Honesty around the potential for harmful events such as data breaches
- Measures in place to protect people's data
- No hidden information e.g., material which is published, but hidden away within websites
- Published agreements on working with companies and organisations in the ecosystem to ensure mutual recognition of digital identities
- Published complaints processes with information on the time it takes to deal with complaints
- Published security policies and plans
- Published statements on how the company is funded, umbrella systems, who its principal investors are, who its main stakeholders are, and who is on the leadership team
- Published statements on what will happen if things go wrong including clarity on who would 'own' which challenge/ problem and how they manage risk
- Published values and ethos statements, including a commitment to 'honest' communications
- Show who within government they have spoken to and why – to avoid the accusation of having lobbied or undermined procurement regulations.

Participants want to see clear terms and conditions written in Plain English. Short sentences and visual guidance are key to this. People need to understand what they are signing up for in a way that is engaging and clear.

> "They give you a long list of terms and conditions and you can't really understand it. It's so wordy. You need a lawyer to read things for you. And you willingly sign up to it. You assume that using this many words must mean you can trust them with your data. But a lot of the time you are trusting an organisation to do the right thing without necessarily being 100% sure. You haven't really checked." Participant, Scotland, Wales & Northern Ireland group

Participants want to ensure that there is clarity of information throughout this process. This means government and OfDIA setting out very specific and detailed rules in the trust framework and digital identity service providers being very specific and clear about how they are abiding by those rules.

> "I think for a lot of us here is a certain level of distrust when it comes to the government and digital data. We've heard too many stories about data being used in ways we weren't informed of or didn't consent to. If the government wants us to trust them with something as personal as our identities, they're going to need to be crystal clear about how they're using that data, who has access to it, and how they're protecting it." Participant, Recollective – online digital identity journal

A public awareness campaign

Participants propose a public awareness campaign to raise awareness across society of what digital identity services are and what they offer. There is an expectation that service providers should tailor communications to different audiences to help to build trust amongst different communities.

> "There are people of different age groups, like people coming from different parts of life. And not everybody has the same understanding about digital

> identity…Many people [are] not very comfortable using their devices, or online services. So I believe an awareness programme is very important." Participant, England group

Some participants explain that they believe an awareness raising campaign will help to mitigate suspicions around service provider motivations.

> "Because if there isn't a big campaign about it people will be really suspicious about this. I think a campaign might help avoid some of that." Participant, Scotland, Wales & Northern Ireland group

Participants suggest using different mediums to reach members of the public. This ranges from 30-minute workshops in community venues such as libraries to advertising on broadcast media.

Clear and accessible communications

Many participants emphasise the importance of accessible and clear communications, given that digital identity services will be used by a diverse range of communities, including those with poor literacy skills. A few participants comment that existing policy papers are full of jargon. They stress that this needs to be avoided. Participants feel that all documentation for a public audience needs to be easy for a layperson, written with someone who has no current knowledge of digital identity services in mind, making the language easy to understand and digest.

> "I think about language, because some people can't read and write in this country, and this could alienate them." Participant, England group

A few participants suggest other ways that information could be presented to make the subject area more accessible. Suggestions include having more of the worked examples within the trust framework to illustrate to the public how digital identity services can be used. This could include visual materials and infographics to show how digital identity services work.

> "A mind map to show all the various aspects [of digital identity services] is needed so that everything is in one place." Participant, England group

Participants suggest a number of principles that should guide communications, such as being honest and authentic in communications about this sensitive and complex topic. We saw clearly in the dialogue that people are mistrustful of communications from digital identity service providers which seem either hyperbolic, inauthentic or dishonest. For example, participants compare this to what they are told by their Internet providers that they offer 'a super-fast connection' when it isn't; or '100% guaranteed connection' when it can't be because you live in a rural area with inadequate connection speeds. Equally participants will be very wary of communications from service providers which state that their data is '100% safe' or 'Will be completely in your control'. They say that service providers should:

- Communicate about digital identity services with empathy and with care
- Treat members of society as equal stakeholders and bring everyone with them
- Address the concerns people have about digital identity services and any misinformation
- Think about the intention behind communications:

> "... the cynical part of me thinks it's just so easy to lie. They need to make the intention behind the communication clear and honest." Participant, England group

There are participants that feel that information about digital identity services is more likely to be trusted if public figures that people trust buy into and promote it.

> "Maybe get somebody like Martin Lewis involved. He's got a high profile… I think a lot of people trust him. And if he buys into it then I think a lot of people (will) take that on board then. It (would be) quite interesting to see his take on it anyway." Participant, England group

Some participants expect communication efforts to consider the varying rates at which members of the public may adopt digital identity services. They explain that this spectrum ranges from individuals who are more likely to be early adopters in the acceptance of new technologies, whilst others will take considerably longer to accept new technologies, waiting for others to test them first.

5.5 Expectations related to trust

During the dialogue, participants were asked to describe experiences, people and/ or organisations that had demonstrated to them that they could be trusted. In this context, people described trusted:

- **Relationships:** a friend or a relative who participant experience has shown can be relied on to treat them with love, respect and care
- **Sectors:** some saying they trust the public sector more than the private sector; others feel their trust in government has been severely undermined in recent years; others speak of health, third and charitable sectors as trusted because they act with empathy, care and altruism
- **People in the media:** such as independent advisers, or broadcasters and commentators who are seen to base their knowledge in evidence and research
- **Private sector organisations:** some mentioned banks, other financial services, or a brand they trust; others spoke of trusting private sector organisations when their values aligned with what they believe in e.g. a policy on the environment, a human-centred approach to service delivery, or ethical working policies for their staff.

> "I guess we want to get to a position of 'institutionalised trust' like we have with the NHS. It's embedded in you, if you were a person of faith you would trust your church. Experience has told you they can be relied on. They act with integrity and honesty." Participant, Scotland, Wales & Northern Ireland group

Many participants discussed their impression that it takes a long time to earn people's trust, but very little time to destroy it.

For a number of participants, this exercise was challenging. They said that they do not trust anyone or any organisation. This was seen in the context of having been 'let down' or 'disappointed' by government, organisations, companies and individuals in their lives. One participant used the experience of Covid-19 to explain the mistrust that they felt:

> “To be honest, during and after Covid, I don't trust any organisations. I am very sceptical these days and find it hard to believe anything is being done ethically.” Participant, Recollective – online digital identity journal

Participants used the words ‘cynical’ and ‘sceptical’ throughout the dialogue in relation to being able to trust systems and services. Some state they are generally suspicious of private sector motivations in providing services which use their personal data. They feel that there is an ulterior motive for the work.

For many, trust is dependent on knowing an organisation or an individual over years. This means that each party in the relationship knows what is expected of them, and their words and actions live up to those expectations. This led some participants to say that they would find it very difficult to trust an organisation, or those overseeing it, with their data given that they do not have these relationships with digital identity organisations.

> “How am I supposed to verify whether or not these organisations are deceitful and incompetent if I don't know them?” Participant Scotland, Wales & Northern Ireland group

Many also say that they trust organisations that they research, that have a good reputation and/ or who have good reviews from others whether online or via word of mouth from the people in their network. Knowing that the sector is well regulated, and the oversight of the system is robust and well developed is also essential for many when describing what creates a trusted system. We share more findings on what trusted oversight looks like in the next chapter.

5.6 Principles of trust

Deliberation on trust and trustworthiness reveals a series of ‘principles of trust’ which participants feel should guide the work of digital identity services. These principles are:

Act with **transparency**, using clear communications and with the expectation of openness in all relationships.

Define, and act within, high **ethical standards** meeting expectations for what good looks like. Look after users’ data, protect them from harm, protect the vulnerable in society from harm and bring them into an inclusive system.

Be **reliable** and **proactive**: say what you are going to do, do it, and tell people that you have done it. This extends to handling complaints and being responsive and supportive to those who need guidance to use the technology.

Be **genuine, authentic and human**: show that service providers care, they are empathetic, and put people at the heart of the service. This includes using clear and honest communications not hyperbolic advertising which over-promise.

Secure the data: data shared with digital identity service providers should not be shared with third parties without express permission being given by the user.

Put **safety** first. Do nothing to harm people or knowingly put them at risk and have safeguards in place for when things do go wrong.

Demonstrate that **public benefit** comes before financial motivations.

Of these, 'transparency' was the principle that came to the fore as highly significant for trusted relationships.

> "We've got to have a very transparent business model to allow us to see that it's a trustworthy system." Participant, Scotland, Wales & Northern Ireland group

6. Proposals for effective oversight

Summary findings

In this chapter we set out what participants expect from the oversight of the system. We explore the role of government as being one of **policy development and big picture oversight** working with the independent OfDIA. Government's role is seen as being to **bring consistency to the system through the trust framework rules and establishing the requirements for certification.**

Participants also see a role for government in laying out a **clear roadmap for designing and delivering digital identity services, setting out the ambitions for the programme**, as the framework currently does, but also giving **detailed plans for an implementation timetable, for review, for monitoring and oversight**.

Some participants suggest a role beyond oversight. **They propose that a government department, working with academia or another public sector body could take responsibility for delivering the services**. These participants articulate **a 'trust tension': whilst they do not trust government, they feel that a public sector organisation, a non-profit organisation or a research consortium might be more trustworthy than private sector organisations**. This is seen as more trustworthy as it would operate without vested interests or the need to satisfy company shareholders.

The chapter also sets out what participants' perceive as OfDIA's role in providing independent oversight for digital identity services and providers. They consider it **vital that OfDIA is independent of government and service providers whilst working closely with both**. They want to know that OfDIA, collaborating with government and service providers will:

- Act with transparency
- Have and communicate the safeguards in place
- Be accountable and demonstrate that they will take responsibility for what could go wrong.

Involving the public is a role participants expect OfDIA to take. They say that **people across society need to know that they are stakeholders in this programme**. As such **they should be involved in the decision making which informs its development and implementation**.

Many participants became very committed to the proposal that the system, from providers delivering services to government and OfDIA providing oversight, could be **co-designed by those who have experienced barriers to proving an identity or an attribute.** Such co-design could **include working with software designers to build the apps; testing the technologies; piloting, testing, consultation and developing communication tools.**

6.1 Government's role

Participants expect government to work in a similar way with OfDIA as it does with the Information Commissioner's Office (ICO) or the Financial Conduct Authority (FCA). They feel in both those scenarios government and the independent authority are working together to oversee the work of a number of private sector organisations.

> "This is almost like the way it is with the Financial Conduct Authority. The government's role in that is that you have all these different banks, but you have to be certified by the Financial Conduct Authority to say you're complying with certain things so that you know that you can trust these banks with your information. I feel like this would be a similar exercise" Participant, England group

For some, the number of private sector companies involved is a problem and a challenge for developing trust in the system and ensuring effective oversight. There is a concern that with over 40 companies in the system it will be hard for individuals to differentiate between the different services on offer. As a result, they call for consistency in approach, set out in the trust framework rules and the certification process, with independent oversight.

> "There has to be consistency, doesn't there? If there's going to be more than one organisation doing digital identities, they all have to have a consistent approach, the same level of information stored, and the same protection mechanisms." Participant, Scotland, Wales & Northern Ireland group

Participants suggest that setting this consistent approach is the role of government, through requirements for certification and establishing the rules within the trust framework. They see the role of verifying that a consistent approach is carried out in line with the trust framework rules is the role of the oversight body OfDIA.

For some participants, how the relationship between government and a body for independent oversight works is not the important consideration. What matters is that there is oversight, there is regulation and there are clear rules through which digital identity services will operate.

Some participants differentiate the responsible department, DSIT, from government more broadly. Given they perceive that trust in government is low, they feel the focus should be on DSIT as the trusted organisation. They understood that DSIT have commissioned, observed and listened to what people have to say in this dialogue. As a result, they feel DSIT can be trusted to provide oversight for digital identity services informed with this knowledge.

> "The Department for Science, Innovation and Technology is the very specific department in charge of this kind of topic. If they are part of the oversight it will definitely be a relief. They've been demonstrably listening, so I thought at the beginning this might be all basically lip service. But I don't think so, they're taking things on board." Participant, Scotland, Wales & Northern Ireland group

Many participants see the role of government as being to lay out a very clear roadmap for designing and delivering digital identity services. They see this as something which sets out the aims and ambitions of the programme, as the trust

framework currently does, but also sets out detailed plans for an implementation timetable, for review, for monitoring and oversight, and for communications around delivery of the roadmap to wider society.

A further role for government?

Some participants wonder if there is a role for government beyond oversight, particularly in the group from England. This is because they question whether it is right that private sector organisations are entrusted with delivering digital identity services. They reflect that it might be more appropriate for a government department such as DSIT or a public sector body to take responsibility for delivering the services. For these participants, there is a 'trust tension'. Many do not trust government or the political system, but they feel that a public sector organisation, a non-profit organisation or research consortium, might be more trustworthy than private sector organisations to deliver services which will hold data related to their identity. They feel that their data might be safer, and less at risk of being sold on or shared inappropriately, if the services are run within a public sector, or an academic, context. Some describe this tension as related to decisions about how other services are run which they do not feel have worked, and have not, in their view, led to a trusted system.

> "My concern is that the UK's government is ideologically attached to using private companies, no matter what, which has led us to so many problems with our infrastructure – water, gas, electricity, railways, Covid tests etc. These decisions have not been good for us as a population, and the private firms are the only ones to benefit." Participant, Recollective – online digital identity journal

> "Nobody trusts the government. But I do think they are the ones that should be running this rather than giving it out to digital companies. I use the HMRC for tax and I was ok to do their identity checks. I felt safe. But you don't know who is behind the private sector companies and how they are going to make money." Participant, Scotland, Wales & Northern Ireland group

For some participants, therefore, the solution is to contract a government funded academic consortium to develop and deliver digital identity services. They consider this a better solution because they have no shareholders to satisfy and no vested interest in the outcome. Others are clear that they wish a government department to run the service just as the Passport Office or DVLA issue and renew passports and driving licences. A few participants in both groups proposed a merger of these bodies to deliver digital identity services. The point comes back to trust, whilst trust in government is low, trust in government sponsored bodies is higher and perceived as more trustworthy than private sector organisations.

> Whilst I'm sceptical of government and their motives, I'd still be 100% more trusting of a government body set up to do this rather than the private sector. When I set up my HMRC online account, it was a faff, but I trusted it more than when I applied for age checking through one of these companies." Participant, Scotland, Wales & Northern Ireland group

This view was not shared by everyone, and other participants are not concerned about private sector involvement as long as the trust framework is clear in the standards it expects, the rules it applies, and the oversight is robust.

6.2 OfDIA's role

Independence

For many participants the involvement of an independent body to oversee digital identity services is an essential part of creating a trusted system. Without this independence they believe the programme is unlikely to succeed with its ambitions for trust.

> "I think there's got to be a standalone, an independent ombudsman. This is where we as the general public would have at least someone or an organisation to go to. Someone the public can trust that's independent of the government. Someone that can police this, because it must be policed."
> Participant, Scotland, Wales & Northern Ireland group

Having independent oversight is also seen as important consistency for the programme, particularly when governments change. However, OfDIA's main role in participants' eyes is to closely monitor the design, development and implementation of digital identity services and the extent to which they are keeping the trust framework rules. They list key roles for OfDIA as both supporting service providers to deliver their best work and sanction them when they do not meet expectations. They list their expectations for OfDIA's role as:

- Working with government to refine and improve the trust framework rules, making them as specific as possible and providing guidance, signposting and sharing access to technological and ethical standards to support the work of service providers
- Reviewing, monitoring and auditing how service providers are implementing the trust framework
- Learning from international examples of using identity services and embedding good practice from that learning into how service providers operate
- Creating templates for key working documents such as an inclusion strategy
- Providing a system for understanding public expectations on an ongoing basis to make sure the needs of individuals and wider society are met
- Employing strong and stringent sanctions when things go wrong, including withdrawal of certification or accreditation, substantial fines (fines which would have an impact on the business), and action to prevent a service provider from operating in the system if they persistently break trust framework rules
- Involving the public in decision making about the detail within the trust framework and monitoring its implementation.

6.3 A joint approach

Given participants' focus on good communications and the high priority they place on transparency, they believe there are a number of steps DSIT and OfDIA can take to be recognised as the trusted overseers for this sensitive and valued data, and equally that digital identity service providers can adhere to.

1. Act with transparency – the key to trustworthiness

Participants stress that transparency is a prerequisite of trustworthiness. Proposals for making the work more transparent include:

- Embed more detail, templates, models and guidance within the trust framework rules, to make it explicit what, for example, an inclusive approach to digital identity looks like
- Publish a version of the rules which is for users of digital identity services, a visual, Plain English and clear summary of what the rules are and how service providers will be monitored to adhere to them
- Showcase examples of best practice in the system as a model for others to follow.

2. Having, and communicating, the safeguards in place

Being very clear about the safeguards in place for the principle of putting safety first was felt to be an essential demonstration of trustworthiness. When discussing this, participants emphasised the importance of:

- Checking, evaluating and communicating data security standards
- Conducting and communicating informed consent with clear statements on which relying parties will have access to data and why
- Include in the consent statements information on when data may be shared with other third parties and why, so that users can decide where they feel it is appropriate to share their data and where not
- Establishing guidance for service providers on what should be done if there is a data breach, a hack or something goes wrong with the technology or the infrastructure around it
- Communicating with all those concerned when something does go wrong and making sure there is effective redress for those who are harmed by the event.

3. Accountability

Participants want to know that all parties will act responsibly and take responsibility for the decisions made now and in the future about the programme. If all stakeholders demonstrate that they are accountable for what happens in the programme it is more likely to be trusted.

> “This is very new to me. I haven't thought about it much before. Everything I'm learning feels very reassuring though. It's been nice to see that regulatory bodies are going to be used well. We can see they will be accountable for what happens.” Participant, Recollective – online digital identity journal

Participants characterise accountability as first and foremost making the rules as clear as possible to ensure that they can be met. They believe that while the system needs to be flexible, to encompass the different ways in which service providers might deliver their services, the rules need to be fixed, clear and specific so that there is no ambiguity in what services providers should do to abide by them.

> “Whilst I think the system needs to be flexible, I think the rules need to be very inflexible, I think they need to be very specific, and they need to not leave margins for people. They need to be very clear cut. There needs to be clear accountability that resides with one organisation overseeing all 40 providers.” Participant, England group

They also list the following as essential routes to accountability:

- Having robust policies in place for oversight

- Evaluating and monitoring service providers to verify they are working within the rules in practice
- Publishing reports which share how effective service providers have been in relation to inclusion, data protection, responses when things go wrong
- A tracking system for the data held by digital identity service providers in case things change substantially for the company, for example if they are sold, bought out, or cease trading, to ensure data isn't lost, or users harmed, at these points of transition.

> "A system of accountability that actually goes with the company. So if X company is sold to Y company then they abide by X company's rules. It will help us secure our data." Participant, Scotland, Wales & Northern Ireland

Many participants believe that the government's proposed approach could make it harder to demonstrate accountability by spreading responsibility between a number of different companies involved in the sector as well as government. For a few participants this also suggests a deliberate plan to avoid responsibility for how the system develops.

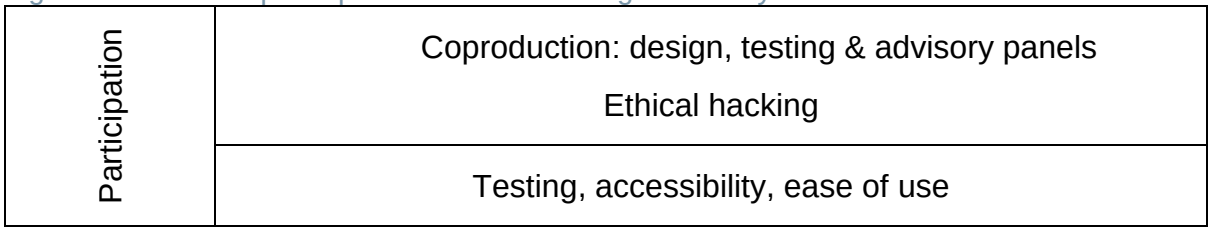
> "The government's trying to get less accountability and they're saying, 'we don't want any part of this, because of all the complications that come with it'. So they outsource it to the private sector so that when the private sectors mess up they can say, 'Well it didn't come from the government, it's not our fault.' Participant, England group

6.4 Involving the public

Participants see a vital role for OfDIA in ensuring the involvement of the public on an ongoing basis for a range of actions in the digital identity programme.

Participants in the dialogue believe that to gain trust people across society need to know that they are stakeholders in this programme. As such they should be involved in the decision making which informs its development and implementation. The proposals made for such involvement ranges from significant in depth co-production activities and advisory panels; testing software and systems; and being kept aware and informed of developments. We draw the suggestions made on involving the public in this process together in figure 4. It works in a similar way to Arnstein's ladder of citizen participation[11], with lighter touch engagement activities on the bottom rungs of the ladder, and equal power relationships with depth involvement at the top of the ladder.

Figure 4: Ladder of participation in relation to digital identity services



[11] Arnstein, S. (1969.) A ladder of citizen participation. Journal of the American Planning Association, 35(4), 216–224

	Engagement
	Being kept informed
Information	Targeted awareness raising activities
	General societal awareness raising
	General societal communications

Many participants became very committed to the proposal that the system could be co-designed by those who have experienced the barriers to proving an identity or an attribute. They thought this could be achieved by:

- Including the elderly, and those who are not at all confident with technology, in the testing of the technologies used by the digital identity service providers, including future testing
- Involve disabled people and neurodivergent people in the building of the apps and the development of the technology

  "It's relevant at this point in the dialogue to share that I am ADHD and autistic. When it comes to documents I struggle massively. Anything in terms of accessibility needs to be led by people who are autistic, who have ADHD, who have learning disabilities. We have to talk to the most vulnerable people to get them to actually build things that they can use. People like me could help design it to make it work for us." Participant, England group

- Including in the framework a requirement that digital identity service providers should involve those who are aware of the issues and the challenges in consultation on, testing and development of the systems being used
- Having a pilot phase for all new digital identity services to test whether the service is accessible, easy to use and inclusive of those with vulnerable IDs.

  "We the public need as a diverse body of people, however that's brought together, to sit on decision making and testing panels. We (should be) actively involved in (ongoing dialogue) and future sandboxes, in the development of the product, and testing it, and bringing it out. And all those things, not just one off giving of views which may or not shape what happens next. It should be ongoing." Participant, Scotland, Wales & Northern Ireland group

7. Conclusion: routes to trust

Summary findings

In this final chapter we summarise the key findings around trust in digital identity services and conclude our findings. We highlight the key points participants believe would ensure digital identity systems can be trusted. They want to be reassured that service providers will work within the rules and operate with a human centred approach which considers the ethical dimensions of the programme.

We begin with specific amendments proposed to the trust framework. These cover points on:

- The benefits of digital identity services
- Embedding simplicity in the trust framework
- The importance to participants of having control over their data
- A rigorous, effective and human centred complaints procedure
- Future proofing digital identity services
- Ensuring there are protections against system over-reach
- The importance of inclusion

The chapter ends with key findings on how trust in digital identity services is established based on five factors:

1. Trust in digital identity services cannot be seen in isolation
2. The importance of the data
3. Benefits to society
4. Accountability and transparency
5. Accessibility, agency and involvement

7.1 Amendments to the trust framework

Throughout this report we have noted where participants feel that amendments or enhancements to the trust framework could be made. In table 3 we collate these points.

Table 3: Proposed amendments/ enhancements to the trust framework

Framework rule/ area	Proposed change or addition to the rules
Benefits	Participants call for the benefits articulated in the framework to be clearly set out. The means going beyond convenience and efficiency to also include benefits such as: • A simplification of identity/ attribute verification processes • Having guaranteed control over their data

	• Offering a system of verification for people who do not have identity documents e.g. as they've experienced homelessness, have recently left prison or have been unable to afford to get or renew a passport/ driving licence.
Simplicity	The trust framework already includes assurances that providers will collect, store and use the minimum data necessary in order to deliver effective digital identity services. Participants welcome this. Keeping things as simple as possible is seen as an effective means for keeping control of the essential data needed for trust in digital identity services to be achieved. Participants suggest creating a simple template version of the terms and conditions applied to using digital identity services. In doing so it is hoped that people will take the time to read them and understand what happens to their data and how potential risks are mitigated.
Control of my data	Participants believe the trust framework should provide a clear statement on how users 'own' and 'control' their data. Factors which participants feel are important in relation to this control (some of which are already included in the framework) are being able to: • Update and correct data about themselves as and when they need to e.g. if they have new information on a credit score, or if they no longer identify with their birth gender • Exercise their right to be forgotten, with swift responses from digital identity service providers when such a request has been made • Protect personal information that they don't wish to share e.g. specific details within medical or criminal records unless completely relevant and specific • Ensure privacy for views, opinions and protected characteristics e.g. political views, marital status, gender identity, ethnicity, disability – all as protected under the Equality Act 2010[12] • Verify that there really is a need for data to be checked, stored and shared for the purposes of digital identity including putting limits on the amount of data that can be collected for the purpose of identity/ attribute verification • Have choice about data can be shared with, and why, within the digital identity services trust framework • Make sure family members can remove the data of a family member who has died.
Complaints	There is strong feeling amongst participants that the trust

[12] https://www.gov.uk/discrimination-your-rights

procedure	framework needs to be explicit about what is expected of service providers in relation to their complaints procedures. They suggest templates should be included in the trust framework to cover in detail: • Restrictions on the automation of the complaints process, participants do not want to share their complaint with a Chatbot or equivalent tool, they want to be assured that a real person will address the issue they have • What should happen when things go wrong in a range of scenarios expressed in a visual format such as a flow chart or decision tree • The need for a dedicated complaints resource – a named team or department with contact details made obvious and clear • What to expect in terms of speed of resolving issues and complaints • How companies ensure that complaints are really heard (not just registered) and action is taken • That the system is responsive and listens to people's needs across the system.
Future proofing digital identity services and provision	Demonstrating within the trust framework that consideration has been given to future proofing both service provision and its oversight. This includes ensuring that: • There are protections against making the system mandatory either by design or default in the future • Changes in business practice do not undermine trust that is built in the system • The digital identity system is secure from shifts in government, policy and changes in the social and economic landscape • Government thinks ahead so that legislation, the rules, policy and practice keep up with the pace of technological advances.
A redline: system over-reach	Participants want the trust framework to give assurances that the data (now and in the future) can only be used for the purposes of verifying identity and nothing else.
Inclusion	Participants like the examples given in the trust framework on inclusion, e.g., who might be excluded if they do not have appropriate technology, or are not confident in using the service, but consider that there could be more examples and more detail to ensure this section is specific enough and does not leave this important aspect of trust to chance. They also feel the section should include more than rules on monitoring and allowing the user to retake an identity or attributes check. More information, for example, could be included on how to

	make the service accessible, and measures to ensure the technology works for everyone in society, whatever their circumstances.

7.2 Key factors for trustworthy digital identity services

Trustworthy digital identity services are characterised by participants under five key factors.

1. Trust in digital identity service cannot be seen in isolation

Participants contextualise their views on trust within broader considerations of trust in government and business. They draw in their examples of how government and others have managed challenging social, economic and political situations such as exiting the European Union (Brexit), the Covid-19 pandemic and the cost of living crisis. Trust in this context is a challenging and complex issue to discuss.

2. Taking care of digital identity service users

The data collected, used, stored and shared by digital identity service providers is significant. Participants perceive it to be an articulation of being human and a demonstration that they have a recognised role in society. Participants believe the importance of identity data is not simply practical but also instrumental in people having control over their lives and life chances. It is not just a means of demonstrating, for example, their age or where they live.

This has ethical implications and means participants expect trusted digital identity service providers to think beyond getting the technology right, to the needs of those who use digital identity services. They want to know that service providers will look after them and their data; protect and support the vulnerable and disadvantaged in society so that they too can accrue benefits from digital identity services.

3. Benefits to society

This leads to the second key factor. Participants want to know that digital identity service providers are motivated by more than generating income. They call for the trust framework to make it clear that public benefit is a core value for those being certified to deliver digital identity services, and the government and OfDIA as overseers of the programme. In this context, convenience on its own is not seen as a strong enough benefit. Delivering services which provide a trusted resource which can be used interchangeably across services and in a range of contexts is more powerful.

To demonstrate to people across society that this public benefit value is being upheld, participants want to ensure that the trust framework is published in ways which will be visible and accessible to them. They describe a visual, Plain English document around which a public awareness campaign can be built to promote the public benefit aspects of digital identity services.

In articulating the benefits to society, some participants feel that DSIT, OfDIA and a consortium of academic and third sector organisations, are better placed to communicate the benefits of digital identity services than individual digital identity service providers. They feel this group is less likely to over-promise or use hyperbolic language in such communications. They believe this would mitigate the risk of a

large number of service providers being part of the delivery system. They see 40 service providers as a risk to accountability, transparency and potentially confusing for service users.

Participants do not see convenience on its own as a compelling enough reason for increased use of digital identities. They want to know how digital identity services are going to benefit society by making proving identity more inclusive.

4. Accountability and transparency

Participants place accountability and transparency at the core of trustworthy digital identity services. To enable this, they call for a clear route map in the trust framework outlining actions to take now to minimise long term risks. They argue for longer term assurances, articulated in the trust framework, that their data will be held carefully and protected. Participants feel that the system of oversight through government and OfDIA should make it clear who is responsible for when things go wrong and what recourse users have when it does. Being accountable, honest and transparent throughout the digital identity services ecosystem is vital for building and retaining trust.

Transparency should include recognition of participants' concerns that the use of digital identity services will become mandatory over time, with assurances that measures are in place to enable people to use alternatives. For participants, trust is not about services being 100% robust or 'guaranteed' trustworthy, but about being 100% transparent in everything all those involved in digital identity services do.

5. Accessibility, agency and involvement

Participants want to know that these services are accessible to those that want and need to use them. Having options that work for everyone is seen as part of an inclusive system, one which enables people to verify their identity or attributes in the way which works for them, whatever their background, level of skills and experience.

Knowing that they have control over their data is important to participants. They want assurances that they have choice about who they share data with and why within the digital identity services ecosystem.

Participants also call for the public voice to be centred in the programme as the primary stakeholder of digital identity services. Participants call for people across society to be involved in all aspects of the design, delivery and ongoing decision making on digital identity services. This includes involving people in the design of digital identity services who have experienced barriers to verifying their identity such as prison leavers, asylum seekers, people who do not have a fixed address and those with experience of coercive control. If those who have been most excluded from society are included in this process it is felt it will be considered as trustworthy.

Next steps

We advise that the dialogue findings are central to policy and strategy work on digital identity services. Policy makers and stakeholders should review the findings to ensure that the trust framework reflects participants' desire for detail, more specific examples, templates and guidance which are:

- Workable and practical for digital identity service providers to implement
- Easy for users of digital identity services to access and understand, enabling

them to see for themselves that trust is being set out in a robust framework.

There has been a lot of qualitative, quantitative, and deliberative research on data generally, limited research has been done on trust in digital identity services. The dialogue has demonstrated to participants that this specific topic is nuanced, complex and has more depth than they originally understood when they began their involvement. As such new questions and tensions emerged which would be valuable to unpack through ongoing public involvement in the ongoing design, development and implementation of digital identity services.

Hopkins Van Mil August 2023

Acknowledgements

Hopkins Van Mil is enormously grateful to participants from across the UK who shared their time and thoughtful reflections as part of this public dialogue. Their commitment to understanding and exploring the topic of digital identities made this the rewarding and insightful process it became.

Particular thanks are due to Oversight Group members, including its Chair Professor Lizzie Coles-Kemp, as well as the stakeholder interviewees and speakers who contributed significantly to our understanding and participants' understanding of salient issues in digital identity. These people are:

- Professor Ana Beduschi, University of Exeter
- Gavin Burton, UK Identity Fraud Advisory
- Professor Lizzie Coles-Kemp, Royal Holloway, University of London
- Anna Colom, Ada Lovelace Institute
- Julie Dawson, Yoti
- Ian Deasha, Information Commissioner's Office
- Professor Mark Elliot, University of Manchester
- Helen Fairfax-Wall, Which?
- Dr Tom Fisher, Privacy International
- Colin Griffiths, Citizens Advice
- Dr Eve Hayes de Kalaf, Institute of Historical Research, University of London
- Hannah Jeffreys, Lloyds Banking Group
- Jonathan Middleton, NayaOne
- Nick Mothershaw, Open Identity Exchange
- Emma Lindley, Women in Identity
- Gareth Narinesingh, Mitek
- Oliver Platt, NayaOne
- Richard Pope, Part Two Digital
- Octavia Reeve, Ada Lovelace Institute
- Liz Ridler, Government Digital Service
- William Sandover, Zamna
- Charlie Harry Smith, Oxford Internet Institute, University of Oxford
- Professor Edgar Whitley, London School of Economics
- Sian Williams, Switchback

We would like to express our gratitude to Gemma, Comfort, Tyrone and Lynton, and Janet and Siôn, who shared their life experiences and reflections on digital identity as part of the project's lived experience interviews. Many thanks also to Dara McClarnon, Jaime Taylor and colleagues at Postcode Films for producing these interviews and the dialogue film.

Finally, we would like to thank Teresa Soter Henriques, Ananya Radhakrishnan, Ellery Shentall, John O'Driscoll and their colleagues at DSIT; Fionnuala Ratcliffe and Diane Beddoes at Sciencewise; Dom McDonald at Navigator Consulting and Louisa Fox at Graphic Science. Their collaboration, guidance and enthusiastic interaction with dialogue participants has been crucial to designing and delivering this project effectively.

Appendix A – Recruitment specification

Client: Department for Science, Innovation and Technology
Study theme: Digital Identity Services and Attributes

1. Aim & objectives:

This public dialogue has been commissioned by the Department for Science, Innovation and Technology (DSIT), and is being delivered in partnership with the UK Research and Innovation (UKRI) programme Sciencewise, which is supporting and co-funding the dialogue.

The dialogue will engage a reflective sample of the UK. Findings from the dialogue will:

- Inform the rules that providers of digital identities must follow in order to become certified against the UK digital identities and attributes trust framework
- Inform the functions, oversight structure and interaction with the public of the governing body for digital identities (the Office for Digital Identities and Attributes - OfDIA).
- Inform planning for public communications initiatives
- Test a new engagement strategy combining a public dialogue and sandbox-style testing with industry.

2. Recruitment summary

This recruitment specification is focused on the recruitment 96 participants reflecting a broad demographic. Our workshops groups will be as follows:

1. 24 people from Northern England
2. 24 people from Southern England
3. 24 people from Wales and Northern Ireland
4. 24 people from Scotland

These groups will broadly reflect the UK population in terms of age, gender, life stage, social grade, household income, geography and ethnicity. We will be gaining informed consent from participants in terms which comply with Data Protection Act 2018 - the UK's implementation of the General Data Protection Regulation (GDPR). Data shared between HVM and Roots Research will be password protected at all times. HVM is registered as a data controller with the Information Commissioner's Office no: Z2969274.

Participants are required to take part in all the activities listed below for which a payment of £400 per participant has been allocated.

Please note support will be provided for participants who need either equipment or data to take part, they will not be excluded for not having access to a laptop, tablet or insecure/ no internet connection.

The following summarises the commitment participants will be making. All events/ workshops are online using Zoom.

Activity	Dates
Main workshops	
Optional tech support session for all participants	4-5pm Tuesday 9th May
Online context webinar for all participants (2 groups running in parallel)	6-8pm Tuesday 9th May
Question review and scoping workshop for Wales/ Northern Ireland & Scotland participants	6-9pm Thursday 11th May
Question review and scoping workshop for Northern and Southern England participants	6-9pm Monday 15h May
Exploratory workshop 1 for Wales/ Northern Ireland & Scotland participants	6-9pm Wednesday 17th May
Exploratory workshop 1 Northern and Southern England participants	6-9pm Thursday 18th May
Exploratory workshop 2 for Wales/ Northern Ireland & Scotland participants	6-9pm Wednesday 24th May
Exploratory workshop 2 Northern and Southern England participants	6-9pm Thursday 25th May
Exploratory workshop 3 for Wales/ Northern Ireland & Scotland participants	6-9pm Wednesday 31st May
Exploratory workshop 3 Northern and Southern England participants	6-9pm Thursday 1st June
Final workshop for Wales/ Northern Ireland & Scotland participants	10am-4pm Saturday 3rd June
Final workshop (part 1) for Northern and Southern England participants	6-9pm Tuesday 6th June
Final workshop (part 2) for Northern and Southern England participants	6-9pm Wednesday 7th June

3. Screener to include:

Criteria for 96 participants	Target – a broad diversity of UK demographics – please work flexibly with these criterial they should be seen as maximum and flexible.
Gender	Appropriately balanced mix of people who identify as male / female / non-binary.

Age	Good age distribution across age groups from every adult life stage from 18 upwards. The sample should be boosted for 18-25 year olds e.g. each group of 24 should have at min. x6 from this age group.
Life stage	A broad range of life stages from students, young professionals, raising young children to empty nesters and those who are retired
Minority ethnic groups	A boosted sample so that for each group of 24 participants a min of 6 participants (e.g. 24 of 96) are from communities experiencing racial inequalities (CERI) above current census data. Asian, Asian British x 1 Black, Black British, Caribbean or African x 2 Mixed or Multiple ethnicities x 2 Other ethnic group x 1
Disabilities/ those with long-term chronic health conditions.	A boosted sample of 10 participants **above current census data** who are disabled/ have chronic illness.
Current working status and type	A range of people who are employed (part-time/ fulltime/ self-employed) and unemployed, plus those who are retired.
Social Grade	Mix of AB (4 participants) C1C2 (8 participants) DE (12 participants) for each group of 24 people
Household income	A balance from across socio-economic groups, but weighted (at least 8 participants in each group of 24 participants) for those in vulnerable financial circumstances.
Geographic location	The group should be drawn from a UK sample. We suggest focusing on communities which have score higher in the indices of multiple deprivation. Each group of should include those from rural and urban/suburban regions.
Sexual orientation	Appropriately balanced mix – boosting above current census data.
Experience of market research/ dialogue	Should not have taken part in a public deliberation/ Citizens' Jury/ Citizens' Assembly or public dialogue in the last **24** months particularly those run by HVM such as WGS for newborn screening; or heath and data use public dialogues for the National Data Guardian; programmes for WWF on land use; and dialogues for Genomics England on researcher access to discovery research.
Perspectives on screening/ data access	**Awareness** 1. I have used a digital service to prove who I am within the last 12 months (e.g. facial recognition to access my banking app) Yes No 2. I have not been able to access a service because I do not have proof of my age or identity in the last 12 months (e.g. using a supermarket checkout) Yes

	No **Attitude** Attitudinal questions should be asked in the screener to understand the range of views we have in the sample. They will not be used as inclusion/ exclusion criteria. 1. Here are some of the ways in which data is collected about you every day. • Store cards/ loyalty cards • Social media platforms such as Facebook or Instagram • Fingerprint or facial recognition to unlock a smart phone Which, if any, do you have concerns about in terms of how the data is collected, stored, and used? 2. On a scale of 1-5 (where 1=extremely concerned and 5=not at all concerned) please state how concerned you are about your data being collected and used for identification purposes. *Fieldworker to probe responses. We are seeking a balance of responses to these data privacy questions within each workshop with 20% of people being extremely concerned, 60% being at a mid-point (having not thought about it or being neither concerned or unconcerned) and 20% being not at all concerned.

Important note: please **do not** recruit friendship pairs or use snowballing techniques.

4. Exclusion criteria

Given the specification of this project, please do **not** recruit people currently or recently (in the past 12 months) working for:

- The Department for Science, Innovation & Technology (DSIT)
- A commercial entity working creating digital identity services

Please contact us to clarify any uncertainties in relation to these criteria.

Appendix B – Stimulus materials

The table below outlines the speakers, their presentation topics and other stimulus materials shared with participants as part of the public dialogue process.

Session	Speakers & Stimulus
Webinar	• 3 animations on identification, attributes and digital identity • Teresa Soter Henriques / Ellery Shentall, DSIT ○ Introducing the UK Digital Identity and Attributes Trust Framework
Question & scope review workshop	• Proving your identity – 'A day in the life' slides • Presentation and review on the dialogue's research questions • Jonathan Middleton / Oliver Platt, NayaOne ○ On interaction with the Sandbox

Exploratory workshop 1	• Professor Edgar Whitley, London School of Economics
	  ○ On the recent history of ID and current landscape
	• Ian Deasha, ICO
	  ○ On the current regulatory framework & ICO response to the trust framework
	• Julie Dawson, Yoti
	  ○ On the role of digital identity services
	• Nick Mothershaw, Open Identity Exchange
	  ○ On trust frameworks and benefits of digital ID
	• Octavia Reeve / Anna Colom, Ada Lovelace Institute
	  ○ On technology & trustworthiness

Exploratory workshop 2	• Lived experience interview #1 – Experience of identity fraud (not available in the public domain)
	• 'Data to Go' – short video by Cifas
	• Gareth Narinesingh, HooYu
	  ○ On the role of digital identity services
	• Gavin Burton, UK Identity Fraud Advisory
	  ○ On identity fraud, prevention and data protection

Exploratory workshop 3	• Lived experience interview #2 – Experience of seeking asylum
	• Lived experience interview #3 – Experience of learning disability & digital exclusion
	• Professor Ana Beduschi, University of Exeter
	  ○ On inclusion and human rights protection
	• Sian Williams, Switchback
	  ○ On inclusion and those with vulnerable IDs
	• Dr Tom Fisher, Privacy International
	  ○ On privacy
	• William Sandover, Zamna
	  ○ On the role of digital ID services for travel

	• Lived experience interview #4 – Experience of criminal justice system and lack of ID documents

Final workshop	• Visual summaries of the trust framework including:
	  ○ Rules for all service providers
	  ○ Rules for identity and attributes service providers

On Recollective (asynchronous activities)	• Jargon buster of key terms in digital identity
	• Charlie Harry Smith, University of Oxford
	  ○ the international context for digital ID
	• Animations
	  ○ What is a digital identity
	  ○ What is an attribute

Appendix C – Process materials

The full set of process materials is available from Hopkins Van Mil on request. Below we share a sample of the process plans used for online workshops.

Excerpt from workshop 1 – scoping and question review – 6-9pm Thursday 11th/ Monday 15th May

Aim & objectives of the dialogue:

The overall aim of the project is to engage a diverse group of the public to inform what further policy is necessary for digital identity services and provision to be trustworthy. Findings from the dialogue will:

- Inform the rules that providers of digital identities must follow in order to become certified against the UK digital identity and attributes trust framework.
- Inform the functions, oversight structure and interaction with the public of the governing body for digital identities (the Office for Digital Identities and Attributes - OfDIA) e.g. complaints structure, advisory functions, support for the public, anti-fraud functions.
- Inform planning for public communications initiatives.
- Test a new engagement strategy combining a public dialogue and sandbox-style testing with industry.

Initial research questions

These will be reviewed by participants in workshop 1 – scoping and questions review - and may change as a result. For now the overarching question is: *What is the government's role in setting system oversight?* The key questions are:

1. What rules should be put on providers regarding user control of data, transparency, privacy and inclusion?
    - What are the red lines of what providers should not be allowed to do with users' data?
    - What does the public expect from the use of biometric technologies in digital identities?
2. What does a digital identity governing body need to have in order to build public trust?
3. What risks does the public see in digital identities?
4. What should the general public know about digital identities?

The dialogue is being held **online using Zoom**. It comprises: • Workshops with two groups of 48 people (England/ Scotland, Wales & Northern Ireland) from 9th May to 7th June • This scoping workshop is the second event in the dialogue	**Team – LF x 1, Facilitators x 8 (including LF), Tech support x 1 for each location.**

• Scotland, Wales & Northern Ireland is held on Thursday 11th May • England is on Monday 15th May	

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
5:15-5:45	Set-up	• Test **link,** and **camera**. • Transfer **host/co-host function** to relevant team members and ensure it is allocated to the right team member(s) for sharing screens. • Change **screen name** to NAME HVM – Facilitator/ Tech Support • Test screen share function for films/ presentations • Check small groups, facilitator allocation	HVM team	PP Slides	Project team set up and ready
5:45-6:00	Participant Check-in	Participants who want to test their learning from the tech-try outs are encouraged to join the zoom session early to check-in and check their video/ mic is working. Open www.menti.com on smart phones/ tab on their computer. Explain about QR code/ link (which will be put in the chat) Participants encouraged to get a pen and paper and have their participant pack with them. Once settled they can mute/ turn video off/ get drinks and snacks before we start promptly at 6pm. Warm chat as people settle in. TS to run a register as people join and change your screen name to **first name** only.	All	Menti.com List of participants	Participants set up and ready
6:00-6:10 (10	Introduction to this workshop	Warm welcome to our second session together, and our first workshop. This will feel different from our webinar. We'll be working more in small groups and have lots more time to interact	HVM	PP Purpose & Agenda Slide	People are clear: Who is in the

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
mins)	and reminders of the overall dialogue programme	with each other and our speakers. The purpose of this workshop is to give you time to review the research questions, think about what matters to you and what you would like to discuss during the dialogue and to prioritise what's important. But first some reminders: 1. HVM team introduce themselves 2. Observers/ speakers present introduce themselves 3. Evaluator to introduce themselves and the evaluation process You'll get a chance to meet each other when we go into small groups Then LF • Reminder of everything in the handbook and where our contact details are • Explains what we'll be doing this evening • Shows visual of the whole programme • Shares visual of all the groups/ numbers involved • Shares the points to help the discussion including reminders about consent (signed during onboarding) • How we work points e.g. facilitation support/ tech support – who to go to when • We'll stay on the call after the workshop if you have any questions you want to ask us	LF using HVM slides	Intro PP LF PP presentation	room and why; who they will be working with What we will be doing together Being clear that this is a participant-led process.

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
		• How/ why we'll capture what is said this evening – we are interested in what you say not who says what, your name will not be linked back to anything we write about in the report • Mention the final report and its purpose			
6:10-6:20 (10 mins)	Menti questions set 1	**Participants asked to get menti.com on their phones/ another tab on their device.** Share the code, the QR code and the link in the chat – as 3 easy ways to get into menti. Reminder no right or wrong here, the questions I'm asking now are about beginning to think about our dialogue topic. LF to share screen with 'hide results' QM1: Share one quick thing about yourself Just a few words with something you feel you can share with us about you, and/ or what you are interested in. Remember we'll be sharing our screen in a minute so make the sentence appropriate. QM2: What comes to your mind now when you think about what you heard at the webinar? LF to share results when more than 12 are in.	LF	Menti.com Tech support to put menti link/ code in the Chat	Getting back in to the space by remembering the webinar Getting to know each other and who we have in the room. Knowledge of digital identities
6:20-6:25 (5 mins)	Short day in the life slides	LF to introduce a short set of 'day in the life' slides – one person's day of proving their identity, showing a variety of situations/ proofs needed.	LF/ TS	In slide deck	A prompt for the next discussion
6:25	TS to move everyone to their pre-allocated small groups – 7 participants per group, based on a mix of demographics, 1 facilitator for each group, tech support available to all groups for immediate Zoom challenges. Facilitation team stay in touch				

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
	via WhatsApp group. Participants supported throughout by the facilitator, also reminded to DM facilitator if anything they wish to ask outside of the group discussion.				
6:25-7:15 (50 mins) 6:25-6:35 (10 mins) 6:35-6:55 (15 mins)	Thinking about verifying your identity A week in the life of your identity	Facilitator to welcome everyone to the group. Note about recording. **RECORDER ON** We asked you before the workshop to find and bring something that you use to verify your identity. Go round the Zoom again, ask participants to share what they have brought and to quickly show it on screen if they feel comfortable doing so, but not so anyone can see details. Let's go round the Zoom, I'll ask you to: **1.** Say hello to the group and where you are zooming in from **2.** Share briefly the thing you use to verify your identity and any points about why it is helpful **3.** Facilitator to start to model the length of the response. **Discussion:** We're going to explore this more now. Think about a typical weekday and all the times you have to prove something (e.g. your age, who you are, that you have registered for a service, that you live at your address) about yourself in order to do something. Let's create a list of why you need to do this. Facilitator to use prompts as necessary: • Have you thought about all the times when you need to prove who you are – on and offline? • Reflections on how you prove who you are, including biometric data e.g. fingerprints, facial recognition	Fs/ Small groups	Facilitator Jamboards for visible note taking/ participants can check & amend what's noted as we go along. List the things people have brought on the Jamboard Note main reasons for using it. Create a list on the Jamboard (images as	Grounding in personal experience of identities. Clarity on the ways in which we do need to prove our identity in various

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
6:55-7:15 (20 mins)		• Reflections on using more than one form of id – a collection of proofs of who you are e.g. opening a bank account needs several proofs of address • Are the times you need to prove something about yourself similar to Evie? Or different? Thinking about attributes, when you reflect on all these ways in which you need to prove something – **Q1. To what extent are some attributes more important than others in different situations, and why?** Facilitator to pick a couple of examples to explore which will explore different situations/ attributes needed e.g. buying alcohol in a supermarket, dating, to access council services e.g. library/ leisure centre, to proving your right to work in the UK. Group to discuss the question. **TS to announce to all groups 3 minutes remaining in small groups at 7:17. Close groups with one minute count down at 7:19. RECORDER OFF**		a prompt) Show 'what is an attribute' on the Jamboard Note down key points made about importance/ Whys. **TS broadcast**	everyday situations. Considering that in some cases you need a bank statement and a utility bill to prove your address. Beginning to think of the understanding of equivalence between in person and digital (picked up again in workshop.

Excerpt from workshop 5 – the rules, governance, trust and summing up – 10am-4pm Saturday 3rd June (Scotland, Wales & Northern Ireland group)[13]

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
9:15-9:45	Set-up	• Test **link,** and **camera**. • Transfer **host/co-host function** to relevant team members and ensure it is allocated to the right team member(s) for sharing screens. • Change **screen name** to NAME HVM – Facilitator/ Tech Support • Test screen share function for films/ presentations • Check small groups, facilitator allocation	HVM team	PP Slides	Project team set up and ready
9:45-10:00	Participant Check-in	Participants who want to test their learning from the tech-try outs are encouraged to join the zoom session early to check-in and check their video/ mic is working. Open www.menti.com on smart phones/ tab on their computer. Explain about QR code/ link (which will be put in the chat) Participants encouraged to get a pen and paper and have their participant pack with them. Once settled they can mute/ turn video off/ get drinks and snacks before we start promptly at 6pm. Warm chat as people settle in.	All	Menti.com List of participants	Participants set up and ready

[13] The same workshop 5 process was followed for the England group but split across two x 3-hour evening sessions on Tuesday 6th and Wednesday 7th June.

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
		TS to run a register as people join and change your screen name to **first name** only.			
10:00-10:10 (10 mins)	Intro this workshop and reminders of the overall dialogue programme	Warm welcome to our sixth session together, this begins our final sessions together, you can think of this as part a, part b is tomorrow evening. In these workshops we will spend more time in our small groups reflecting on what we feel are the opportunities, challenges, redlines, and expectations of trusted digital identity services. But first some reminders: 1. HVM team (re)introduce themselves 2. Observers/ speakers introduce themselves 3. Evaluator to (re)introduce themselves and the evaluation process You'll get a chance to meet each other when we go into small groups LF – to share consistent reminders at beginning of each workshop: • Reminder of everything in the handbook and where our contact details are • Explains what we'll be doing this evening • Shows visual of the whole programme • Shares visual of all the groups/ numbers involved • Shares the points to help the discussion including reminders about consent (signed during onboarding) • How we work points e.g. facilitation support/ tech support – who to go to when • We'll stay on the call after the workshop if you have any questions you want to ask us	HVM LF using HVM slides	PP Purpose & Agenda Slide Intro PP LF PP presentation	People are clear: Who is in the room and why; who they will be working with What we will be doing together Being clear that this is a participant-led process.

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
		• How/ why we'll capture what is said this evening – we are interested in what you say not who says what, your name will not be linked back to anything we write about in the report • Mentions the report this feeds into			
10:10-10:20 (10 mins)	Menti questions set 1	**Participants asked to get menti.com on their phones/ another tab on their device.** Share the code, the QR code and the link in the chat – as 3 easy ways to get into menti. Reminder no right or wrong here, the questions I'm asking now are about beginning to think about our dialogue topic. LF to share screen with 'hide results' QM1: Share one hope you have for digital identity services QM2: Share one concern you have for digital identity services Complete this sentence: QM3: Trusted digital identity services will be… In each case LF to share results when more than 12 are in	LF	Menti.com Tech support to put menti link/ code in the Chat	Getting back in to the space by remembering the webinar Thinking about hopes and concerns as a route to trust.

10:20-10:45 (20 mins) 10:20-10:35 (15	Summary of what we've done so far	**Presentation 1**: LF to present a summary of all we've done so far:
		• What's been covered in each workshop
		  • Who has spoken to the group on what
		  • Stimulus shared in relation to DSIT plans/ the trust framework
		  • Lived experience films we've seen
		• The activities on Recollective
			LF	Questions in the chat shared by participants as we go through these	A full review of what we've discussed/ shared/ worked on over the last 3 weeks.

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
mins) 10:35-10:45 (10 mins)		• Answers to the questions that we've uploaded to Recollective • Reassurance that this is a process, and can be difficult, you may change your mind, you may want to explore something in depth – that's fine, we can do that today. Questions on what we've done together/ shared/ discussed fielded by HVM/ DSIT. This is our last question session. Now we need to shift our thinking from asking questions to saying what we want. Think about this as your trust framework and your dialogue. What do you want to focus on to propose clear recommendations for DSIT on how the trust framework and oversight of the system should work.		review points.	
10:45	TS to move everyone to their pre-allocated small groups – 7 participants per group, same groups as in previous workshop				
10:45-11:15 (30 mins)	A focus on the trust framework and the 'Rules'	In the UK digital identity & attributes trust framework you have seen summaries of key sections about the 'rules' for: • Identity service providers • Attribute service providers • Identity and attribute service providers • Orchestration service providers • Scheme owners • all identity, attribute and orchestration service providers We're going to work through our summaries (which you'll have already seen on the online community space now). We'll start this now and continue after the break. **RECORDER ON**		Facilitators have beta version trust framework in full open to share as necessary Infographic/ visual suite summarising sections	Making sure the elements already in the trust framework are being reviewed not re-invented

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
		Q1: What stands out for you as important? **Q2: What stands out for you as reassuring?** **Q3: What is missing which might give further reassurance?** Discussion – focused on what you want to see in relation to: 1. Making sure there is consistency across providers e.g. I can use the same app when buying alcohol in all the supermarkets (full framework 15.1 making your products and services interoperable with others/ 15.15 working with relying partners) 2. What happens when things go wrong – responding to complaints (full framework 15.3 responding to complaints) 3. Reassurance – standards/ principles/ values (full framework 15.6 service and quality management) 4. Inclusion (full framework 13.3 make sure your products and services are inclusive) Participants can explore the topics they want to discuss in depth – you can be guided by them in this discussion using the framework as a guide. **TS to announce to all groups 3 minutes remaining in small groups at 11:12. Close groups with one minute count down at 11:14.** **RECORDER OFF**		12-16 of the trust framework Fs to share Jamboard with each of the visuals. Screen divided into 3 Important Reassuring Missing **TS broadcast**	

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
11:15-11:30 (15 mins)	**Break –** LF to remind people to stay in Zoom just to turn off their cameras/ mics and put the camera back on when they return promptly at 11:40.				
11:30	TS to move everyone to their pre-allocated small groups – same 7 participants per group				
11:30-12:00 (30 mins)	Continued focus on the trust framework and the rules.	**RECORDER ON** **Q1: What stands out for you as important?** **Q2: What stands out for you as reassuring?** **Q3: What is missing which might give further reassurance?** Discussion – focused on: 1. Management of data (full framework 15.7 information management, 15.8 information security) • Who owns/ controls the data • How do I expect my data to be cared for/ managed 2. Risk management (full framework 15.9 risk management) • Privacy (full framework 15.13 privacy and data protection) • Fraud (full framework 15.10) • Theft (full framework 15.8 information security) 3. Questions of cost/ monetisation – what do you think? • Who should pay? • Solutions for people who can't pay • Who benefits/ losses Participants can explore the topics they want to discuss in depth – you can be guided by them in this discussion using the framework		Visuals on the 'rules' within the trust framework Screen divided into 3 Important Reassuring Missing .	Making sure the elements already in the trust framework are being reviewed not re-invented

Time	Agenda	Process	Who?	Process Tools	Expected Outcomes
		as a guide.			
12:00-12:40 (40 mins) 12:00-12:20 (20 mins) 12:20-12:40 (20 mins)	Lived experience review	Review case studies including: • Day in the life (from 1st workshop) • Lived experience films • Journal activities. As a result of this review, thinking through these specific cases: **Q4: What are your concerns for digital identity services** • Including those things which are red-lines e.g. what di service providers should never be allowed to do **Q5: What are your aspirations for digital identity services** • Including those things which will really give assurances In both cases considering: • Inclusion • Data protection including against theft/ fraud • Re-usability • Being able to use the identity in a range of contexts • Reassurances needed. We'll continue/ conclude our deliberations after lunch. **TS to announce to all groups 3 minutes remaining in small groups at 12:37. Close groups with one minute count down at 12:39.** **RECORDER OFF**		Lived experience reminders on Jamboard – drawn from what participants shared in workshop 1/ our own materials Concerns/ aspirations same column on one Jamboard	Using the examples proposed by participants to understand views on key topics and themes

Appendix D – Analysis and reporting tools

Analysis and reporting on this public dialogue took place over several months, beginning with the initiation of fieldwork in May 2023 and culminating in the completion of this report in August 2023. Our analysis is rooted in what people have said and so it was essential to capture their views thoroughly. Rigorous processes were instigated to ensure data collection remained robust all the way through this process.

Each facilitator recorded their own small group discussions, with plenary discussions and text-based chat contributions recorded by either the lead facilitator or a dedicated tech support team member. Facilitators also took visible notes by sharing their screens whilst typing. This allowed participants to amend what was written, review what they had discussed and prioritise key points made as required. These notes were not part of the data capture process but were useful in understanding the points on which participants placed particular emphasis and provided a useful summary of discussions that fed into subsequent reviews including the team analysis workshop.

The HVM analysis and reporting team met regularly to reflect on emerging themes and to develop our thematic analysis approach. After each participant session, facilitators reflected on emerging views from their group discussions. Facilitator reflections were shared verbally (in discussion with each other and the lead facilitator) and in writing via facilitator feedback forms. Emerging findings from participant discussions were explored and validated with participants in later workshops to test and refine our understanding.

All workshop discussions were recorded using Zoom's internal recording feature, which automatically stores combined audio-video files and audio-only files. Audio-only files were sufficient for our analysis, so all video recordings of workshop discussions could be deleted immediately. All small group discussions were transcribed verbatim using the audio-only files. Transcripts were anonymised so that no one can be traced back to comments included in this report. These transcripts are the main source drawn on in our analysis, alongside transcripts generated from participants' contributions to the online space Recollective and full results from the questions posed in workshops using Menti.com.

All qualitative data was thematically coded using the qualitative analysis software NVivo. The analysis team applied grounded theory to ensure findings were drawn directly from the data, based on a thorough reading of the transcripts. We collated what was said into key themes and used those themes to draw out meaning from the discussions. We chose this approach to ensure the findings are rooted in what participants said, rather than looking for confirmation of preconceived ideas.

Before coding any data, we held an analysis workshop involving facilitators and members of the analysis and reporting team. This workshop was used to further develop emerging themes and findings. Discussion drew on facilitator feedback forms and their broader reflections, as well as the visible notes taken within workshops. A coding framework was drawn up at this stage to structure our subsequent analysis and maintain consistency across the team. This was developed iteratively as we read through the transcripts, with sense-checking sessions and updates shared across the team as further codes emerged. The coding framework

can be seen in full in the table below.

The report was drafted by a small team who had been closely involved in the facilitation and analysis of the project. Report drafts were reviewed by core team members at DSIT and Sciencewise, as well as by members of the Oversight Group with time and resource allocated for feedback received to be implemented.

Main code	Subcode(s)
Accountability	Digital identity providers
	Government
	Other regulatory bodies (e.g. ICO)
	Oversight body
Commercialisation (monetisation)	How profits should be made and communicated
	Risks
	Who should and should not bear the costs, pay for the service
Communications, awareness, education	Barriers
	How to communicate the information
	What to inform and educate services & organisations about
	What to inform and educate the public about
Concerns about when digital ID should and should not be used	
Concerns over reliance on technology (e.g. mobile phones, WiFi, data)	Ways to address this (support, infrastructure etc.)
Control (over my data)	'my data, my control'
	Right to be forgotten
	Updating or changing data and information
	What happens upon death
	What happens when you lose access or your phone
	Who sees what
Customer service	Complaints process
	Real person on the other end
Data protection and security	3rd party access
	How & where data is stored
	Plans for when things go wrong (e.g. data breaches)
	Prevention of hacking or fraud
	Responsibility of user to keep data secure
Ease of use and user friendly interface	
Future proofing the system	government policy changes or potential for abuse
	technological advances (e.g. AI)
	tensions with other social issues (e.g. environment)
Improvements e.g. a published road map for roll out	
Inclusion	Accessibility
	Affordability

	Alternatives to digital
	Bias, discrimination (e.g. biometrics, inclusion of protected characteristics)
	Co-design of the system, e.g. with people who have experienced barriers
	Exclusion
	Fairness
	Flexibility (e.g. not just common documents, to the different circumstances people live in)
	Human rights and civil liberties
	Inclusion vs privacy issues
	Opportunities or possible improvements to society & lives of an inclusive digital ID service
	Repercussions of not having access to proof of identity
	Showing only the docs you need to
	Support offered
	Vulnerable IDs
Oversight	Certification
	Evaluations, gathering insights from diverse group of users
	Government's role
	How it will work across devolved governments
	Language, terminology, tone of framework
	Monitoring (e.g. audits, inspections)
	Need for legislation
	OfDIA having independence
	OfDIA having teeth, meaningful consequences, accountability
	OfDIA's role
	Ongoing public involvement in decision making
	Training, vetting and corporate culture
	Who is involved (e.g. diversity and range of skills, backgrounds, sector expertise)
Perceptions of digital identity	Common ways people need to prove their identity
	Explicit comments about changes or shifts in thinking
	Importance or meaning of being able to prove your identity
Possible benefits or added value to current situation	Access
	Convenience
	Future aspirations or ideals
	Possibility of increased privacy
	Simplicity
Privacy	How data is used by digital ID services - Selling to 3rd parties
	Who has access or sight of the data uploaded
Risks	Other concerns
	Risk management, protocols, safeguards
Systemic challenges (e.g. perpetuating institutional racism)	

Technology - barriers and opportunities	
Transparency	Clarity of information
	What information should services share
	Why is transparency important
Trust	Cynicism & fears - Becoming mandatory - System over-reach e.g. if the Home Office has access to my data
	What creates trustworthiness - Experiences of those you know - Importance of customer reviews or track record
	What leads to a lack of trust (government, big corporations)
Universality - will it work abroad	
Who should be running or developing digital ID services	Challenges or concerns about number of providers or decentralised system
	What type of organisations should be delivering these services
Holding codes (used to collate cross-cutting themes when they couldn't be coded to the above or 'test out' new codes)	00Biometrics
	00Context - wider socio or economic concerns
	00Dialogue process
	00How the system works
	00Public security
	00Stories
	00Trade offs
	00Why trust is important

Henrietta Hopkins, Director
Jamie Hearing, Researcher
Louis Mylne, Research Assistant

Hopkins Van Mil
Coppergate House
10 Whites Row
London E1 7NF

info@hopkinsvanmil.co.uk
www.hopkinsvanmil.co.uk

MRS™ Awards 2022
Winner
Public Policy/
Social Research