Data governance systems for supply chains

Use case: Farming & food production

Document: IB1-DGSSC-2024-REPORT
Version: v2024-12-19

SUPPORTED BY

CATAPULT Digital

MADE SMARTER INNOVATION | DIGITAL SUPPLY CHAIN HUB

Contents

Document title: IB1 Data governance systems for supply chains

Document code: IB1-DGSSC-2024-REPORT

URL https://ib1.org/agriculture/supply-chains

Version: v2024-12-19

Copyright and citations

IB1 Data governance systems for supply chains, v2024-12-19, https://ib1.org/agriculture/supply-chains

The executive summary of this document is available at the URL above. If you would like any further information, would like to get involved or if you need a version of this document in a more accessible format, please contact research@ib1.org.

[1] Creative Commons, CC BY 4.0 Attribution 4.0 International https://creativecommons.org/licenses/by/4.0/

Executive summary

The Digital Supply Chain Hub[2] (DSCH) initiative operated by the Digital Catapult[3] aims to better connect supply chain stakeholders in order to improve efficiency, reduce costs and contribute towards the UK's net-zero targets. Such connections between stakeholders rely on building trust within and throughout supply chains.

Throughout this project Icebreaker One (IB1) focused on defining one specific use case within the food supply chain, through stakeholder engagement and defining an MVP to establish the data infrastructure for trusted data sharing.

Throughout this project IB1 took a use-case-driven and user-needs-based approach to:

1. Prioritise one use case to map the data value chains
2. Establish a governance process including an Advisory Group to ensure the co-design and implementation of a market-wide solution
3. Document a Minimum Viable Product (MVP) for the use case - defining the data infrastructure for trusted data sharing

Doing one thing well: prioritising a use case

The defined use case focuses on one of the most significant inputs for UK farmers, fertilisers. Fertilisers are a significant driver of global greenhouse gas emissions, accounting for 2.6 gigatonnes of CO_2e annually—more than the emissions from aviation and shipping combined.[4]

Farmers have substantial potential to reduce the emissions associated with fertiliser use. Studies suggest that global fertiliser emissions could be reduced by as much as 80% by 2050 through measures such as optimising application techniques, adopting precision agriculture, and transitioning to organic or low-emission alternatives.[5]

At the same time, financial organisations, such as banks, are interested in understanding their financed emissions within agriculture as well as financing the transition to sustainable farming practices. To do this effectively, financial organisations require access to trustworthy data from the food supply chain. However, current methods of sharing data from farm to financial organisation can often be manual and inconsistent. This creates additional costs and inefficiencies as well as risks regarding data quality.

Prioritised Use Case: To access green financing, UK farmers must share assurable data on fertiliser usage reduction with financial organisations.

[2] Digital Catapult (2024) Made Smarter Innovation | Digital Supply Chain Hub https://hub.digitalsupplychainhub.uk/
[3] Digital Catapult (2024) Homepage https://www.digicatapult.org.uk/
[4] Ritchie H et al, 2020, Breakdown of carbon dioxide, methane and nitrous oxide emissions by sector, Our World in Data, https://ourworldindata.org/emissions-by-sector
[5] Gao H, Serrenho A, 2023, Greenhouse gas emissions from nitrogen fertilizers could be reduced by up to one-fifth of current levels by 2050 with combined interventions, Nature, https://www.nature.com/articles/s43016-023-00698-w

Recommendations

In order to fully implement a data governance framework we recommend to:

1. **Validate assurance signals:** UK arable farmers and their supply chain actors **must** be engaged in order validate assurance signal feasibility.
2. **Establish a full governance framework:** An Advisory Group **must** continue to be convened to ensure the co-design and implementation of a market-wide solution, which addresses specific user, technical and non-technical requirements.
3. **Onboard demonstrator partners:** Relevant partner organisations from the supply chain **must** be brought together to deliver a demonstrator that shows assurable data flowing from farm to bank.
4. **Co-design implementation of a technical demonstrator:** Relevant partner organisations **must** co-design and establish the data infrastructure, including assurance metadata records.

Go far together: good governance accelerates adoption

With a complex, multi-stakeholder problem, it's critical that solutions are defined together. For this project, IB1 launched an Advisory Group representing stakeholders from across the food supply chain as a governance mechanism to co-define the use case,and steer the direction of travel for our technical MVP. The group advised on the proposed rules to enable data sharing in an open, automated, scalable, decentralised and interoperable way.

Building better trust in data

Assurance is a person's confidence in the reliability or trustworthiness of something, based on evidence or predefined standards. Assurance Signals can be attached to data using metadata that gives evidence for how trustworthy the data is. Machine-readable assurance signals make this process efficient by allowing computers to quickly verify and assess the data's trustworthiness.

The project's MVP defines a model of how assurance signals can be used to provide a higher degree of trust when it comes to farm's fertiliser reduction, that flows from a farm management system to a carbon accounting platform and on to a financial organisation like a bank. This creates value for multiple stakeholders, in addition to unlocking green financing opportunities for farmers.

The potential for impact

The development of a robust data governance framework for the DSCH ecosystem has the potential to transform UK agriculture by promoting trust, enhancing financial accessibility, and driving sustainability. It aligns with net-zero ambitions while supporting the resilience and productivity of UK farms, ultimately contributing to a more secure and sustainable food supply chain.

Project deliverables

Consensus mechanism: Establish an Advisory Group to enable participants to co-design the rules for governing the exchange of information and value with ecosystem members.

Data governance framework: Lay the groundwork for codifying these rules into a technology solution which maintains a light layer of identity management, governance, definitions, principles and standards for data sharing.

Develop Minimal Viable Product (MVP) The solution will be explored as a complement to other collaboration technology tools that are being developed across the Digital Supply Chain Hub ecosystem.

Engagement and impact

Section	Description	Metrics
Engagement	*Number of people engaged and the degree to which they were meaningfully engaged.*	• Initial outreach to 100 potential Advisory Group candidates. • Convened two Advisory Groups involving 20 separate stakeholders. • Interviewed 12 stakeholders representing different parts of the use case supply chain
Impact	*What has actually been done in terms of tangible impact?*	• Validation of use case by Advisory Group and other stakeholders • Initial direction on viable assurance signals for an MVP

Project context and introduction

Goal of this document

In the context of environmental information, comprehensive financial and non-financial reporting by organisations, IB1 demonstrates the real-world implementation of a programme that can help unlock access to capital for SMEs, while materially reducing complexity and friction in reporting.

Using IB1's collaborative, pre-competitive and open market approach, this project complements ongoing international initiatives around standards, regulation and engagement in the race to net zero.

This document presents the substantial scope and complexity of what is needed, those involved, the progress made to date and plans for the future. It highlights challenges and opportunities and describes the process undertaken to rapidly convene, design and decide on actions. The project's focus, its systems design, market architecture and its implementation elements will improve efficiency, unlock innovation (such as policy and regulatory progress, legal, technical and perception shifts and behavioural changes) and produce value.

This document will aid the understanding of the transformative potential of data sharing and how its connection and use can be unlocked at scale; enabling it to act as a flow of evidence that informs action. While this includes a technology approach, it is not 'about' technology. Rather, it addresses designing the conditions for success that can enable experts, practitioners and organisations to create trust and impact through better access and use of the data needed to make informed decisions.

Audience

Our primary audience are decision-makers and their advisors who wish to understand how to implement change, using multi-sector collaboration and a joined-up, systemic approach to de-risk investment. This includes, but is not limited to, farmers, processors, manufacturers, distributors, financial organisations, policy makers, regulators, trade associations and commercial practitioners working on sustainable supply chains, corporate reporting, finance, carbon reporting solutions and supporting supply chains participants. Many of the principles and lessons herein are applicable beyond the scope described.

Outcomes

In the course of this project, IB1 has delivered the following outcomes:

- A system to create rules around information and value sharing between ecosystem participants that is co-designed with participants.
- Development of a technology solution that is able to monitor and enforce the rules for:
    - Sharing information across supply chains and between technology companies

    - The attribution of value based on that data sharing
- De-risking information sharing between participants resulting in an increase in the exchange of information and value between participants in the Digital Supply Chain Hub ecosystem partners, with an initial focus on the Digital Supply Chain Hub testbeds.
- Improved decision making across stakeholders due to the enhanced transparency and collaboration the system will provide.
- Development of a minimum viable product (MVP).

Research Methodology

The methodology adopted for this research was qualitative in nature, focusing on a comprehensive understanding of data sharing practices in food supply chains. The approach combined primary data collection with secondary data analysis, supported by stakeholder engagement and feedback loops to validate findings.

Ecosystem mapping
To establish a foundational understanding of food supply chains, an ecosystem map was developed. This map identified key components of the supply chain and highlighted relevant stakeholders. The mapping exercise provided a strategic framework for targeted stakeholder engagement and informed subsequent research activities.

Primary data collection
Primary data was gathered through stakeholder interviews, targeting a sample of individuals and organisations identified via the ecosystem mapping process. Over 90 stakeholders were mapped, and 12 interviews were conducted. These interviews offered insights into current practices, challenges, and opportunities for data sharing in food supply chains. Stakeholders spanned various roles across the supply chain, with interviews conducted remotely to maximise participation.

Secondary data analysis
Secondary data analysis involved desk-based research to contextualize findings from primary data. Reports recommended during stakeholder interviews were reviewed, which provided key insights into carbon accounting practices in agriculture. Additional desk research explored existing data-sharing protocols, frameworks, and models offering comparative examples and lessons learned.

Legislative, policy, and regulatory review
A legislative and policy review was undertaken to identify regulatory barriers and potential enablers for data sharing in the sector. This analysis provided an understanding of the legal context within which data-sharing initiatives operate.

Stakeholder validation
Findings were validated through two Advisory Group (AG) meetings comprising diverse stakeholders from government departments, environmental NGOs, consultants, carbon accounting platforms, financial organisations, insurers, trade bodies and academia. The

initial meeting focused on validating the proposed use case, ensuring its relevance and feasibility. The second meeting concentrated on technical aspects, such as assurance signals required by financial organisations. Feedback from these sessions directly informed the refinement of the research findings and recommendations.

Methodological considerations

New sector engagement

Agriculture is a new sector for IB1, requiring the establishment of new relationships within a short timeframe. This challenge was mitigated through proactive engagement across the supply chain and leveraging introductions between stakeholders. Existing relationships within the finance sector also supported initial outreach efforts.

Sector dynamics

The team had to quickly learn the political and social dynamics of organisations within the supply chain. Support from partners such as Digital Catapult, including Co-chair introductions, facilitated access and accelerated relationship-building.

Farmer engagement

Direct engagement with farmers proved challenging due to the operational demands of their day-to-day business. However, connections were established through intermediaries, such as the Farming and Countryside team at Defra, who facilitated introductions to farmers participating in the Sustainable Farming Incentive (SFI) program.

Despite these constraints, the methodology ensured robust data collection and analysis, with mitigations in place to address challenges. The use of an approach combining qualitative interviews, desk research, and stakeholder validation ensures that the findings are both credible and actionable.

Research findings

Financial landscape of UK farms

Through comprehensive desk research, these insights into UK agriculture's financial landscape were compiled from credible sources, including government reports, industry analyses, and lender publications.

- A significant portion of UK farms carry substantial debt, often exceeding £400,000 for 20% of farms in 2022/23, particularly in the dairy, pig, and poultry sectors. Many farmers rely on loans or refinancing to sustain operations, secured against assets, with tailored options from banks.[6]

[6] Defra (2024) Balance sheet analysis and farming performance, England 2022/23, GOV.UK, https://www.gov.uk/government/statistics/balance-sheet-analysis-and-farming-performance-england/balance-sheet-analysis-and-farming-performance-england-202223-statistics-notice

- Larger farms tend to have higher debt per hectare due to capital-intensive operations.[7]
- Inflation in fuel, fertiliser, and feed costs, along with challenges from Brexit, labour shortages[8], and global events, have strained farm finances.[9]
- Programs like the Sustainable Farming Incentive (SFI)[10] and Environmental Land Management Schemes (ELMS)[11] provide financial support to reduce reliance on debt while encouraging sustainable practices.

Carbon accounting platforms for agriculture

These insights were gathered through a series of interviews with key stakeholders across the agricultural and environmental sectors, including farmers, financial organisations, technology providers, and sustainability experts. The discussions explored the challenges and opportunities in implementing carbon accounting systems for farms, focusing on data reliability, scalability, and integration with financial and regulatory frameworks.

- The lack of standardised protocols across the agriculture sector hinders data comparability and reliability which are needed to streamline integration with financial institutions.
- Supply chain complexities and diverse farming practices add layers of variability that need tailored solutions.
- Accurate emission factors for farms are critical but challenging due to the diversity of agricultural practices and conditions. Factors such as livestock emissions, sequestration, and soil health vary widely between farms, requiring localised data and multi-year averages to improve accuracy.
- Current models often depend on generalised factors, which can misrepresent actual emissions, emphasising the need for farm-specific calculations and continuous refinement of methodologies.
- Accurate carbon accounting methods, such as soil sampling and on-farm inspections, provide trustworthy data but require significant time and financial investment, making scalability a challenge for widespread adoption.
- Many farms lack digital infrastructure or rely on outdated systems like spreadsheets, limiting automated data sharing.
- Farmers are cautious about sharing sensitive data, requiring assurances about privacy, usage, and value exchange.
- Larger farms are better positioned to adopt carbon accounting tools due to economies of scale, whereas smaller farms face resource constraints.

[7] Defra (2024) Balance sheet analysis and farming performance, England 2020/21, GOV.UK, https://www.gov.uk/government/statistics/historic-balance-sheet-analysis-and-farming-performance-england/balance-sheet-analysis-and-farming-performance-england-202021-statistics-notice?utm
[8] Environment, Food and Rural Affairs Committee (2022) Labour shortages in the food and farming sector, publications.parliament.uk, https://publications.parliament.uk/pa/cm5802/cmselect/cmenvfru/713/report.html
[9] Eardley F (2022) Rising cost of agricultural fertiliser and feed: Causes, impacts and government policy, House of Lords Library,https://lordslibrary.parliament.uk/rising-cost-of-agricultural-fertiliser-and-feed-causes-impacts-and-government-policy
[10] Defra (2022) Sustainable Farming Incentive: guidance for applicants and agreement holders, GOV.UK, https://www.gov.uk/government/collections/sustainable-farming-incentive-guidance
[11] Defra (2023) Environmental Land Management (ELM) update, GOV.UK, https://www.gov.uk/government/publications/environmental-land-management-update-how-government-will-pay-for-land-based-environment-and-climate-goods-and-services/environmental-land-management-elm-update-how-government-will-pay-for-land-based-environment-and-climate-goods-and-services

The potential of fertiliser

Fertilisers are a significant driver of global greenhouse gas emissions, accounting for 2.6 gigatonnes of CO_2e annually—more than the emissions from aviation and shipping combined. For many arable farms, fertilisers can contribute to 80% or more of their total carbon footprint, highlighting their central role in agricultural emissions.[12] Addressing fertiliser-related emissions is therefore critical for achieving global climate targets, particularly in agriculture.

Farmers have substantial potential to reduce the emissions associated with fertiliser use through improved practices and innovative solutions. Studies suggest that global fertiliser emissions could be reduced by as much as 80% by 2050[13] through measures such as optimising application techniques, adopting precision agriculture, and transitioning to organic or low-emission alternatives. This demonstrates that with the right interventions, significant progress can be made toward decarbonising agriculture.

Defining the use case

Use case criteria

Defining criteria before exploring use cases ensures alignment with strategic goals, streamlines decision-making, and helps identify the most impactful and feasible opportunities efficiently. As part of this process IB1 defined 4 key criteria:

1. **Impactful**: The use case should have the potential to make a significant contribution toward achieving net-zero carbon emissions.
2. **Understandable**: The scenario should be well-defined and easily comprehensible to participants who are already engaged in similar data-sharing activities.
3. **Scalable**: The use case should demonstrate clear potential for adoption by multiple organisations across various industries or sectors.
4. **Local**: The use case should operate within a limited geographic scope, such as the UK or EU, to simplify compliance with data regulations.

Prioritised use case

To access green financing, UK farmers must share assurable data on fertiliser usage reduction with financial organisations.

Problem statement

Financial organisations, such as banks or lenders struggle to accurately measure a farmer's progress to reduce their emissions as they do not have access to assurable farm data. Proving progress towards net zero may require annual reviews, on-site checks, and remote sensing technology to be deployed. This is currently costly for the farmer and can still generate a wide margin of outcomes depending on data granularity,

[12] Ritchie H et al (2020) Breakdown of carbon dioxide, methane and nitrous oxide emissions by sector, Our World in Data, https://ourworldindata.org/emissions-by-sector
[13] Gao H, Serrenho A (2023) Greenhouse gas emissions from nitrogen fertilizers could be reduced by up to one-fifth of current levels by 2050 with combined interventions, Nature https://www.nature.com/articles/s43016-023-00698-w

models used, emission factors and standards and methods applied. Sharing of this data between farm and lender is not well linked up. In some instances data is shared via email or even USB directly using Excel spreadsheets or PDF files.

User needs

Farmers Needs	Lenders Needs

• access to (green) financing
• an easy way to share data with others
• reduce costs
	• assurable and consistent data on a farms progress towards net zero to:
	  ○ report their financed emissions
	  ○ base lending decisions on

Actors and stakeholders

Primary	Secondary	Wider
Farmers: Collect and share fertiliser use data.	**Lenders**: Provide financing to farms, influenced by reduced fertiliser use. **Technology Providers:** Offer ways to collect and share data.	**Third-Party Auditors:** Validate and provide authoritative assessments of farm data for financial organisations to trust. **Regulatory Bodies**: May have a role in defining frameworks for farms and financial organisations to work together. **Insurance Providers:** May have a role in also incentivising sustainable practices on the farm. **Retailers:** May be interested to track carbon reduction in products due to less fertiliser use. **Water Companies:** May be interested in monitoring agricultural run off **Environmental NGOs:** May want to track progress of the farming industry and use learnings to fund projects.

Goals

Increase British food security whilst also meeting UK net zero targets

Impact(s)

1. **Food Security:** By ensuring that farms remain operational and productive through accessible financing, domestic food production is preserved, reducing the UK's reliance on imports.
2. **Decrease carbon:** Farms are incentivised to adopt more sustainable practices, contributing to environmental goals, as they would have the financial support linked directly to their green efforts lowering CO_2e.
3. **Farm Resilience:** Easier access to finance based on practices rather than assets can ensure the survival of struggling farms, which would otherwise face challenges due to volatile financial market conditions. Create more financing for farms.

Benefits and barriers

Benefits	Barriers
Increased farm productivity: By financing sustainable practices, farms can become more efficient, productive, and profitable. **Reduction in financial risk:** Providing more tailored financing based on operational practices might lower risk for both financial organisations and farms, allowing for more reliable investment. **Preservation of domestic farming:** Sustainable financing could prevent farm closures, maintaining the UK's agricultural capacity and supporting local food systems.	**Technology adoption:** Farms often use outdated systems (Excel or on-premise servers) with limited ability to share data, making it difficult to integrate automated data streams into a bank's system. **Data sensitivity:** Farmers are protective of their data due to the competitive nature of agriculture and are hesitant to share information without clear purpose and performance assurances. **Regulatory gaps:** There's a lack of clear regulatory frameworks connecting farming practices, sustainability measures, and bank financing. **Financial organisations understanding of farm operations:** financial organisations currently focus on physical assets and might not fully understand the nuances of sustainable farm practices, adding complexity to developing appropriate financial products.

Supply Chains Advisory Group

The purpose of an Advisory Group is to gain expert input to programmes while addressing commercial, non-commercial and public needs. For this project, we convened a group of members that accurately represented stakeholders across the Food Supply Chain in order to help shape, co-design and implement a Trust Framework solution.

By leveraging the IB1 community, previous Advisory Group members, LinkedIn, and IB1's newsletter audience we formed a list of 100 potential stakeholders. Then, following a number of introductory calls, presentations of our use case and follow up emails, we secured a group of 20 members. These stakeholders made up a comprehensive range of positions in the Food Supply Chain, namely: environmental NGOs, trade associations, insurance and technology providers. The importance of having such a wide range of stakeholders was critical to avoid siloed work, though we still lacked participation from farmers. Financial organisations also proved difficult to recruit but we eventually secured participation from Lloyds, Rabobank and the Development Bank of Wales.

During the Advisory Group recruitment process we quickly identified Helena Diffey, Policy Team Lead at the Department for Environment, Food and Rural Affairs (Defra), as a suitable co-chair. Helena's work with the Food Data Transparency Partnership[14] was aligned with the focus of this project and her expertise and connections to the wider Food Supply Chain were an integral part of the project's success. Helena, alongside co-chair Frank Wales, Chief Technical Officer, Icebreaker One, helped to steer the meetings while ensuring active participation from our Advisory Group members.

The Advisory Group had a critical role in connecting organisations, providing valuable insights. Louis Willock, Founder of Zero Twenty Fifty[15] and group member echoed this:

> *"Participating in the IB1 Food Supply Chain Advisory Group was an awesome experience. The opportunity to listen and exchange ideas with various members of the supply chain and hear their pain points was an insightful experience. I'd participate in any future groups because of how easy it was to participate in the process and how well IB1 brought it all together and made it flow smoothly. Apart from the excellent real-world insights we gained, the connections we made with other organisations looking to progress data sharing and further advance decarbonisation measures have been indispensable."*

Additional Advisory Group materials:
The Advisory Group scope details the specific group scope and intended outcomes of the group for the duration of the programme. The key insights from each meeting can be found below:

- Advisory group session one blog
- Advisory group session two blog

[14] Defra, Food Data Transparency Partnership (FDTP) https://www.gov.uk/government/groups/food-data-transparency-partnership
[15] Zero Twenty Fifty, 2024, https://www.zerotwentyfifty.com

Assurance signals

As part of our research process through talking with various stakeholders we started to define what assurance signals may look like for our use case. Assurance signals were further discussed within our second Advisory Group meeting.

Financial organisations currently rely on auditors to audit reports to a given international standard and provide a sufficient level of assurance that the data is accurate. This is a pragmatic approach, as there is no standardised form of detailed assurance information, and standardised audits are the only reliable information available.

However, audits are very time intensive and expensive to perform, limiting the scale at which green loans can be written. Assurance signals from across the supply chain can replace these reports to a sufficient level of assurance, and give an indepth view of the process where the assertions of individual organisations can be weighted according to the level of trust.

This will, however, require a cultural change to move from relying on auditors to perform analysis of assurance signals as part of the lending decision process.

Assurance Signals are embedded in the Provenance Record, and signed by the participant who is asserting quality of data. The monitoring and dispute resolution procedures of the Trust Framework enable confidence in these assertions.

Potential assurance signals include:

Audit	The data has been audited to: • a specified international standard • by an industry body
Materials	The measurements of materials used in an industrial process were: • Measured • Derived from other data sources • Estimated
Tracking	Materials are tracked within the supply chain by: • Specific batch • Interchangeable stock from a single supplier • Interchangeable stock from multiple suppliers
Missing data	Data sets are: • Complete • Some values are missing • Some values have been substituted from other sources or are estimated
Correlation	Data: • is from a single source • has been matched to another data source, for example, matching purchases on a bank account

A new technical approach to trust

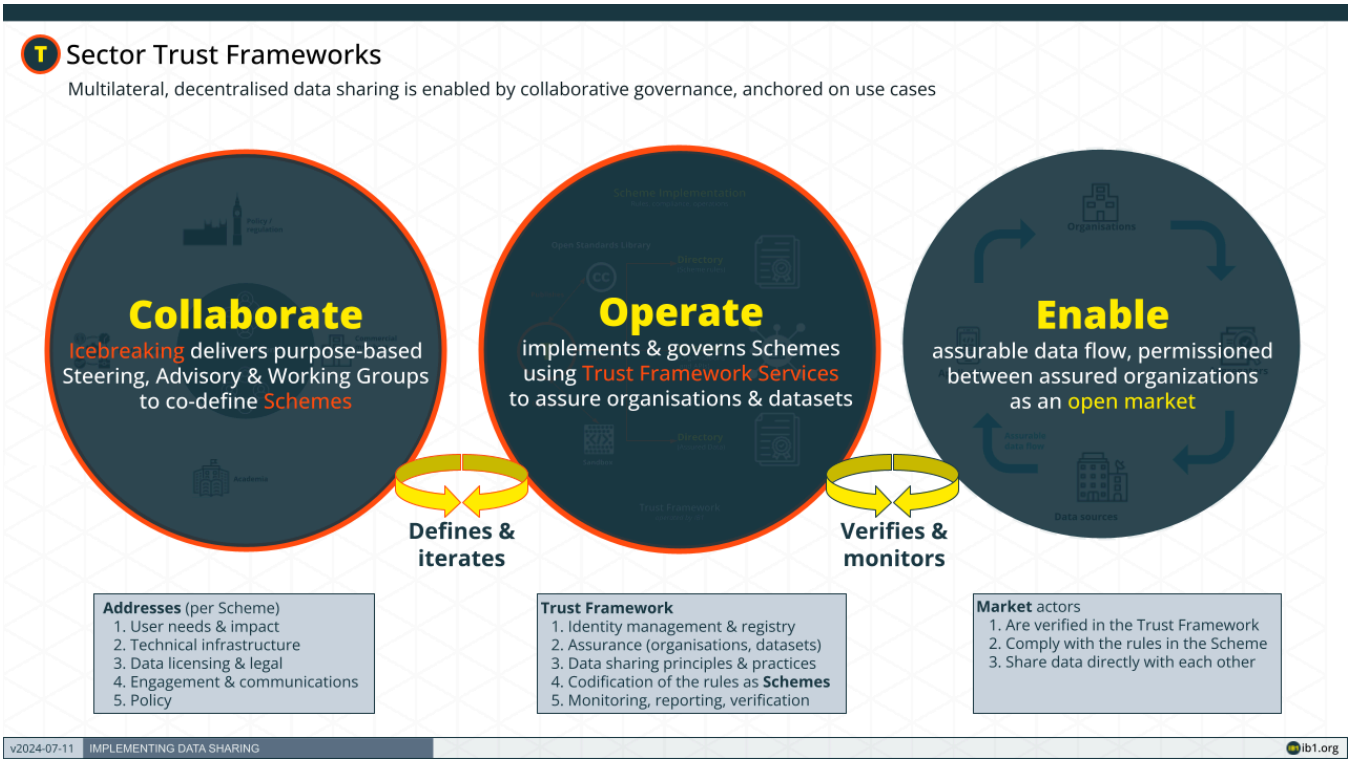
Signed Provenance Records can be used to address trust in the Supply Chain and provide assurance about the data quality to organisations which rely on good data to make decisions.

An example Provenance Record has been created, shown in the MVP (*page 22*) to illustrate the metadata which can be made available from a supply chain. The lender at the end of the supply chain has complete visibility of where the data came from and signals of data quality, and can verify the signatures, and therefore identity, of the participants who are making these assertions.

Establish a Trust Framework

A Trust Framework provides a Directory to establish the **identity of participants** and issue **digital certificates for signing** Provenance records.

A formal governance process convenes industry participants to identify **use cases** and agree **Assurance signals** and how Provenance records are used with the sector.



Identify clear incentives

Each participant will need to do some one-off implementation work to operate within the Trust Framework, and there must be clear incentives to make this investment.

These could be financial, by enabling green loans, demonstrating compliance with regulations, or providing verification for existing schemes such as farm carbon credits.

Attach Provenance Records to data with Assurance signals

A Provenance Record needs to be attached to all data transfers between participants, and stored in logs in such a way that the Provenance Record can be retrieved for any given data point. For rapid adoption, existing data transfer mechanisms should be adapted to include Provenance.

Assurance signals need to be gathered as part of the participant's processes, and embedded in the Provenance Records, and decision makers need to verify the signatures on records and use the assurance information within them.

Gradually move to standardised APIs and security standards

The full benefits of a Trust Framework is realised when the governance process is used to define interchange formats and APIs to eliminate duplication of efforts in the sector.

A solution for supply chains is based on a tried and tested foundation that has delivered Open Banking, Open Energy and Perseus. The implementation codifies the rules into a Trust Framework[16] that specifies how data can be used.

How a Trust Framework operates

A Trust Framework is a very thin layer that enables the implementation of data sharing by:

(a) Verifying and assuring that organisations are who they say they are.
(b) Verifying and assuring legal permission is given to share data with the pre-agreed rules.
(c) Enabling those permissions to be linked to rules for licensing, liability transfer, and legal and operational processes (e.g. open standards for data, APIs, etc.).

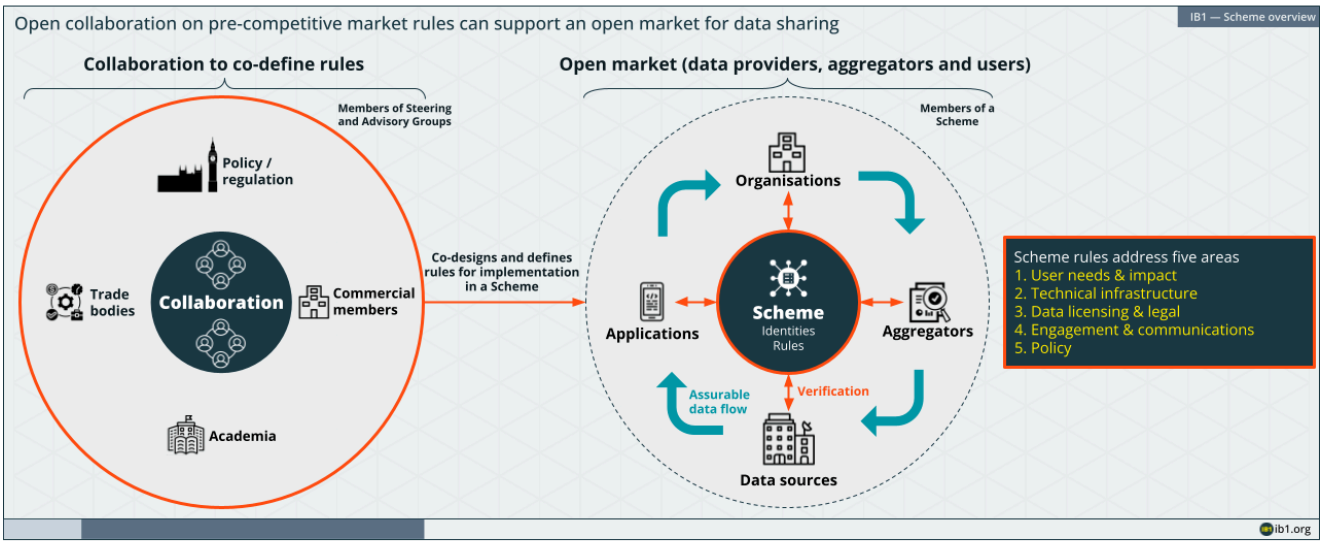
To enable pre-authorised access to data, Trust Frameworks include verification and assurance services for organisations who wish to share, access and use data. Tiers for verification and assurance include verification and assurance at organisational and dataset levels:

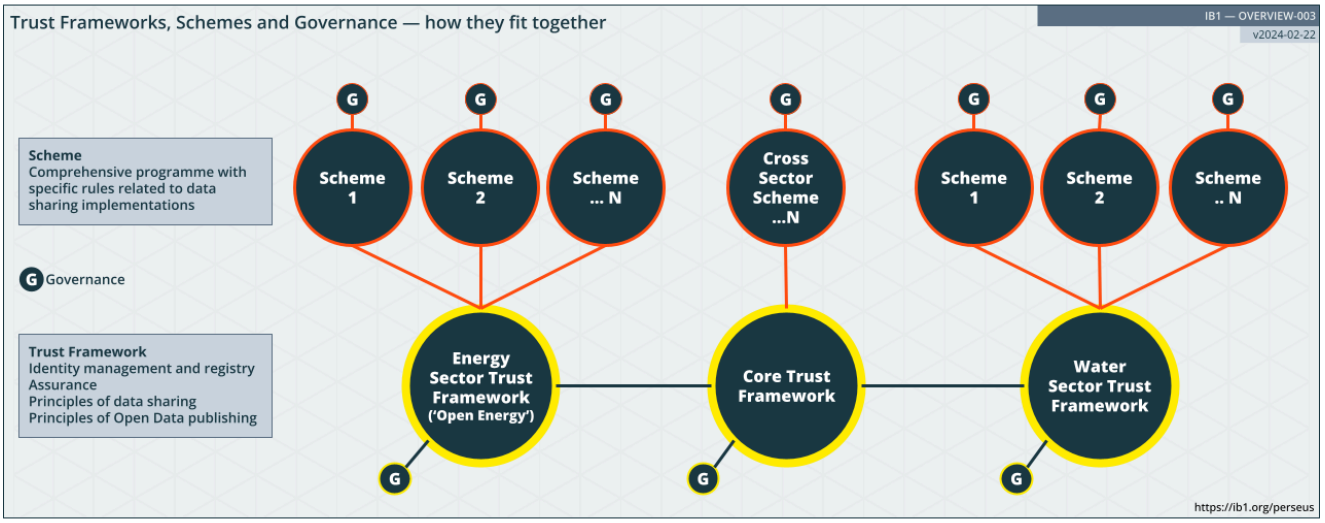
1. **Organisational checks**: for example, confirming the organisation is a legal company entity with a membership agreement. Higher levels include KYC[17] checks.
2. **Organisational policy alignment and/or compliance with policies and standards**: for example, alignment with regulatory guidance, such as Open Data best practices; published data strategy; and, published net zero related reports (e.g. TCFD and PCAF).
3. **Dataset alignment and/or compliance**: for example, license checks for Open Data licenses; machine-readable meta-data; usage of Open Data Certificates;

[16] Icebreaker One, 2024, Trust Frameworks https://ib1.org/trust-frameworks
[17] Swift, 2024, What is KYC?
https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/meaning-kyc

alignment with Data Sensitivity Classes; and, compliance with Trust Framework License Agreements.

The checks are made on two levels: organisational and machine. Organisations sign membership agreements that embody the rules. Machines check each other (continuously) to ensure that they have permission to share.





Innovations that build trust

Demonstrating trust through the supply chain with a scalable technical solution is enabled by four key innovations:

Firstly, a decentralised technical architecture with strong guarantees of identity through signed certificates issued by a Directory. These certificates encode the identity and roles of each party, along with a description of their use of data in a machine readable format. These can be looked up in a machine readable Registry which encodes the rules and standards of the Trust Framework.

Secondly, attaching verifiable Provenance Records to all data transfers which record the precise details of how the data was originated and processed through the supply chain in a lightweight manner. They contain digital signatures from each participant, building up a multi-party record where the identity of the participant making an assertion can be verified without communication with them or a central authority.

Thirdly, a novel legal architecture which combines machine readable licences agreements, executed by signed steps within the Provenance record. This reduces barriers to entry by eliminating the need for individual negotiations between members, with high levels of trust through transparency enabled by digital execution of the agreements for each data transfer, non-repudiable audit trails and monitoring and dispute resolution procedures to enforce rules.

Fourthly, machine readable Assurance signals piggyback on the Provenance records, sending actionable indications of data quality and accuracy alongside each data transfer.

These innovations enable a participant in a supply chain to have full visibility of every organisation that has supplied or processed materials, how they have originated and processed data, and assurance signals to determine how much trust they can place in the data.

They are particularly valuable in an ecosystem which spans multiple countries and jurisdictions, where there is a low level of trust in some participants, as:

- Any attempt to hide or fabricate data can be easily detected, because the expected steps in the Provenance record will not be present, as it is impossible for an organisation to claim another organisation made any assertion about data.
- Precise identity of each participant in the individual supply chain enables analysis over the reliability of their assertions to be factored into the overall decision making process.

Provenance

The records of Provenance are decentralised, passed directly between data providers and data consumers in the data payload. Each participant involved in data origination and processing describes their activity by adding *steps* to a provenance record.

Records are signed using certificates issued by the Directory. After steps have been added by a participant, they sign the entire record, including the signatures of previous participants. This forms an unbreakable chain of signatures, where attempting to alter previous steps would break the final signature.

Assurance signals are included in the Provenance record to piggyback on transport alongside the data and the participant's signatures. While the overall record is standardised across the Trust Framework, the Assurance data is specific to the Scheme.

Provenance and Assurance records are non-repudiable. Once passed to another participant, the timestamped signatures ensure that the creator cannot deny that they signed that record. The Scheme standards require the records are logged and available for audits.

Provenance records contain five types of steps:

- **Origin** - to describe how the data was originated, whether generated by the participant or brought into the Trust Framework from an external source
- **Permission** - to record permissions given by the end user
- **Transfer** - with a description of the dataset and the participants it was transferred between,
- **Receipt** - where the recipient acknowledges receipt of the expected data, and
- **Process** - to record the use of data.

Steps may contain:

- Timestamps
- Permissions relevant to this step
- Participants and Applications (as Directory URLs)
- Dataset / Data Services used (as Directory URLs)
- Processing performed (as Registry URLs)
- URL of endpoints used to retrieve data
- Licences
- FAPI Transaction ID
- Scheme-specific information, including Assurance signals

The contents of each step and format of the Provenance record is documented in *Appendix 1*.

Permission

Within supply chains, the data exchanged is about organisations, not people. While the Provenance Records do take account of data protection laws and consent (as defined by GDPR), they are not relevant to supply chains except in the case where the end user is a sole trader.

Provenance Records record the grant of Permission by end users on behalf of their organisation. The Permission is very precise about what data, and the purpose for which it's used by the provider and any other participant they transfer the data to. The end user may withdraw permission at any time. This precision and control is a key enabled for trust and adoption by the sector.

While records of Permission are included, they do not contain any identifiable information about the end user. Instead, they contain opaque identifiers which can be used to look up information in audit trails. Trust Framework agreements and policies set standards for logging and audit trails to ensure that evidence can be provided for permission.

Implementing assurance signals & provenance records

Assurance signals are defined through the Trust Framework governance process:

- The supply chain ecosystem is mapped to identify participants.
- Use cases are identified to provide definite requirements.
- The use case requirements define the data to be transferred and how it is originated.
- The process of origination is used to identify the variables which affect the data quality and level of assurance.

The signals identified are likely to be descriptions about how the data was collected and factors which affect reliability, rather than quantifiable measurements. The Trust Framework does not define how the signals are used, leaving the data consumers free to interpret them to evaluate the accuracy of the data and how it affects their specific use.

The descriptions of the assurance signatures are used to define machine readable definitions, which are added to the Registry. Software and processes are changed to create Provenance Records with embedded assurance signals, and attach these records to data when it is transferred between participants.

Security

All security choices should meet the FAPI standard, as used in Open Banking, for measurable adherence to standards suitable for sensitive high value data.

By adhering to this standard, all data transfers use Mutual TLS (mTLS), an encrypted transport where each side of a connection provides a digital certificate to prove their identity.

The certificates are issued by the Directory, and assert the identity of the Member, their roles, and the Application for which they are using the data.

The use of mTLS provides a “virtual VPN” between members. All certificates are issued by a private Certificate Authority which signs certificates using a root certificate. Members only accept connections if their certificate is signed using the root certificate, so a successful connection provides assurance of communicating with another Trust Framework member.

As well as checking the root certificate, API servers must check the Roles embedded in the client certificate to ensure the client is a member with the right role to access this data.

Certificates issued by the Directory have an appropriate expiry date, these will be relatively short-lived with automated renewal, complementing a process to halt issuance of certificates to non-compliant or otherwise former TF members.

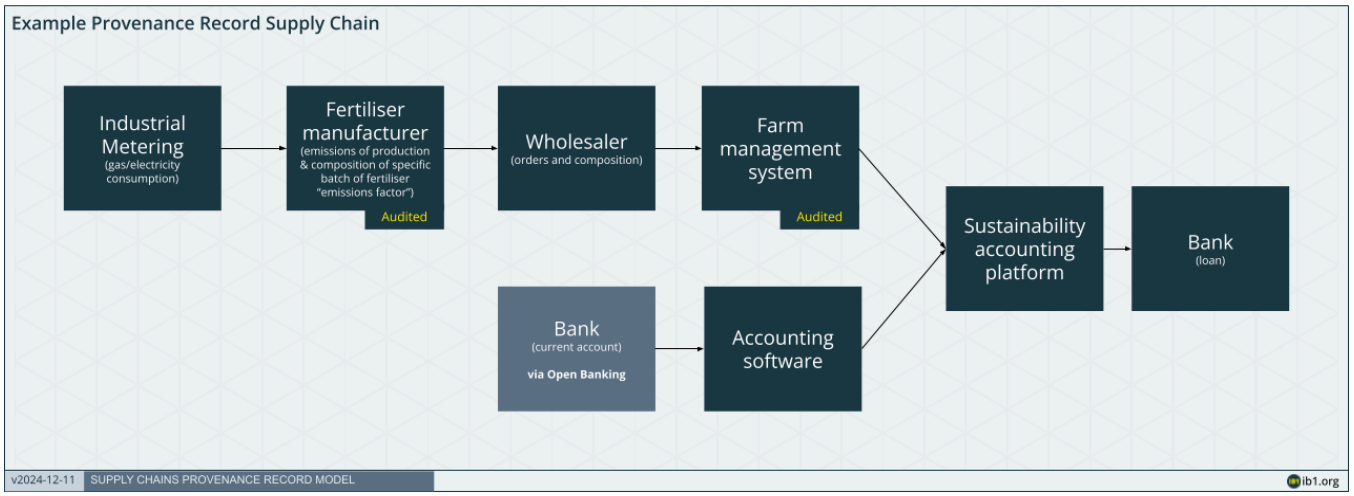
OAuth uses the mTLS client certs for identifying the participant accessing the data. So that leaked OAuth tokens cannot be used, the token embeds the identity of the client certificate. API servers check that the mTLS client accessing the data presents a client certificate that matches the participant that was issued the token.

FAPI requires that every data exchange has a unique identifier, which is used for operational logging, and evidence of data transfer in provenance records.

Minimum Viable Product

To illustrate the technical innovations outlined in this report, an MVP has been created to show a supply chain for fertiliser use on a farm, using a Provenance Record with embedded assurance metadata.

- An industrial metering company measures gas supply to a fertiliser manufacturer and provides consumption data.
- A fertiliser manufacturer supplies to a wholesaler, providing emissions and fertiliser constituents from a specific batch of fertiliser manufacture. Their operations are audited by an external auditor.
- A wholesaler sells some of that batch to a farm, and provides emissions data from the batch.
- A farm management system tracks use of that fertiliser supply as it is applied to the fields on a farm, and provides usage and emissions data to the sustainability accounting platform. Their operations are audited by an external auditor.
- An accounting system uses Open Banking to fetch current account transactions from outside the Trust Framework, and provides information on fertiliser purchase to the sustainability accounting platform.
- The sustainability platform checks data by correlating usage with expenditure, and provides a report to the bank.

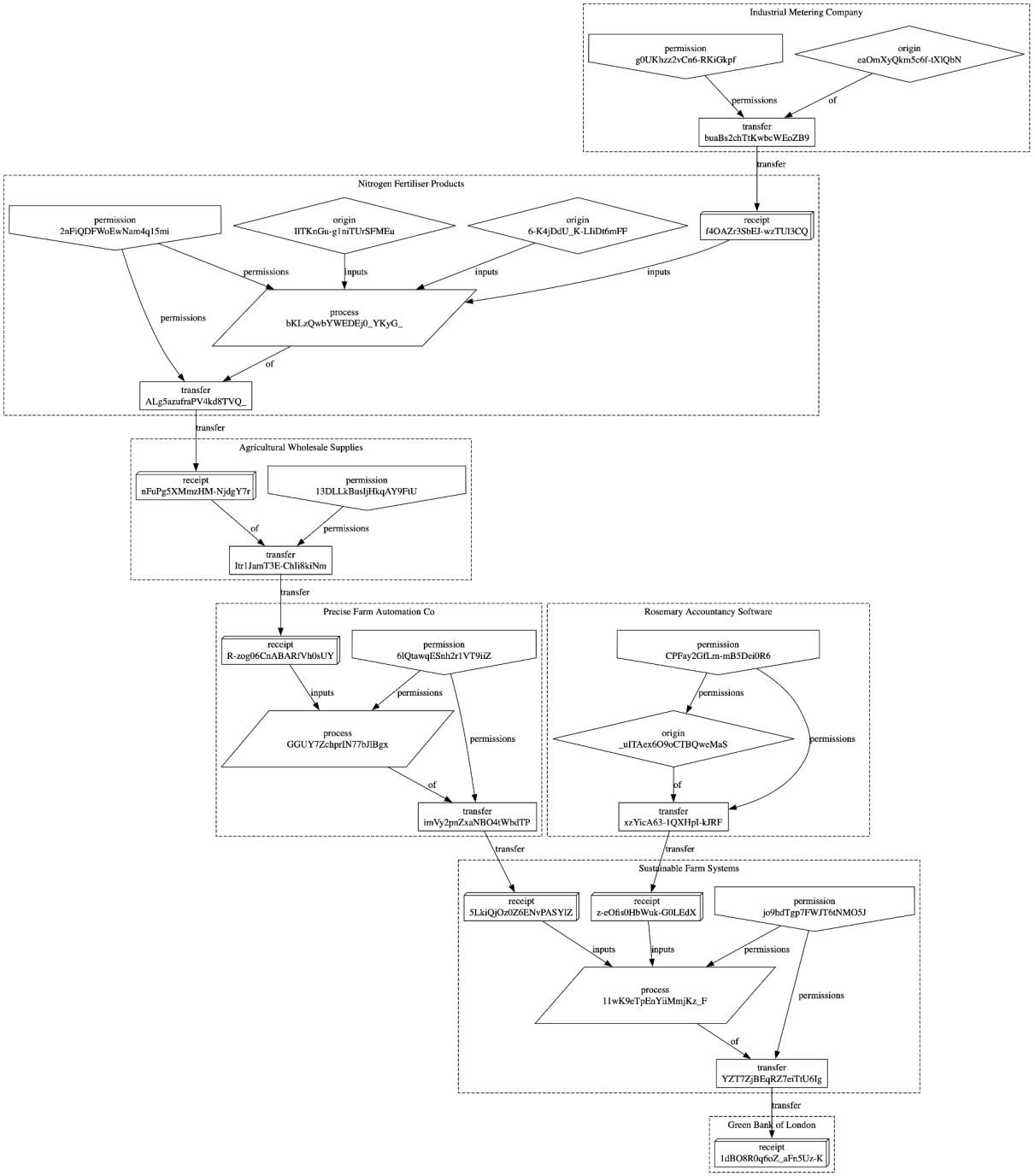


As data is passed between participants in the supply chain, a Provenance Record is built up. The encoded and signed example record[18] allows verification of the digital signatures, and the decoded record[19] allows humans and software to interpret the supply chain.

The format of the encoded and decoded records is specified in *Appendix 1* (*page 30*).

The record represents the actions of the participants in the supply chain with a series of steps.

[18] https://github.com/icebreakerone/dc-supply-chains-2024/blob/main/output/provenance-record.json
[19] https://github.com/icebreakerone/dc-supply-chains-2024/blob/main/output/decoded-record.json



Supply Chain Provenance Record - [End to end diagram](https://raw.githubusercontent.com/icebreakerone/dc-supply-chains-2024/refs/heads/main/output/diagram.svg)[20]

[20] https://raw.githubusercontent.com/icebreakerone/dc-supply-chains-2024/refs/heads/main/output/diagram.svg

Representative code

The representative code of the MVP is shown in an open GitHub repository[21].

Industrial metering company

Permission	The account holder grants permission for metered supply data to be transferred.
Origin	The company originates data from meters that they operate for a give metering period. Assurance: The data was measured directly, but there is missing data.
Transfer	Metered supply data is transferred to the manufacturer under the metered supply data licence, for a given metering period, authorised by the Permission.

Nitrogen fertiliser manufacturer

Receipt	The manufacturer confirms receipt of the data.
Permission	The account holder grants permission for their data to be used to make calculations about the manufacturing process, and transfer data about supply.
Origin	The manufacturer originates two sources of data: 1) Grid intensity data from an external API. Assurance: Data set is complete. 2) Internal metering of materials. Assurance: The data was measured directly, and the data set is complete.
Process	Data from the external metering company, internal metering, and grid intensity data is combined to calculate emissions. Assurance: Missing data has been substituted, and the process has been audited to a specified standard.
Transfer	Data about the supplied goods is transferred to the wholesaler, given an invoice number.

Wholesaler

Receipt	The wholesaler confirms receipt of the data.
Permission	The account holder grants permission for supplied goods data to be transferred.
Transfer	Data about the supplied goods is transferred to the farm automation platform. While no processing is performed by the wholesaler, the invoice number identifies the subset of data transferred. Assurance: Materials have been tracked by specific batches.

[21] https://github.com/icebreakerone/dc-supply-chains-2024/blob/main/output/decoded-record.json

Farm automation platform

Receipt	The farm automation platform confirms receipt of the data.
Permission	The account holder grants permission for their data to be used to manage their farm, and transfer data about materials supplied.
Process	The data has been used as part of farm management. Assurance: There is no missing data, and the process has been audited to a specified standard.
Transfer	Data about the supplied goods used in the specified period is transferred to the environmental reporting provider.

Accountancy software provider

Permission	The account holder grants permission for supply data to be transferred.
Origin	Data is originated from a high street bank using Open Banking, for a specific time period. Assurance: The data is complete.
Transfer	Bank transaction data is transferred to the environmental reporting provider under the bank transaction data licence, for a given period, authorised by the Permission.

Environmental reporting provider

Receipt	The environmental reporting provider includes two receipts from: 1) Farm management system 2) Accountancy software provider
Permission	The account holder grants permission for their data to be used to generate sustainability reports, and transfer the reports to a financial service provider.
Process	A sustainability report has been generated from this data. Assurance: There is missing data, and the results have been checked by correlating data from more than one source.
Transfer	The sustainability report has been transferred to the financial service provider.

Financial Service Provider

Receipt	The financial service provider confirms receipt of the sustainability report.

Detailed Recommendations

In order to fully implement a data governance framework we recommend to:

1. Validate assurance signals
UK arable farmers and supply chain actors must collaborate to test and validate the practicality of assurance signals. This involves designing assurance signals that are both machine-readable and context-specific, ensuring they are easy to integrate into existing farming practices and systems. Stakeholder engagement is essential to understand the variability in data reliability and to align assurance standards across diverse agricultural contexts.

2. Establish a full governance framework
Convening an Advisory Group with representatives across the food supply chain ensures the co-design of a robust governance structure. This framework should address both technical and non-technical user needs while enabling scalable and decentralised data-sharing mechanisms.

3. Onboard demonstrator partners
Key organisations from the supply chain must be brought together to implement a demonstrator that showcases how assurable data can flow seamlessly from farm to financial institutions. The demonstrator should highlight practical applications, such as tracking fertiliser use and linking it to carbon reduction efforts, providing measurable value to farmers, banks, and other stakeholders.

4. Co-design implementation of technical demonstrator
Relevant partners must collaboratively establish the technical infrastructure needed to support data assurance. This includes integrating provenance records with embedded assurance metadata, creating standardised APIs, and ensuring that data privacy and security measures meet regulatory and sectoral standards. The demonstrator should be iterative, allowing for refinement based on stakeholder feedback.

Bibliography

Defra, 2022, Sustainable Farming Incentive: guidance for applicants and agreement holders, GOV.UK
https://www.gov.uk/government/collections/sustainable-farming-incentive-guidance

Defra, 2023, Environmental Land Management (ELM) update: how government will pay for land-based environment and climate goods and services, GOV.UK
https://www.gov.uk/government/publications/environmental-land-management-update-how-government-will-pay-for-land-based-environment-and-climate-goods-and-services/environmental-land-management-elm-update-how-government-will-pay-for-land-based-environment-and-climate-goods-and-services

Defra, 2024, Balance sheet analysis and farming performance, England 2022/23, GOV.UK
https://www.gov.uk/government/statistics/balance-sheet-analysis-and-farming-performance-england/balance-sheet-analysis-and-farming-performance-england-202223-statistics-notice

Defra, 2024, Balance sheet analysis and farming performance, England 2020/21, GOV.UK
https://www.gov.uk/government/statistics/historic-balance-sheet-analysis-and-farming-performance-england/balance-sheet-analysis-and-farming-performance-england-202021-statistics-notice?utm

Defra, 2024, Food Data Transparency Partnership (FDTP)
https://www.gov.uk/government/groups/food-data-transparency-partnership

Eardley F, 2022, Rising cost of agricultural fertiliser and feed: Causes, impacts and government policy, House of Lords Library
https://lordslibrary.parliament.uk/rising-cost-of-agricultural-fertiliser-and-feed-causes-impacts-and-government-policy.com

Environment, Food and Rural Affairs Committee, 2022 Labour shortages in the food and farming sector, publications.parliament.uk
https://publications.parliament.uk/pa/cm5802/cmselect/cmenvfru/713/report.html.com

Gao H, Serrenho A, 2023, Greenhouse gas emissions from nitrogen fertilizers could be reduced by up to one-fifth of current levels by 2050 with combined interventions, Nature
https://www.nature.com/articles/s43016-023-00698-w

Icebreaker One, 2024, Github, dc-supply-chains-2024
https://github.com/icebreakerone/dc-supply-chains-2024/blob/main/output/decoded-record.json

Icebreaker One, 2024, Github, Output Diagram
https://raw.githubusercontent.com/icebreakerone/dc-supply-chains-2024/refs/heads/main/output/diagram.svg

Icebreaker One, 2024, Github, Provenance Records
https://github.com/icebreakerone/dc-supply-chains-2024/blob/main/output/provenance-record.json

Icebreaker One, 2024, Trust Frameworks https://ib1.org/trust-frameworks

Ritchie H et al, 2020, Breakdown of carbon dioxide, methane and nitrous oxide emissions by sector, Our World in Data
https://ourworldindata.org/emissions-by-sector

Swift, 2024, What is KYC?
https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/meaning-kyc

Zero Twenty Fifty, 2024, https://www.zerotwentyfifty.com

Appendix 1

Provenance Record specification

Provenance Records record how data inside the Trust Framework is originated, processed, and transferred between participants, alongside records of the licences covering the data transfer, and any permission granted by end users.

Provenance is recorded in a decentralised manner, with signed records being passed between participants whenever data is transferred. The format is extensible by Schemes.

Encoded and signed container format

Records are composed of steps which describe a discrete component of provenance. Participants create a series of steps, then sign them with signing certificates issued by the Directory.

Steps are serialised as JSON, then Base64 encoded for inclusion in a JSON encoded container. The structure and cryptographic choices borrow from JWS[22], with adaptations for nested signatures and use of x509 certificates to provide keys and identify participants.

Participants receive Provenance Records alongside the data transferred from other participants, and then add additional steps to describe their processing. To preserve the signatures of the participant who created those steps, their encoded and signed form is included as received. To assert that the participant creating the record is relying on these steps and to prevent modification later, this encoded data and signature is included in the data to be signed.

A Python reference implementation of a Provenance library is available at https://github.com/icebreakerone/provenance

[22] https://datatracker.ietf.org/doc/html/rfc7515

Container structure

```
{
    "ib1:provenance":
            "https://registry.core.trust.ib1.org/trust-framework",
    "origins": [
        "JlktJgnddq45PldDsKMf"
    ]
    "steps": [
        [ included steps ],
        "Base64 encoded JSON",
        "Base64 encoded JSON",
        ...
        [
            0, // version
            "certificate serial",
            "signing timestamp",
            "signature"
        ]
    ],
    "certificates": {
        "34983462": ["PEM encoded cert", "issuer serial", ...]
        // ...
    }
}
```

- ib1:provenance
  - The URL of the Trust Framework. All signatures are from certificates issued by this Trust Framework's Directory.
  - This property identifies the structure as a Provenance Record.
- origins
  - An array of the id properties of the origin steps, in the order they appear in the record.
  - Scheme logging policy may require that all participants are able to find all the Provenance records they rely on which match an origin ID.
- steps
  - A *Signed Step List*, *see page 32*.
- certificates
  - (Optional) Map of certificate serial number (as a string) to array of a PEM encoded certificate followed by the serial numbers of issuer certificates in the chain to the root CA certificate.
  - If the certificates are not included to reduce the size of the record, they may be obtained from the Directory identified using the Trust Framework URL in the ib1:provenance property.

Schemes MAY NOT add any top level properties to a Provenance document.

Signed step list format

A *Signed Step List* (the value of the top level steps property) is an array which has one or more elements which are either a Base64 encoded step, or another Signed Step List, followed by a final signature element.

The signature element is an array with 4 elements, in order:

- 0 - the version of the container and steps.
- Serial number of the signing certificate, as a String.
- Timestamp of signature as an ISO8601 date with 'Z' denoting UTC
- String encoded signature, using the algorithm required by the format of the public key in the certificate.
    - All implementations are required to support the "ES256" algorithm from JWS.

To generate the signature:

- Create an array (the signature data array) containing the Trust Framework URL from the ib1:provenance property.
- For each element in the step list array (without the final signature element):
    - If the element is an Array
        - Push "%" to the signature data array
        - Recurse into the Array.
        - Push "&" to the signature data array
    - else
        - Convert the value to a String, and push it to the signature data array
- Join the contents of the signature data array into a single String with a "." separator between elements.
- Sign this String and generate the signature element of the Signed Step List.

Versioning

Two Provenance records need to be combined into a single Provenance record when a process combines data from two sources. These records could be created with different versions of the Provenance specification, as participants may migrate to new formats at different speeds and use historic data.

The version number of the container and the data within the steps is included in the Signed Step List signature element so that Records can be merged without migrating data and breaking signatures. The decoding library must transform the data to a single version.

Schemes must version their data by using different property names.

Steps

Each participant involved in the data origination and processing adds *steps* to the record which describe their activity.

Common properties

```
{
    "id": "3E9qRZRpmHgvAljB1wzh",
    "type": "transfer",
    "timestamp": "2024-09-16T15:32:56Z",
    "scheme": "https://registry.core.trust.ib1.org/scheme/perseus",
    "assurance": { ... },
    "perseus:assurance": { ... },
    "perseus:region": "scheme defined value",
    // ...
}
```

- `id`
  - 15 bytes of random data generated from a cryptographically secure random number generator, base64 encoded.
  - IDs are unique within Trust Framework to enable records to be merged without having to alter any of the signed data.
- `type`
  - See below for step types and their definitions
- `scheme`
  - The Registry URL of the Scheme where this data originated or was processed. Every step must have an explicit scheme property.
  - Steps may have different scheme properties to allow cross-Scheme data transfer, but all Schemes must be members of the same Trust Framework.
- `timestamp`
  - ISO8601 date with 'Z' denoting UTC, of the time the action described in this step took place.
  - The step timestamp may be different to the signing timestamp in the container.
- `assurance`
  - Assurance metadata defined across the Trust Framework.
- `<scheme>:assurance` (e.g. `perseus:assurance`)
  - Assurance metadata defined by a Scheme MUST be represented as a data structure under this property.
  - Multiple assurance properties may be used in a single step for different Schemes.
- `<scheme>:scheme` (eg `perseus:scheme`)
  - Other scheme defined information SHOULD be represented as a data structure under this property.

- `<scheme>:property` (eg `perseus:otherThing`)
  - A Scheme MAY define any additional property where the name is prefixed by the scheme's short name and a :, where representation under the `<scheme>`:scheme property would be inappropriate.
- `_<name>`
  - Properties with a _ prefix are reserved for use by the library to add additional information when decoding and verifying the record.
- `_signature`
  - Added by the library when decoding a record to give information about which participant signed and relied on each step.

Steps do not contain the identifier of the participant who created the step. This identifier is specified by the certificate used to sign this step. The library makes the URL of the participant available in the _signature.signed.member property.

Permission

Permission steps are added to explicitly state that permission has been obtained and provide details of how to find the evidence in the logs. The `id` of this step is used in the `permissions` properties of Origin, Transfer and Process steps to show the permission they rely on.

The `permission` step does NOT need to be created by the same member that is relying on it, where a member is relying on a signed assertion of permission which was obtained by another member.

There is no relationship between the `permission` step and the Permission record created as part of the OAuth mechanism. This is to ensure that the Provenance records are not personal data. Schemes will generally require the participant which generates the `permission` step must be able to use the `timestamp` and `account` properties to locate the evidence for this permission in their audit trail.

```
{
    "id": "V1VFKWxXsXUtiaFEInSF",
    "type": "permission",
    "timestamp": "2024-09-16T15:32:56Z",
    "account": "iuPgAg4c8x4diYfdl6ADN4ULy3ir/B88",
    "allows": {
        "licences": [
            "https://registry.core.trust.ib1.org/scheme/
                  perseus/licence/energy-consumption-data/2024-12-05",
            "https://smartenergycodecompany.co.uk/
                                documents/sec/consolidated-sec/"
        ],
        "processes": [
            "https://registry.core.trust.ib1.org/scheme/
                      perseus/process/emissions-calculations/2024-12-05"
        ]
    },
    "expires": "2025-09-16T15:32:56Z",
}
```

- “type”: “permission”
- account
    - An identifier for the account holder or end user.
    - The identifier MUST be opaque to everyone apart from the participant who provided the data and MUST NOT be the OAuth token.
    - Identifiers must never be reused for different account holders.
    - The value IS NOT required to be the same for every data transfer relating to this account holder or end user across the entire Trust Framework for the account holder’s relationship with the participant, but the creator of the

permission step must be able to match it to the account holder during an audit.

- `allows`
  - A statement of the things that the permission is sufficient to use or do:
    - `licences`
      - An array of Licence URLs.
      - These may be Registry URLs, or external licences, eg the SEC licence for smart meter data by an EDP)
    - `processes`
      - An array of Process URLs
- `expires`
  - Timestamp of when the permission expires, when processing and transfer must cease. The Scheme may require that stored data is deleted.

Origin

This step describes how data is originated, whether by the participant, or brought into the Trust Framework from an external source.

A Provenance record must contain at least one origin step. It may include more than one when Provenance records are merged.

The `id` value is copied to the top level `origins` property.

```
{
    "id": "4cN6b85eT7F5MCTTxhiI",
    "type": "origin",
    "timestamp": "2024-09-16T15:32:56Z",
    "scheme": "https://registry.core.trust.ib1.org/scheme/perseus",
    "sourceType": "https://registry.core.trust.ib1.org/scheme/
                                            perseus/source-type/Meter",
    "origin": "https://www.smartdcc.co.uk/",
    "originLicence": "https://smartenergycodecompany.co.uk/
                                    documents/sec/consolidated-sec/",
    "external": true,
    "permissions": ["V1VFKWxXsXUtiaFEInSF", ...],
    // ...
}
```

- `“type”: “origin”`
- `sourceType`
  - Registry URL of the type of source of data.
- `origin`
  - A URL describing the origin of the data.
- `originLicence`
  - The URL of the licence which applies to the data, if a licence explicitly applies.

    - When bringing open data into the TF, this will be the URL of the licence document specified by the owner of that data.
- `external`
    - Flag to note whether data was generated by a party who is not a member of **this** Trust Framework.
- `permissions`
    - If Permission has been granted by the account holder (usually using an OAuth issuer), the ID of one or more Permission steps that are being relied on to bring data into this Trust Framework.
- The Scheme COULD include assurance metadata.

Transfer

Created by a participant to record their transfer of data to another participant.

```
{
    "id": "51H/KU9Yw4VDxLnaIx+O",
    "type": "transfer",
    "timestamp": "2024-09-16T15:32:56Z",
    "of": "4cN6b85eT7F5MCTTxhiI",
    "to": "https://directory.core.trust.ib1.org/member/387262",
    "scheme": "https://registry.core.trust.ib1.org/scheme/perseus",
    "standard": "https://registry.core.trust.ib1.org/scheme/
                perseus/standard/energy-consumption-data/2024-12-05",
    "licence": "https://registry.core.trust.ib1.org/scheme/
                        perseus/energy-consumption-data/2024-12-05",
    "service": "https://api.example.com/v1/consumption",
    "path": "/readings",
    "parameters": {
        "measure": "import",
        "from": "2023-10-18Z",
        "to": "2023-10-19Z"
    },
    "permissions": ["V1VFKWxXsXUtiaFEInSF", ...],
    "transaction": "CDBDBE88-7263-4541-8F01-9CB9DC12025D",
    // ...
}
```

- `“type”: “transfer”`
- `of`
    - The `id` of a previous Origin, Process or Receipt step to identify the data transferred.
- `to`
    - The Directory URL of the participant that the data has been transferred to.
- `standard`

    - URL of Scheme Catalog Requirements document in the Registry, which defines the API used.
- `licence`
    - The licence governing the use of the data.
- `service`
    - The Directory URL of the instance of this type of data source (the ID allocated by the participant for their DCAT catalogue entry)
- `path`
    - The path from the OpenAPI file for the specific endpoint used within the data service.
- `parameters`
    - Any parameters used for the API call, excluding any which contain personal data.
- `permissions`
    - If Permission has been granted by the account holder (usually using an OAuth issuer), the ID of one or more Permission steps that are being relied on to make this transfer.
- `transaction`
    - FAPI transaction ID

Receipt

Confirmation that a data transfer has taken place to the satisfaction of the receiving party. Complete Provenance records will contain matching Transfer and Receipt pairs, where the sending participant creates and signs a Transfer step to assert what they did, and the receiving participant creates and signs a Receipt step to assert they received some data and the Transfer step meets their expectations.

```
{
    "id": "1Qo4LTEXAG7SMP1Z6t7a",
    "type": "receipt",
    "timestamp": "2024-09-16T15:32:56Z",
    "scheme": "https://registry.core.trust.ib1.org/scheme/perseus",
    "transfer": "3E9qRZRpmHgvAljB1wzh"
}
```

- `“type”: “receipt”`
- `transfer`
    - The ID of the transfer step which is being confirmed.
- Assurance data COULD be included.

The participant confirming receipt is implied by the signature.

The receiving party is expected to verify the transfer step before adding a receipt step, including:

- `to` is the URL of the receiving party
- `standard`, `licence`, `service` and `path`
- `parameters` matches the API call (unless varied by the Scheme)

- `account` is present if an OAuth token was used, otherwise not present
- The step is signed by the expected participant.
- Any other requirements in the Scheme rules

Process

Data processing performed on one or more input data sets.

```
{
    "id": "4cN6b85eT7F5MCTTxhiI",
    "type": "process",
    "timestamp": "2024-09-16T15:32:56Z",
    "scheme": "https://registry.core.trust.ib1.org/scheme/perseus",
    "inputs": [
        "4cN6b85eT7F5MCTTxhiI",
        "RkAnE+6fwkGzRiMVZqu+"
    ],
    "process": "https://registry.core.trust.ib1.org/scheme/
                    perseus/process/emissions-calculation/2024-12-05",
    "permissions": ["V1VFKWxXsXUtiaFEInSF", ...],
    // ...
}
```

- `“type”: “process”`
- `inputs`
    - Array of IDs of other steps in this record which were used as inputs to the process.
    - Only origin, receipt and process steps can be used as inputs.
- `process`
    - Registry URL of the process performed on the data
    - This property may be omitted (where permitted by the Scheme), in which case the `_signature.signed.application` property identifies the data processing.
- `permissions`
    - If the processing relies on Permission being granted by the account holder, the ID of one or more Permission steps that are being relied on for this data processing.
- Assurance data COULD be added if the process identifies anything relevant to the scheme.

The Application URL which performed the process is not included as it is within the certificate. It is available in the `_signature.signed.application` property added on decoding the record.