Centre for Finance, Innovation and Technology (CFIT)

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

Meeting Minutes

Sprint Session 15

5th December 2025 | Microsoft Teams Meeting

Attendees:

Name	Company
Ghela Boskovich (Co-Chair)	Smart Data and Technology Association
Nick Mothershaw (Co-Chair)	Select ID
James McGreevy	CFIT
Sajni Shah	CFIT
Ryan Wu	CFIT
Mark Terry	Lloyds
Daniel Jonas	Pay.ID
Gilbert Hill	PrivTech
Georgina Stracey	A&O Shearman
Luca Britos	A&O Shearman
John Harrison	UCDx
Sophie Laing	EY
Chor Te	Moodys
Richard Seaman	Dun & Bradstreet
Stuart Young	Etive Technologies
Lewis Utley	DNB
Katarina Pranjic	LexisNexis Risk Solutions
Cindy van Niekerk	Umazi
Florian Chevoppe-Verdier	DSIT
Emily Hyett	Yoti

David Rennie	OIdentity
Stephen Abbott Pugh	KYCKR
Calum Roberts (Secretariat)	Fuse, A&O Shearman
Katherine Pittalis (Secretariat)	Fuse, A&O Shearman

Agenda:

1. Welcome
2. Considerations for Working Group Members Discussion
3. Additional Questions
4. Next Steps
5. Appendix

1. WELCOME

Speaker: James McGreevy (JM)

1.1 JM welcomed all participants to the 15th meeting of the Trust & Governance Framework Working Group.

1.2 The primary objective of this meeting was outlined:

(a) Address the gaps from the previous sprints where:

(i) No consensus was reached where in one of the sprints there has been disagreements which require working group resolution.

(ii) Items that were intentionally deferred to future working group or implementation phrases

(iii) Outstanding questions and open discussion items for analysis and future consideration were to be considered in the report.

1.3 JM 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.

2. CONSIDERATIONS FOR WORKING GROUP MEMBERS DISCUSSION

Speakers: Nick Mothershaw (NM), Ghela Boskovich (GB), John Harrison (JH), Cindy van Niekerk (CvN), Daniel Jonas (DJ),

2.1 Fraud Checks and Liability Models

(a) NM introduced the fraud section, querying whether additional fraud content was needed given the Digital Identity and Attributes Framework (DIATF), already imposing extensive fraud obligations on IDSPs and equivalent roles. NM proposed reframing the report to leverage DIATF requirements rather than creating a parallel prescriptive regime.

(b) **Fraud References**. JH queried where fraud checks should be placed as it should be dependent on the kind of fraud that takes place. He noted that "fraud" is a broad term. GB explained that the remit for the Digital Company ID is within the realm of a fraudulent company rather than a company engaging in fraudulent activity. The DIATF already contains fraud mitigation, as such the report does not need to include any additional rules of requirements. NM recommended that the report be clear on the

specific type of fraud being discussed (e.g., first-party fraud / credit behaviour) that focuses on corporate ID fraud.

(c) **Authoritative Data Sources and Data Sharing.** CvN raised the point about open banking and the transition into open data with. GB proposed distinguishing open data (government data) from smart data (industry data), recommending triangulation across government datasets (e.g. Companies House with HMRC) to address data quality. DJ referenced quantum technology, emphasising that the interaction between quantum technology with different data sources is developing considerably. GB, thus, recommended the report state how the government should monitor oversight of the data sources that currently exist and ones that could exist that could enhance the attribute validation exercise. GB also recommended that the report note that, for the time, there is a limit on the emerging technologies that can be considered. A caveat should be included in the report, recommending the government continue to monitor how emerging technologies could affect risk, fraud and exploitation in the context of digital verification.

2.2 Role Demarcations and Ecosystem Evolution

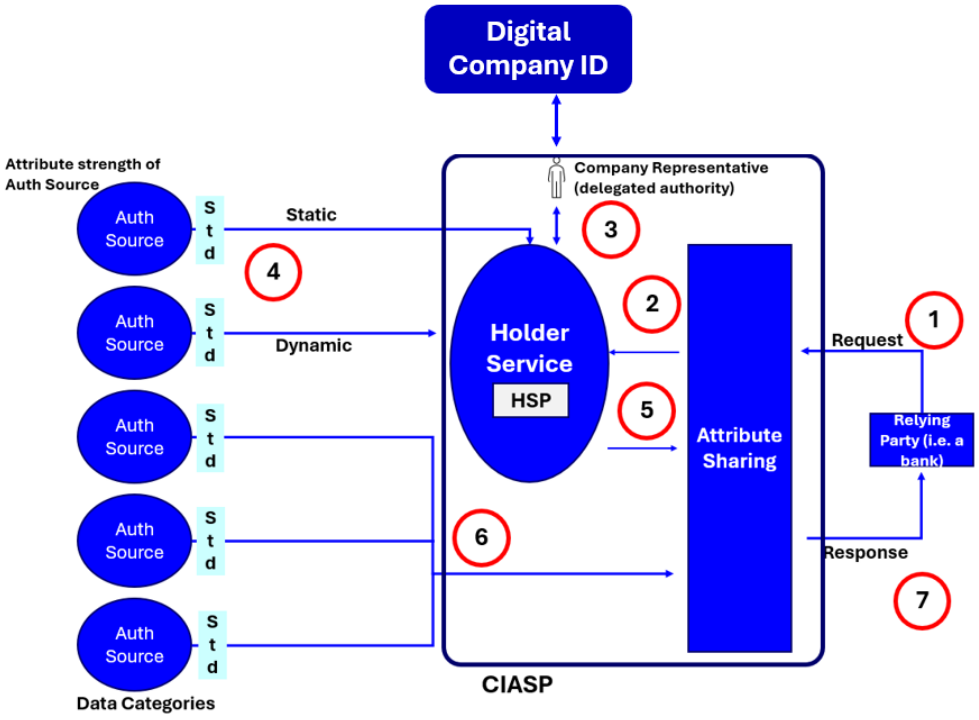
(a) NM introduced this section by discussing the CIASP construct in Figure I. NM queried whether the CIASP element was being overloaded and proposed making this clearer in the report by unpacking the roles. NM recommended an ongoing group that looks at this and feeds into the framework.

(b) **Separation of Roles.** NM clarified that you can separately be a company ID provider and not a CISP. GB followed up that you can serve multiple roles but not all at once. You can as an individual company get the provision or the certification for multiple roles, but these do not necessarily need to be fulfilled.

(c) **Model Presentation.** GB confirmed that the goal of the report is to present multiple viable models with different caveats with a risk-based approach tied to each model chosen and selected.

(d) GB clarified that even though there are different working groups and reports, different points will be addressed in the market opportunity report and some in the trust and governance. GB expressed that the roles and responsibilities for the model is chosen by the market and will continue to evolve as the market evolves.

Figure I - CIASP Diagram



2.3 Regulatory Alignment and Interoperability

(a) NM invited the group to provide views on how firmly the report should anticipate international interoperability, including the EU. DJ recommended a clear read-across between the UK DIATF roles and eIDAS roles. GB supported EU alignment due to companies having an interest in market expansion. GB emphasised the point that closer alignment, the easier the interoperability and less costly it is for companies to do business beyond the borders should be underscored.

(b) NM observed that the EU frameworks define issuers and authoritative sources more precisely than the UK, which largely treats "authoritative sources" lightly and mainly via GPG 45. He suggested that after the project, an encouragement could be made for the UK framework to deepen its treatment of issuers, issuers of information and authority resources which are sometimes treated as the same thing.

(c) JH requested the report clearly differentiate 'Type 1' and 'Type 2' data. JM confirmed that these concepts were addressed in earlier sprints but will be noted.

(d) CvN recommended that interoperability not be limited to EU alignment but anchored in broader international standards (e.g., ICAO-style standardisation analogies), so that varying national implementations still interoperate through common standards; NM agreed EU is proximate and deep, but should not be exclusive, with GB proposing that DSIT consider the widest set of global standards while prioritising EU alignment for proximity and momentum. DJ highlighted cross-border payment interlinking and "one-leg-out" models (EPC) as forums where reciprocity and pre-validation discussions are advancing and where identity standards alignment is a prerequisite; he proposed linking these conversations, while noting governance trade-offs.

3. ADDITIONAL QUESTIONS

3.1 Fraud Signals

(a) NM proposed clarifying the fraud section to reflect DIATF's existing fraud obligations and adding a recommendation for coordinated fraud "signal sharing" across the ecosystem, given DIATF references signal sharing but lacks specificity on mechanism and participants. JH reiterated that fraud controls depend on the market model: in a "credit reference plus" model, back-office checks naturally sit with attribute/data providers purchased by relying parties, whereas wallet providers in a front-office model might not be best placed for those checks; GB responded that the signal-sharing recommendation addresses ecosystem-wide red flags rather than delegating checks to individual parties and is model-agnostic.

(b) NM distinguished corporate identity fraud scenarios the framework must guard against - synthetic/company impersonation and corporate ID takeover - while excluding first-party fraud by legitimate companies from scope; the report will sharpen scope accordingly. Cindy supported expanding fraud-related considerations to reflect the distinct attributes and risk levels in company identity versus personal identity, including data quality controls.

3.2 DSIT's Role and Market-Led Responsibilities

(a) GB discussed delineating responsibilities between DSIT and the market. CvN questioned whether market-developed rules would be formalised into the DIATF. GB clarified the intended model where the industry should develop common rulebooks through consultation and DSIT then formulise these into the trust framework as appropriate, with ongoing coordination across multiple regulators and departments.

(b) JH urged explicit inclusion of identity-payments coverage for SMEs as a forward-looking area for DSIT to consider.

(c) JH expressed concern that a single model (credit reference plus) had dominated thinking, urging explicit consideration of a managed market of wallets and asking that DSIT be tasked to plan for convergence of SME company identity with payments in such a model. Cindy and GB responded that technical standards should remain model-agnostic, enabling multiple roles and models, and that multiple regulators and departments will be involved; GB agreed convergence with payments is a natural longer-term consideration and should be signposted, while noting it is unlikely to be an immediate recommendation but should be captured for future planning.

(d) JH cautioned against repeating open banking's early over-emphasis on technical standards at the expense of business and funding models; GB acknowledged the point, noting that payments regulation and data sharing are treated distinctly by the FCA and that reconciling these strands is part of open finance evolution. CvN added a final request to include a standing recommendation for monitoring future technical advances and their implications for governance, preserving parity in safety, security, and risk mitigation as technology evolves. GB agreed to frame this as a joint responsibility of government and industry to share and act on emerging risk intelligence.

4. NEXT STEPS

Speakers: James McGreevy (JM)

JM thanked attendees for joining the meeting and recommended that group members send via email any information that they would like to be considered for the report. A draft of the report would be circulated before the next sprint for group members to review and provide feedback.

The 16th sprint will be held in Q1 in 2026. This sprint will focus on reviewing the report.

5. APPENDIX

ASP – Attribute Service Provider

CIASP – Company Identity and Attribute Service Provider

DIATF – Digital Identity and Attributes Trust Framework

DSIT – Department for Science, Innovation and Technology

eIDAS – EU Electronic IDentification, Authentication and trust Services

HSP – Holder Service Provider

IDSP – Identity Service Provider