Centre for Finance, Innovation and Technology (CFIT)

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

Meeting Minutes

Sprint Session 11

25th September 2025 | Meeting at A&O Shearman, One Bishops Square, London, E1 6AD and over Microsoft Teams.

Attendees:

Name	**Company**
Participating in person	
Ghela Boskovich (Co-Chair)	Financial Data and Technology Association
James McGreevy	CFIT
Rob Haslingden	CFIT
Louise Beaumont	Independent
Sajni Shah	CFIT
Adrian Field	OneID
Daniel Jonas	Pay.UK
Richard Seaman	DnB
John Harrison	UCDx
Katherine Pittalis (Secretariat)	Fuse, A&O Shearman
Calum Roberts (Secretariat)	Fuse, A&O Shearman
Participating online	
Nick Mothershaw (Co-Chair)	Select ID
James Deely	Umazi
Lewis Utley	SmartSearch

Florian ChevoppeVerdier	Leading Point
Xiaodi Wang	GLEIF
Sally Henstock	Trans Union
Sophie Laing	N/A
Stuart Young	etive

Agenda:

1. Welcome
2. Objectives
3. Overview of Data Sharing Models
4. Open Discussion
5. In-Person and Online Activity
6. Next Steps

1. WELCOME

Speaker: James McGreevy (JM)

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

1.2. 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. OBJECTIVES

Ghela Boskovich (GB) and Nick Mothershaw (NM)

2.1. The primary objective of this meeting was to review and discuss different models for Company Digital Identity, particularly how authoritative sources and attribute sharing are managed.

2.2. The goal was to ensure that the report captures all viable data sharing models without endorsing a single solution and that supporting diagrams and role descriptions reflect these options. outlined:

(a) Assess various approaches for data sharing models (digital wallets and UK eIDAS Adaptation). This included outlining the pros and cons of each along with key recommendations.

(b) Understand the roles of Attribute Service Providers (ASPs) and Holder Service Providers (HSPs) in the data sharing models.

(c) Assess how to categorise data variables into the three models based on how well they accommodate them.

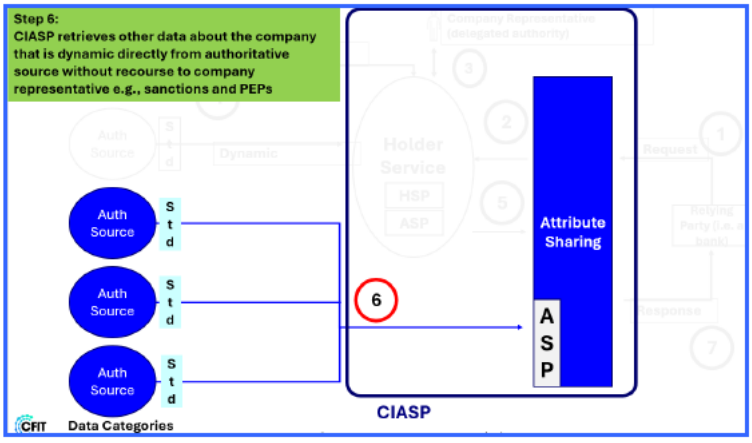
3. OVERVIEW OF DATA SHARING MODELS

Nick Mothershaw (NM)

3.1. NM presented an overview of the data sharing models for Digital Company IDs and confirmed that the report would present all viable data sharing models rather than endorsing a single solution. NM reiterated that supporting diagrams and role descriptions must be accurately reflected in the report.

3.2. NM outlined four main models for data sharing:

Model 1: Direct API Access from Authoritative Sources



- NM stated that his model involves direct, real-time access to authoritative data sources via APIs whenever a relying party requests company attributes. The key considerations were described as follows:

(a) **Dynamic data handing**: this model is suited for attributes that are dynamic – those that change frequently or require up-to-date verification at the point of use (e.g. sanctions, fraud risk or other risk-related data).

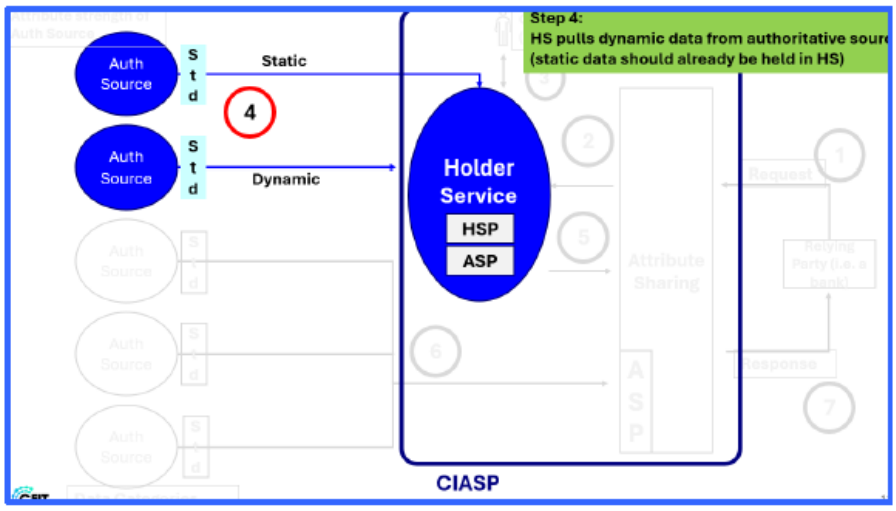
(b) **Integration complexity**: real-time access increases integration complexity, as the system must be able to fetch and process data on demand from multiple sources.

(c) **Standardisation needs**: NM highlighted the importance of API standardisation across different authoritative sources to ensure consistency and reduce the need for data normalisation at the CIASP level. NM posed the question of who would define those standards.

(d) **User visibility**: Certain data (non-visible risk data) is not exposed to the subject or HSP but fetched and delivered directly to the relying party.

- NM stated that the downsides of this model involved increased integration complexity and required API standardisation across sources to avoid the need for bespoke data normalisation layers

Model 2: Aggregation via Holder Service Provider (HSP) / Company Identity Attribute Service Provider



- NM explained that in this model an HSP aggregates and stores company attributes which may include both static and dynamic data. NM outlined key considerations which included:

(a) **Attribute Storage:** The HSP stores attributes in a repository (cloud or device-based), with static attributes held until needed and dynamic attributes flagged for refresh at the point of sharing.

(b) **Visibility and Control:** Users (or their delegates) can view and manage the data held by the HSP, making it suitable for visible corporate data such as Companies House registration details.

(c) **Delegated Authority:** NM noted that the model makes it easier to delegate authority, allowing designated individuals (e.g., company directors) within the CIASP to control and grant sharing right across different data items.

(d) **Refresh and Maintenance**: Dynamic attributes require mechanisms for regular refresh or validation to ensure data remains current. NM noted that rules for attribute re-fresh and maintenance, as defined in the DIATF for ASPs, should also apply to HSPs when they hold such data. NM pointed out that if the HSP is holding attributes, and keeping them up-to-date, it must meet the rules for Attribute Service Providers (ASPs), such as checking if an attribute has been updated and keeping it current.

(e) **Role Clarification:** The group discussed the need for clear definitions and obligations for the roles of HSP, ASP, and CIASP, especially where functions overlap.

Model 3: Digital Wallets (device-based and/or cloud-based)

- NM described digital wallets typically device-based where private keys are held on the device, allowing for authentication.

- Portability and Reusability: NM noted that if implemented, wallets allow credentials to be moved from one wallet to another, provided wallets adhere to the same standards.

- NM noted that in the UK, the HSP model is designed to embrace wallets and that portability and reusability are possible if wallets are interoperable.

- NM gave the example of the German wallet implementation, where even the ID credential is a pointer back to the authoritative source and must be refreshed.

- Rule and governance: NM raised practical governance questions around device management, such as whose device the wallet sits on (personal device, company-issued device or bring-your-own devcide), what happens when directors change, and potential issues in organisational contexts where multiple people may need access to the wallet.

- The group agreed that both device-based and cloud-based models are valid and should be recognised in the report, but rules surrounding portability, reusability and device management required consideration.

Model 4: Unsecured Data Sharing – e.g. screen scraping, outside current framework.

- NM discussed the fourth model which such as screen scraping or unsecure data sharing. NM noted that these methods are outside the scope of the Trust and Governance Framework.

4. OPEN DISCUSSION

Ghela Boskovich (GB), Nick Mothershaw (NM), John Harrison (JH), Rob Haslingden (RH), Lewis Utly (LU), Daniel Jonas (DJ), and Adrian Field (AF)

3.1. NM opened the discussion to the group to consider questions regarding the different data sharing models. This included considering their dynamics, how this would be managed and shared and which of the four models would best accommodate the different data variables.

(a) Role Definitions and Responsibilities

- The group discussed the definition and placement of Attribute Service Providers (ASPs) and Authoritative Sources.

- AF raised a question regarding the location of ASPs in the model diagrams proposing that ASPs are the sources of data. NM highlighted, that under the DIATF definitions, ASPs “collect, create, check and share” attributes and support re-use and are not the source of the data and therefore should manifest as an intermediary role in the middle of the CIASP. He noted that authoritative sources are referenced in GPG45 as places to check integrity/up-to-datedness of information but are not an DIATF role with obligations

- GB emphasised that the ASP is distinct from the authoritative source and that there is a need for clearer definitions and role separation in the framework. NM recommended that the DIATF would benefit from

explicit definitions for "authoritative source" with clarity on who [scores] attributes. Where HSPs maintain attributes, applicable ASP rules (e.g. freshness checks) should apply.

(b) Clarification of Data – Static vs Dynamic / Visible vs Non-Visible

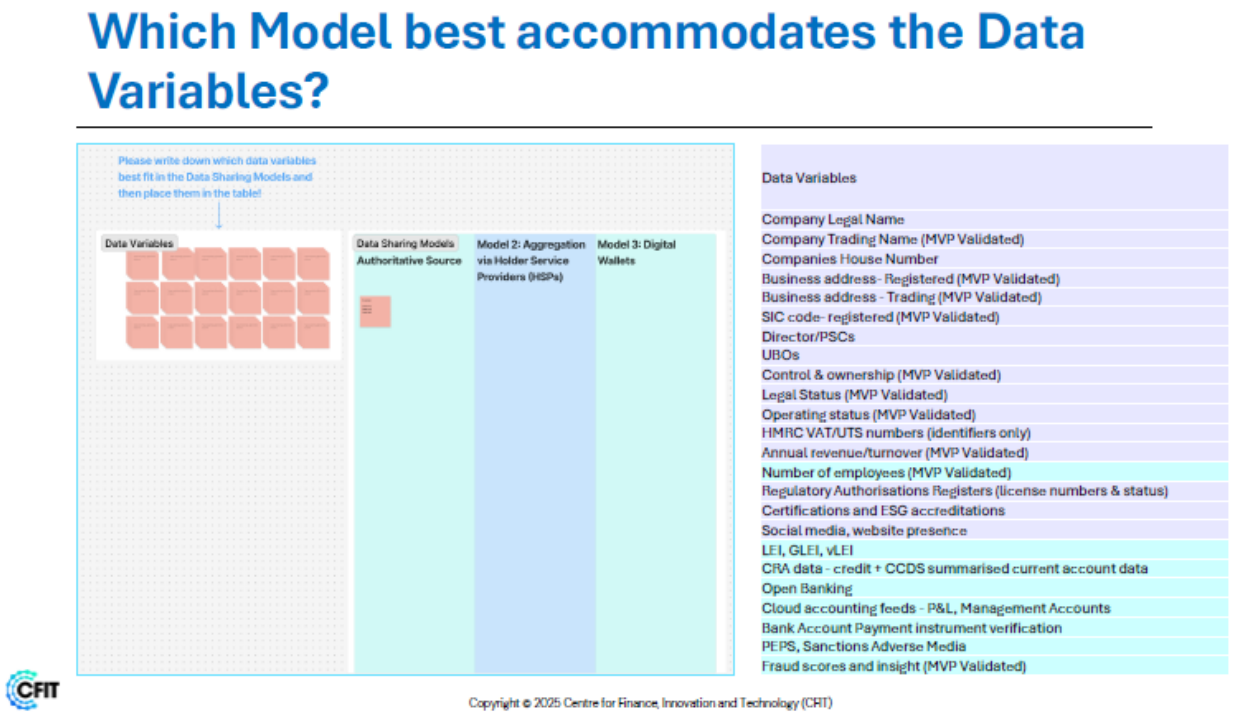
- On discussing digital wallets, JH sought clarification on the definition of static and dynamic data. He suggested that dynamic data changes regularly and needed to be maintained.
- AF notes that there was a distinction to be made between visible-to-subject data and non-visible risk data .
- NM agreed that non-visible data, such as risk, fraud, PEPs and sanctions should not be shown to the data subject and should be routed via Model 1.
- It was agreed that visible corporate data (e.g. Companies House registration) is better suited to Models 2 and 3. The group agreed that for attributes that can change and matter at the point of use, a mechanism to ensure freshness is required (such as a direct re-fresh or time-bound validity in a holder/wallet model).

(c) Data Verification and Chain of Custody

- The group discussed the important of triangulation, liability and auditability in the data sharing models.
- The group discussed the need for robust certification and management of the HSP role, and whether it should be a structured collection of roles or a loose aggregation.
- JH reintroduced Type A and Type B data, highlighting the differences:
    - Type A data that is issued by authoritative sources (e.g. Companies House) which is typically provided because of the relationship between the subject (e.g. a Small to Medium-Sized Enterprise) and the authority. There is generally no additional cost for accessing this data as it is already paid for through standard processes (e.g. company registration).
    - Type B data involves CRAs or similar providers acting as aggregators, performing triangulation and validation, and selling the resulting data package to relying parties. Type B data is only sold from one single, relying party (e.g. CRA) which can be bought by a relying party.
- RH and GB noted that achieving certainty in Digital Company IDs required triangulation of both personal and business attributes and that specific methodologies used for triangulation are the intellectual property of the provider.
- LU and GB pointed out that banks may not rely on external 'confidence scores' and that it is preferable to deliver a chain of evidence so that relying parties can apply their own risk models.
- The group agreed on the importance of a cohesive approach to data validation and triangulation. They recommended that a differentiation between core and value-added data is important and recognised that different business models (Type A vs Type B) may be appropriate for different data types.

5. IN-PERSON AND ONLINE ACTIVITY

5.1. JM asked the group to participate in a collaborative exercise designed to map data attributes to the most suitable data sharing models. The purpose of the activity was to help the group evaluate which models best accommodate different types of data variables, considering factors such as data dynamism (static vs dynamic), visibility to the data subject and technical or business requirements. The group was presented with the below slide and asked to complete the exercise:



5.2. GB asked the group to complete this activity over the course of the next two weeks so that the results could be included in the ongoing report.

6. NEXT STEPS

6.1. The group was also reminded that there were additional questions assigned for the session that were not addressed due to time constraints. GB recommended reviewing the slides and any outstanding questions from the session and to provide responses and feedback within two weeks. These responses should be sent to JM to include in the ongoing report.

The 12th sprint will be held on 10th October 2025. This sprint will focus on Certification and Provider Services.

7. APPENDIX: ABBREVIATIONS

ASP – Attribute Service Provider

CIASP – Company Identity Attribute Service Provider

CRA – Credit Reference Agency

DIATF – Digital Identity and Trust Framework

HSP – Holder Service Provider