UN Transparency Protocol

Table of contents:

- Business Case
- The Business Case for Change
  - Business Case Template (BCT).
  - Community Activation Program (CAP).
  - Value Assessment Framework (VAF).
- Business Case temaplates
  - For Buyers and Suppliers in the Value Chain
  - For Conformity Assesment Bodies
  - For Industry Associations
  - For Regulators
  - For Software Vendors
- Community Activation Program
- Community Activation
- Value Assessment Framework
- Ongoing Value Asessment
- 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

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.

Presentations & Videos

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

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

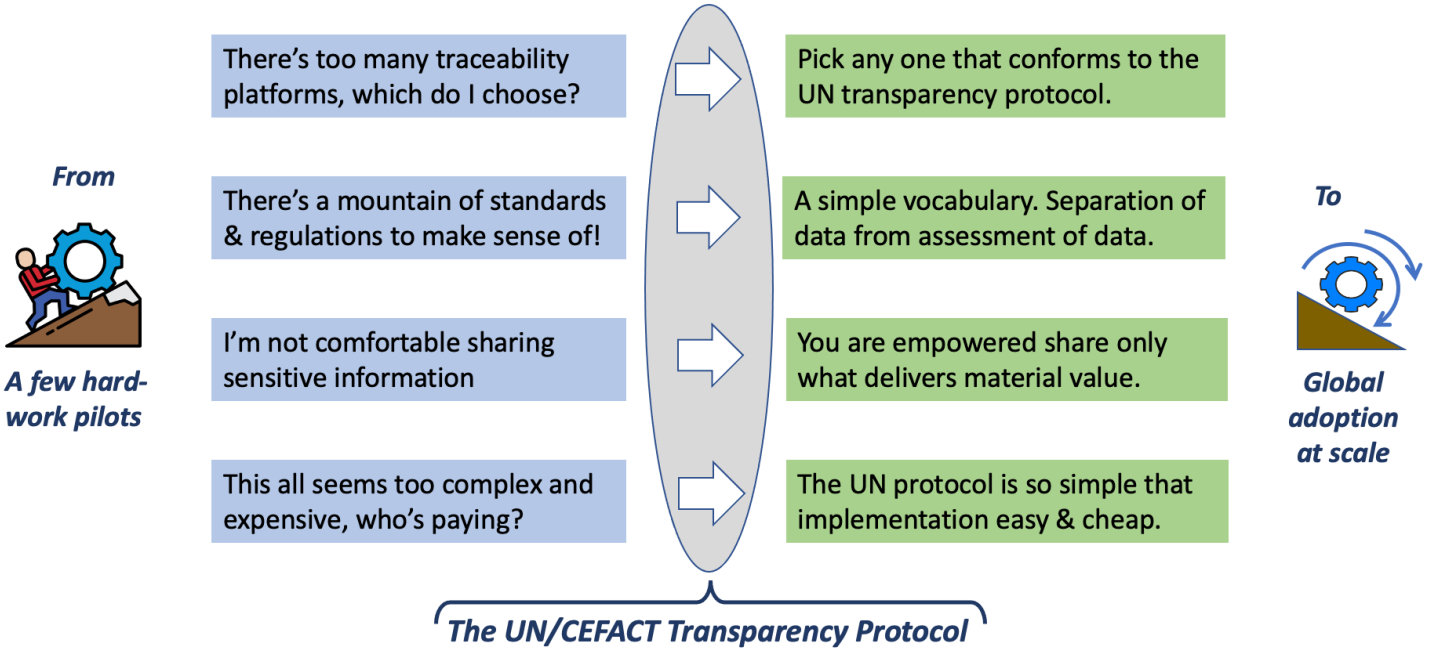
The world's supply chains must reach to the point where digital verifiable traceability and transparency information are available to meet regulatory compliance, satisfy investors, and motivate consumers for

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 protcool 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.



Audience, Benefits & Goals

> **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 verifible 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 trust 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-goverened accreditation frameworks and **issue** (or revoke) UNTP accreditation credentials then they are able to participate in the digital trust ecosystem as trust 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 clearnance 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
Regulators	10	1	20	10	50	20	200

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

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

Requirements

> **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 catgories. 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 goverened in an open and transparent manner, is freely avaialable 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	Governance

ID	Name	Requirement Statement	Solution Mapping
		minimum of 2 years - so that implementers can have confidence in the durability of their investment.	
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 extension can be confident that their implementation is interoperable with UNTP core.	Extensions
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 ot 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 - so that every implementers of UNTP can confidently proceed without dependency on the capability or readiness of upstream or downstream actors.	Data Carriers

ID	Name	Requirement Statement	Solution Mapping
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 indutries - 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 epxections 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	Data Carriers

ID	Name	Requirement Statement	Solution Mapping
		only a product batch ID or goods shipment ID can find ESG data about that product or shipment.	
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
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	Digital Product Passport,

ID	Name	Requirement Statement	Solution Mapping
		product buyers can meet their recycled content goals and recyclers can optimise their recycling processes.	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 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.	Trust Anchors
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	Identifiers

ID	Name	Requirement Statement	Solution Mapping
		can be sure that ESG claims are made by parties genuinely authorised to do so.	
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 authrority 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

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

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 trceability & 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

ID	Name	Requirement Statement	Solution Mapping
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
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.	

ID	Name	Requirement Statement	Solution Mapping
CI.05	Blockchain	Whilst some implementers MAY choose blockchain technologoes to underpin their solutions, the UNTP MUST NOT require the use of blockchain for conformant implementations - so that implementers that wish to avoid the costs and complexity of blockahin 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 benefots of their implementation	Business Case

ID	Name	Requirement Statement	Solution Mapping
		outweighs the cost. UNTP SHOULD provide a set of business case templates so that each stakholder type can fast-track their decision to proceed	
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 confidenet 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
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 mechansim 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	Greenwashing KPIs

ID	Name	Requirement Statement	Solution Mapping
		MUST develop a set of greenwashing KPIs that can be tracked to assess whether UNTP is having a material impact.	

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.

Management process

The UNTP development follows the same **standard governance rules** as any UN/CEFACT project.

- Free to use,
- Open source licensed,
- Maintained via an open process
- Version controlled
- Lifecycle managed

Releases

As per docusaurus version management practices, the latest stable version of UNTP will always be shown be default at /docs (this site). In-progress future version will be hosted at /docs/next and previous versions at /versioned-docs/version-x.y. The version history includes major versions (breaking) and minor versions (non-breaking but with functional change) but not patch versions (bug fixes and typos) which overwrite the relevant minor version.

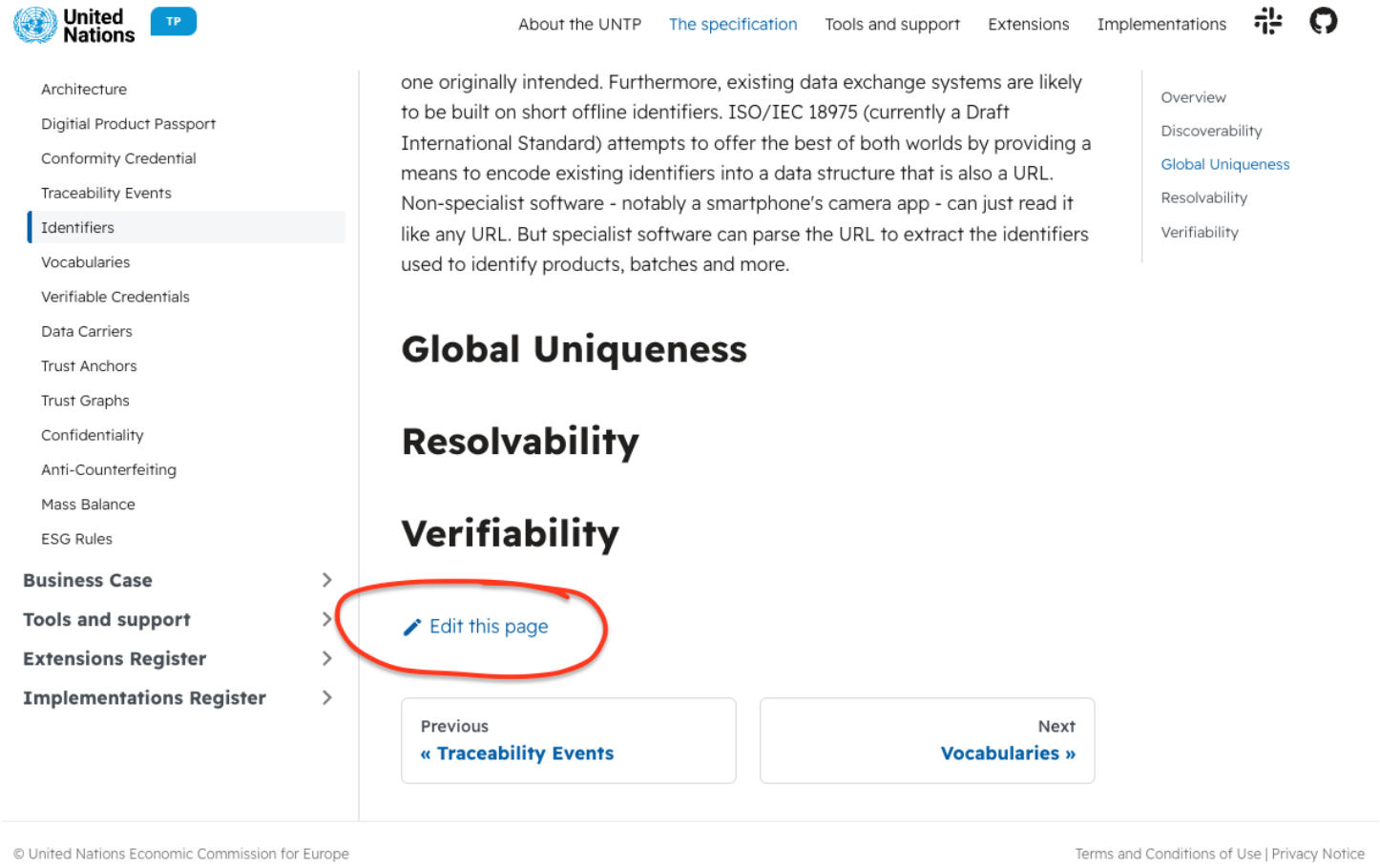
The UNTP includes a number of distinct and separately versioned components such as passport schema, traceability event schema and so on. To simplify implementaiton management, all seaprate component versions are grouped together and listed under each aggregated UNTP version.

UNTP Version	Status	Date	Componenets	Comment
0.0.0	Raw	2024-01-01	TBA	Empty framework

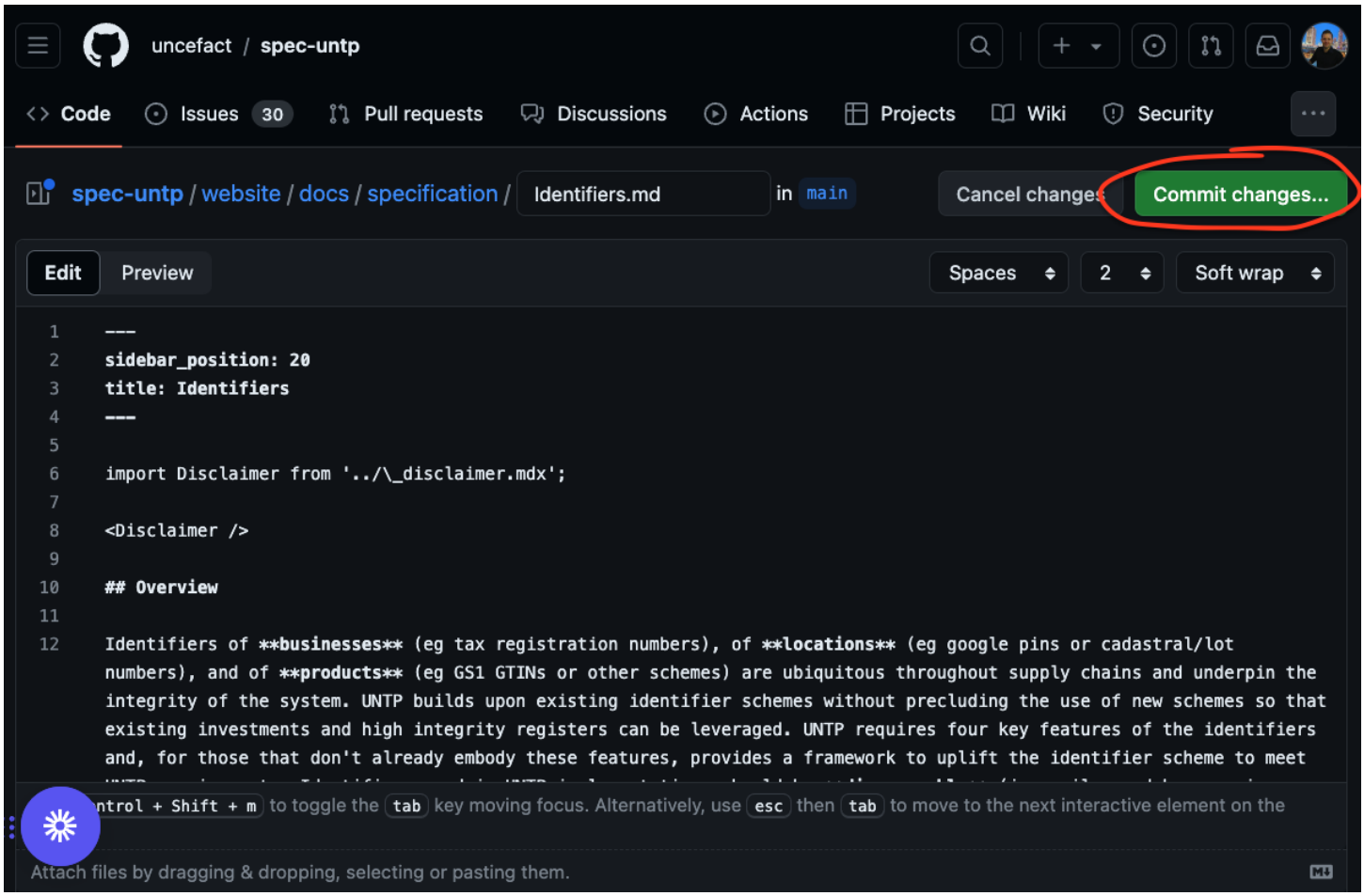
Contribution Process

In general we follow the standard GIT Pull Request process.

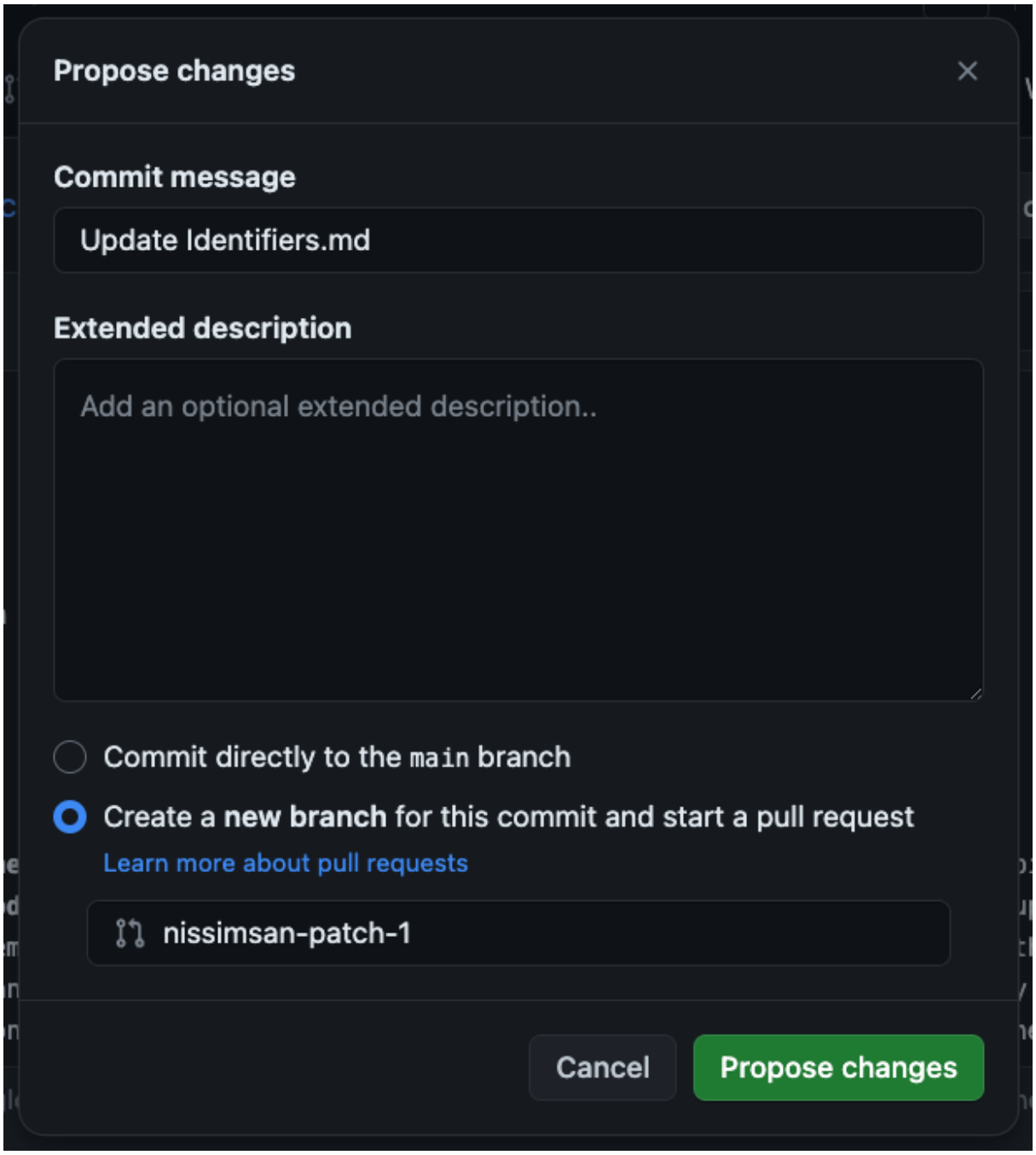
1. By far the easiest way is to start from the Edit feature, here:



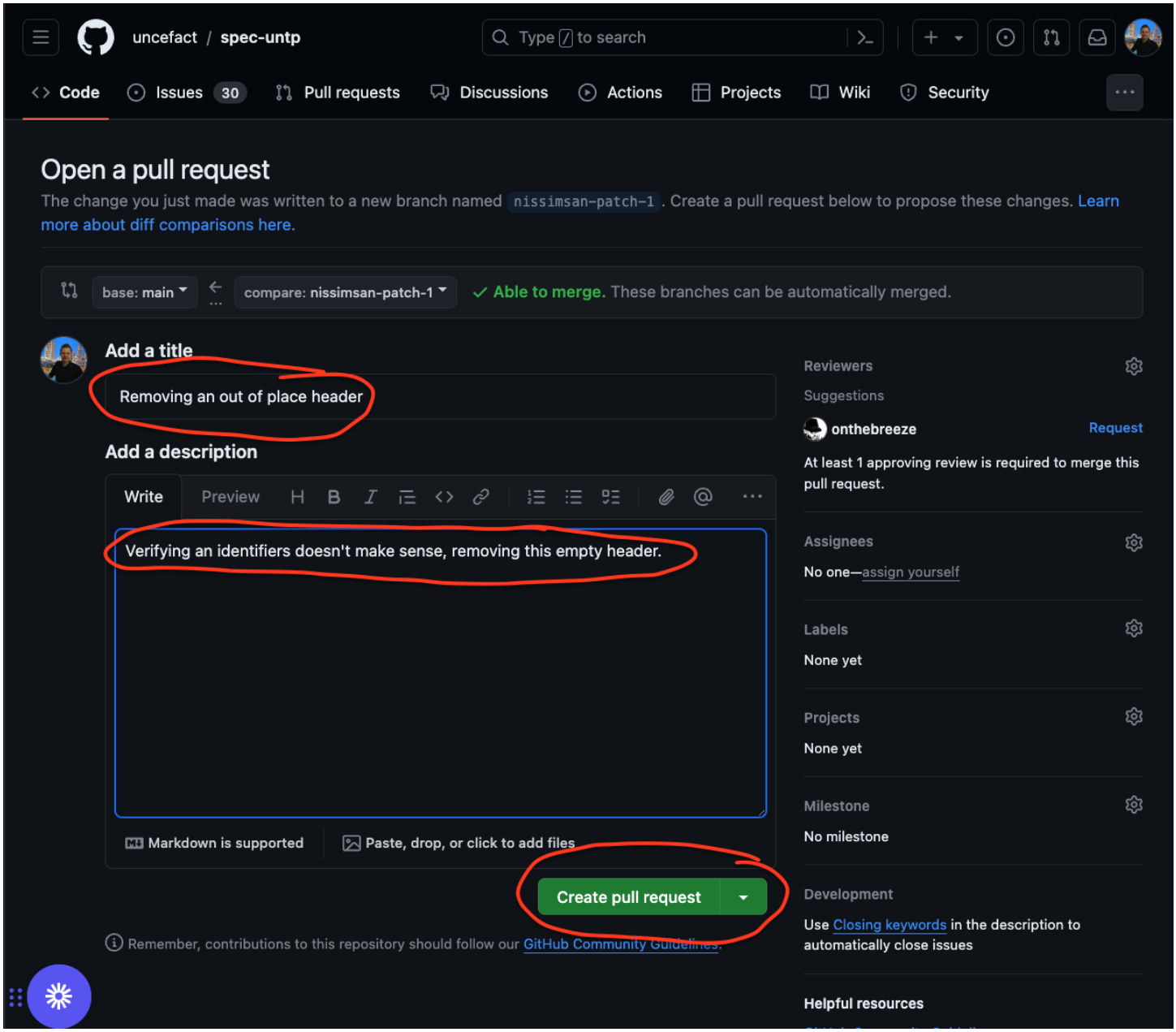
2. Make your changes in the markdown file, then commit:



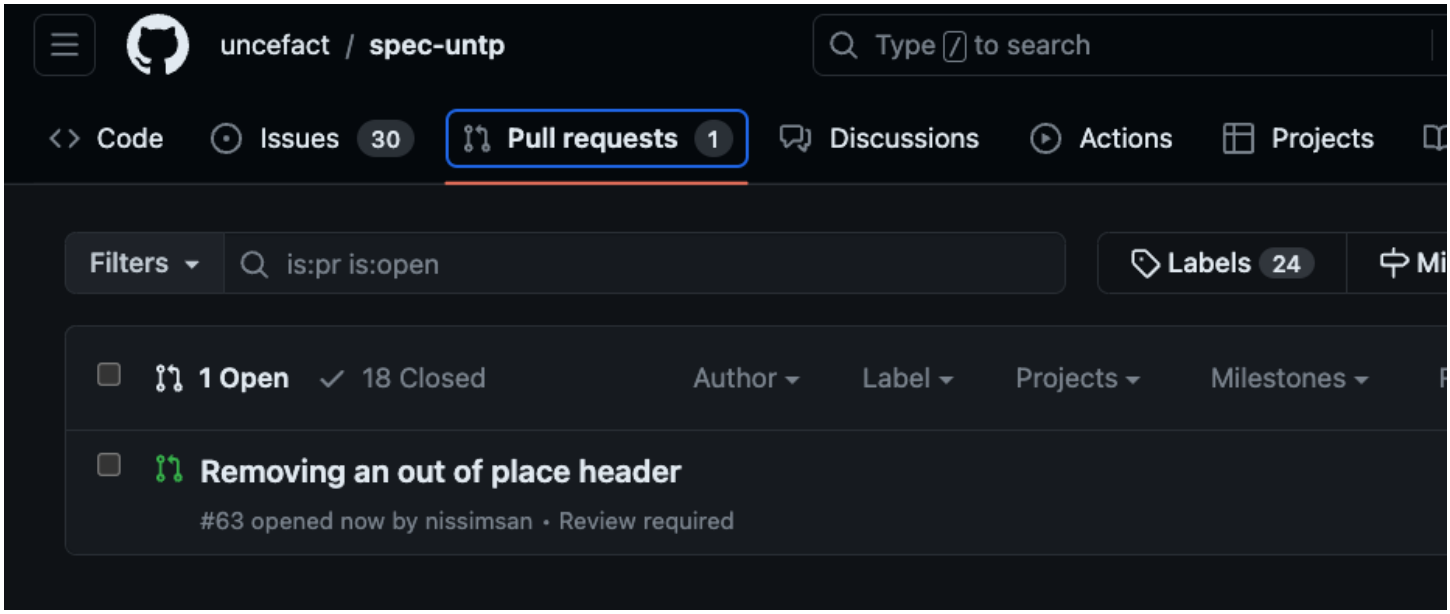
3. Just click okay on this (we don't have a commit message policy):



4. Then create a pull request for your change request. Here we do prefer a suitable title and a brief description of the change you are suggesting:



5. We will process your PR in the next meeting. Note that you will not see your change on the website before that happens, and we have agreed to merge your PR.


uncefact / spec-untp
Type / to search
Code
Issues 30
Pull requests 1
Discussions
Actions
Projects
Filters
is:pr is:open
Labels 24
1 Open
18 Closed
Author
Label
Projects
Milestones
Removing an out of place header
#63 opened now by nissimsan • Review required

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 Change

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 regulation that demands digital product passports for products sole 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 supply 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 string 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 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. Also, there is 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.

Business Case temaplates

> **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.

For Buyers and Suppliers in the Value Chain

For Conformity Assesment Bodies

For Industry Associations

For Regulators

For Software Vendors

Community Activation Program

> **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.

Community Activation

Value Assessment Framework

> **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

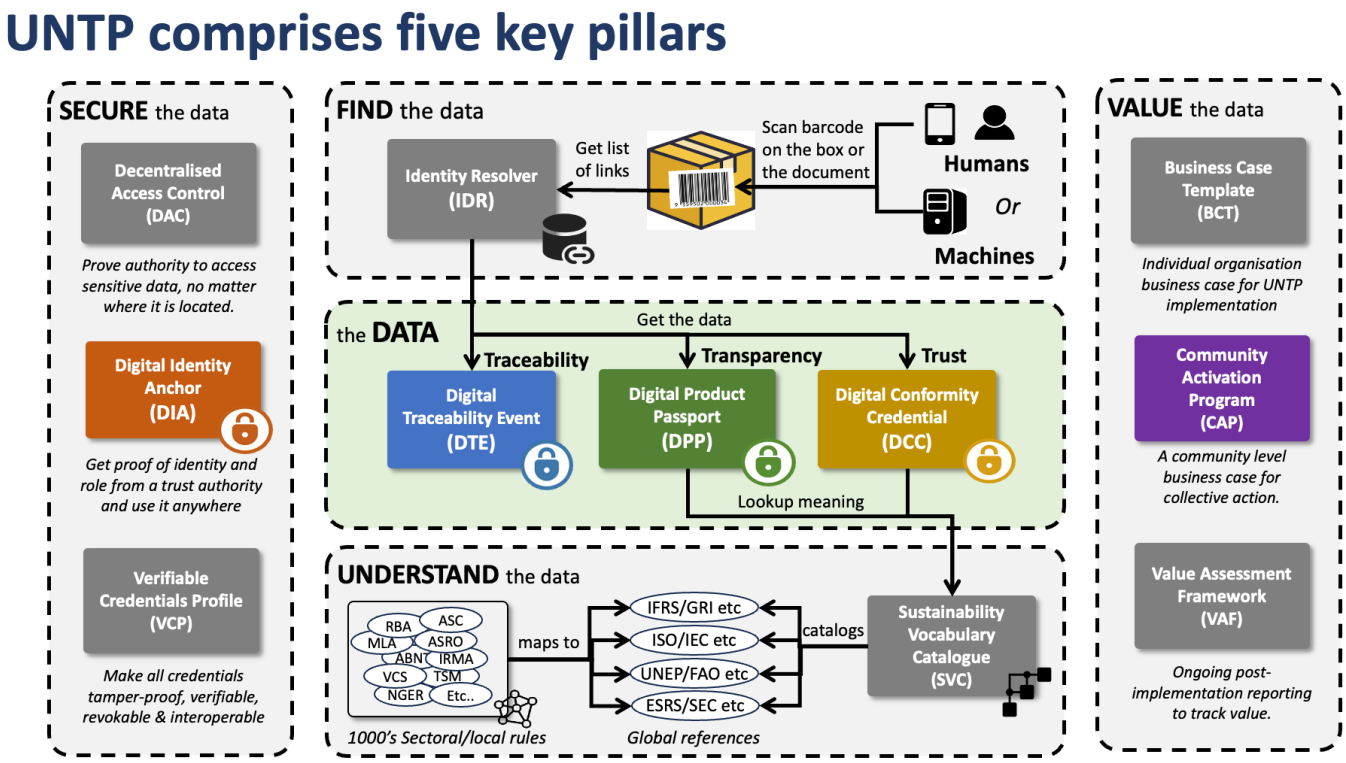
Specification

> **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 it's 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 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 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 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), 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

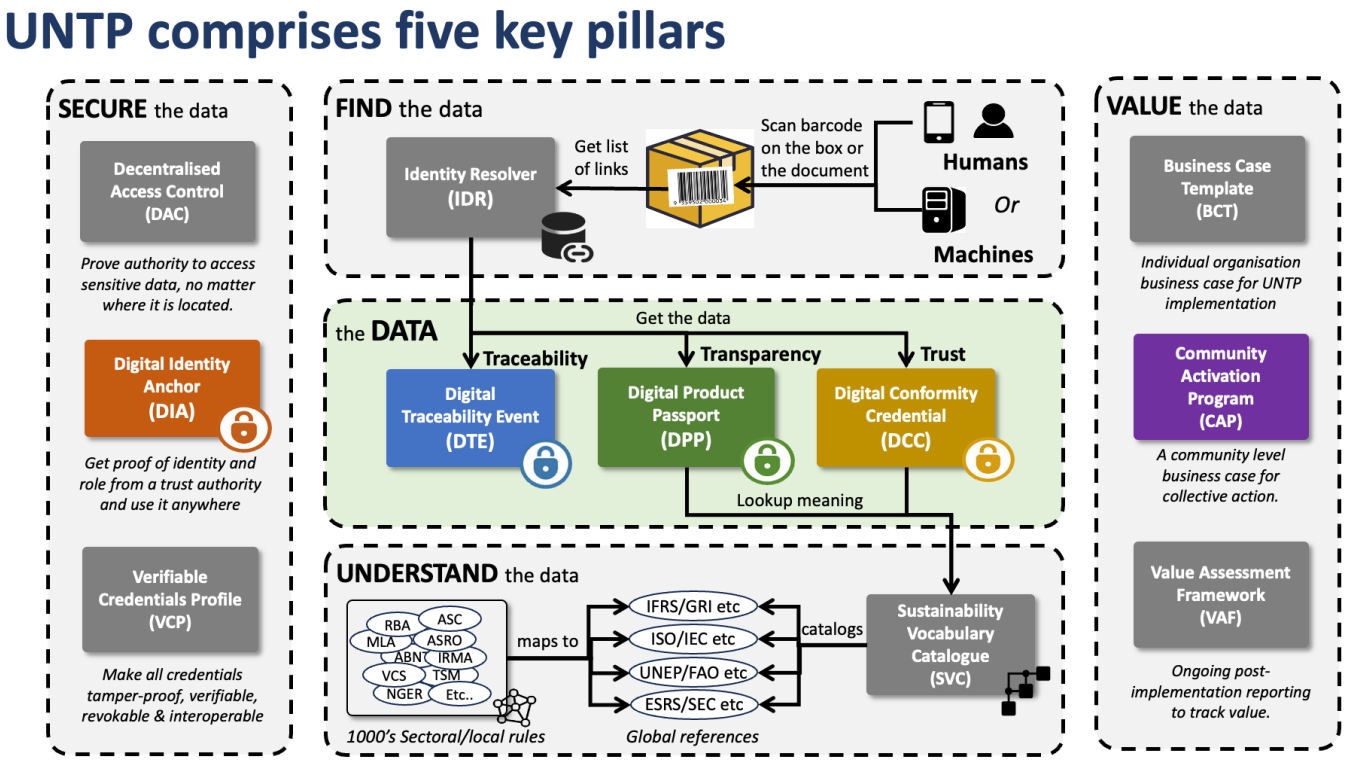
The architecture principles that guide the UNTP design are

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

Name	Principle	Rationale
		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
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** standrds 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 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 link types 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)** provides a framework to map sustainability knowledge across different standards, regulations and industry practices. It may not always answer the question but it provides a decentralised semantic governance model that allows mappings and corresponding value to grow over time and gaps to be fixed as they are found. The SVC is a W3C DCAT-conformant catalog of external sustainability standards and regulations. Mappings are defined using W3C SKOS and can be made either by UN working groups external standards **or** by external authorities to the UN catalog. This allows for a decentralised mapping effort that is far more scalable than depending on a small centralised team.

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 is 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.

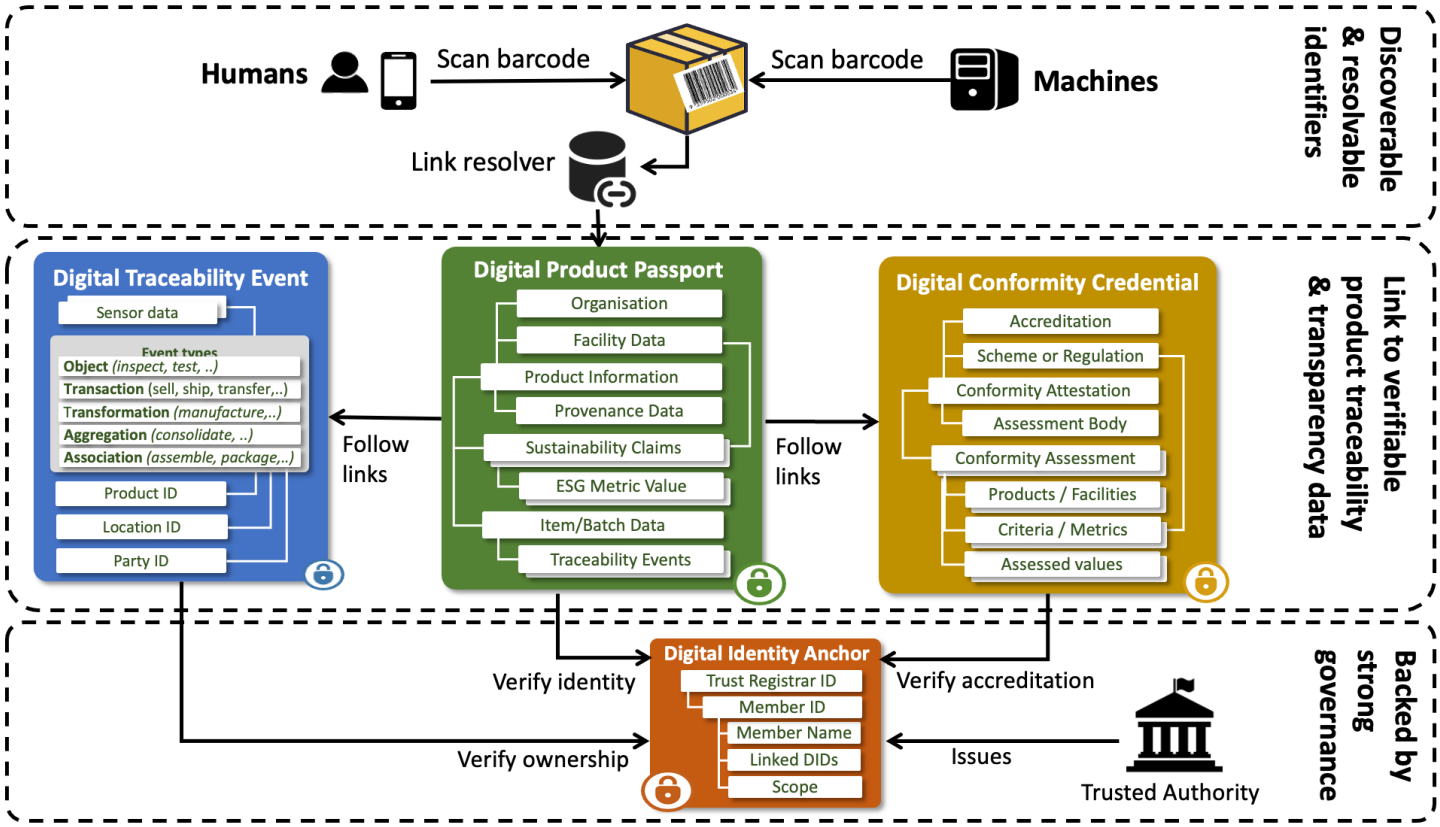
UNTP for one product

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

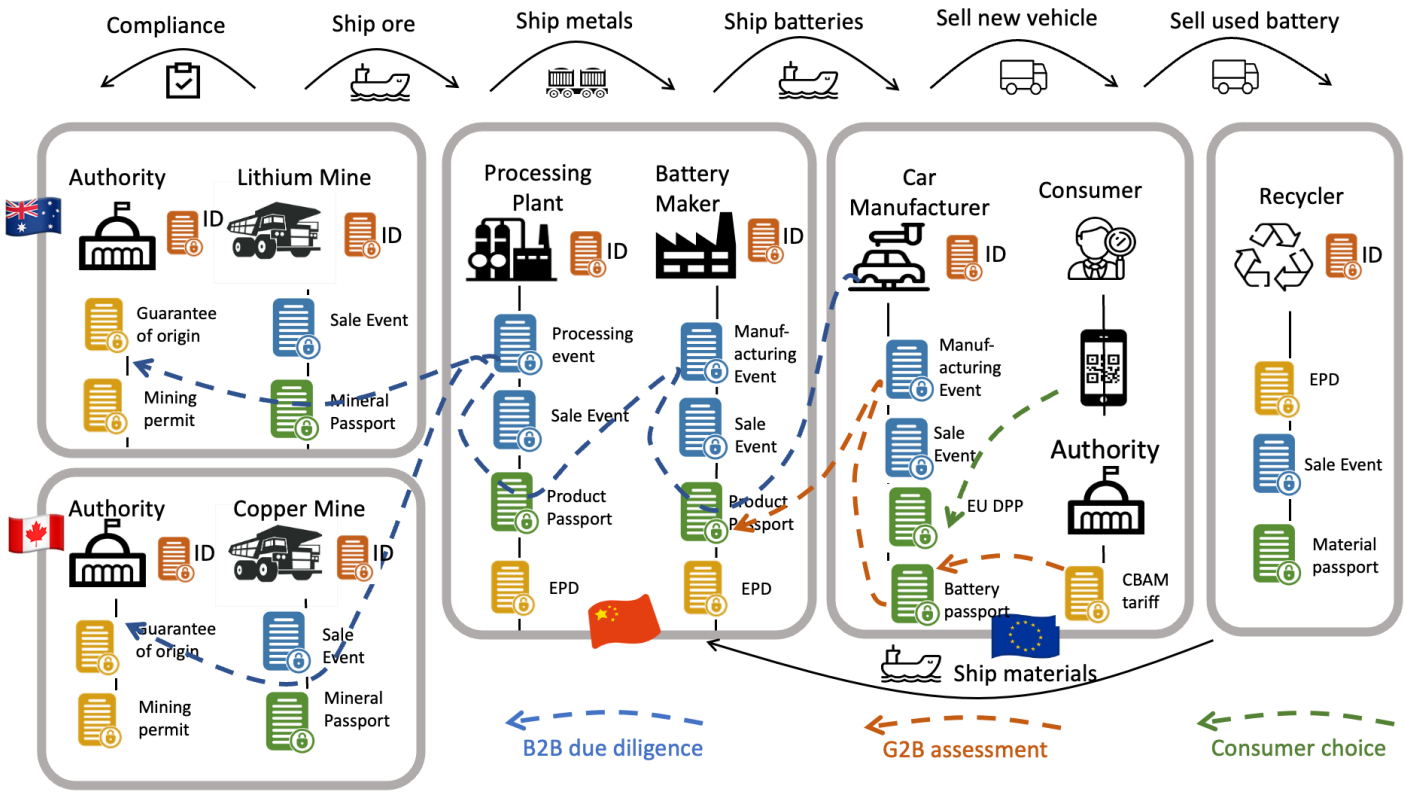
- Digital Product passport (DPP)

- Digital Conformity Credential (DCC)
- Digital Traceability Event (DTE)



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 can be confident of the integrity of UNTP credentials.	All VC options support this 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	Basic profile

ID	Name	Requirement Statement	Solution Mapping
		credentials of any size can be traversed and verified efficiently.	
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

VC basic 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 v1.1 using the JSON-LD Compacted Document Form
- SHOULD 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 checks including revocation checks
- 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)

- SHOULD implement the embedded proof mechanism defined in W3 Data Integrity proof

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.

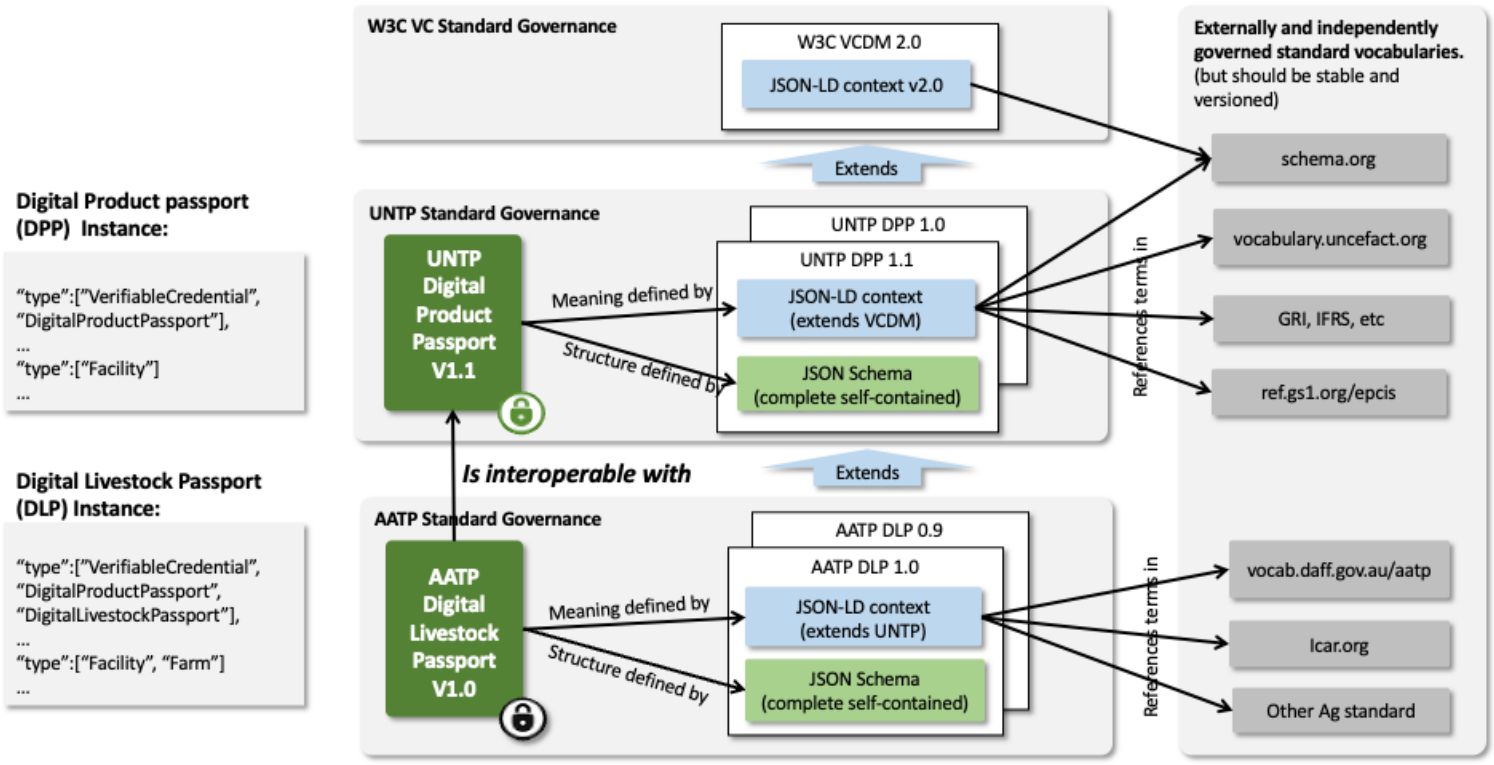
Vocabularies

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 (eg when VCDM 2.0 will change from SHOULD support to MUST support)

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.

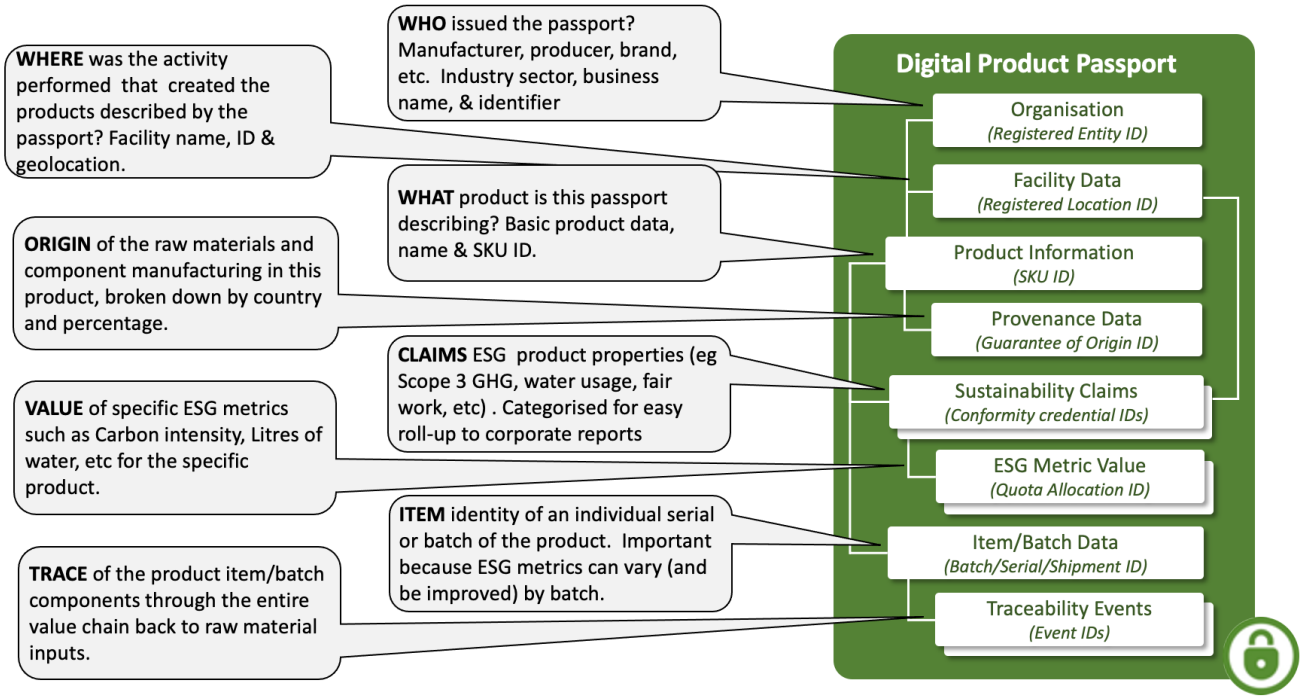
Versions

DPP Version	Date	status	Change summary	JSON-LD Context	JSON Schema
0.3.0	01-07-2024	Raw	refactored to buuild on untp-core	@context	Schema

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(https://uncefact.github.io/spec-untp/docs/about/Requirements)]

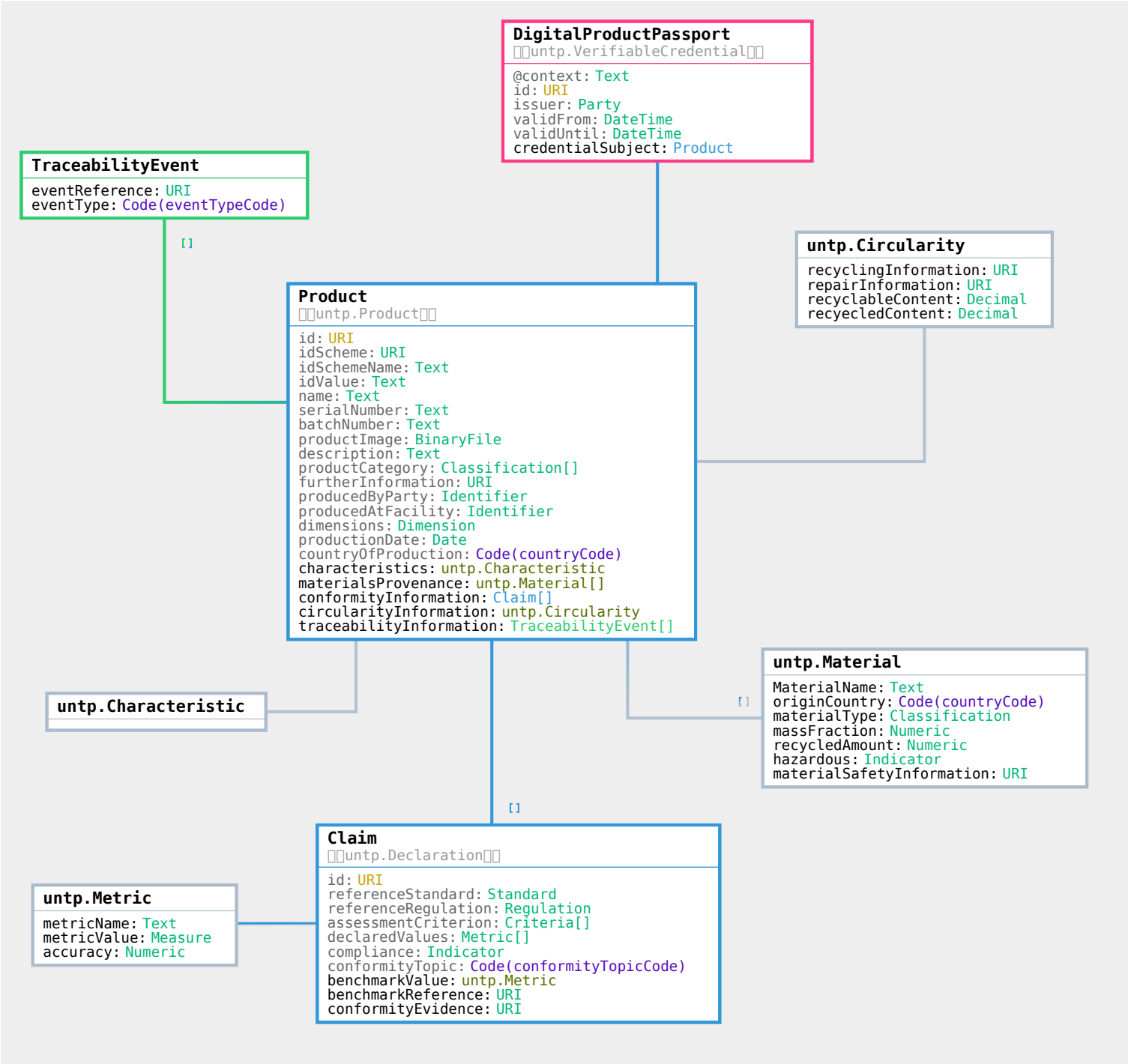
ID	Name	Requirement Statement	Solution Mapping
DPP-01	product, batch, item	The DPP should support use at either product level or at batch level or at individual serialised item level.	Claims are made at the passport level, which MUST have a related product and MAY have a related batch and item
DPP-02	Classification	The DPP should support any number of product classifications using codes from a defined classificaton scheme (eg UN-CPC)	The classifications property

ID	Name	Requirement Statement	Solution Mapping
DPP-03	Materials provenance	The DPP should provide a simple structure to allow issuers to breakdown 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.
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 incliding the location class is designed to meet this need
DPP-05	Dimensions	The DPP must support the definision 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), prevenance claims can be verified to any arbitrary depth upt o primary production	The links to EPCIS traceability event credentials from the productBatch class is designed to meet this need
DPP-07	characteristics	The DPP should allow issuer to provide descriptive information about the product (image, description, etc)	Characteristics property as an industry extnesion point

ID	Name	Requirement Statement	Solution Mapping
		that is extensible to meet industry specific needs.	
DPP-08	Verifiable Party	The DPP should provide DPP issuer, product manufacturer, and facility operator identification inclding 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 SHOUL have related resolvable Digital Identity Anchor 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
DPP-11	Metrics	The DPP MUST provide a simple mechanism to quantify a conformity claims (eg carbin 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

ID	Name	Requirement Statement	Solution Mapping
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 inter 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 confidenc elevel attached ot the evidence should be clear.	The Claim.conformityEvidence property references a relevant digital conformity credential

Logical Model



Data Definitions

Core Types

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

DPP Classes

Digital Product Passport Classes

DPP Code Tables

Digital Product Passport Code Tables

Sample

Note - this sample describes the digital product passport payload only - ie the subject of the verifiable credetial without the envelope. Needs some more realistic data.


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://test.uncefact.org/vocabulary/untp/untp-v1"
  ],
  "type": [
    "VerifiableCredential",
    "UNTPDigitalProductPassportCredential"
  ],
  "credentialSchema": {
    "type": "JsonSchema",
    "id": "https://uncefact.github.io/spec-
untp/docs/specification/DigitalProductPassport"
  },
  "id": "urn:untp:e5adbeg6-2n1s-4669-bd54-321d903re998",
  "issuer": {
    "type": ["Organization"],
    "id": "did:web:zerowave.example.com",
    "name": "Zero Wave Riding Co."
  },
  "validFrom": "2023-06-22T10:00:00.000Z",
  "credentialSubject": {
    "type": ["UNTPDigitalProductPassport"],
    "product": {
      "type": ["Product"],
      "id": "https://shop.zerowave.example.com/cruizer",
      "batchIdentifiers": [
        "http://zerowave.example.com/01/09520123456788/10/ABC123"
      ],
      "itemIdentifiers": [
        "http://zerowave.example.com/01/09520123456788/21/12345",
```

```
      "http://zerowave.example.com/01/09520123456788/21/12346"
    ],
    "modelName": "Cruizer",
    "image": "https://shop.zerowave.example.com/media/cruizer.jpg",
    "description": "12kW, 3.6 kWh self-propulsion surfboard",
    "classifications": "eSurf",
    "furtherInformation": "https://shop.zerowave.example.com/cruizer",
    "manufacturedDate": "2024-05-08",
    "dimensions": {
      "type": "Dimensions",
      "weight": {
        "value": 15.9,
        "unit": "kg"
      },
      "length": {
        "value": 169,
        "unit": "cm"
      },
      "width": {
        "value": 65.5,
        "unit": "cm"
      }
    },
    "manufacturer": {
      "type": "Organization",
      "id": "did:web:hitech-assembly.example.com",
      "name": "Hitech Assembly, Inc.",
      "location": "Manufacturered in the EU"
    },
    "materialsProvenance": [
      {
        "type": "MaterialProvenance",
        "originCountry": "EU",
        "materialType": "EPP",
        "massFraction": 0.6,
        "recycled": true,
        "hazardous": false
      }
    ],
    "conformityClaims": [
      {
        "type": "LinkRole",
        "target": "https://supplier.example.com/material/reuse-certificate",
        "linkRelationship": "untpConformity"
      },
      {
        "type": "LinkRole",
        "target": "https://supplier.example.com/manufacturing/carbon-emissions-
```

```
certificate",
          "linkRelationship": "untpConformity"
        }
      ],
      "recyclingInstructions": "http://brand-owner.example.com/nordic-
pioneer/recycling",
      "traceabilityInformation": [
        {
          "type": "UNTPAggregationEvent",
          "id": "http://manufacturer.example.com/293847293847"
        }
      ]
    },
    "guaranteeOfOriginCredential":
"https://supplier.example.com/manufacturing/certificate-of-origin"
  }
}
```


Schema


```
title: UNTP Digital Product Passport Credential
description: 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.
type: object
properties:
  '@context':
    type: array
    readOnly: true
    const:
      - https://www.w3.org/ns/credentials/v2
      - https://test.uncefact.org/vocabulary/untp/untp-v1
    default:
      - https://www.w3.org/ns/credentials/v2
      - https://test.uncefact.org/vocabulary/untp/untp-v1
```

```
    items:
      type: string
      enum:
        - https://www.w3.org/ns/credentials/v2
        - https://test.uncefact.org/vocabulary/untp/untp-v1
  type:
    type: array
    readOnly: true
    const:
      - VerifiableCredential
      - UNTPDigitalProductPassportCredential
    default:
      - VerifiableCredential
      - UNTPDigitalProductPassportCredential
    items:
      type: string
      enum:
        - VerifiableCredential
        - UNTPDigitalProductPassportCredential
  id:
    type: string
    format: uri
  credentialSchema:
    type: object
    properties:
      id:
        title: Schema URL
        description: The url of the schema file to validate the shape of the json
object
        type: string
        format: uri
        const: https://uncefact.github.io/spec-
untp/docs/specification/DigitalProductPassport
      type:
        title: Type
        description: The type of validation to be run against the defined schema
        const: JsonSchema
    additionalProperties: false
    required:
      - type
      - id
  validFrom:
    type: string
    format: date-time
  validTo:
    type: string
    format: date-time
  issuer:
```

```
    title: Issuer Organization
    type: object
    properties:
      type:
        type: array
        readOnly: true
        const:
          - Organization
        default:
          - Organization
        items:
          type: string
          enum:
            - Organization
      id:
        title: Issuer's Identifier
        description: Issuing organization identifier, typically a Decentralized
Identifier (DID).
        type: string
      name:
        title: Name
        description: Issuing organization name.
        type: string
      street:
        title: Street
        description: The street address expressed as free form text. The street
address is printed on paper as the first lines below the name. For example, the name
of the street and the number in the street, or the name of a building.
        type: string
      locality:
        title: Locality
        description: The locality in which the street address is, and which is in the
region; for example, a city or town.
        type: string
      region:
        title: State
        description: Text specifying a province or state in abbreviated format; for
example, NJ.
        type: string
      postalCode:
        title: Postal Code
        description: Text specifying the postal code for an address.
        type: string
      country:
        title: Country
        description: The two-letter ISO 3166-1 alpha-2 country code.
        type: string
    additionalProperties: false
```

```
    required:
      - type
      - id
      - name
  credentialSubject:
    type: object
    properties:
      type:
        type: array
        readOnly: true
        const:
          - UNTPDigitalProductPassport
        default:
          - UNTPDigitalProductPassport
        items:
          type: string
          enum:
            - UNTPDigitalProductPassport
      product:
        title: Product
        type: object
        properties:
          type:
            type: array
            readOnly: true
            const:
              - Product
            default:
              - Product
            items:
              type: string
              enum:
                - Product
          modelName:
            title: Model Name
            description: Model name of the product.
            type: string
      guaranteeOfOriginCredential:
        title: Guarantee of Origin Credential
        type: string
        format: uri
    required:
      - type
required:
  - '@context'
  - type
  - credentialSchema
  - validFrom
```

```
  - issuer
  - credentialSubject
```

Examples from pilot projects

Project	DPP Version	Description	Credential	Rendered View
AATP	0.1.0	Packaged Meat DPP	sample DPP VC	DPP VC Viewer

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.

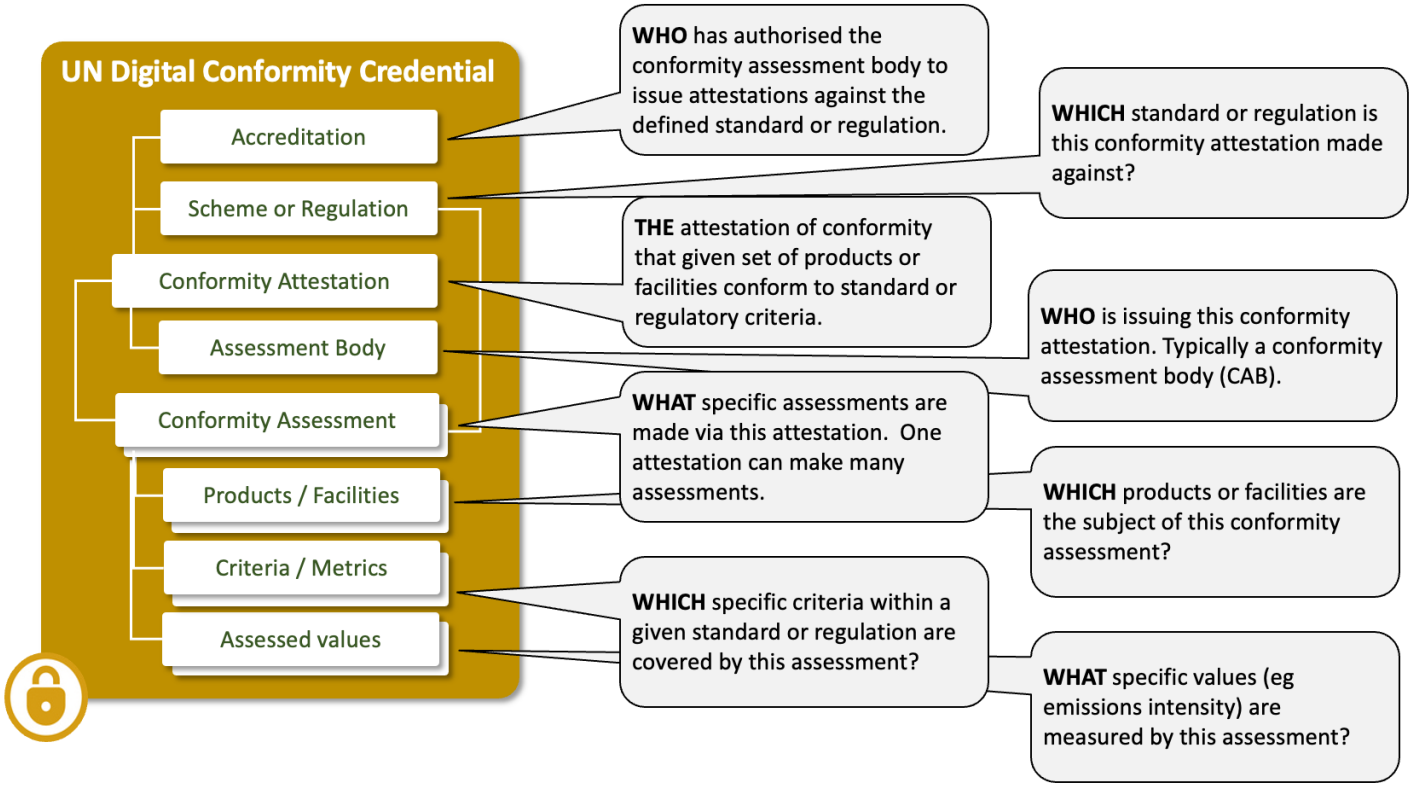
Versions

DPCC Version	Date	status	change log	JSON-LD Context	JSON Schema
0.3.0	01-07-2024	Raw	rebuilt on untp-core vocabulary	DPP context - TBA	DPP schema - TBA

Overview

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.

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 source	The DPCC MUST be verifiable as issued by an authorised source, 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	Subject of conformity	The DPCC MUST unambiguously identify the subject of the conformity	Assessment. assessedProducts,

ID	Name	Requirement Statement	Solution Mapping
		assessment, whether a product or facility.	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 appropriate this must include specific measurable trhesholds (eg minimum tensile strength)	ConformityAssessment. referenceStandard and ConformityAssessment. assessmentCriterion
DPCC-05	Conformity Attestation	The DPCCE MUST unambiguosly state whether or not the subject of the assessment is conformat 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 auditable evidence (eg instrument recordings, satellite images, etc) to support the assessment. If so then the hash of the evidence fileset 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

Data Definitions

Core Types

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 buuilding blocks for construction of Digital Product Passports and Digital Conformity Credentials.

DCC Classes

DCC class & property definitions

DCC Code Tables

DCC code tables

Sample

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://test.uncefact.org/spec-untp/untp-v1"
  ],
  "type": ["VerifiableCredential", "ConformityCredential", "ExampleCredential"],
  "id": "https://example.com/credentials/123",
  "issuer": {
    "id": "did:web:issuer.example.com"
  },
  "validFrom": "2022-04-01T00:00:00Z",
  "validUntil": "2027-04-01T00:00:00Z",
  "evidence": {
    "type": ["ConformityAttestationEvidence"],
    "evidenceRootHash": "string",
    "description": "string",
    "evidenceData": [
      {
        "fileHash": "string",
        "fileLocation": "http://example.com",
        "fileType": "string",
        "EncryptionMethod": "none"
      }
    ],
    "decryptionKeyRequest": "http://example.com"
  },
  "credentialSubject": {
    "type": ["Organization"],
    "id": "did:web:producer.example.com",
    "hasAttestation": {
      "id": "http://example.com",
      "assessorLevel": "Self",
      "assessmentLevel": "GovtApproval",
      "type": "certification",
      "description": "string",
      "scope": {
        "id": "http://example.com",
        "name": "string",
        "trustmark": {
          "fileHash": "string",
          "fileLocation": "http://example.com",
          "fileType": "string",
          "EncryptionMethod": "none"
        },
        "issuingBody": {
          "identifiers": [
            {
              "scheme": "http://example.com",
```

```
            "identiferValue": "string",
            "identifierURI": "http://example.com",
            "verificationEvidence": {
              "format": "w3c_vc",
              "credentialReference": "http://example.com"
            }
          }
        ],
        "name": "string"
      },
      "dateOfIssue": "2019-08-24"
    },
    "assessments": [
      {
        "referenceStandard": {
          "id": "http://example.com",
          "name": "string",
          "issuingBody": {
            "identifiers": [
              {
                "scheme": "http://example.com",
                "identiferValue": "string",
                "identifierURI": "http://example.com",
                "verificationEvidence": {
                  "format": "w3c_vc",
                  "credentialReference": "http://example.com"
                }
              }
            ],
            "name": "string"
          },
          "issueDate": "2019-08-24"
        },
        "referenceRegulation": {
          "id": "http://example.com",
          "name": "string",
          "issuingBody": {
            "identifiers": [
              {
                "scheme": "http://example.com",
                "identiferValue": "string",
                "identifierURI": "http://example.com",
                "verificationEvidence": {
                  "format": "w3c_vc",
                  "credentialReference": "http://example.com"
                }
              }
            ],
```

```
      "name": "string"
    },
    "effectiveDate": "2019-08-24"
  },
  "assessmentCriterion": {
    "id": "http://example.com",
    "threshold": [
      {
        "name": "string",
        "value": {
          "value": 0,
          "unit": "string"
        },
        "minimumValue": {
          "value": 0,
          "unit": "string"
        },
        "maximumValue": {
          "value": 0,
          "unit": "string"
        }
      }
    ],
    "name": "string"
  },
  "attestedProducts": [
    {
      "identifiers": [
        {
          "scheme": "http://example.com",
          "identiferValue": "string",
          "identifierURI": "http://example.com",
          "verificationEvidence": {
            "format": "w3c_vc",
            "credentialReference": "http://example.com"
          }
        }
      ],
      "marking": "string",
      "name": "string",
      "classifications": [
        {
          "scheme": "http://example.com",
          "classifierValue": "string",
          "classifierName": "string",
          "classifierURL": "http://example.com"
        }
      ],
```

```
      "testedBatchId": "http://example.com",
      "verfifiedByCAB": true
    }
  ],
  "attestedLocations": [
    {
      "type": [],
      "identifiers": [
        {
          "scheme": "http://example.com",
          "identiferValue": "string",
          "identifierURI": "http://example.com",
          "verificationEvidence": {
            "format": "w3c_vc",
            "credentialReference": "http://example.com"
          }
        }
      ],
      "name": "string",
      "classifications": [
        {
          "scheme": "http://example.com",
          "classifierValue": "string",
          "classifierName": "string",
          "classifierURL": "http://example.com"
        }
      ],
      "geolocation": "http://example.com",
      "verfifiedByCAB": true
    }
  ],
  "measuredResults": [
    {
      "name": "string",
      "value": {
        "value": 0,
        "unit": "string"
      },
      "minimumValue": {
        "value": 0,
        "unit": "string"
      },
      "maximumValue": {
        "value": 0,
        "unit": "string"
      }
    }
  ],
```

```
      "compliance": true,
      "sustainabilityTopic": "environment.energy"
    }
  ],
  "accreditation": {
    "number": "string",
    "authorityEvidence": {
      "format": "w3c_vc",
      "credentialReference": "http://example.com"
    },
    "trustmark": {
      "fileHash": "string",
      "fileLocation": "http://example.com",
      "fileType": "string",
      "EncryptionMethod": "none"
    },
    "authority": {
      "identifiers": [
        {
          "scheme": "http://example.com",
          "identiferValue": "string",
          "identifierURI": "http://example.com",
          "verificationEvidence": {
            "format": "w3c_vc",
            "credentialReference": "http://example.com"
          }
        }
      ],
      "name": "string"
    }
  },
  "regulatoryApproval": {
    "number": "string",
    "authorityEvidence": {
      "format": "w3c_vc",
      "credentialReference": "http://example.com"
    },
    "trustmark": {
      "fileHash": "string",
      "fileLocation": "http://example.com",
      "fileType": "string",
      "EncryptionMethod": "none"
    },
    "authority": {
      "identifiers": [
        {
          "scheme": "http://example.com",
          "identiferValue": "string",
```

```
              "identifierURI": "http://example.com",
              "verificationEvidence": {
                "format": "w3c_vc",
                "credentialReference": "http://example.com"
              }
            }
          ],
          "name": "string"
        }
      },
      "certificate": {
        "fileHash": "string",
        "fileLocation": "http://example.com",
        "fileType": "string",
        "EncryptionMethod": "none"
      }
    }
  }
}
```

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.

Versions

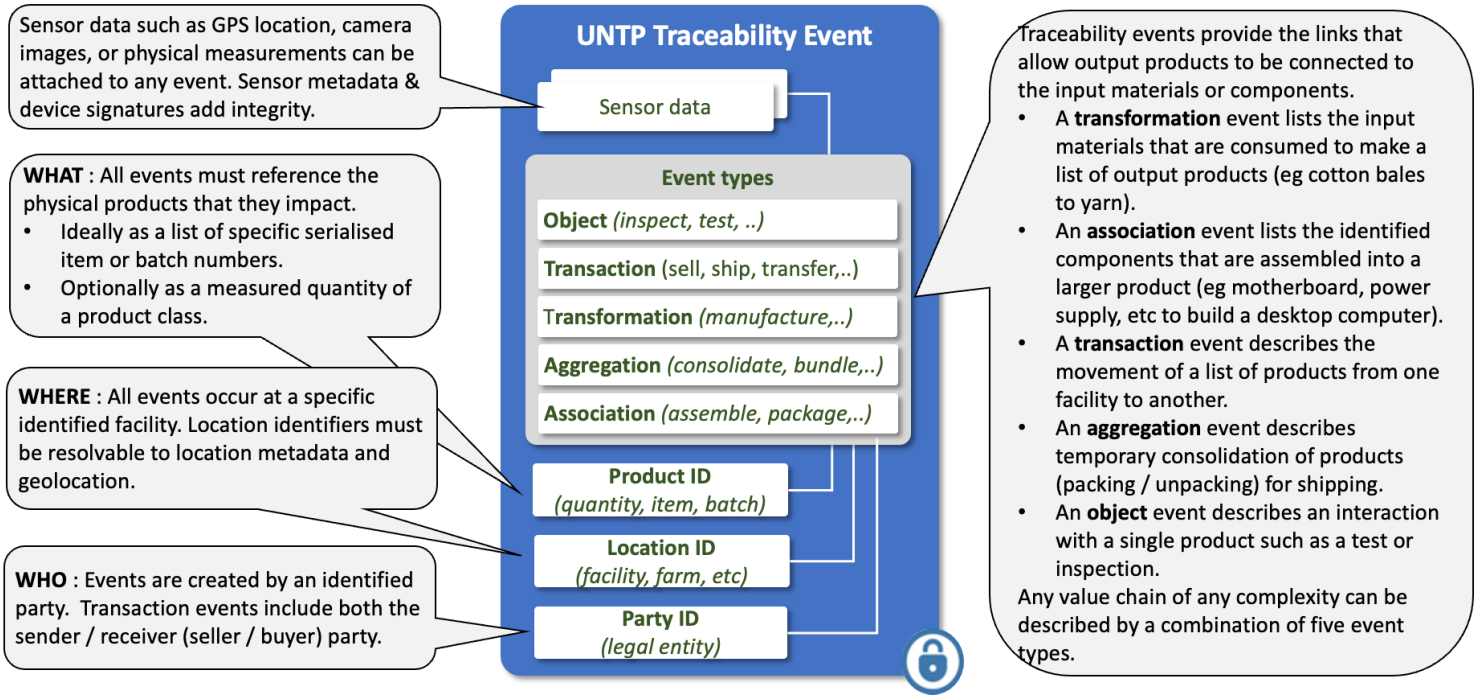
traceability Version	Date	status	JSON-LD Context
0.3.0	20-04-2024	Raw (for review)	Coming soon - fixing a bug

The current version of this specification is v0.3.0

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



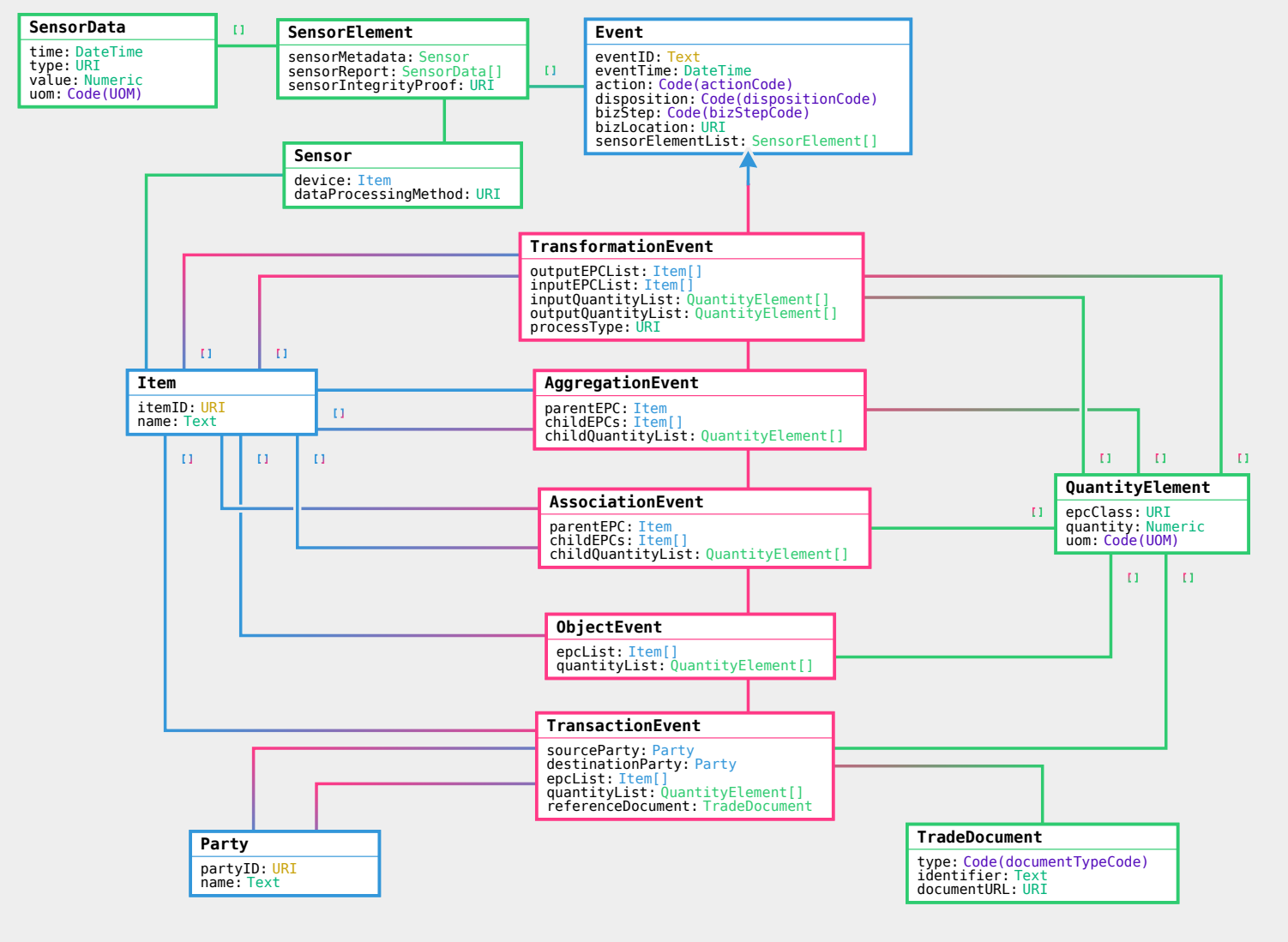
Requirements

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
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](#transformationevent)
TEV-03	Aggregated bundles	When a DPP represents an aggregated bundle of similar items (eg a pallet of	Aggregation Event

ID	Name	Requirement Statement	Solution Mapping
		cotton bales) then the traceability event MUST provide a means to allocate the aggregate measures to each individual item (ie each bale)	
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



Data Definitions

Event

> This abstract event structure provides a common language to describe supply chain events such as shipments, inspections, manufacturing processes, etc. There are four types of event but this is an abstract class representing all common properties of an event.

Property	Definition	Type
eventID	The unique identifier of this event - SHOULD be a UUID	Text
eventTime	The ISO-8601 date time when the event occurred.	DateTime

Property	Definition	Type
action	Code describing how an event relates to the life-cycle of the entity being described.	Code (actionCode)
disposition	Disposition code describing the state of the item after the event.	Code (dispositionCode)
bizStep	A business step code drawn from a controlled vocabulary.	Code (bizStepCode)
bizLocation	A Business Location is a uniquely identified and discretely recorded geospatial location that is meant to designate the specific place where an object is assumed to be following an EPCIS event until it is reported to be at a different Business Location by a subsequent EPCIS event. The bizLocation must be a resolvable URI that links to facility information and geolocation data.	URI
sensorElementList	An array (one for each sensor) of sensor device data sets associated with the event.	SensorElement

Object Event

> Object represents an event that happened to one or more physical or digital objects - such as an inspection or certification of a product or shipment. The physical objects may be identified either as specific items (eg a unique consignment number) or as a quantified amount of a product class (eg 100Kg of cotton yarn)

Note that object event includes all the properties of Event as well as the additional properties described below.

Property	Definition	Type
epcList	A list of uniquely identified items (eg specific items serial numbers or tagged shipments / packages) that are the focus of	Item

Property	Definition	Type
	this object event.	
quantityList	A quantified list of product classes (eg GS1 GTINs) that are the focus of this object event	QuantityElement

Aggregation Event

> Aggregation represents an event that happened to one or more objects that are physically aggregated together (physically constrained to be in the same place at the same time, as when cases are aggregated to a pallet). This event is also used to represent de-aggregation (eg unpacking) when businessStepCode is unpacking.

Note that aggregation event includes all the properties of Event as well as the additional properties described below.

Property	Definition	Type
parentEPC	The unique item identifier that is the result of this aggregation. Typically a packaging ID used in shipments that represents a box/ pallet / container of contained items.	Item
childEPCs	The list of child items that have been aggregated into the parent (or dis-aggregated from the parent). Maybe a list of package references (eg boxes on a pallet) or may be individual items (eg products in a box).	Item
childQuantityList	List of quantified product classes that have been aggregated into the parent. Used when the child items do not have unique identifiers (eg 100 Kg of cotton bales)	QuantityElement

Transaction Event

> Transaction represents an event in which one or more objects become associated or disassociated with one or more identified business transactions - such as the purchase /

> shipment of goods between buyer and seller.

Note that transaction event includes all the properties of Event as well as the additional properties described below.

Property	Definition	Type
sourceParty	The source party for this supply chain transaction - typically the seller party	Party
destinationParty	The destination party for this supply chain transaction - typically the buyer party.	Party
epcList	The list of uniquely identified trade items included in this supply chain transaction.	Item
quantityList	List of quantified product classes that are included in this transaction. Used when the trade items do not have unique identifiers (eg 100 reels of yarn)	QuantityElement
referenceDocument	The supply chain document reference for this transaction event - eg the invoice, order, or dispatch advice	TradeDocument

Transformation Event

> Transformation represents an event in which input objects are fully or partially consumed and output objects are produced, such that any of the input objects may have contributed to all of the output objects - for example consuming bales of cotton to produce yarn.

Note that transformation event includes all the properties of Event as well as the additional properties described below.

Property	Definition	Type
outputEPCList	The list of uniquely identified items that are the output of this transformation event - for example a list of	Item

Property	Definition	Type
	individually identified bolts of cloth that are the output of a weaving process.	
inputEPCList	The list of uniquely identified items that are the input of this transformation event - for example a list of individually identified bobbins of yarn that are the input of a weaving process.	Item
inputQuantityList	The quantified list of product classes that are the input of this transformation event - used when each item does not have a unique identity. for example the weight of raw cotton that is the input to a ginning process.	QuantityElement
outputQuantityList	The quantified list of product classes that are the output of this transformation event - used when each item does not have a unique identity. for example a count of the bales of cleaned cotton that are the output of a ginning process.	QuantityElement
processType	An industry specific process type code.	URI

AssociationEvent

> The association event represents the assembly of child sub-components to create a parent assembled item. For example a desktop computer assembled from power supply, hard drive, and motherboard. The association event is very similar in structure to the aggregation event but is used for physical assembly. An association event may represent a bill of materials used to assemble a product whilst an aggregation event may represent a packing list or items for transport.

Note that association event includes all the properties of Event as well as the additional properties described below.

Property	Definition	Type
parentEPC	The unique item identifier that is the parent of this association. Typically an assembled product ID such as a desktop computer that is built from the associated child components.	Item
childEPCs	The list of child items that have been assembled to create the parent - for example the power supply or hard drive components of a desktop computer.	Item
childQuantityList	List of quantified product classes that have been assembled into the parent. Used when the child items do not have unique identifiers (eg brackets and screws used in the assembly of a desktop computer)	QuantityElement

QuantityElement

> The quantity element is used to define the quantities (eg 100), units of measure (eg Kg) and product class (eg GTIN or other class identifier) of products that are inputs or outputs or the subject of supply chain events.

Property	Definition	Type
epcClass	THe identifier of a product class (as opposed to a product instance) such as a GTIN code for a manufactured product.	URI
quantity	The numeric quantity of the product class (eg 100 kg of cotton)	Numeric
uom	The unit of measure for the quantity value (eg Kg or meters etc) using the UNECE Rec 20 unit of measure codelist.	Code (UOM)

TradeDocument

> A trade transaction between two parties such as an invoice, purchase order, or shipping notification.

Property	Definition	Type
type	The document type representing the trade transaction drawn from the business transaction type vocabulary.	Code (documentTypeCode)
identifier	The identifier of the trade transaction document - eg an invoice number or bill of lading number. Must be unique for a given source party	Text
documentURL	The URL of the referenced trade document. For integrity reasons, it is recommended (but not required) that the documentURL is a hash-link (https://w3c-ccg.github.io/hashlink/) so that if the document the URL is changed then the hash verification will fail.	

Item

> A specific trade item /product code which could be either a product serial number or a consignment identifier

Property	Definition	Type
itemID	The globally unique identifier (eg GS1 GTIN or digital link) of the product item.	URI
name	The name of the product class to which the product item belongs.	Text

Party

> A trade party

Property	Definition	Type
partyID	The globally unique identifier of the party. This must be expressed as a URI that is (preferably) resolvable to an entity register such as a national business register - eg https://abr.business.gov.au/ABN/View?abn=41161080146	URI

Property	Definition	Type
name	The entity name of the identified party - usually the business name from the corresponding national registry -eg ACME LTD	Text

SensorElement

> A SensorElement is used to carry data related to an event that is captured one sensor such as an IoT device. Include one sensor property and an array of sensor data values.

Property	Definition	Type
sensorMetadata	Data that describes the physical sensor that recorded the sensor data set.	Sensor
sensorReport	A list of sensor readings from the given sensor relevant to the traceability event context.	SensorData
sensorIntegrityProof	An optional reference to a verifiable credential signed by the sensor device or device manufacturer that contains the digitally signed raw data associated with this sensor report.	URI

Sensor

> A physical sensor that records a sensor data set.

Property	Definition	Type
device	The device Identifier for the sensor as a URI (typically an EPC)	Item
dataProcessingMethod	The data processing method used by the sensor - should reference a documented standard criteria as a URI	URI

SensorData

> A data point read by a sensor.

Property	Definition	Type
time	the timestamp at which the sensor reading was made.	DateTime
type	the measurement type of the sensor reading, as a URI reference to a measurement method specification.	URI
value	the sensor reading	Numeric
uom	the unit of measure for the sensor reading	Code (UOM)

Code Tables

actionCode

The Action type says how an event relates to the lifecycle of the entity being described. For example, AggregationEvent is used to capture events related to aggregations of objects, such as cases aggregated to a pallet. Throughout its life, the pallet load participates in many business process steps, each of which may generate an EPCIS event. The action field of each event says how the aggregation itself has changed during the event: have objects been added to the aggregation, have objects been removed from the aggregation, or has the aggregation simply been observed without change to its membership? The action is independent of the bizStep (of type BusinessStepID) which identifies the specific business process step in which the action took place.

Name	Description
observe	The entity in question has not been changed.
add	The entity in question has been created or added to.
delete	The entity in question has been removed from or destroyed altogether.

dispositionCode

Disposition code is a vocabulary whose elements denote a business state of an object. An example is a code that denotes “recalled”. The disposition field of an event specifies the business condition of the event’s objects, subsequent to the event. The disposition is assumed to hold true until another event indicates a change of disposition. Intervening events that do not specify a disposition field have no effect on the presumed disposition of the object.

```
Code values for this table can be found here:
https://ref.gs1.org/cbv/Disp
```

bizStepCode

BusinessStep is a vocabulary whose elements denote steps in business processes. An example is an identifier that denotes “shipping.” The business step field of an event specifies the business context of an event: what business process step was taking place that caused the event to be captured?

```
Code values for this table can be found here:
https://ref.gs1.org/cbv/BizStep
```

UOM

UNECE Recommendation 20 Unit of Measure code list.

```
Code values for this table can be found here:
https://vocabulary.uncefact.org/UnitMeasureCode
```

documentTypeCode

Document type codes for trade and logistics documents supporting the event such as purchase order, invoice, shipping notification, bill of lading, etc.

```
Code values for this table can be found here:
https://ref.gs1.org/cbv/BTT
```

Samples

Object Event


```
{
  "epcList": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "quantityList": [
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
  "eventTime": "2019-08-24T14:15:22Z",
  "action": "observe",
  "disposition": "string",
  "bizStep": "string",
  "bizLocation": "http://example.com",
  "sensorElementList": [
    {
      "sensorMetadata": {
        "device": {
          "itemID": "http://example.com",
          "name": "string"
        },
        "dataProcessingMethod": "http://example.com"
      },
      "sensorReport": [
        {
          "time": "2019-08-24T14:15:22Z",
          "type": "http://example.com",
          "value": 0,
          "uom": "string"
        }
      ],
      "sensorIntegrityProof": "http://example.com"
    }
  ]
}
```


Transaction Event

Note that the sensorElementList property exists in the transaction event but is not expanded in the sample below for brevity purposes.


```
{
  "sourceParty": {
    "partyID": "http://example.com",
    "name": "string"
  },
  "destinationParty": {
    "partyID": "http://example.com",
    "name": "string"
  },
  "epcList": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "quantityList": [
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
  "referenceDocument": {
    "type": "string",
    "identifier": "string",
    "documentURL": "http://example.com"
  },
  "eventTime": "2019-08-24T14:15:22Z",
  "action": "observe",
  "disposition": "string",
  "bizStep": "string",
  "bizLocation": "http://example.com",
  "sensorElementList": [..]
}
```


Aggregation Event

Note that the sensorElementList property exists in the transaction event but is not expanded in the sample below for brevity purposes.

```
{
  "parentEPC": {
    "itemID": "http://example.com",
    "name": "string"
  },
  "childEPCs": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "childQuantityList": [
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
  "eventTime": "2019-08-24T14:15:22Z",
  "action": "observe",
  "disposition": "string",
  "bizStep": "string",
  "bizLocation": "http://example.com",
  "sensorElementList": [..]
}
```


Transformation Event

Note that the sensorElementList property exists in the transaction event but is not expanded in the sample below for brevity purposes.


```
{
  "outputEPCList": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "inputEPCList": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "inputQuantityList": [
```

```
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
  "outputQuantityList": [
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
  "processType": "http://example.com",
  "eventTime": "2019-08-24T14:15:22Z",
  "action": "observe",
  "disposition": "string",
  "bizStep": "string",
  "bizLocation": "http://example.com",
  "sensorElementList": [..]
}
```

Association Event

Note that the sensorElementList property exists in the transaction event but is not expanded in the sample below for brevity purposes.

```
{
  "parentEPC": {
    "itemID": "http://example.com",
    "name": "string"
  },
  "childEPCs": [
    {
      "itemID": "http://example.com",
      "name": "string"
    }
  ],
  "childQuantityList": [
    {
      "epcClass": "http://example.com",
      "quantity": 0,
      "uom": "string"
    }
  ],
```

```
  "eventTime": "2019-08-24T14:15:22Z",
  "action": "observe",
  "disposition": "string",
  "bizStep": "string",
  "bizLocation": "http://example.com",
  "sensorElementList": [..]
}
```

Working Examples

TBC

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.

Overview

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.

VC Representation

Public Web Representation

Identity Credentials

Accreditation Credentials

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. 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).

Discoverability

The term 'data carrier' applies to all 1- and 2-dimensional barcode symbols and radio frequency tags. A very large number of data carriers are in use, including proprietary ones tied to specific apps. For UNTP, the important data carriers are those defined by ISO/IEC Joint Technical Committee 1, Steering Committee 31. These include different types of linear symbol most people think of as 'a barcode', as well as Data Matrix, QR Code and RFID tags. The standards for those data carriers do not define the type of identifier(s) that can be encoded so that, for practical purposes, it's necessary to also consider the origin and management of the identifiers to be encoded, the syntax to be used for that encoding, the devices and software necessary to print and read the data. It is this multi-layered complexity that makes "Automatic Identification and Data Capture" (AIDC) a professional activity in its own right.

Given this background, 'discoverability' itself has several aspects. It is reasonable to assume that someone inspecting goods in the course of their work will be equipped with a specialist device. This is

always necessary for RFID tags, the principal advantage of which is that hundreds, if not thousands, of tags can be scanned within a given volume, even without line of sight. But be aware that the device needs to be running software that can interpret the data it receives. Handheld optical scanners are also in common use and these will typically be able to read a very wide variety of optical symbols. But again, the key question is whether or not the software can interpret the data read from the carrier.

It hardly needs saying that the more standardized the identifiers and the encoding used, the more widely used the data carrier, and the more ubiquitous the software used to interpret the data read from the carrier, the more interoperable and therefore the more discoverable the identifiers will be. It is this kind of consideration that often leads industry to choose established identifier and data exchange systems such as that offered by GS1. That said, modern smartphones can read any almost any optical barcode and NFC tag *if* the user first opens an app that can interpret the data. This is true for proprietary data carriers and identifiers as well as standardized ones. Installing an app can readily turn a general-purpose smartphone into a specialist device. This opens up the option of using less-established identifier schemes and syntaxes including Decentralized Identifiers (DIDs). Then it's a question of whether the identifiers are equally disoverable at different points along the supply chain.

One case deserves special mention: a URL encoded in a QR Code. Almost all smartphone users can scan a QR Code just using the native camera app and, if the QR Code contains a URL, the Web browser will open the relevant Web page. This kind of identifier is therefore the most disoverable of all. That is, if a URL in the QR code is treated as the identifier then disoverability is a given. However, using a URL itself as the identifier brings some issues of its own. For example, over the medium to long term, many URLs suffer 'link rot' - that is, the URL no longer functions. Or if it does, it may lead to a Web page very different from the one originally intended. Furthermore, existing data exchange systems are likely to be built on short offline identifiers. ISO/IEC 18975 (currently a Draft International Standard) attempts to offer the best of both worlds by providing a means to encode existing identifiers into a data structure that is also a URL. Non-specialist software - notably a smartphone's camera app - can just read it like any URL. But specialist software can parse the URL to extract the identifiers used to identify products, batches and more.

Global Uniqueness

To be useful across a supply chain, identifiers must be globally unique. This can be achieved in a variety of ways

Issuing Agencies

Issuing Agencies act as a root that manages an identifier space. Examples include the internet domain name system, Digital Object Identifiers (DOIs), Legal Entity Identifiers (LEIs) and GS1 identifiers. In all these examples, the eventual identifier is created by appending a locally-defined string on the end of a prefix that is managed by the issuing agency that takes *its* authority from a central root. A well-known example is ICANN, which is the root authority for the internet domain name system. By renewable contract, they issue ".com" to Verisign who then license individual domain names under .com to others (usually via intermediaries). The licensee then creates their URLs under that domain name. Because ICANN is solely responsible for the internet's domain name system, global uniqueness is assured.

The same principle applies in all managed identifiers. For LEIs, GLEIF acts as the root authority that gives prefixes to its Local Operating Unit who then issue specific identifiers and so on.

ISO/IEC 15459 Issuing Agencies

In the world of Automatic Identification and Data Capture (barcoding etc), the ISO/IEC 15459 series of standards establishes a registry that acts as the root authority. Organisations that wish to issue identifiers that are intended to be encoded in barcodes and/or RFID tags are assigned a unique Issuing Agency Code that ensures their identifiers do not clash with any others. A further standard, ISO/IEC 15418, defines so-called *Data Identifiers* and *Application Identifiers* that "qualify" identifiers. It is this system that enables those Issuing Agencies to efficiently encode globally unique identifiers in optical and radio frequency data carriers without any duplication and for the print and scan industry to be able to create and interpret the barcodes and tags.

For example, the Data Identifier `2B` is for a *Gas Cylinder Container Identification Code assigned by the manufacturer in conformance with U.S. Department of Transportation (D.O.T.) standards*. The Application Identifier `01` is for a *Global Trade Item Number (GTIN)*. Data Identifiers are managed under the auspices of ANSI, Application Identifiers are managed by GS1.

Generated identifiers

As an alternative to being issued, identifiers can be algorithmically-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 many instances where duplicates have arisen (known as "collisions").

Decentralised Identifiers (DIDs) are also generated but the methods used vary significantly and typically depend on some piece of data that the originating person owns. This might be their private cryptographic key or some other extremely hard to guess piece of data. Collisions are all-but

impossible but the identifiers are usually significantly longer. The most widely used DID method is "DID Web" which uses the owner's internet domain name as the basis for identification, thus mixing the issued and generated philosophies with one advantage being that the resulting DIDs are short. It's important to note though that the primary purpose of a DID is to provide a means of proving control over the identifier and, having done that, retrieving the DID owner's public cryptographic key.

Resolvability

An identifier is nothing more than a string of characters. In isolation, it has no specific meaning. However, in most cases, the identifier will have a recognisable structure that gives a strong hint about its intended purpose and how it can be processed. In the context of UNTP, what's important is that the identifier can be *resolved* - that is looked-up online - and connected to a source of data, most notably, the identified entity's DPP. Approaches to resolving identifiers vary but a common feature is that it is typically a multi-stage process. Again taking the internet's domain name system as an example, an internet domain *resolves* to an IP address - the actual internet address of the server(s) that provide the content expected from that domain.

Decentralised Identifiers *resolve* to a "DID Document" - a small piece of data that includes the public cryptographic key for the DID's controller and, optionally, a list of servies related to that identitifier. At the time of writing, the established method for DID resolution is being formally standardised at W3C. An app is needed to recognise and resolve a DID, and to process the returned DID Document.

ISO/IEC (FDIS) 18975 defines a framework for resolving any existing identifier that is globally unique in its own right, most notably, those issued under the ISO/IEC 15459 series. It sets out two options for how those identifiers can be encoded in a regular HTTP URI (Web addrress), using Data Identifiers and Application Identifiers, and how that URI can resolve to a set of links to information about the identified entity. That linkset can be operationalised in a resolver. This defines a framework for creating a simple query interface for any identified entity. ISO/IEC 18975 enables identity issuing agencies to develop conformant standards that specify the following:

- The identifiers can be encoded in a URL within a QR Code printed on a product that can be scanned just using a mobile phone's camera, without any need for a specialist app. The user can select the DPP from the list of available links to information (i.e. manually select the correct link from the linkset).
- The identifiers can be encoded in a URL within a QR Code printed on a product that can be scanned using a specialist app that queries the resolver and returns the DPP.

The GS1 Digital Link and GS1-Conformant resolver standards conform to ISO/IEC (FDIS) 18975.

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 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.

Discoverable Public Data

Public Data with GUID key

Encrypted Data with Shared Key

Encrypted Data with Requestable Key

Selective Redaction

Private Data

Usage Patterns

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.

Overview

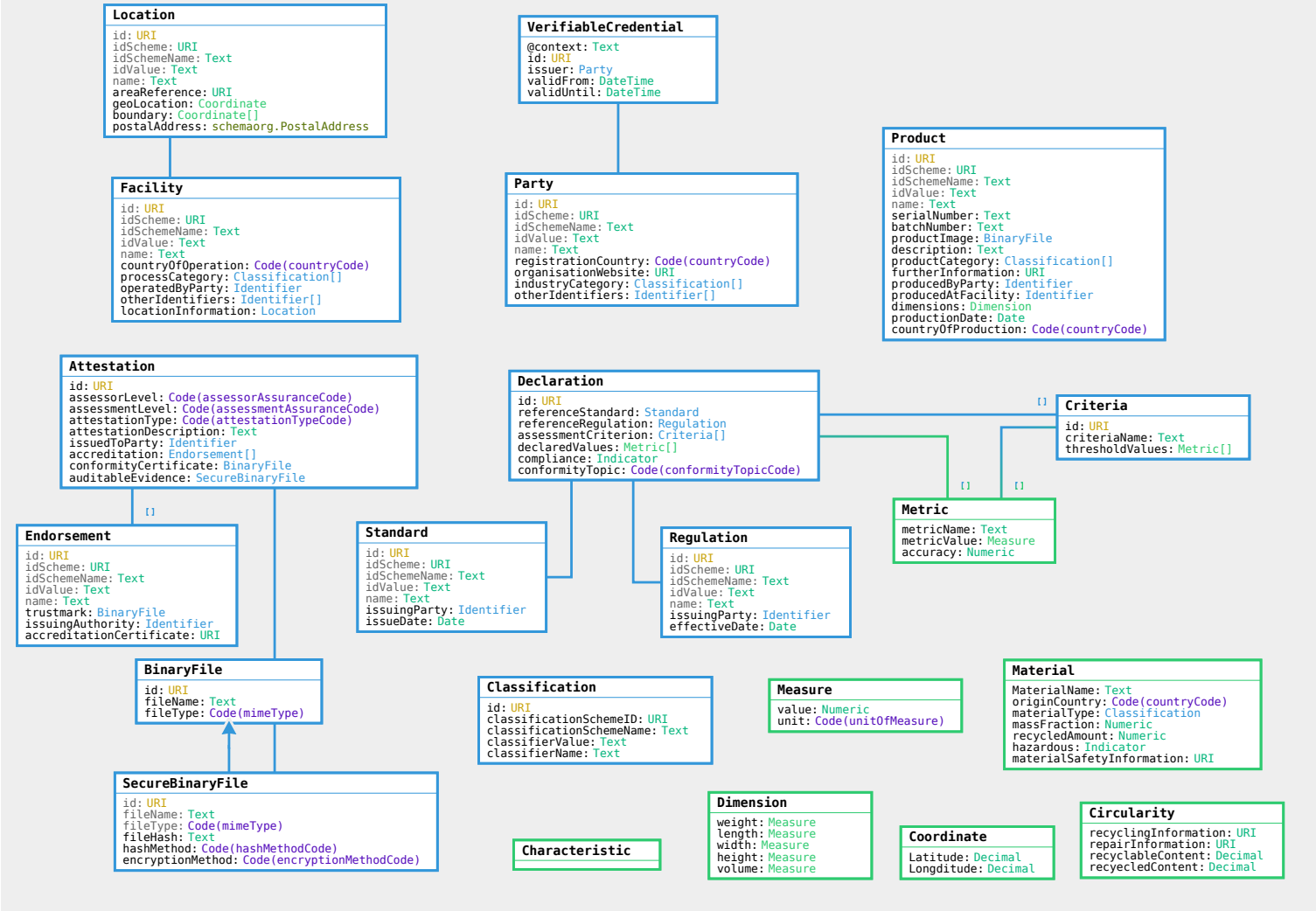
Web **vocabularies** are a means to bring consistent understanding of **meaning** to ESG claims and assessments throughout transparent value chains based on UNTP. There are hundreds of ESG standards and regulations around the world, each with dozens or hundreds of specific conformity **criteria**. Any 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, Locaiton, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the buuilding 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 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 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 latest draft untp core vocabulary is published as a JSON-LD graph at UNTP Core Vocabulary

UN ESG Topic Map

TBC

Sustainability Vocabulary Catalog

TBC

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 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 "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.

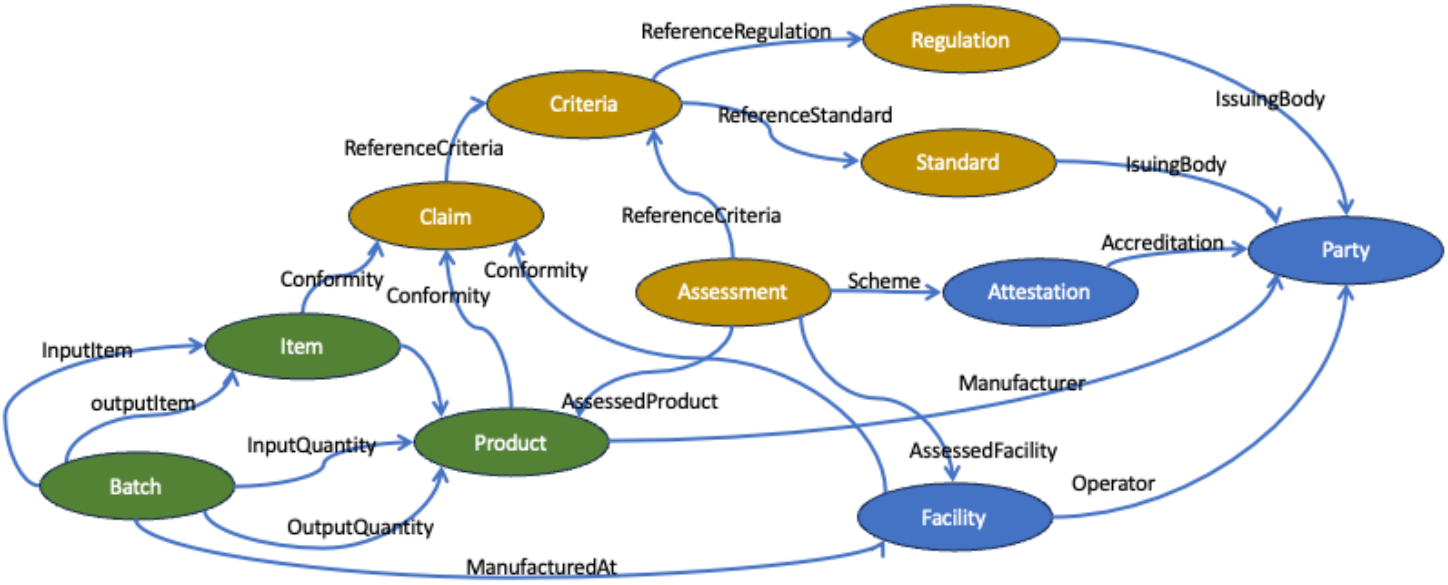
Transparency Graphs

The UNTP core vocabulary defines the uniquely identified linked data entities such as Product, Locaiton, Facility, Party, Standard, Regulation, Criteria, Declaration, Attestation, Endorsement. These entities provide the buuilding 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 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 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.



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

Mass Balance

> **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 (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

> **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 Guidance

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.

For Buyers and Suppliers in the Value Chain

For Registry Operators

For Conformity Assesment Bodies

For Industry Associations

For Regulators

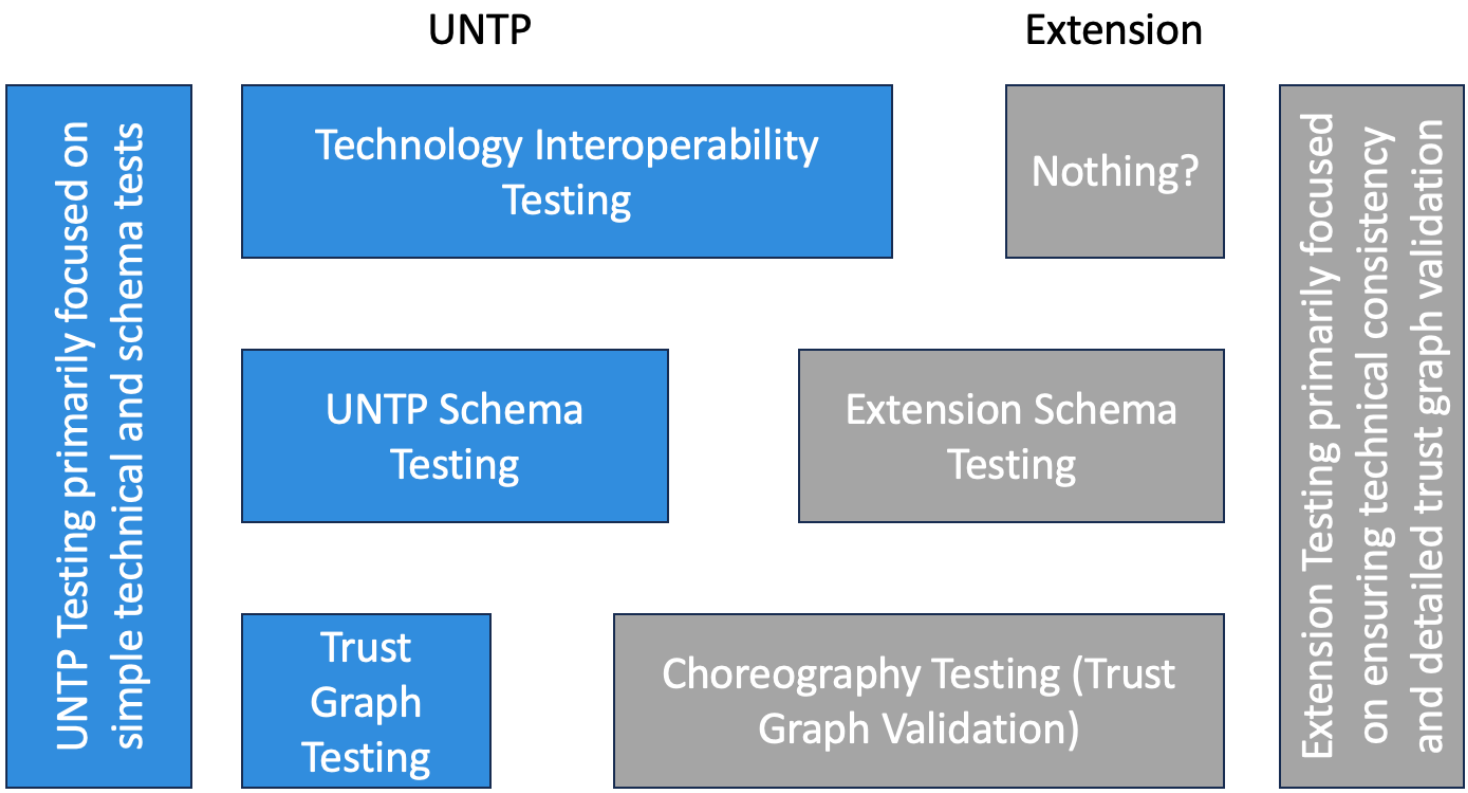
For Software Vendors

Test Services

> **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.

Help and 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.

Implementation Support

Reference Implementation

> **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,	Active Development

Tool	Link	Description	Status
		correct schema, and correct choreography)	

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.

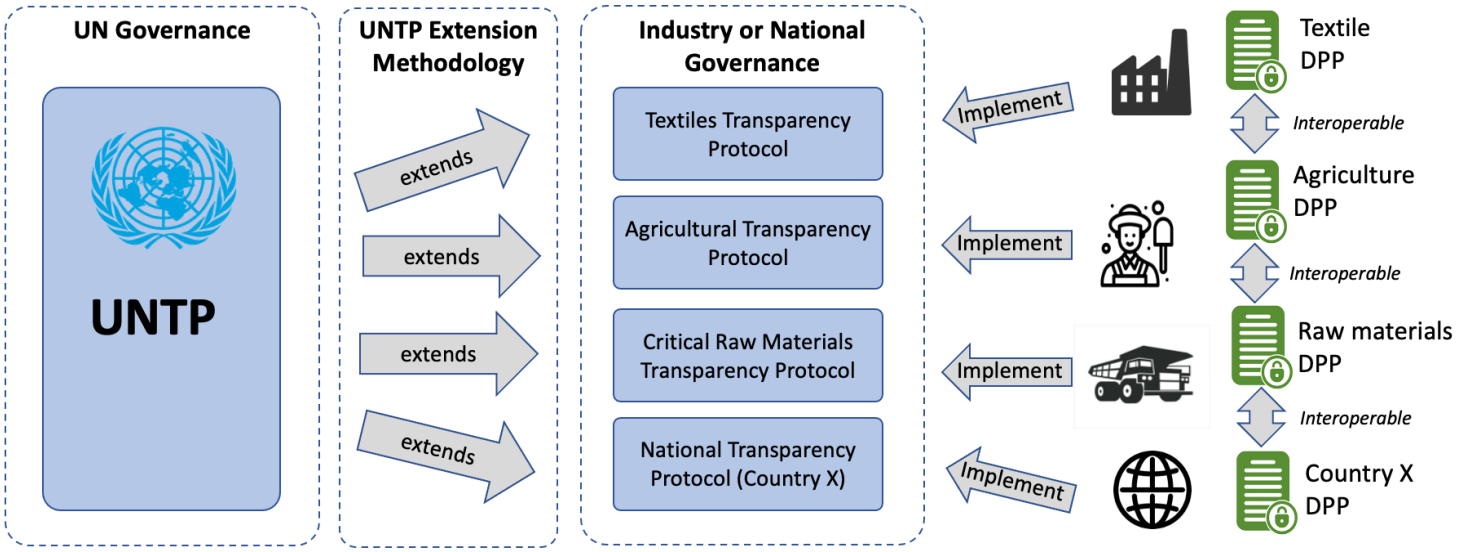
Extensions Register

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 extnesions 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.

To be registered as UNTP conformant, an extension MUST remain interoperable with UNTP. This is achieved by limiting extensions to the extension points described below and be completing interoperability testing.

Extension Points

Schema Extensions

Vocabulary Extensions

Identifier Extensions

Choreography Extensions

Testing Extensions

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

Implementations Register

Implementation Conformity

Implementations Register