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