UN Transparency Protocol

Table of contents:

        - W3C Decentralised Identifiers
        - ISO Product Circularity Data Sheet
        - CEN CENELEC Digital Product Passport Framework
        - ISO EPC Information Services
- Business Case
    - The Business Case for UNTP implementation
    - Stakeholder Motivations
    - Business Case for Industry.
    - Business Case for Government.
    - Community Activation Program.
    - Value Assessment Framework.
- Business Case for Industry
    - Industry Cost Benefit Model
    - Benefits - Revenue Uplift
        - Market Access
        - Unit Price Uplift
        - Anti-Counterfeiting
    - Benefits - Cost Reduction
        - Compliance Costs
        - Finance Costs
            - Access to Trade Finance
            - Reduced Finance Costs
            - Improved margins
            - Cost of Goods Sold
        - Digitalisation Efficiency
    - Benefits - Corporate Value
        - Brand Reputation
        - Improved Disclosures
    - Costs - Sustainable Practices
        - Process Improvement
        - Audits & Certification
    - Costs - Transparency System
        - Capital investment
        - Operational costs
    - Industry Business Case Template
- Business Case for Government
    - Regulator Cost Benefit Model
        - Benefits - National Economy
        - Benefits - Compliance Outcomes
        - Benefits - Government Efficiency
        - Costs - Implementation
        - Costs - Operational
        - Regulator Business Case Template
- Introduction
- CAP delivers value to industries and creates a flywheel of adoption
- CAP supports a structured approach to extension development and adoption
- A successful UNTP extension project is a team effort

- A UNTP extension team requires specialist skills
- CAP membership provides access to valuable resources
- Starting a community is simple
- Ongoing Value Asessment
- Case Studies
- Specification
  - Architecture
  - Verifiable Credentials Profile (VCP)
  - Digital Product Passport (DPP)
  - Digital Conformity Credential (DCC)
  - Digital Traceability Events (DTE)
  - Digital Identity Anchor (DIA)
  - Identity Resolver (IDR)
  - Decentralised Access Control (DAC)
  - Sustainability Vocabulary Catalog (SVC)
- Architecture
  - Overview
  - Principles
  - UNTP conceptual overview
    - The data
    - Finding the data
    - Securing the data
    - Understanding the data
    - Valuing the data
  - UNTP for one product
  - UNTP for a value chain
- Verifiable Credentials
  - Overview
  - Business requirements for UNTP application of VCs
  - Verifiable Credential Profile
    - VCDM profile
    - DID methods
    - Render Method
    - Presentations
  - Vocabularies
  - Roadmap
- Digital Product Passport
  - Artifacts
    - Stable Releases For Implementation
    - Release for Pilot Testing
    - Latest Development Version
    - Version History
    - Default Render Template
    - Sample Credential
  - Overview
  - Conceptual Model
  - Requirements

- Logical Model
  - Core Vocabulary Documentation
  - DPP Documentation
- Implementation Guidance
  - Verifiable Credential
  - Product
  - Dimensions
  - Materials Provenance
  - Emissions Scorecard
  - Circularity Scorecard
  - Traceability Information
  - Conformity Information
- Conformity Credential
  - Artifacts
    - Stable Releases For Implementation
    - Release for Pilot Testing
    - Latest Development Version
    - Version History
    - Default Render Template
    - Sample Credential
  - Overview
  - Conceptual Model
  - Requirements
  - Logical Model
    - Core Vocabulary
    - DCC Documentation
  - Implementation Guidance
    - Verifiable Credential
    - Conformity Attestation
    - Authorisations (Endorsements)
    - Conformity Certificate and Auditable Evidence (Secure Link)
    - Scope (Conformity Assessment Scheme)
    - Conformity Assessments
  - Sample
- Digital Traceability Events
  - Artifacts
    - Stable Releases For Implementation
    - Release for Pilot Testing
    - Latest Development Version
    - Version History
    - Visualization
  - Overview
  - Conceptual Model
  - Requirements
  - Logical Model
    - Core Vocabulary Documentation
    - DTE Documentation

- Critical Raw Materials Transparency Protocol

About the UNTP

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

The United Nations Transparency Protocol (UNTP) aims to support governments and industry with practical measures to counter greenwashing by implementing supply chain traceability and transparency at the scale needed to achieve meaningful impacts on global sustainability outcomes.

Watch a 15 min overview of UNTP or continue learning more below:

Incentives for sustainable supply chains are increasing

Incentives for sustainable supply chains are increasing fast.

- Regulations such as the European Regulation on Deforestation (EUDR) and Carbon Border Adjustment Mechanism (CBAM) will present market access barriers or increased border tariffs for non-sustainable produce.
- These regulations impose due diligence obligations on entire supply chains, not just final products. Penalties for repeated non-compliance can be as high as 4% of global revenue.

- Financial institutions are rapidly moving to ensure that capital is preferentially focussed on ESG assets. According to Bloomberg, within a few years, around $50 Trillion or one third of all global assets under management will be ESG assets.
- Consumer sentiment is driving purchasing decisions to favour sustainable products. At the same time, consumers are increasingly mistrustful of unverifiable claims and look for third party certification based on trusted standards.

But endemic greenwashing risks devaluing the incentives

Greenwashing is a term used to describe a false, misleading, or untrue action or set of claims made by an organization about the positive impact that a company, product or service has on the environment or on social welfare. Just as the incentives described above provide a strong motivation for genuine sustainability in products, so they also provide stronger motivations for greenwashing.

The evidence from multiple research activities is that greenwashing is already endemic with around 60% of claims being proven to be false or misleading. This presents a significant threat to sustainability outcomes. But there is room for optimism because around 70% of consumers expect higher integrity behaviour and are willing to pay for it. There are two plausible pathways ahead of us.

To win the race to the top, fake claims need to be hard to make. The best way to achieve that is to make supply chains traceable and transparent so that unsustainable practices have nowhere to hide. But, to have any impact, the traceability and transparency measures must be implemented at scale.

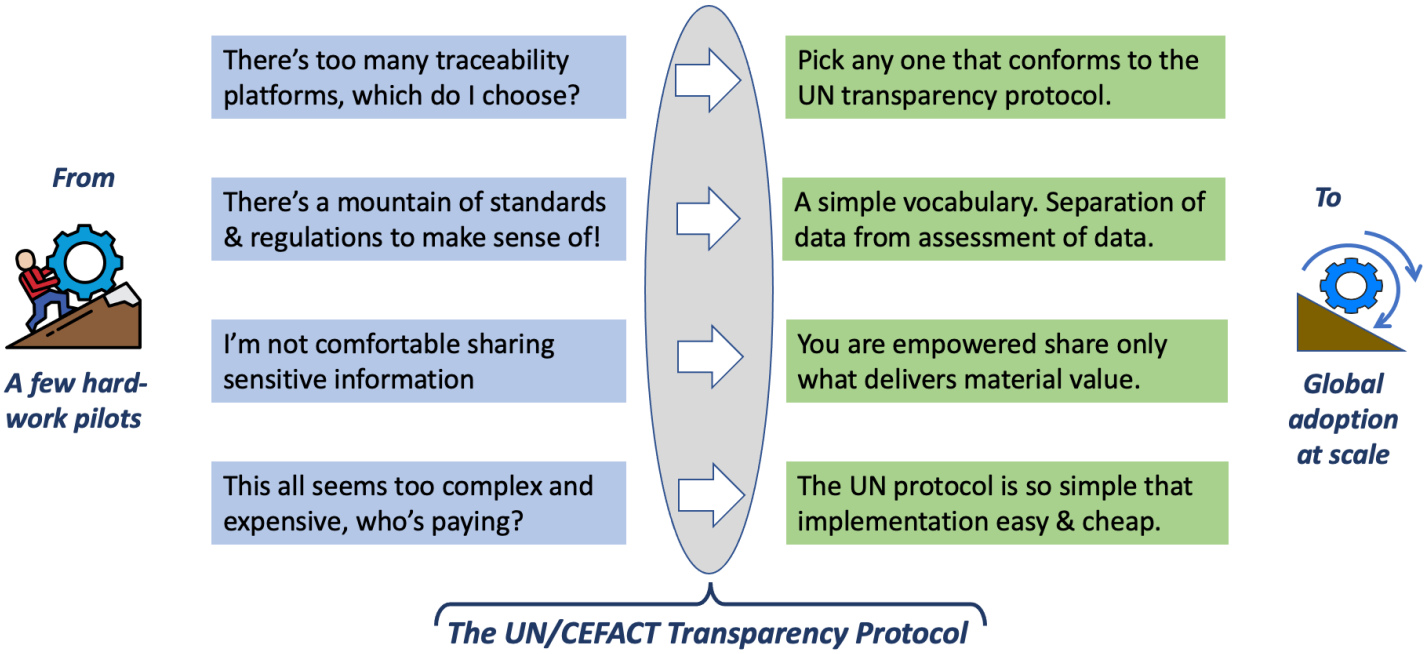
Challenges

The world's supply chains must reach to the point where digitally verifiable traceability and transparency information is available to meet regulatory compliance, satisfy investors, and motivate consumers for the majority of products on the market. However, achieving transparency at that scale presents some challenges.

- **Which software to choose?** There are many traceability & transparency solutions on the marketplace. Many expect all actors in a given value chain to subscribe to the same platform in order to collect the data for end-to-end traceability. However, just as expecting your customers and suppliers to create accounts at your bank so that you can pay them is not rational or practical (that's why inter-bank payment standards exist), so the adoption of all actors in value chains to one platform is also not feasible or scalable. The UNTP is a standard protocol, not a platform, and assumes that supply chain data remains with each natural owner. So the answer to "which software to choose?" is "pick any, so long as it conforms to the UNTP".
- **Coping with a growing mountain of ESG standards and regulations.** The current count of ESG standards and regulations around the world runs into the thousands. Some are specific to particular commodities, jurisdictions, or ESG criteria and some cover multiple dimensions. There is very significant overlap between them and very little formal mutual recognition. The consequence is that it becomes very challenging for supply chain actors that sell to multiple export markets to know which criteria matter and how to demonstrate compliance. There is a risk that too much of the available ESG incentive is spent on demonstrating compliance and too little is left for implementing more sustainable practices. The UNTP does not add to the complexity by defining more ESG standards. Rather it seeks to minimise cost of compliance by making it simpler to test on-site ESG processes and data against multiple ESG criteria. Essentially this is about implementing a sustainable practice once and then re-using it to satisfy multiple overlapping criteria.
- **Protecting confidential information.** "Sunlight is the best auditor" and so verifiable transparency is the best greenwashing counter-measure. However, increased supply chain transparency for ESG purposes also risks exposure of commercially sensitive information. A viable transparency protocol must allow supply chain actors to share ESG evidence whilst protecting sensitive information. Rather than dictate what must be shared and what should not, the UNTP includes a suite of confidentiality measures that allow every supply chain actor to choose their own balance between confidentiality and transparency. The basic principle is that actors should be empowered to share only what delivers value.
- **Making a business case for implementation.** Each supply chain actor (or their software provider) will need to make a viable business case for implementation of the UNTP. The transparency incentives discussed in this section represent the benefit side of the equation. To keep the cost side as low as practical, UNTP has a strong "keep it simple" focus and offers a suite of implementation tools to further reduce cost. Some sample business case templates are provided to help actors make their case for action.

The United Nations Transparency Protocol (UNTP)

The UNTP provides a solution to the transparency challenges facing the world's supply chains. By implementing a simple protocol that can be supported by existing business systems, stakeholders will realise immediate benefits and will become visible contributors to the sustainability of global supply chains.



Presentations & Videos

- Short UNTP Presentation PDF PPT
- Longer UNTP Presentation PDF PPT
- Video presentation (15 mins) Youtube

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Goals

The primary goal of UNTP is to make significant reductions in the incidence of greenwashing by giving unsustainable behaviour nowhere to hide. This will also uplift the value of legitimate ESG credentials from supply chain actors that have implemented sustainable practices. UNTP will have achieved it's purpose when

Goals	Description
Most supply chain shipments are accompanied by verifiable ESG performance data.	In complex supply chains this means that at each supply chain step verifiable product and ESG information accompanies products via a Digital Product Passport.
Greenwashing is a niche activity that is easily detected and quickly penalised by markets and regulators.	Businesses that chose not to share verifiable information about their products are assumed to be doing the wrong things from an ESG perspective and therefore get lower prices for their products or lose access to markets.
Products with the best sustainability characteristics enjoy the greatest market access and price uplift.	Sharing data about your products becomes a competitive advantage and your business choses to compete on the basis of high quality information.

Target Audience & Benefits

All stakeholders in the global supply chain have a role to play and benefits to realise through implementation of the UNTP. As explained in the Architecture Overview, the UNTP is a decentralised architecture where actors can be issuers, or subjects, or verifiers of digital credentials. In many cases, actors will be issuers of some credentials, subjects of others, and verifiers of others. Therefore, the stakeholder roles and benefits described here are separated into the issuer, subject, and verifier roles as appropriate.

Regulators

Regulators define rules, issue permissions, and manage compliance. By implementing UNTP, regulators will uplift the value of the permissions they issue and improve the efficiency and integrity of compliance operations.

- The primary role of regulators as **issuers** is as a trust anchor. When identity credentials such as business registration certificates are issued as digital verifiable credentials according to UNTP then the subjects of those credentials (trading

businesses) can add strong verifiable identity to their supply chain transactions. Verifiable identity can facilitate green-lane pre-clearance at import border and higher confidence lending from financial institutions. Similarly, when ESG permits and certificates that demonstrate compliance with domestic regulations are issued digitally, then traders can also attach that evidence to their transactions. In short, when regulators act as digital trust anchors, they will be uplifting their balance of trade by improving access to export markets and trade finance for their traders.

- As **verifiers** of increasingly transparent supply chain data, regulators can significantly uplift compliance activities. Rather than depend on unverifiable claims in regulatory reports that are occasionally audited at high cost, regulators can confidently automate compliance assessment on most trade transactions, leaving a much smaller volume of trade for manual compliance and enforcement activities.

Finally, as national authorities increasingly seek to uplift environmental performance through regulatory initiatives such as consumer centric product passports, we recommend that national regulators consider the UNTP as the basis for their national initiatives. By designing national initiatives as UNTP extensions, regulators will not only be able to re-use a rich and tested body of work, but will also reduce compliance costs for their domestic industry because they will be better aligned with international supply chains.

ESG Standards Organisations

Standards organisations include the national and international standards authorities as well as industry led organisations. There are a wide variety of governance arrangements in place that impact the legitimacy and value of the published standards. Unlike regulators, standards bodies do not manage compliance which can be self-assessed, or third party audited by test & certification bodies. There are hundreds of standards organisations which collectively issue thousands of ESG standards, each with dozens of specific conformity criteria (i.e. the rules). Most of these are published as PDF documents. The key role for standards authorities under UNTP is to make their ESG rules machine readable so that they can be accurately referenced in conformity credentials.

- When ESG standards organisations publish their ESG criteria as a machine readable vocabulary then they are empowering their community of certifiers to issue digital conformity credentials that unambiguously reference the scope of the conformity claims so that the credentials can be digitally verified.
- Standards authorities will generally not be issuers, subjects, or verifiers of digital credentials unless they also act as accreditation authorities for third party certifiers that will make conformity assessments - in which case they will be issuers of accreditation credentials as described in the next paragraph.

Accreditation & Certification Organisations

There is a very well established global framework for conformity assessment of entities, processes, and products that has been in place for over 50 years. It provides assurance that products sold on the marketplace meet applicable quality, safety or ESG standards. Under the framework, independent third parties (certifiers) assess products against recognised standards and issue conformity certificates. Furthermore, a global network of mutually recognised national accreditation authorities assess the certifiers to ensure that the conformity certificates are issued by suitably qualified organisations. For example, a manufacturer may claim that their product meets a particular environmental standard. You might ask "how do I know that claim is true?" and the answer would be "because a third party tested the product and issued a certificate". You might then ask "yes, but how do I know that the third party can be trusted?" and the answer would be "because they have been accredited by the national accreditation authority". Despite all this, it's still a relatively simple process to create realistic looking but fake paper

certificates. UNTP provides a standard way to digitally verify this chain of trust that is much harder to fake. UNTP does not demand that every product claim is third-party assessed, nor that every third party certifier is formally accredited, but does make that chain of trust visible where it exists. UNTP also recognises that less formal but still valuable chains of trust can exist - for example a farmer's environmental land management claims might be verified by a community organisation that is endorsed by a well-known global environmental organisation.

- When national accreditation authorities or other well-known and trusted organisations **issue** their accreditations as UNTP standard digital credentials then they are creating a digital identity anchor that empowers verifiers of ESG conformity certificates to decide whether they can be trusted. The **subject** of the accreditation is the third party conformity assessment body. Implementation of UNTP will amplify the value of the accreditation and the brand or 'trust mark' of the accreditation authority.
- When third party conformity assessment bodies (certifiers) **issue** their product ESG certificates as UNTP standard digital credentials then they are empowering verifiers of the ESG certificates to digitally confirm that the certificates are genuine, have not been tampered, and have not been revoked. Furthermore if the digital conformity certificate contains a link to the accreditation credential then the full digital chain of trust is established. Producers, manufacturers, brands & retailers that implement UNTP will also demand digital versions of the conformity credentials that they can attach to their products. Therefore, conformity assessment bodies that can provide UNTP standard digital credentials will be preferred over those that cannot.

Primary Producers & Manufacturers

Most physical products are made of materials that either grow above the ground or are dug out from below the ground. Primary producers such as farmers and miners represent the starting point for most supply chains. Recyclers are a special case and are treated separately by UNTP because they are both the end and the (re)start of circular supply chains. Manufacturers take raw or recycled materials and produce intermediate components or final products. Primary producers and manufacturers collectively represent the upstream feedstock supply chain for the branded products sold to consumers.

- When producers and manufacturers implement UNTP by **issuing** B2B digital product passports (DPP) and linking them to every shipment of goods to their customers, then they are simplifying life for their customers by providing data at the right granularity for them to incorporate their inputs such as scope 3 CO2 emissions into their own product environmental footprint.
- When producers and manufacturers **issue** UNTP traceability events linked to product passports then they are providing provenance evidence that can inform supply chain resilience and preferential treatment decisions by their customers and export market regulators.
- When producers and manufacturers link third party issued UNTP conformity credentials then they are adding trust to the ESG claims in their DPPs that will uplift the value or market access for their products.
- When producers and manufacturers **issue** the complete collection of passports, traceability events, and conformity credentials and link them to product shipments then they will significantly uplift value to their downstream customers by empowering them to easily and verifiably meet their own ESG due-diligence obligations.
- When producers and manufacturers link their issuer identity to a strong identity credential (such as a government business registration or trademark ownership credential) and implement the UNTP anti counterfeiting mechanism then they will add strong anti-fraud measures to their products and preserve the value of their sustainability actions.

Producers and manufacturers are themselves **verifiers** of any UNTP credentials linked to their upstream supply chain. The confidentiality measures defined by UNTP allow supply chain actors to selectively redact upstream credentials before passing

them on to their downstream customers so that ESG evidence can be passed on without revealing commercially sensitive information.

Brands & Retailers

Brands and retailers consume products from their upstream producers and manufacturers and sell to the consumer. Whilst it is of course true that some brands are also manufacturers and that some retail is to business rather than consumers, the key distinction that UNTP makes is between B2B activities vs B2C activities. Sales to the consumer market is highly regulated in most economies and some are starting to develop regulations that also require product passports to support informed consumer choice and/or improved recycling processes. Brands and retailers must meet domestic regulations and face scrutiny from an increasingly greenwashing-aware consumer as well as from environmental activist organisations. The potential for reputational damage and high fines for non-compliance present brands and retailers with a strong motivation to ensure that sustainable practices are in place both for themselves and their entire supply chain.

- When brands and retailers can **verify** UNTP credentials linked to shipments from their upstream suppliers then they can confidently meet their due-diligence obligations and have the rich and verifiable information necessary to issue any consumer-centric product passports required under domestic regulations.
- UNTP should not conflict with local regulations. When international brands and retailers **issue** UNTP product passports, conformity credentials and traceability events across all markets then they are providing a consistent way for consumers to discover and verify ESG performance and are establishing a strong framework for compliance with any current or emerging domestic regulations.
- When brands and retailers request UNTP credentials from their upstream suppliers then they avoiding the challenges associated with imposing specific traceability software solutions on their supply chain. Instead, they are simply requesting conformance with a common standard, irrespective of software platform.
- When brands and retailers that have already made significant investments in GS1 identifiers and standards implement the UNTP, they can follow the GS1 binding to build upon and re-use their existing investments. It should also be noted that UNTP does not impose GS1 solutions on organisations that have not already invested in GS1 standards.
- When brands and retailers link their issuer identity to a strong identity credential (such as a government business registration or trademark ownership credential) and implement the UNTP anti counterfeiting mechanism then they will add strong anti-fraud measures to their products and preserve the value of their sustainability actions.

Recyclers & Refurbishers

Recyclers & refurbishers play a critical role in the transition to a circular economy. Recyclers process used products into raw materials for re-use in new production processes. Refurbishers take old products and restore them for re-use. The goal of both processes is to improve sustainability outcomes by re-using natural resources rather than producing new raw materials. As regulators start to impose minimum recycled content requirements and other circularity regulations, the current linear economic model (produce, use, dispose) will require significant change to provide sufficient recycled materials to meet regulatory goals and consumer expectations. The UNTP is designed to support circular economies by including verifiable information on recycled content of products. UNTP also incentivises manufacturers to design new products to optimise recyclability and provides access to product data to better inform recycling processes.

- When manufacturers optimise their product design for recyclability and provide access to that information via **issued** UNTP passports then they are uplifting the end-of-life value of their products. Recyclers can leverage this data (especially

for high value products like EV batteries) to optimise the efficiency of their recycling processes.

- When recyclers **issue** UNTP passports with their recycled material shipments, they are empowering their customers (manufacturers) to make verifiable claims about the percentage of recycled content in their products. This reduces the due diligence burden and non-compliance risk for manufacturers that face mandated minimum recycled content thresholds.
- When consumers see recycled content claims on products then they can **verify** them with confidence.

Environmental & Human Welfare Organisations

There are a large number of national and global not-for-profit organisations who's purpose is to promote environmental or human welfare causes. Some "trust marks", such as the WWF panda, have very high global brand recognition. Although these organisations don't have the enforcement teeth of regulators, they can strongly influence product market success when their trust mark is added (or revoked).

- When influential ESG trust marks establish well-governed accreditation frameworks and **issue** (or revoke) UNTP accreditation credentials then they are able to participate in the digital trust ecosystem as identity anchors, thereby multiplying the power of their brand to drive sustainable production practices.

Consumers

Consumer sentiment around sustainable production is strong and growing with over 70% of consumers in some economies actively choosing sustainable goods where possible. At the same time cynicism around greenwashing is increasing which acts to devalue sustainability claims. As greenwashing countermeasures such as UNTP and national regulations become widely adopted, it is reasonable to expect that consumers will become familiar with product passports and ESG verification techniques.

- When consumers can confidently **verify** the sustainability performance of products simply by scanning barcodes, QR codes or RFID tags then they will be more likely to choose products with verifiable and trustworthy ESG qualities over that that simply make unverifiable claims. When this behaviour is ubiquitous then consumers will have played a pivotal role in combatting greenwashing and winning the race to the top.
- When products are also equipped with the UNTP anti-counterfeiting measures then consumers can not only **verify** ESG performance but also confirm that the performance is associated with an authentic product and not a fake. Producers, manufacturers, brands, and retailers can be confident that their sustainability investments are not devalued by counterfeit products.

Transport & Logistics Providers

The movement of cargo by sea, air, and land accounts for around 10% of global emissions and, unless transport itself becomes more sustainable, will account for the largest fraction of global emissions by 2050. Transport (especially by road) is therefore a key part of the emissions intensity of a product on the market. In the same way that UNTP makes ESG credentials discoverable from product batch identifiers, so UNTP allows ESG credentials for transport services to be discoverable from consignment identifiers such as waybill numbers. But is it the buyer of goods or the seller fo goods that is responsible to include transportation in the ESG footprint? The UNTP answer is that it follows the INCOTERMS - essentially whoever pays for the

transport has the responsibility to include the transport in their product footprint. This ensures there are no gaps or double counting and that incentives are appropriately aligned.

- When transport & logistics providers **issue** UNTP transport credentials and link them to consignment identifiers then they are providing their customers with quantifiable and verifiable transport related ESG metrics to include in their product footprint. As producers, manufacturers, brands, and retailers seek to drive improvements in sustainability performance they will be incentivised to choose low emissions transportation services. This will uplift the value of sustainable transport services per tonne-kilometre.

Financial Institutions

Financial institutions are under increasing pressure from both regulators and the investment community to grant preferential terms for investment capital to sustainable businesses. The finance industry will increasingly verify sustainable performance via their customer annual reporting according to IFRS sustainability standards. Just as financial transactions such as bills, invoices and payments aggregate up to corporate financial statements such as profit & loss and balance sheets, so corporate level annual sustainability metrics are constructed from operational data such as UNTP digital product passports. Furthermore, at consignment level, trade finance instruments such as documentary letters of credit normally require sufficient documentation for goods clearance to be presented prior to payment release. For cases where goods may be blocked at the border due to non-compliance with ESG regulations, then financial institutions will require ESG compliance evidence prior to releasing funds.

- When banks can use UNTP product passports and conformity credentials to digitally **verify** ESG compliance for shipments covered by letters of credit then they can more confidently release payment.
- When banks that are providing investment capital on sustainability grounds to businesses that have implemented UNTP then there is a clear line of sight from UNTP-based operational processes to IFRS-based corporate ESG performance, thereby reducing the financial risk associated with the investment.

Industry Member Associations

There are over 100,000 industry associations world-wide. Most represent a specific industry sector within a specific jurisdiction. These member associations typically provide advocacy on behalf of the community and offer best practice advice. In many cases the associations define quality standards and branding that distinguish their member's products in the marketplace (eg genuine manuka honey). These member associations are well positioned to assist their members in navigating the complexity of domestic and international ESG standards and in assisting them to implement the UNTP. When a particular association member engages in fraudulent practices then it can quickly damage the reputation of the entire industry. Therefore, member associations are strongly incentivised to ensure that their membership adheres to quality standards and to eject non-compliant members. This includes supporting the adoption of industry-wide sustainable practices and UNTP as the digital evidence of those practices.

- Industry member associations may add value to their membership by developing develop UNTP industry profiles that provide their members with targeted implementation guidance that meets the needs of their industry and jurisdiction.
- Industry member associations may develop training and implementation services, possibly in partnership with local service providers, thereby adding both a valuable service and also a revenue stream for the member association.
- Industry member associations may act as a trusted independent quota managers to counter mass balance fraud amongst their membership. The value of this service would be increased if the industry association is accredited by either

a national accreditation authority or a global environmental or human welfare organisation.

Software Developers

Software developers provide the tooling that is needed to implement UNTP because they hold the data that is needed to **issue** UNTP credentials and they will also consume the data from UNTP credentials that are discovered and **verified**. This category includes enterprise resource planning (ERP) systems, ESG management systems, and traceability platforms. By implementing UNTP, software developers are empowering their customers to participate in global transparent supply chains. For large organisations with heavily customised systems, UNTP implementation may be a customer specific project. For smaller organisations that subscribe to off-the-shelf packages, UNTP conformity is more likely to be simply a new feature in a release roadmap.

- ERP systems are the natural issuers of UNTP product passports and traceability events because they manage the finance and logistics operations around the manufacturing, sales, and shipment of products.
- ESG management systems are the source of the ESG data such as carbon intensity that will populate UNTP product passports as well as the conformity credentials referenced by the product passport.
- Traceability platforms are used to provide traceability maps of the upstream supply chain. Rather than gathering this data by direct enrolment of upstream actors, UNTP provides a means to gather the same data by following verifiable linked data trails.

The three system types described here may exist in separate software products or may be parts of a more integrated system. Some ERP systems also manage ESG data. Some ESG platforms include traceability functions. It is not unlikely that ERP systems, whether through native product features or acquisition or partnerships, will evolve to offer this integrated set of capabilities to their customers. UNTP defines a simple and implementable standard for software developers to empower their customers to connect into global transparent and sustainable supply chains.

Service Providers

The adoption of UNTP by hundreds of millions of micro (under 5 employees) and small (under 50 employees) business will most likely be driven by implementation of UNTP as out-of-the-box capability by their chosen business software systems. However, the adoption of UNTP by tens of millions of medium (under 500 employees) and large (over 500 employees) business will most likely require some business analysis and systems integration investment. To minimise cost and risk, such businesses are likely to seek UNTP implementation support from a marketplace of experienced service providers.

- When service providers such as system integrators develop skills in UNTP implementation then they will be able to offer attractive service packages to their existing customers. They may also be able to leverage UNTP implementations skills to access new customers and markets.

Success Measures

Although reduced greenwashing and improved sustainability are the ultimate goals of UNTP, the most direct measure of success is uptake. Therefore, UNTP will measure uptake by counting the number of pledges (i.e. promises to implement) and

the number of successfully completed conformity tests (i.e. actual implementations). For UNTP to achieve it's goals, uptake will need to exceed the minimum thresholds shown in the uptake trajectory below.

Stakeholder type	2024 pledge	2024 implement	2026 pledge	2026 implement	2028 pledge	2028 implement	2030 pledge	2030 implement
Regulators	10	1	20	10	50	20	200	100
ESG Standards	10	0	20	10	50	20	200	100
Accreditation & certification	20	2	50	25	100	50	300	150
Producers & manufacturers	50	10	500	100	2,000	1,000	10,000	5,000
Brands & retailers	50	10	500	100	2,000	1,000	10,000	5,000
Recyclers & refurbishers	10	0	20	10	50	20	200	100
Transport & logistics	20	2	50	25	100	50	300	150
Financial institutions	10	0	20	10	50	20	200	100
Member associations	20	10	200	100	1,000	500	3,000	1,500
Software developers	20	2	50	25	100	50	300	150
Service providers	20	2	50	25	100	50	300	150

Actual progress towards these targets will be tracked via the Implementations pages.

INFO

Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

UNTP Business Requirements

This page provides a summary of the high level business requirements for UNTP, grouped into 7 categories. Each requirement is linked to the page(s) where the solution to the requirement is defined.

Governance Requirements

This set of requirements aim to ensure that UNTP is governed in an open and transparent manner, is freely available to all, and is extensible to meet specific industry and jurisdictional needs.

ID	Name	Requirement Statement	Solution Mapping
GV.01	Consensus driven process	UNTP development MUST me managed via a transparent and consensus-driven process that is open to contributions from all stakeholders - so that implementers can have confidence that the UNTP will meet their requirements.	Governance
GV.02	Freely available	The UNTP IP MUST be owned by the UN and be permanently free to access and free to use - so that implementers can have confidence that there will never be any fees for use or IP infringement claims.	Governance
GV.03	Backwards compatible	New versions of UNTP SHOULD be backwards compatible with earlier versions and each version MUST remain active and supported for a minimum of 2 years - so that implementers can have confidence in the durability of their investment.	Governance
GV.04	Open source	UNTP implementation tools including reference implementations and test services MUST be available under open source and royalty free licensing - so that implementers can confidently use the tools to minimise their own implementation costs	Tools & Support
GV.05	Extensible	The UNTP MUST define a non-breaking extensions methodology - so that UNTP can be extended to meet specific jurisdictional or industry requirements and so that implementers of a registered	Extensions

ID	Name	Requirement Statement	Solution Mapping
		extension can be confident that their implementation is interoperable with UNTP core.	
GV.06	Reusable extensions	Industry and/or jurisdictional extensions to the UNTP SHOULD also be governed via an open process and released under royalty free license terms - so that implementers of extensions can have same fees & IP confidence as with UNTP core.	Extensions
GV.07	Implementation register	UNTP MUST provide a mechanism for implementers to register their planned and actual implementations - so that implementers can choose to register both their sustainability commitment and conformant solutions for discovery by a global community of users and/or customers.	Implementations

Architectural Requirements

This set of requirements aim to ensure that UNTP is scalable enough to achieve global implementations at a volume of global trade that is sufficient to have a material impact on greenwashing - by building on top of existing industry systems and practices and using the simplest possible framework that meets the goals.

ID	Name	Requirement Statement	Solution Mapping
AR.01	Protocol over platform	The UNTP MUST define a standard protocol that is easily implemented by any business software system - so that every supply chain actor can continue to use their preferred business software without any need for upstream or downstream actors to agree on the use of shared platforms.	Architecture
AR.02	Decentralisation	The UNTP MUST define a decentralised protocol where data is stored wherever the owner chooses - so that supply chain actors retain control of their data and are able to monetise their evidence of sustainable behaviour.	Architecture
AR.03	Natural business	The UNTP MUST accommodate the continued use of existing natural business, product, batch, and shipment identifiers - so that UNTP implementation imposes minimal disruption to existing business processes and can leverage existing business and product registers.	Identifiers
AR.04	Technical maturity	The UNTP MUST accommodate varying levels of technical maturity from (and including) paper based documents up to fully digitalised systems -	Data Carriers

ID	Name	Requirement Statement	Solution Mapping
		so that every implementers of UNTP can confidently proceed without dependency on the capability or readiness of upstream or downstream actors.	
AR.05	Simplest possible core	The UNTP MUST prioritise simplicity by focussing on only the minimum specification that represents the common core needs across different jurisdictions and industries - so that that implementation cost is minimised and interoperability is maximised.	Architecture
AR.06	Re-use not re-invent	The UNTP MUST re-use (rather than re-invent) existing standards (e.g. W3C Verifiable Credentials, GS1 EPCIS, UN vocabularies, etc) wherever they are fit for purpose - so that interoperability is maximised and existing investments in software components is re-used.	Architecture
TT.07	Rules as code	The UNTP MUST define a mechanism to simplify the compliance assessment of entities, products, and processes against the fast growing set of ESG standards and regulations - so that any actor's investment in sustainable practices is easily tested against multiple criteria.	ESG Rules

Traceability & Transparency Requirements

This set of requirements aim to ensure that UNTP provides the traceability and transparency data needed for each supply chain actor to confidently meet their due diligence obligations and customer expectations for verifiable evidence of sustainable practices.

ID	Name	Requirement Statement	Solution Mapping
TT.01	Data carriers	The UNTP MUST define consistent methods for the discovery of data about products from both new and existing data carriers such as ID bar codes, 2D matrix, QR codes, and RFID tags - so that any party that has only a product batch ID or goods shipment ID can find ESG data about that product or shipment.	Data Carriers
TT.02	item/batch granularity	The UNTP MUST provide data at the granularity of the individual items or batch in a shipment so that the downstream actor can easily aggregate their material inputs (e.g. scope 3 emissions) into their own ESG performance data.	Digital Product Passport

ID	Name	Requirement Statement	Solution Mapping
TT.03	end-to-end traceability	Subject to privacy & confidentiality constraints, the UNTP traceability model MUST be able to trace value chains from finished product to raw materials through any number of commercial boundaries (sale of goods), or logistics boundaries (consolidation & deconsolidation), and process boundaries (manufacturing transformation of inputs to different outputs) so that the provenance and ESG footprint of goods can be verified as the sum of component parts.	Traceability Events
TT.04	Sustainability data	The UNTP MUST provide a simple and consistent way to access and verify all available sustainability metrics (eg carbon intensity, deforestation, water usage, fair work, etc) about a given product item or batch - so that product buyers can easily meet their sustainability and due diligence obligations	Digital Product Passport, Conformity Credential
TT.05	Provenance data	The UNTP MUST provide verifiable provenance information (raw material content and manufacturing origin countries) about a given product item or batch - so that product buyers can easily meet their supply chain resilience and goods origin controls.	Digital Product Passport, Guarantee of Origin
TT.06	Circularity data	The UNTP MUST provide a simple mechanism to access circularity data including both recycled content metrics as well as end-of-life recycling information - so that product buyers can meet their recycled content goals and recyclers can optimise their recycling processes.	Digital Product Passport, Circularity Data
TT.07	ESG Vocabulary	Given the volume and diversity of ESG standards and regulations, the UNTP MUST define a simple and scalable mechanism to define both the precise meaning and general category of ESG claims - so that downstream actors can map either the specific criteria or the general category of ESG data confidently.	Vocabulary

Trust & Integrity Requirements

This set of requirements aim to ensure that UNTP provides data that can be be trusted and is resilient to several greenwashing attack vectors.

ID	Name	Requirement Statement	Solution Mapping
TI.01	Trust anchors	Trust in truth of sustainability claims can be established by third party audits, or by attestation of trusted authorities, or by long standing	Trust anchors

ID	Name	Requirement Statement	Solution Mapping
		evidence of sustainable behaviour. The UNTP MUST provide a mechanism to link ESG claims to any or all of these "trust anchors" so that downstream actors can have confidence that claimed ESG performance is true.	
TI.02	Identity integrity	Identifiers of businesses, locations, products, and shipments underpin the UNTP. Therefore, the UNTP MUST provide a mechanism to verify that ESG claims made about products or locations or entities are made by actors that are genuine owners of the identifiers or their authorised delegates - so that downstream actors can be sure that ESG claims are made by parties genuinely authorised to do so.	Identity Anchors
TI.03	Accreditation	Third party audits and assessments add trust. But if the verifier does not know the auditor / certifier then there's a risk that define a mechanism to link third party certifiers to the accreditation authority under which they perform their work so that downstream actors can trust the certificates even when they do not know the certifiers.	Conformity
TI.04	Verification of documents	The UNTP MUST define standard and interoperable mechanisms to prevent spoofing or tampering of any documents issued by upstream actors so that downstream actors can be confident that ESG credentials were genuinely issued by the claimed identity and have not been altered in any way.	Verifiable Credentials
TI.05	Verification of graphs	Evidence of ESG performance in supply chains is not concentrated in one document but rather is distributed along the entire value chain. The UNTP MUST define a mechanism to describe and verify the collection of evidence that is available from chains of linked documents so that downstream actors can verify the full ESG footprint and provenance data for any shipment.	Trust graphs
TI.06	Product substitution	As the brand value of verifiably sustainable products increases, so does the incentive to make fake products and attach them to genuinely verifiable sustainability evidence. The UNTP MUST define an anti-counterfeiting mechanism so that downstream actors can confirm that they have purchased genuine goods.	Anti-counterfeiting
TI.07	Mass balance fraud	Mass balance fraud occurs when a supply chain actor blends sustainable materials with cheaper non-sustainable materials as inputs to a manufacturing process and then claims that the manufactured product is 100% sustainable. The UNTP MUST define mechanisms to detect mass balance fraud so that downstream actors can be confident of the integrity	Chain of Custody

ID	Name	Requirement Statement	Solution Mapping
		of their sustainable supply chain and the value of sustainable products is maintained.	

Security & Confidentiality Requirements

This set of requirements aim to ensure that UNTP provides mechanisms to protect the security and confidentiality of supply chain data, allowing each actor to make their own choices about the balance between traceability & transparency.

ID	Name	Requirement Statement	Solution Mapping
SC.01	Transparency vs confidentiality	The UNTP MUST allow every supply chain actor to choose their own balance between transparency and confidentiality - so that each actor can choose to share only what delivers value whilst protecting the information they deem confidential.	Confidentiality
SC.02	Multi-layered security	Information about products have a range of commercial sensitivity from public data to highly confidential data. The UNTP MUST provide a range of data protection mechanisms that can be applied appropriately so that supply chain actors can choose the right protection level for specific data sets.	Confidentiality
SC.03	Selective redaction	ESG data and credentials from sellers may contain data that buyers do not want to pass on to their own customers. The UNTP MUST define a selective redaction method that allows any supply chain actor to redact information (without affecting the cryptographic integrity) from credentials received from upstream suppliers before passing it on to their downstream customers - so that verifiable ESG data can be passed on without leaking commercially sensitive data.	Confidentiality
SC.04	Revocation	The UNTP MUST provide a mechanism to revoke previously issued conformity certificates when an actor is found to be non-compliant so that downstream actors can be confident of the currency of the ESG assessments they receive.	Verifiable Credentials
SC.05	Availability	UNTP MUST define a mechanism for high availability and long term durability of ESG evidence - so that data can be accessed by verifiers even when source systems are down, and so that data for long-lifetime products such as batteries or building materials can be accessed long after source systems are retired.	Verifiable Credentials

ID	Name	Requirement Statement	Solution Mapping
SC.06	Cryptography	The UNTP MUST support flexibility in cryptographic methods so that new algorithms can be supported as they emerge to meet new challenges such as quantum computing.	Verifiable Credentials
SC.07	Key management	The UNTP MUST provide mechanisms for the discovery of public keys, the protection of private keys, and the rotation of key pairs so that keys remain secure and can be easily chained if compromised.	Verifiable Credentials

Compatibility & Interoperability Requirements

This set of requirements aim to ensure that UNTP is compatible with existing standards for technology, ESG criteria, and supply chain practices so that implementers can maximise the leverage of existing investments.

ID	Name	Requirement Statement	Solution Mapping
CI.01	National regulations compatibility	UNTP conformant data SHOULD be straightforward to map to national ESG regulations so that it can usefully provide the upstream B2B ESG evidence to support national B2C product conformance.	Vocabulary, Extensions
CI.02	Entity ESG reporting compatibility	UNTP conformant ESG data about products & shipments MUST be straightforward to map to entity level ESG reporting obligations so that UNTP transaction level ESG data can be easily aggregated to inform annual ESG reporting that conforms to standards like IFRS sustainability.	Vocabulary
CI.03	ESG standards compatibility	The UNTP MUST be able to support ESG claims against criteria from any ESG standard and MUST provide a mechanism to map those claims to a common vocabulary - so that implementers can align with standards of their choice and verifiers can make sense of the claims even when they are unfamiliar with specific standard criteria	Vocabulary, ESG Rules
CI.04	Credential interoperability (VCs)	The UNTP MUST provide the flexibility to support multiple credential standards such as W3C Verifiable Credentials and Hyperledger Airies Anoncreds - so that ESG data along a value chain can be verified even when different credential standards are adopted by different actors along the value chain.	
CI.05	Blockchain	Whilst some implementers MAY choose blockchain technologies to underpin their solutions, the UNTP MUST NOT require the use of blockchain for conformant implementations - so that implementers that	

ID	Name	Requirement Statement	Solution Mapping
		wish to avoid the costs and complexity of blockchain technologies are free to do so.	
CI.06	GS1 compatibility	GS1 identifiers and standards are ubiquitous at the downstream consumer goods end of most supply chains. The UNTP MUST be compatible with GS1 standards but MUST NOT require the use of GS1 standards - so that supply chain actors that are already invested in GS1 identifiers and standards can maintain and build upon that investment	
CI.07	Other registry compatibility	The UNTP MUST define a mechanism to support existing identity registers so that implementers can continue to leverage existing business identifiers such as tax registration numbers, cadastral lot numbers, shipping container numbers, and so on under UNTP	Identifiers, Extensions

Implementation Requirements

This set of requirements aim to ensure that UNTP is implementable at the lowest possible cost, and that early implementers gain a marketing advantage, and that the impact of implementations can be tracked.

ID	Name	Requirement Statement	Solution Mapping
IM.01	Making a business case	Every UNTP implementer will need confidence that the benefits of their implementation outweighs the cost. UNTP SHOULD provide a set of business case templates so that each stakeholder type can fast-track their decision to proceed	Business Case
IM.02	Open source tools	The UNTP MUST include an open source reference implementation that any supply chain actor can embed into their solutions to help fast-track their implementation.	Tools
IM.03	Conformity testing	the UNTP MUST include a conformance test suite and test service so that each implementer can self-assess their conformance and be confident that their implementations will be interoperable.	Test service
IM.04	Implementation Support	UNTP MUST provide mechanisms for implementers to get either community support or professional support so that they can minimise their implementation risk.	Support

ID	Name	Requirement Statement	Solution Mapping
IM.05	Tracking implementations	UNTP MUST provide a mechanism to track implementations so that uptake and impact can be measured and so that early implementers can publicise their solutions.	Implementations
IM.06	Tracking extensions	UNTP MUST provide a mechanism to track and publish industry & jurisdictional extensions so that new extensions can find and re-use relevant work.	Extensions
IM.07	Tracking outcomes	Although uptake is a simple and concrete success measure, the real purpose of UNTP is to lift the value of sustainable practices by countering greenwashing. Therefore, UNTP MUST develop a set of greenwashing KPIs that can be tracked to assess whether UNTP is having a material impact.	Greenwashing KPIs

Governance

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

The UNTP governance framework follows UN/CEFACT standard governance methodology and is designed to provide implementers with confidence that UNTP:

- is a public good that cannot be captured by any specific commercial interest and is permanently free to use.
- is developed via a consensus based process that ensures it will meet the needs of value chain actors and member states.
- is specific, testable, and rigorously versioned so that implementers can be confident of stability and interoperability.
- is compatible with relevant national and international standards and regulations.

The governance framework described on this page is designed to meet these criteria.

UN/CEFACT Governance Framework

UN/CEFACT is the United Nations Centre for Trade Facilitation and Electronic Business. It was established as an intergovernmental body in 1996 with a mandate to develop standards and recommendations for the facilitation of digitalised and sustainable trade. Although UN/CEFACT is a global body, secretariat functions are provided by the United Nations Economic Commission for Europe (UNECE). The UN/CEFACT mandate, terms of reference, program of work, and related governance documentation is available from the UN/CEFACT policies and procedures. The governance documents are approved by member states at the UN/CEFACT annual plenary.

Standards such as this United Nations Transparency Protocol (UNTP) and recommendations such as Recommendation 49 "Transparency at scale" are developed under the UN/CEFACT Open Development Process (ODP). All contributing participants in UN/CEFACT working groups must register as UN experts with the approval of their country head of delegation. All contributing participants must waive their intellectual property rights (IPR) to any contributions under the IPR policy so that UN/CEFACT can continue to publish freely usable standards and recommendations.

UN/CEFACT maintains formal liaison arrangements with other UN organisations as well as other global standards bodies such as ISO, ITU, and IEC following a memorandum of understanding.

Voluntary Standard

Like all UN/CEFACT standards, the UNTP is a voluntary standard that is not mandated by any regulatory framework. Uptake and implementation will be the result of perceived business value. For this reason, UNTP includes

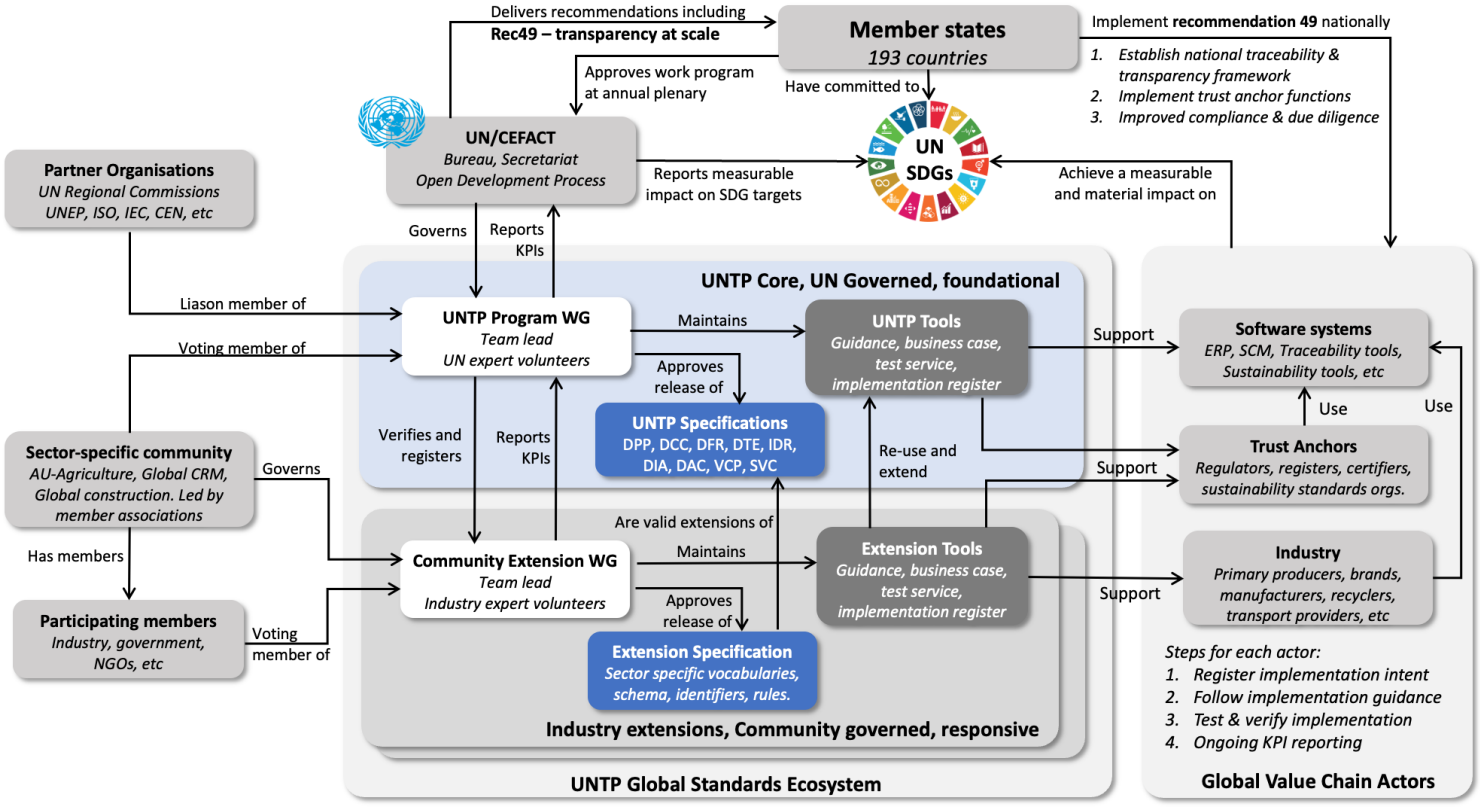
- Business case templates for industry and government)to assist implementers with their cost/benefit assessments.

- A Value Assessment Framework that will collect performance metrics from implementers to track UNTP impact on UN Sustainable Development Goals.
- An extensions methodology and governance framework that provides an incentive for implementations across entire communites led by member associations.

UNTP aims to be the highest value and lowest cost framework for scaling traceability & transparency across global supply chains.

UNTP Governance Details

UNTP is one program within the overall UN/CEFACT governance framework. The diagram below shows how UNTP and recommendation 49 fit within the global UN/CEFACT governance framework and also specifically how UNTP extensions fit within the UNTP governance framework. Extensions are designed to accommodate industry or geographic specific needs of a specific community of implementers and are typically governed by a member association. To be formally registered as UNTP extension, the extension must also be freely available under a Creative Commons Attribution 4.0 International license and must be interoperable with UNTP specifications.



The diagram represents the following key governance concepts:

- The UNTP Program Working Group maintains this site and comprises members from UN expert community and sector specific communities.
- UNTP comprises a suite of version-managed technical specifications as well as some supporting tools that include implementation guidance, business case, best practices, test services, and an implementations register.

- The tooling ensures that implementation is as simple and cost effective as possible and also that implementations are interoperable since all implementations must pass the same test cases.
- UNTP extensions working groups develop industry and/or geography specific extensions of UNTP following a methodology that ensures all extensions remain interoperable with UNTP core implementations and any other industry extension.
- Extensions are governed by the community that creates them, usually led by a representative member association. Extensions will typically include sector specific vocabularies, specific credential schema (eg a livestock passport as an extension of a product passport) and specific rules and constraints such as allowed identifier schemes.
- Extensions must also provide test services to ensure interoperability between different implementers of the same extension specification. The generic UNTP test and reference implementation tooling is re-usable for this purpose.
- All implementers that register their system or business on the UNTP website or an extension website are required to provide some basic KPI reporting (eg number of product passports issued) so that performance metrics can be rolled up from implementer to extension community and then up to UN/CEFACT and member states. The performance reporting framework is defined by the UNTP Value Assessment Framework (VAF) and is designed to capture quantifiable performance measures that can be mapped to UN Sustainable Development Goals and Targets. Anonymised reporting and performance dashboards will be published by the UNTP program.

The diagram shows three classes of implementers within the global value chain.

- **Software systems**, whether commercial or open-source, provide all other implementers with the core technology capability needed to support UNTP. In many cases the underlying software systems supports any industry or geography sector and so would focus on core UNTP conformity, perhaps also supporting some extensions when they have a concentration of customers in a particular industry or geographic sector. UNTP maintains a register of software system implementations.
- **Industry actors** such as primary producers, manufacturers, brands, recyclers, transport services, and so on will generally occupy specific industry and geography sectors and so are more likely to be implementers of one or more UNTP extensions. Software systems used by industry actors will generally have implemented core UNTP and will provide some flexibility to configure and support specific rules required by industry and/or geography specific UNTP extensions.
- **Trust anchors** such identity registers would implement core UNTP specifications such as Identity Resolver and Digital Identity Anchor. UNTP provides certifiers with the opportunity to make their existing product and facility certifications digital and verifiable. Regulators may issue regulatory permits, licenses, and certificates (eg mine permits). Additionally, regulators such as border authorities have the opportunity to automate compliance assessments as verifiers of credentials linked to trade shipments.

UNTP Extension Governance

UNTP extensions for a specific industry and/or geography should be designed and implemented at community level following the community activation program guidance. This helps to ensure interoperability between members of the community - so, for example, a fabric supplier to multiple fashion brands can implement once for many customers. Consequently there is a need for a governing body to manage the specification development and implementation support on behalf of community members. This task is best suited to existing member associations that already represent the interests of multiple organisations within a sector.

It is tempting to think that the scope of extensions could be governed by UNTP to ensure that there are no overlaps or gaps. However, the real world is not as simple as that and it is inevitable that different communities will overlap. For example a

national government critical minerals office may leverage UNTP to create a national traceability and transparency framework in a specific country. At the same time a global member association for a specific mineral (e.g. copper or lithium) may also extend UNTP to support it's global members. Some members will inevitably face both. The UNTP governance approach aims to minimise duplication and complexity through visibility.

- By categorising every extension by both country (using ISO country codes) and industry sector (using UN ISIC codes), cases where multiple extensions overlap become visible. Conversely visibility of gaps provides opportunities and incentives for relevant member associations to fill the gaps.
- By requiring that all registered extensions are public and free to use, any communities that find themselves overlapping with an existing industry and/or country sector can see what has already been done and, if appropriate, re-use the existing work without restriction.
- By providing test services to confirm that each extension remains conformant and interoperable with core UNTP, cross-border and cross-industry interoperability is maintained, thereby reducing the impact of differences between overlapping extensions.

UNTP Consensus Driven Development Process

UNTP development follows an agile and iterative approach with maximum public visibility and seeks consensus for each change.

- Anyone can participate as an observer simply by watching development on this UNTP website and by joining the informal chat channel.
- Anyone can formally join the UNTP working group as a contributing member once they have completed the UN/CEFACT expert registration process which includes formal acceptance of IPR policy.
- Contributing members who wish to propose changes to existing content or contribute new content should raise a new issue using the GitHub issue workflow - that describes the change. Any other contributing member can comment on the issue. In this way, the issue can be used as a permanent record of working group discussion around the specific issue. Some issues like this one on identifiers can be long running whilst others like this one on context file versions can be short and quick to resolve.
- Once the creator of the issue is confident that there has been sufficient exposure and discussion, then a formal request to change content should be lodged - using the GitHub pull request workflow. All pull requests require at least one reviewer to approve the proposed changes and all approved pull requests are discussed at fortnightly meetings. If there are no objections then the changes are merged into the main website. All pull requests remain visible for public scrutiny.
- If there are objections then they are discussed and, hopefully, resolved with full consensus. In the rare case of objections that cannot be resolved by consensus then meeting chair will hold a vote. A simple majority is required to accept the change.
- All meetings are recorded, transcribed, summarised, and published to the UNTP meetings page.
- A google group mailing list is also maintained and can be used by any observer or contributing member. All group emails are archived and searchable.

For participants less familiar with GitHub tools and processes, there is a guidance page on how to write content and how to request changes via the pull request workflow.

UNTP Version and Release Management

Within the UNTP business governance framework, there also needs to be some technical governance to ensure quality and stability of UNTP technical deliverables.

Version Management

All UNTP artifacts are rigorously versioned following semver best practices.

- Version numbers are indicated as a dot-separated triple `{major}.{minor}.{patch}`. For example version 2.3.4.
- `{patch}` version number increments indicate non-breaking bug fixes that do not add new capabilities of features. For example, implementers should see no difference between version 1.4.5 and version 1.4.6.
- `{minor}` version number increments indicate non-breaking enhancements. For example, implementations of version 1.4.5 are still compatible with version 1.5.0 but may not take advantage of new features.
- `{major}` version number increments indicate significant and breaking releases. For example implementations of version 1.5.0 will be incompatible with version 2.0.0 and may fail in unpredictable ways.

Note that 0.x.y versions do not strictly follow semver and may include breaking changes in minor versions. However all versions after 1.0.0 first formal release will strictly observe this versioning process.

Release Management

Every version change is automatically published to the UNTP `test.uncefact.org/vocabulary` end point following a defined URL structure

Linked data vocabulary (test)

- Pattern: `https://test.uncefact.org/vocabulary/untp/{vocab-name}/{major-version}/{artefact}`
- Example: `https://test.uncefact.org/vocabulary/untp/dpp/0/Product`

Schema and context files (test)

- Pattern: `https://test.uncefact.org/vocabulary/untp/{credential-type}/{versioned-file-name}`
- Example: https://test.uncefact.org/vocabulary/untp/dpp/untp-dpp-schema-0.5.0.json

When a given version meets criteria to justify a production release then the governance process will approve a release that will publish the artefacts to the UNTP `vocabulary.uncefact.org` end point.

Linked data vocabulary (production)

- Pattern : `https://vocabulary.uncefact.org/untp/{vocab-name}/{major-version}/{artefact}`
- Example : `https://vocabulary.uncefact.org/untp/dpp/1/Product`

Schema and context files (production)

- Pattern: `https://vocabulary.uncefact.org/untp/{credential-type}/{versioned-file-name}`
- Example: `https://vocabulary.uncefact.org//untp/dpp/untp-dpp-schema-1.1.0.json`

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Relationships To Other Standards And Initiatives

A core principle of UNTP is to avoid re-inventing standards by building upon existing work and maximising interoperability with similar initiatives. In many cases, UNTP provides complementary value to other initiatives (for example by providing a data exchange protocol for business standards). This page provides an overview of related standards and details the relationship with relevant UNTP specifications.

Summary

Standard	UNTP Relationship
W3C Verifiable Credentials (VCDM)	UNTP ensures data integrity by requiring that Product passports, conformity credentials, facility records, and traceability events are issued as W3C verifiable credentials.
W3C Decentralised Identifiers (DID)	UNTP ensures identity integrity by requiring that all credential issuers are identified by a W3C DID that is cryptographically linked to an authoritative register (of organisations or facilities or products)
ISO Product Circularity Data Sheet (PCDS)	UNTP provides a simple and interoperable mechanism to digitalise ISO PCDS using the DPP and DCC `Declaration` structure
CEN/CENELEC Digital Product passport System (CEN DPP)	UNTP will work to enure interoperability where there is overlap (3 of 11 UNTP specifications). For example, whilst CEN DPP will define a specific data carrier and product identifier scheme, UNTP will support many existing industry schemes and so will include the CEN schemes in the list of supported schemes.
ISO Electronic Product Code Information Services (EPCIS)	UNTP Digital Traceability Events present a simplified but conformant subset of EPCIS that is optimised for packaging as verifiable credentials.

Matrix

Standards relationship matrix as downloadable excel (coming soon)

Expanded Descriptions

W3C Verifiable Credentials Data Model

Standard Overview

Credentials like drivers licenses, diplomas, visas, permits, and even invoices are integral to our daily lives. W3C Verifiable Credentials provide a mechanism to express these sorts of credentials on the Web in cryptographically secure, privacy-respecting, and machine-verifiable way.

UNTP Relationship

All UNTP credentials (product passports, facility records, conformity attestation, traceability events) are issued as Verifiable Credentials so that security and integrity is assured irrespective of how the credentials are exchanged. The additional UNTP requirement for VC rendering templates ensures that all UNTP credentials are both human and machine readable. The additional UNTP requirement for VC rendering templates ensures that all UNTP credentials are both human and machine readable. The UNTP VC Profile specification provides further details.

W3C Decentralised Identifiers

Standard Overview

W3C Decentralised Identifiers(DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. The design enables the owner of a DID to prove control over it without requiring permission from any other party. DIDs are often used as the issuer identifier for Verifiable Credentials.

UNTP Relationship

UNTP Verifiable Credentials Profile requires the use of W3C DIDs as the issuer ID of all credentials (DPP, DCC, DTE etc) so that there is cryptographic and non-repudiable proof of the issuer identity. In some cases (similar to very well known websites), a verifier will be able to relate a DID to a well known identity. In most cases, however, the DID may not be known to the verifier - therefore UNTP defines a Digital Identity Anchor which provides a high integrity link between a DID and an identity in an authoritative register such as a national business register.

ISO Product Circularity Data Sheet

Standard Overview

ISO-59040 (also known as the "Product Circularity Data Sheet") defines a standard set of measures and corresponding reporting standard for product circularity. It includes both circular content (i.e. the extent to which the product is made from recycled, refurbished materials) and circular design (i.e. the extent to which the product has been designed to facilitate repair and recycling). The standard is presented as a PDF document with sample reporting layouts.

UNTP Relationship

UNTP does not re-invent any of the criteria in the ISO PCDS. Rather the UNTP Digital Product Passport provides a simple mechanism to digitalise product product circularity data in a way remains ISO-59040 conformant. The UNTP Digital Product Passport data model includes the organisation, facility, and product meta-data required by ISO-59040. The `Declarations` structure within the UNTP DPP data model can be used to convey each specific circularity criteria defined by ISO-59040. Since UNTP DPPs are both human and machine readable and can carry other sustainability information such as carbon footprint, product manufacturers can issue UNTP DPPs with confidence that the single DPP can conform to multiple sustainability standards and be equally valuable to human and machine verifiers.

Sample ISO-59040 conformant UNTP DPP - to be provided.

CEN CENELEC Digital Product Passport Framework

Standard Overview

The CEN/CENELEC Digital Product Passport Framework and System (CEN EU DPP) is a new initiative that will deliver the underlying technical standards (data carriers, identifiers, data exchange) to support the European Commission Eco-design for Sustainable Products Regulation (ESPR). There are three outputs defined by the CEN DPP working group.

- Unique Identifiers - unique identifier system that supports both centralised and decentralised identifiers and supports product identification at the model, batch, or item level.
- Data Carriers - the format, error correction, encoding methods, printing & durability of the product data carrier (eg QR code).
- Data Exchange Protocols - An open, secure, reliable, and high integrity data exchange protocol for the exchange of DPP data between two or more systems. Includes access control mechanisms for sensitive data.

The CEN/CENELEC DPP standardization work is in-progress. This information will be refreshed as updated information is published.

UNTP Relationship

The UNTP is a voluntary standard that must be easy to apply to any existing industry specific product data carriers and identifiers - and must work within any member country regulatory framework. For example, 100 million livestock (sheep and cattle) in Australia are identified with RFID data carriers that carry NLIS identifiers and comply with national regulations. UNTP builds upon ubiquitous technical standards from W3C and IETF to ensure technical interoperability and will leverage semantic web technologies and established vocabularies for semantic interoperability. Therefore is is expected that interoperability with CEN/CENELEC DPP standards will be straightforward.

- Identifiers and Carriers : UNTP will maintain a human and machine readable register of organisation, facility, and product identifier schemes together with data about how to parse data carriers, resolve identifiers to discover passports, and verify ownership of the identifier and integrity of the passport. Any EU product registers that implement CEN standards will be added to the UN register of schemes.
- Data Exchange Protocol : UNTP leverages open technical standard including JSON Schema, W3C JSON-LD semantics, and IETF Linksets. CEN DPP is likely to leverage similar technical standards. Furthermore, UNTP Digital product passport data is mapped to well established semantic vocabularies such as vocabulary.uncefact.org, schema.org and others as

needed. UNTP will maintain mappings to any EU specific passport data semantics to ensure interoperability at the semantic level.

This information will be refreshed as updated information is published. UN/CEFACT remains committed to ensure interoperability with CEN/CENELEC DPP standards as they emerge.

ISO EPC Information Services

Standard Overview

ISO/IEC 19987:2024, also known as Electronic Product Code Information System (EPCIS) is a well established standard for supply chain traceability. EPCIS defines six event types that can be combined as required to accurately describe a value chain from raw material to finished product. The event types are `Object Event` (eg an inspection), `Transaction Event` (eg a shipment of goods from seller to buyer), `Aggregation Event` (eg loading multiple packages on a pallet), `Transformation Event` (eg manufacturing process that consumes input materials to create output products), and `Association Event` (eg linking products to other products or facilities). EPCIS also defines a suite of APIs for machine-to-machine exchange.

UNTP Relationship

The UNTP Digital Traceability Event (DTE) is a conformant and simplified profile of EPCIS that identifies the minimum subset of EPCIS that is necessary to support value chain transparency. The UNTP DTE profile is also optimised for packaging as verifiable credentials and discovery as linked data - rather than the machine-to-machine API mechanisms defined by the ISO standard.

Business Case

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

The Business Case for UNTP implementation

In this section we provide a broad analysis of the key drivers, impacts, costs, and benefits associated with the implementation of the United Nations Transparency Protocol (UNTP) in an overall digital trade facilitation program.

- Stakeholder motivations summarizes the full range of stakeholder types and their motivations.
- Business case for industry details the business value propositions and costs for UNTP implementation by industry at individual company level and provide a simple business case template.
- Business case for government details the business case for governments at both individual agency and national economy levels.
- Community activation program defines a methodology and business case for industry member associations to engage their membership for collective implementation at the community level.
- Value assessment framework is essentially the UNTP business case for UNECE because it defines the UNTP KPIs that will be measures so that global impact can be tracked.

Stakeholder Motivations

The table below provides an overview of the different stakeholders participating in the trade ecosystem, including their role and, key motivating factors and link to the UNTP benefit statement in the Audience, Benefits & Goals section.

Stakeholder	Motivation
Consumers/Consumer Groups - Purchase and use products.	*We want to make informed choices about the products we buy, but it's hard to find reliable information about their origins and manufacturing.*
Regulators - Enforce compliance with laws and regulations.	*We struggle to ensure that all companies comply with safety and environmental regulations because we lack visibility into their supply chains.*
Producers and Manufacturers - produce raw materials and manufacture goods.	*We face difficulties proving the ethical sourcing and quality of our raw materials to our customers.*

Stakeholder	Motivation
Brands and Retailers - Market and sell products to consumers	*Our customers want to know where our products come from and how they are made, but it's hard to provide that information.*
Recyclers and Refurbishers - Manage end-of-life products.	*We often don't have enough information about the materials we receive, making recycling and refurbishment less efficient.*
Industry Member Associations - Represent and advocate for industry interests	*Our members need support in adapting to new regulations and industry practices, but it's challenging to provide consistent guidance.*
Environment and Human Welfare Organisations - Advocate for environmental protection and human rights.	*It's difficult to hold companies accountable for their environmental and human rights practices without clear information.*
Standards Organisations - Develop and maintain industry standards.	*It's challenging to keep our standards relevant and ensure they are adopted consistently across the industry.*
Accreditation Bodies and Certifiers - Provide certification and accreditation services	*We need a reliable way to verify that companies are truly adhering to industry standards and ethical practices.*
Transport and Logistics Providers - Manage the movement of goods.	*We need to track shipments accurately and ensure timely deliveries, but our current systems lack the necessary transparency.*
Financial Institutions - Provide financial services and investments.	*We need to assess the risks associated with our investments, but it's hard to get clear information about companies' supply chains.*
Software Developers - Develop software solutions to support transparency.	*We want to create solutions that meet market needs, but it's hard to anticipate what businesses require for supply chain transparency.*
Consultants & Advisors - Offer various advice services to businesses.	*Our clients need help complying with new transparency regulations, but it's difficult to offer the right services without clear guidelines.*

Business Case for Industry.

In today's global marketplace, commercial incentives drive business action. With regard to sustainable business practices and products, there is a maturity trend in the way businesses think about value.

- **Historically** sustainability was a marketing exercise that focused primarily on green labeling to promote sales. This led to an explosion in green-washing and precipitated a race to the bottom of devalued incentives.
- **Currently** the green-washing explosion has led to a similar dramatic increase in company-level and product-level disclosure regulations to counter green-washing and to support national net-zero promises. For most businesses today, sustainability has moved from a marketing concern to a risk and compliance concern. UNTP has much to offer in support of organizational compliance and due-diligence obligations.
- **In future** more and more organisations are likely to follow today's leading organisations in placing sustainability at the front and center of their business strategy, profitability, and brand value. UNTP can offer the value chain transparency at scale so that brands can be confident in the implementation of sustainability strategies.

At a high level adopting UNTP offers several key benefits:

- **Supply Chain Optimization** : Detailed supplier data allows for informed selection of more sustainable and resilient supply options.
- **Enhanced Disclosure Accuracy** : Access to granular, product-level sustainability data enables precise reporting and provides the key information needed for organisations to select supply so that their year-on-year sustainability disclosures demonstrate a clear improving trend.
- **Reputational Risk Management** : Transparency in the supply chain helps mitigate risks associated with unsustainable supplier practices.
- **Financial Advantages** : The financial sector increasingly rewards strong sustainability credentials with improved terms for trade finance and investment capital.

For more information and templates, please visit the Business Case for Industry. page.

Business Case for Government.

The implementation of the UN Transparency Protocol (UNTP) is expected to yield significant economic benefits for participating nations. While the precise impact may vary based on a country's existing trade infrastructure, regulatory environment, and level of digitalization, there are several opportunities for improvement.

- **Trade cost reduction** : Implementation of the UNTP is projected to reduce trade costs through the standardisation and digitization of processes. This includes streamlining customs clearance, documentation, inspections, and other administrative procedures.
- **Enhanced Revenue Collection** : Improved compliance and reduced fraud, facilitated by the UNTP's transparency measures, may lead to more effective revenue collection from customs duties and taxes.
- **Facilitate Trade Policy Development** : Receiving granular data and attributes of what gets in and out of the country and being able to aggregate that data can help policy makers in shaping policy in a more targeted way to enhance their countries competitiveness.
- **Foreign Direct Investment (FDI)** : Nations adopting the UNTP may become more attractive to foreign investors due to increased efficiency and predictability in trade processes.
- **Supply Chain Resilience and Competitiveness** : The real-time data and transparency provided by the UNTP can enhance the resilience of supply chains to disruptions and improve overall competitiveness in the global market.

The realisation of these benefits may depend on several factors, including:

- The nation's initial conditions and existing trade barriers
- The extent and effectiveness of UNTP implementation
- Complementary reforms in areas such as infrastructure, governance, and technology

The UNTP is supported by UNECE policy Recommendation 49 - traceability and transparency at scale that defines specific recommendations for member states that wish to reap the economic benefits of increased supply chain traceability, transparency, and trust.

For more information and templates, please visit the Business Case for Government. page.

Community Activation Program.

Supply chain actors are often reluctant to proceed with a specific initiate like UNTP unless they have some confidence that others in their industry are doing the same. There are not only obvious interoperability benefits from industry wide adoption but also cost benefits. For example, it is often the case that a small number of commercial software platforms are commonly used by larger numbers of businesses in a given industry and jurisdiction. So a software vendor that implements UNTP once will benefit all it's customers. Additionally there are often a few standards and a few certifiers that are common to an industry and country. Finally, when a large community is willing to act together, there will often be financial incentives from governments and/or development banks that can assist with initial funding. In short, there are many reasons to approach UNTP implementation at a community level.

The Community Activation Program (CAP) is a methodology and business case for a community level adoption of UNTP including a tool for financial cost/benefit modelling at community level. The CAP is an ideal vehicle for existing industry member associations to bring new value to their members by supporting their connections into global sustainable value chains.

For more information, please visit the Community Activation Program page.

Value Assessment Framework.

Once a community or individual implements UNTP and transparency data starts to flow at scale, it will become important to continuously assess the actual value that is realised. Dashboards and scorecards that measure key performance indicators will energise ongoing action and provide valuable feedback at both community and UN level. Therefore the UNTP defines a minimal set of KPIs that each implementer can easily measure and report to their community - and which communities can report to the UN so that global impact can be measured and mapped to the 169 specific targets defined by the 17 UN Sustainable Development Goals.

For more information, please visit the Value Assessment Framework page.

Business Case for Industry

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

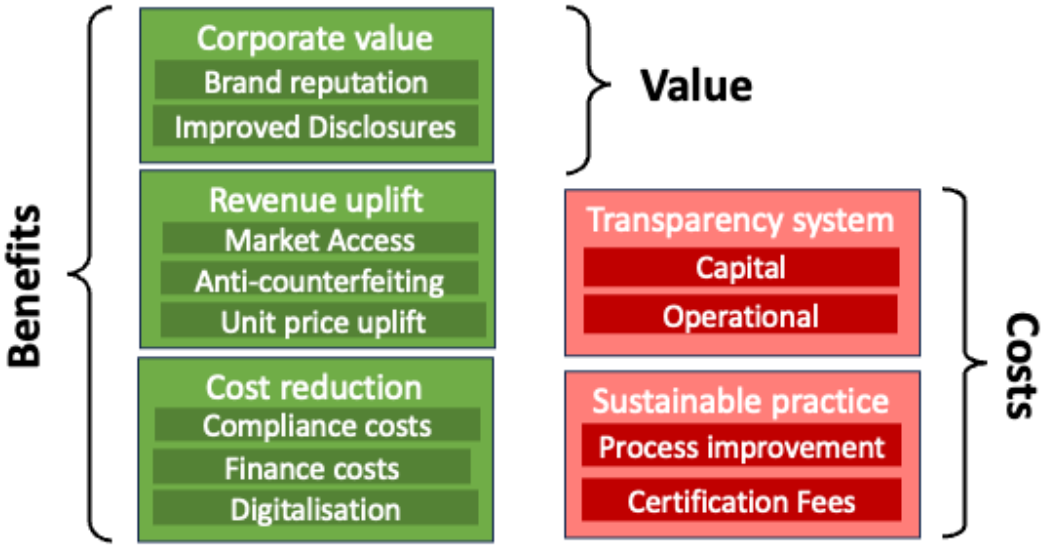
The decision to implement UNTP needs a positive business case to justify the investment. The purpose of this page is to provide a framework for business case development. We provide a generalized cost / benefit model and then discuss its application to specific roles and industries. We also provide a separate cost benefit model and business case template for regulators.

Note: The economic impacts described in this document are projections based on available data and economic models. Actual results may vary. Regular monitoring and evaluation of the UNTP's effects are recommended to assess its efficacy and guide any necessary adjustments to the protocol.

Industry Cost Benefit Model

The high level model shown below breaks benefits into three categories and costs into two categories.

- Benefits accrue through increasing revenue and/or decreasing cost. Improved margins that result from that of course contribute to corporate value but there are also less tangible benefits at the corporate level such as brand reputation.
- Costs are incurred through changes to production processes to achieve greater sustainability and the implementation of traceability & transparency systems to communicate that verifiable sustainability.



Actual benchmarks for benefits and costs by industry sector and geographic region will become increasingly available over time through the UNTP Value Assessment Framework (VAF). At this point in time, benefits and costs are described qualitatively

and supported with metrics from public research.

Benefits - Revenue Uplift

Market Access

Legislation increasingly requires companies to prove ESG credentials to be able to trade in certain countries. Examples include the EU Deforestation Regulation EUDR as well as several due-diligence regulations such as the EU CSDDD and US UFLPA. Legislation effectively put pressure for on buyers to prove provenance and sustainability requirements for certain products, as well as a higher burden of truth from suppliers from to certain regions. In many cases, these regulations reverse the burden of proof - namely that companies must prove that they are compliant in order to maintain market access. UNTP based transparency allows companies to keep trading in said areas, rewarding suppliers ensuring good practices rather than being forced outright out of these markets.

- *Quantification.* The percentage of revenue that is either retained or increased will depend on the commodity and footprint of any given supplier in a regulated market. The value of imported goods impacted by EUDR is approximately $400Bn which is around 1.2% of world trade. The volume of trade impacted by Due Diligence acts is similar or larger than EUDR.
- *References.* EU market import volumes, Krungsri EUDR impact analysis,

The impact of these trade barriers for any given company will be between 0% and 100% of revenue depending on which commodities they sell to which market. But given the collective impact of between 2% and 3% of world trade, an average benchmark of 1% of revenue seems conservative.

Unit Price Uplift

Consumers are increasingly selective about product choice based on believable sustainability criteria. There are several surveys that indicate around two-thirds of consumers consider sustainability in product choices and that around one third are willing to pay a premium. The amount of the price premium varies widely and there is evidence that consumer behaviour change is slow and sometimes only temporary. There is also evidence that rich data (for example UNTP DPPs) drives stronger behaviour. The amount of end product price increase that flows through to the upstream supply chain is more difficult to quantify but may be very limited. Nevertheless, if buyers select supply based on sustainability criteria then non-conforming suppliers and products are likely to be forced into lower-priced commodity markets. Buyers tend to be reacting more quickly than suppliers to these demands, as a result, moving forward it is likely that there will be a shortage of suppliers able to deliver products with satisfying ESG credentials. Buyers who are able to sign long term contracts today and develop partnerships with aligned suppliers will have a considerable price advantage compared to market laggards.

- *Quantification* Estimates of the average sustainability premium that consumers will pay vary widely from around 1% to 12%. If 30% of consumers are willing to pay a 5% premium then the overall unit price impact is around 1.5%.
- *References.* Consumer high estimates, Consumer low estimates.

The unit price uplift for verifiable sustainable goods will vary widely depending on commodity and market. However an average benchmark of 1% seems reasonable and conservative.

Anti-Counterfeiting

Global trade in counterfeit goods is estimated at between 2% and 5% of trade. The most impacted commodities are pharmaceuticals and luxury goods including quality wines & spirits. The volumes increase when pirated / smuggled goods are taken into account including illicit tobacco into high tax markets. What is more difficult to quantify is the proportion of counterfeit goods that are un-knowingly purchased as genuine goods since, in many cases, buyers of fake luxury goods or illicit tobacco make purchases knowing that the goods are fake or pirated. UNTP offers a simple but effective anti-counterfeit protocol that works well when buyers are motivated to confirm that goods are genuine.

- *Quantification.* 4% of global trade represents about $1.2Tn in counterfeit goods. If approximately 50% of that trade can be impacted by improved anti-counterfeiting measures then the average value is around 2%. If the effectiveness of anti-counterfeiting measures is estimated at 50% then the value falls to around 1% of trade.
- *References.* OECD trends in counterfeit goods, USTPO counterfeit estimates.

The value of sales recovered by reductions in illicit goods will vary from 0% for commodity goods to as much as 10% for pharmaceuticals and some luxury goods. A benchmark value of 1% industry-wide seems reasonable and conservative.

Benefits - Cost Reduction

Compliance Costs

Regulatory compliance costs encompass the administrative burden of reporting, processing fees, tariffs, border clearance delays, and penalties. As sustainability regulations increase, these will be more rigorously enforced at borders, likely resulting in higher compliance costs. The UNTP offers customs authorities and corporate regulators higher confidence data, which can streamline border processing, reduce administrative costs, and minimize delays. As countries advance towards net zero commitments and implement domestic carbon pricing, it is increasingly likely that more countries will impose carbon border tariffs, such as the planned EU Carbon Border Adjustment Mechanism (CBAM). High-quality evidence of a low carbon footprint via UNTP Digital Product Passports (DPPs), along with full traceability, can help importers prove compliance with the EU rules of emission estimation, and reduce the burden of data collection and management for tariff treatment. Additionally, high-quality evidence of conformance of imported goods reduces the risk of punitive non-compliance fines. Importers with traceable, high-quality data can ensure that they are only paying CBAM charges on actual emissions. Without accurate data, importers might overestimate emissions, leading to higher costs. Detailed tracking allows them to minimize over-payment and reduce their carbon liabilities if the carbon price effectively paid in the export country can be deducted.

- *Quantification.* The compliance cost under CBAM, a steel producer with a high emission profile, might face a carbon levy in the range of €50–€90 per ton of CO_2 emitted, depending on current EU ETS carbon prices. High-quality evidence of carbon price paid in the export country can substantially adjust that value.
- *References.* EU Carbon Border Adjustment Mechanism, Wood MacKenzie CBAM Analysis

Finance Costs

UNTP provides a framework based on international standards which can accommodate different ESG risks, enabling development banks to standardize their reporting and ensuring their mandate, without having to create ad-hoc structures for each Sustainable Supply Chain Finance Deal. This unlocks a significant trade finance gap, and enables preferential finance to

reach deep-tier suppliers. Access to lower financing costs for suppliers results in lower cost of goods sold and improved margins. These trade finance arrangements often come with grants that can support costs associated with the ESG transition, such as support certification, consulting or implementation of new ERP systems for reporting.

Access to Trade Finance

The Asian Development Bank (ADB) estimates that the global trade finance gap was approximately $2.5 trillion in 2022, up from $1.5 trillions in 2016 with a significant portion attributable to SMEs applicants, lack of visibility, and issues with country risk, credit-worthiness and lack of sufficient information by the applicant. At the same time, Supply Chain Finance (SCF) has grown from $330 billion in 2015 to $1.8 trillion in 2021, despite this growth, SCF has has not yet had a major impact in reducing the trade finance gap due to difficulty reaching past tier 1 suppliers. By adopting the UNTP, this gap can be reduced by enabling more companies to access preferential financing thanks to increased visibility over ESG credentials and ability to provide identity assurance from a trusted register, combined with SCF reverse factoring operating models which reduce applicants risk by tying the financing to the buyer credit risk.

- *References* Asian Development Bank (ADB), Trade Finance Gaps Growth and Jobs Survey 2021, Trade finance gaps growth jobs survey 2023. Deep-Tier Supply Chain Finance 2022

Reduced Finance Costs

According to the International Finance Corporation (IFC), companies that adopt sustainable practices can reduce their financing costs by up to 20% due to lower risk premiums and better access to capital.

- *References* International Finance Corporation (IFC), "Sustainable Finance: Creating Value for Companies and Investors," 2020.

Improved margins

A study by the Global Reporting Initiative (GRI) found that companies with strong ESG performance can achieve up to a 10% improvement in profit margins due to enhanced operational efficiencies and lower financing costs.

- *References* Global Reporting Initiative (GRI), "The Business Case for ESG: How Sustainability Can Drive Financial Performance," 2019.

Cost of Goods Sold

A report by McKinsey & Company indicates that companies with optimized supply chain financing can reduce their cost of goods sold by 5% to 10% due to lower financing costs and improved supply chain efficiencies.

- *References* McKinsey & Company, Unlocking success in digital transformations, 2018

Digitalisation Efficiency

Digitalisation through UNTP enables automated data collection and processing, reducing manual labor and errors. This leads to streamlined operations and faster decision-making. Enhanced digitalisation provides real-time visibility into supply chain activities, allowing for better inventory management and demand forecasting. Access to accurate and timely data enables

companies to make informed decisions, improving overall business performance. Finally, digitalisation allows for better tracking of product quality and delivery times, leading to improved customer satisfaction and loyalty.

Digitalisation as a whole of organisation initiative can deliver a 10% to 20% reduction in operational costs due to automation and improved data accuracy. Improved supply chain visibility can reduce inventory holding costs by 15% to 30% and decrease stock-outs by 20%. Data-driven decision-making can increase productivity by 5% to 10% and enhance profitability by 3% to 5%. Enhanced customer satisfaction can lead to a 10% increase in repeat business and a 5% boost in overall sales.

- *Quantification* The digitalisation cost savings are for enterprise wide digital transformation. A smaller but significant proportion of those savings could be allocated to digitalisation of supply chain traceability & transparency through UNTP implementation. A 1% reduction in operating costs is a conservative estimate.
- *References* McKinsey & Company reports on digital transformation, Deloitte insights on operational efficiency. Gartner reports on supply chain visibility, Accenture studies on inventory management. Harvard Business Review articles on data analytics, PwC reports on data-driven strategies. Forrester Research on customer experience, Bain & Company studies on customer loyalty.

Benefits - Corporate Value

Brand Reputation

Transparency in supply chains builds consumer trust, as customers are increasingly concerned about the ethical and environmental impact of their purchases. Companies that can demonstrate their commitment to sustainability and ethical practices are more likely to gain consumer loyalty. Companies with strong ESG credentials often see an increase in brand value. This is because consumers, investors, and other stakeholders perceive these companies as more responsible and forward-thinking. Companies that adopt the UNTP can differentiate themselves from competitors by showcasing their commitment to transparency and sustainability. This can lead to a stronger market position and increased market share. Finally, transparent supply chains help companies identify and mitigate risks related to unethical practices, environmental violations, and other ESG issues. This proactive approach can prevent reputational damage and associated financial losses.

Studies reveal that over 50% of global consumers and over 75% of millennials are willing to pay more for sustainable brands. Also that over 80% of consumers will purchase a product because a company advocated for an issue they cared about, and over 70% will refuse to purchase if they find out a company supports an issue contrary to their beliefs. Brands with high ESG scores have been found to achieve a brand value premium of up to 10%. Brands with strong reputations recover more quickly from crises, with a 5% to 10% faster recovery in stock prices.

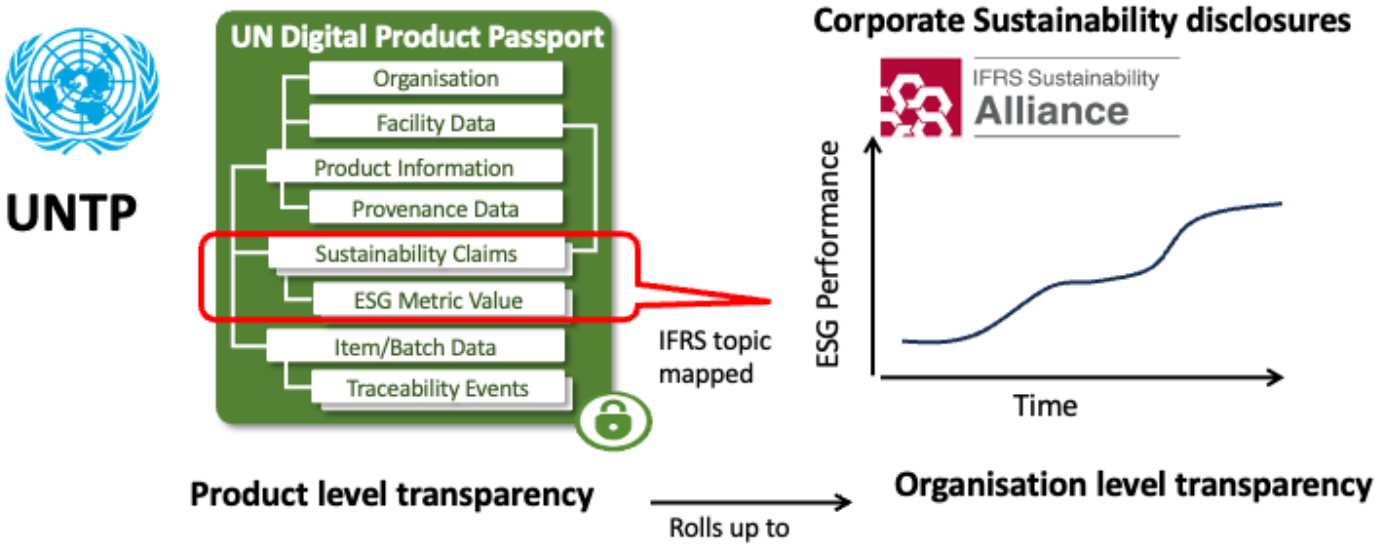
- *Quantification.* The brand value benefits listed above will accrue for companies that place sustainability at the center of their corporate strategy and implement a range of measures. UNTP implementation is only one measure but will add considerable trust to sustainability claims and can therefore conservatively account for a 1% increase in brand value.
- *References.* Nielsen, "The Sustainability Imperative: New Insights on Consumer Expectations," 2015, Brand Finance, "Global 500 2020: The Annual Report on the World's Most Valuable Brands," 2019. RepTrak, "Global RepTrak 100: The World's Most Reputable Companies," 2019. Cone Communications, "2017 Cone Communications CSR Study," 2017.

Improved Disclosures

Regulations that mandate annual corporate sustainability disclosures are being drafted or already in force in most economies. They generally require reporting of concrete metrics such as CO2 equivalent emissions and almost all include scope 3 emissions (ie emissions associated with upstream supply. The World Business Council for Sustainable Development (WBCSD) defines a generic model for emissions reporting and highlights the fact that, for most companies, scope 3 emissions represent around 70% to 80% of their emissions footprint.

We have included a separate category for corporate disclosures because there is a serious problem facing most corporates today. The problem is that most corporates simply do not have the data from their upstream suppliers to directly measure their scope 3 emissions footprint. Therefore the only viable option is indirect measures such as using industry average intensity for each input product or material. Without direct information from suppliers there is no mechanism to select lower intensity supplies - and, correspondingly, there is no incentive for suppliers to reduce their emissions. Corporates that increase sales volume year on year are therefore likely to also report increased emissions (increased volume multiplied by an unchanged industry average). Companies that show deteriorating emissions performance are likely to be punished through reduced consumer loyalty, reduced brand value, increased border tariffs, and reduced access to finance.

Direct measures of supplier sustainability performance through UNTP digital product passports will provide corporates with the means to select more sustainable supply and therefore directly improve their own aggregate performance year on year.



- *Quantification.* The same metrics as apply to brand reputation apply here.
- *References.* WBCSD Pathfinder 2.0 Framework

Costs - Sustainable Practices

Process Improvement

Suppliers are often requested to bring ESG improvements based on the materiality matrix of their buyers, so as to align with the buyers ESG strategic priorities: Examples may include: Reducing carbon emissions of particular energy intensive processes (i.e. by adopting less energy intensive processes or switching to renewable energy sources) Reducing or eliminating the use of harmful chemicals in heavy industrial processes Improving human or labour rights issues within their supply chains These

improvements are often costly, which are often absorbed by loans. Green finance mechanism can help reduce the financing cost of these improvements, and are often related to these improvements, while the establishment of long term contracts with buyers can on the one hand secure cash flow for suppliers to absorb those costs over the years, while on the other guarantee to the buyer the flow of conform goods.

- *Quantification.*
- *References.*

Audits & Certification

Suppliers that improve their processes towards sustainability practices have three ways to prove their credentials to their buyers, namely carrying out a self assessment, being audited by the buyers and being audited and certified by a third party, the latter of which carries the greatest weigh in terms of credibility, both for voluntary improvements and certainly for regulated ones. These certifications and audits often need to be made for each ESG risk where mitigating actions have occurred, with certifications starting in the 5 figures for each certification type.

- *Quantification.*
- *References.*

Costs - Transparency System

Establishing a transparency systems along a supply chain carries its own costs in the form of consulting fees to map and study the structure and processes and actors involved in a specific supply chain, the data elements of it and how those conform to an interoperability protocol such as UNTP as well as software and IT integration and adaptation costs, all of which is expected to range in the six figures. It also carries costs to run such a system on a day to day basis. At the same time, UNTP's principle is to use what is already available and being used, or planned to be used, by participants, rather than buying new software; once implemented we expect the operational costs to be in a similar range to what existed before hand, with any additional cost related to additional features related to benefits which the industry might require.

Capital investment

In order to adapt a digital ecosystem to an interoperability protocol such as UNTP, adopters will likely rely on consulting companies to assess the supply chain, identify data elements, and evaluate compatibility with UNTP standards and may decide to rely on consultants also to project manage and implement the project. Equally buyers will need to integrate their systems with their suppliers systems, or decide to commonly use a system that conforms to UNTP.

- *Quantification.*
- *References.*

Operational costs

As a UNTP complaint system set up is designed to work with what is already available, we expect adopters to get back more for the same resources they were already using for transparency purposes AUTOMATION, COST SAVINGS.. At the same time,

the wealth of information resulting from full traceability will likely drive adopters to capitalise on their investment and add resources to analyse and disclose their supply chain data where they see a return.

- *Quantification.*
- *References.*

Industry Business Case Template

Business Case for Government

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

The decision to implement UNTP needs a positive business case to justify the investment. The purpose of this page is to provide a framework for business case development. We provide a generalised cost / benefit model and then discuss it's application to specific roles and industries. We also provide a separate cost benefit model and business case template for regulators.

Regulator Cost Benefit Model

TBD - insert model diagram here

Benefits - National Economy

Benefits - Compliance Outcomes

Benefits - Government Efficiency

Costs - Implementation

Costs - Operational

Regulator Business Case Template

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Introduction

The Community Activation Program (CAP) serves as a comprehensive framework and collaborative community designed to support industries in developing and implementing their own UNTP extension projects. Communities, supported by UNECE, continue to thrive long after the project is complete, aiding industries in adopting extensions and associated tools.

Recognizing the need for industry-wide collaboration to address challenges such as interoperability and costs, CAP offers structured solutions. Corporations often prefer not to act in isolation due to the risks and challenges associated with independent initiatives; CAP addresses this by fostering collective action, enabling industries to achieve shared goals through collaboration and mutual support. By leveraging a unified methodology, comprehensive toolkit, open-source software platforms, and globally recognized standards, CAP empowers industries to reduce costs, improve efficiency, and build trust among stakeholders, including regulators, financial institutions, and software vendors. This fosters deeper collaboration and shared benefits across sectors.

Through CAP, industries can assess the value of their extension projects and effectively engage diverse stakeholders to drive adoption.

Starting a UNTP project requires careful consideration of specific foundational elements that ensure the project's alignment with industry needs and its potential for widespread adoption. These include:

- **Catalyst for adoption**: Identifying a clear and compelling driver for the project, such as new regulatory requirements (e.g., EUDR or Carbon Border Adjustment Mechanism), or the need to align with a national or sectoral traceability strategy, provides focus and urgency for stakeholders.

- **Engaged buyers**: Buyers must perceive significant value in supplier data, such as enhanced product quality, compliance assurance, or risk mitigation. This engagement is essential to drive demand for the project outcomes.

- **Committed suppliers**: Suppliers must be willing and able to share critical data with buyers, especially when the project demonstrates a direct benefit to them, such as cost reductions, increased market access, or reputational gains.

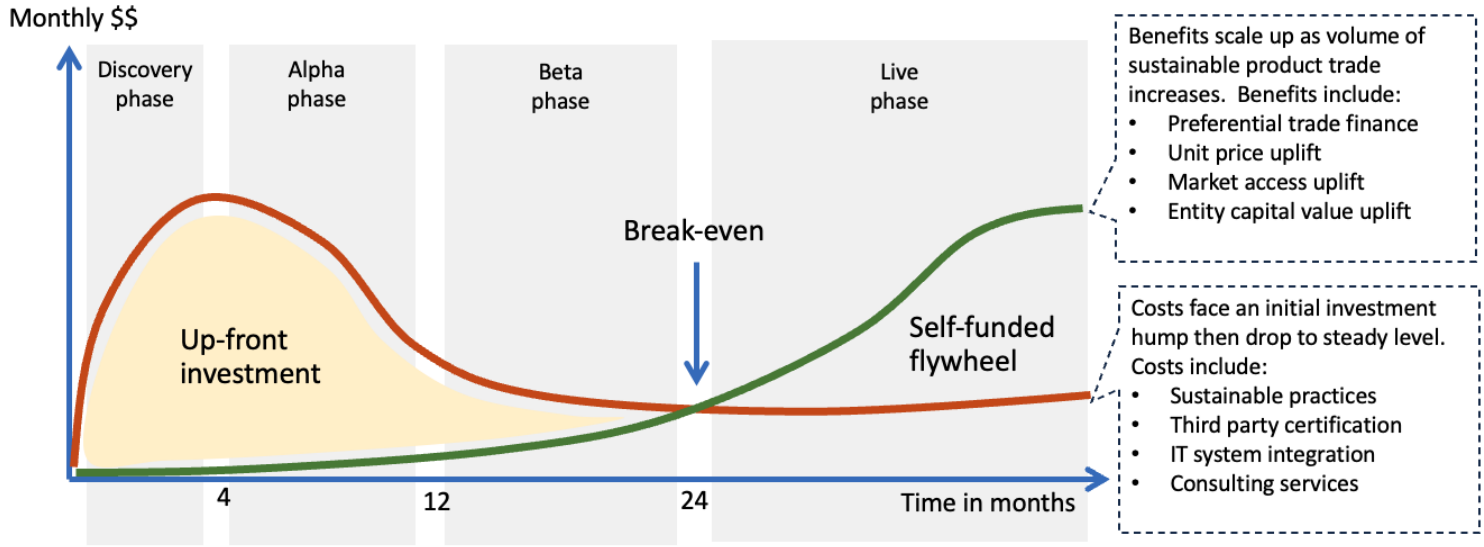
- **Funding mechanism**: Robust and sustainable funding is crucial for supporting the project's initial phases, covering development, outreach, and pilot testing. This ensures that the project gains traction and delivers early successes to build momentum.

CAP delivers value to industries and creates a flywheel of adoption

Industry associations engaging with CAP to develop UNTP extensions benefit from:

- Shared costs and reduced financial risks for members.
- Increased value proposition for association membership.
- Enhanced trust and credibility within industries and stakeholders.
- Accelerated momentum for product passports, trust services, and registries.
- Alignment with emerging extensions, solving interoperability challenges.
- Access to global experts, case studies, and robust tools.

As extension projects mature, they generate a self-sustaining flywheel effect. This mechanism drives innovation and growth by aligning stakeholders, fostering collaboration, and incentivizing continuous improvement. By enabling shared benefits, CAP ensures long-term progress and success.



CAP supports a structured approach to extension development and adoption

The CAP toolkit offers a proven, six-phase methodology:

Inception Phase: This initial phase is centered on identifying key catalysts for change, such as emerging regulations, national traceability strategies, or industry-specific challenges. Stakeholders work collaboratively to build consensus, define project goals, and create a compelling business case that articulates value. Communities may already exist and catalyze around a pressing business problem, identifying UNTP as the most effective solution. At the end of this phase, a community may formally register their extension with UNTP, solidifying their commitment and alignment with global standards. Securing initial funding ensures the project is adequately resourced for success.

Discovery Phase: In this exploratory phase, current practices are systematically mapped to identify strengths, gaps, and opportunities. Stakeholders prioritize areas for improvement and establish clear objectives that align with industry needs and

regulatory demands. This phase sets the foundation for a targeted and actionable implementation plan.

Alpha Phase: During the alpha phase, prototypes of the proposed systems and frameworks are developed and tested within controlled environments. This stage allows stakeholders to assess functionality, refine tools, and demonstrate tangible value to participants. Feedback loops are critical in ensuring the solution is robust and addresses real-world challenges effectively.

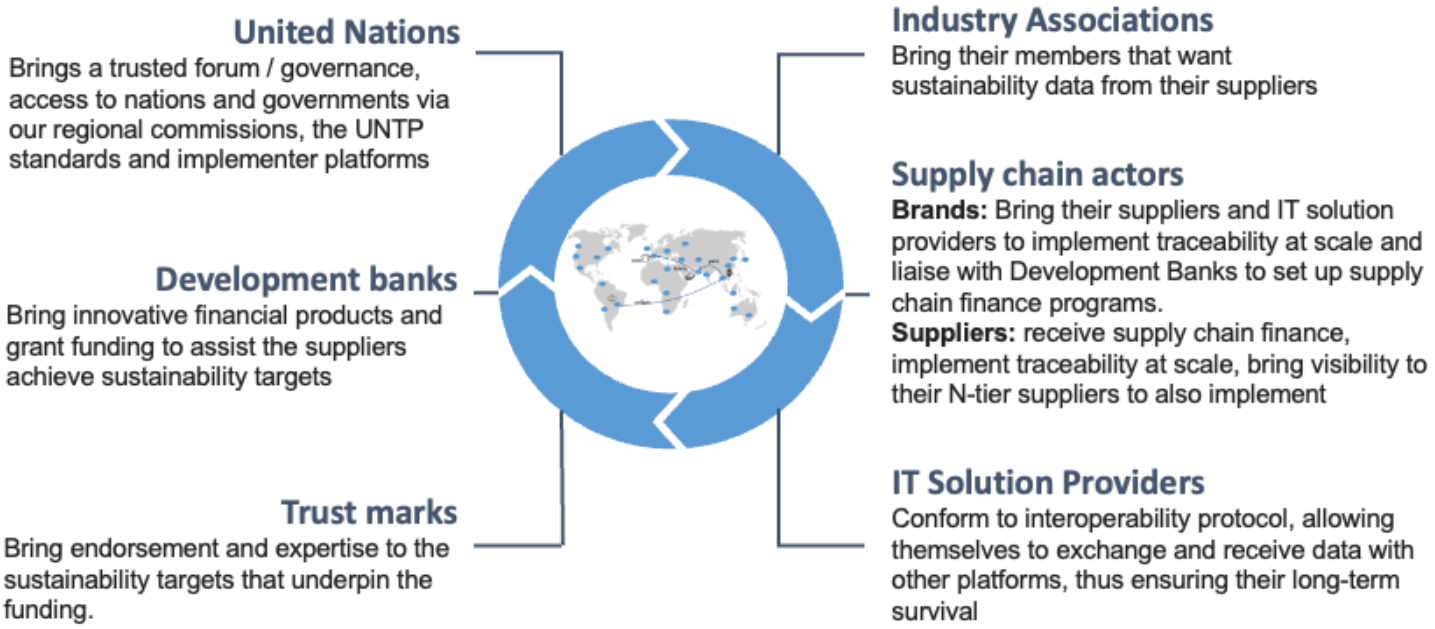
Beta Phase: Building on the alpha phase, the beta phase scales the project to a broader set of participants. Emphasis is placed on resolving interoperability challenges, ensuring compatibility with existing systems, and refining operational workflows. The project is tested in live scenarios to validate its scalability and effectiveness.

Live Phase: The final phase transitions the project into full-scale implementation. Stakeholders work to achieve widespread adoption, leveraging continuous improvement mechanisms to adapt to evolving industry needs. This phase ensures the extension remains sustainable, impactful, and aligned with broader industry objectives.

More on the methodology here.

A successful UNTP extension project is a team effort

UNTP extension projects thrive through collaboration with a wide range of stakeholders.



CAP member stakeholders bring unique needs and derive tailored benefits:

- **Industry associations**: Drive collective industry efforts by providing leadership and fostering collaboration to develop interoperable standards, ensuring enhanced member value and a unified industry voice.
- **Suppliers**: Contribute essential data that ensures compliance with ESG standards and enables access to broader markets. Their participation demonstrates alignment with global sustainability efforts and supports trust across supply chains.

- **Buyers**: Play a pivotal role by demanding traceability and guiding the adoption of data standards. This ensures reliable and transparent information flow, bolstering brand trust and improving consumer confidence.

- **Trust marks and government agencies**: Provide critical policy frameworks and credentials that establish the credibility of sustainability efforts. They ensure alignment with environmental, social, and governance (ESG) goals and offer a foundation for industry-wide adoption.

- **Development banks**: Facilitate sustainable growth by offering ESG-linked financing and investment mechanisms. These institutions provide crucial resources that reduce financial barriers and encourage broader participation in UNTP extension projects.

- **IT solution providers**: Deliver the technical expertise needed to develop traceability systems and ensure seamless data interoperability. Their innovations enable scalable and robust solutions for managing complex supply chains.

- **UNECE**: Act as a global steward, offering governance frameworks that ensure alignment and interoperability across projects. Their involvement fosters cooperation, providing guidance that strengthens the foundation for sustainable and globally consistent practices.

A UNTP extension team requires specialist skills

To deliver a successful extension project, teams require a range of specialist skills. In addition to deep industry knowledge brought by the industry association and its members, a project should have:

- **Project management expertise**: Successful execution of UNTP extension projects relies heavily on effective project management. Teams must coordinate a wide range of activities, oversee resource allocation, and ensure that milestones are achieved on time. They must navigate complex interdependencies while maintaining a clear focus on objectives.

- **IT systems knowledge**: Teams need expertise in deploying and integrating advanced tools for data exchange, supply chain tracking, conformance testing, and process automation. Knowledge of software compatibility, system scalability, and data security is vital to ensure seamless operations.

- **Trust architecture expertise**: A trust architect is essential in ensuring that the systems and frameworks designed foster credibility and reliability among stakeholders. This role involves creating mechanisms to validate and certify data integrity, establishing clear accountability processes, and building frameworks that enhance trust across supply chains. Trust architects play a pivotal role in ensuring all participants have confidence in the system, paving the way for sustained adoption and collaborative success.

- **ESG standards expertise**: Proficiency in environmental, social, and governance (ESG) standards is critical for aligning projects with global sustainability goals. This includes implementing ESG frameworks, tracking compliance, and producing transparent reports that enhance trust among stakeholders.

- **Stakeholder engagement skills**: Effective communication and relationship management are essential for fostering collaboration among diverse participants. Teams must balance competing interests, mediate conflicts, and build consensus to align priorities and drive collective action.

- **UNTP extension knowledge**: Deep understanding of the UNTP framework is indispensable for designing and implementing extensions that meet global standards. Teams must navigate trade protocols, ensure data governance, and address technical interoperability challenges to deliver scalable and impactful solutions.

CAP membership provides access to valuable resources

As a member of the Community Activation Program, members can access a wide range of resources:

- **Frameworks and toolkits**: The UNTP Business Case Templates and traceability frameworks provide a comprehensive foundation for project planning. These tools are designed to streamline decision-making processes, ensuring that stakeholders can effectively map out goals, objectives, and resource requirements. The templates also offer guidance for measuring and communicating the value of UNTP extensions to participants and decision-makers.
- **UNECE guidance**: The UNECE plays a pivotal role in ensuring global alignment and promoting interoperability through its lightweight governance framework. By offering strategic guidance, the UNECE ensures that extension projects remain consistent with international standards, thereby fostering cooperation across borders and industries. This guidance reduces redundancies and ensures projects are sustainable and impactful.
- **Consultant support network**: Expert advisors provide indispensable support throughout each phase of the project. Their deep understanding of UNTP frameworks and industry best practices ensures that projects are both scalable and aligned with stakeholder needs. Consultants can help troubleshoot complex challenges, streamline workflows, and ensure that all participants achieve their objectives. [to be discussed]
- **Collaboration networks**: Engaging with established UNTP extension programs offers valuable opportunities for shared learning and innovation. These networks allow new participants to benefit from the experiences of others, adapt proven methodologies, and align their projects with broader industry goals. Collaboration also strengthens the ecosystem, making it easier for new extensions to integrate seamlessly.
- **Software tools**: A suite of software solutions is available to support UNTP extension projects. These tools facilitate rigorous testing, ensure conformance with established standards, and simplify supply chain management processes. By automating critical workflows and enabling data interoperability, these tools reduce the complexity of project implementation and drive efficiency.

Starting a community is simple

- **Join the community**: Join the UNTP chat channel to connect with a UNTP leader and discuss your community needs. By joining the community, participants gain access to ongoing support, exclusive updates, and a global network of peers dedicated to advancing UNTP standards.

- **Download the CAP toolkit**: Access resources, including methodologies, templates, and tools. This comprehensive toolkit is designed to guide organizations through every phase of a UNTP extension project, providing detailed frameworks for planning, execution, and evaluation. Toolkit Download

- **Engage with other programs**: Collaborate with established communities for shared learning and best practices. These connections allow participants to align their projects with proven methodologies, reducing duplication of effort and accelerating implementation timelines. Extensions Register

INFO

Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Ongoing Value Asessment

INFO

Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Case Studies

TBD

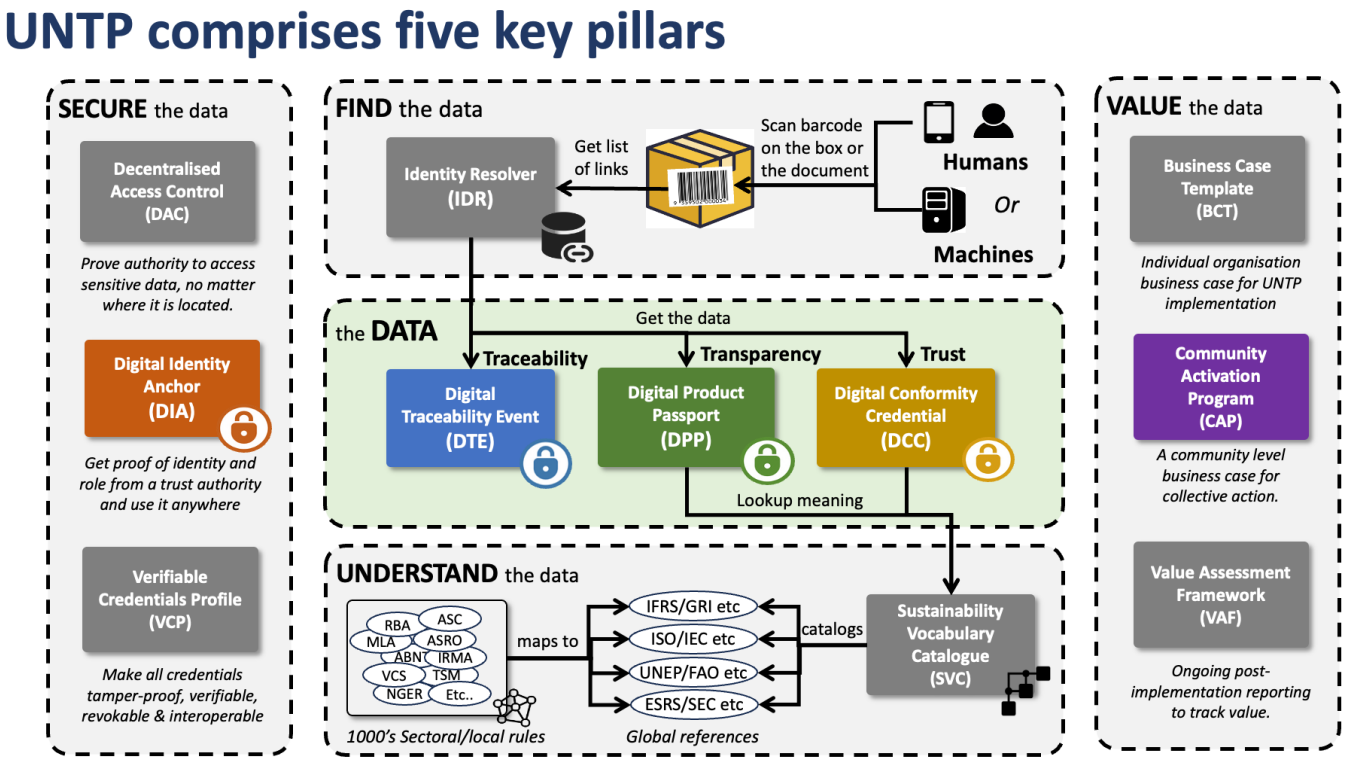
Specification

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

The specification is the heart of UNTP. It defines the detailed specifications for interoperable implementations. This page provides an outline of the purpose and scope of each component of the specification.

Architecture

The architecture is the blueprint for all the components of the specification and how they work together. It defines the **design principles** which underpin the UNTP and shows the components working together from the perspective of a **single actor** and across the **entire value-chain**. The UNTP is a fundamentally **decentralised architecture** with no central store of data.



Verifiable Credentials Profile (VCP)

The World-Wide-Web Consortium (W3C) has defined a standard called Verifiable Credentials (VCs). A VC is a portable digital version of everyday credentials like education certificates, permits, licenses, registrations, and so on. VCs are digitally signed

by the issuing party and are tamper proof, privacy preserving, revokable, and digitally verifiable. The UN has previously assessed this standard and has recommended its use for a variety of cross border trade use cases in a recent white paper. VCs are inherently decentralised and so are an excellent fit for UNTP which recommends that passports, credentials, and traceability events are all issued as W3C VCs. A related W3C standard called Decentralised Identifiers (DIDs) provides a mechanism to manage the cryptographic keys used by verifiable credentials and also to link multiple credentials into verifiable trust graphs. DIDs are not the same as the business / product / location identifiers maintained by authoritative agencies - but can be linked to them.

Digital Product Passport (DPP)

The digital product passport (DPP) is issued by the shipper of goods and is the carrier of **product and sustainability information** for every serialised product item (or product batch) that is shipped between actors in the value chain. It is deliberately **simple and lightweight** and is designed to carry the minimum necessary data at the **granularity** needed by the receiver of goods - such as the scope 3 emissions in a product shipment. The passport contains links to **conformity credentials** which add trust to the ESG claims in the passport. The passport also contains links to **traceability events** which provide the "glue" to follow the Linked Data trail (subject to confidentiality constraints) from finished product back to raw materials. The UNTP DPP does not conflict with national regulations such as the EU DPP. In fact, it can usefully be conceptualised as the **upstream B2B feedstock** that provides the data and evidence needed for the issuing of high quality national or regional level product passports.

Digital Conformity Credential (DCC)

Conformity credentials are usually issued by independent third parties and provide a **trusted assessment** of product ESG performance against credible **standards or regulations**. As such the credential provides trusted verification of the ESG claims in the passport. Since the passport may make several independent claims (eg emissions intensity, deforestation free, fair work, etc) there may be many linked conformity credentials referenced by one passport. As an additional trust layer, the conformity credential may reference an **accreditation** credential that attests to the authority of the third party to perform the specific ESG assessments. The conformity credential data model has been developed by a separate UN/CEFACT project on digital conformity that has expert membership from accreditation authorities and conformity assessment bodies.

Digital Traceability Events (DTE)

Traceability events are very lightweight collections of identifiers that specify the “what, when, where, why and how” of the products and facilities that constitute a value chain. The UNTP is based on ISO/IEC 19987, which is equivalent to the GS1 EPCIS standard, for this purpose because it is an existing and proven mechanism for supply chain traceability. Note that UNTP supports but does not require the use of GS1 identifiers. The basic idea behind the traceability event structure is that any supply chain of any complexity can always be accurately modelled using a combination of four basic event types. An **object** event describes an action on specific product(s) such as an inspection. A **transaction** event describes the exchange of product(s) between two actors such as sale of goods between seller and buyer. An **aggregation** event describes that consolidation or de-consolidation of products such as stacking bales of cotton on a pallet for transportation. Finally, a **transformation** event describes a manufacturing process that consumes input product(s) to create new output product(s). The UNTP uses these events in a decentralised architecture as the means to traverse the Linked Data "graph" that represents the entire value-chain.

Digital Identity Anchor (DIA)

UNTP credentials will include identifiers of products, locations or businesses. UNTP credentials will also include ESG performance claims like emissions intensity values. But how can a verifier of these identifiers or ESG claims be confident that the claims are true and that they are made by the genuine party at a verifiable location? Trust anchors are national or international authorities that typically run existing business or product registration, certification, accreditation, or other high integrity processes. Examples of trust anchors include national regulators that govern things like land ownership or business registrations. Another example are the national accreditation bodies that audit and accredit certifiers to issue third party assessments. UNTP depends on trust anchors to add digital integrity to ESG claims and identities by linking them to the authority under which they are made. In essence, UNTP defines a protocol for existing trust anchors to continue doing what they have always done, but in a digitally verifiable way.

Identity Resolver (IDR)

Identifiers of **businesses** (eg tax registration numbers, Legal Entity Identifiers (LEIs), of **locations** (eg google pins, cadastral/lot numbers, GS1 GLNs), and of **products** (eg GS1 GTINs or other schemes) are ubiquitous throughout supply chains and underpin the integrity of the system. UNTP builds upon existing identifier schemes without precluding the use of new schemes so that existing investments and high integrity registers can be leveraged. UNTP requires four key features of the identifiers and, for those that don't already embody these features, provides a framework to uplift the identifier scheme to meet UNTP requirements. Identifiers used in UNTP implementations should be **discoverable** (ie easily read by scanning a barcode, QR code, or RFID), **globally unique** (ie by adding a domain prefix to local schemes), **resolvable** (ie given an identifier, there is a standard way to find more data about the identified thing), and **verifiable** (ie ownership of the identifier can be verified so that actors cannot make claims about identifiers they don't own).

Decentralised Access Control (DAC)

There is a balance between the demands of transparency (more supply chain visibility means it's harder to hide greenwshing) and confidentiality (share too much data and you risk expososing commercial secrets). A key UNTP principle is that every supply chain actor should be able to choose their own balance between transparency and confidentiality. To achieve this, UNTP defines six data confidentiality patterns with different degrees of data protection so that they can be appropriately combined to meet the confidentiality goals of each party. This includes the ability to selectively redact data from credentials received from upstream suppliers before passing them on to downstream buyers - without affecting the cryptographic integrity of the data.

Sustainability Vocabulary Catalog (SVC)

Web **vocabularies** are a means to bring consistent understanding of **meaning** to ESG claims and assessments throughout transparent value chains based on UNTP. There are hundreds of ESG standards and regulations around the world, each with dozens or hundreds of specific conformity **criteria**. Any given value chain from raw materials to finished product is likely to include dozens of passports and conformity credentials issued against any of thousands of ESG criteria. Without a consistent means to make sense of this data, UNTP would provide a means to discover a lot of data but no easy way to make sense of it. The UNTP defines a standard and extensible topic map (taxonomy) of ESG criteria and provides a mechanism for any standards authority, or national regulator, or industry association to map their specific terminology to the UNTP vocabulary.

Architecture

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

The architecture is the blueprint for all the components of the specification and how they work together. It defines the **design principles** which underpin the UNTP and shows the components working together from the perspective of a **single actor** and across the **entire value-chain**. The UNTP is a fundamentally **decentralised architecture** with no central store of data.

Principles

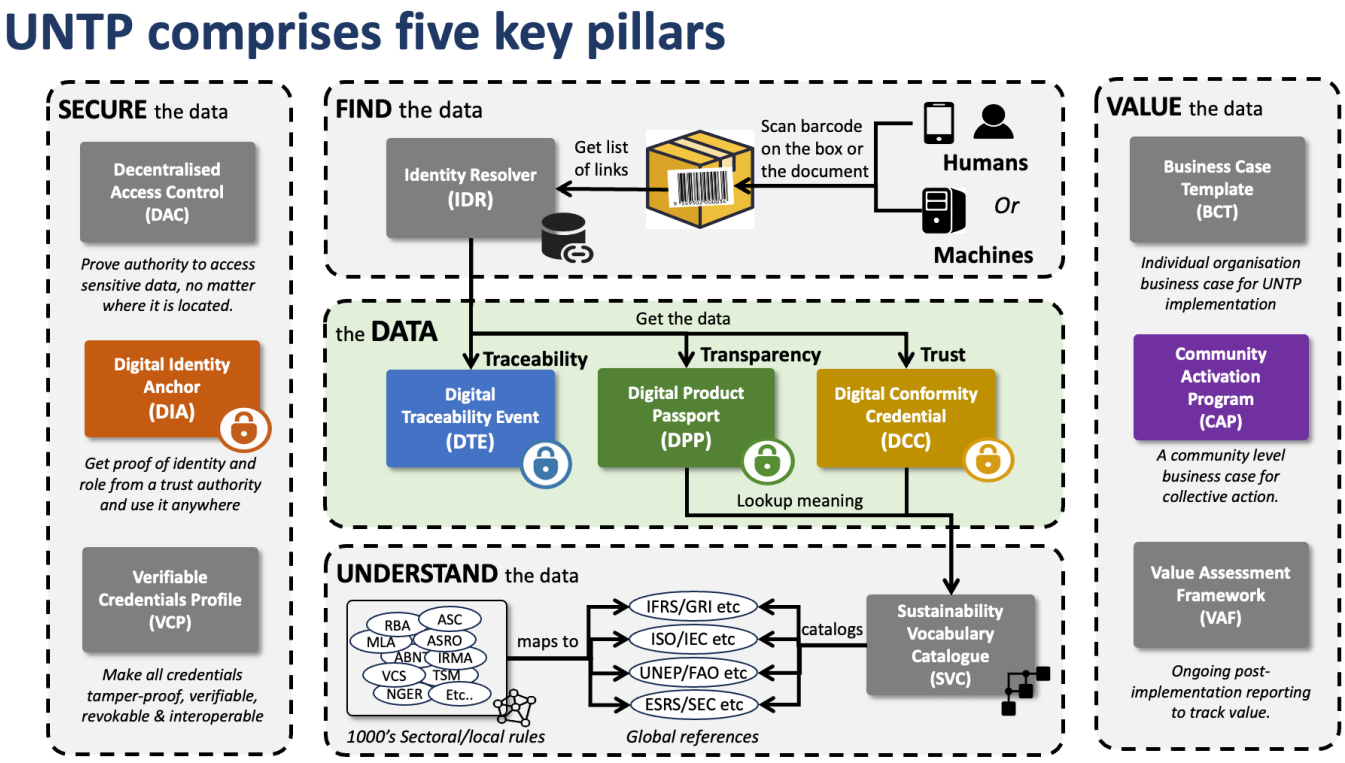
The architecture principles that guide the UNTP design are

Name	Principle	Rationale
No dependency	UNTP should not require any collaboration or dependency between issuers, consumers and verifiers of DPPs	Imposing such collaboration as a pre-requisite for action in a complex many-to-many ecosystem would essentially stall progress
Unknown verifier	UNTP should not assume that that the consumer / verifier of UNTP data is known to the issuer, even when confidential data access is required	In a decentralised architecture with thousands of issuers, it would be impractical to register every authorised verifier with every issuer.
Any maturity	UNTP should not assume any technical maturity for verifiers	DPPs and other credentials must work equally for human and machine verifiers - otherwise an insurmountable complexity of knowing which customer has what capability would be required
Legacy data carriers	UNTP should work with any carrier of a product identifier including 1D barcodes, RFID tags, 2D codes and digital documents	1D barcodes and RFID tags are ubiquitous and will only be replaced slowly. Uptake should not require manufacturers to re-instrument their production lines and printing processes

Name	Principle	Rationale
Verifiability	UNTP should provide confidence in the integrity and trustworthiness of the data	Without trustworthy data, the value of sustainability claims is reduced - possibly to the extent that the business case for adoption is non viable.
Any criteria	UNTP should not dictate any specific sustainability criteria but make the criteria transparent and allow criteria to be mapped (to achieve interoperability)	Costs will explode if every exporter must provide certification to every export market criteria. Where criteria are equivalent, mutual recognition provides a much more cost effective sustainability trajectory.
Action requires value	The benefits of UNTP implementation must exceed the costs.	If not then there will be no implementation

UNTP conceptual overview

Our mission is to support global traceability and transparency **at scale**. To achieve that mission we must not only define the **data** standards but also solve all the barriers to adoption as scale. That includes how to **find** the data, how to **secure** the data, how to **understand** the data, and most critically, how to realise enduring business **value** from the data. These are the five pillars of UNTP.



Small scale tests are possible with any of these pillars missing but scalability to full production volumes is not.

The data

The data is the heart of the UNTP. There are three different data types, each represented as digital Verifiable Credentials.

- The **Digital Product Passport (DPP)** is issued by the product manufacturer and is designed to carry basic product data plus the conformity data (including sustainability assurance data) that is needed by the next actor in the supply chain (ie the buyer of the product). The DPP represents the conformity information as a set of "claims" that specify product performance against specified criteria. In this way, the DPP is essentially a bundle of differentiated value that a buyer can use to choose a preferred supplier. The DPP also provides a statement of material provenance (ie what materials is this product made from and where were the materials sourced). The provenance data assist with ensuring conformance to minimum local content rules or sources under sanction.
- The **Digital Conformity Credential (DCC)** is issued by an independent auditor or certifier and it carries one or more "assessments" of an identified product or facility against well defined criteria. When the product ID and the conformity criteria in the DCC "assessment" match those in the DPP "claim" then the DPP data value is enhanced through independent verification. The DCC must include the identity of the accreditation authority and, where relevant, links to the accreditation authority, so that verifiers can be sure that the auditor or certifier is genuine.
- **The Digital Traceability Event (DTE)** provides a means to trace product batch data throughout the value chain. The DTE links input products (eg bales of cotton from the primary producer) to output products (eg woven cotton fabric). Therefore the DTEs provide a means to trace product provenance through manufacturing processes to discover an entire value chain. DTEs are only available when products are managed and traceable at batch level. DTEs provide links to reach deeper into the value chain which may contain commercially sensitive data and so may only be available to authorised roles.

All three UNTP data structures are designed to be extensible to meet the needs of specific industry sectors or jurisdictions.

Finding the data

We deliberately say "finding" the data rather than "exchanging" the data because a very critical principle is that the issuer of the data usually will not know who will ultimately use it. Obviously each seller knows their immediate buyer but many other actors in a circular economy may also encounter the identified product and need to access the DPP information. It follows that a key principle of UNTP is "if you know the identifier of a product then you can get the data about the product" - even many years after the product was created.

- **Identity Resolver (IDR)** specifications are a concretisation of ISO/IEC 18975 that provide a standardised way to resolve an identifier (of a product, batch, item, facility or entity) to a list of links (URLs) to further information about the identified object. The format of the linkset itself is defined by RFC9264. One identifier can resolve to multiple links, each of which is annotated with a specific link type (eg UNTP DPP). The IDR works with simple identifiers (eg encoded as a traditional 1D barcode) or complex identifiers (eg encoded as a QR code). In this way a single barcode or QR code can return a rich variety of information tailored to the requestor's needs. Furthermore, the IDR can return a collection of similar types of link with different date stamps or versions. One important use case for this capability to to return post-manufacture events such as consumption and eventual recycling of identified products.

Securing the data

As the value of sustainability attributes increases, so the temptation to make fake claims increases. Without confidence in the integrity of data, value is diminished. Additionally, as businesses publish more and more data about their products and

upstream value chains, there is an increased risk of leakage of commercially sensitive information. Without confidence that sensitive data is accessible only to authorised parties, businesses will be less likely to participate. The UNTP security specifications address these challenges.

- **Verifiable Credentials Profile (VCP)**. All UNTP data objects (DPP, DCC, DTE, DIA) are issued as W3C Verifiable Credentials. This ensures that the data, once issued, cannot be tampered with, that the issuer is identifiable, and that status changes like revocation are immediately visible. The VCP defines a simple subset of the larger W3C specifications so that interoperability is simpler and cheaper to achieve. The VCP also includes an human-readable rendering template extension to the W3C specification so that anyone can verify UNTP credentials even if they have no technology maturity.
- **Digital Identity Anchor (DIA)**. The issuers and subjects of Verifiable Credentials are identified using W3C Decentralised Identifiers (DIDs) which provide a means to discover the cryptographic keys necessary to verify the credentials. However, DIDs are self-issued and do not ensure that the issuer is really who they say they are, only that the owner of the DID was certainly the issuer of the credential. The DIA is a Verifiable Credential issued by a trusted authority (eg a government agency) that links a DID to a known public identity such as VAT registration number. In this way, verifiers can be assured of the identity of issuers. The DIA also has a "scope" so that, for example a national accreditation authority can attest to the identity of a certifier but also specify the scope of the accreditation.
- **Decentralised Access Control (DAC)**. Not all traceability and transparency data for a given product is public information. Some is accessible only to authorised roles like a customs authority or a recycling facility. Some is accessible only to the verified purchaser of a product. In centralised systems, this kind of access control is managed by granting privileged access roles to authenticated users. But in decentralised systems such as the world of DPPs, this approach is not practical. There could be thousands of different platforms that host DPPs and it would be impractical for each authorised actor to create accounts on thousands of systems. The DAC defines a simple way to encrypt sensitive data with a unique key for every unique item and a way to distribute decryption keys to authorised roles without any advance knowledge about who has which role. Even if a decryption key is lost or leaked, the scope of data access is limited to one item. The DAC also provides a mechanism for the verified purchaser of an item to **update** the DPP record with post-sale events like consumption, repair, or recycling.

Understanding the data

The UNTP data objects (DPP, DCC, DTE, DIA) are deliberately simple so that they are easy to understand and low cost to implement. However a lot of the structural simplicity of a DPP is achieved via the "claims" object which is a simple abstraction that can carry any sustainability or conformity metric measures against any criteria from any standard or regulation. So this simple abstraction hides a world of complexity. In a world of thousands of standards or regulations, each with dozens or hundreds of distinct criteria, how can one claim about social welfare or biodiversity be meaningfully compared to another? How can an importer know whether a product sustainability criteria from an exporting economy is equivalent to the regulated criteria in the importer's economy? As a corporate subject to sustainability disclosures under IFRS or ESRS, how can I know how to match the claims in a received product passport with the impact areas of my disclosures statement? The UNTP cannot and should not dictate which sustainability standards or regulations any given claim or assessment references. However it can provide a way to map these criteria to a harmonised vocabulary to achieve interoperability.

- The **Sustainability Vocabulary Catalog (SVC)** defines a framework to map sustainability and compliance criteria across different standards, regulations and industry practices. The framework also allows unstructured product, facility, or entity evidence documents to be assessed against compliance criteria, indicating where there are gaps and opportunities to improve compliance. The framework is based on an AI architecture called Retreival Augmented Generation and aims to provide organsiations with a fast and efficient mechanism to quickly assess a complex set of compliance requirements.

As uptake of UNTP grows, maintenance of the SVC is one of the key activities that grows with uptake and adds continuously increasing value to the global sustainability effort.

Valuing the data

Without sufficient commercial incentive, businesses will not act. In some cases the commercial incentive is regulatory compliance. But few economies (The European Union is a notable exception) have current or emerging regulations that demand digital product passports for products sold or manufactured in their economy. However, there is much wider regulatory enforcement of annual corporate sustainability disclosures. But without sustainability data from supply chains at product level, there is no easy way for corporates to accurately meet their annual disclosure obligations. Worse, without product level data from suppliers, there is no way at all for corporates to select suppliers in such a way that they can demonstrate year-on-year improvements to sustainability performance. On top of the disclosure obligation, most corporates are very concerned about reputational risk associates with un-sustainable behaviour from their upstream suppliers. Furthermore, the financial sector is increasingly able and willing to provide improved financial terms for trade finance or investment capital to businesses with strong sustainability credentials. All these incentives drive behaviour and value but there is still some effort needed for each implementer to make a positive business case for change. UNTP offers some tools to determine the value that can inform a positive case for change.

- **Business Case Template (BCT).** A simple template for each role (buyer, supplier, certifier, software vendor, regulator, etc) to make a business case for the investment needed to implement UNTP. Continuously updated and improved with lessons from early implementations, the BCT provides a quick way for sustainability staff to support for their budget requests.
- **Community Activation Program (CAP).** Supply chain actors are often reluctant to proceed with a specific initiative like UNTP unless they have some confidence that others in their industry are doing the same. There are not only obvious interoperability benefits from industry-wide adoption but also cost benefits. For example, it is often the case that a small number of commercial software platforms are commonly used by larger numbers of businesses in a given industry and jurisdiction. So a software vendor that implements UNTP once will benefit all its customers. Additionally there are often a few standards and a few certifiers that are common to an industry and country. Likewise, there are very often one or more existing member associations that represent most of the actors in a given industry and country. Finally, when a large community is willing to act together, there will often be financial incentives from governments and/or development banks that can assist with initial funding. In short, there are many reasons to approach UNTP implementation at a community level. The CAP is a business template for a community level adoption of UNTP including a tool for financial cost/benefit modelling at community level.
- **Value Assessment Framework (VAF).** Once a community or individual implements UNTP and transparency data starts to flow at scale, it will become important to continuously assess the actual value that is realised. Dashboards and scorecards that measure key performance indicators will energise ongoing action and provide valuable feedback at both community and UN level. Therefore the UNTP defines a minimal set of KPIs that each implementer can easily measure and report to their community - and which communities can report to the UN.

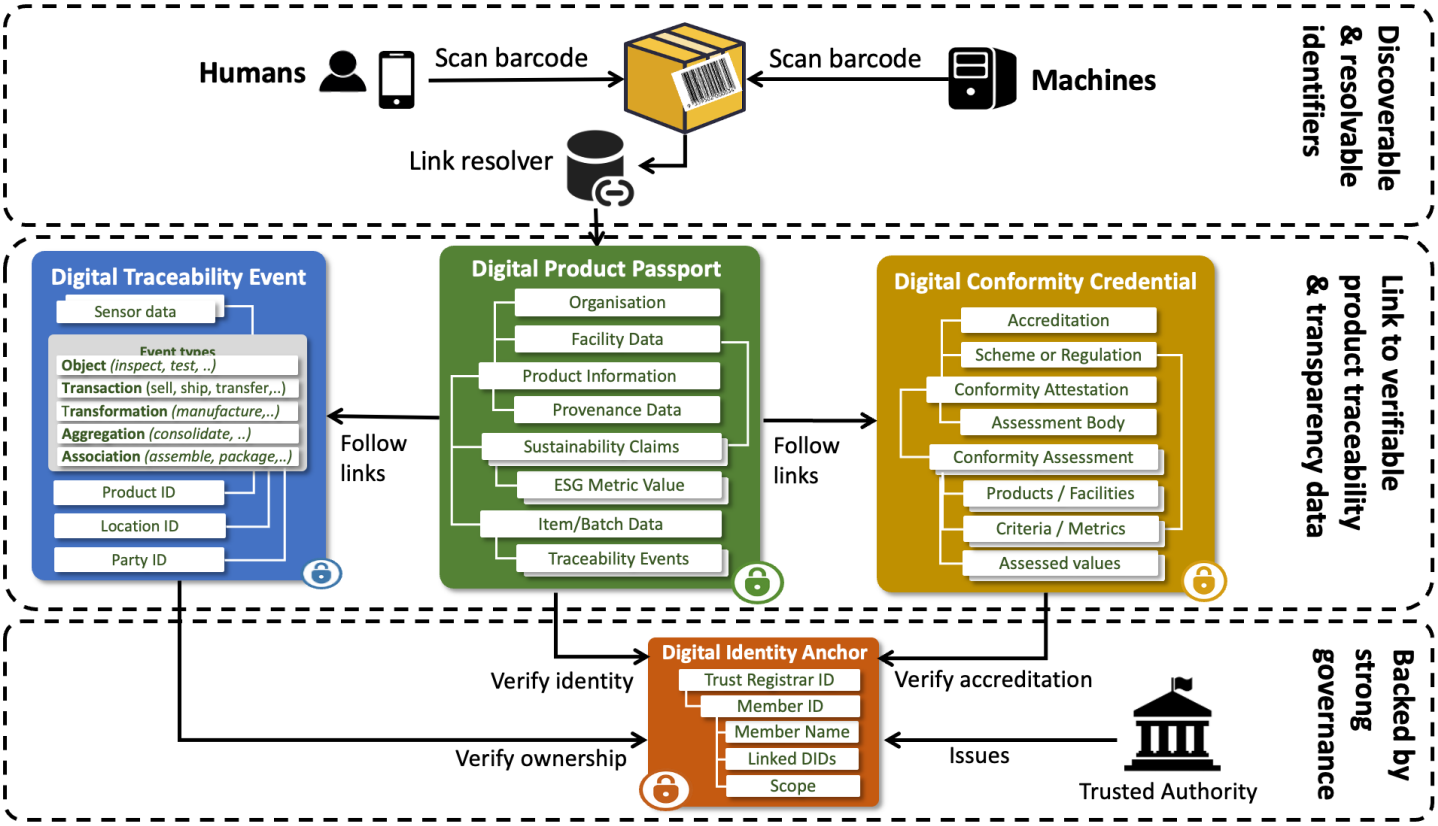
UNTP for one product

This section drills down a little into the key credentials that UNTP defines to answer "what's in a product passport or conformity credential or traceability event?". The diagram shows the perspective of one product. The product identifier (at product, batch or item level) is the key for an Identity Resolver (IDR) to provide links to the UNTP credentials (and any other product related data). Every credential is both human and machine readable so that the same product scan will return a nicely

formatted DPP and related data to a human scanning a barcode or QR code with their phone - or a structured digital data set to an automated scanner at the factory door.

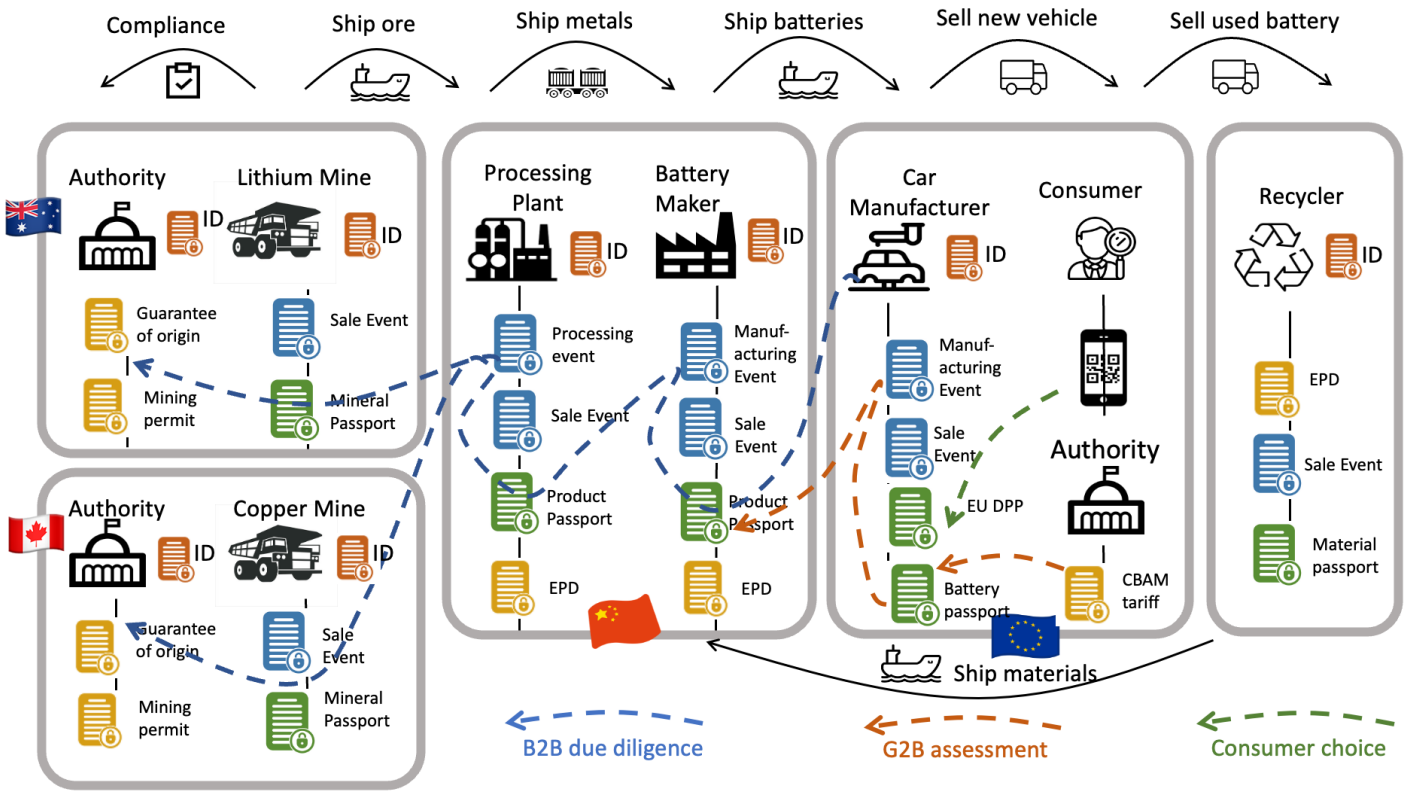
Summary and detailed information about the content of each UNTP credential is available on this site and need not be repeated here

- Digital Product passport (DPP)
- Digital Conformity Credential (DCC)
- Digital Traceability Event (DTE)
- Digital Facility Record (DFR)



UNTP for a value chain

When each actor in a value chain implements UNTP then it becomes possible to trace product provenance across value chains back to primary production. There is no need for all actors in a value chain to collaborate or to implement at the same time. In many cases, the timing and incentives in different industry sectors of the same value chain will be very different. For example a leather goods manufacturer will usually be unable to influence the behaviour of cattle farmers because leather is a by-product and their focus in on the food value chain. Nevertheless, when an agriculture sector implements UNTP for their own reasons, the leather manufacturer can still access the data because UNTP provides a traceability mechanism that crosses industry boundaries without requiring collaboration between those industry sectors. In the example below, a battery can be traced to raw material production even when, from the perspective of the miner, the copper in the anode represents a tiny fraction of production.


Compliance
Ship ore
Ship metals
Ship batteries
Sell new vehicle
Sell used battery
Authority
Lithium Mine
ID
ID
Guarantee of origin
Sale Event
Mining permit
Mineral Passport
Authority
Copper Mine
ID
ID
Guarantee of origin
Sale Event
Mining permit
Mineral Passport
Processing Plant
Battery Maker
ID
ID
Processing event
Manuf-acturing Event
Sale Event
Sale Event
Product Passport
Product Passport
EPD
EPD
Car Manufacturer
Consumer
ID
Manuf-acturing Event
Sale Event
EU DPP
Authority
Battery passport
CBAM tariff
Recycler
ID
EPD
Sale Event
Material passport
Ship materials
B2B due diligence
G2B assessment
Consumer choice

Verifiable Credentials

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

The World-Wide-Web Consortium (W3C) has defined a data model for Verifiable Credentials (VCs). A VC is a portable digital version of everyday credentials like education certificates, permits, licenses, registrations, and so on. VCs are digitally signed by the issuing party and are tamper evident, privacy preserving, revocable, and digitally verifiable. The UN has previously assessed this standard and has recommended its use for a variety of cross border trade use cases in a recent white paper. VCs are inherently decentralized and so are an excellent fit for UNTP which recommends that passports, credentials, and traceability events are all issued as W3C VCs. A related W3C standard called Decentralized Identifiers (DIDs) provides a mechanism to manage the cryptographic keys used by verifiable credentials and also to link multiple credentials into verifiable trust graphs. DIDs are not the same as the business / product / location identifiers maintained by authoritative agencies - but can be linked to them.

Business requirements for UNTP application of VCs

Verifiable Credentials technology is one of the key tools in the UNTP anti-green-washing toolbox. But there are many different technical implementation options which presents an interoperability risk - namely that credentials issued by one party will not be understandable or verifiable by another party. UNTP will not design new technical standards as that is the role of technology standards bodies such as W3C or IETF. However, be recommending the use of the narrowest practical set of technical options for a given business requirement, the UNTP can enhance interoperability.

A key design principle that is applicable to decentralized ecosystems such as UNTP recommends is Postel's robustness principle which, for UNTP, means that **an implementation should be conservative in its sending (issuing) behavior, and liberal in its receiving (verifying) behavior.** That is because the sustainability evidence that is discovered in any given value chain may be presented as many different versions of W3C VCs, or ISO mDL credentials, or Hyperledger Anoncreds, or as human readable PDF documents. Being as open as possible in what is received and verified will allow sustainability assessments to be made over a wide set of evidence. Conversely, choosing a narrow set of ubiquitous technology options when issuing UNTP credentials such as digital product passports will simplify the task of verifiers and minimise costs for the entire ecosystem.

ID	Name	Requirement Statement	Solution Mapping
VC-01	Integrity	VC technology recommendations must support tamper detection, issuer identity verification, and credential revocation so that verifiers	All VC options support this

ID	Name	Requirement Statement	Solution Mapping
		can be confident of the integrity of UNTP credentials.	requirement
VC-02	Compatibility	VC technology recommendations for issuing UNTP credentials should be as narrow as practical and should align with the most ubiquitous global technology choices so that technical interoperability is achieved with minimal cost	Basic profile
VC-03	Human readable	VC technology recommendations must support both human readable and machine readable credentials so that uptake in the supply chain is not blocked by actors with lower technical maturity.	Render method
VC-04	Discovery	VC technology recommendations must support the discovery and verification of credentials from product identifiers so that verifiers need not have any a-priori knowledge of or relationship to either the issuers or the subjects of credentials.	Presentations
VC-05	Semantics	VC technology recommendations must support the use of standard web vocabularies so that data from multiple independent credentials can be meaningfully aggregated.	Vocabularies
VC-06	Performance	VC technology recommendations should value performance so that graphs containing hundreds of credentials of any size can be traversed and verified efficiently.	Basic profile
VC-07	Compliance	VC technology recommendations must meet any technology based regulatory requirements that apply in the countries in which credentials are issued or verified.	Basic profile
VC-08	Openness	VC DID method recommendations must not drive users towards closed ecosystems or proprietary ledgers so that there is no network effect coercion towards proprietary ledgers.	DID methods
VC-09	Portability	VC DID method recommendations must allow users (issuers) to move their DID documents between different service providers so that long duration credentials can remain verifiable even when issuers change service providers.	DID methods
VC-10	Evolution	VC technology is evolving and UNTP recommendations must evolve as newer tools and versions become ubiquitous	Roadmap

Verifiable Credential Profile

VCDM profile

The VC basic profile is designed to be as simple, lightweight, and interoperable as possible. A conformant implementation

- MUST implement the W3C VC Data Model v2.0 using the JSON-LD Compacted Document Form
- MUST implement W3C VC Bitstring Status List for credential status management including revocation
- MUST implement W3C-DID-CORE using DID methods defined in DID methods
- MUST implement the enveloping proof mechanism defined in W3C VC JOSE / COSE with JOSE (Section 3.1.1)

DID methods

There are a large number of did methods listed in the W3C did register. It is reasonable to expect that this proliferation of did methods will consolidate to a much smaller number of did methods, each designed to meet a specific business need. In future the UNTP may provide a did method decision tree with different methods for different use cases (eg legal entities vs products). In the meantime, a conformant implementation

- MUST implement the did:web method as an Organizational Identifiers
- SHOULD implement the did:web method using the web domain of the issuer to avoid portability challenges.

> Note that there is activity within the VC technical community to define new did methods that achieve the ubiquity of did:web whilst still maintaining portability across web domains. For example Trusted DID Web. This work may impact future UNTP DID method recommendations.

Render Method

To support uptake across supply supply chain actors with varying levels of technical maturity, human rendering of digital credentials is essential. A conformant implementation

- SHOULD use the `renderMethod` property as defined in the VC data model.

Presentations

Verifiable Presentations (VP) are widely used in the verifiable credentials ecosystem to support holders to combine one or more credentials in a digital wallet and then present them for in-person or online verification purposes. The VP is signed by the holder did and so provides a holder binding mechanism. In UNTP supply chain implementations, the subject of most claims is an inanimate object (eg bar-coded goods) and digital credentials about the goods are discovered by any party that has access to the goods. The box of goods does not create verifiable presentations on demand and the binding is to the identity of the goods. A conformant UNTP implementation

- MUST issue and publish product passports, product conformity credentials, and traceability events as verifiable credentials and MUST include the identifier of the goods within the VC subject.
- MAY exchange these and any other credentials as verifiable presentations in wallet-to-wallet transfers or any other method.

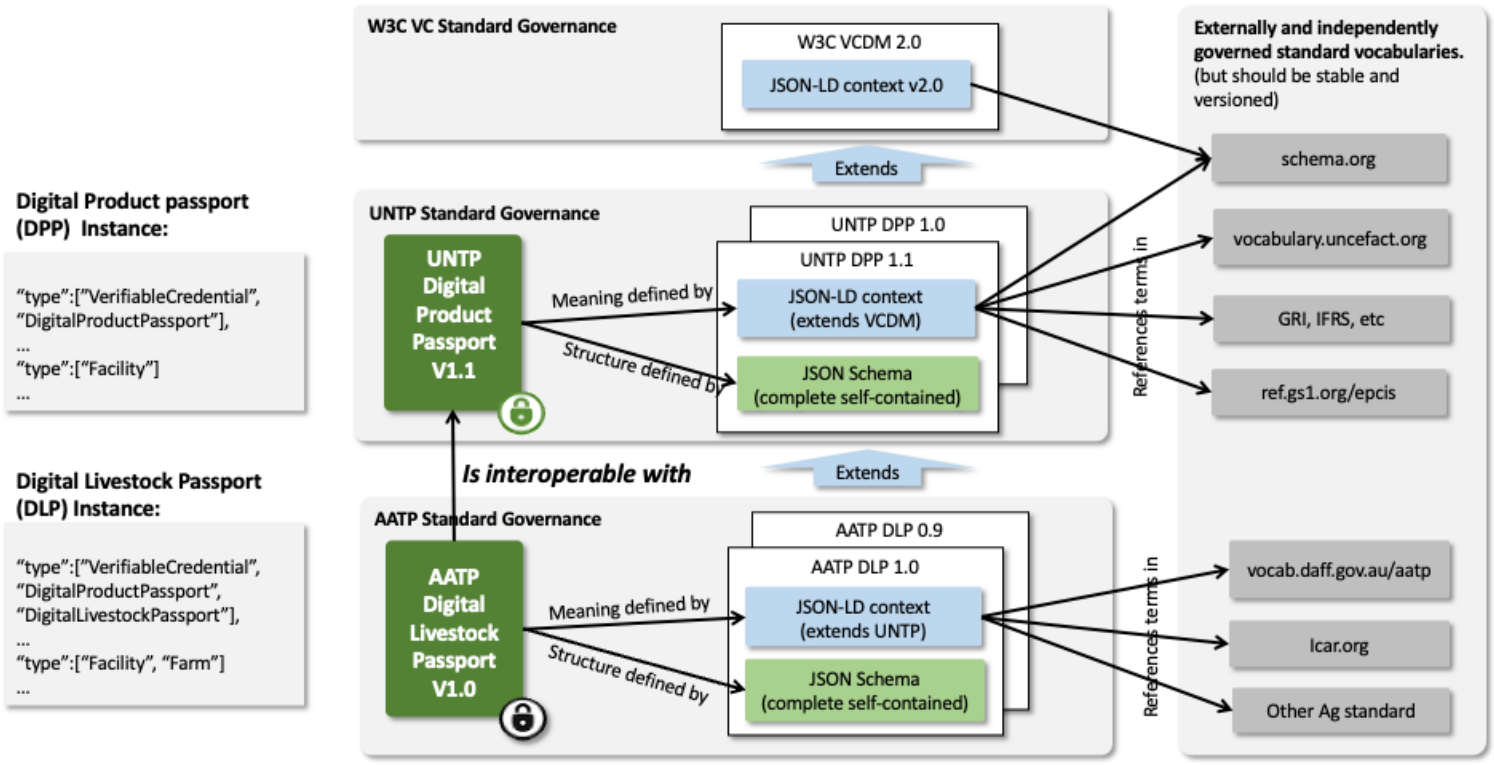
Vocabularies

A shared understanding of the meaning of claims made in verifiable credentials is essential to interoperability. To this end, conformant UNTP implementations

- MUST use the JSON-LD syntax for the representation of data in all issued credentials.
- MUST reference the relevant UNTP @context file for the given credential type. These context files are themselves extentions of the W3C VC Data Model 2.0 context.
- MAY extend credentials with additional properties but, if so, MUST include additonal @context file reference that defines the extended properties. The @vocab "catch-all" mechanism MUST NOT be used.
- SHOULD implement widely used industry vocabularies such as schema.org or GS1 web vocabulary as a first choice for UNTP extensions requiring terms not in the UN vocabulary.
- MAY use any other published JSON-LD vocabulary for any other industry or country specific extensions.
- MUST maintain @context files at the same granularity and version as the corresponding credentila type. This prevents the risk of verification failures when context files change after credentials are issued.
- SHOULD provide a complete and versioned JSON schema for each credential type. This is to facilite simple and robust implementations by developers without detailed knowledge of JSON-LD.

The data governance architecture for UNTP credentials is shown below. the key points to note are

- That credential instances contain Verifiable Credential Data Model (VCDM) type references for each unquely identified linked-data object. Each extension builds upon parent types and is enumerated in the type array (eg `["Facility", "Farm"]`).
- UNTP @context types are `protected` and so MUST not be duplicated in extensions. Similarly UNTP @context does not duplicate `protected` terms in WCDM @context.
- Unlike @context files, the JSON schema for each credential MUST be a complete schema that defines the entire credential including terms from VCDM and UNTP.



Roadmap

Future versions of this specification will

- Provide richer guidance on did methods via a decision tree that helps to select the right method for the right purpose
- Provide guidance on selective redaction methods to better support confidentiality goals.
- Provide timelines for transition between versions of technical specifications

Digital Product Passport

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at https://test.uncefact.org/vocabulary/untp/dpp/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Jan 2025

Release for Pilot Testing

Version 0.5.0 release artifacts can be used for pilot testing.

- JSON-LD @context
- JSON Schema
- Sample JSON Instance

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

Version History

History of releases is available from the **Version history** page.

Default Render Template

A UNTP digital product passport may be rendered in any format desired by the issuer. However a default **Template Design** is provided here and includes mapping of visual rendering elements to the Logical Data Model.

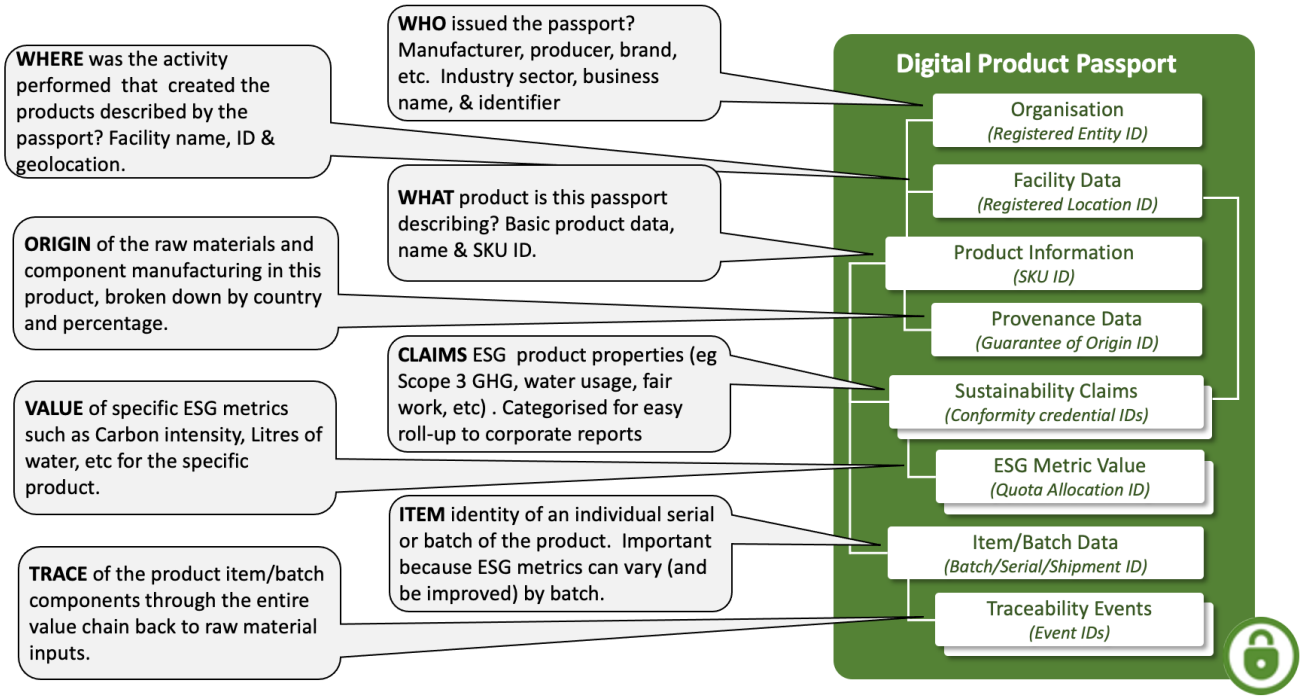
Sample Credential

URL	QR	Description
Sample Digital Battery Passport		A sample digital product passport as a JWT envelope signed Verifiable Credential. The URL (or QR scan) resolved to a hosted verifier that displays a human readable version. Raw JSON data can be viewed via the `JSON` tab and the full credential can be dlownloaded via the download button.

Overview

The digital product passport (DPP) is issued by the shipper of goods and is the carrier of **product and sustainability information** for every serialised product item (or product batch) that is shipped between actors in the value chain. It is deliberately **simple and lightweight** and is designed to carry the minimum necessary data at the **granularity** needed by the receiver of goods - such as the scope 3 emissions in a product shipment. The passport contains links to **conformity credentials** which add trust to the ESG claims in the passport. The passport also contains links to **traceability events** which provide the "glue" to follow the linked-data trail (subject to confidentiality constraints) from finished product back to raw materials. The UNTP DPP does not conflict with national regulations such as the EU DPP. In fact, it can usefully be conceptualised as the **upstream B2B feedstock** that provides the data and evidence needed for the issuing of high quality national level product passports.

Conceptual Model



Requirements

The digital product passport is designed to meet the following detailed requirements as well as the more general UNTP Requirements.

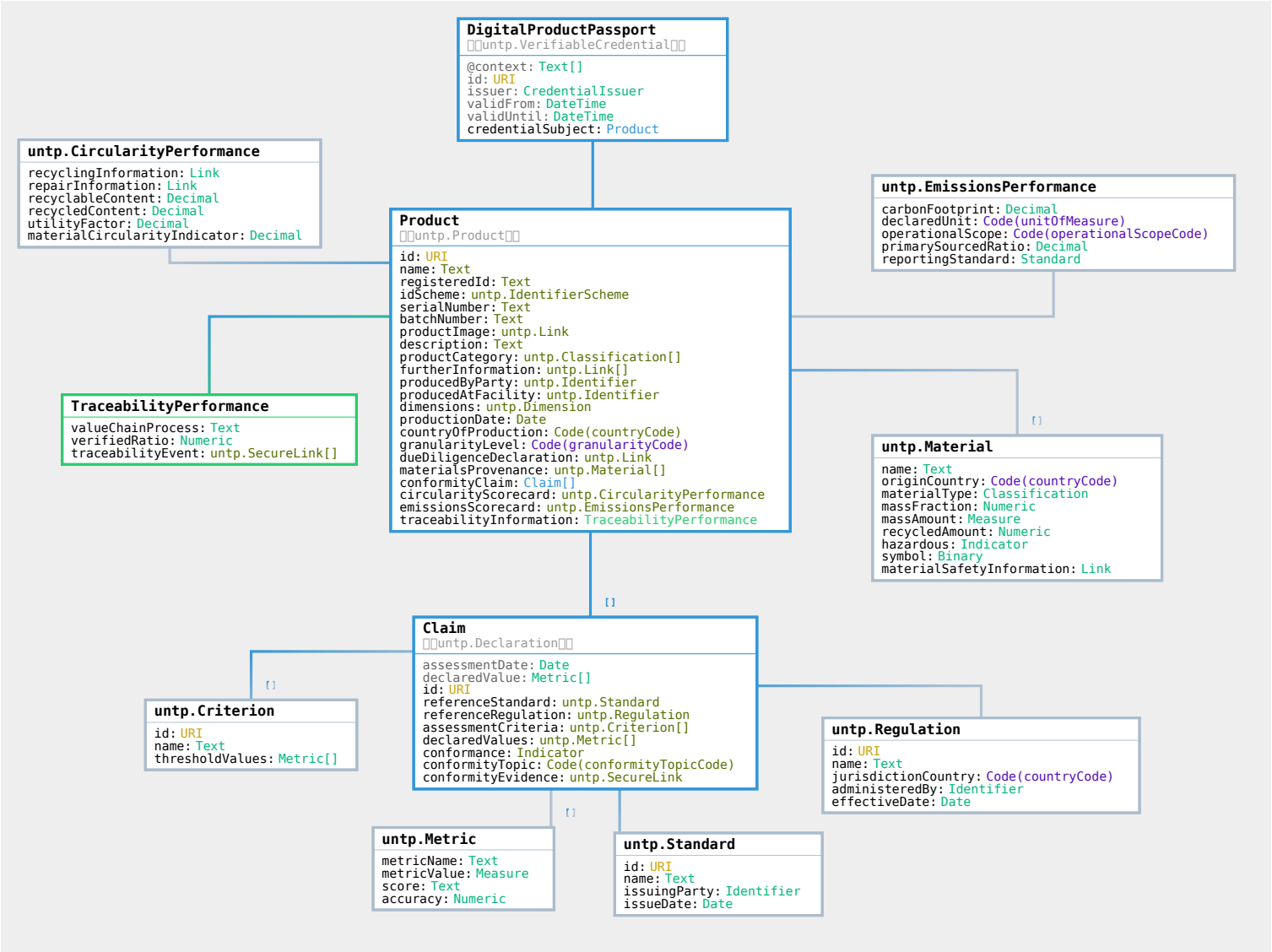
ID	Name	Requirement Statement	Solution Mapping
DPP-01	Granularity	The DPP should support use at either *model* level or at *batch* level or at serialised *item* level.	Claims are made at the passport level, which MUST have a related model and MAY have a related batch and item
DPP-02	Classification	The DPP should support any number of product classifications using codes from a defined classification scheme (eg UN-CPC)	The classifications property
DPP-03	Materials provenance	The DPP should provide a simple structure to allow issuers to break down the material composition of their products by mass fraction and origin country so that raw material provenance requirements are easily assessed and met.	The DPP "materialsProvenance" structure is designed to meet this need.

ID	Name	Requirement Statement	Solution Mapping
DPP-04	Produced at	The DPP should provide a simple structure to describe the manufacturing facility at which the product was made. The facility identifier SHOULD be resolvable and verifiable and SHOULD link to cadastral boundary information.	The "Facility" structure including the location class is designed to meet this need
DPP-05	Dimensions	The DPP must support the definition of key product dimensions such as length, width, height, weight, volume so that conformity claims made at the unit level (eg Co2 intensity in Kg/Kg) can be used to calculate actual values for the shipped product	Dimensions class
DPP-06	Traceability	The DPP should provide a means to follow links to further DPPs and conformity credentials of constituent products so that (subject to confidentiality constraints), provenance claims can be verified to any arbitrary depth up to primary production	The links to ISO/IEC 19987 (EPCIS)-based traceability event credentials from the productBatch class is designed to meet this need
DPP-07	characteristics	The DPP should allow an issuer to provide descriptive information about the product (image, description, etc) that is extensible to meet industry specific needs.	Characteristics property as an industry extension point
DPP-08	Verifiable Party	The DPP should provide DPP issuer, product manufacturer, and facility operator identification including a name, a resolvable and verifiable identifier, and proof of ownership of the identifier	DigitalProductPassport.Issuer Product.ProducedByParty, Product.ProducedAtFacility - all are uniquely identified objects and SHOULD have related resolvable Identity Resolver credentials
DPP-09	Claims	The DPP MUST provide a means to include any number of conformity claims within one DPP so that it can provide simple single point to aggregate all claims about the product in one place	The "conformityClaims" array is designed to meet this need
DPP-10	Conformity Topic	The DPP MUST provide a simple mechanism to express the sustainability/circularity/conformity topic for each claim so that similar claims can be grouped and the high level scope easily understood.	The ConformityTopic code list is designed to meet this need

ID	Name	Requirement Statement	Solution Mapping
DPP-11	Metrics	The DPP MUST provide a simple mechanism to quantify a conformity claim (eg carbon intensity, water consumption, etc) and to express any accuracy range and also to compare the claimed value to a relevant benchmark such as a standard/regulation requirement or an industry average	The "Metric" class is designed to meet this need
DPP-12	Criteria	The DPP MUST provide a means to reference a standard or regulation as well as the specific criteria within that standard or regulation - so that claims can be understood in terms of the criteria against which they are made.	Claim.referenceRegulation, Claim.referenceStandard, Claim.referenceCriterion
DPP-13	Evidence	The DPP MUST provide a means to reference independent conformity assessments that support and verify the claims being made. The related evidence SHOULD be digitally verifiable but MAY be a simple document or web page. The confidence level attached to the evidence should be clear.	The Claim.conformityEvidence property references a relevant digital conformity credential

Logical Model

The Digital Product Passport is an assembly of re-usable components from the UNTP core vocabulary.



Core Vocabulary Documentation

The UNTP core types vocabulary defines the uniquely identified Linked Data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the building blocks for construction of Digital Product Passports and Digital Conformity Credentials.

DPP Documentation

The DPP documentation provides a technology-neutral definition of classes, properties and code lists in the DPP model.

Implementation Guidance

This section provides sample JSON-LD snippets for each DPP component.

Verifiable Credential

All DPPs are issued as W3C Verifiable Credentials and MUST conform to the VCDM 2.0. Also note that all identified objects (ie those with an "id" property also have a "type" property that indicates the Linked Data type of the object. The "type" values must be defined in the associated JSON-LD @context file. Key points to note from the VC sample below are

- That the credential type is both a W3C "VerifiableCredential" and a UNTP "DigitalProductPassport". The DPP is an extension of the VCDM.
- That the "@context" reference similarly lists both the W3C VCDM context URL and the UNTP DPP context URL.
- The "id" is any globally unique reference for this specific DPP credential - typically a domain/UUID pattern.
- The issuer property, unlike most VC examples, is an object with multiple properties.
  - The object conforms to the UNTP "CredentialIssuer" type.
  - The id SHOULD be a DID and, if it is a DID then it MUST be a did:web.
  - The name property provides a human readable name of the issuer.
  - The array of "otherIdentifiers" is used to provide references to authoritative business identifiers for the issuer. In the example shown the issuer is also identified as an Australian Business with an ABN and link to the authoritative business register entry.
- The validFrom and ValidTo fields are as defined in the W3C VCDM. They are optional but UNTP DPPs SHOULD include a validFrom date representing the date that the DPP was issued.
- The credential subject carries the bulk of the digital product passport information. It's type is both a UNTP "Entity" and a UNTP "Product".


```
{
  "type": [
    "DigitalProductPassport",
    "VerifiableCredential"
  ],
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://test.uncefact.org/vocabulary/untp/dpp/0.3.10/"
  ],
  "id": "https://example-company.com/credentials/2a423366-a0d6-4855-ba65-2e0c926d09b0",
  "issuer": {
    "type": [
      "CredentialIssuer"
    ],
    "id": "did:web:identifiers.example-company.com:12345",
    "name": "Example Company Pty Ltd",
    "otherIdentifier": [
      {
        "type": [
          "Identifier"
        ],
        "id": "https://business.gov.au/ABN/View?abn=1234567890",
        "name": "Sample Company Pty Ltd",
        "registeredId": "1234567890",
        "idScheme": {
          "type": [
            "IdentifierScheme"
          ],
          "id": "https://business.gov.au/ABN/",
          "name": "Australian Business Number"
        }
      }
```

```
    ]
  },
  "validFrom": 2024,
  "validUntil": 2034,
  "credentialSubject": {
    "type": [
      "Product",
      "Entity"
    ],
    "id": "https://id.gs1.org/01/09520123456788/21/12345",
    ... remainder of product passport information goes here ...
```

Product

The Product object is the the subject of the verifiable credential. Key points to note from the product snippet below are

- That the product identification comprises five properties that identify both the specific product and the identifier scheme as defined by the UNTP Entity core type. The expectation is that the product ID in the DPP will match the information printed on the physical product or its container (for bulk goods) and that the identifier is a resolvable and verifiable ID. So, scanning a physical product QR code (or resolving its 1D barcode) should return a link type that is a pointer to the DPP described by the specification.
- DPPs may be issued at product class level (i.e. all shoes of the same model) or at the individual item level (ie this specific serialised pair of shoes). `serialNumber` and/or `batchNumber` MUST be provided if the DPP is issued at item level.
- The `productImage` is expected to be an instance of the UNTP `Link` object that provides linkURL and metadata.
- `productCategory` is expected to be an array of UNTP `Classification` objects that classify the product using a global scheme such as UN CPC. Industry-specific classification schemes (eg cattle breed) may also be used.
- `furtherInformation` is an array of UNTP `Link` types that optionally provide links to additional information such as material safety data sheets etc. The `linkType` values should match the linkTypes returned by an Identity Resolver service for the same product ID.
- `producedByParty` is a UNTP `Entity` type that identifies the producer or manufacturer of the product.
- `producedAtFacility` is a UNTP `Entity` type that identifies the manufacturing site or farm or mine site where the product was produced.
- The `dimensions` object defines the `length`, `width`, `height`, `weight`, `volume` dimensions of the product. Implementers should choose the relevant dimensions to include for the product.
- The `productionDate` is relevant for batch or serialised items and should indicate the date that the specific batch or item was produced.
- The `countryOfProduction` property must carry the ISO-3166 two letter country code for the country where the product was manufactured. Note that this represents only the country of manufacture for the identified product. The provenance of materials used to make the product are defined separately.
- The `characteristics` property provides an extension point for commodity-specific properties such as battery capacity in AmpHours or shirt size. UNTP does not define values for this property but does provide guidance for industry extensions.
- `granularityLevel` indicates whether this digital product passport is issued at product class level, batch level, or serialised item level.

- `dueDiligenceDeclaration` is a link to a due diligence declaration that meets the legal requirement of the importing economy.
- `materialsProvenance` is an array of UNTP `Material` types that define the origin and characteristics of constituent materials in the product.
- `conformityClaims` is an array of `Claim` types that list the product quality or sustainability claims made by the manufacturer against criteria defined by a reference standard or regulation. The sustainability vocabulary is designed to accommodate the very diverse set of conformity criteria expressed by various standards and regulations.
- `circularityScorecard` is a simple object that defines the overall percentage of recycled content (and recyclable content) as well as links to recycling and repair information.
- `emissionsScorecard` is a simple object that defines the carbon footptint of the product against a defined reporting standard, the scope 3 boundaries, and the extent to which the data is accruately measured.
- `traceabilityInformation` is an array of `Link` objects that reference UNTP Digital Traceability Events. This provides traceability through the value chain via events such as the TransformationEvent that lists the input product identifiers and the output product identifiers for a manufacturing process.


```
"credentialSubject": {
   "type": [
      "Entity",
      "Product"
      ],
  "id": "id.example.com/01/09520123456788/10/6789/21/12345",
  "name": "Baked beans, tinned, 500g.",
  "idValue": "09520123.456788",
  "idScheme": "ref.gs1.org/ai/",
  "idSchemeName": "GS1 SGTIN",

  "serialNumber": "12345",
  "batchNumber": "6789",
  "productImage": {},
  "description": "Big and tender Great Northern Beans in tasty tomato sauce. These beans are rich in
fiber and low in fat. Fiber rich food helps to maintain a healthier digestive system & reduces
cholesterol.",
  "productCategory": [],
  "furtherInformation": [],
  "producedByParty": {},
  "producedAtFacility": {},
  "dimensions": {},
  "productionDate": "2024-04-25",
  "countryOfProduction": "AU",
  "granularityLevel":"batch",
  "dueDiligenceDeclaration":{ },
  "characteristics": { },
  "materialsProvenance": [],
  "conformityClaim": [],
  "circularityScoreCard": {},
  "emissionsScorecard" : {},
  "traceabilityInformation": []
```


Dimensions

The `dimension` type is a simple array of decimal values for length, width, height, weight, and volume. Units MUST be drawn from UNECE recommendation 20 units of measure

```
"dimensions": {
  "length": {"value": 0.87,"unit": "MTR"},
  "width": {"value": 0.5,"unit": "MTR"},
  "height": {"value": 0.3,"unit": "MTR"},
  "weight": {"value": 8, "unit": "KGM"},
  "volume": {"value": 7.5,"unit": "LTR"}
```

Materials Provenance

An array of `Material` objects is used to describe the constituent materials in a product and to define some key properties of each material

- A human readable `name`
- The `originCountry` as a 2-letter ISO-3166 code.
- The material type as a UNTP `Classification` object. The relevant classification scheme to use depends on the commodity type of the products but, unless otherwise stated the material CAS number together with a URI to a relevant registry entry (eg https://chem.echa.europa.eu/100.028.325)
- The `massFraction` is the percentage by mass of the product that is made from this constituent material.
- The `recycledAmount` is the percentage by mass of this material constituent that is made from recycled sources.
- The `hazardous` flag is a boolean that indicates whether this material constituent is a hazardous material
- If the hazardous flag is `true` then a `Link` object should provide `materialSafetyInformation`.

```
"materialsProvenance": [
  {
  "name": "Egyptian Cotton",
  "originCountry": "EG",
  "materialType": {},
  "massFraction": 50,
  "massAmount":{"value":10,"unit":"KGM"}
  "recycledAmount": 50,
  "hazardous": "false",
  "materialSafetyInformation": {}
}
```

Emissions Scorecard

The Emissions scorecard provides an overall GHG emissions performance indicator for the product. More detailed emissions performance data measured against specific criteria and standards would be placed into the `conformityInformation` structure.

- The carbonFootprint represents GHG emissions intensity CO2eq for the product.
- The declared unit defines the product unit per KG Co2Eq (usually KGM)

- the operational scope represents the scope 3 boundary - which should be cradle to gate for DPPs (ie does not include post sale footprint)
- the primarySourcedRatio indicates the proportion of scope 3 emissions data that is directly sources (rather than estimated)

```
  "emissionsScorecard": {
    "carbonFootprint": 1.5,
    "declaredUnit": "KGM",
    "operationalScope": "Scope123toGate",
    "primarySourcedRatio": 0.3,
    "reportingStandard": {
      "type": [
        "Standard"
      ],
      "id": "hhttps://www.wbcsd.org/resources/pathfinder-framework-version-2-0/",
      "name": "WBSCD Pathfinder framework - V.2.0",
      },
      "issueDate": 2023
    }
  },
```

Circularity Scorecard

The circularity Scorecard provides a simple high level summary of circularity performance of the product. This summary may be further supported by detailed information and evidence in one or more `Declarations` within the `conformityInformation` data.

- `recyclingInformation` provides a `Link` to recycling instructions. Primarily targeted at recycling centers.
- `repairInformation` provides a link to repair instructions. Primarily targeted at end users or repair service centers.
- `recyclableContent` is a percentage indicating the proportion by mass of the product that is designed to be recycled.
- `recycledContent` is a percentage indicating the proportion by mass of the product that is made from recycled materials
- `utiltiyFactor` provides a measure of durability of the product above or below industry average
- `materialCircularityIndicator` provides an overall circularity score which is a function of all three of the above measures MCI reference

```
  "circularityScorecard": {
    "recyclingInformation": {
      "linkURL": "https://files.example-company.com/products/123456789/recycling.pdf",
      "linkName": "Recycling instructions",
      "linkType": "https://www.gs1.org/voc/recyclingAndRepairInfo"
    },
    "repairInformation": {
      "linkURL": "https://files.example-company.com/products/123456789/repair.pdf",
      "linkName": "Repair instructions",
      "linkType": "https://www.gs1.org/voc/recyclingAndRepairInfo"
    },
    "recyclableContent": 0.5,
    "recyecledContent": 0.3,
    "utilityFactor": 1.2,
```

```
      "materialCircularityIndicator": 0.67
    },
```

Traceability Information

Traceability Information is an array of TraceabilityPerformance objects which are designed to group traceability data according to value chain process. Each value chain step SHOULD specify the extent to which materials and compon ents in that step have been verifiably traced. An array of links (with context information) to UNTP Digital Traceability Event (DTE) structures by also be provided.

```
"traceabilityInformation":[
   {"valueChainProcess":"Cell Manufacture",
    "verifiedRatio":0.5,
    "traceabilityEvent":[
     {
       "linkURL": "https://files.sampleCompany.com/events/123456789.json",
       "linkName": "Battery Assembly Event",
       "linkType": "https://test.uncefact.org/vocabulary/linkTypes/dte",
       "hashDigest": "50af99a26f4af48c9f4ad8cf9d2f5018780ab4bb1167f0e94884ec228f1ba832",
       "hashMethod": "SHA-256",
       "encryptionMethod": "AES"
     }]
  }]
```

Conformity Information

Conformity information is included in the DPP as an array of UNTP `Declaration` structures. The same structure is re-used for third party assessments in UNTP Digital Conformity Credentials (DCC). Please refer to the Sustainability Vocabulary Page for further information and examples.

Conformity Credential

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at https://test.uncefact.org/vocabulary/untp/dcc/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Jan 2025

Release for Pilot Testing

Digital Conformity Credential version 0.5.0 release artifacts can be used for pilot testing.

- JSON-LD @context
- JSON Schema
- Sample Instance

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

Version History

History of releases is available from the **Version history** page.

Default Render Template

A UNTP digital product passport may be rendered in any format desired by the issuer. However a default **Template Design** is provided here and includes mapping of visual rendering elements to the Logical Data Model.

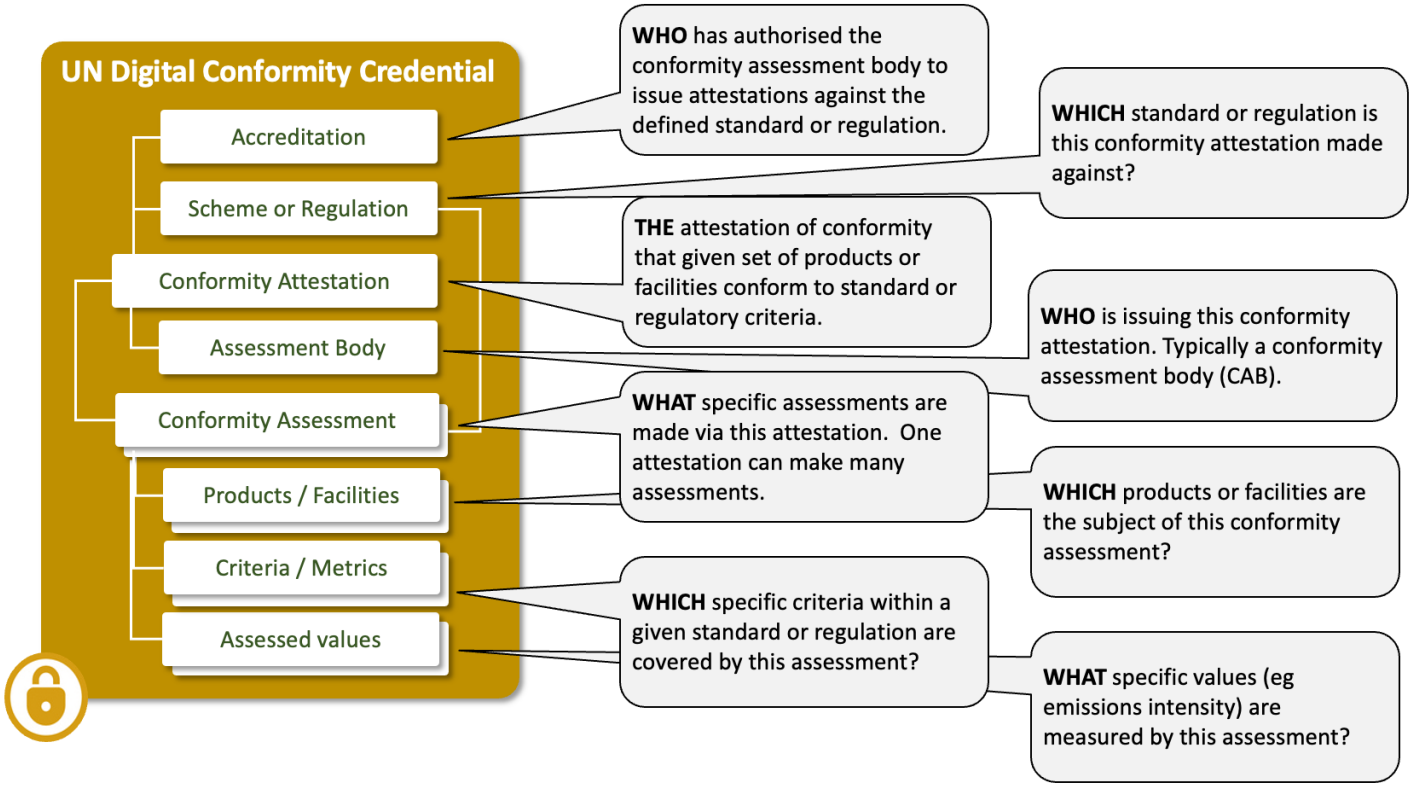
Sample Credential

URL	QR	Description
Sample Battery Performance and Safety Certificate		A sample digital conformity credential as a JWT envelope signed Verifiable Credential. The URL (or QR scan) resolved to a hosted verifier that displays a human readable version. Raw JSON data can be viewed via the `JSON` tab and the full credential can be dlownloaded via the download button.

Overview

Conformity credentials are usually issued by independent parties and provide a **trusted assessment** of product ESG performance against credible **standards or regulations**. As such the credential provides trusted verification of the ESG claims in the passport. Since the passport may make several independent claims (eg emissions intensity, deforestation free, fair work, etc) there may be many linked conformity credentials referenced by one passport. As an additional trust layer, the conformity credential may reference an **accreditation** credential that attests to the authority of the party to perform the specific ESG assessments. The conformity credential data model has been developed by a separate UN/CEFACT project on digital conformity that has expert membership from accreditation authorities and conformity assessment bodies.

Conceptual Model



Requirements

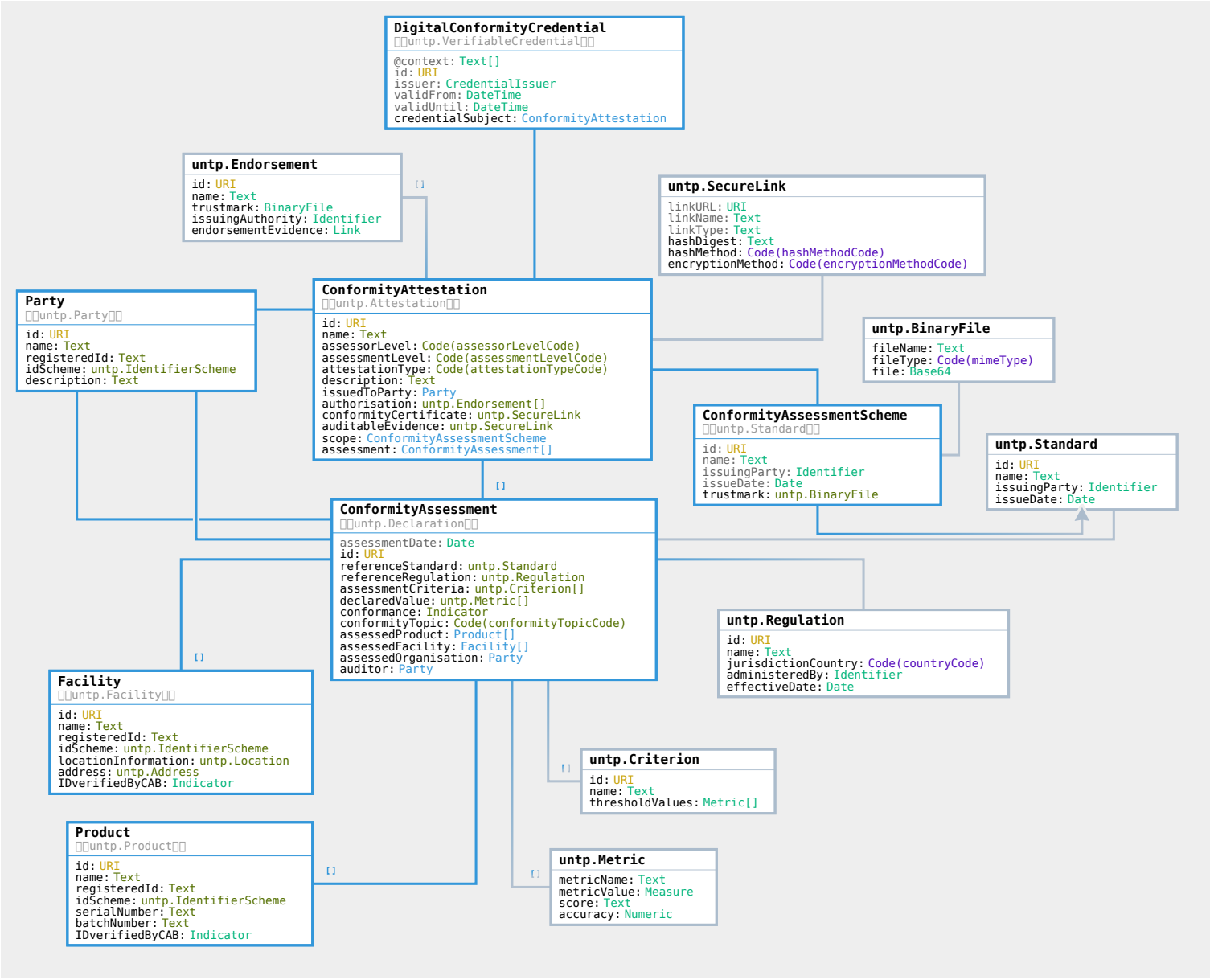
The digital product conformity credential (DPCC) is designed to meet the following detailed requirements as well as the more general [UNTP Requirements(https://uncefact.github.io/spec-untp/docs/about/Requirements)]

ID	Name	Requirement Statement	Solution Mapping
DPCC-01	Authorised	The DCC MUST be verifiable as issued by an authorised body, typically a conformity assessment body (CAB)	DPCC MUST be issued as a digital verifiable credential signed by the CAB
DPCC-01	Assurance level	The DPCC MUST the identify the nature of any authority or support for attestation, such as formal recognition by a Governmental authority or an Accreditation Body	Attestation. accreditation property
DPCC-03	Object of conformity	The DPCC MUST unambiguously identify the object of the conformity assessment, whether a product or facility.	Assessment. assessedProducts, Assessment. assessedFacilities
DPCCE-04	Reference standard or regulation	The DPCC MUST identify the reference standard(s) and/or regulation(s) that specify the criteria against which the conformity assessment is made. If	ConformityAssessment. referenceStandard and ConformityAssessment. assessmentCriterion

ID	Name	Requirement Statement	Solution Mapping
		appropriate this must include specific measurable thresholds (eg minimum tensile strength)	
DPCC-05	Conformity Attestation	The DPCCE MUST unambiguously state whether or not the object of the assessment is conformant to the reference standard or regulation criteria	ConformityAssessment.compliance
DPCC-06	Measured metrics	The DPCCE SHOULD include actual measured values (eg emissions intensity, tensile strength, etc) with the conformity assessment	ConformityAssessment.declaredValues
DPCC-07	Evidence	The DPCCE MAY include references to audit-able evidence (eg instrument recordings, satellite images, etc) to support the assessment. If so then the hash of the evidence file-set SHOULD be included (so that an auditor can be sure that the evidence data has not changed). The evidence data MAY be encrypted with decryption keys provided on request	ConformityAttestation.auditableEvidence

Logical Model

The Digital Conformity Credential is an assembly of re-usable components from the UNTP core vocabulary.



Core Vocabulary

The UNTP core types vocabulary defines the uniquely identified Linked Data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the building blocks for construction of Digital Product Passports and Digital Conformity Credentials.

DCC Documentation

The DCC class & property definitions provide a technology-neutral definition of classes, properties and code lists in the DCC model.

Implementation Guidance

Verifiable Credential

Digital Conformity Credentials are issued as Vierifiable credentials. Please refer to DPP VC Guidance for information about the use of the verifiaible credentials data model for UNTP.

Conformity Attestation

The `ConformityAttestation` type is the root content of the `credentialSubject` of the DCC. It is best thought of as the digital version of the paper product or facility conformity certificate.

- The `type` property is mandatory and must be populated with the value `ConformityAttestation` indicating the JSON-LD type of the data.
- the `id` MUST be a globally unique identifier (URI) for the attestation. Typically a certificate number with the CAB web domain as a prefix. `name` should contain a human readable text string that describes the attestation.
- `assessorLevel` (how assured is the party doing the assessment?), `assessmentLevel` ("how assured is the process by which the object product/facility is being assessed?) and `attestationType` (is this a test report, a certificate, or some other type?) are coded values that help to classify the type and integrity of the attestation.
- `issueToParty` identifies the entity to who the conformity attestation is issued - usually the product manufacturer or facility operator.
- `authorisation` describes a list of accreditations that a competent authority (such as a government agency or a national accreditation authority or a trusted global standards body) has issued to the conformity assessment body that is issuing this attestation. It provides trust that the certifier is properly accredited to issue certificates.
- `conformityCertficate` is a secure link to the full version (eg a PDF document) of this attestation.
- `auditableEvidence` is a secure link to an unstructured collection of files which provided the original evidence basis for the conformity assessments made by this DCC. The evidence files are usually commercially sensitive and encrypted but are an important information source for audits.
- `scope` defines the conformity scheme under which this attestation is issued. A scheme is a high level framework describing the context for the entire attestation. Each individual assessment included in this attestation will usually reference more fine grained criteria within any standards or regulations that are part of the scheme.
- `assessment` is an array of detailed conformity assessments made about an identified product or facility - against a specific criteria contained in a standard or regulation.

```
"credentialSubject": {
   "type": ["ConformityAttestation"],
   "id": "https://exampleCAB.com/38f73303-a39e-45a7-b8b7-e73517548f27",
   "name": "Carbon Lifecycle assessment 12345567",
   "assessorLevel": "3rdParty",
   "assessmentLevel": "Accredited",
   "attestationType": "certification",
   "attestationDescription": "Assessment of battery products against the GHG Protocol.",
   "issuedToParty": {..},
   "authorisation": [{..}],
   "conformityCertificate": {..},
   "auditableEvidence": {..},
   "scope": {..},
   "assessment": [{..},{..}]
}
```

Authorisations (Endorsements)

Authorisations are endorsements or accreditations issued by a competent authority (such as a government agency or a national accreditation authority or a trusted global standards body) has issued to the conformity assessment body that is issuing this attestation. It provides trust that the certifier is properly accredited to issue certificates.

- The `id` is a URI providing a unique ID of the endorsement / accreditation.
- `trustmark` is a base64 binary file that is typically shown on paper accreditations or endorsements.
- The `issuingAuthority` object defines the identity details of the competent authority that issued the endorsement. For example, in Australia the accreditation authority for conformity test labs is NATA.
- `accreditationCertificate` is a link to the actual accreditation details. This link SHOULD point to a trusted source of evidence such as a web page on the accreditation authority site (example) or a digital verifiable credential.

It should be noted that this `authorisations` structure is part of the attestation issued by the conformity assessment body. As such it is only an unverified claim until confirmed via the `accreditationCertificate` link.


```
    "authorisation": [
      {
        "type": [
          "Endorsement"
        ],
        "id": "https://authority.gov/schemeABC/123456789",
        "name": "Accreditation of certifiers.com under the Australian National Greenhouse and Energy
Reporting scheme (NGER).",
        "trustmark": {
          "fileName": "NGER Accreditation",
          "fileType": "image/png",
          "file":
"iVBORw0KGgoAAAANSUhEUgAAADkAAAA2CAYAAAB9TjFQAAAABGdBTUEAAi/9H3pWy6vI9uFdAAAAAElFTkSuQmCC"
        },
        "issuingAuthority": {
          "type": [
            "Entity"
          ],
          "id": "https://abr.business.gov.au/ABN/View?abn=72321984210",
          "name": "Clean Energy Regulator",
          "registeredId": "72321984210",
          "idScheme": {
            "type": [
              "IdentifierScheme"
            ],
             "id": "https://business.gov.au/ABN/",
             "name": "Australian Business Number"
          }
        },
        "endorsementEvidence": {
          "linkURL": "https://files.example-authority.com/1234567.json",
          "linkName": "NGER conformity certificate",
          "linkType": "https://test.uncefact.org/vocabulary/linkTypes/dcc"
        }
      }
```

Conformity Certificate and Auditable Evidence (Secure Link)

The `conformityCertificate` and `auditableEvidence` objects are both the same `SecureLink` type. The purpose is to provide a verifiable link to further details about the attestation (the certificate) or the auditable evidence (eg test results) that informed the attestation.

- `linkURL` points to the external certificate or evidence described by `linkName`.
- `linkType` is an optional identifier that, if present, should be drawn from a controlled vocabulary of linktypes (example.
- `hashDigest` should equal the hash of the target. This provides an integrity measure to ensure that the external certificate or evidence has not been tampered since the DCC was issued. `hashMethod` code defines which hash algorithm to use.
- `encryptionMethod` defines whether the target is encrypted and, if so, using which algorithm. THis provides a privacy/confidentiality mechanism to protect more sensitive content. The decryption key is assumed to be passed out of bounds.


```
  "conformityCertificate": {
    "linkURL": "https://files.example-certifier.com/1234567.json",
    "linkName": "GBA rule book conformity certificate",
    "linkType": "https://test.uncefact.org/vocabulary/linkTypes/dcc",
    "hashDigest": "7d294dd556fc7c5c7ee1123fbd18a59686b74e9697fee2299906e00f80ec1dc8",
    "hashMethod": "SHA-256",
    "encryptionMethod": "AES"
  },
  "auditableEvidence": {
    "linkURL": "https://files.example-certifier.com/1234567.json",
    "linkName": "GBA rule book conformity certificate",
    "linkType": "https://test.uncefact.org/vocabulary/linkTypes/dcc",
    "hashDigest": "73af1e7404283545909e9714e51e4b1653ff168ecfbe69dddcf4feece01e0c87",
    "hashMethod": "SHA-256",
    "encryptionMethod": "AES"
  },
```


Scope (Conformity Assessment Scheme)

`scope` defines the conformity scheme under which this attestation is issued. A scheme is a high level framework describing the context for the entire attestation. many individual assessments can be made under one scheme, and each may reference different standards or regulations.

- the `id` and `name` identifies the scheme. `issuingParty` identifies the scheme owner.
- the `issueDate` defines when the scheme was created and the `trustMark` is a binary file representing the mark or logo of the scheme.


```
  "scope": {
    "type": [
      "ConformityAssessmentScheme",
      "Standard"
    ],
    "id": "https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-master.pdf",
    "name": "GBA Battery Passport Greenhouse Gas Rulebook - V.2.0",
    "issuingParty": {
```

```
        "type": [
          "Entity"
        ],
        "id": "https://kbopub.economie.fgov.be/kbopub/toonondernemingps.html?
ondernemingsnummer=786222414",
        "name": "Global Battery Alliance",
        "registeredId": "786222414",
        "idScheme": {
          "type": [
             "IdentifierScheme"
           ],
          "id": "https://kbopub.economie.fgov.be/",
          "name": "Belgian business register"
        }
      },
      "issueDate": "2023-12-05",
      "trustmark": {
        "fileName": "GHG protocol trust mark",
        "fileType": "image/png",
        "file":
"iVBORw0KGgoAAAANSUhEUgAAADkAAAA2CAYAAAB9TjFQAAAABGdBTUEAAi/9H3pWy6vI9uFdAAAAAElFTkSuQmCC"
      }
    },
```


Conformity Assessments

One conformity credential may include many assessments. Each assessment includes

- subjects of the assessment (ie what was assessed) which may reference one or more products, facilites, or organisaitons. For example a 300Ah Lithium battery.
- a reference standard and/or regulation against which the assessment was made. For example the global battery alliance rulebook.
- one or more specific critieria within the referenced standard or regulation which may include benchmark or threshold values. For example the industry bechmakr carbon intensity of lithium batteries
- one or more actual declared values. For example the actual carbon intensity of the assessed battery.
- an indicator of conformance against the regulation or standard. For example, the battery conforms to the GBA rulebook.
- the ID and name of the auditor if different to the issuer of the conformity credential.


```
    "assessment": [
      {
        "type": [
          "ConformityAssessment",
          "Declaration"
        ],
        "assessmentDate": "2024-03-15",
        "id": "https://exampleCAB.com/38f73303-a39e-45a7-b8b7-e73517548f27/01",
        "referenceStandard": {
          "type": [
            "Standard"
          ],
          "id": "https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-master.pdf",
          "name": "GBA Battery Passport Greenhouse Gas Rulebook - V.2.0",
```

```
          "issuingParty": {...},
          "issueDate": "2023-12-05"
        },
        "referenceRegulation": {...},
        "assessmentCriteria": [
          {
            "type": [
              "Criterion"
            ],
            "id": "https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-
master.pdf#BatteryAssembly",
            "name": "GBA Battery rule book v2.0 battery assembly guidelines.",
            "thresholdValues": [
              {
                "metricName": "GHG emissions intensity",
                "metricValue": {
                  "value": 10,
                  "unit": "KGM"
                },
                "score": "BB",
                "accuracy": 0.05
              }
            ]
          }
        ],
        "declaredValue": [
          {
            "metricName": "GHG emissions intensity",
            "metricValue": {
              "value": 10,
              "unit": "KGM"
            },
            "score": "BB",
            "accuracy": 0.05
          }
        ],
        "conformance": true,
        "conformityTopic": "environment.emissions",
        "assessedProduct": [
          {
            "type": [
              "Product"
            ],
            "id": "https://id.gs1.org/01/09520123456788/21/12345",
            "name": "EV battery 300Ah.",
            "registeredId": "09520123456788.21.12345",
            "idScheme": {
              "type": [
                "IdentifierScheme"
              ],
              "id": "https://id.gs1.org/01/",
              "name": "Global Trade Identification Number (GTIN)"
            },
            "serialNumber": "12345678",
            "batchNumber": "6789",
            "IDverifiedByCAB": true
          }
        ],
        "assessedFacility": [...],
        "assessedOrganisation": {...},
```

```
        "auditor": {...}
      }
    ]
  }
```

Conformity assessments are included in the DCC as an array of UNTP `Declaration` structures. The same structure is re-used for third party assessments in UNTP Digital Product Passport (DPP). Please refer to the declarations structure for further information and examples.

To help understand the difference between a `Scheme` that defines the scope of the overall attestation and the `Criterion` that defines the rules for a specific conformity assessment, an example can help.

- ACRS operates a structural steel product certification scheme which will include a specific assessment assessment criteria for many different steel product types. For example on criteria could be about minimum tensile strength of a concrete reinforcing steel bar under criteria define by standard AS/NZS 4671: 2019.

Sample

Digital Traceability Events

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at https://test.uncefact.org/vocabulary/untp/dte/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Jan 2025

Release for Pilot Testing

Version 0.5.0 release artifacts can be used for pilot testing.

- JSON-LD @context
- JSON Schema
- Sample Instance

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

Version History

History of releases is available from the **Version history** page.

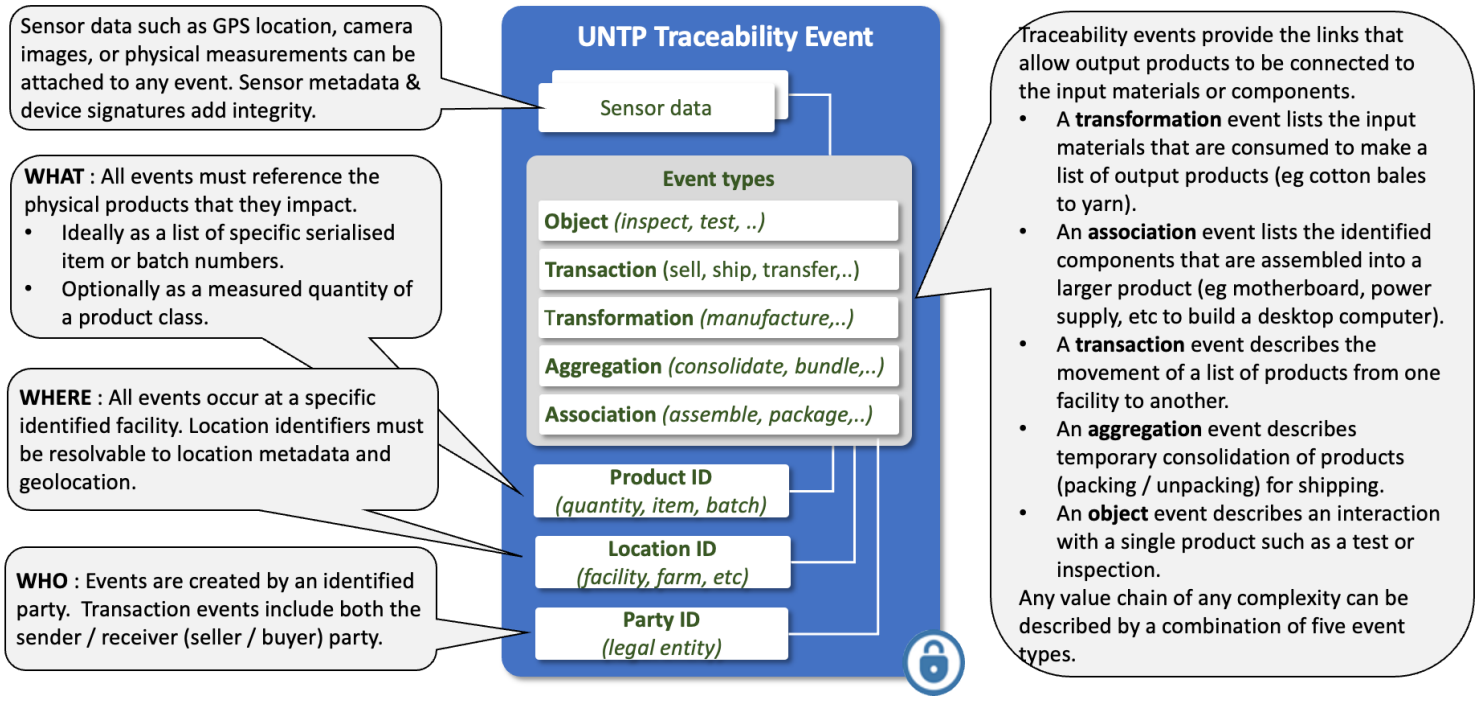
Visualization

A UNTP digital traceability event may be rendered in any format desired by the issuer. However a default **Visualization** is provided here and includes mapping of visual rendering elements to the Logical Data Model.

Overview

Traceability events are very lightweights collections of identifiers that specify the “what, when, where, why and how” of the products and facilities that constitute a value chain. The UNTP is based on the GS1 EPCIS standard for this purpose because it is an existing and proven mechanism for supply chain traceability. Note that UNTP supports but does not require the use of GS1 identifiers. The basic idea behind the traceability event structure is that any supply chain of any complexity can always be accurately modeled using a combination of four basic event types. An **object** event describes an action on specific product(s) such as an inspection. A **transaction** event describes the exchange of product(s) between two actors such as sale of goods between seller and buyer. An **aggregation** event describes the consolidation or de-consolidation of products such as stacking bales of cotton on a pallet for transportation. An **association** event describes the assembly of sub-components to make a composite product. Finally, a **transformation** event describes a manufacturing process that consumes input product(s) to create new output product(s). The UNTP uses these events in a decentralised architecture as the means to traverse the linked-data "graph" that represents the entire value-chain.

Conceptual Model



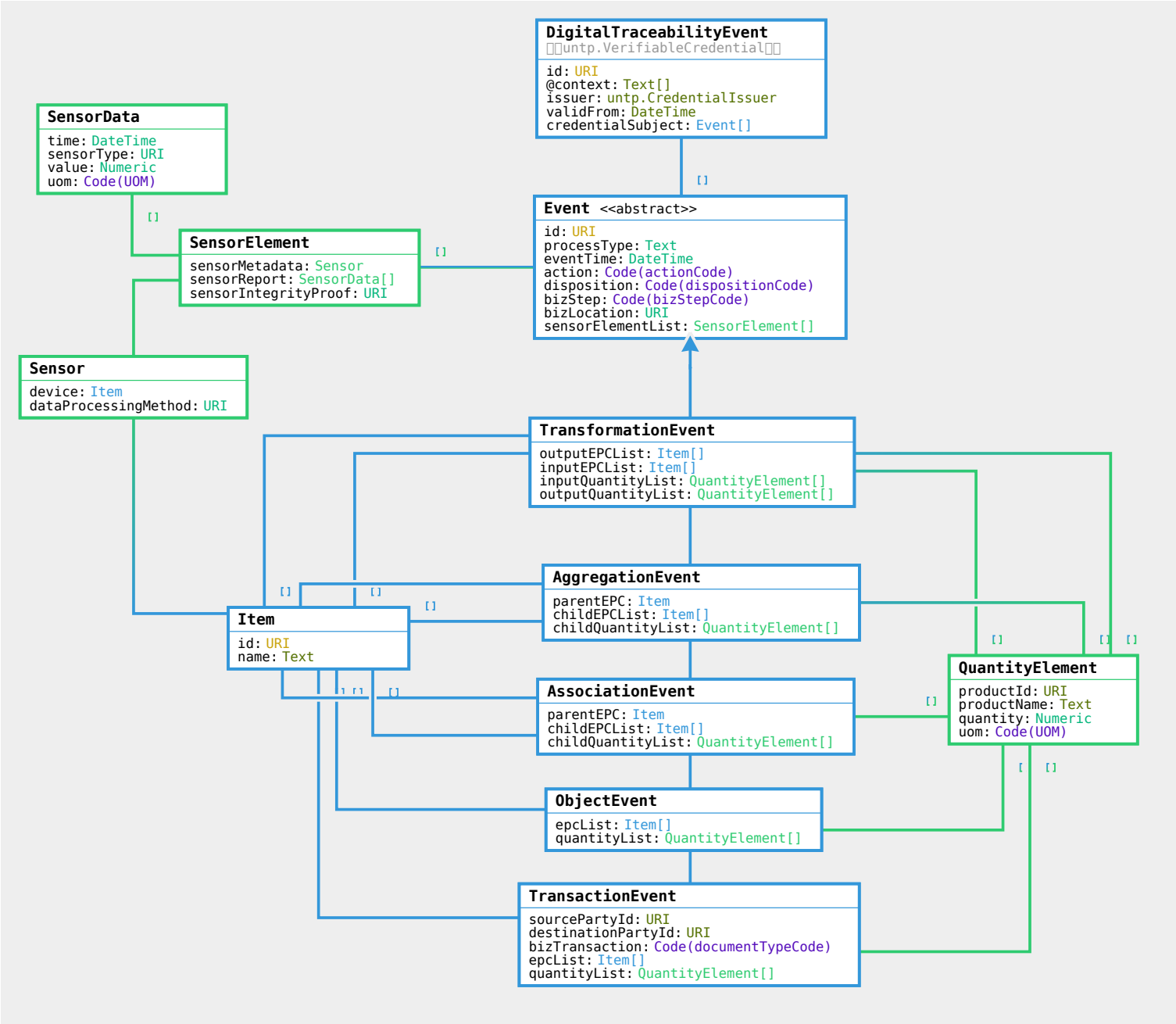
Requirements

The traceability event is designed to meet the following detailed requirements as well as the more general [UNTP Requirements(https://uncefact.github.io/spec-untp/docs/about/Requirements)]

ID	Name	Requirement Statement	Solution Mapping
TEV-01	Sub-components	The traceability event MUST provide a mechanism to trace from a DPP representing a product assembly to the individual DPPs of each sub-assembly component part	Association Event

ID	Name	Requirement Statement	Solution Mapping
TEV-02	Consumed materials	The traceability event MUST provide a mechanism to trace a manufactured product DPP back to the DPPs representing batches of input materials that are consumed in manufacturing one or more output products.	Transformation Event
TEV-03	Aggregated bundles	When a DPP represents an aggregated bundle of similar items (eg a pallet of cotton bales) then the traceability event MUST provide a means to allocate the aggregate measures to each individual item (ie each bale)	Aggregation Event
TEV-04	Transportation	when a product (or consolidated consignment) is shipped from one physical location to another, the traceability event MUST provide a means to record the movement and associate sustainability measures such as transport emissions to the shipped bundle	Transaction event
TEV-05	items or quantities	Traceability events MUST work equally well whether the input or output items are individually serialised items or measured quantities (mass or volume) of a product class.	Items Quantity
TEV-06	IoT Sensor data	Traceability events will often be generated by or associated with physical sensor readings. In such cases, the traceability event SHOULD support the association of sensor data with the event	Sensor element
TEV-07	Time & Location	Traceability events MUST always record the timestamp and physical location of the event so that multiple events can be be connected in time and space	Event

Logical Model



Core Vocabulary Documentation

The UNTP core types vocabulary defines the uniquely identified Linked Data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the building blocks for construction of Digital Product Passports and Digital Conformity Credentials.

DTE Documentation

The UNTP Digital Traceability Events Vocabulary defines the core traceability event and it's variants including aggregation event, transformation event, association event, transaction event, and object event.

Implementation Guidance

Verifiable Credential

Digital Traceability Events are issued as Vierifiable credentials. Note that one UNTP Digital Traceability Event credential may contain multiple events.

Please refer to DPP VC Guidance for information about the use of the verifiaible credentials data model for UNTP.

Traceability Event

There are five types of traceability event which all extend the same abstract `Event` model.

- A `TransformationEvent` describes manufacturing processes where input materials are consumed and/or assembled to create new output products. For example cotton thread is consumed to make woven cotton fabric.
- An `AssociationEvent` is used to establish relationships between otherwise independent items. For example new tyres on a car.
- An `AggregationEvent` describes the grouping (or un-grouping) of a quantity of similar items, usually for transport. For example the stacking of several bales of cotten onto a pallet.
- A `TransactionEvent` represents the transfer of products between organisations or facilites. For example the sale of some cotton cloth from seller to buyer.
- An `ObjectEvent` represents an action on an idividual item or quantity of product. For example an inspection or test of a battery.

Any value chain of any complexity can be represented as a combination of these types of events. However for UNTP value chain traceability, the most important event is the transformation event because it represents a manufacturing step that consumes inputs to create new outputs. When an identified output product (with it's digital product passport) can be traced to it's identified input products (each with their own digital product passport) then a linked set of credentials can be followed to define an entire value chain.

Transformation Event

This transformation event example describes the manufacture of a battery cell (output EPC) from an anode and a cathode (input EPC list) and a quantity of electrolyte (input quantity list).

```
 "credentialSubject": [
  {
    "type": [
      "TransformationEvent",
      "Event"
    ],
"id": "https://events.sample.com/b681df10-c682-454a-b11b-d0b9374c01bd",
"processType": "Cell Manufacture",
"eventTime": "2024-09-01T12:00:00",
"action": "Add",
"disposition": "https://ref.gs1.org/cbv/Disp-active",
"bizStep": "https://ref.gs1.org/cbv/BizStep-commissioning",
"bizLocation": "https://plus.codes/8CGRC78W+MM",
"sensorElementList": [...],
"outputEPCList": [
```

```
    {
      "type": [
        "Item"
      ],
      "id": "https://id.gs1.org/01/09520123456788/21/12345",
      "name": "EV battery 300Ah."
    }
  ],
  "inputEPCList": [
    {
      "type": [
        "Item"
      ],
      "id": "https://id.gs1.org/01/09520123456788/21/99876",
      "name": "Graphite Anode"
    },
    {
      "type": [
        "Item"
      ],
      "id": "https://id.gs1.org/01/09520123456788/21/99987",
      "name": "Copper Cathode"
    }
  ],
  "inputQuantityList": [
    {
      "productId": "https://id.gs1.org/01/095201299876",
      "productName": "Lithium electrolyte",
      "quantity": 2,
      "uom": "KGM"
    }
  ],
  "outputQuantityList": [...]
}
```

Association Event

This association event example describes the replacement of a new battery cell (child EPC) in an elctric vehicle (parent EPC).

```
 "credentialSubject": [
    {
      "type": [
        "AssociationEvent",
        "Event"
      ],
  "id": "https://events.sample.com/b681df10-c682-454a-b11b-d0b9374c01bd",
  "processType": "Replace battery",
  "eventTime": "2024-09-01T12:00:00",
  "action": "Add",
  "disposition": "https://ref.gs1.org/cbv/Disp-active",
  "bizStep": "https://ref.gs1.org/cbv/BizStep-commissioning",
  "bizLocation": "https://plus.codes/8CGRC78W+MM",
  "sensorElementList": [...],
  "parentEPC": {
    "type": [
      "Item"
```

```
    ],
    "id": "https://sample-car-company/VIN-Number/12345678987654",
    "name": "My Electric car."
  },
  "childEPCs": [
    {
      "type": [
        "Item"
      ],
      "id": "https://id.gs1.org/01/09520123456788/21/12345",
      "name": "EV battery 3000Ah."
    }
  ],
  "childQuantityList": [...]
}
```

Aggregation Event

This aggregation event describes the packaging for shipment of two battery cells (child EPCs) into a battery consignment (parent EPC)

```
 "credentialSubject": [
  {
    "type": [
      "AggregationEvent",
      "Event"
    ],
"id": "https://events.sample.com/b681df10-c682-454a-b11b-d0b9374c01bd",
"processType": "Packing",
"eventTime": "2024-09-01T12:00:00",
"action": "Add",
"disposition": "https://ref.gs1.org/cbv/Disp-active",
"bizStep": "https://ref.gs1.org/cbv/BizStep-commissioning",
"bizLocation": "https://id.gs1.org/414/9520123456788",
"sensorElementList": [...],
"parentEPC": {
  "type": [
    "Item"
  ],
  "id": "https://consignments.com/1234567890",
  "name": "shipment of batteries"
},
"childEPCs": [
  {
    "type": [
      "Item"
    ],
    "id": "https://id.gs1.org/01/09520123456788/21/12345",
    "name": "EV battery 300Ah."
  },
  {
    "type": [
      "Item"
    ],
    "id": "https://id.gs1.org/01/09520123456788/21/678910",
    "name": "EV battery 300Ah."
```

```
    }
  ],
  "childQuantityList": [...]
}
```

Transaction Event

This trasnaction event describes the sale of 200 batteries (quantity list) from source party to destination party.

```
   "credentialSubject": [
    {
      "type": [
        "TransactionEvent",
        "Event"
      ],
  "id": "https://events.sample.com/b681df10-c682-454a-b11b-d0b9374c01bd",
  "processType": "shipping",
  "eventTime": "2024-09-01T12:00:00",
  "action": "Add",
  "disposition": "https://ref.gs1.org/cbv/Disp-active",
  "bizStep": "https://ref.gs1.org/cbv/BizStep-commissioning",
  "bizLocation": "https://plus.codes/8CGRC78W+MM",
  "sensorElementList": [...],
  "sourcePartyId": "https://somebusinessregister/ID/9988765443",
  "destinationPartyId": "https://abr.business.gov.au/ABN/View?abn=90664869327",
  "bizTransaction": "https://ref.gs1.org/cbv/BTT-prodorder",
  "epcList": [...],
  "quantityList": [
    {
      "productId": "https://id.gs1.org/01/09520123456788",
      "productName": "EV battery 300Ah.",
      "quantity": 200,
      "uom": "KGM"
    }
  ]
}
```

Object Event

This object event describes the repair of a battery cell (EPC list).

```
   "credentialSubject": [
    {
      "type": [
        "ObjectEvent",
        "Event"
      ],
  "id": "https://events.sample.com/b681df10-c682-454a-b11b-d0b9374c01bd",
  "processType": "Repair",
  "eventTime": "2024-09-01T12:00:00",
  "action": "Add",
  "disposition": "https://ref.gs1.org/cbv/Disp-active",
```

```
  "bizStep": "https://ref.gs1.org/cbv/BizStep-commissioning",
  "bizLocation": "https://id.gs1.org/414/9520123456788",
  "sensorElementList": [...],
  "epcList": [
    {
      "type": [
        "Item"
      ],
      "id": "https://id.gs1.org/01/09520123456788/21/12345",
      "name": "EV battery 300Ah."
    }
  ],
  "quantityList": [...]
}
```

Item

The item structure is desinged to represent serialised items such as a specific battery cell.

```
      "epcList": [
        {
          "type": [
            "Item",
            "Entity"
          ],
          "id": "https://id.gs1.org/01/09520123456788/21/12345",
          "name": "EV battery 300Ah.",
          "registeredId": "90664869327",
          "idScheme": {
            "type": [
              "IdentifierScheme"
            ],
            "id": "https://id.gs1.org/01/",
            "name": "Global Trade Identification Number (GTIN)"
          }
        },
```

Quantity Element

THe quantity element structure is designed to represent a measured quantity of lithium hydroxide.

```
      "quantityList": [
        {
          "product": {
            "type": [
              "Entity"
            ],
            "id": "https://sampleRegister.com/material/876544321",
            "name": "Lithium hydroxide",
            "registeredId": "876544321",
            "idScheme": {
              "type": [
```

```
            "IdentifierScheme"
          ],
          "id": "https://sampleRegister.com/material",
          "name": "Register of mining products"
        }
      },
      "quantity": 20,
      "uom": "KGM"
    },
```

Sensor Element

The sensort element structure accomodates the association of one or more sensor readings to a given event. Each reading is measured by an identified sensor.

```
  "sensorElementList": [
    {
      "sensorMetadata": {
        "device": {
          "type": [
            "Item"
          ],
          "id": "https://sampledeviceregister.com/123456",
          "name": "Temperature sensor",
          "registeredId": "123456",
          "idScheme": {
            "type": [
              "IdentifierScheme"
            ],
            "id": "https://sampledeviceregister.com",
            "name": "Sample sensor device register"
          }
        },
        "dataProcessingMethod": "https://standards.org/sensorMethod#1234"
      },
      "sensorReport": [
        {
          "time": "2024-07-24T12:00:00",
          "sensorType": "https://samplesensors.com/model1234",
          "value": 25,
          "uom": "KGM"
        },
        {
          "time": "2024-07-24T12:00:00",
          "sensorType": "https://samplesensors.com/model1234",
          "value": 25,
          "uom": "KGM"
        }
      ],
      "sensorIntegrityProof": "..."
    }
  ],
```

Samples

Digital Facility Profile

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at https://test.uncefact.org/vocabulary/untp/dfr/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Jan 2025

Release for Pilot Testing

Version 0.5.0 release artifacts can be used for pilot testing.

- JSON-LD @context
- JSON Schema
- Sample Instance

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

Version History

History of releases is available from the **Version history** page.

Default Render Template

A UNTP digital facility record may be rendered in any format desired by the issuer. However a default **Template Design** is provided here and includes mapping of visual rendering elements to the Logical Data Model.

Sample Credential

URL	QR	Description
Sample Battery Manufacturing Facility Record		A sample digital facility record as a JWT envelope signed Verifiable Credential. The URL (or QR scan) resolved to a hosted verifier that displays a human readable version. Raw JSON data can be viewed via the `JSON` tab and the full credential can be dlownloaded via the download button.

Overview

The digital facility record (DFR) is issued by the owner or operator of a production or manufacturing facility and is the carrier of **facility data and sustainability information** for an identified facility in the value chain. It is very similar to the digital product passport except that it describes a facility rather than a product. The DFR is discoverable in the same way as a DPP - namely by resolving the facility ID to an Identity Resolver service that will return links to facility records. The sustainability performance metrics are also at the facility annual total level rather than at the product level. In many value chains, facility level information may be sufficient to meet the due diligence requirements of buyers and so the facility record can be used independently of the product passport. However product passports should reference the facility at which the product was produced. Where both facility and product information are available, verifiers can perform an approximate mass-balance assessment for quantity based criteria such as GHG emissions. For example, the total individual emissions recorded in all products shipped from a facility should approximately equal the reported annual emissions of the facility.

Conceptual Model

TBA

Requirements

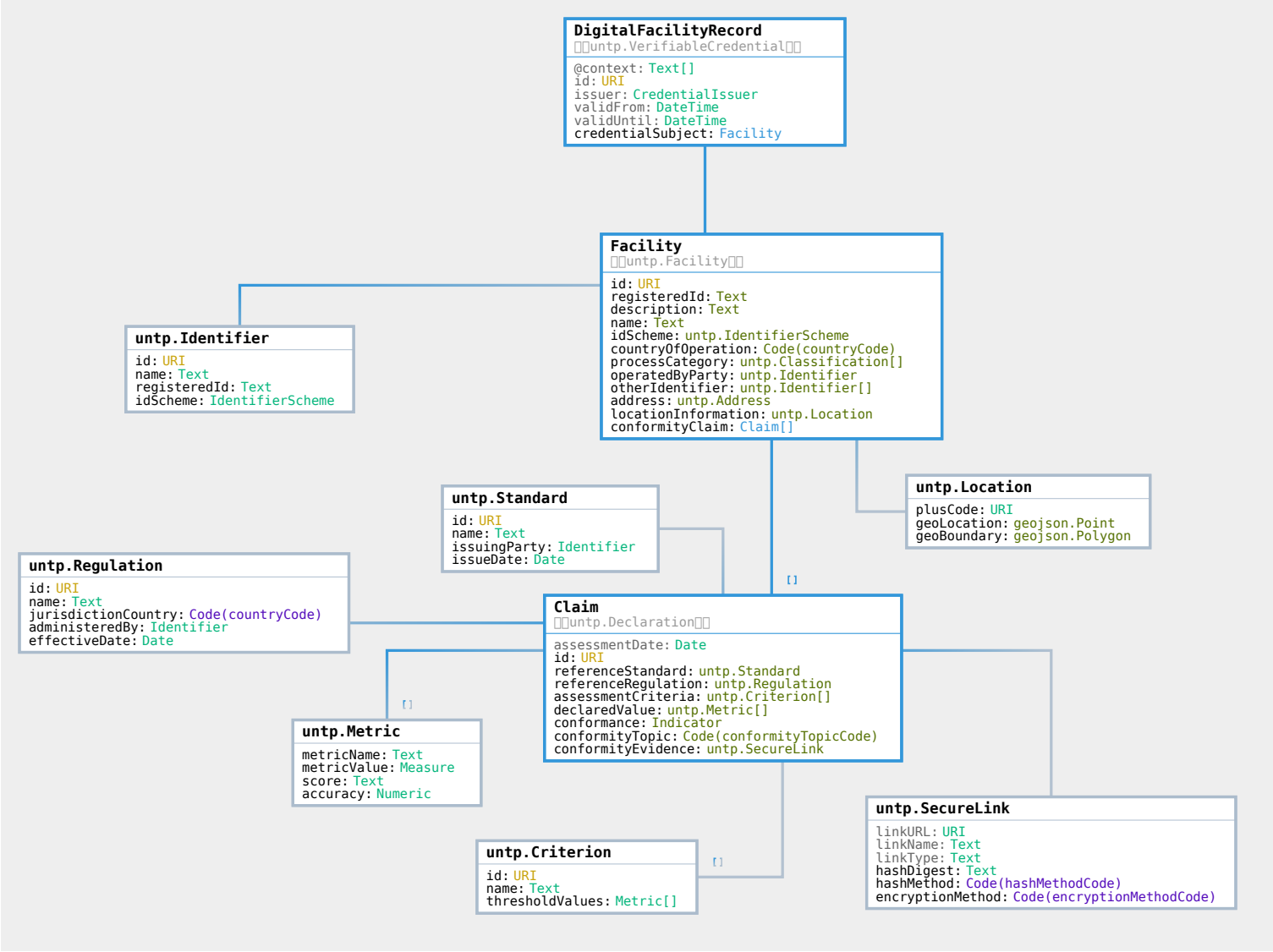
The digital facility record is designed to meet the following detailed requirements as well as the more general UNTP Requirements

ID	Name	Requirement Statement	Solution Mapping
DFR-01	Resolvable ID	Each facility must have at least one resolvable identifier that can be used in digital product passports	Facility.id

ID	Name	Requirement Statement	Solution Mapping
		and other data exchanges so that verifiers can always access the latest facility data.	
DFR-02	Process categories	The DFR should support any number of industry process classifications using codes from a defined classification scheme (eg UN-CPC)	The classifications property
DFR-03	Geo-Location	The DFR should should provide a means to specify both a geo-location point (aka pin) and a boundary geometry (aka polygon) so that verifiers can geo-locate supplier facilities	The Location class meets this need.
DFR-04	Owner / operator	The DFR should specify the owner and/or operator entity of the facility using one or more globally unique and resolvable entity identifiers.	Facility.OperatedByParty is a UNTP Entity structure that meets this need.
DFR-05	Declarations	The DFR MUST provide a means to include any number of conformity declarations so that it can provide simple single point to aggregate all claims about the facility in one place	The "conformityDeclarations" array is designed to meet this need
DFR-06	Conformity Topic	The DFR MUST provide a simple mechanism to express the sustainability/circularity/conformity topic for each claim so that similar claims can be grouped and the high level scope easily understood.	The ConformityTopic code list is designed to meet this need
DPP-07	Metrics	The DFR MUST provide a simple mechanism to quantify a conformity claim (eg carbon intensity, water consumption, etc) and to express any accuracy range.	The "Metric" class is designed to meet this need
DPP-08	Criteria	The DPP MUST provide a means to reference a standard or regulation as well as the specific criteria within that standard or regulation - so that claims can be understood in terms of the criteria against which they are made.	Declaration.referenceRegulation, Declaration.referenceStandard, Declaration.referenceCriteria
DPP-09	Evidence	The DPP MUST provide a means to reference independent conformity assessments that support and verify the claims being made. The related evidence SHOULD be digitally verifiable but MAY be a simple document or web page. The confidence level attached to the evidence should be clear.	The Declaration.conformityEvidence property references a relevant digital conformity credential

Logical Model

The Digital Facility Record is an assembly of re-usable components from the UNTP core vocabulary.



Core Vocabulary Documentation

The UNTP core types vocabulary defines the uniquely identified Linked Data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the building blocks for construction of the Digital Facility Record.

DFR Documentation

The DFR documentation provides a technology-neutral definition of classes, properties and code lists in the DFR model.

Implementation Guidance

This section provides sample JSON-LD snippets for each DFR component with guidance on their purpose and usage.

Verifiable Credential

Digital Facility Records are issued as Vierifiable credentials. Please refer to DPP VC Guidance for information about the use of the verifiaible credentials data model for UNTP. THe issuing party for the VC should be the facility owner or operator.

Facility

The facility object is the `credentialSubject`. It comprises

- An identifier for the facility. This could be a self-issued DID, or an ID managed by an industry association such as a member / facility register, or a global location scheme such as a GS1 GLN. Whatever the facility identifier scheme, facility IDs should be resolvable and verifiable.
- An industry process category, preferably using a global standard classificaiton scheme such as UN ISIC.
- The `operatedByParty` for the facility, typically identified using a national business register or a glbal business identifier scheme.
- The semi-strucutred address for the facility.
- The geolocation information for the facility (using PlusCodes adn GeoJSON - see below)
- The confirmity claims about the facility made by the facility owner or operator - following the same `Declaratoion` structure as used by the UNTP Digital Product Passport.

```
"credentialSubject": {
  "type": [
    "Facility"
  ],
  "id": "https://samplefacilityregister.org/1234567",
  "registeredId": "1234567",
  "description": "LiFePO4 Battery plant number 7",
  "name": "Example facility 7",
  "idScheme": {
    "type": [
      "IdentifierScheme"
    ],
    "id": "https://samplefacilityregister.org",
    "name": "A facility register"
  },
  "countryOfOperation": "AU",
  "processCategory": [
    {
      "type": [
        "Classification"
      ],
      "id": "https://unstats.un.org/unsd/classifications/Econ/isic/2611",
      "code": "2611",
      "name": "Manufacture of solar cells, solar panels and photovol",
      "schemeID": "https://unstats.un.org/unsd/classifications/Econ/isic",
      "schemeName": "UN Standard Industry Classification"
    },
    {...}
  ],
```

```
    "operatedByParty": {
      "type": [
        "Identifier"
      ],
      "id": "https://abr.business.gov.au/ABN/View?abn=90664869327",
      "name": "Sample Company Pty Ltd.",
      "registeredId": "90664869327",
      "idScheme": {
        "type": [
          "IdentifierScheme"
        ],
        "id": "https://abr.business.gov.au",
        "name": "Australian Business Number"
      }
    },
    "otherIdentifier": [..],
    "address": {
      "streetAddress": "level 11, 15 London Circuit",
      "postalCode": "2601",
      "addressLocality": "Acton",
      "addressRegion": "ACT",
      "addressCountry": "AU"
    },
    "locationInformation": {..},
    "conformityClaims": [..]
  }
}
```

Location

Facility location is a value object (ie it does not have a unique identifier). It's purpose it to locate the facility in a geographic area with whatever degree of resolution required. A location object must include at leaqst one of the following geolocation properties:

- An open location code (also know as Plus Codes). Plus codes are essentially a grid reference and can define an small area that is virtually a pin location (eg https://plus.codes/8CGRC78W+MM) or a much larger area (eg Roughly Madrid city - https://plus.codes/8CGRC700+) by removing digits after the "+" and replacing grid digits with an even number of trailing zeros.
- A geoLocation as a GeoJSON Point as a decimal lattitude / longditude pair.
- A geoBoundary as a GeoJSON Polygon that defines any closed boundary (or collection of closed boundaries) as a sequence of lat/long pairs where the first and last pair represent the same point.

```
    "locationInformation": {
      "plusCode": "https://plus.codes/8CGRC78W+MM",
      "geoLocation": {
        "type": "Point",
        "coordinates":[
            40.416688,
            -3.703313,
          ]
      },
      "geoBoundary": {
```

```
        "type": "Polygon",
         "coordinates": [
              [
                 [100.0, 0.0],
                 [101.0, 0.0],
                 [101.0, 1.0],
                 [100.0, 1.0],
                 [100.0, 0.0]
              ]
           ]
      }
```

Confomrity Claims

Conformity information is included in the Digital Facility Record as an array of UNTP Declaration structures. The same structure is re-used for confomrity Information in Digital Product Passports nad for third party assessments in UNTP Digital Conformity Credentials (DCC). Please refer to the Sustainability Vocabulary Page for further information and examples.

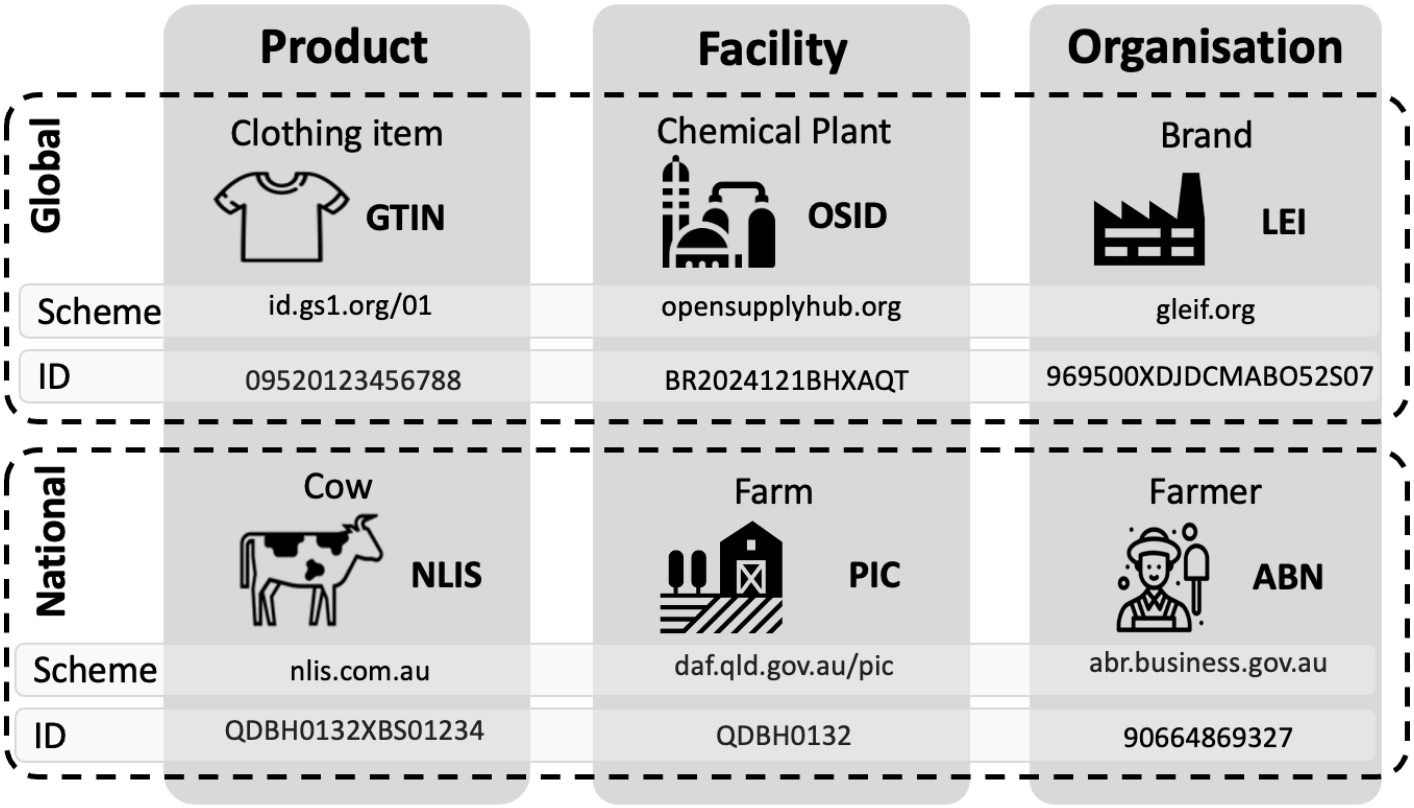
Samples

Identity Resolver

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

Identifiers of **businesses** (eg tax registration numbers), of **locations** (eg google pins or cadastral/lot numbers), and of **products** (eg GS1 GTINs or other schemes) are ubiquitous throughout supply chains and underpin the integrity of the system. The diagram shows an example of a global and a local scheme for three types of entity. These are just a few of thousands of existing identifier schemes. This identity resolver specification builds upon these identifier schemes so that existing investments and high integrity registers can be leveraged. This specification also supports the use of self-issued decentralised identifiers.



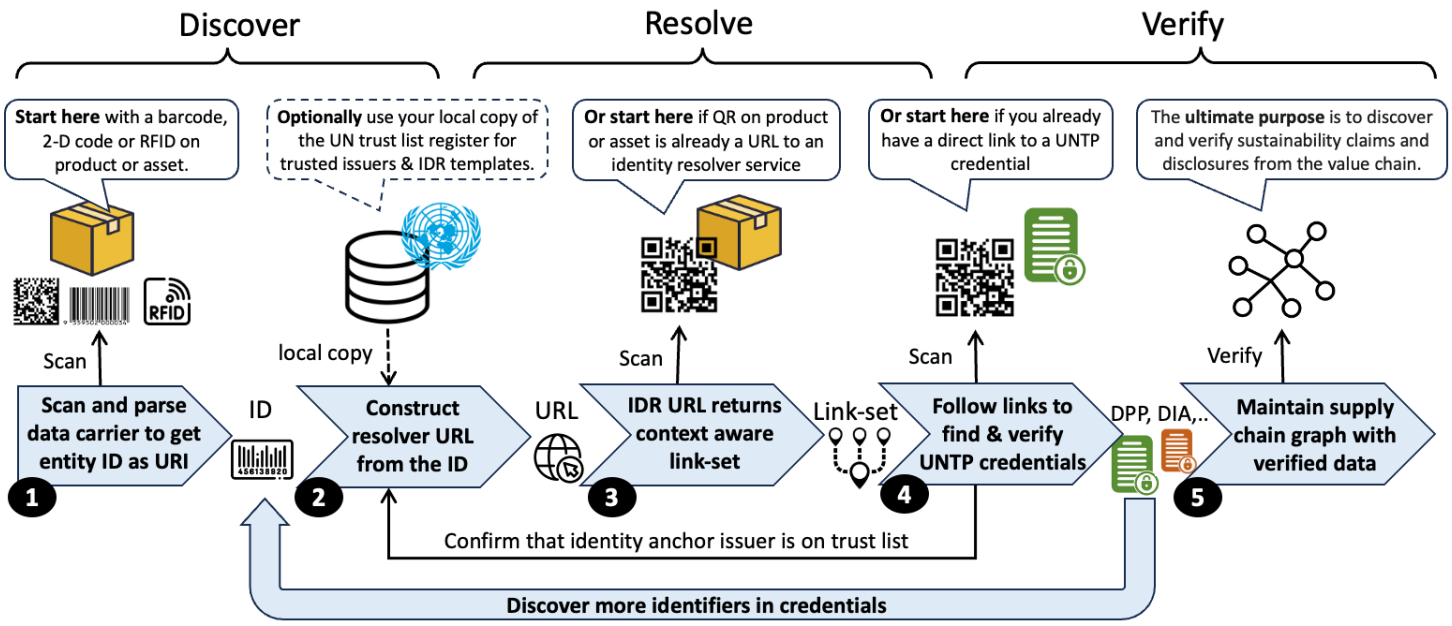
UNTP requires four key features of identifier schemes and, for those that don't already embody these features, provides a framework to uplift the identifier scheme to meet UNTP requirements. Identifiers used in UNTP implementations should be

- **unique** so that there is no risk of collision with identifiers across different schemes,
- **discoverable** either as structured data in documents or easily read by scanning a barcode, QR code, or RFID,

- **resolvable** so that, given an identifier, there is a standard way to find more data about the identified thing, and
- **verifiable** so that claims about identifiers made by the identifier's controller can be distingished from reviews and other third party claims.

Conceptual Model

A fundamental UNTP principle is "given an ID of a thing, I can find verifiable data about that thing". This Identity Resolver (IDR) specification describes how this is achieved.



A typical IDR workflow is as follows.

1. Each item in an inbound shipment of supplies to a manufacturing facility is barcoded - using the same well known barcode scheme that has been in use for many years (so nothing special for UNTP). A barcode reader captures the identifier of an item - eg `1234567`.
2. The scanner system may already know how to construct a URL from the ID (eg following ISO/IEC 18975) or may lookup the scheme in a local copy of the UN global register of schemes. A resolver template such as `https://resolver.example/{id}` can be used to replace `{id}` with the actual identifier to get `https://resolver.example/1234567`.
3. Calling the URL `https://resolver.example/1234567` returns an IETF link-set that includes one or more links (also URLs). Each link is annotated so that the type of information provided by the link is declared. **Link types** may include things like product safety data sheet, instruction manual, brand homepage, a digital product passport (DPP), and a digital conformity credential (DCC). Further annotations are used to declare things like the format of the linked information (HTML, PDF, JSON etc.). This is achieved using IANA-registed Media Types.
4. A link typed of `dpp` with a format declaration of `application/vc` is a hint that the target URL will yield a UNTP DPP credential which is verified to confirm integrity. The DPP includes several sustainability claims including the emissions footprint of the product, which the manufacturing facility can use to calculate the contribution of the received item to their scope 3 total. Following the DCC link type yields a conformity credential issued by a third party certifier that attests to the carbon intensity of the product.

5. The DPP and DCC both include an issuer DID like `did:web:sample-supplier.com` and `did:web:sample-certifier.com` which resolve to DID documents that link to digital identity anchor credentials confirming the identity of the supplier and certifier. The DPP also contains the ID of the manufacturing facility which can be resolved in the same way as the product ID (step 2) and therefore can be used to find facility level credentials such as fair work certificates. In this way a due-diligence transparency graph can be created by the manufacturer, providing strong evidence of regulatory compliance and sustainability performance.

The process is very flexible

- If instead of a barcoded item arriving at a manufacturing plant, it were a cow arriving at a processing plant, the same process would work using the livestock identifier encoded in the RFID tag on the cow's ear. The link-set would include a livestock passport which would, in turn, include the ID of the farm which could be used to find a deforestation credential for the farm.
- If the supplier of goods to the manufacturer switched from 1D barcodes to QR codes at any time, then this just means that step 2 is not needed because the QR is already likely to be an IDR URL that will return a link-set.
- If the barcode or QR is on a finished product and is scanned by a consumer in the EU using a smartphone then the IDR can use `http` header user context information to return the DPP by default (with additional links as options) and in the language of the user settings.

In this way, a single data carrier, whether a traditional barcode or a QR code, provides access to a wealth of further information which can be tailored to suit the user context - irrespective of whether the user is a human or a machine.

Requirements

This section defines the formal requirement statements for Identity Resolver implementations.

- **Scheme** means an identifier scheme such as a national business identifier scheme.
- **Carrier** means a machine readable device such as a barcode, QR code or RFID tag that encodes an identifier issued under a scheme.
- **Link** means a URL that points to a page or document or credential that contains further information related to the identifier.
- **Target** means the document or credential that the link references.
- **link-set** means a collection of links with meta-data that describe each link.
- **Resolver** means an implementation of this specification that returns a link-set about a given identifier.

ID	Short name	Requirement	Solution Mapping
IDR-01	Global uniqueness	All identifiers, whether for products, assets, facilities, or businesses used in UNTP credentials MUST be globally unique so that they can be unambiguously referenced and resolved.	Globally Unique Identifier Representation
IDR-02	One carrier, many links	One data carrier on a physical product or asset MUST be able to reference any amount of linked data or documents so that	Identity resolver services

ID	Short name	Requirement	Solution Mapping
		user or system confusion from multiple carriers on products can be avoided	
IDR-03	Leverage existing schemes	Existing identifier schemes MUST be usable for UNTP IDR functions so that existing investments can be leveraged and UNTP rollout can be accelerated because there is no need to re-tool existing identifier infrastructure.	This specification supports any identifier scheme.
IDR-04	Leverage existing carriers	Existing data carriers, whether 1D barcodes on products or RFID tags on livestock are entrenched and unlikely to change quickly. Therefore identity resolvers MUST be able to work with existing carriers so that digitalisation can proceed at pace without the need to re-tool existing physical scanning infrastructure.	Data carriers
IDR-05	Seamless transition to 2D	As industry transitions from 1D barcodes to 2D/QR codes, the UNTP identity resolver process MUST work equally well with either so that implementers can transition at their own pace	The Conceptual model - either create a resolver query from an 1D barcode / 2D matrix or embed the query into a QR.
IDR-06	Understanding link-sets	When a link-set is returned by a resolver, each link MUST include sufficient meta-data so that user systems can understand the purpose and usage of each link as well as the relationship between links	Identity resolver services
IDR-07	Filtering link-sets	Resolvers MUST allow users to request specific links, all links, or (if unspecified) then receive a default link - so that user experience can be optimised.	IDR Query
IDR-08	Responsive links	Resolvers SHOULD leverage available user information such as language preferences to return tailored link-sets and default links - so that user experience is optimised.	Defaults and Automatically returning the right language
IDR-09	Logical grouping of links	Link-set meta-data SHOULD provide an ability to group related link targets such as a product passport and related traceability events - so that user experience can be optimised.	
IDR-10	Versioning of link targets	When multiple version of link targets exist (eg multiple version of a product passport) then resolvers MUST include version information in link metadata and MUST ensure that any defaults	Versioned targets

ID	Short name	Requirement	Solution Mapping
		reference the latest version - so that users receive current information and can audit historical data	
IDR-11	Resolver redirection	Resolvers SHOULD, where available, include links that reference secondary resolvers so that product/facility owners can maintain additional document and credential links in their own resolvers. A typical example is the case where a global scheme maintains identifiers only at product class level but the manufacturer manages identifiers and related data at serialised item level. In such cases the primary resolver would say "here's what I know about the product and here's a link to another resolver that can tell you about the serialised item"	Secondary resolvers
IDR-12	Self-issued product identifiers	This specification MUST support self-issued identifiers so long as they are equally discoverable, resolvable, and verifiable - so that each value chain actor is free to make their own choice between third party product registers and self-managed product registers without any lock-in.	Decentralised Identifiers and DID to IDR linkset
IDR-13	Existing standards	This specification SHOULD use existing standards such as ISO/IEC 18975 and IETF RFC 9264 so that implementers can maximise re-use of existing infrastructure and maintain interoperability.	ISO/IEC 18975 is the basis for mapping an ID to a query. IETF RFC 9264 is the bases for the structure of the linkset response.

Globally Unique Identifier Representation

Linked Data Needs

Linked data architectures, of which UNTP is an example, depend on unique and consistent identifiers of entities such as product and facilities so that they can be matched across different credentials. For this reason URIs are heavily used as identifiers of entities throughout UNTP credential types. But without consistency in the way globally unique identifiers are constructed, there is a high risk that valuable links are not made. For example, consider the same product identified in two credentials:

- A digital product passport issued by a manufacturer with a sustainability claim about product `http://product.sample-register.example/123456789`
- A digital conformity credential with a third party sustainability assessment about product `urn:example:sample-register:product:123456789`

Although these are the same product, the construction of the ID is different and so a validation that attempts to confirm that a product passport claim is genuinely supported by third party assessment may fail.

There are thousands of identifier schemes in active use around the world and only a few have well defined conventions for consistent representation of their identifiers as globally unique URIs. To address these challenges, in this section, we define conventions for the consistent representation of identifiers that can be leveraged by any existing or new identifier scheme, whether the identifiers are managed by an issuing authority or self-managed.

Uniform Resource Name (URN)

URNs are a type of URI that are designed to be used as globally unique and persistent identifiers that remain available long after a specific resource that they identify ceases to exist or becomes unavailable. URNs MAY be used for any identifier and SHOULD be used as persistent identifiers for long lived entities such as organisations, facilities and long-lived products.

In patterns below,

- `{identifier-scheme}` is any string of characters permitted in URN Namespace Specific Scheme (alphanumeric characters, hyphen ,period, underscore, colon).
- `{identifier-value}` is the string of characters after the last colon (limited to alphanumeric characters, hyphen ,period, underscore).

For existing IANA registered URN namespaces

Use your IANA registered URN namespace.

- pattern `urn:{ns}:{identifier-scheme}:{identifier-value}`
- examples:
  - `urn:epc:id:sgtin:1234567.089123.2`
  - `urn:lei:7LTWFZYICNSX8D621K86`

For all other schemes

Either register your own scheme with IANA or use the UN global trust register `gtr` URN namespace (IANA registration pending).

- pattern: `urn:gtr:{identifier-scheme}:{identifier-value}` where `gtr` represents the UN global trust register namespace.
- examples:
  - `urn:gtr:register.business.gov.xx:90664869327` - representing any typical national business registration number
  - `urn:gtr:nlis.com.au:QDBH0132XBS01234` - representing an Australian livestock identifier

The `gtr` namespace represents identifier schemes that are listed in the UN global trust register (GTR). When the `gtr` namespace is used, the `{identifier-scheme}` MUST be a DNS domain name comprising URN allowed or percent-encoded characters (ie no `/` unless encoded as `%2F`).

Uniform Resource Locator (URL)

URLs are a type of URI that represent addressable web locations. URLs as identifiers have the advantage that they are immediately resolvable but the disadvantage that they may become dead/broken links whenever a document is moved or a web site is restructured or a domain name changes.

IDR URLs as identifiers

When URLs are used as identifiers in UNTP credentials they SHOULD be Identity Resolver URLs that conform to the ISO/IEC 18975 *structured path syntax* without parameters.

- pattern: `https://{identifier-scheme}/{identifier-value}` where `{identifier-scheme}` is a DNS domain name (without `/` characters unless `%2F` encoded) and `{identifier-value}` is a valid ISO/IEC 18975 path (which can include `/` characters to separate class, sub-class, and instance id as defined in ISO-18975)

- examples:

  - `https://products.sample-company.example/1234567`
  - `https://facilities-register.example/ABC123456`
  - `https://example.com/01/733240226591`
  - `https://example.com/01/733240226591/21/1234`

When a given identifier scheme uses both URN and URL mechanisms to represent identifiers as URIs then the `{identifier-scheme}` part SHOULD be the same for both. If the identifier scheme is registered in the UN global trust register then the `{identifier-scheme}` MUST match the corresponding scheme ID in the trust register.

Decentralised Identifiers (DID)

Decentralised Identifiers (DIDs) are a type of URI that are resolvable and verifiable by design. They are self-issued by any party and do not depend on any central register or issuing authority. The general structure of a DID is defined by the W3C Decentralised Identifiers recommendation as

- DID pattern: `did:{did-method}:{did-method-specific-identifier}`

The allowed structure of the `{did-method-specific-identifier}` depends on the `{did-method}`. There are a number of registered did methods including several blockchain based methods but the most widely used DID method is did:web

- DID Web pattern: `did:web:{domain-name}[:{path}]` where `:path` is an optional colon-delimited path to the identifier.
- examples:
  - `did:web:sample-company.example` - representing the DID of sample-company.example
  - `did:web:sample-company.example:products:123456789` - representing the DID of a product made by sample-company.example

Universally Unique Identifier (UUID)

As an alternative to being issued by an issuing agency, identifiers can be algorithm-generated. The best-known example of this is the Universally-Unique Identifier (UUID). This relies on it being *extremely* unlikely, but not impossible, that the same

identifier will be generated twice. For many practical applications, that can be "good enough" although there are some instances where duplicates have arisen (known as "collisions").

UUIDs as the complete identifier

When using a UUID as the identifier for an entity, the syntax would be

- pattern: `uuid:{UUID}`
- example: `uuid:709f3df6-4cdf-4bda-94d9-ce0ec9428616`

Such identifiers have no scheme information which could be used for resolvability and verifiability. Therefore usage SHOULD be limited to cases where there is no need for discovery of further data.

UUIDs as the scheme specific identifier value

UUIDs can be useful as scheme specific identifiers, particularly when there is value in the identifier being un-guessable. For example as a means to limit visibility of item specific data to the genuine holder of the goods - as described in the UNTP Decentralised Access Control specification.

- pattern: `{uri-scheme}:{identifier-scheme}[:or/]{UUID}`
- examples:
  - `urn:gtr:products.sample-register.example:709f3df6-4cdf-4bda-94d9-ce0ec9428616`
  - `https://products.sample-register.example/709f3df6-4cdf-4bda-94d9-ce0ec9428616`

Discoverability

This section describes the challenges and solutions in the first step of the identity resolver conceptual model - from an identifier encoded in some kind of data carrier to a consistent URI representation. UNTP does not define any new data carrier standards but rather aims to support any existing or future scheme.

Data Carriers

The term "data carrier" covers all 1D and 2D barcode symbols and RFID tags. Many exist, including proprietary ones, but for UNTP, the recommended carriers are those defined by ISO/IEC JTC 1/SC 31, such as linear barcodes, Data Matrix, QR Codes, and RFID. While these standards define the carrier format, they do not dictate identifier types, encoding syntax, or required devices, making "Automatic Identification and Data Capture" (AIDC) a specialized field.

Discoverability depends on equipment and software. RFID requires specialist readers, capable of scanning multiple tags without line of sight. Optical scanners can read various barcodes, but their software must interpret the data correctly. The more standardized the identifiers and encoding, the more interoperable and discoverable they are, leading industries to favor established systems.

Modern smartphones can read most optical barcodes and NFC tags via apps, enabling decentralized identifiers (DIDs) and alternative schemes. However, **QR Codes with URLs** are the most discoverable, as native camera apps can instantly open links.

Yet, URL-based identifiers pose risks like "link rot" and incompatibility with offline systems. ISO/IEC 18975 addresses this by embedding structured identifiers within *structured path* URLs, balancing broad accessibility with specialist data use.

In **Automatic Identification and Data Capture (AIDC)**, the **ISO/IEC 15459** series establishes a registry for short codes in data carriers. Organizations issuing barcode and RFID identifiers receive a unique **Issuing Agency Code** to prevent conflicts. **ISO/IEC 15418** defines **Data Identifiers (DIs)** and **Application Identifiers (AIs)**, which qualify identifiers, ensuring globally unique encoding in optical and RFID data carriers.

For example:

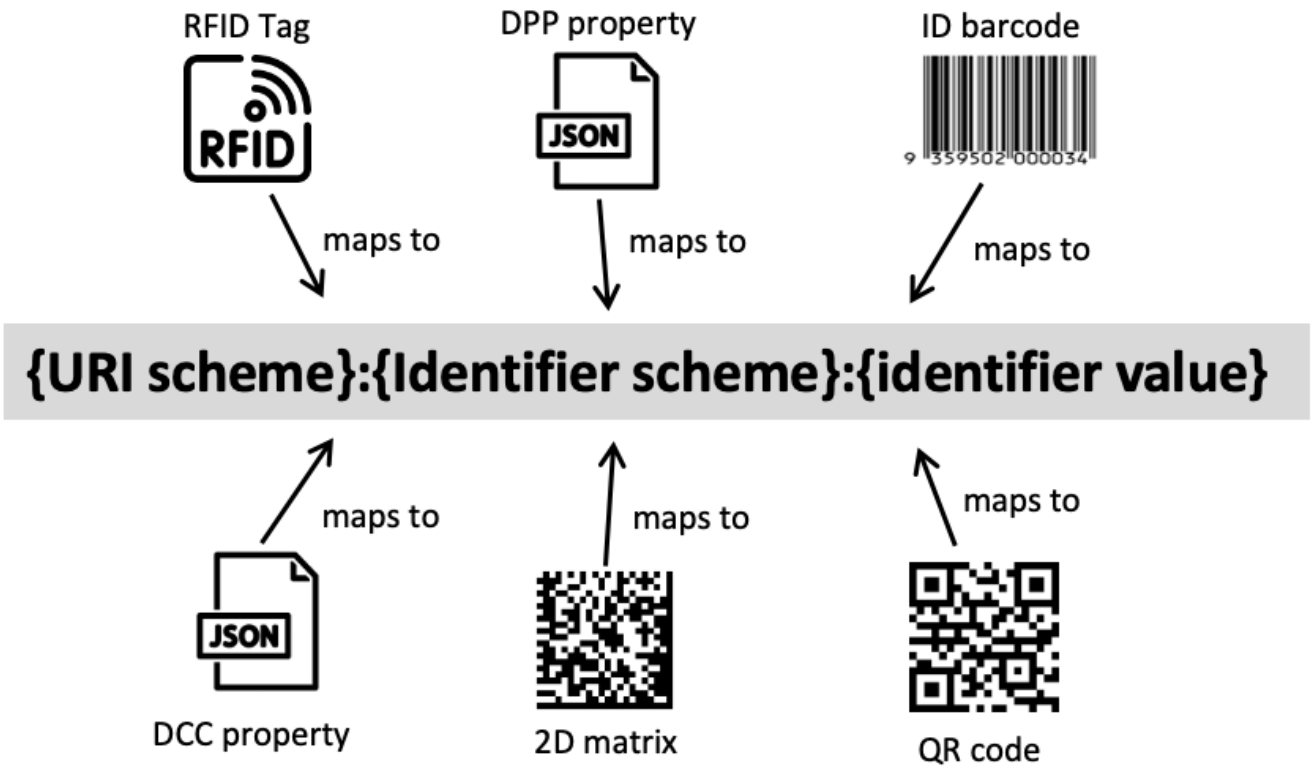
- **DI** `2B` identifies gas cylinders per U.S. D.O.T. standards.
- **AI** `01` represents a **Global Trade Item Number (GTIN)**.

DIs are managed by **ANSI**, while AIs fall under **GS1**.

Mapping to consistent URIs

A key challenge is to ensure that all these different data carrier representations are mapped to a consistent globally unique identifier when building value chain transparency graphs.

- A 2D Matrix code might yield the string `0107332402265910211234567890240+A01=442.001-UP001T9145649876549876546543213216875 3` where `733240226591` is the product ID (with company prefix) and `1234567890` is the serial number
- An RFID Tag for the same product might yield a string like `urn:epc:tag:sgtin-96:1.7332402.026591.1234567890` where `7332402.026591` is the product ID and `1234567890` is the serial number.
- A QR code may may yield `https://id.sample-resolver.example/01/733240226591/21/1234567890` where `733240226591` is the product ID (with company prefix) and `1234567890` is the serial number.



Existing data carrier schemes are very varied but usually well documented. Therefore it is reasonable to expect that scanners will be aware of the context and will include scheme specific logic to read the data carriers and construct UNTP standard URNs or URIs to match against identifiers using in credentials such as digital product passports.

For new identifier schemes or existing schemes that have not already defined data carrier specifications, UNTP implementers SHOULD

- directly encode the UNTP URN structure into 2D matrix codes and RFID tags.
- directly encode the UNTP URL structure into QR codes.

Resolvability

This section describes the challenges and solutions in the second and third steps of the identity resolver conceptual model - from a consistent URI representation of an identifier to a link-set about the identified entity. In the context of UNTP, that means easily resolving a product or facility identifier to credentials such as the identified product's DPP or the identified facility's DFR.

Identity Resolver Services

This UNTP identity Resolver (IDR) specification builds upon these existing standards by defining some specific constraints that improve interoperability and meet UNTP specific requirements.

Identity Resolver Example

IDR Query URL

IDR queries are URLs that take the general form

`https://{domain}/{path}?{query}` where

- `domain` is the web domain of the resolver service, usually operated by the identifier scheme register - eg `resolver.sample-register.example`
- `path` carries the specific ID of the product or facility being queried and may include qualifiers - eg `products/ABCD9876/items/1234`
- `query` contains a list of URL parameters that are used to filter the response - eg `linkType=untp:dpp&language-en`

A typical IDR query might be something like this

`https://resolver.sample-register.example/products/ABCD9876/items/1234?linkType=linkset`

which is requesting

- the complete link-set
- about a product class `ABCD98765`
- issued using an identifier scheme supported by `sample-register.example`
- with specific serial number `123456789`

To get a different response, the query might be modified as follows

- `https://resolver.sample-register.example/products/ABCD9876?linkType=linkset` to get data about the product class only, not a specific serialised item.
- `https://resolver.sample-register.example/products/ABCD9876/items/1234?linkType=untp:dpp` to get only the DPP for the item.
- `https://resolver.sample-register.example/products/ABCD9876/items/1234?linkType=all&language=de` to get all links to German language targets.
- `https://resolver.sample-register.example/products/ABCD9876/items/1234` to get a redirect to the target of the `default` link.

IDR LinkSet Response

The response to an IDR query is an IETF `linkset` which contains one or more `contexts`, each of which contain one or more `targets`.

- a context describes what the links are about using the `anchor` property. Often there is only one `anchor` that represents the requested `identifier`. But as described in the resolver workflow, a resolver may return links about related entities. For example a query about a specific serialised item may return some links about the item, and some links about the product class, and even some links about the manufacturer or brand that sells the product.
- a target describes a specific link identified with the `href` property together with other properties that provide useful meta-data about the link.

A typical response the the sample query `https://resolver.sample-register.example/products/ABCD9876/items/1234?linkType=linkset` might be as shown in the snippet below.

- there are two `contexts`, one is at serialised item level `"anchor": "https://resolver.sample-register.example/products/ABCD9876/items/1234"` and one is at product class level `"anchor": "https://resolver.sample-register.example/products/ABCD9876"`.
- the first context has two `targets`, both of which have a linkType "untp:dpp" (UNTP digital product passports) and MIME type `application/vc+jwt` but one is rendered in German and the other in English.
- the second context is at product and has one target which points to the manufacturers product information web page. This highlights that link resolvers can return all kinds of relevant links, only some of which point to UNTP credentials.


```
{
    "linkset": [
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876/items/1234",
            "untp:dpp": [
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
                    "type": "application/vc+jwt",
                    "title": "Digital Product Passport",
                    "hreflang":["en"]
                },
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869311.json",
                    "title": "Digitaler Produktpass",
                    "hreflang":["de"],
                    "type": "application/vc+jwt"
                }
            ]
        },
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "gs1:pip": [
                {
                    "href": "https://sample-company.example/productInformation/ABCD9876",
                    "type": "text/html",
                    "title": "Product Information"
                }
            ]
        },
    ]
}
```


Creating the IDR Query URL

There are several forms in which an identifier might be discovered (eg as a data carrier on a physical product or as a URI in a structured document). The identifier representation format is often not an IDR query URL and so may need to be translated into an IDR URL query format. As shown in the conceptual model, the generalised process to derive an IDR query URL has two steps

- Map the native format found in a data carrier to a consistent global URI as described in the globally unique identifier representation section.
- Map the global URI to an IDR query string as described in the following paragraphs.

This mapping architecture is designed to ensure that UNTP can accommodate any new or existing identifier scheme and any data carrier and still maintain linked data consistency (ie consistent URI representation) as well as resolvability and verifiability of identifiers.

From a URN to IDR linkset

The UN global trust register will include resolver templates for each scheme and so the UNTP requirement that identifiers be resolvable is met by substituting the URN `{identifier-value}` into the `{id}` placeholder in the resolver template related to the matching `{identifier-scheme}`. For example

- given a URN ID of `urn:gtr:nlis.com.au:QDBH0132XBS01234`, the `{identifier-scheme}` is `nlis.com.au`
- and a resolver template of `https://resolver.nlis.com.au/{id}` is registered for scheme `nlis.com.au`
- then the resolver URL would be `https://resolver.nlis.com.au/QDBH0132XBS01234` which would return an IDR LinkSet

From a URL to IDR linkset

As described in IDR URLs as identifiers, URL identifiers SHOULD already be Identity Resolver URLs that conform to the ISO-18975 structured path syntax without parameters. Client applications may of course add parameters to the URL before calling the resolver service to get more specific link sets.

From a DID to IDR linkset

By design, all DIDs resolve to a URL that addresses a DID document. The way in which a DID resolves to a DID document is specific to the DID method. In the case of DID web, the resolution works by replacing ":" with "/" and appending "did.json".

- DID : `did:web:sample-company.example:products:123456789` is an example of a product identifier the did:web scheme.
- URL : `https://sample-company.example/products/123456789/did.json` would be the URL of the DID document according to did:web method specification

The DID document `did.json` has a standard data model defined by the W3C DID recommendation core properties. It is primarily designed to define the cryptographic methods by which control of a DID can be verified, including associated public keys. The DID service property can be used to reference further information such as UNTP credentials like a digital product passport. The UNTP approach to using a DID document as a resolver service combines conformant use of DID `service` properties with maximum alignment with IETF linksets.

- The DID document `service.id` property is the same as the linkset `anchor` property with the optional `#fragment` suffix to ensure that `service.id` is unique.
- The DID document `service.type` property is the same as the linkset linkType value.
- The DID document `service.serviceEndpoint` property is exactly the same as the the linkset `target` object.

```
{
  "id": "did:web:sample-company.example:products:123456789",
  ..other did document properties ..
```

```
  "service": [{
    "id":"did:web:sample-company.example:products:123456789#untp:dpp",
    "type": "untp:dpp",
    "serviceEndpoint": {
          "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
          "title": "Digital Product Passport",
          "hreflang":["en"],
          "type": "application/vc+jwt"
     },
    "id":"did:web:sample-company.example:products:123456789#untp:idr",
    "type": "linkset",
    "serviceEndpoint": {
          "href": "https://resolver.sample-company.example/products/123456789",
          "title": "Identity Resolver Service",
          "type": "application/linkset+json"
     }
  }]
}
```

The example above shows two ways of using the DID document serviceEndpoint as an identity resolver service.

- The first target references a UNTP DPP credential directly.
- The second target references a resolver service end point which itself would return a linkset.

In this way, simple scenarios can be achieved simply by placing link targets directly in the DID document whilst richer and more dynamic link resolver services can also be delivered by including a DID document service which is itself a link resolver.

Link-set Response Variations

This section covers specific linkset use cases that SHOULD be supported by conforming link resolvers. The general approach to solving linkset specific needs is

- Where possible, always use IETF linkset standard properties and IANA standard link types.
- Where necessary, use custom link types and linkset properties but always define them in a public vocabulary and reference them using a profile link type.

Defaults

Default link types allow a resolver to return just the target URL of the default link - which means that client applications (including just a camera on a mobile phone) need not have any knowledge of link resolvers and how they work.

Link resolver services SHOULD define DEFAULT link type for each `anchor` which defines the `href` target to which a client will be redirected when no `linkType` is specified in the matching query URL. In the previous IDR example, calling the resolver URL without a `linkType` parameter;

`https://resolver.sample-register.example/products/ABCD9876/items/1234?linkType=linkset`

Would redirect the client directly to the target `href` of the default link type

`https://sample-credential-store.com/credentials/dpp-90664869327.json`

Automatically Returning The Right Language

HTTP headers often contain `accept` header properties that can be useful hints for link resolver behaviour. For example browsers will normally include a language accept header that matches the users configured preference. This can be used to return only those links that match the users language even if the IDR query string does not specify a preference. For example, consider an IDR that

- defines a default link type as `untp:dpp`
- maintains DPP links in a dozen languages

and receives the following HTTP query URL

```
GET /products/123456789 HTTP/1.1
Host: resolver.sample-company.example
Accept-Language: de
```

Even though there are a dozen DPP links maintained by the IDR service, only one of them is in German and so the IDr can again redirect the client to the specific target URL of the German language DPP.

`https://sample-credential-store.example/credentials/dpp-90664869311.json`

Secondary Resolvers

There are some cases where an identifier scheme owner manages identifiers at a coarse granularity by issuing globally unique prefixes but allows the subject to manage more fine grained identifiers themselves. For example

- GS1 maintains GTIN product identifiers in a single global register but management of SGTIN (serialised items) is left to the owner of the GTIN.
- IATA issues 3 character carrier identifiers but allows each carrier to add the 7 digit suffix for each cargo consignment to make a globally unique 11 digit consignment number.
- Australian government manages 8 alpha-numeric character farm identifications codes such as `QDBH0132` and allows each farmer to add a unique suffix to identify each unique livestock animal born on the farm.
- and many more examples exist.

The result is that a client may construct an IDR query to the genuine scheme operator's IDR service but that service may not hold information at the requested granularity. In such cases, a conformant IDR SHOULD return links relevant to the more coarse grained item and, if available, a link to a secondary resolver service (eg hosted by the serialised product manufacturer) that can return more fine grained information. For example the following query to a link resolver about a serialised item

`https://resolver.sample-register.example/products/ABCD9876/items/1234`

May return a link to a secondary resolver that maintains data at serialised item level as well as a link to a DPP at product class level.

```
{
    "linkset": [
```

```
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876/items/1234",
            "linkset": [
                {
                    "href": "https://resolver.sample-company.example/products/ABCD9876/items/1234",
                    "rel": ["untp:idr", "gs1:handledBy"],
                    "title": "Secondary Identity Resolver",
                    "hreflang":["en"],
                    "type": "application/linkset+json"
                }
            ]
        },
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "untp:dpp": [
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
                    "title": "Digital Product Passport",
                    "hreflang":["en"],
                    "type": "application/vc+jwt"
                }
            ]
        },
    ]
}
```

Versioned Targets

In some cases, a publisher may wish to maintain multiple versions of a credential as available links in a linkset. The recommended method is to add the relevant IANA version link relation to the `rel` value array as shown in the example below. In this case there are two links for the same anchor, both include `untp:dpp` as a link relation value but one also has the IANA link relation `predecessor-version`

```
{
    "linkset": [
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "untp:dpp": [
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
                    "title": "Digital Product Passport",
                    "hreflang":["en"],
                    "type": "application/vc+jwt"
                },
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869111.json",
                    "rel":["predecessor-version"],
                    "title": "Digital Product Passport",
                    "hreflang":["en"],
                    "type": "application/vc+jwt"
                }
            ]
        }
    ]
}
```

Creating New Links

In some cases, an identity resolver service may wish to accept updates such as creation of new links from appropriately authorised users. For example, adding a maintenance event to a battery passport record after the battery has been sold into the market. An identity resolver SHOULD accommodate this possibility by including a link in the linkset for the given product that specifies how to POST an event to the resolver. In the example below, an `anchor` representing product `https://resolver.sample-register.example/products/ABCD9876` has two links. The first is a simple link to a DPP describing the product. The second describes a method to create a new maintenance event.

- The standard IANA link relation `edit` indicates that the target resource is used to edit the link's context.
- The custom link relation `untp:dte` indicates that the target expects a digital traceability event.
- The custom property `method` indicates that the HTTP header requires a POST method and a secret key in the `X-API-Key` HTTP header property.

```
{
    "linkset": [
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "untp:dpp": [
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
                    "title": "Digital Product Passport",
                    "hreflang":["en"],
                    "type": "application/vc+jwt"
                 }],
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "untp:dte": [
                {
                    "href": "https://sample-credential-store.com/credentials/dte",
                    "rel":["edit"],
                    "title": "Create Maintenance Event",
                    "method":["POST","X-API-Key"],
                    "type": "application/vc+jwt"
                 }
            ]
        }
    ]
}
```

Secure Targets

In some cases the target of a link contains sensitive data that is not generally accessible to the public. In such cases, as described by the decentralised access control specification, the target of the link is encrypted and requires a decryption key or proof of authorised role to decrypt. The corresponding link in the resolver linkset SHOULD specify the encryption method and allowed list of access roles.

```
{
    "linkset": [
        {
            "anchor": "https://resolver.sample-register.example/products/ABCD9876",
            "untp:dte": [
```

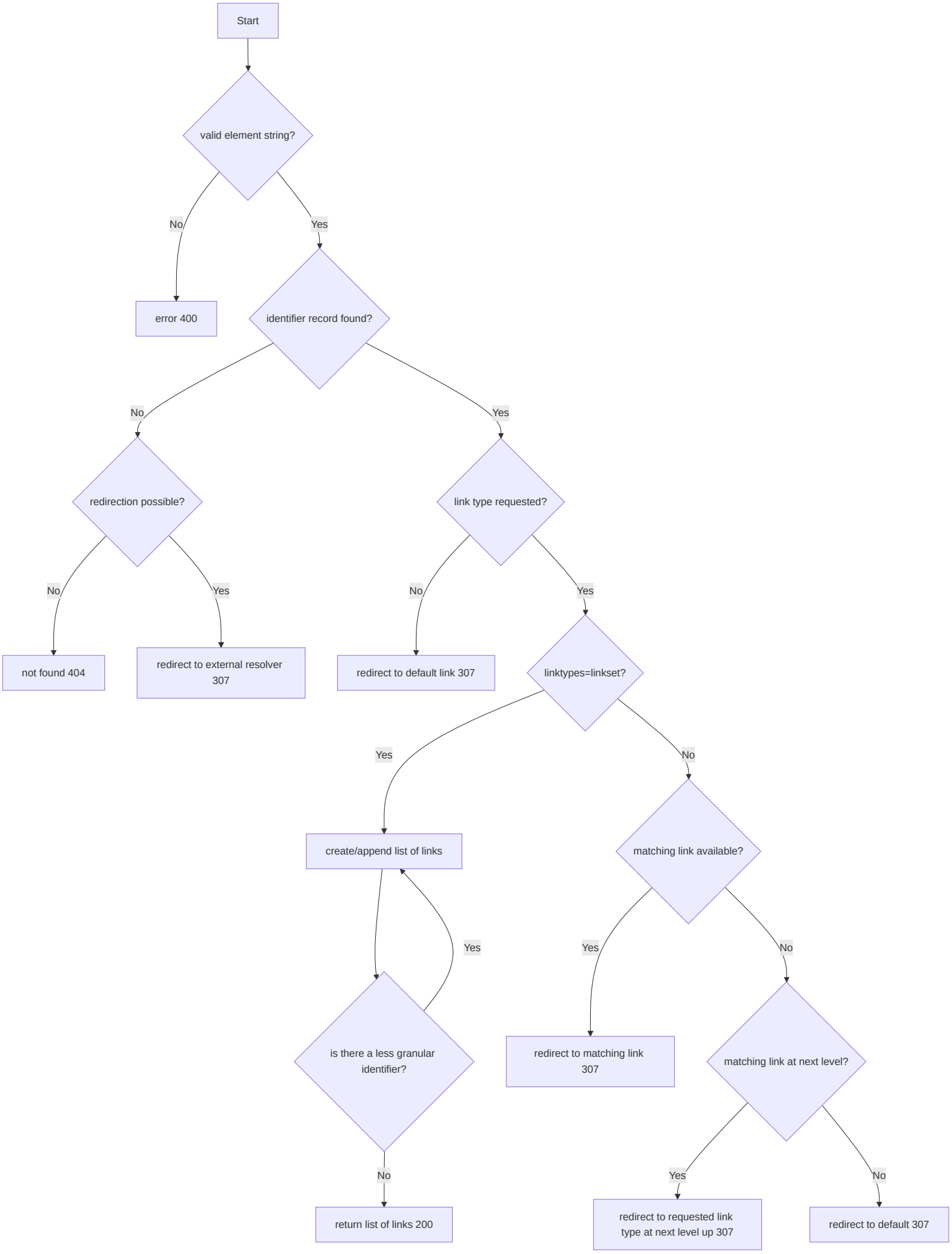
```
                {
                    "href": "https://sample-credential-store.example/credentials/dpp/90664869327.json",
                    "title": "Product Traceability",
                    "encryptionMethod": "AES-128",
                    "accessRole":["untp:accessRole#Owner"],
                    "hreflang":["en"],
                    "type": "application/vc+jwt"
                }
            ]
        }
    ]
}
```

Resolver Service Workflow

The internal workflow of an identity resolver service is not defined by this specification. However, there are some common conditions that a link resolver service SHOULD manage consistently. For example

- When a query URL is not valid
- When there is no data for the requested entity ID.
- When there is no data for an item level ID but there are available links for product class level ID
- When a requested link type does not exist.

These cases are shown in the example resolver workflow diagram below.


Start
valid element string?
No
Yes
error 400
identifier record found?
No
Yes
redirection possible?
link type requested?
No
Yes
No
Yes
not found 404
redirect to external resolver 307
redirect to default link 307
linktypes=linkset?
Yes
No
create/append list of links
matching link available?
Yes
Yes
No
is there a less granular identifier?
redirect to matching link 307
matching link at next level?
No
Yes
Yes
No
return list of links 200
redirect to requested link type at next level up 307
redirect to default 307

Verifiability

Once identifiers have been resolved to a linkset and links have been followed to retrieve UNTP (or other) credentials, then the final step is verification. There are several types of verification.

Verifying Individual Credentials

Each link target that has a `type` property that indicates it is a verifiable credentials (`application/ld+json` , `application/vc+jwt`) SHOULD be verified according to W3C Verifiable Credential validation rules. This verifies

- Integrity (the credential has not been tampered-with)
- Currency (the credential has not been revoked)

The UNTP Verifiable Credential Profile provides further guidance.

Verifying Identity Integrity

A credential such as a digital product passport can be valid in it's own right but may not be valid in context. For example

- The named issuer of the DPP may not be the party they claim to be.
- The DPP might be issued by a party that is not the legitimate owner of the product identifier.

These kind of validation rules are define in the UNTP Digital Identity Anchor - Use Cases page.

Anti-Counterfeiting

In the particular case of data carriers on physical goods, there is also a counterfeiting risk.

- The product may have copied a valid data carrier from a real product to a counterfeit one.
- The data carrier might resolve to verifiable claims that are about a different product.

Countermeasures to these kind of counterfeiting behaviour are described in the UNTP Anti-Counterfeiting best practices page.

Chain of Custody Accounting

A particularly important and challenging verification in supply chains is chain of custody / mass-balance accounting.

- A high carbon batch of input materials might be mixed with a low carbon batch of the same commodity and the output may be fraudulently associated with only the low carbon input.
- A verifiable assessment of total emissions of a facility may not be accurately allocated across the individual product shipments from the facility.

Countermeasures to this kind of mass balance fraud are described in the UNTP chain of custody best practices page.

Verifying Regulatory or Industry Standards Compliance

Verification such as due-diligence across entire supply chains of fair work practices or chain of custody accounting accuracy of mass-balance processes are achieved by verifying entire graphs of data rather then individual credentials. Furthermore, these kind of verification rules tend to be industry and/or geography specific and are defined in UNTP extension projects rather than UNTP core specification.

Some best practice guidance is available in the UNTP Transparency Graphs page.

Digital Identity Anchor

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at - https://test.uncefact.org/vocabulary/untp/dia/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Feb 2025

Release for Pilot Testing

Version 0.5.0 release artifacts (when available) are suitable for pilot testing.

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

- JSON-LD @context
- JSON Schema (full credential)
- JSON Schema (credentialSubject only)
- Sample Instance

Sample Credential

URL	QR	Description
Sample Digital Identity Anchor		A sample digital identity anchor as a JWT envelope signed Verifiable Credential. The URL (or QR scan) resolved to a hosted verifier that displays a human readable version. Raw JSON data can be viewed via the `JSON` tab and the full credential can be dlownloaded via the download button.

Version History

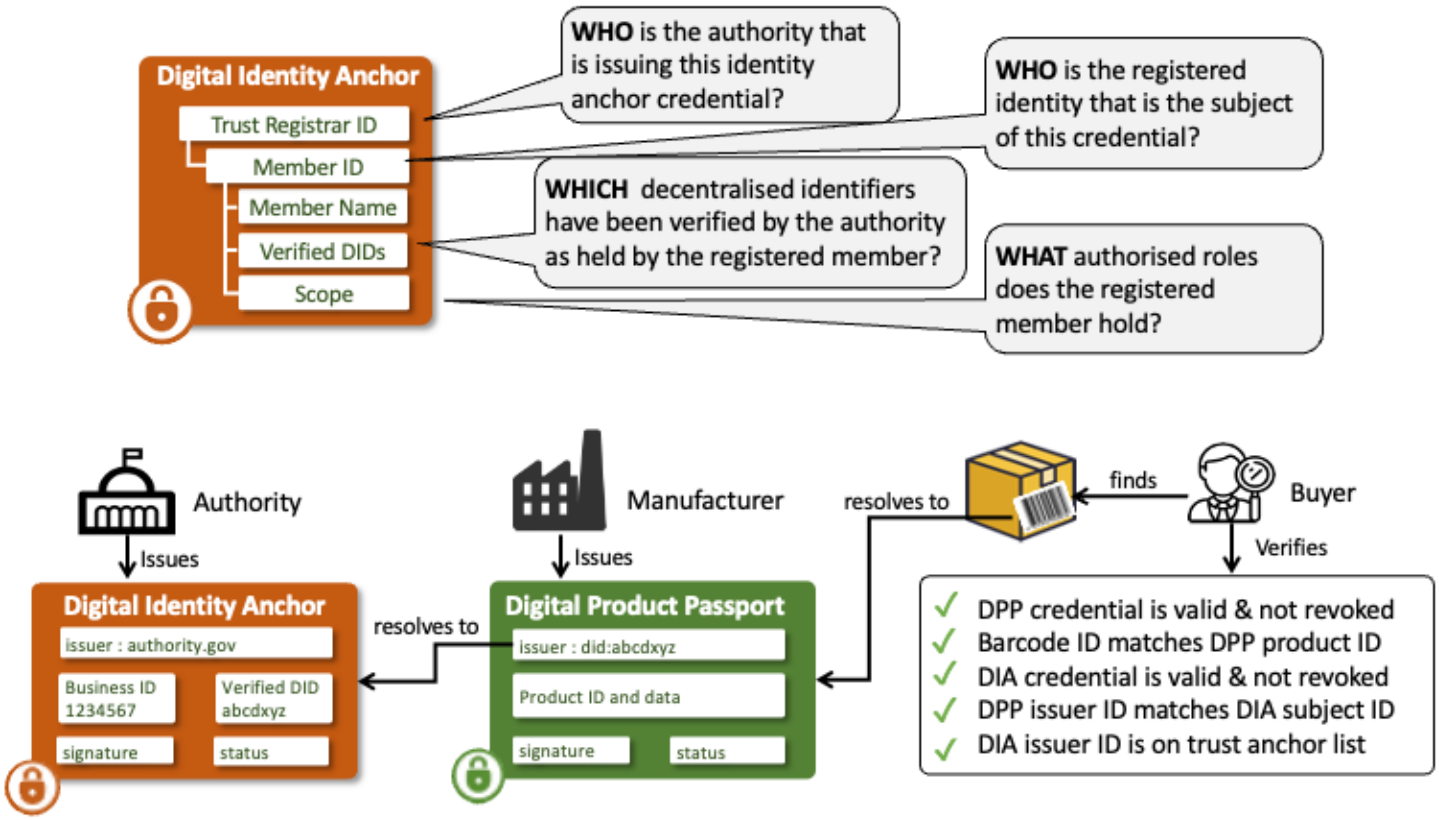
History of releases is available from the Version history page.

Overview

The Digital Identity Anchor (DIA) credential provides a simple means to verify the identity of UNTP credential issuers. The `issuer.id` property of all UNTP credentials is defined as a W3C decentralized identifier (DID) so that credentials like product passports can be cryptographically verified as genuinely issued by the issuer of the DID. But, as a self-issued identity, the DID does not provide confidence that the issuer is really who they claim to be. Authoritative identity registers such as national business registers, trademark registers, and land registers exist in most countries and have well established and trusted registration and maintenance processes. Unfortunately, most authoritative registers only issue paper or PDF registration certificates that are easily faked and are not usable for digitally verifiable proof of identity. The UNTP DIA is essentially a digitally verifiable version of a registration certificate. It is issued by the authoritative register to authenticated members when the member proves ownership of their DID to the register. When a DIA accompanies a UNTP credential such as a DPP, a verifier can confirm not only that the DPP was issued by the holder of the DID, but also that the controller of the DID is also the holder of the authoritative registered identity.

Conceptual Model

The Digital Identity Anchor (DIA) is a very simple credential that is issued by a trusted authority and asserts an equivalence between a member identity as known to the authority (eg a VAT number) and one or more decentralised identifiers (DIDs) held by the member. Before issuing the DIA, the authority should verify DID ownership (eg using DID Auth).



The outcome is that the subject of the DIA (eg the VAT registered business) can prove that they are the registered identity to any other party. In the UNTP context the DIA provides assurance that a DPP (or DCC/DFR/DTE) issuer really is who they say they are. The verification workflow is as follows

- A verifier (eg buyer of an identified product) discovers a DPP for the product and verifies the credential - confirming that the DPP has not been tampered-with, is genuinely issued by party identified by the issuer DID.
- The DID is resolvable to the DID document which contains a link to the DIA in the DID document `service` end point.
- Verify the DIA credential and confirm that the DPP issuer DID is contained in the `verifiedDIDList` of the DIA.
- Confirm that the issuer `did:web` of the DIA (the authoritative register) is on the white list of trust anchors.

The DIA can also be used for similar trust anchoring purposes such as:

- Accreditation authorities issue DIA to assert that a conformity assessment body is accredited against a given scheme.
- IP Offices issue DIA to assert that a registered party is the genuine owner of a trademark.
- Land registers issue DIA to assert that a regulated party is the owner of a geo-located property.

Requirements

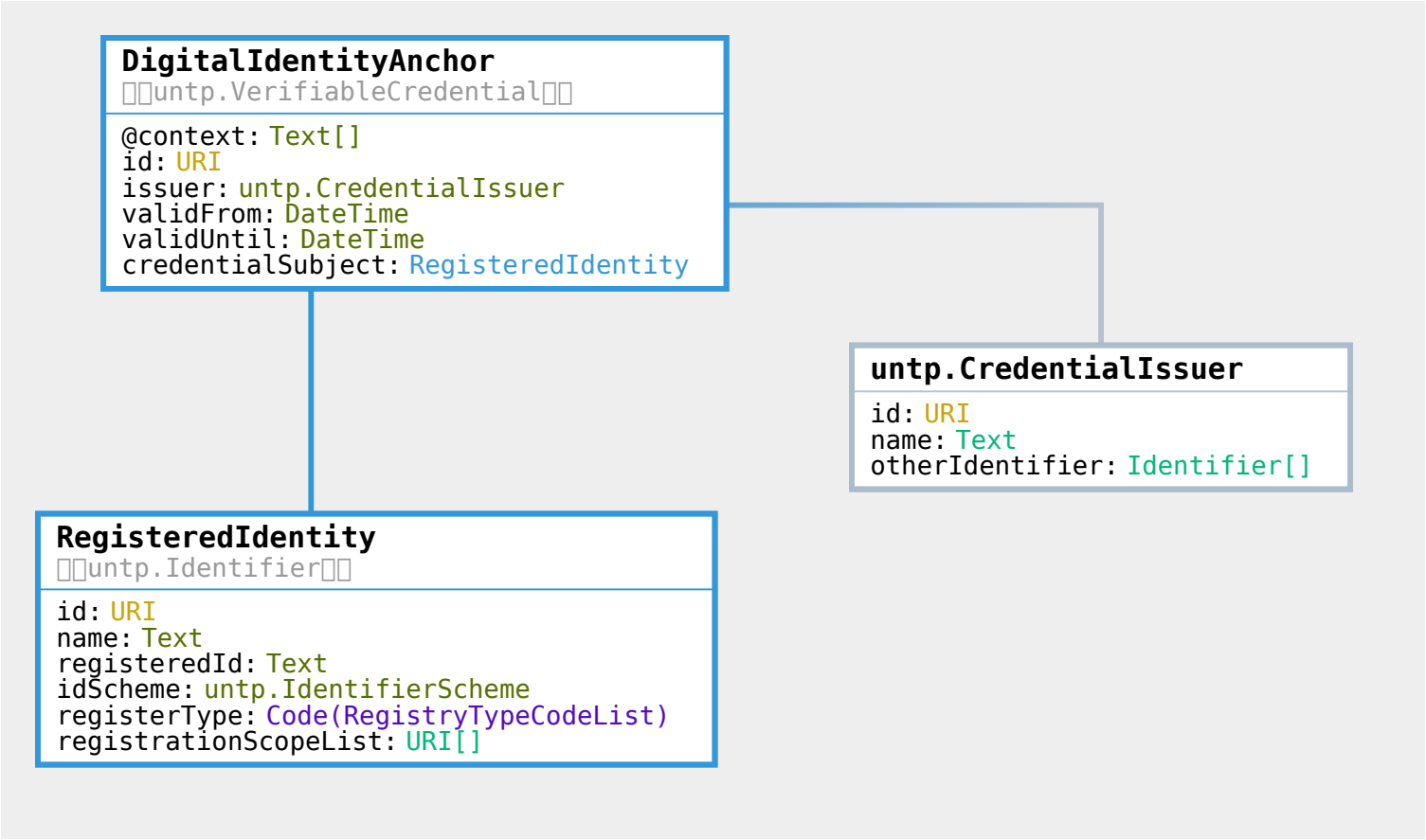
The digital identity anchor is designed to meet the following detailed requirements as well as the more general [UNTP Requirements(https://uncefact.github.io/spec-untp/docs/about/Requirements)]

ID	Name	Requirement Statement	Solution Mapping
DIA-01	DID Verification	The DIA issuer (registrar) MUST confirm that the registered member (subject) is the legitimate controller of a DID before issuing a DIA credential so that the registrar is protected against members falsely claiming ownership of well known DIDs	MAY use the DID Auth protocol for this purpose.
DIA-02	DIA Issuer DID	The DIA issuer MUST use did:web as the DIA issuer and the web domain MUST match the well known domain of the issuing authority so that verifiers can confirm authority identity via public web records.	DIA issuer specification
DIA-03	Scheme registration	The DIA issuing authority SHOULD register the identity scheme (including the trusted issuer DIDs) with the UN/CEFACT identifier scheme registry so that verifiers can leverage UN maintained scheme metadata to simplify DIA discovery and verification.	See UNTP Identity Resolver
DIA-04	Multiple DIDs	A registered member may need to link multiple DIDs to one registered ID, either because there is a need to transition between DID service providers or because an organisation may choose to use different DIDs for different purposes.	Issue multiple DIAs
DIA-05	Scope List	The DIA MUST include a list of scope URIs that unambiguously define the authorised role(s) of the member in the register so that verifiers can confirm the scope of the membership.	`scopeList` property
DIA-06	Register Type	The DIA MUST specify the register type so that verifiers can understand the context of the `registrationScopeList`	`registerType` property
DIA-07	DIA Discovery	The DIA SHOULD be discoverable given either the DID or the registeredID	DIA Discovery
DIA-08	White list	The DIA should include a mechanism to avoid malicious actors who are not the registrar from issuing DIAs that claim links to authoritative registered IDs	Maintain white list of trusted issuer DIDs on UN/CEFACT identifer scheme registry

The examples below help to clarify the application of DIA-05 and DIA-06.

Logical Model

The Digital Identity Anchor logical model.



Core Vocabulary Documentation

The UNTP core types vocabulary defines the uniquely identified Linked Data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. The Digital Identity Anchor only re-uses the UNTP core `VerifiableCredential` and `Identifier` classes.

DIA Documentation

The DIA documentation provides a technology-neutral definition of classes, properties and code lists in the DIA model.

Implementation Guidance

This section provides sample JSON-LD snippets for each DIA component.

Digital Identity Anchor

The Digital Identity Anchors is a Verifiable credential. Please refer to DPP VC Guidance for information about the use of the verifiable credentials data model for UNTP. The issuing party for the VC MUST be the authority that owns or operates the identity register.

Registered Identity

The registered identity class represents the registry member. For example, in a national business register, the registered identity would be one of the registered businesses.

- `type` MUST contain constant value array `["RegisteredIdentity", "Identifier"]` which declares to linked data processors that this is a registered identity which is a sub-type of identity.
- the `id` MUST contain DID of the registered member that is linked to the `registredID` and for which the registrar has verified is controlled by the subject.
- `name` is the human readable registered entity name and SHOULD match the registered name as it appears in the authoritative register.
- `registeredId` contains the simple identifier value that is unique within the register (but may not be globally unique) for example the VAT registration number.
- `idScheme` identifies the authoritative register. If the identity scheme is registered with UN/CEFACT then the `idScheme.id` MUST match the `identityRegister.id` in the UN/CEFACT scheme register.
- `registerType` is a coded value that allows verifiers to distinguish between different DIA use cases
- `registrationScopeList` contains a list of URIs that define the scope of the member registration. The values are very specific to the register. For example a national business register would typically have a controlled vocabulary of entity types (eg Australian Entity Types)

```
"credentialSubject": {
  "type": [
    "RegisteredIdentity",
    "Identifier"
  ],
  "id": "did:web:samplecompany.com/123456789",
  "name": "Sample business Ltd",
  "registeredId": "90664869327",
  "idScheme": {
    "type": [
      "IdentifierScheme"
    ],
    "id": "https://sample-register.gov",
    "name": "Sample National Business Register"
  },
  "registerType": "Business",
  "registrationScopeList": [
    "https://sample-register.gov/EntityType?Id=00019"
  ]
}
```

DIA Trust Anchors

The integrity of the DIA depends on verifiers knowing the authoritative list of authoritative registry issuer DIDs. Whilst it is possible for each verifier to maintain their own whitelist of trusted issuers, scalable global uptake would be facilited if there is a UN maintained and trusted whitelist.

The data model for a UN maintained identifier scheme register is defined in the Identity Resolver specification and a prototype will be implemented for UNTP testing. A production implementation will require a new UN/CEFACT project proposal

which will be submitted in due course.

DIA Discovery

DIA credentials SHOULD be discoverable from either identifier:

- Given a DID (eg as the issuer of a DPP) via DID document `service` endpoint.
- Given a registered identifier (eg a VAT registration number) via the ID scheme resolver service.

Via DID Service Endpoint

As described in the W3C Decentralized Identifiers specification, DIDs are resolvable to a DID document. The `service` property of a DID document contains an array of typed `serviceEndpoint` which can point to services or credentials relevant to the DID. A DID document may also contain an "alsoKownAs" property which is typically used to reference other identifiers. Controllers of DIDs that are linked to authoritative register SHOULD

- Add the ID URI from the authoritative register to the `alsoKnownAs` list. In the snippet below `https://sample-register.gov/90664869327` has been added.
- Add proof that the relationship is reciprocal by adding a `service` object that references the DIA credential. In the example below, the DIA credential URL is `https://sample-credential-store.com/credentials/dia-90664869327.json`

```
{
  "id": "did:web:sample-business.com:123456789",
  "authentication": [{..}],
  ..
  "alsoKnownAs": ["https://sample-register.gov/90664869327"],
  "service": [{
    "id":"did:web:sample-business.com:123456789#90664869327",
    "type":"untp:dia"
    "serviceEndpoint": {
        "href":"https://sample-credential-store.com/credentials/dia-90664869327.json",
        "title":"Digital Identity Anchor",
        "type": "application/vc+jwt"
    }
  }]
}
```

Via Identity Resolver

As described in the UNTP Identity Resolver specification, existing identity registers are encouraged to make their registered identities *resolvable* and *verifiable*.

- Identifiers are made *resolvable* by implementing ISO-18975 to encode IDs as URLs and returning an IETF rfc-9264 link-set with links to relevant further data about the ID.
- Identifiers are made *verifiable* by issuing DIAs per this specification.

This presents the opportunity to make the DIA discoverable by returning an appropriate link in the link-set. For example, given a VAT registration number `90664869327` issued under scheme `https://sample-register.gov` and applying the scheme resolver template may yield a resolver service URL of `https://resolver.sample-register.gov/vatNumber/90664869327`

The resolver service may be called with parameters that define which link-types to return. `https://resolver.sample-register.gov/vatNumber/90664869327?linkType=all` will return a linkset that SHOULD contain the DIA credential link (among other links such as the registration history) as follows.


```
{
    "linkset": [
        {
            "anchor": "https://resolver.sample-register.gov/vatNumber/90664869327",
            "untp:dia": [
                {
                    "href": "https://sample-credential-store.com/credentials/dia-90664869327.json",
                    "title": "Digital Identity Anchor",
                    "type": "application/vc+jwt"
                }
            ]
        },
        {
            "anchor": "https://resolver.sample-register.gov/vatNumber/90664869327",
            "about": [
                {
                    "href": "https://sample-register.gov/registrationHistory?id=90664869327",
                    "title": "Registration History",
                    "type": "text/html"
                }
            ]
        },
    ]
}
```


Alternatively, invoking the resolver service with the DIA specific link type `https://resolver.sample-register.gov/vatNumber/90664869327?linkType=untp:digitalIdentityAnchor` would redirect directly to the matching link

```
https://sample-credential-store.com/credentials/dia-90664869327.json
```

DIA Use Cases

This section provides some example use cases for the UNTP DIA credential for different authoritative registr types

Business Registers

TBC

Facility Registers

TBC

Trademark Registers

TBC

Accreditation Registers

TBC

Land Registers

TBC

Product Registers

TBC

Decentralised Access Control

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

There is a balance between the demands of transparency (more supply chain visibility means it's harder to hide green-washing) and confidentiality (share too much data and you risk exposing commercial secrets). A key UNTP principle is that every supply chain actor should be able to choose their own balance between transparency and confidentiality. To achieve this, UNTP defines data confidentiality patterns with different degrees of data protection so that they can be appropriately combined to meet the confidentiality goals of each party.

The ability to enforce access control to non-public data is a critical capability for any traceability and transparency framework. But when the non-public data is distributed across thousands of different systems and needs to be accessed by authorised parties previously unknown to the holder of the data, traditional access control systems will not work. A decentralised data architecture also needs a decentralised access control mechanism.

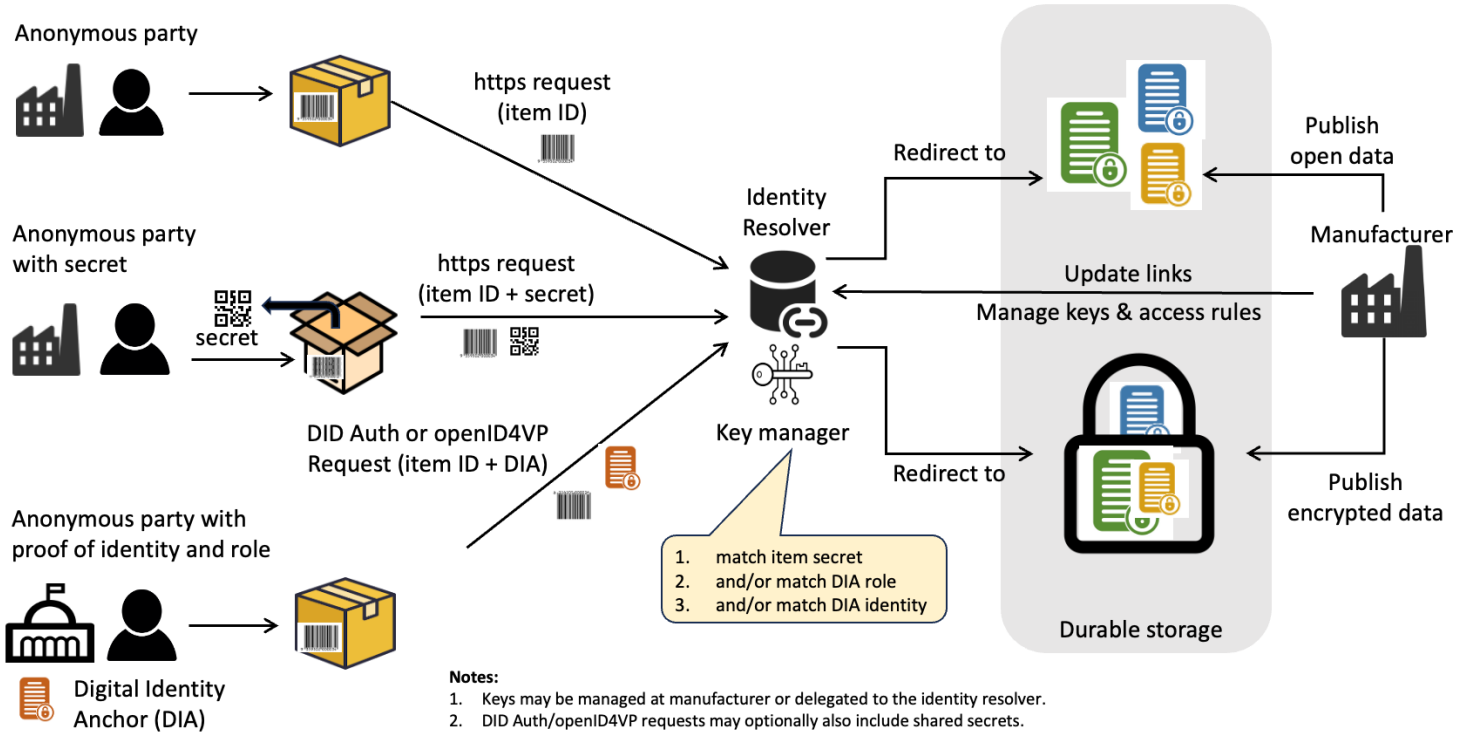
Conceptual Model

The conceptual model for decentralised access control is relatively simple. All non-public credentials are encrypted with a unique key for each credential. Access to encrypted data then boils down to the mechanism by which authorised parties acquire decryption keys from a data holder that may not know the requestor. There are only two ways to prove rights to encrypted data.

1. **You already have the key:** The key is passed by the data holder to the data requestor by a separate channel. For example, to empower access to non-public data by the legitimate purchaser of the goods, the key could be located inside the packaging of the product.
2. **You have a right to the key:** The key is made available to any data requestor that can prove their authorised role to the data holder via an authentication mechanism such as DID Authentication.

Each uniquely identified item will have a unique encryption key. Therefore the keys provided by either of the above methods is usable only to decrypt the data about a single item. Similarly, for confidential data about products or facilities each will have it's own unique encryption key.

Shared secrets and DID Authentication can be used in conjunction - for example a data holder may allow anonymous users to read non-public data with just a secret but may require both the secret (to prove item ownership) and DID Authentication (to confirm identity or role of the data requestor) to update item data.



The decryption of previously issued and encrypted verifiable credentials is preferred over any dynamic service because

- The same encrypted UNTP credential is used for both the shared secret and DID authentication access models.
- The access control is easily delegated to Identity Provider services and can continue to work even after the original issuer is no longer in business.

Requirements

- **data holder** is the party that created and maintains the information about a product or facility. Typically the product manufacturer or brand. The holder maintains both public and non-public data about the product or facility.
- **data requestor** is the party seeking access to product data held and maintained by the data holder.

ID	Name	Requirement	Solution Mapping
DAC-1	Anonymous access	As a data requestor that requires access to public product information, I should be able to access the information without any registration or identification - so that my privacy remains protected.	Anonymous public access
DAC-2	Access by legitimate owner	As the legitimate owner or user of a specific serialised item, I should be able to access non-public information such as usage and maintenance history about my item and also be able to update post-sale	Anonymous access with secret

ID	Name	Requirement	Solution Mapping
		life-cycle events without any need to register or identify myself to the data holder.	
DAC-3	Access with verifiable role	As an authorised actor such as an accredited recycling plant or a government authority, I should be able to access and update non-public product information according to my authorised role even if I am otherwise unknown to the data holder.	Decentralised authentication - role `registrationScopeList` property
DAC-4	Access with verifiable identity	As a known and trusted data requestor party I should be able to prove my identity to the data holder and be granted access according to my permissions.	Decentralised authentication - ID `registeredId` property or any federated identity protocol
DAC-5	Confidential supply	As a buyer who received credentials from my suppliers that provide confidence in the sustainability or quality of my upstream supply chain, I would like to pass on the sustainability or quality confidence to my customers without revealing the identity of my suppliers.	N-tier supplier visibility
DAC-6	Discoverability	As any data requestor that queries available data about a product or facility from an identity resolver service, I would like to understand not only what public data is available but also what confidential data is available and what evidence I need to provide to access the confidential data.	Discoverability of encrypted content
DAC-7	Durability	As a data requestor seeking information about a product or facility, I want to access the necessary data according to my role even if the original manufacturer is no longer in business and whether or not the data is open or confidential.	Durable storage options
DAC-8	Limit impact	The confidential data access scope associated with a specific secret key should be limited to one product or item so that the consequence of un-authorised access to confidential data minimised	Encryption granularity
DAC-9	Small footprint	Where space is tight (eg under a wine bottle cap) then a small format secret key option is available.	Secret key carrier

Decentralised Access Control

The simple matrix below will assist the reader to understand the context of the access control guidance and when to use each access model.

Security context	no secret key	access with secret key
no authentication	publicly discoverable data	item specific confidential data (eg service history) for the legitimate product owner
authenticated & authorised role	authorised role access to confidential data about multiple items (eg a customs authority)	authorised role access to specific item data only (eg repair facility update to item history) or facility level confidential data.

The following paragraphs provide guidance on how to secure data and grant access for various scenarios.

Anonymous public access

Anonymous access to public data is the default UNTP access pattern. It is already described in the identity resolver specification. From a security and resilience perspective, the only requirements are

- That data providers MUST NOT **require** personal identifying information from the data requestor as a condition of providing public information.
- That data SHOULD remain available for the lifetime of the product, irrespective of whether the original manufacturer still exists.

Both of these requirements are met using the identity resolver specification.

Item identifier as shared secret

Most item identifiers are relatively short numbers and are issued sequentially. So, for example, if `https://example.com/product/11223/serial/44556` is a known product and serial identifier then it is likely that the next serialised item ID could be `https://example.com/product/11223/serial/44557` or that the next product and serial in the range could be `https://example.com/product/11224/serial/00001`. When identifiers are easily guessed then information about the products is easily discovered even when the data requestor is not in possession of an actual product or serialised item.

However, if the product and serial numbers are issued as **genuinely random** large numbers then they become un-guessable and so any public (ie non-encrypted) data linked to the ID can be considered to be accessible only to the party in possession of the item. For example `https://example.com/product/11223/serial/44FDB2AFC91B898893CF36CB18863D26` is a product with a 32 character hexadecimal (128 bit) serial number and, provided the serial number is genuinely random, is computationally impractical to guess (1 billion guesses per second would still take many universe lifetimes).

Large random serial numbers are not common practice in industry and so are more likely to be considered for new rather than existing identifier schemes. However, depending on the sensitivity of the data, shorter serial numbers such as the 20-character GS1 SGTIN (eg `https://example.com/01/0952400005919/21/419A2845FD8050A0DD56`) may provide adequate confidentiality provided they are issued randomly and not sequentially. For example, if serial number `419A2845FD8050A0DD56` were one of a million serialised items of product ID `0952400005919` then it would still take a few years to guess one matching serial number at 1 billion guesses per second.

When non-guessable large identifiers are used as a security mechanism to access non-encrypted sensitive data, then;

- the access mechanism is no different to anonymous public access.
- the identifiers MUST be **genuinely random** strings
- the data MUST NOT be index-able by search engines.
- the web repository that holds the data MUST NOT be searchable or expose lists of stored file.

Confidential data encryption

In many cases, relying on an un-guessable identifier is not possible or not sufficiently secure. In such cases, confidential data SHOULD be encrypted.

- Encryption MUST be done with a symmetric encryption algorithm such as AES with a minimum of 128 bit key length.
- Each distinct identified entity (i.e. facility, product, product batch, or serialised item with a unique IDR path) MUST use a separate and unique encryption key.
- Where there are multiple different authorised roles that require access to different non-public data then a unique encryption key SHOULD be used for each role.
- Where there are multiple non-public documents or credentials for a given unique entity and authorised role then they SHOULD be encrypted with the same key.

These encryption requirements will result in an optimal granularity of encryption where one or more encrypted objects about a specific item and for access by a specific authorised role are all encrypted with the same key. But data for other roles or other items are not accessible with the given key.

Decryption key as shared secret

When confidential data about serialised items is encrypted then decryption keys SHOULD be included with the product and be optimised for easy use.

- The key SHOULD be presented as a QR code (either included with the product or, for bulk/raw materials, sent separately)
- The code MUST resolve to an Identity Resolver query URL for the given item and with the symmetric key secret as a `key` parameter.
- For cases with limited space such as a QR under a wine bottle cap, implementers MAY use a shorter URL that redirects to the same full identity resolver URL. The short URL SHOULD include 128 bit entropy so that it is sufficiently un-guessable.

For example, for a 128 bit AES key in a query to a resolver about product ID 90664869327 that returns only encrypted link targets for anonymous access the resolver URL would be `https://resolver.product-register.com/01/90664869327?key=2b7e151628aed2a6abf7158809cf4f3c&accessRole=untp%3AaccessRole%23Anonymous`

Small footprint codes

A 128 bit short redirect URL (in capitals because that creates smaller QR codes) can be used for cases where there is limited space for QR codes. For example `HTTPS://REDIRECT.IO/E05778C659733E222758AC5179AE4611` could redirect to the same full URL `https://resolver.product-register.com/01/90664869327?key=2b7e151628aed2a6abf7158809cf4f3c&accessRole=untp%3AaccessRole%23Anonymous`

The full and short URLs would produce the following QR codes

Full resolver URL	Short redirect URL
	

Federated authentication workflow

In some cases access to (and update of) confidential data requires more than a shared secret that proves ownership of a serialised item but also requires evidence that the data requestor has an authorised role such as a competent authority, a recycling plant, or accredited auditor. When the data requestor is already known and registered with the data provider then a conventional "sign-in-with" federated authentication and authorisation mechanism such as OAuth 2.0 or OIDC can be used. UNTP does not impose any restrictions on how a data provider authenticates and authorises access to protected data for users that are already known to the provider.

However, these kind of protocols require a relying-party relationship between the data provider that requires evidence of identity (eg a product passport issuer) and an identity provider that is the manager of the identity (eg a regulatory authority). Although this "sign-in-with" protocol is easy to implement with social network identity providers who deliberately place low barriers to relying parties, more authoritative registers such as national business registers, land registers, trademark registers, and so on are much more conservative. They mostly either don't offer federated identity or even if they do, they are very restrictive about allowed relying parties.

Decentralised authentication workflow

Decentralised protocols provide a much simpler and more scalable authentication and authorisation approach for decentralised architectures that avoids any need for direct collaboration or dependencies between data providers and identity providers. For example, consider an access rule defined by a China based battery manufacturer that says "to update battery status to `recycled` the requestor must be an accredited recycling establishment operating in a recognized jurisdiction (eg Australia). The workflow would be

- Australian recycling plant "Sample Recyclers" is accredited under the Australian Government Department of Environment stewardship scheme and has obtained a Digital Identity Anchor credential that links their DID to their government accreditation status.
- Sample Recyclers receives a battery for recycling after 7 years of use that was originally made by "China Batteries Sample Co". It has a serialised item specific QR secret printed on the battery.
- Sample Recyclers scans the QR (which includes presentation of the secret), receives a IDR link-set response that includes a UNTP standard link that defines an authenticated method and URL to add a recycled event to the battery history that requires evidence of accredited recycler status.
- Sample Recyclers authenticates to the specified endpoint using DID-Authentication and presents their Australian Government issued DIA credential as a verifiable presentation.
- China Sample Batteries Co verifies the presentation (which confirms DID control) and checks that the issuer (AU government) is on their trusted white-list, and then adds the recycled event to the item history.

Decentralised authentication protocol options.

UNTP does not define any new protocols for decentralised authentication but rather supports the use of any of the existing standards listed below.

- DID Auth specification link : https://w3c-ccg.github.io/vp-request-spec/#did-authentication
- DID SIOP specification link : https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
- OID4VP specification link : https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

Aspect	DID Authentication	DID-SIOP	OpenID4VP
Primary Purpose	DID-based authentication with credential integration	Decentralized login using OIDC	Credential presentation in OIDC
Workflow Complexity	Moderate	Moderate	Complex
OIDC Integration	No	Yes	Yes
Use Case Focus	Proving DID control with credential attachment	Decentralized login	Claim verification and presentation

The best choice will eventually be the specification(s) that demonstrate the widest market implementation. At this time, the UNTP recommendation is that implementers SHOULD use **DID-Authentication** but MAY also use either **DID-SIOP** or **OpenID4VP**.

Confidential data discovery

Identity resolvers MUST include information to indicate when a link target is encrypted. Resolvers MUST also provide information about how to POST update events, where appropriate.

- When a link target is encrypted, the `encryptionMethod` custom property MUST be included with a value drawn from the UNTP encryption method code list.
- When a link target is encrypted, the `accessRole` custom property MUST be included. The allowed values are an array of URIs that will be used to match against `registrationScopeList` in digital identity anchor credentials.
- To indicate that access is allowed by any party that holds a secret key, the accessRole `untp:accessRole#Anonymous` MUST be included.
- To indicate that the link target is an update service, the `method":"POST"` property is required, together with the `accessRole` needed for the update to be accepted.

For example

```
{
    "linkset": [
        {
            "anchor": "https://resolver.product-register.com/01/90664869327",
            "https://vocabulary.uncefact.org/untp/linkType#digitalTraceabilityEvent": [
                {
                    "href": "https://sample-credential-store.com/credentials/dte-90664869327.json",
                    "title": "Battery maintenance event",
                    "type": "application/ld+json",
                    "lang": ["en"],
                    "encryptionMethod": "AES-128",
                    "accessRole":["untp:accessRole#Anonymous"]
                 },
                {
                    "href": "https://api.sample-credential-store.com/credentials",
                    "title": "Battery recycling event",
                    "type": "application/ld+json",
                    "lang": ["en"],
                    "method": "POST",
                    "accessRole":["untp:accessRole#Recycler"]
                 }
            ]
        }
    ]
}
```

Implementation Considerations

To do - add guidance relevant to decentralised access control for common concerns and use-cases.

Linked confidential data

Data about a value chain comprises multiple credentials about products and facilities in a linked-data graph. Any of the credentials in the graph may be considered confidential and therefore be protected by an appropriate access control method. This will present challenges for verifiers such as supply chain traceability systems that need to traverse long graphs for their customers. A typical scenario might work as follows:

- A verifier encounters a serialised product ID and performs an IDR lookup which returns a link-set which contains:
  - link to an un-encrypted Digital Product Passport (DPP) which also contains an ID of the facility that manufactured the item
  - links to an encrypted Digital Traceability Event (DTE) with `"encryptionMethod": "AES-128"` and `"accessRole": ["untp:accessRole#Anonymous"]` properties.
- The verifier has the secret key for the given item and so decrypts the DTE to find that it is a transformation event that lists the identifiers and quantities of input products.
  - For some of the input product ID, the verifier is able to resolve link-sets from relevant IDRs and access public data (eg DPPs) about the input products.
  - The input product IDR process also returns encrypted links but they cannot be decrypted because the verifier has no access to the secret key for supplier input products.
- The verifier resolves the facility ID found in the DPP to a new link-set that contains links to both public and private data about the facility.
  - A link to a public digital facility record (DFR) includes precise geo-location information as well as some public sustainability claims.
  - A set of links to facility level conformity credentials (DCC) that are encrypted and have `"accessRole": ["untp:accessRole#Customer"]` property. The verifier uses DID-Authentication to connect to the DCC end points and presents a Digital Identity Anchor (DIA) that proves the verifier ID which matches a facility customer list. Decryption keys are provided with a new link-set of the authorised customer.

In general, when a verifier hits a graph node that in encrypted and does not have access keys, then graph traversal cannot proceed beyond that node. Perhaps the most common scenario will be transformation events that reveal the input products (and suppliers) in a manufacturing process.

N-tier supplier visibility

To do - guidance about how to handle upstream product / supplier data that is considered sensitive. There are likely to be four "levels" of transparency that implementers may choose:

- Make it all public
- Make your suppliers visible only to your direct customers (eg if the ID in your DIA matches the destination party ID in a transaction event)
- Use a trusted third party to assess to your supply chain sustainability without revealing supplier identities - and issue a more public digital conformity credential that attests to qualities without identities.
- Make it all private and never share anything.

Durable storage

To do - write some words about how to manage protected data even after the supplier / publisher is no longer in business.

Sustainability Vocabulary Catalog

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Artifacts

Are maintained at https://test.uncefact.org/vocabulary/untp/core/0/about

Stable Releases For Implementation

Version 1.0 stable release for production implementation is due Jan 2025

Release for Pilot Testing

UNTP Core Vocabulary version 0.5.0 release artifacts can be used for pilot testing.

- JSON-LD @context
- JSON-LD Vocabulary

Note that the vocabulary is accessible either in human readable form or machine readable form via the same URL - but with different accept header:

curl https://test.uncefact.org/vocabulary/untp/core/0/ -H 'Accept: application/ld+json'

Latest Development Version

Latest development versions are used to reflect lessons learned from pilots but should not be used for either pilot testing or production purposes.

Version History

History of releases is available from the **Version history** page.

Overview

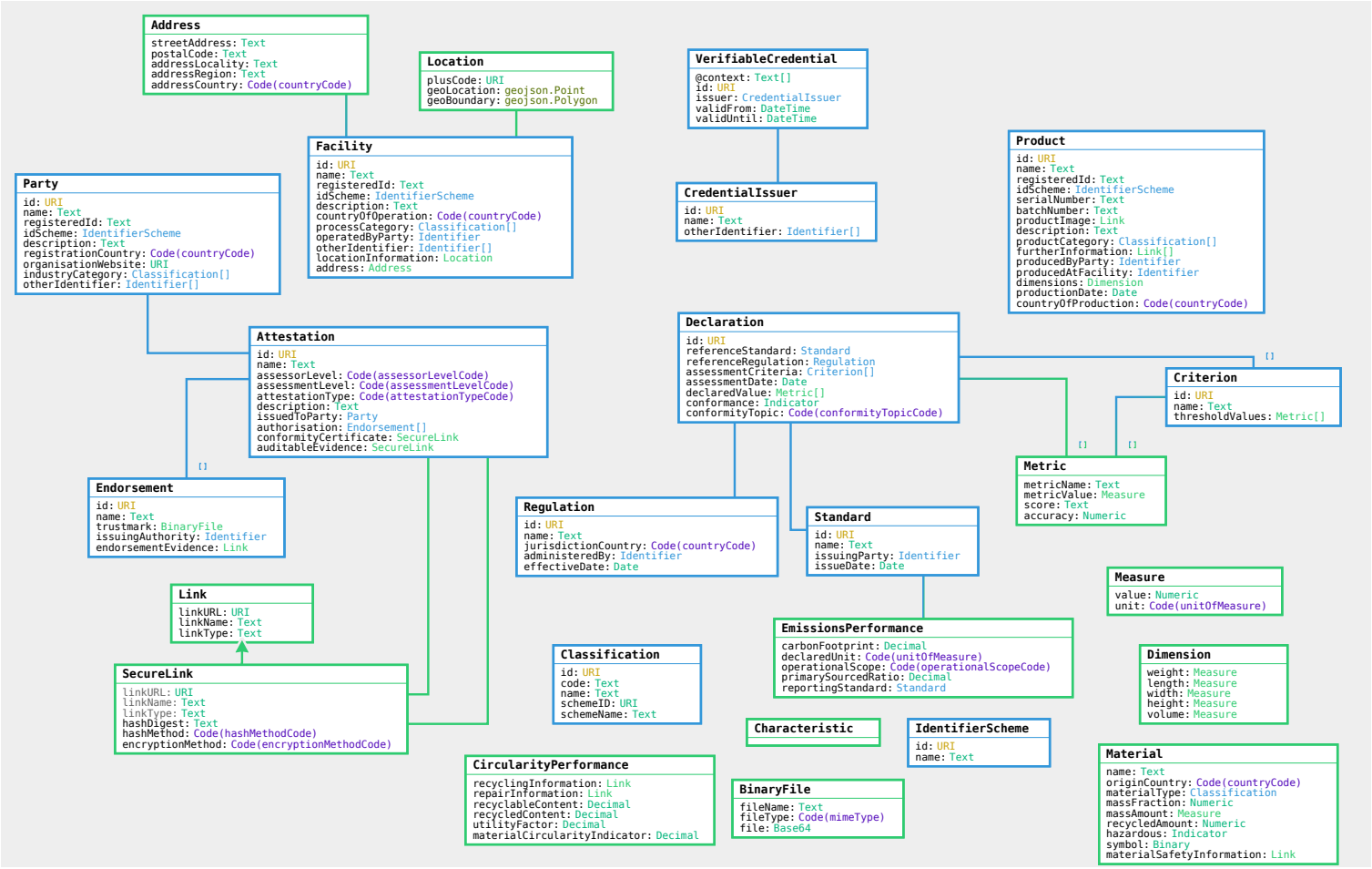
Web **vocabularies** are a means to bring consistent understanding of **meaning** to ESG claims and assessments throughout transparent value chains based on UNTP. There are hundreds of ESG standards and regulations around the world, each with dozens or hundreds of specific conformity **criteria**. Any given value chain from raw materials to finished product is likely to include dozens of passports and conformity credentials issued against any of thousands of ESG criteria. Without a consistent means to make sense of this data, UNTP would provide a means to discover a lot of data but no easy way to make sense of it. The UNTP defines a standard and extensible topic map (taxonomy) of ESG criteria and provides a mechanism for any standards authority, or national regulator, or industry association to map their specific terminology to the UNTP vocabulary.

UNTP Core Vocabulary

The UNTP core vocabulary defines the uniquely identified linked data entities such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the building blocks for construction of Digital Product Passports and Digital Conformity Credentials.

- A Digital Product Passport is a set of declarations (claims) against sustainability criteria defined in regulations or standards - made by a manufacturer party about a given product that is manufactured at a facility in a defined location.
- A Digital Conformity Credential is an attestation made by an endorsed conformity assessment body - which includes one or more assessments of a list of identified products or facilities against specific criteria.

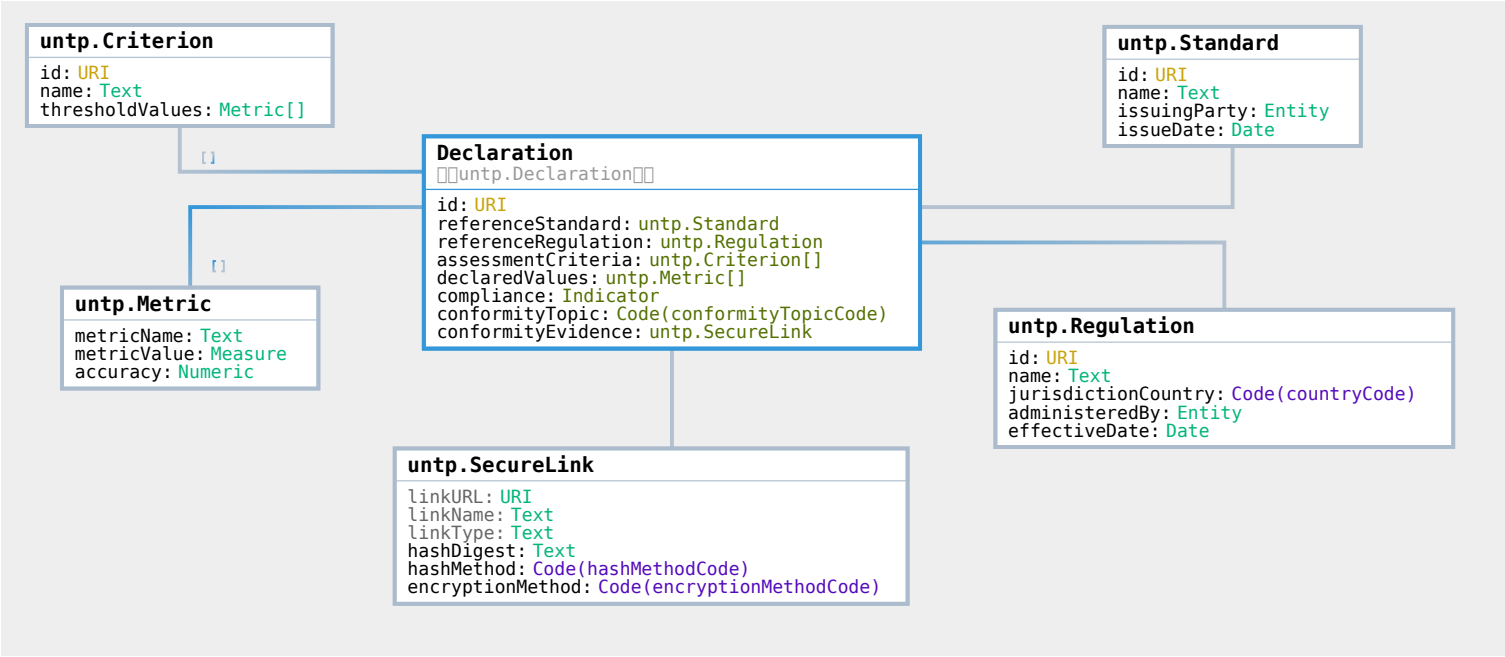
Although these two credential types have different structures, they are assembled from the same core vocabulary building blocks. This allows a supply chain transparency system to easily construct a linked data graph (a.k.a "transparency graph") from a stream of DPPs and DCCs. Claims about a product found in a DPP can be linked to assessment of the same product in DCC when both credentials have matching product and criteria identifiers.



The core vocabulary data model and browsable documentation

Declarations Structure

The declarations structure defined in the core vocabulary is re-used by both the Digital Product Passport (as manufacturer self-assessments) and the Digital Conformity Credential (as third party conformity assessments). The declarations structure is defined here and referenced by both the DPP and DCC pages.



The conformity Information structure in the DPP is an array of UNTP `Declaration` types that carry product conformity or sustainability claims made by the manufacturer. The key properties are

- The `id` which must be globally unique and may be either a UUID or a URI in the DPP issuer's domain.
- The `referenceStandard` against which the conformity claims are made. This is a UNTP `Standard` object
- The `referenceRegulation` against which the conformity claims are made. In most cases a conformity claim will reference either a `Standard` or a `Regulation` but in some circumstances both will apply.
- The `assessmentCritieria` is an array of UNTP `Criterion` objects that define the specific rule(s) within the standard or regulation against which this conformity claim is made.
- The `thresholdValues` are an array of UNTP `Metric` objects that define the minimum or maximum values that are required to be met. For example, a construction steel standard might specify 300 MPa as the minimum tensile strength threshold.
- The `declaredValues` property defines the actual specified values for the DPP product. For example, a minimum tensile strength of 350 Mpa within a 5% confidence range. In many cases this may be sensitive data and can be replaced by a simple `compliance` assertion.
- The `conformance` boolean is a declaration by the product manufacturer that the product meets the conformity criteria specified.
- The `conformityTopic` is a high level UNTP classification scheme for safety and environmental and social sustainability.
- `benchmarkValue` (eg 10 Tons per Ton carbon intensity) is used in cases where a `declaredValue` (eg 5 Tons per Ton) is usefully compared to an industry average performance (benchmark) value. When a `benchmarkValue` is provided, a `benchmarkReference` link MUST also be provided and should provide a link to an authoritative reference to support the benchmark value.
- `conformityEvidence` is a `Link` to a second or third party attestation such as a UNTP Digital Conformity Credential that provides independent verification of the claims made. Note that this property may also link to a PDF or a website or some other format of conformity evidence.

```
"conformityDeclaration": [
     {
```

```
        "type": [
          "Declaration"
        ],
        "id": "https://files.example-company.com/declarations/90664869327/",
        "referenceStandard": {
          "type": [
            "Standard"
          ],
          "id": "https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-master.pdf",
          "name": "GBA Battery Passport Greenhouse Gas Rulebook - V.2.0",
          "issuingParty": {
            "type": [
              "Entity"
            ],
            "id": "https://kbopub.economie.fgov.be/kbopub/toonondernemingps.html?
ondernemingsnummer=786222414",
            "name": "Global Battery Alliance",
            "registeredId": "786222414",
            "idScheme": {
              "type": [
                "IdentifierScheme"
              ],
              "id": "https://kbopub.economie.fgov.be/",
              "name": "Belgian business register"
            }
          },
          "issueDate": 2023
        },
        "referenceRegulation": {
          "type": [
            "Regulation"
          ],
          "id": "https://www.legislation.gov.au/F2008L02309/latest/versions",
          "name": "National Greenhouse and Energy Reporting (Measurement) Determination",
          "jurisdictionCountry": "AU",
          "administeredBy": {
            "type": [
              "Entity"
            ],
            "id": "https://abr.business.gov.au/ABN/View?abn=72321984210",
            "name": "Clean Energy Regulator",
            "registeredId": "72321984210",
            "idScheme": {
              "type": [
                "IdentifierScheme"
              ],
              "id": "https://abr.business.gov.au/ABN/",
              "name": "Australian Business Number"
            }
          },
          "effectiveDate": 2024
        },
        "assessmentCriteria": [
          {
            "type": [
              "Criterion"
            ],
            "id": "https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-master.pdf",
            "name": "GBA Battery rule book v2.0 battery assembly guidelines.",
            "thresholdValue": [
```

```
            {
              "metricName": "Industry Average emissions intensity",
              "metricValue": {
                "value": 1.8,
                "unit": "NIL"
              },
            }
          ]
        }
      ],
      "declaredValue": [
        {
          "metricName": "GHG emissions intensity",
          "metricValue": {
            "value": 1.5,
            "unit": "NIL"
          },
          "accuracy": 0.05
        },
        {
          "metricName": "GHG emissions footprint",
          "metricValue": {
            "value": 15,
            "unit": "KGM"
          },
          "accuracy": 0.05
        }
      ],
      "conformance": true,
      "conformityTopic": "environment.energy",
      "conformityEvidence": {
        "linkURL": "https://files.example-certifier.com/1234567.json",
        "linkName": "GBA rule book conformity certificate",
        "linkType": "https://test.uncefact.org/vocabulary/linkTypes/dcc",
        "hashDigest": "6239119",
        "hashMethod": "SHA-256",
        "encryptionMethod": "AES"
      }
    }
  ],
```


Sustainability Vocabulary Catalog

The sustainability vocabulary catalog is designed to provide a reference-able digital library of sustainability conformity standards, regulations, and criteria that can be used as an allowed set of terms to use in conformity declarations. The library also aims to provide a mechanism for mutual recognition of conformity criteria between different regulations and standards.

TBA

Best Practices

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Design patterns are non-normative but provide best practice guidance for UNTP implementers.

Trust Graphs

The ESG footprint of a finished product is the aggregation of it's components and processes through the value chain. Verification of ESG claims therefore involves assessing a bundle of linked credentials (aka a "trust graph") drawn from all or part of a value chain. Whilst each credential may be valid in it's own right, one challenge is verifying the context of related credentials. For example, a conformity assessment body that is accredited to test strength of structured steel might not be accredited to issue emissions intensity certificates. A technically valid emissions certificate linked to a technically valid accreditation certificate that has a different scope would be fraudulent. To address this problem, the UNTP defines a simple method to verify the contextual scope of linked credentials. Essentially this provides a mechanism to verify a linked graph of data at a layer above individual credential verification.

Data Carriers

Digital data needs to be linked to the physical product it describes and should be discoverable through the identifiers printed on that product serial or batch number. For high volume goods and easy / reliable discovery, these identifiers are already typically represented as barcodes, matrix codes, QR codes, or RFID encoded data. UNTP supports the use of these existing data carriers. A basic UNTP principle is that if you have a product then you should be able to find ESG data about that product even when the identifier is not a web link. Therefore, the UNTP defines a generalised protocol (based on GS1 Digital Link) to allow any identifier scheme (GS1 or otherwise) to be consistently resolvable so that product passports and other data can always be accessed from the identifier of the product. The UNTP also defines a specific QR based data carrier format for use on paper/PDF versions of conformity credentials or other trade documents that provides secure access to credentials in a way that is both human and machine readable. This provides a simple but powerful mechanism to facilitate uptake of digital solutions alongside existing paper/PDF based frameworks.

Anti-Counterfeiting

As the value of genuinely sustainable goods increases, so do the incentives to sell fake goods as the real thing. UNTP defines a simple and decentralised anti-counterfeiting protocol that can be implemented by any producer at very low cost. It builds upon the W3C DID standard by issuing a unique DID (and corresponding keypair) for every serialised (individual or batch) product. The DID (and therefore the public key) is discoverable from the product serial number using the standard link resolver protocol. The item/batch level DID is cryptographically linked to the product class level DID The private key is discoverable

from a QR code hidden inside the product packaging. Scanning the QR provides the necessary key to update the individual serialised product public status to indicate consumption. Attackers that copy genuine serial numbers will find that their products are quickly identifiable as fakes. Attackers that try to create new serial numbers will not be able to create valid links to the genuine product class. The UNTP anti-counterfeiting protocol provides additional value/incentive for UNTP uptake beyond ESG integrity.

Mass Balance

Mass balance fraud is a particularly challenging greenwashing vector. It happens when a fraudulent actor buys a small quantity of high ESG integrity inputs (eg genuine carbon neutral, organic, deforestation free cotton) and mixes that input with lower quality alternatives and then sells the full volume of manufactures product (eg woven cotton fabric) as sustainable product, re-using the valid credentials from the niche supply. The UNTP solution to this problem involves trusted third parties (certifiers or industry associations) to act as quota managers that issue "guarantee of origin" credentials (a type of conformity credential). In this model, the guarantee of origin certificate for 10 Tons of cotton fabric (for example) can only be issued when the third party has evidence of the purchase of at least 10 Tons sustainable input materials. The third party will also mark the input batch as consumed (in a similar way to the anti-counterfeiting protocol) so that the valid sustainble input cannot be re-presented to a different third party.

ESG Rules

Yet another greenwashing attack vector is to deliberately apply incorrect rules to the determination of criteria such as emissions intensity. The verification question in this case is "yes, but how do I know you calculated it right?". The UNTP proposes an independent calculator service offered either by the standards body or regulator that defined the rules or by an accredited service provider. The Supply chain actor presents raw data to the calculator which returns with a signed credential confirming that the rules were correctly applied. This protocol has an additional benefit for legitimate actors if widely adopted by rules authorities - which is to significantly simplify the assessment of compliance against multiple different rules. By separating observed facts from the assessment of those facts against specific rules then it becomes relatively simple to test compliance against multiple standards and regulations.

Data Carriers

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

Digital data needs to be linked to the physical product it describes and should be discoverable through the identifiers printed on that product, including serial or batch number as appropriate. For high volume goods and easy / reliable discovery, these identifiers are already typically represented as barcodes, matrix codes, QR codes, or RFID encoded data. UNTP supports the use of these existing data carriers. A basic UNTP principle is that if you have a product then you should be able to find ESG data about that product even when the identifier is not a web link. Therefore, the UNTP defines a generalised protocol (based on ISO/IEC DIS 18975) to allow any identifier scheme (GS1 or otherwise) to be consistently resolvable so that product passports and other data can always be accessed from the identifier of the product. The UNTP also defines a specific QR based data carrier format for use on paper/PDF versions of conformity credentials or other trade documents that provides secure access to credentials in a way that is both human and machine readable. This provides a simple but powerful mechanism to facilitate uptake of digital solutions alongside existing paper/PDF based frameworks.

Resolvers

A *resolver* is a service that connects an identifier to one or more sources of information about the identified thing. An internet domain name *resolves* to one or more actual servers (identified by their IP addresses). Digital Object Identifiers (DOIs), commonly used to identify research papers, *resolve* to the paper itself (wherever it may be). In the UNTP context, identifiers for products, locations and supply chain operators must resolve to information about those entities. This can include the DPP, ESG certificates and more, some of which may be access-controlled. That is, knowing the location of information is not the same as automatically having access to it.

ISO/IEC DIS 18975 specifies two different approaches for encoding identifiers in HTTP URIs (web addresses). Either can be used to point to a resolver that associates an identifier with a set of links to one more sources of relevant information following the IETF's Linkset standard RFC9264. A conformant resolver can respond to queries for a particular type of information about the identified entity by providing the appropriate link from the linkset. GS1 Digital Link is conformant to this model. The URI syntax follows the *structured path* approach set out in ISO/IEC DIS 18975 and the GS1-Conformant resolver standard defines the related service. An example will make this clearer:

Imagine a white t-shirt that has a GTIN of 9506000164908. This can be encoded in a GS1 Digital Link URI as https://id.gs1.org/01/09506000164908, which can, in turn, be encoded in a QR Code. Following that link, without any specialist software, will take you to a landing page for the white t-shirt from which there are links to specific types of information. One of those links is to sustainability information. Using an app, it's possible to ask the resolver directly for that sustainability information by appending the GS1 Digital Link URI with an instruction thus: https://id.gs1.org/01/09506000164908?

linkType=gs1:sustainabilityInfo. The resolver recognises the `linkType` parameter and redirects immediately to that page. Alternatively, software can request the full linkset and either present it to the user or process it as it sees fit. See the next section for more on link types.

Link Vocabulary

With very few exceptions, all websites include hyperlinks to different pages within those websites. Users understand that clicking a 'menu' option will take them to that kind of information. Online newspapers provide a good example. There will typically be a home news section, foreign news, economics, sport, arts, lifestyle, weather, TV guide and so on. Applying this to UNTP, when looking for information about a product the user will want the DPP, certificates covering ESG issues and conformance, perhaps manufacturer's details. These can all be provided using the same infrastructure and methods as used for consumer information such as the sustainabilty page in the white t-shirt example above.

The IETF's RFC9264 defines how sets of links can be made machine-discoverable and machine-interpretable. The key feature being that each link is annotated with the type of thing it points to. There is no limit on those link types but interoperability is lost if everyone uses their own. Therefore it is preferable to choose link types from a defined list that is under formal change management. GS1 provides one such list as part of its Web Vocabulary.

1D Barcodes

2d Matrix Codes

QR Codes

RFID Codes

Transparency Graphs

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

The sustainability footprint of a finished product is the aggregation of it's components and processes through the value chain. Verification of sustainability claims therefore involves assessing a bundle of linked credentials (aka a "transparency graph") drawn from all or part of a value chain. Whilst each credential may be valid in it's own right, one challenge is verifying the context of related credentials. For example, a conformity assessment body that is accredited to test strength of structured steel might not be accredited to issue emissions intensity certificates. A technically valid emissions certificate linked to a technically valid accreditation certificate that has a different scope would be fraudulent. To address this problem, the UNTP defines a simple method to verify the contextual scope of linked credentials. Essentially this provides a mechanism to verify a linked graph of data at a layer above individual credential verification.

Trust Chains

In the world of verifiable credentials, it is crucial that such credentials are issued by trusted and accredited entities. Consider the scenario where GHG emissions of a product result in a GHG emissions tax that must be paid. In such cases, the potential for fraud is significant, as some manufacturers might falsely claim zero GHG emissions in their digital product passport or in a separate GHG emissions credential. To combat this, verifiers must be able to construct a chain of trust. For example

- A manufacturer issues a declaration in a UNTP Digital Product passport (DPP) that states an emissions footprint for a given product ID. If the verifier trusts the manufacturer then this may be sufficient. But often a third party attestation is needed.
- A third party Conformity Assessment Body (CAB) issues an attestation as a UNTP Digital Conformity Credential (DCC) about the same product ID that confirms the emissions footprint. If the verifier knows and trusts the CAB then this pay be sufficient. But there are thousands of CABs and so it is very possible that the verifier does not know the specific CAB.
- A national accreditation authority issues an endorsement as a UNTP Digital Identity Anchor (DIA) which states that the CAB is accredited to issue certifications under a recognised scheme such as the GHG Protocol. The number of accreditation authorities only a little large than the number of countries. So verifiers only need a short list of accreditation authorites ("trust anchors") in order to trust the chain from product manufacturer -> CAB -> national authority. But the list could be even shorter.
- Most national acreditation authorites are members of a global association such as ILAC. If ILAC were to issue a credential attesting that national authority is a member then there is a chain of trust from manufacturer -> CAB -> national authority -> ILAC.

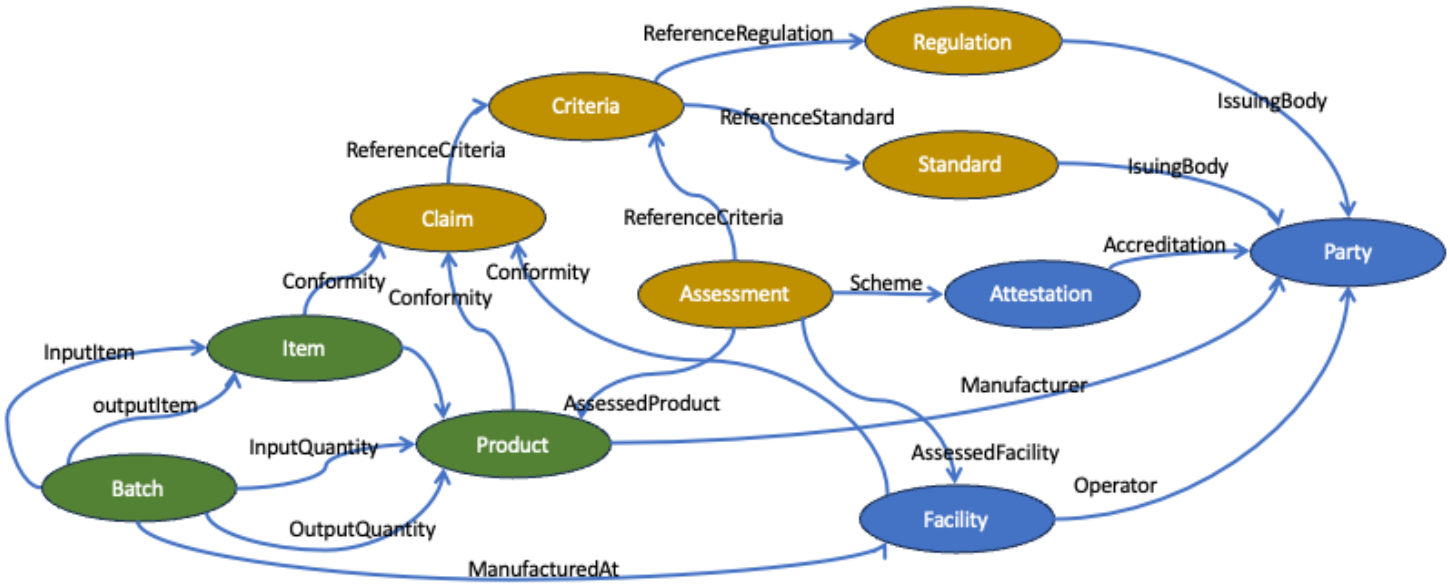
There are other trust chains that can be followed to anchor trust to a national or global authority that follows rigorous processes to manage it's accreditations and memberships. For example a battery passport may link to a certifier who is, in turn, accredited by the global battery alliance. Verifiers of credentials should follow these linked credential chains until a trusted entity is reached. That could be at the first step or after several steps.

Transparency Graphs

A transparency graph is a linked set of identified nodes such as Product, Location, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, or Endorsement. The data to construct a transparency graph comes from multiple individual credentials. When multiple credentials identify the same entity (eg a business, a facility, a product) then the graph will draw meaningful connections that can be used to make valuable verifications such as "product XYZ has a GHG assessment from CAB ABC". UNTP is designed to simplify the task of creating linked data graphs because UNTP credentials are represented as a collection of uniquely identified entities that are ready to be added to a graph.

- A Digital Product Passport is a set of declarations (claims) against sustainability criteria defined in regulations or standards - made by a manufacturer party about a given product that is manufactured at a facility in a defined location.
- A Digital Conformity Credential is an attestation made by an endorsed confomrity assessment body - which includes one or more assesments of a list of identified products or facilities against specific criteria.

Although these two credential types have different structures, they are assembled from the same core vocabulary building blocks. This allows a supply chain transparency system to easily construct a transparency graph from a stream of DPPs and DCCs. Claims about a product found in a DPP can be linked to assessment of the same product in DCC when both credentials have matching product and criteria identifiers.



JSON-LD Representation

TBA

SCHACL Graph verification

TBA

Anti-Counterfeiting

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

As the value of genuinely sustainable goods increases, so do the incentives to sell fake goods as the real thing. UNTP defines a simple and decentralised anti-counterfeiting protocol that can be implemented by any producer at very low cost. It builds upon the W3C DID standard by issuing a unique DID (and corresponding keypair) for every serialised (individual or batch) product. The DID (and therefore the public key) is discoverable from the product serial number using the standard link resolver protocol. The item/batch level DID is cryptographically linked to the product class level DID The private key is discoverable from a QR code hidden inside the product packaging. Scanning the QR provides the necessary key to update the individual serialised product public status to indicate consumption. Attackers that copy genuine serial numbers will find that their products are quickly identifiable as fakes. Attackers that try to create new serial numbers will not be able to create valid links to the genuine product class. The UNTP anti-counterfeiting protocol provides additional value/incentive for UNTP uptake beyond ESG integrity.

Product Serial DID

Product Serial VC

Brand Trust Root

Public Verification

Private Acquittal

Chain of Custody

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

Mass balance fraud is a particularly challenging greenwashing vector. It happens when a fraudulent actor buys a small quantity of high ESG integrity inputs (e.g., genuine carbon neutral, organic, deforestation-free cotton) and mixes that input with lower quality alternatives and then sells the full volume of manufactured product (e.g., woven cotton fabric) as sustainable product, re-using the valid credentials from the niche supply.

The UNTP solution to this problem involves trusted third parties (certifiers or industry associations) to act as *quota managers* that issue "guarantee of origin" credentials (a type of conformity credential). In this model, the guarantee of origin certificate for, say, 10 Tons of cotton fabric can only be issued when the third party has evidence of the purchase of at least 10 Tons of sustainable input materials. The third party will also mark the input batch as consumed (similar to the anti-counterfeiting protocol) so that the valid sustainable input cannot be re-presented to a different third party.

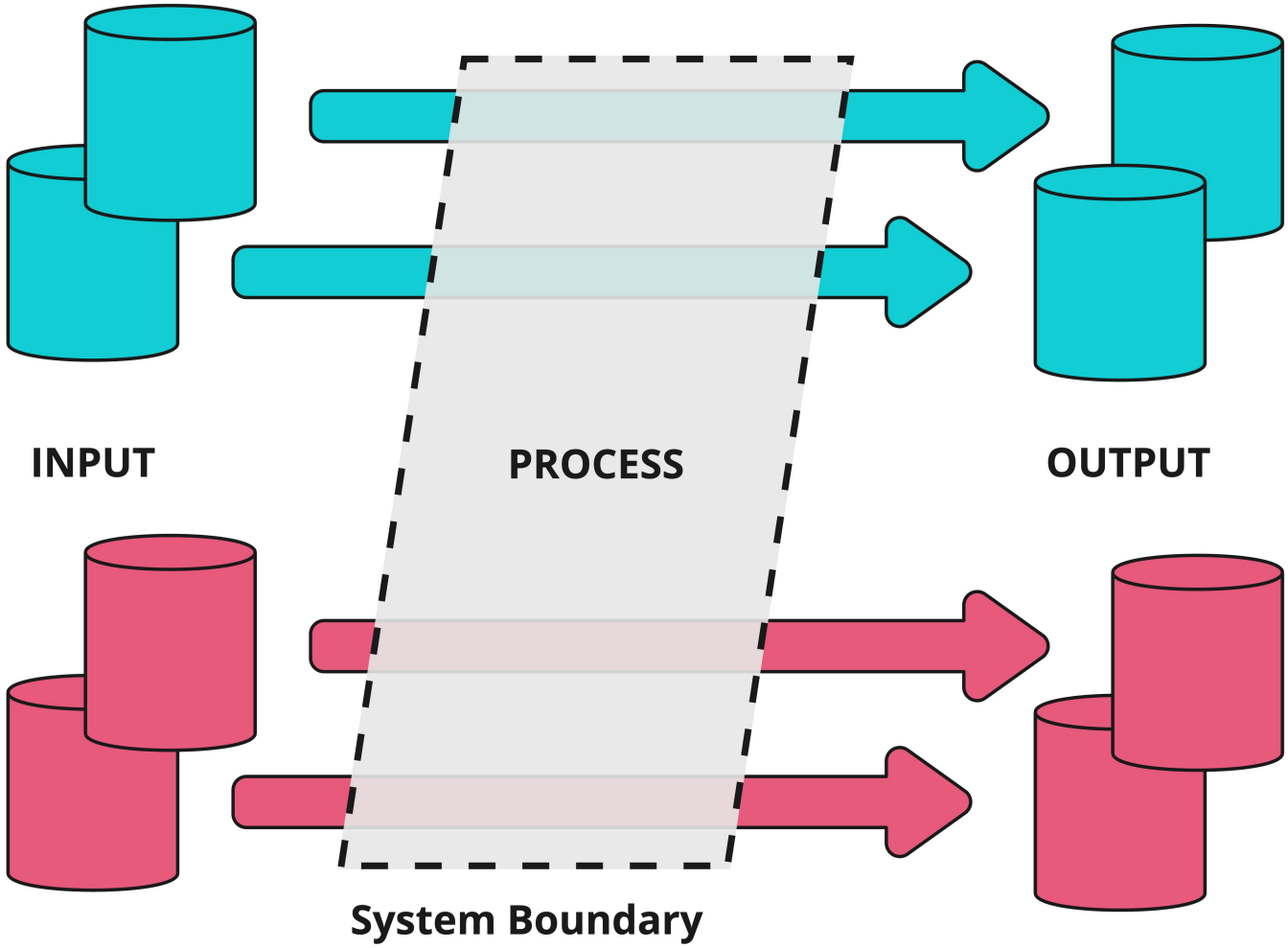
Chain of Custody Categorizations

Below are four categorizations of supply chain custody with aims of defining how sustainability claims and certified products are managed across supply chains.

Each categorization balances operational practicalities and assurance in different ways.

1. Identity Preserved (IP)

Under **Identity Preserved**, the exact certified source of the product remains unchanged and unblended throughout the supply chain. Every step, from producer to end-user, tracks and segregates the qualifying quantity so it is never mixed with non-qualifying quantities (or even other qualifying goods from a different source).



Benefits

This approach achieves maximum traceability, the strongest assurance, and a direct link back to a specific manufacturer, farm or origin. Its presence within a supply chain facilitates additional sustainability conformance requirements with minimal additional effort.

Challenges

Identity Preserved is among the most costly and complex approaches to implement, as it requires physical or instance-level identification and segregation at every stage of the supply chain.

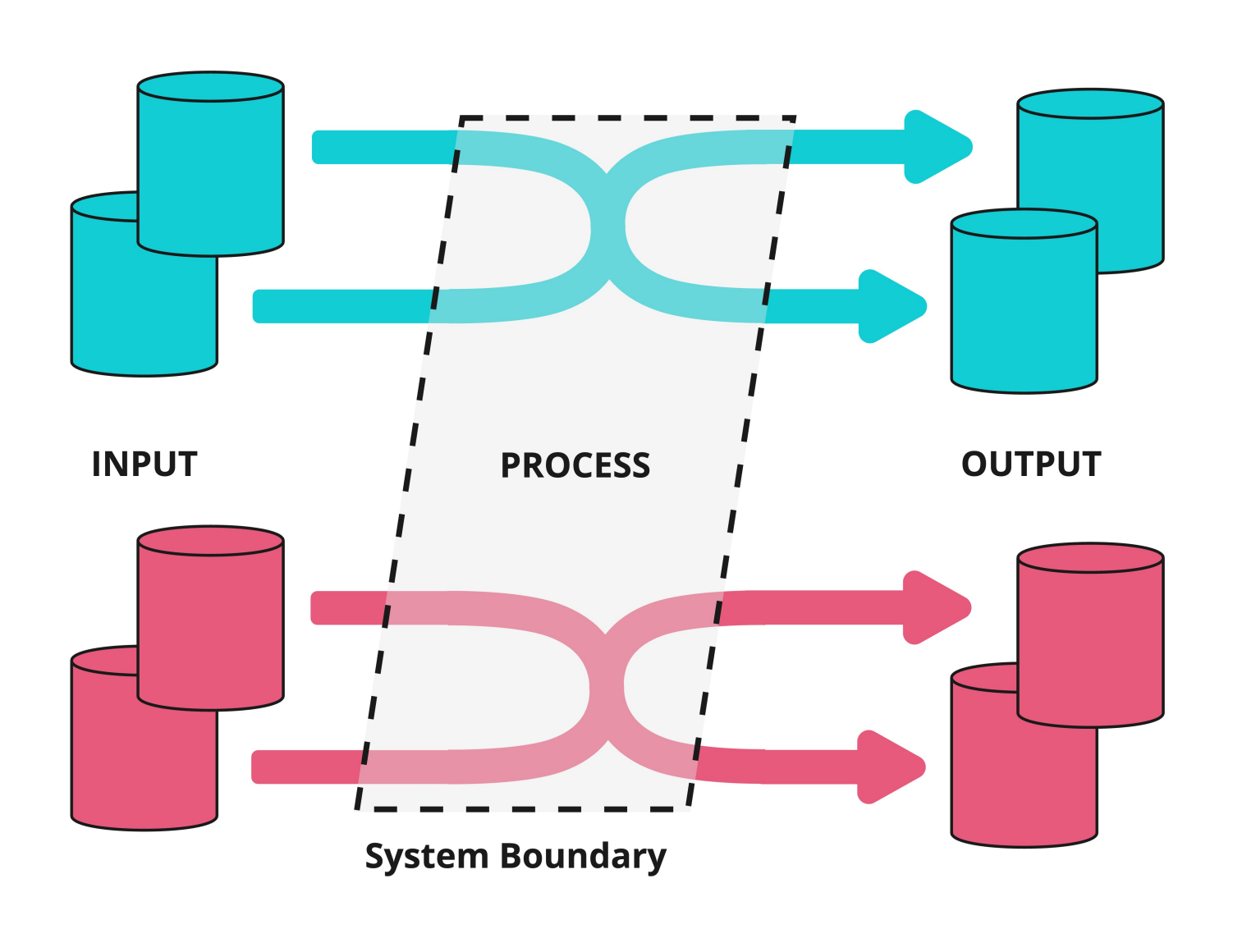
Example

A bag of coffee beans labeled "single-origin" from a specific farm, and remains separate from other coffee beans (qualifying or non-qualifying) throughout processing and transport.

Two production batches of coffee beans, from different origins, cannot be mixed. Even if both batches have identical ESG claims about them.

2. Segregated (SG)

In the **Segregated** model, qualifying quantities and non-qualifying quantities are never mixed. However, qualifying quantities from different certified sources (all meeting the same standard) may be combined. The final product is still 100% qualifying, but it is not guaranteed to come from a single farm, manufacturer, or origin.



Benefits

This scheme guarantees that the final product contains only qualifying material while allowing flexibility to pool multiple certified batches.

Challenges

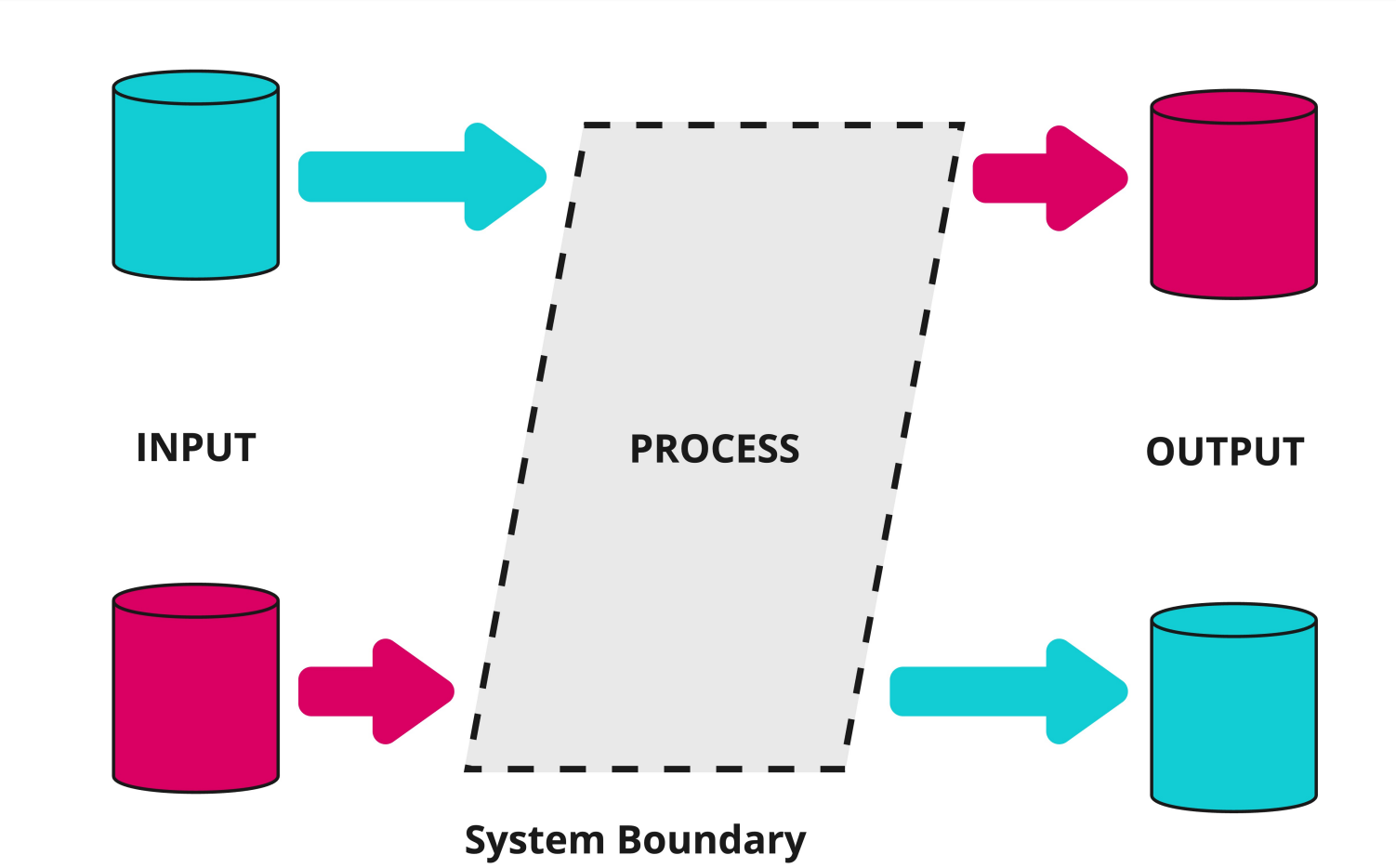
Still requires physical separation from non-qualifying quantities, which can increase logistics and storage costs.

Example

A chocolate manufacturer mixes cocoa beans from several accredited farms or origins, without adding any non-qualifying beans. The resulting cocoa batch is 100% qualifying but is not linked to a single farm, but many.

3. Mass Balance (MB)

In a **Mass Balance** system, controlled commingling of qualifying quantities and non-qualifying quantities is allowed, as long as the overall volume of qualifying outputs does not exceed the volume of qualifying inputs. Facilities and manufacturers track quantities over time to ensure that the percentage (or total amount) of "sustainable" outputs matches the actual qualifying inputs in the system.



Benefits

Mass Balance allows for the mixing of qualifying and non-qualifying goods at any stage in the supply chain. When such mixing occurs, only the equivalent quantities of qualifying goods can be sold or claimed to be "Mass Balanced" products.

This approach is well-suited for complex supply chains and provides flexibility for manufacturers to source goods sustainably, even when certain constraints exist, such as:

- Facilities unable to keep products separate during transportation or storage.
- Minimum quantities required for manufacturing or production not being fully met by qualifying quantities.
- The cost of keeping qualifying and non-qualifying materials separate leading to non-competitive pricing and hindering market development of certified materials.

Challenges

Dilution occurs at the physical level, meaning end-users and buyers cannot be certain that their specific product is made from qualifying materials—only that an equivalent volume of qualifying material was used elsewhere in the process.

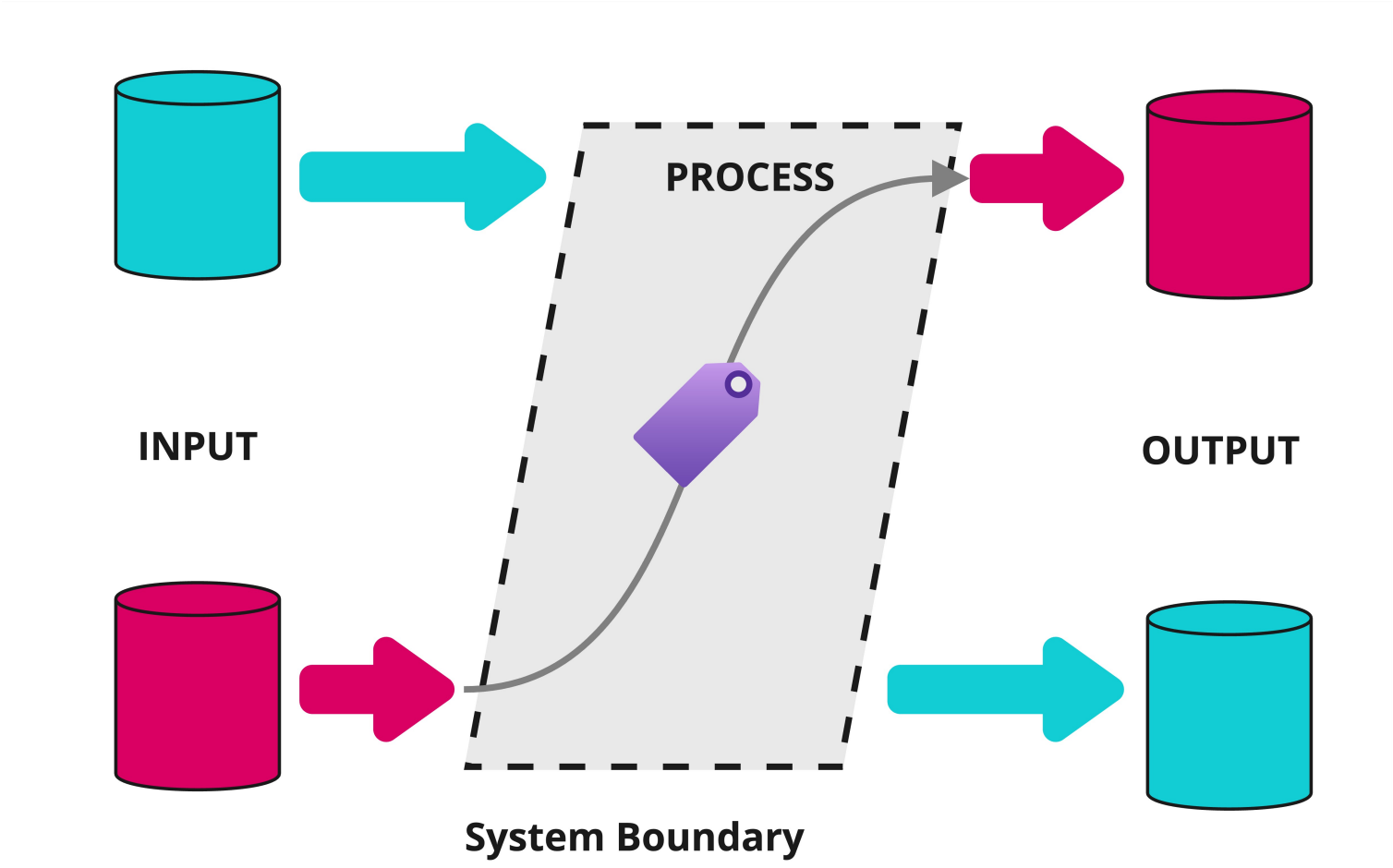
Example

A flour mill receives both certified organic wheat (40%) and conventional wheat (60%). During processing, these grains are mixed together. Under Mass Balance, the mill can sell up to 40% of its total flour output as "organic" since this matches the proportion of organic input wheat. The remaining 60% must be sold as conventional flour.

If the mill processes 100 tons of wheat in total (40 tons organic, 60 tons conventional), they can sell up to 40 tons of the resulting flour as organic, regardless of which specific flour particles came from which wheat source. This allows efficient processing while maintaining accurate sustainability claims based on input ratios.

4. Book-and-Claim (BC)

In **Book-and-Claim** models, sustainability attributes (e.g., "deforestation-free," "carbon-neutral") are fully ***decoupled entirely from the physical flow of goods***. A producer meeting the standard "books" or issues credits into a registry, and a buyer can purchase (or "claim") those credits even if the physical product they receive is not the certified batch or instance.



Benefits

Book-and-Claim simplifies sustainable sourcing in complex supply chains where full traceability across all actors is prohibitively expensive. It provides a pathway for small and medium enterprises (SMEs), smallholder farmers, and similar entities to participate in sustainability initiatives without requiring their local procurers (e.g., mills, aggregators, or intermediaries) to adopt traceability or compliance practices.

For producers:

- SMEs or smallholder farmers can "book" credits for certified production and sell their goods into local, uncertified supply chains as usual. These credits can be transacted globally, overcoming geographic limitations and enabling access to new markets and potential premium pricing.

For buyers:

- When uncertified inputs are used in the production of final goods, purchasing or "claiming" credits allows buyers to offset the environmental or social impact of those uncertified inputs.

The number of credits a producer can sell is strictly governed by the certification standard backing the credits they "book." This enables sustainable production to extend its reach even in supply chains lacking comprehensive traceability infrastructure.

Challenges

A trusted registry is essential to ensure that no double-counting or over-issuance of credits occurs, as the decoupled nature of this model requires robust governance and verification mechanisms.

Example

A palm oil producer in Indonesia receives certification that their production methods are deforestation-free. They sell their physical palm oil to local processors (who may not track sustainability credentials), but can separately sell "deforestation-free credits" to global manufacturers.

A soap manufacturer in Europe, unable to source certified deforestation-free palm oil directly, can purchase these credits to offset their use of conventional palm oil. For every ton of conventional palm oil they use, they purchase and retire one ton of deforestation-free credits. This allows them to claim their soap products support deforestation-free palm oil production, even though the physical palm oil in their products may not be from certified sources.

The credits ensure that for every ton of conventional palm oil used in Europe, an equivalent ton of certified deforestation-free palm oil was produced somewhere in the world.

Transparency and Evidence

As always, a balance between the demands for transparency (more supply chain visibility means it is easier to prove either IP, SG, MB, or BC) and confidentiality (share too much data, and risk exposing commercial secrets) is required. As always a key UNTP principle is allowing all supply chain actors to be able to choose their own balance between transparency and confidentiality.

The following address the three of the four models proposed against varying levels of transparency. "Book-and-Claim" due to it's unique nature of being decoupled from physical products is outlined separately here.

Third Party Attestations

Commercial sensitivities or purchasing requirements from the buyer are likely to introduce the need of a third party making a attestation. This protects the sellers commercial interests of procured volumes and sources, it also appeases the buyers concerns of the seller double counting, or performing fraudulent activities.

The trusted third party collects evidence to support either IP, SG, or MB chain of custody, are issues a credential to the seller attesting their compliance.

Identity Preserved (IP)

The credential issued by the third party attests that:

- Identity Preserved practices have occurred.
- The credential schema of the "original" sustainability credential for the qualifying goods.

```
{
    "category": "identityPreserved",
    "credentials": [{
        "schema": "...",
        "hashOfSource": "..."
     }]
}
```

- `schema` is a reference to the original sustainabilities credential schema, allowing the verifier/buyer to know what claims are being attested.
- `hashOfSource` is a hash of the original sustainability credential, in case of a audit.

Segregated (SG)

The credential issued by the third party attests that:

- Segregation practices have occurred.
- The credential schema of the "original" sustainability credential for the qualifying goods.

```
{
    "category": "segregated",
    "credentials": [
        {
            "schema": "...",
            "hashOfSource": "..."
        }
    ]
}
```

- `schema` is a reference to the original sustainabilities credential schema, allowing the verifier/buyer to know what claims are being attested.

- `hashOfSource` is a hash of the original sustainability credential, in case of a audit.

Mass Balance (MB)

The credential issued by the third party attests that:

- Mass balance evidence has been collected
- The credential schema of the "original" sustainability credential for the qualifying quantities
- The percentage of output quantities that can be claimed against the schema

```
{
    "method": "massBalance",
    "credentials": [
        {
            "schema": "...",
            "hashOfSource": "...",
            "startDateTime": "...",
            "endDateTime": "..."
        }
    ]
}
```

In the schema above,

- `schema` is a reference to the original sustainabilities credential schema, allowing the verifier/buyer to know what claims are being attested.
- `hashOfSource` is a hash of the original sustainability credential, in case of a audit.
- `startDateTime` and `endDateTime` are the audit period mass balance was determined over.

Discoverable Evidence

Specification will be outlined on the feasibility, and practicalities on data discoverability within a transparency graph to support different chain of custody models, without relying on a third party making an assessment.

Book-and-Claim

Due to nature of **Book-and-Claim** in that the sustainability credential is entirely decoupled from the physical goods, different challenges arise.

1. Credentials holders need a method to "book" quantities of certified goods that they eligible for.
2. Credential holders need to be able to "transfer" these credits to buyers globally.
3. Credential holders cannot "book" the same quantity multiple times, or "transfer" the same credit to multiple buyers.
4. Buyers of these credits must be able to subsequently transfer to future buyers, without the original party who created the credential knowing.

5. Holders of credits must be able to "retire" when a quantity associated with the credit is used in the manufacturing process.
    - Example, a credit represents 1kg of carbon-neutral wheat, and a miller consumes 1kg of non-qualifying wheat. The credit is retired, and the miller can claim the sustainability credential for 1kg of the flour produced.
6. Manufactures consuming credits can provide evidence to their buyers of credit ownership, and retirement in their manufacturing process.
    - Example, the miller producing the flour can show evidence to buyers that equivalent credits were purchased for it's production, and also retired.

Implementation

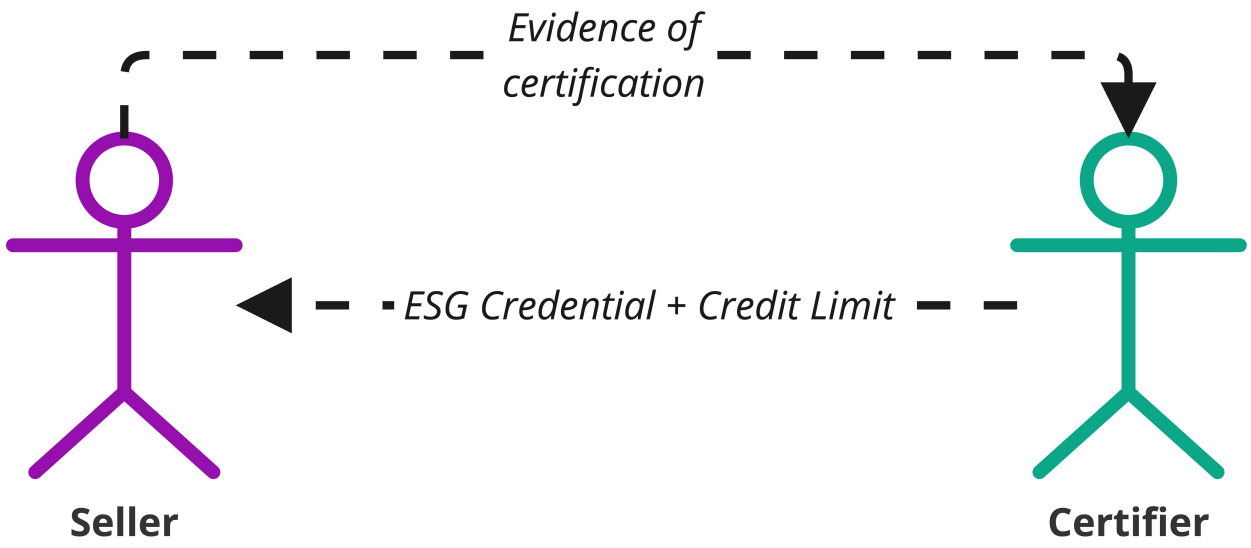
Below is a potential implementation and workflow using generic actor names - representative of any supply chain, commodity, product, or ESG credential.

Each section is appended with a rolling use case of a wheat producer receiving a carbon-neutral certification from a trust anchor, **tokenizing** that credential against a specific quantity of wheat produced, transferring ownership of that credit to a miller outside their supply chain or geographic region. And finally, the miller subsequently retiring the credit(s) after milling milled an equivalent of non-qualifying wheat and presenting evidence to buyers of their flour that appropriate credits were used.

1. Credential issuance

A certifier makes an assessment against a ESG criteria and issued sustainability credential to the seller. The credential also specifies the allowable production quantities that can be "booked" (converted into credits) under the claim.

The issuer could make the assessment of the upper limit of credits that can be booked based on volume prediction models, looking at historical averages, or comparable industry bench marks for the seller.



Example: The wheat producer provides sufficient evidence that their farming enterprise is carbon-neutral and receives a credential confirming attesting this. The certifier, using wheat production averages for the region, an understanding of the production area size of the farm, and satellite imagery assesses that a production volume of 1000t of wheat for the upcoming harvest period is feasible for this particular producer.

The wheat producer now has the ESG credential, and the ability to "book" up to 1000t of wheat produced from their farm.

2. "Booking" Credits

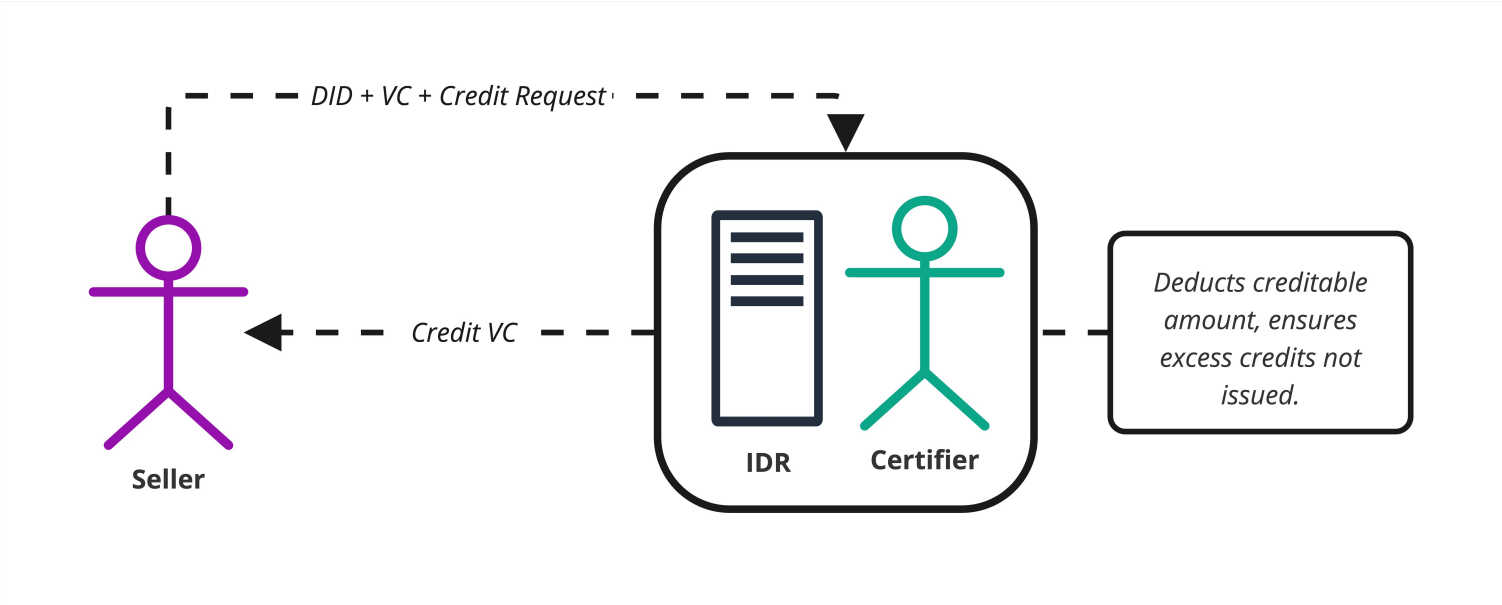
The seller performs their production/manufacturing activities, and when a quantity of product is produced, they can then tokenize the ESG credential as a credit.

The seller tokenizes credits against the certifiers register (potentially an IDR operated by, or on behalf of, the certifier). By doing so, the seller receives a credential from the certifier for the qualifying quantity.

```
{

    "credentialSubject": {
        "id": "did:example:seller",
        "quantity": {
            "quantity": 1,
            "uom": "KGM"
        },
        "schema": "https://.../schema.json",
    },
    "proof": { ... }
}
```

This VC enables the seller to present evidence of their certified claim to potential buyers. Buyers can independently verify the credential's authenticity and confirm that the credit is genuinely held by the seller via the certifiers IDR.



Example: The wheat producer has harvest 75t of wheat, and receives 75 1t carbon-neutral credits from the certifier. The wheat producer now has 75 credits to sell to a potential buyer somewhere in the world.

Potential buyers are able to verify the VC attesting the credit to ensure it is valid, not revoked, in date, and is in fact owned by the wheat producer as well as the ESG schema the token reflects.

The wheat producer is free to sell any allotment of these 75 credits to any number of buyers.

3. Transferring (selling) credits

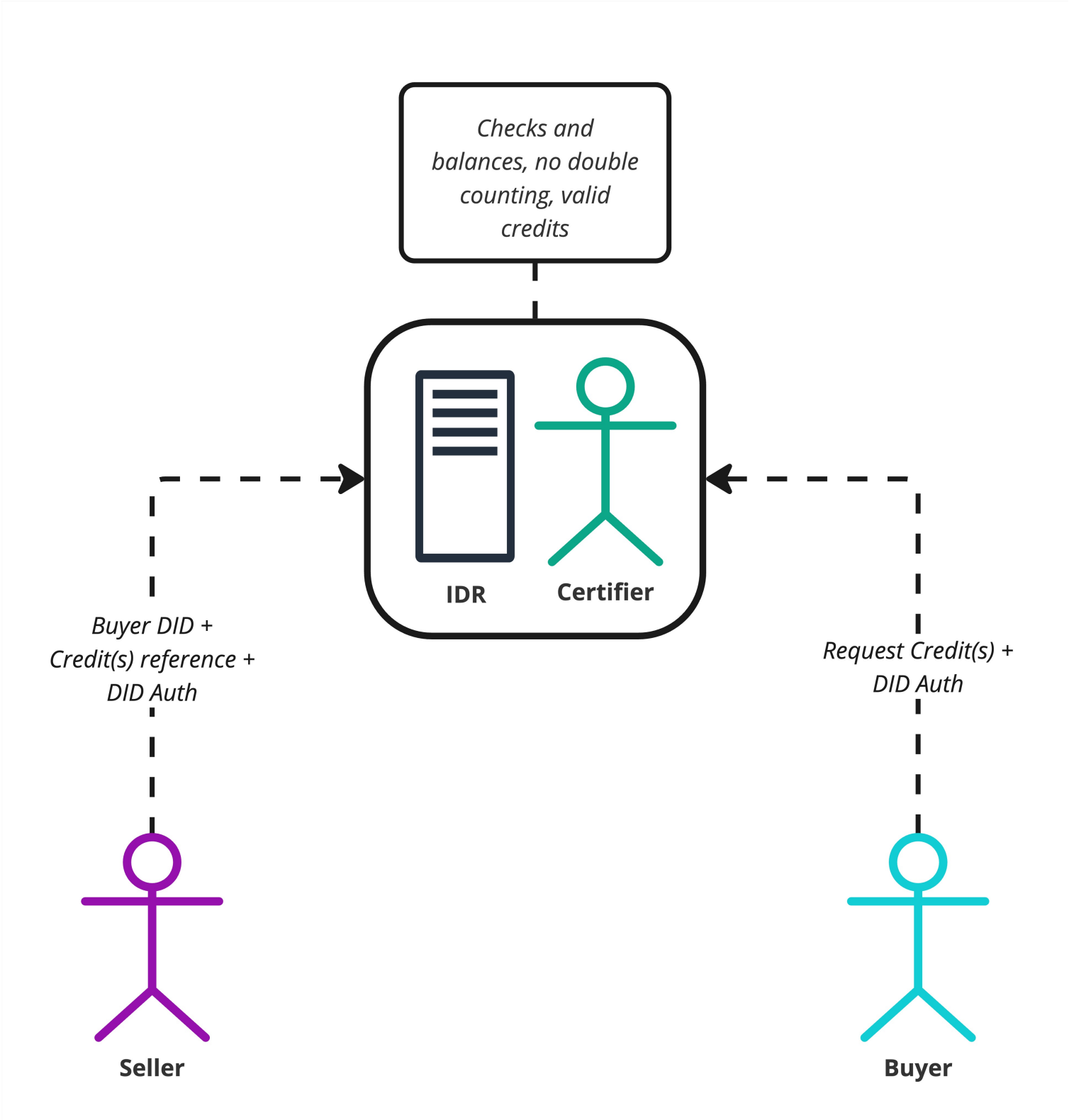
The seller wishes to sell the credit to a buyer in a different geographic region.

To initiate the transfer:

1. The seller submits a transfer request to the certifier register operator (e.g., the IDR system), providing:
    i. The buyer's DID.
    ii. A reference to the specific credit(s) being transferred.
    iii. A digital signature generated using the sellers private key.
2. The register operator verifies the transfer request by:
    i. Authenticating the seller and buyer DIDs.
    ii. Confirming the validity of the credit(s) referenced in the request.
3. Upon approval:
    i. Ownership of the credit is transferred to the buyer.
    ii. The original credential held by the seller is revoked.
    iii. The buyer receives a new credential representing the transferred credit.

The buyer can receive this credential for the credit purchased by making a request using did authentication.

The register operator is able to ensure no double counting is occurring, and any other verification requirements for their industry.



Example: The wheat producer and a miller have come in agreement to transfer 10 1t credits of carbon-neutral wheat. The wheat producer initiates the transfer with the certifier by providing information about the buyer, and the 10 credits to be transferred.

The register operator for the carbon-neutral credits can verify the credits are legitimate, no double counting is occurring, the credits are not in escrow in another concurrent transaction, and any other industry requirements pertaining to carbon-neutral wheat credits.

The buyer can then request the register operator for these 10 credits, and the register operator can issue a new set of 10 credits to the buyer, and revoke the previous 10 held by the seller.

The buyer is then free to then transfer these 10 credits, or provide as evidence, to other actors in the supply chain, without the *original* seller knowing.

4. Retiring credits

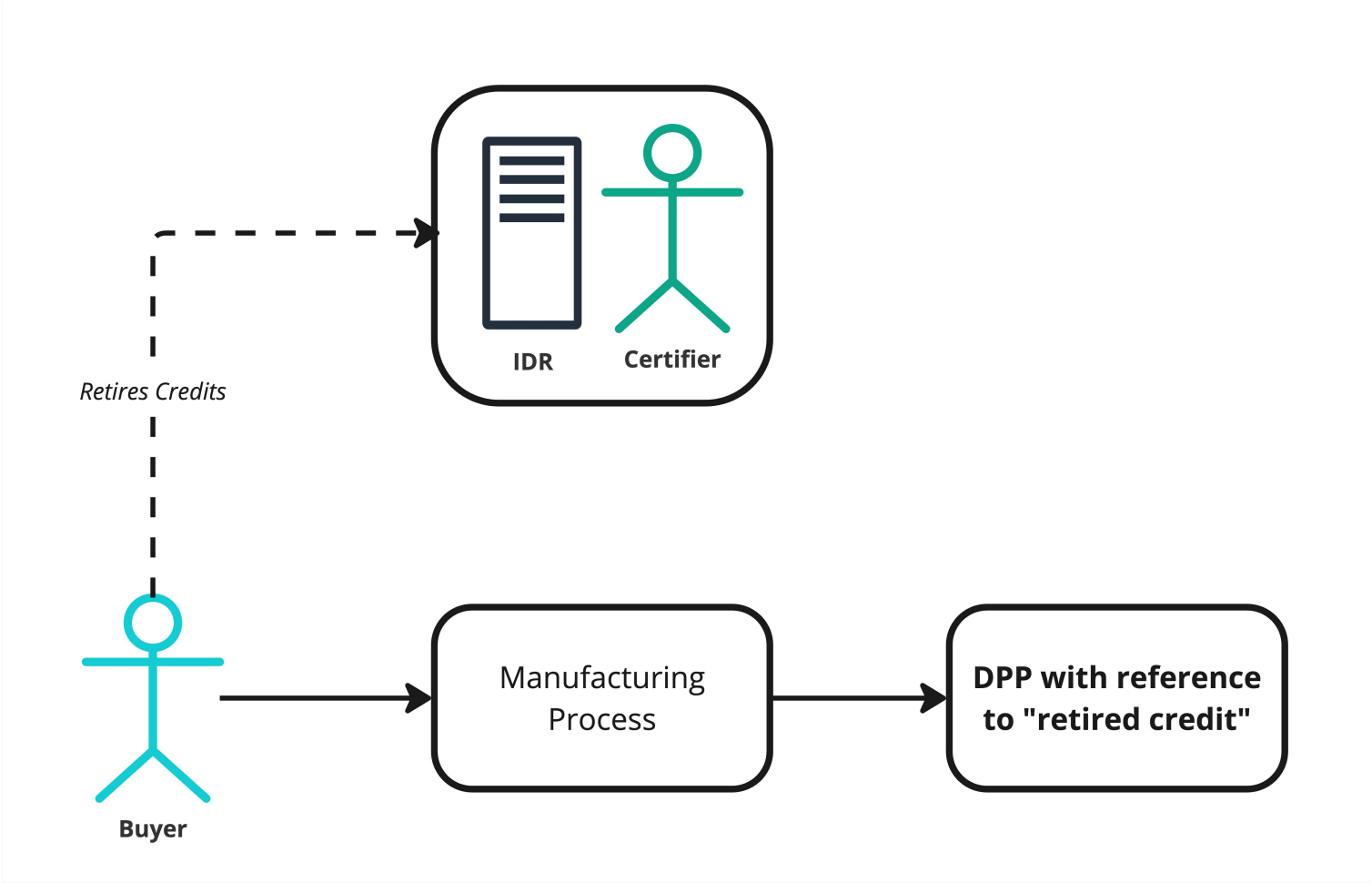
Once the buyer performs a manufacturing process and uses non-qualifying quantities of the product their process. They retire the equivalent quantities of credit to ensure its sustainability attributes are appropriately accounted for.

Steps to retire the credit:

1. The buyer submits a retirement request to the certifier register, authenticated using their DID. The request references the specific credit(s) being retired.
2. The certifier register processes the request, marking the credit as retired and preventing it from being reused or double-counted, or transferred in the future.
3. The buyer receives evidence of retirement, potentially in the form of another Verifiable Credential that references the original credit - forming a link of evidence of retirement, evidence of credit purchase, and reference to the underling ESG schema from the credential from the original seller.

This retirement evidence can then be linked to the Digital Product Passport (DPP) for the manufactured products, enabling downstream buyers to verify:

- The schema associated with the original credit.
- The identity of the certifier who issued the initial credential to the seller.
- The integrity of the credit lifecycle, including its transfer and retirement, validated by the certifier registor operator to prevent double counting.



Example: The miller has purchase 10 1t carbon-neutral wheat credits from the farmer. The miller mills 10t of non-qualifying wheat as they have no practical and physical access to certified carbon-neutral wheat. The miller, however, wants to claim 10t of output flour as carbon-neutral.

The miller retires the 10 credits with the certifier register operator, and receives evidence of credit retirement. The miller, in a Digital Product Passport for the flour, can reference this evidence as proof to buyers.

The buyer of the flour can be confident that 10t of production of carbon-neutral wheat occurred somewhere globally, under a framework that they trust as per the credential schema, and that this 10t has not been double counted elsewhere in the supply chain.

Outcomes

- Producers are incentivized to receive ESG credentials, even if their local supply chain does not demand it.
- Producers are able to sell these credits to buyers globally, and receive a premium for their sustainable practices.
- The Book-and-Claim model is not dependent on a single technology choice, or platform.
- The certifier register operator can ensure credit quotas are not exceeded, double counting did not occur, and proper transfer of credits.
- Manufacturers are able to retire purchased credits, and provide evidence their buyers that credits have been purchased against the ESG schema of interest.

ESG Rules

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

Yet another greenwashing attack vector is to deliberately apply incorrect rules to the determination of criteria such as emissions intensity. The verification question in this case is "yes, but how do I know you calculated it right?". The UNTP proposes an independent calculator service offered either by the standards body or regulator that defined the rules or by an accredited service provider. The Supply chain actor presents raw data to the calculator which returns with a signed credential confirming that the rules were correctly applied. This protocol has an additional benefit for legitimate actors if widely adopted by rules authorities - which is to significantly simplify the assessment of compliance against multiple different rules. By separating observed facts from the assessment of those facts against specific rules then it becomes relatively simple to test compliance against multiple standards and regulations.

Implementation Guidance

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Implementation Of UNTP

Implementation of UNTP will be a very different experience for organisations of different size, industry/geography sector, and stakeholder type. The purpose of this page is to help potential implementers navigate quickly and simply to the relevant scope of work.

Has Five Simple Steps

At a macro-level, there are just five steps for any UNTP implementer to follow.

Step	Action	Outcome
1	Review the business case section to confirm that UNTP implementation is likely to deliver value for your organisation. Establish key performance measures to track costs and benefits.	Positive business case
2	Review the UNTP and/or UNTP extensions pages relevant to your organisation type and to determine which credentials you should be issuing. Register your (non-binding) intent to implement so that you gain access to community support.	Implementation intent registered
3	Choose a software product or request your existing software system provider to implement UNTP. Test your implementation using the UNTP test service. Use support channels as needed.	Update implementation register with positive test results
4	Run a pilot with any other registered implementer(s) that has completed testing to confirm interoperability and value. Contact support to facilitate coordination of pilot activities	Successful pilot
5	Ramp up to full production volumes, routinely issuing and verifying UNTP credentials. Measure cost and benefit performance indicators to track ongoing value	Consider publishing your story as an UNTP case study

Details Vary With Your Context

Organisation Size

- **Small businesses** (under 20 employees) are likely to find themselves using UNTP simply because their commercial off the shelf (COTS) business software system has implemented UNTP to support transparent digitalised supply chains. Just as small businesses make international payments without knowing anything about ISO-20022, so they would issue and verify digital product passports without knowing about UNTP.
- **Medium businesses** (20 to 200 employees) will also be using commercial off the shelf software but are likely to have developed some customized solutions and internal integrations that mean UNTP implementation is not simply a case of just using compliant software. Some implementation and testing costs will be incurred.
- **Large enterprise** (over 200 employees) will usually have a complex ICT landscape with multiple systems and will usually need to engage their ICT department for a UNTP implementation.

Organisation Type

Stakeholder	Implementation Scope
Producers, Manufacturers, and Brands - produce raw materials, manufacture goods, own brands.	**Implement UNTP Extensions** *Issue Product Passports, Facility Records, and Traceability Events according to guidelines specified in industry extensions so that your customers can easily verify your compliance and meet their due diligence obligations*
Registry Operators - Maintain authoritative registers of products, assets, facilities, and businesses.	**Implement UNTP Core** *Implement Identity Resolver and Identity Anchor so that your registered members can prove their identity and link discoverable credentials such as Product Passports, Facility Records to their product or facility identifiers.*
Conformity Assessment Bodies - Provide test and certification services to certify compliance with recognised schemes and regulations	**Implement UNTP Extensions** *Issue Digital Conformity Credentials according to extensions defined by the relevant Scheme owners or Regulators*
Member Associations - Represent and advocate for industry interests	**Create UNTP Extensions** *Activate communities to participate in transparent and traceable value chains by governing the design and maintenance of UNTP industry extensions.*
Regulators - Enforce compliance with laws and regulations.	**Implement UNTP Core** *Issue regulatory permits, licenses, and certificates as Digital Conformity Credentials so that exporters can prove their compliance to customers and other authorities. Also automate border compliance and risk assessments by verifying Product Passports, Conformity Credentials and Identity Anchors that accompany imports*

Stakeholder	Implementation Scope
Software Vendors - Develop software solutions that underpin business operations and facilitate participation in transparent value chains.	**Implement UNTP Core** *Add support for Verifiable Credentials and Decentralised Access Control to software products and, depending on your target market, the ability to issue all UNTP credential types (DPP, DFR, DCC, DTE, DIA) including relevant industry specific extensions.*
Scheme Owners - Develop sustainability standards and associated assessment criteria	**Create Sustainability Vocabularies** *Describe your existing schemes and criteria as a digital Sustainability Vocabulary Catalog so that your conformity criteria can be referenced by issuers of claims in Product Passports and assessments in Conformity Credentials.
Consumers - Choose, purchase and use products.	**Verify Sustainability Claims** *Scan data carriers, view digital product passports, make purchase decisions*

Industry and Geographic Sector

UNTP has been designed as an industry and geography agnostic standard - with a framework for multiple industry and/or geography specific extensions. This raises the question for implementers - whether to implement support for UNTP core or for specific industry extensions. The answer depends on your role.

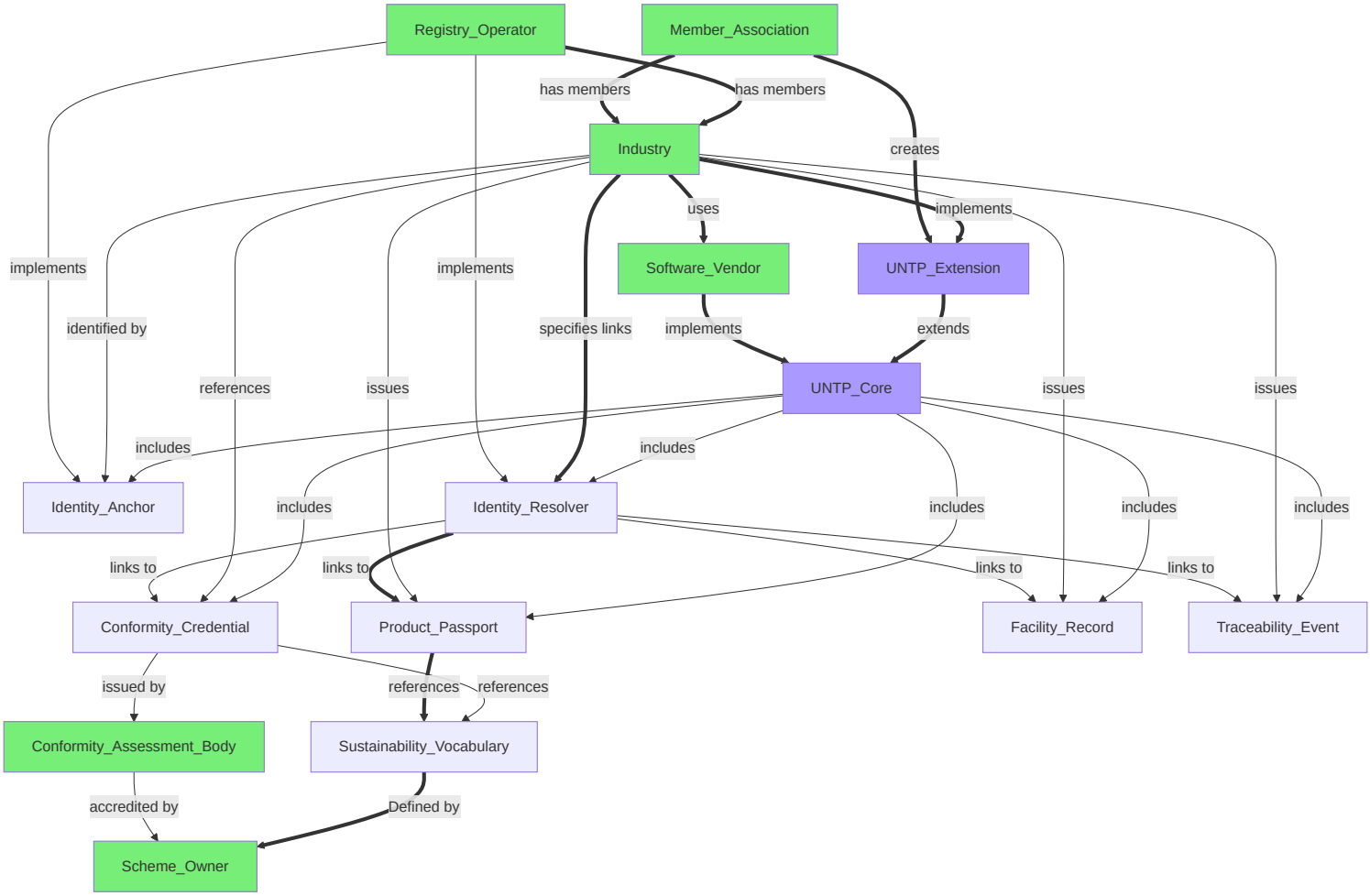
- UNTP Core specifications are targeted at Software Vendors, Registry Operators, Regulators and Scheme Owners.
- UNTP industry extensions are created by Industry Associations and implemented by Producers, Manufacturers, and Brands that are members of the association using UNTP compliant software.

And Some Key Dependencies

Whilst any individual industry actor can choose to implement UNTP in isolation, there are some important economies of scale that make implementation at scale far more feasible. The dependency map below shows UNTP specification elements in purple and stakeholder type in green with dependencies between them described by the arrows. The most important dependencies are highlighted in bold:

- A **UNTP Extension** adds industry specific needs to the generic **UNTP Core** specification and is best coordinated by a **Member Association** that creates the extension once for use by all members.
- A **Software Vendor** such as a production management system implements UNTP within their software package once and it becomes available for use by all their **Industry** customers.
- A **Registry Operator** implements the UNTP **Identity Resolver** and **Identity Anchor** specification so that every identifier (of a product or facility) issued to any of their **Industry** members can be used as a pointer to the **Product Passport**
- A **Scheme Owner** specifies their rules as a **Sustainability Vocabulary** so that claims in **Product Passports** and assessments in **Conformity Credentials** can unambiguously reference the sustainability criteria.

The focal point for coordinating the participation of Industry, Software Vendors, Registry Operators and Scheme Owners is the Member Association that creates a UNTP Extension



Implementation Plans

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

This page provides some template UNTP implementation plans for each stakeholder type.

For Producers Manufacturers and Brands

For Registry Operators

For Conformity Assessment Bodies

For Member Associations

For Regulators

For Software Vendors

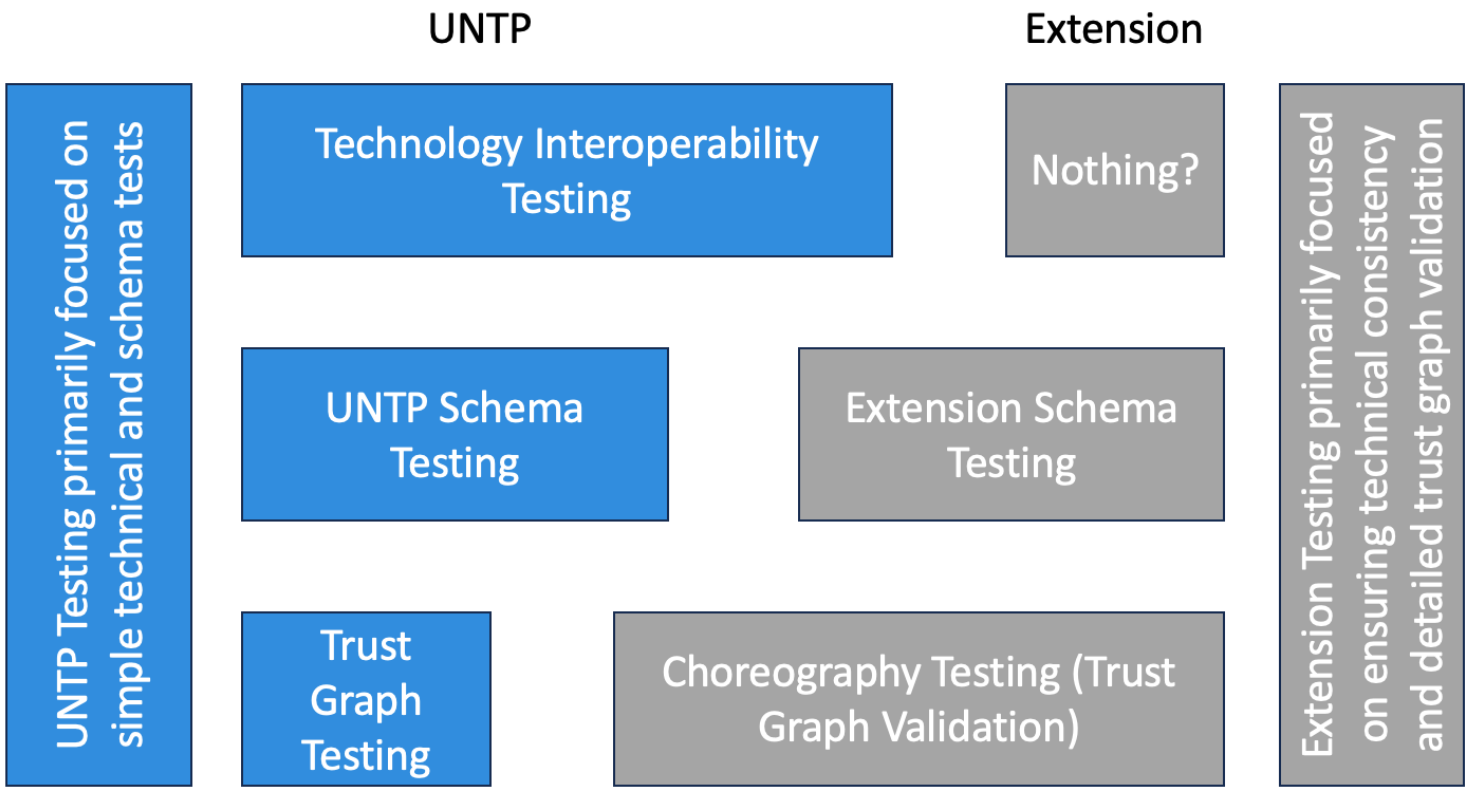
For Scheme Owners

For Consumers

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

3 Tier Test Architecture

There is a 3 tier testing architecture to help implementors ensure that they are issuing UNTP interoperable digital product passports. This architecture also ensures that as implementors 'extend' the UN Transparecy Protocol they do that in a non-breaking fashion.



At each tier we articulate the specific testing for UNTP and for an extension.

UNTP Testing (the blue sections in the diagram)

The UNTP testing is intended to provide implenentors the ability to validate that they have a complete valid reference implementation of UNTP. This testing gives a starting point so that implenters know that their implemenation is starting as UNTP compliant and that any externsions that they make need to have validations added to ensure continued UNTP interoperability.

Tier 1: UNTP Test: Technology Interoperability Testing

This testing is intended to provide implementers confidence that the technical implementation is correct. It is primarily focused on W3C verifiable credential compliance.

Tier 2: UNTP Test: UNTP Schema Testing

This tests that the schema that are being used to issue credentials are a valid UNTP schema. This will enable an implementor to validate that they are starting with a valid UNTP set of schema.

Tier 3: UNTP Test: Trust Graph Testing

This validates that the links between the different components of the UNTP schema (DPP, DTE, DCC) are validated. It is anticipated that this is relatively simple at generic UNTP level, but will get more involved for each extension.

Extension Testing (grey boxes)

UNTP has been designed so that each industry and jurisdicton can extend UNTP to meet their specific busines, governance and community needs. In order to ensure that supply chain customers downstream can consume details from their upstream supply chain partners - it is important that extensions maintain UNTP compliance. Extension testing is intended to provide that confidence to implementors.

Tier 1: Extension Test: Nothing?

It is expected that there won't be changes at Tier 1 of the testing architecture for extensions. This is because we are using W3C standards and if there are requirements for extenisons it is beyond the scope of UNTP to manage. We are including it in the architecture to faciliate future unforeseen needs.

Tier 2: Extension Test: Extension Schema Testing

This testing is designed to ensure that as implementors are extending UNTP schema (DPP, DTE, DCC) to meet their specific needs that they are not breaking compatibility with UNTP and that they are able to provide the implementors of their extensions with confidence that their extension is correct.

Tier 3: Extension Test: Choreography Testing (Trust Graph Validation)

This provides the ability for extendors to map the different credentials together to validate specific industry or regional scenarios. In Australia NATA is the national accrecditor for laboratories - so the link from NATA to an accredited laboratory to a specific accreditation would be validated by a test in this component.

INFO

Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Implementation Support

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Reference Implementation

The following tools make up a reference implementation.

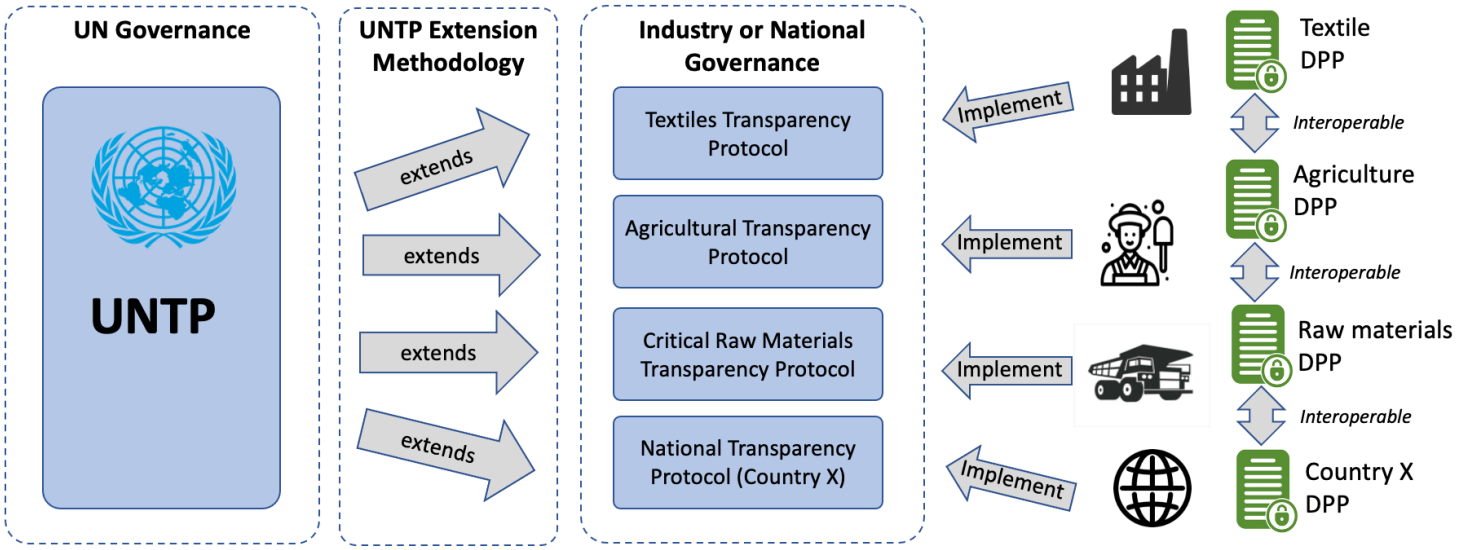
Tool	Link	Description	Status
Project VC Kit	https://github.com/uncefact/project-vckit	This is a tool that verifies and issues credentials.	Active Development
Mock Apps	https://github.com/uncefact/tests-untp/tree/next/packages/mock-app	Tool to build testable supply chain implementations to enable testing and validation of your DPPs and supply chain	Active Development
Identity Resolver	https://github.com/uncefact/project-identity-resolver	Tool that enables to go from the identifier to more information about the identified object including a DPP	Not yet release (expected Sept 2024)
UNTP Test Suite	https://github.com/uncefact/tests-untp/tree/next/packages/untp-test-suite	Provides tooling for implementers to validate their DPP's across the 3 tiers (correct credential, correct schema, and correct choreography)	Active Development

Extensions Register

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Extensions Methodology

UNTP is designed as a common core that is usable by any industry sector or in any regulatory jurisdiction. This extensions methodology describes how to extend UNTP to meet the specific needs of any industry sector or regulated market in such a way that the extension maintains core interoperability with any other extension. This cross-industry and cross-border interoperability is a core value of UNTP because almost every value chain will cross industry and/or national borders.



Anyone can take UNTP and extend it for any purpose. But for the extension to be registered as UNTP conformant, an extension MUST remain interoperable with UNTP. This is achieved by following the governance, methodology, and testing processes described on the Extensions Methodology Page

Extensions Register

The UNTP project maitnains a list of registered industry and/or geography specific extensions.

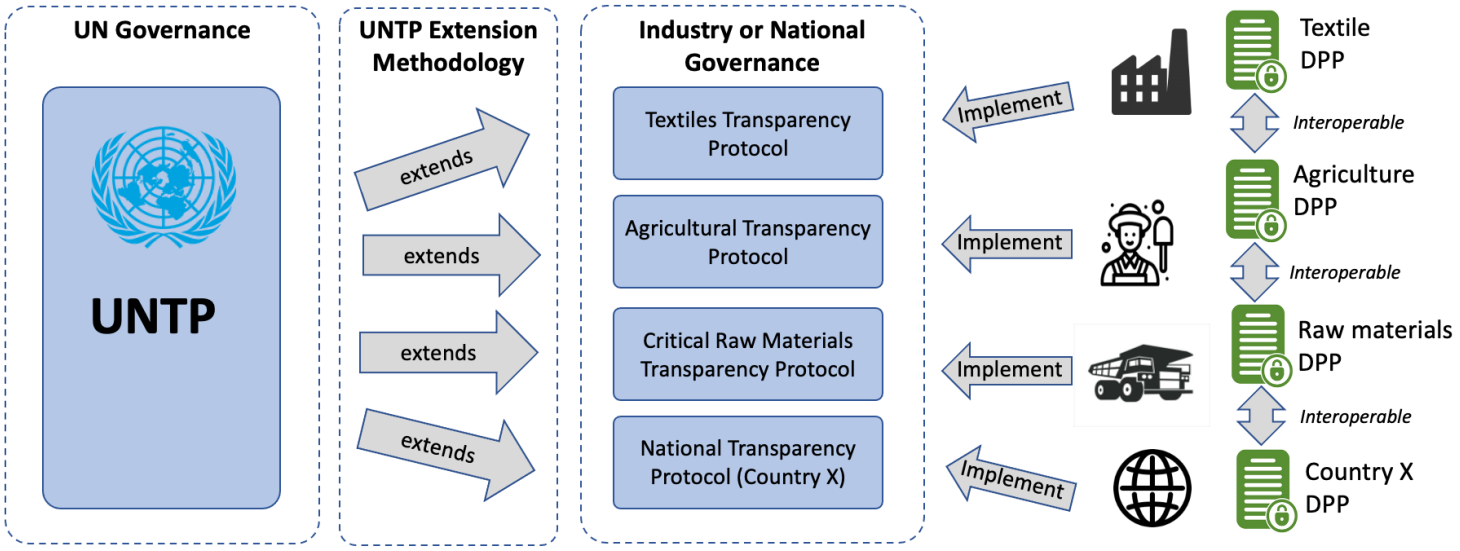
In some cases, UNTP extensions are themselves UN projects - such as the extensions defined by the UN critical raw materials traceability and transparency project. In most cases however, industry sectors and/or national projects will govern their own extensions.

Extensions Methodology

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Overview

UNTP is designed as a common core that is usable by any industry sector or in any regulatory jurisdiction. This extensions methodology describes how to extend UNTP to meet the specific needs of any industry sector or regulated market in such a way that the extension maintains core interoperability with any other extension. This cross-industry and cross-border interoperability is a core value of UNTP because almost every value chain will cross industry and/or national borders.



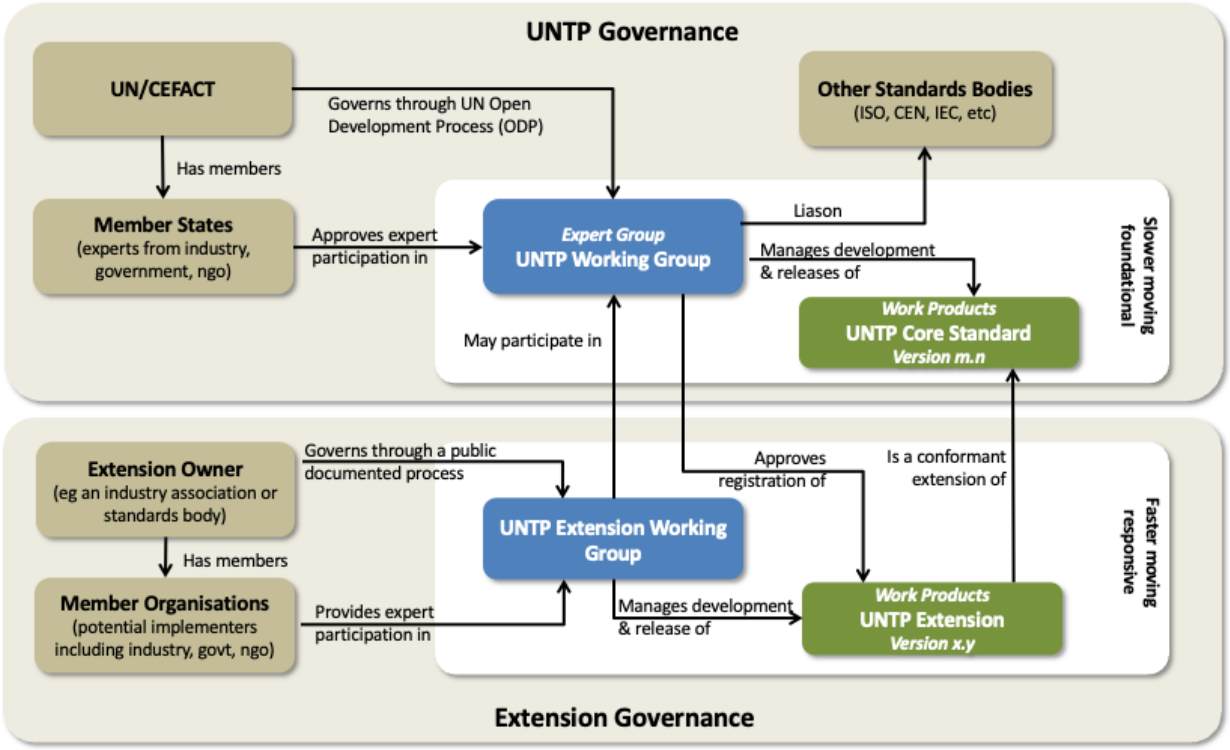
In some cases, UNTP extensions are themselves UN projects - such as the extensions defined by the UN critical raw materials traceability and transparency project. In most cases however, industry sectors and/or national projects will govern their own extensions.

Anyone can take UNTP and extend it for any purpose. But for the extension to be registered as UNTP conformant, an extension MUST remain interoperable with UNTP. This is achieved by following the governance, methodology, and testing processes described below.

Extension Governance

As shown in the diagram below, UNTP development follows the UN/CEFACT Open Development Process (ODP) and is maintained by a group of experts that are approved by their member state delegate. UNTP Intellectual Property is owned by

the UN and the standard is available free for anyone to use. There are formal liaisons with other standards bodies including ISO so that UNTP remains aligned with similar initiatives.



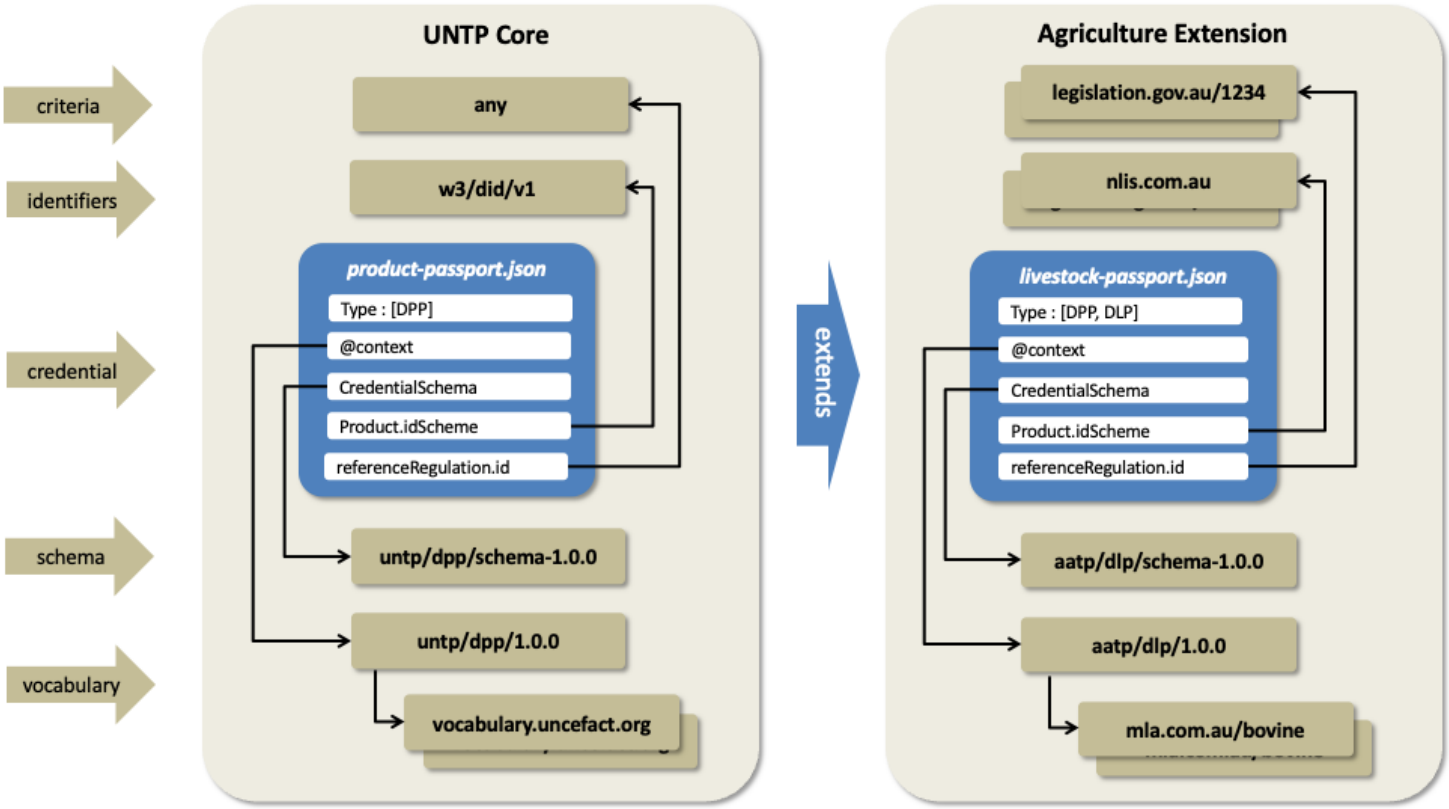
Registered UNTP extensions

- MUST follow an open and transparent development process that is open to participation from representative persons and organisations.
- MUST be freely available under a permissive or creative commons license.
- MUST be version managed (major.minor) and each extension version MUST state which UNTP major version from which it is derived.
- MUST be documented as a public website with reference-able URI for each specification component.

Since registered extensions have a clear vested interest in the ongoing development of UNTP, extension working groups SHOULD nominate at least one member as a participant in the UNTP working group.

Extension Methodology

UNTP extensions must be interoperable with UNTP core. This means that a credential that conforms to a UNTP extension is also conformant with UNTP core. This requirement ensures that credentials issued in a specific industry or geographical context are still understandable across industry or geographic boundaries.



Schema Extensions

UNTP credential JSON schema allow additional properties in most objects to provide flexibility to accommodate industry extensions.

- UNTP extensions MAY define any number of variants to UNTP schema. For example an agriculture extension my define both a livestock passport and a horticulture passport as extensions of the UNTP digital product passport.
- UNTP extension schema MUST NOT redefine any properties in UNTP schema.
- UNTP extension instances MUST validate against both the extension schema and the corresponding UNTP core schema.

Vocabulary Extensions

Industry extensions will often leverage existing industry specific vocabularies. For example an agriculture extension may reference terms from Codex Alimentarius. This is achieved through JSON-LD @context files.

- Each credential defined by a UNTP extension MUST reference a JSON-LD @context file that defines all additional terms.
- JSON-LD @context files defined by a UNTP extension MUST NOT redefine terms in the corresponding UNTP @context file.
- External vocabularies referenced by UNTP extensions SHOULD be stable, version managed, and should not delete terms.

Identifier Schemes

UNTP and it's extensions have a dependency on resolvable and verifiable identifiers. Industry extension will typically define specific identifier schemes (for products, facilities, and organisations) that are relevant for the specific industry and/or geography. For example, Australian livestock are identified by a National Livestock Identifier that is carried as an RFID tag in the animal's ear.

- All identifier schemes used by registered UNTP extensions MUST be registered in the UNTP identifier scheme register.
- Identifiers used by UNTP extensions SHOULD be resolvable and verifiable as defined by the UNTP Identity Resolver specification.

Conformity Criteria

UNTP is deliberately agnostic of specific standards and regulations. The generic `Declaration` object that is used by DPP, DFR, and DCC credentials is designed to support any conformity criteria defined by any standard or regulation. UNTP extensions, however, will normally agree a specific set of standards and regulations that are applicable in the extension context.

- UNTP extensions MUST list all relevant standards and regulations on the extension specification website.
- The specific conformity criteria within Standards and Regulations referenced by UNTP extensions SHOULD be reference-able as stable URIs.

Extension Conformity Testing

TBC

Extensions Register

> **INFO**
>
> Please note that this content is under development and is not ready for implementation. This status message will be updated as content development progresses.

Extensions Register

Summary list of registered UNTP Extensions

Extension Name	Extension Owner	Geographic Scope	Industry Scope	Status
Responsible Business Transparency Protocol (RBTP)	Responsible Business Alliance	Global	Electrical, electronic & automotive parts	new
Universal Data Protocol (UDP) for the Global Built Environment	Standards Australia and the International Code Council	Global	Construction	new
Australian Agriculture Traceability Protocol (AATP)	Food Agility CRC	Australia	Agriculture	draft
UN Critical Raw Materials Transparency Protocol (CRMTP)	UN/CEFACT	Global	Critical minerals mining & processing	draft

Extension Details

Responsible Business Transparency Protocol

- Extension Launched: Nov-2024
- Release Date: TBA
- Industry: Electrical, electronic & automotive
- Geography: Global

Logo	Implementation Statement
	The Responsible Business Alliance (RBA) is a coalition of companies driving sustainable value for workers, the environment and business throughout the global supply chain. Our members, suppliers and stakeholders collaborate to improve working and environmental conditions and business performance through leading standards and practices. Transparency and traceability in value chains is key to building confidence and value of sustainable business practices. Accordingly, the RBA is pleased to build upon the foundational capabilities provided by the UN Transparency Protocol (UNTP) to deliver a suite of interoperability standards for the electrical and electronic goods and automotive parts industries.

Credential Extensions

Credential	Description	Extension of
Responsible Minerals Initiative Credential (RMIC)	A conformity credential attesting to the responsible sourcing of minerals in supply chains.	Digital Conformity Credential
Responsible Labour Initiative Credential (RLIC)	A conformity credential attesting that the rights of workers vulnerable to forced labor in global supply chains are consistently respected and promoted.	Digital Conformity Credential
Responsible Environment Initiative Credential (REIC)	A conformity credential attesting to the performance of a facility in the areas of Decarbonization, Chemical Management, Water Stewardship, and Circular Materials	Digital Conformity Credential
Responsible Factory Initiative Credential (RFIC)	A conformity credential attesting that a supplier facility meets the RBA Code of practice.	Digital Conformity Credential
Electrical Goods Passport (EGP)	A digital product passport tailored to the needs of electrical and electronic products and their conformity to Environmental, Social, and Governance standards.	Digital Product Passport
Digital Battery Passport (DBP)	A digital product passport that is designed to meet the needs of RBA members whilst also offering compliance with emerging EU standards.	Digital Product Passport
Electrical Facility Record (EFR)	A digital facility record tailored to the needs of manufacturing facilities in the electrical and electronic industry sectors and their sustainability performance.	Digital Facility Record

Universal Data Protocol for the Global Built Environment

- Extension Launched: Nov-2024
- Release Date: TBA
- Industry: Built Environment (construction)
- Geography: Global

Logo	Implementation Statement
	The Universal Data Protocol (UDP) is an extension of the UNTP and is seeking to leverage its decentralised framework to provide transparent, trustworthy, and verifiable data in the global built environment. The UDP is an open protocol that will allow for the efficient exchange of verifiable data, enhancing reporting and compliance across jurisdictions and life cycle stages. This project seeks to improve the interoperability of data across the built environment, aiming to make reporting more cost effective, accurate and efficient for all stakeholders.

Credential Extensions

Credential	Description	Extension of
Built Environment Vocabulary	Catalog of sustainability criteria for the built environment	SVC

Australian Agriculture Traceability Protocol

- Extension Launched: Feb-2024
- Website : https://aatp.foodagility.com/
- Release Date: TBA
- Industry: Agriculture
- Geography: Australia

Logo	Implementation Statement
	The AATP is an adaptation of the UN Transparency Protocol and is designed to help Australian producers meet emerging environmental, social, and governance (ESG) regulatory and consumer requirements. Operating as a governance framework, the AATP facilitates the interaction between multiple certifiers, farm systems, and enterprise systems. Interoperability and traceability tools help the Australian agriculture sector attain higher quality information about the value of Australian-made products.

Credential Extensions

Credential	Description	Extension of
Digital Livestock Passport	Quality and sustainability characteristics of cattle including bovine characteristics and veterinary treatment history	DPP
Deforestation Credential	A farm-level attestation of conformity to EU Deforestation Regulation	DCC

Critical Raw Materials Transparency Protocol

- Extension Launched: Jan-2024
- Release Date: TBA
- Industry: Critical Minerals Mining & Processing
- Geography: Global

Logo	Implementation Statement
UNECE	In line with the United Nations (UN) Sustainable Development Goals (SDGs) and building on the success of the UNECE Textile & Leather traceability project, this project seeks to empower the Critical Raw Material (CRM) industry with practical, low cost tools for digital data exchange to achieve product differentiation, maximize the value of existing permitting and ESG compliance efforts, counter green-washing, and support a more sustainable global economy. This project supports the UN focus on extractive industries and leverages the UN Center for Trade Facilitation and Electronic Business' (UN/CEFACT) role and capabilities to deliver digital standards for sustainable supply chains.

Credential Extensions

Credential	Description	Extension of
Copper Passport	Quality & sustainability characteristics of copper concentrate	DPP
TSM Credential	Towards Sustainable Mining Mine-site sustainability performance credential	DCC