Centre for Finance, Innovation and Technology (CFIT)

Digital Company ID & Fighting Economic Crime: Trust & Governance Framework Working Group

Meeting Minutes

Sprint Session 12

10th October 2025 | Microsoft Teams meeting

Attendees:

Name	Company
Ghela Boskovich (Co-Chair)	Financial Data and Technology Association
Nick Mothershaw (Co-Chair)	Select ID
James McGreevy	CFIT
Sajni Shah	CFIT
Ryan Wu	CFIT
Adrian Field	OneID
Lewis Utley	DNB
Georgina Stracey	A&O Shearman
Nikki Johnstone	A&O Shearman
John Harrison	UCDx
Daniel Jonas	We are Pay
Florian Chevoppe-Verdier	DSIT
Sophie Laing	N/A

Francis O'Neill	Lloyds
Gilbert Hill	PrivTech
David Rennie	OIdentity
Helena Wood	CIFAS
James Deely	Umazi
John Harrison	UCDx
Xiaodi Wang	GLEIF
Richard Seaman	Dun & Bradstreet
Sally Henstock	TransUnion
Stuart Young	Etive Technologies
Mark Devlin	Lloyds
Lorraine Salmond	Lexis Nexis Risk
Nitesh Palana	Thought Machine
Calum Roberts (Secretariat)	Fuse, A&O Shearman
Katherine Pittalis (Secretariat)	Fuse, A&O Shearman

Agenda:

1. Welcome
2. Eligibility to Become a Provider
3. Who May Want to Become a Company ID Attribute Provider
4. The Role of DSIT VS Market Responsibilities
5. Governance Models
6. Next Steps
7. Appendix
8. Group Exercise From Sprint 11

1. WELCOME

Participants: Ghela Boskovich [GB], Nick Mothershaw [NM]

1.1. GB welcomed all participants to the twelfth meeting of the Trust & Governance Framework Working Group.

1.2. GB reminded all working group members of the importance of adhering to the guiding principles on competition (as set out in the slides) and encouraged participants to engage and collaborate with the working group in an open and respectful manner.

1.3. NM outlined the agenda and noted that the session would deviate from the original sprint plan in places to bring threads together outstanding topics for discussion ahead of the forthcoming legal and regulatory sprints.

1.4. The primary objectives of this meeting were outlined:

- Discuss eligibility requirements for Digital Company ID Providers.
- Discuss who might take on provider roles.
- Explore delineation of responsibilities between DSIT versus and the market, including questions of self-monitoring and self-regulation.

2. ELIGIBILITY TO BECOME A DIGITAL COMPANY ID PROVIDER

Participants: Nick Mothershaw (NM), Adrian Field (AF), Daniel Jonas (DJ), Florian Chevoppe-Verdier (FCV), John Harrison (JH)

2.1. NM introduced the proposed eligibility criteria for Digital Company ID and attribute providers, which included capability to source, verify and attest identity data, robust data sharing mechanics, UK regulatory compliance, eIDAS/DIATF alignment, independent audit, and readiness for certification. NM asked whether any additional eligibility criteria were required and how certification should be treated.

2.2. AF suggested that CFIT recommend that only corporate ID service provider roles be incorporated into the DIATF, with certification administered by accreditation bodies under the established UKAS regime. AF noted that nothing in the DIATF is self-asserted and recommended that this remains the case.

2.3. FCV questioned whether putting roles into the framework would imply mandatory certification. NM clarified that inclusion of the roles in the DIATF does not itself mandate certification; mandating, where required for a defined purpose, is set externally (e.g. Right to Work / DBS) and relying parties can also mandate certification contractually via procurement and RFPs.

2.4. NM recommended that the report should clearly note that inclusion of roles in the DIATF does not mandate certification, however it should be considered whether mandating is necessary, and, if so, why?

2.5. DJ, JH, AF & GB further discussed whether the working group should recommend that all ID checks are down within the DIATF and by a certified provider or whether the market should self-select. It was noted that the market may converge around common utilities which could result in anti-competitive dynamics if a single system emerged. GB recommended that the report acknowledge the '*natural law of systems*' – that there may be a coalescing around a particular model or system which could present competition challenges. The report should acknowledge that a recommendation to use a specific model that will support certain providers this could result in competition issues.

3. WHO MAY WANT TO BECOME A DIGITAL COMPANY ID ATTRIBUTE PROVIDER

Participants: Nick Mothershaw (NM), John Harrison (JH), Adrian Field (AF), Daniel Jonas (DJ), Ghela Boskovich (GB)

3.1. NM introduced the topic of who might want to become a Digital Company ID / Attributes Provider.

3.2. JH questioned whether the CIDASP would be used for ongoing authentication beyond onboarding and if so then banks should be included as a potential CIDASP. NM agreed that banks should be captured.

3.3. AF suggested splitting the CIDASP into two: the Company ID Provider and the ASP and that a provider may choose to do one or both components. NM acknowledged the separate aspects of the CIDASP and recommended that the report note the CIDASP as being one role with two functionally separate components.

4. THE ROLE OF DSIT VS MARKET-LED RESPONSIBILITIES

Participants: Nick Mothershaw (NM), Florian Chevoppe-Verdier (FCV), Adrian Field (AF), John Harrison (JH), Richard Seanman (RS), Daniel Jonas (DJ), Ghela Boskovich (GB)

4.1. NM initiated a discussion on delineating roles and responsibilities between DSIT and the market, presenting a table of suggested responsibilities (as set out in the slides).

4.2. Remit of DSIT: FCV confirmed DSIT's remit was to enable market adoption and to work with the market to achieve that aim, noting that the CFIT's recommendations in the report should articulate what is being asked of DSIT. NM and GB framed the report's intent to specify where DSIT should act versus what should be left to the market, including areas of overlap. The group agreed to position DSIT's role as enabling, proportionate and modular, while preserving space for market-led innovation.

4.3. Access to Government-held authoritative data: AF emphasised that enabling verifiable access to Companies House data, ideally tied to Gov.UK One Login, is critical. He cited the Information Gateway under the Data Act as the legal basis for government-to-private sector data sharing and advocated for an API and / or director credential route from Companies House that can be relayed to private sector ID services. AF recommended that DSIT should ensure a mechanism exists for verifying a director (e.g. via One Login) with a similar mechanism for HMRC or other

government-held data. GB agreed that only government can ensure for flow of government-held data and that DSIT should be responsible and accountable for making such data portable and accessible where required for digital ID. The group agreed to recommend that DSIT secure the necessary interdepartmental commitments and delivery mechanisms, emphasising that DSIT is in the prime position to ensure that any government held data is operable and portable

4.4. Wallet-mediated data exchange: JH added that there are two ways approaches to this data exchange: (1) Government-verified identity presented to Companies House, then proof of directorship issued to the individual's wallet and (2) Direct government API enablement. The group agreed to present in the report both API-mediated and wallet-mediated paths as viable models, while maintaining the core principle that DSIT must ensure the flow of government data.

4.5. Fraud and intelligence sharing: RS observed that effective fraud prevention requires collective action and that responsibilities should be shared between government and the market. GB supported the proposition: DSIT and the government can set expectations and encourage coordination, but the market should collaborate to report fraud and tackle fraud. The group agreed to recommend industry-led fraud intelligence sharing across sectors to reduce fraud risk and enable near-real-time dissemination of information, with consideration of strongly encouraged or potentially mandated mechanisms.

4.6. Convening power and technical standards: JH stated that some elements – particularly technical standards and orchestration utilities – cannot be delivered solely by either government or the market. GB emphasised DSIT's convening power to compel market collaboration where necessary. The group agreed to recommend that DSIT exercise its convening power to coordinate and compel the market to act.

5. GOVERNANCE MODELS

Participants: Daniel Jonas (DJ), Ghela Boskovich (GB), Nick Mothershaw

5.1. NM presented the group with a table of potential governance models (as set out in the slides).

5.2. Governance models and market collaboration: AF suggested framing options by reference to what already exists (DSIT, OfDIA) versus additional market intermediaries and a "leave-it-to-the-market" approach akin to eIDAS wallet implementations, where open standards and market

interoperability projects predominate. The group agreed to prefer market-led collaboration with targeted government enablement, and to avoid premature over-structuring unless justified by measurable need.

5.3. Iteration and review: DJ suggested embedding feedback mechanisms to assess system performance and identify when additional governance or intervention is warranted. GB noted that the report should acknowledge uncertainty and recommend periodic review to allow the ecosystem to evolve. The group agreed to recommend explicit measurement frameworks and ongoing review.

5.4. Reference matrix of international approaches: DJ recommended creating a typology of governance/market models from international jurisdictions (e.g. Estonia, France, Nordics, Thailand etc) to help inform UK choices. NM noted that OfDIA had prepared documentation on why certain models had not been adopted in the UK which includes a matrix of potential governance models mapped to the UK context. The group agreed to include a succinct comparative matrix based on the OfDIA research to guide model assessment on a side-by-side basis.

5.5. Consortium/Orchestration Model – Risks and Practicalities: JH outlined a possible DSIT-pointed consortium as an orchestration provider with staged equity entry to manage market development. GB cautioned that setting up such a vehicle is complex and time-consuming, pointing to current open banking governance reforms as an example. The group noted benefits of shared orchestration but recognised the significant effort required. There was no consensus to recommend this at present beyond acknowledging it as a potential future option should a need be required in the future.

6. NEXT STEPS

6.1. Due to time constraints, GB presented the slides that discussed *Certification for Model Selection* and *Certification Criteria – Proposed Overlays.* She requested that participants reflect on these slides and e-mail any additional comments and insights to include in the report.

6.2. The 13th sprint will be held on 24th October 2025. This sprint will focus on the risk, regulatory and legal framework, chaired by Nikki Johnstone.

7. APPENDIX

Acronyms

API – Application Programming Interfaces

ASP – Attribute Service Provider

CIDASP – Company Identity Digital Attribute Service Provider

CRA – Credit Reference Agency

DIATF – Digital Identity and Trust Framework

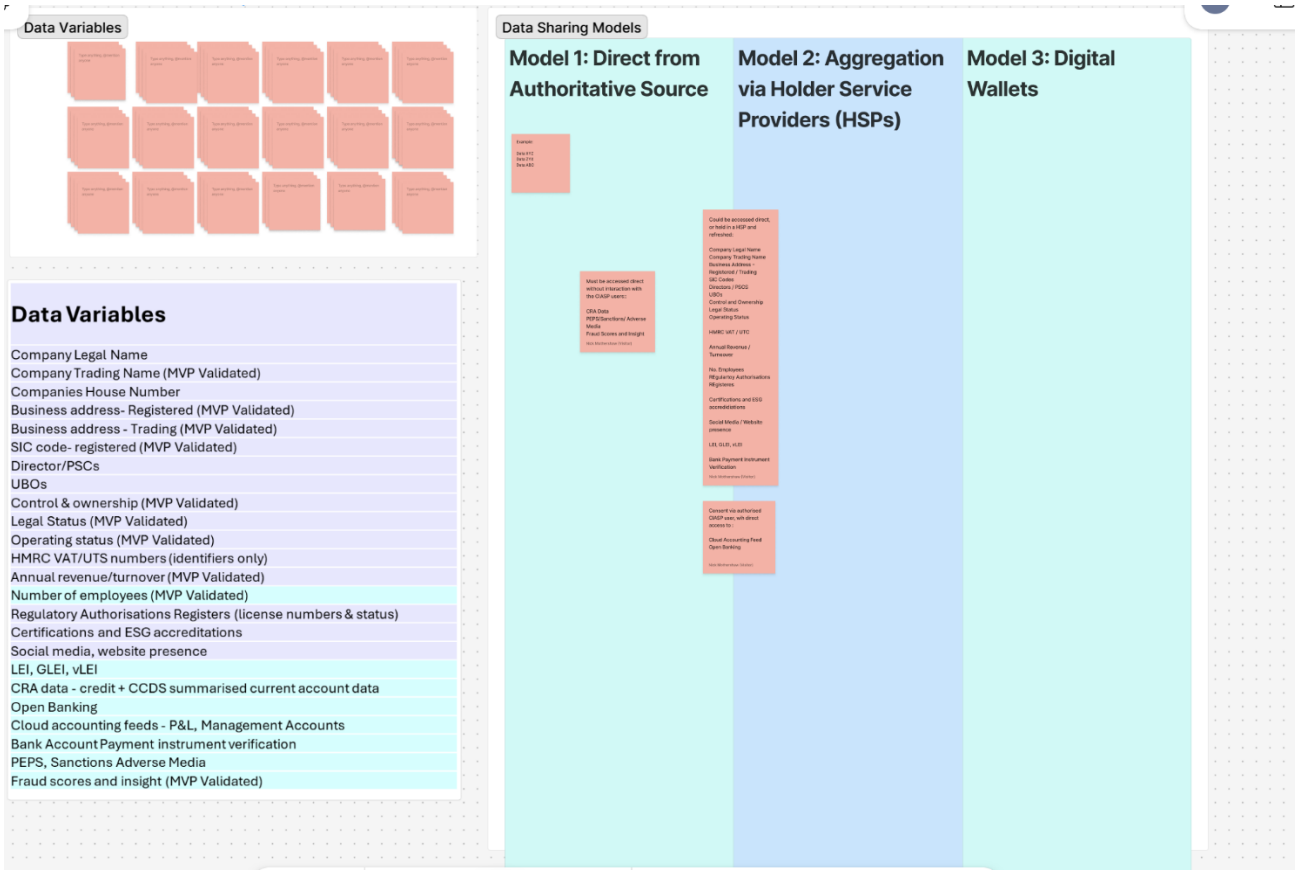
DSIT – Department for Science, Innovation and Technology

HMRC – His Majesty's Revenue and Customs

OfDIA – Office for Digital Identities and Attributes

8. GROUP EXERCISE FROM SPRINT 11

Set out below for are the results of the group exercise in Sprint 11:



Data Variables

Company Legal Name
Company Trading Name (MVP Validated)
Companies House Number
Business address- Registered (MVP Validated)
Business address - Trading (MVP Validated)
SIC code- registered (MVP Validated)
Director/PSCs
UBOs
Control & ownership (MVP Validated)
Legal Status (MVP Validated)
Operating status (MVP Validated)
HMRC VAT/UTS numbers (identifiers only)
Annual revenue/turnover (MVP Validated)
Number of employees (MVP Validated)
Regulatory Authorisations Registers (license numbers & status)
Certifications and ESG accreditations
Social media, website presence
LEI, GLEI, vLEI
CRA data - credit + CCDS summarised current account data
Open Banking
Cloud accounting feeds - P&L, Management Accounts
Bank Account Payment instrument verification
PEPS, Sanctions Adverse Media
Fraud scores and insight (MVP Validated)