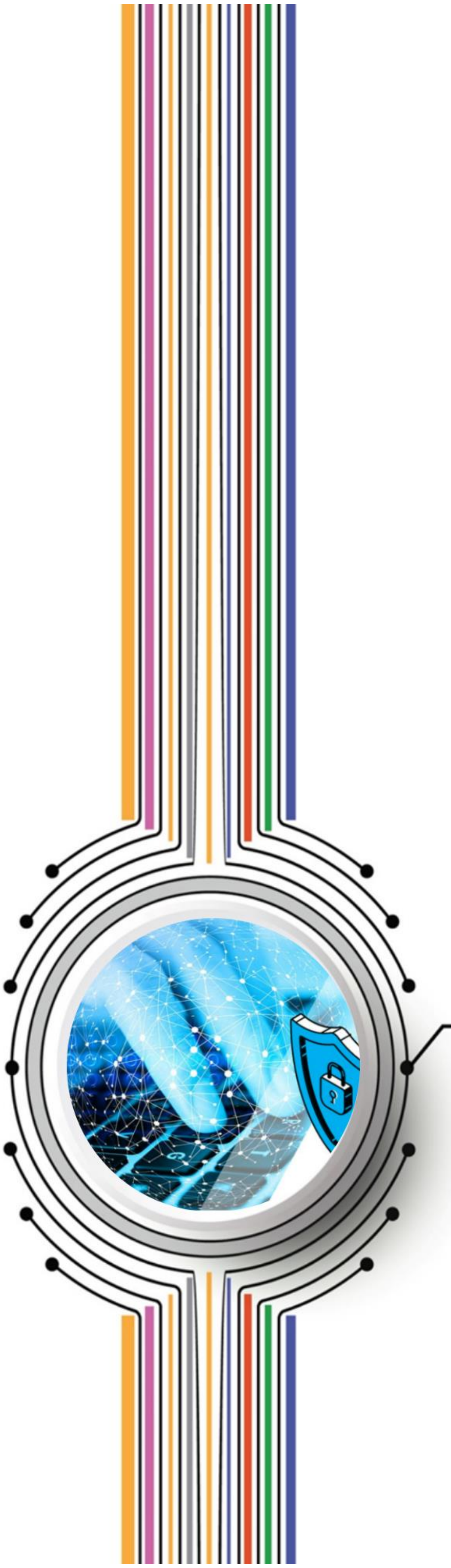


UNECE
UN / CEFACT

White Paper

eDATA Verifiable Credentials for Cross Border Trade

September 2022

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

This document was prepared under the leadership of United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) eDATA management Domain Coordinator Kaushik Srinivasan with the guidance of UN/CEFACT Vice Chair Tahseen Ahmad Khan; with support Maria Rosaria Ceccarelli, Chief of Trade Facilitation Section, in the United Nations Economic Commission for Europe (UNECE). ECE hosts UN/CEFACT, which develops standards and best practices for trade facilitation and electronic business. The project leadership would like to thank the following experts who contributed in their private and professional capacity to make this paper possible: Steven Capell (project lead and editor), Dr Wang Xiang (co-lead), Ian Watt, Nis Jespersen, Peter Carter, Ren Yuh Kay, Sin Yong Loh, Rudy Hemeleers, Virginia Cram-Martos, Phil Archer, Cheryl Wong, Kseniya Shychko, Serena Koh, Geoffrey Bowering, Sue Probert, Marek Laskowski, Chris Gough.

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)

Simple, Transparent and Effective Processes for Global Commerce

The mission of UN/CEFACT is to improve the ability of business, trade and administrative organizations from developed, developing and transitional economies to exchange products and relevant services effectively. Its principal focus is on facilitating national and international transactions through the simplification and harmonization of processes, procedures and information flows in order to contribute to the growth of global commerce.

Participation in UN/CEFACT is open to experts from United Nations Member States, intergovernmental organizations and non-governmental organizations recognized by the United Nations Economic and Social Council (ECOSOC). Through this participation of government and business representatives from around the world, UN/CEFACT has developed a range of trade facilitation and e-business standards, recommendations and tools that are approved within a broad intergovernmental process and implemented globally.

www.unece.org/cefact

Table of Contents

1 EXECUTIVE SUMMARY

The international supply chain is growing in complexity at the same time as nation states seek to improve their border compliance for imports and facilitate access to export markets for their domestic producers. The global value chain is highly dependent on smooth cross-border supply flows (tangible, intangible and data). In an uncertain world that is buffeted by rapid technological change, environmental and health crises, and political uncertainties, national policies can have significant impacts on cross border trade challenges[1].

- The "cost of trade"[2] roughly doubles the landed price of goods in export markets (compared to domestic wholesale prices) with around one third of that cost related to non-tariff border costs. Nations that can reduce their cost of trade with their trading partners will confer a significant comparative advantage for their exporters and thereby improve the national balance of trade.
- At around $1.7 trillion[3], the trade finance gap (i.e., trade finance requested but not approved) is heavily weighted against small and medium enterprises (SMEs) and acts as one of the most significant barriers to SME participation in cross-border trade. Nations who can uplift SME participation rate in cross border trade will experience greater growth and improved balance of trade.
- At around 3 per cent of world trade volume[4], the value of fake / illicit goods trade is at least $600 billion and rising. The consequences include market losses for exporters of genuine goods and potential reputational damage for entire market segments. Nations who can help their exporters prove the authenticity of goods will enjoy a comparative advantage over those that do not.
- With annual carbon emissions at around 25 billion tons[5] and with approximately 25 million people in forced labour[6], and 400 million tons of hazardous waste produced annually[7], there is a rapidly increasing consumer demand for sustainable products. Nations that can prove the sustainability of their exported goods through verifiable supply chain transparency will enjoy both higher prices for their goods and lower tariffs as importing nations start to penalize un-sustainable imports.
- With border authorities only able to inspect around 1 per cent of around 1 billion sea containers[8] and a much smaller proportion of 100 billion parcel shipments[9] per year, the challenge of managing border risk against illicit goods and biosecurity threats has never been greater. Nations that can leverage high integrity data about import consignments can both increase seizures and facilitate legitimate imports.

The challenges described above are quite significant. Equally, the opportunities for nations that can address these challenges more effectively than their competitors are also significant. Digitisation is a key enabler of all strategies to address these challenges. Although many nations have made significant progress in digitizing trade processes within their borders such as implementing trade single windows, there remain significant challenges in digitizing cross-border processes.

Diverse regulatory models and priorities across nations amplify the challenge. National policy making will reflect a complex mixture of market-oriented, security-oriented, rights-oriented, and domestic development-oriented priorities. These differences lead to problems of compatibility or interoperability among nations, and fragmentation of the digital space at the global level[10]. Any scalable solution to the digitisation of cross border trade must embrace and not conflict with diverse policy making priorities.

This paper describes a highly scalable operating model for digitisation and trust of cross border trade based on verifiable credentials, linked data, and decentralised identifiers. It provides national regulators with implementation guidance that will facilitate the following outcomes.

[1] https://www.wto.org/english/res_e/booksp_e/wtr21_e/00_wtr21_e.pdf
[2] https://www.unescap.org/resources/escap-world-bank-trade-cost-database
[3] https://www.adb.org/publications/2021-trade-finance-gaps-growth-jobs-survey
[4] https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm
[5] https://ourworldindata.org/co2-emissions
[6] https://www.globalslaveryindex.org/2018/findings/global-findings/
[7] https://www.theworldcounts.com/challenges/planet-earth/waste/hazardous-waste-statistics
[8] https://data.worldbank.org/indicator/IS.SHP.GOOD.TU
[9] https://www.statista.com/statistics/1140055/parcel-shipping-volume-worldwide-country/
[10] https://unctad.org/system/files/official-document/der2021_en.pdf

- Full and rapid digitisation of all exports without any dependency on trading partner readiness. This is because the framework supports the seamless blend of human readable and digital data so that exporting nations can go 100 per cent digital whilst their trading partner nations can adopt digital processes at their own pace.
- Traceability through the supply chain. By linking the export document and product labels to digital evidence created earlier in the supply chain, a linked data graph of verifiable documents can be created. Importers & consumers can follow the links to verify that what is stated on the product label is true. Importing regulators can independently and digitally verify that their compliance criteria are met.
- Automated compliance and risk. As exports are increasingly digitised, importing regulators can leverage the digital chain of trust to automate compliance assessments. This will reduce border costs for goods with strong digital credentials and improve risk targeting because border authorities can focus their efforts on imports with lower or unknown trust. Similarly, banks can automate their risk assessments and consequently lower the costs of trade finance, allowing small exporters to compete on more equal terms with their larger competitors.

The role of regulators in this model is to provide trust anchors. For example, a national trademarks office can issue digital proofs that an identified producer is indeed the owner of a trademark, allowing that producer to attach verifiable authenticity claims to their exported products.

The decentralised nature of the model means that every trade document in can be issued by a different party or authority using tools and systems of their choice. With no dependency on centralised systems, market innovators can successfully occupy a niche. Regulators act as the catalyst for market innovation within their economies.

A similar pattern is seen with the emergence of digital vaccination passports in response to the COVID pandemic. The vaccination passport is issued by a national competent authority to the person who has been vaccinated. The person carries the vaccination passport with them in both paper and digital forms, and can present it to any verifier (e.g., border, airline, or any venue) who can confirm the integrity of the document without contacting the issuer. A few different physical implementations such as International Civil Aviation Organization (ICAO)[11], The EU Digital COVID Certificate (EUDCC)[12], New Zealand COVID Pass (NZ COVID Pass[13]) have emerged but all follow the same pattern. An e-passport is also an example of the same pattern, allowing the holder to prove their identity to digital readers at airport smart gates or even to a verifier with a smartphone[14]. The message of this white paper is that any cross-border trade document can also be managed using the same decentralised digital trust architecture. Like the chip in an e-passport or the QR on a COVID vaccination record, trade documents can be digitised and verified at scale whilst still retaining compatibility with paper-based processes.

The chapters in this paper are designed to take the reader from concept to implementation. Chapter 2 explores and quantifies the current challenges and opportunities in the international supply chain in more detail, thereby providing the business case for change. Chapter 3 describes the key technology innovations that power the decentralised future using non-technical language and plentiful analogies, providing business leaders and policy makers with the confidence to support the case for change. Chapter 4 articulates implementation best practices that support the transition to successful implementation, avoiding pitfalls and mitigating risks. Chapter 5 provides several business use-cases so that all stakeholders can glimpse the future through realistic examples.

Verifiable credentials and decentralised identifiers represent an opportunity for nations to quickly go 100 per cent digital, improving both export market access and border security.

[11] https://www.icao.int/Newsroom/Pages/ICAO-VDS-gains-acceptance-for-global-health-proof-verification.aspx

[12] https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

[13] https://nzcp.covid19.health.nz/

[14] https://www.forbes.com/sites/jumio/2020/09/10/its-time-to-jump-on-the-e-passport-bandwagon/?sh=113134d042c9

2 BUSINESS DRIVERS

2.1 The cost of trade is high

With global trade volumes above $20 trillion in 2020, even small changes in the cost of trade can have very significant impact for exporting economies. There is significant variation in trade costs across countries.

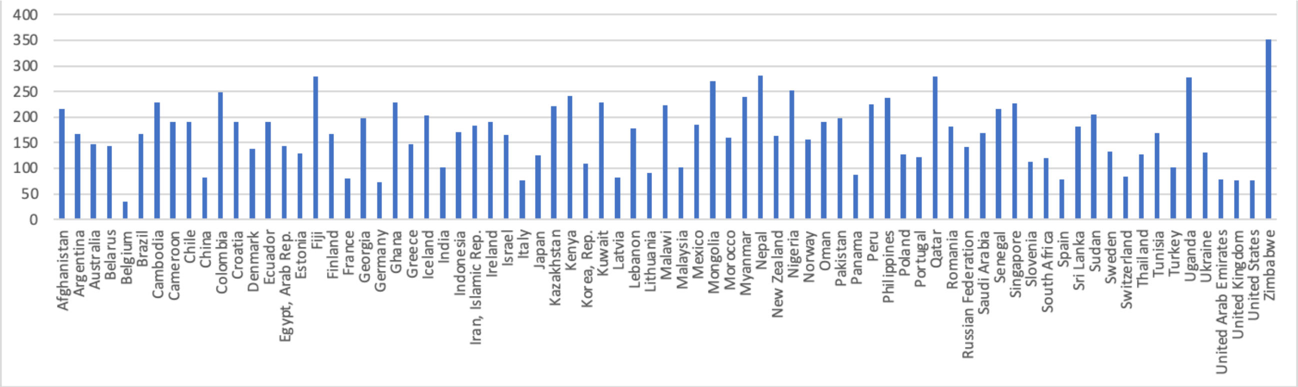


Figure 1 Cost of trade by country

A frequently cited paper from 2004 by Andersen and Wincoop[15] brings some science to the analysis of cross-border trade costs. Broadly, the cost of trade is measured by comparing the cost of goods trade internationally with the cost of the same goods traded domestically.

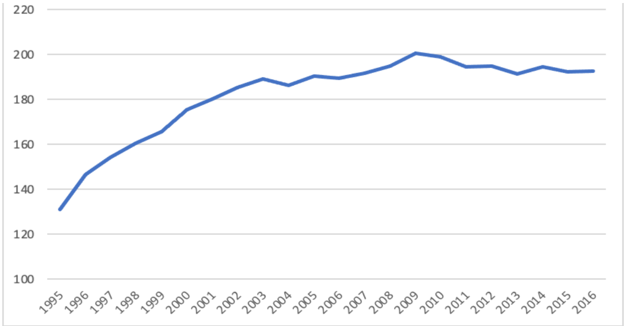


Figure 2 - cost of trade global average by year

The Economic and Social Commission for Asia and the Pacific (UNESCAP) and the World Bank have maintained a database[16] since 1995 of the cost of trade per bilateral relationship for manufactured and agricultural goods. We can see that the cost of trade rose gradually from 1995 till 2008 and then levelled off. However, it remains very high – at just under 100 per cent (i.e., goods cost double from domestic to international markets) for industrialised economies and is much higher for many developing economies.

A 2007 paper[17] published by UNESCAP analysed how the cost of trade breaks down and found that:

- Just under half of the cost of trade is retail & wholesale distribution costs (i.e., intermediary markup);
- Approximately 20 per cent of the cost of trade is international freight and transit transport costs;
- The remaining 30 per cent is traceable to various border related barriers including tariffs, compliance, currency, language, information and security. Only a small proportion are tariffs.

The lesson here is plain to see. Trade costs add significantly to the landed cost of goods in export markets. If countries A and B both export the same commodity to country C, but A->C trade costs are 10 per cent higher than B->C trade costs then producers in country A will need to have 10 per cent lower prices to remain competitive. A mid-sized economy that exports $300 billion of goods per year can expect to increase export volumes (and hence balance of trade) by a few billion dollars for every percentage point advantage in comparative cost of trade with their competitor nations. A 2014 UNESCAP policy brief [18] estimates the benefit to the APAC region to be over $250 billion in increased export volumes through trusted digitisation of origin certificates, phytosanitary certificates, and trade finance letters of credit. This paper includes guidance for policy makers on exactly these use cases and how to implement them with verifiable credentials.

[15] NBER working paper "Trade Costs" https://www.nber.org/system/files/working_papers/w10480/w10480.pdf
[16] https://www.unescap.org/resources/escap-world-bank-trade-cost-database
[17] https://www.unescap.org/resources/impact-trade-costs-trade-empirical-evidence-asian-countries-awp-no-27
[18] https://www.unescap.org/resources/estimating-benefits-cross-border-paperless-trade

2.2 Access to Trade finance is a barrier to trade

Trade finance refers to the financial instruments and products that companies use to facilitate international trade. The most common products are letters of credit and insurance. Letters of credit guarantee payments to sellers when goods are verifiably shipped. The World Trade Organization (WTO) estimates[19] that 80 per cent to 90 per cent of world trade relies on trade finance.

The Asian Development Bank (ADB) estimates that global trade finance gap (i.e., finance that is requested but not provided) at $1.7 trillion[20]. The gap is disproportionately weighted towards smaller businesses and lower value shipments with rejection rates well over 50 per cent.

The Organisation for Economic Co-operation and Development (OECD) found SMEs contribute around 60 percent of goods traded and represent 80 per cent of consignments shipped[21]. Therefore, improving the availability of trade finance to SMEs (and hence to export markets) can have a large impact on national balance of trade.

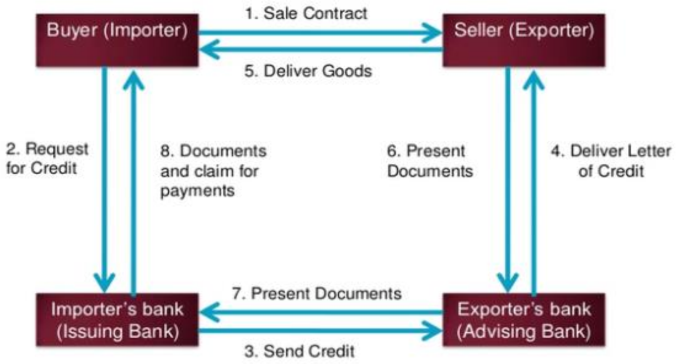


Figure 3 - Letter of credit procedure

Current trade financing challenges include addressing the uncertainty of the identification of the end-to-end trade parties involved, the poor quality of the trade data, and the profitability of the deal to the bank. The ADB survey is the world's leading barometer of trade finance health and includes 79 banks and 469 firms, covering all regions of the world.

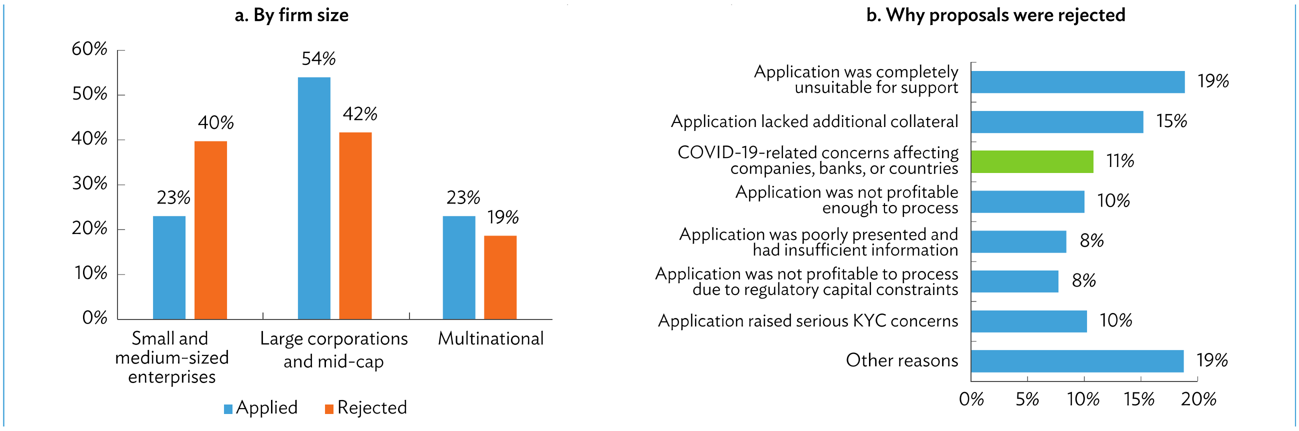


Figure 4 - ADB 2021 Trade Finance Access Gaps

Weaker balance sheets and macroeconomic uncertainty during the pandemic enlarged the gap. Regulations designed to curb money laundering and fraud continued to inadvertently pose obstacles to servicing trade finance needs. To close the gap, the report recommends increased digitisation and greater coordination with the private sector as well as global agreement on common standards, practices, and legislation.

This report will show how verifiable credentials can be used to increase identity confidence (thereby the reducing KYC based rejections), increase document integrity (reducing rejections due to inadequate or unverifiable supporting documents) and potentially allow banks to automate low value applications through algorithmic due-diligence (improving profitability of low value finance for banks).

[19] https://www.wto.org/english/thewto_e/coher_e/tr_finance_e.htm
[20] https://www.adb.org/publications/2021-trade-finance-gaps-growth-jobs-survey
[21] https://www.oecd.org/cfe/smes/Highlights-Financing-SMEs-and-Entrepreneurs-2018.pdf

2.3 Illicit & Counterfeit goods are increasing

There are very strong commercial incentives to manufacture and sell fake versions of high value products such as fashion brands and medicines. There are also very strong incentives to smuggle real products such as cigarettes into markets with very high taxes.

- OECD estimates[22] that in 2019, counterfeit goods represented about 2.5 per cent of world trade at around USD $464 billion in value.
- The World Health Organization (WHO) estimates[23] that 1 in 10 medical products sold in low & middle income countries are fake.
- Nearly 12 per cent of the global cigarette market is illicit[24], representing over $40 billion in lost tax revenue and tens of thousands of lives lost.
- Last year, Australian authorities alone made over 214,000 illicit tobacco seizures[25] including 827 tonnes of loose-leaf tobacco and 598 million cigarettes, with an excise value of $1.92 Billion.
- United Nations Office on Drugs and Crime (UNODOC) 2020 report[26] shows that around 20,000 Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) seizures were made in 2017 alone, representing the tip of an iceberg of illicit trade in endangered plants and animals.
- The UNODC world drug report 2021[27] estimates that size of the global illicit drug trade at over $200 billion and reports seizures of 45 tons of amphetamine-type stimulants (ATS) and 4500 tons of cocaine.

The Word Customs Organisation (WCO) Illicit trade report 2021[28] provides some interesting metrics on the number and size of seizures (left panel) and tobacco specific metrics (bottom).

When considering the potential impact of digital verification, it is important to distinguish between illicit trade where both buyers and sellers are acting outside of legal markets (e.g., drug trade), and illicit trade where sellers are injecting their illicit product into licit markets (e.g., tobacco and fake pharmaceuticals). In general, digital traceability and integrity solutions will have a much bigger impact in markets where legal consumers are motivated to detect and avoid fake goods (e.g., tobacco & brands) and rather less in purely illicit markets such as drugs.

This paper provides use cases and guidance on tackling illicit trade and counterfeiting using verifiable credentials - with use cases for tobacco tracing and CITES permits.

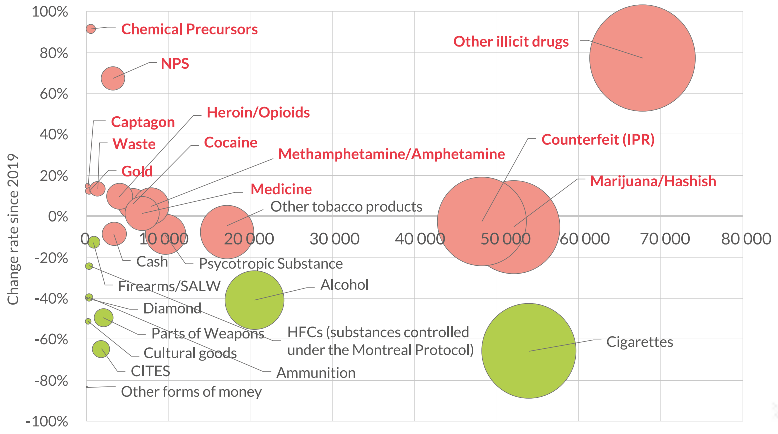


Figure 5 - Value & quantity of seizures

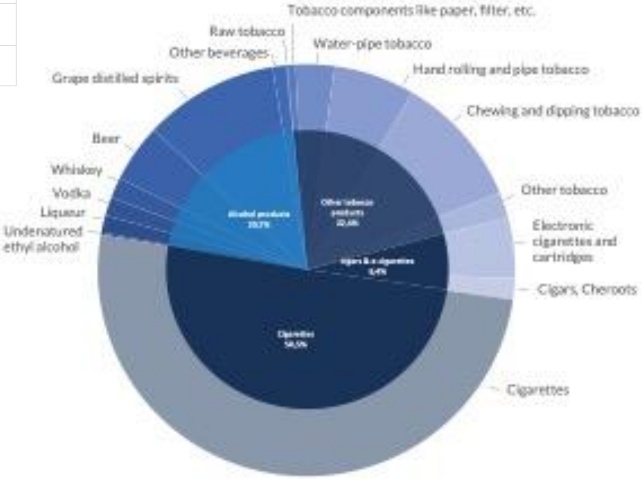


Figure 6 - seizure volumes by type of product

[22] https://www.oecd.org/publications/global-trade-in-fakes-74c81154-en.htm

[23] https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

[24] https://www.tobaccofreekids.org/assets/global/pdfs/en/ILL_global_cig_trade_summary_en.pdf

[25] https://minister.homeaffairs.gov.au/jasonwood/Pages/abf-seizes-record-amount-of-illicit-tobacco.aspx

[26] https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf

[27] https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html

[28] http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2021_en.pdf?db=web

2.4 Consumers demand sustainability

Unsustainable or unethical development practices are having increasingly obvious impacts on the environment and on social welfare.

- United Nations Environment Programme (UNEP) estimates[29] that 80 per cent of wastewater from household and industrial usage in inadequately treated. 3.5 million tons of annual pesticides runoff are impacting health biodiversity[30].
- The world consumes around 4 trillion cubic metres of fresh water per year, around 70 per cent of which is for agriculture[31]. 24 per cent of that water consumption exceeds local replenishment rates[32].
- The 6th report of the Intergovernmental Panel on Climate Change (IPCC)[33] indicates annual COs emissions at 60 gigatons and growing.
- 3.75 million hectares[34] (MHa) of primary (old growth) forest was lost in 2021. 68 MHa or 7 per cent of world coverage has been lost since 2002 - primarily to agriculture and forestry.
- The world consumes about 200 million tons of seafood per year[35]. The Food and Agriculture Organization (FAO) estimates that 80 per cent of the world's fisheries are over-exploited[36].
- The International Labour Organization (ILO) estimates that 40 million people[37] (5.4 in every 1000) are victims of modern slavery and that 71 per cent are women and girls.

In addition to the environmental and social impacts, many governments are increasingly concerned about supply chain integrity in the context of geopolitical risks and are taking steps to ensure continued supply of critical resources such as food, energy, critical minerals, and electronic components during conflicts.

Consumers are increasingly demanding products that are sustainably produced and are willing to pay price premiums for such products. In response, standards bodies and regulators have developed measurable criteria against which products can be assessed and certified. The International Trade Centre (ITC) standards map[38] provides a useful map of such standards. Anti-modern slavery legislation has been enacted in several countries. The European Union (EU) is preparing legislation[39] that will require EU businesses to prove sustainability of their supply chains.

The key to sustainable supply chains is transparency. Buyers, including end consumers, should have visibility of the supply chain from primary producer to finished product. The mechanism to achieve transparency is end-to-end traceability - from cotton farm to T-shirt or from lithium mine to electric vehicle together with verifiable evidence of sustainable practices at each step.

End-to-end traceability is an easily stated goal but faces significant challenges in implementation.

- As price premiums for verifiably sustainable produce increase so the incentive for fraud increases. Fraud vectors include fake certificates, fake products, fake origin criteria, and mass-balance fraud (e.g., claiming 100 per cent organic cotton fabric when only 10 per cent of your supply is verifiably organic).
- Providing full supply chain visibility would expose supplier and customer lists that are often commercially sensitive – imposing a disincentive for participants to engage.
- A plethora of non-interoperable technology solutions to traceability are emerging. But no single platform can ever achieve the geographic or market segment footprint to cover an end-to-end complex supply chain. A scalable traceability solution must be designed from the ground up to work in a highly decentralised environment that includes hundreds or thousands of information systems.

[29] https://www.unep.org/explore-topics/chemicals-waste/what-we-do/policy-and-governance/global-chemicals-outlook
[30] https://foodprint.org/issues/pesticides/
[31] https://ourworldindata.org/water-use-stress
[32] https://pubs.acs.org/doi/abs/10.1021/acs.est.0c01544
[33] https://www.ipcc.ch/report/ar6/wg3/
[34] https://gfw.global/3OHe9ie
[35] https://ourworldindata.org/fish-and-overfishing#global-fish-production
[36] https://www.un.org/depts/los/convention_agreements/reviewconf/FishStocks_EN_A.pdf
[37] https://www.ilo.org/wcmsp5/groups/public/@dgreports/@dcomm/documents/publication/wcms_575540.pdf
[38] https://www.standardsmap.org/en/identify
[39] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1146

This paper provides guidance on how verifiable credentials, decentralised identifiers, and standard semantic vocabularies can solve the supply chain traceability problem across multiple platforms whilst protecting sensitive data and providing strong cryptographic integrity against fraud.

2.5 Regulators seek to reduce risk & automate compliance

Regulators are fighting a constant battle against illicit goods, duty evasion, and border risk (biosecurity, counter-terrorism, etc.). Seizure rates remain stubbornly low, especially for containerised sea freight. Published metrics[40] from a mid-sized economy such as Australia's reveals that

- Approximately 1 per cent of around 60 million imported cargo items are inspected and 500 tons of Illicit tobacco and 20 tons of illicit drugs are seized at the border each year.
- Approximately 0.1 per cent of around 6 million import declarations are audited and $60 million of under-reported duty revenue is collected each year.

Inspections and audits performed by customs authorities are based on risk targeting and so these seizures and revenue recovery figures cannot be simply extrapolated. Nevertheless, it is reasonable to expect that further volumes of illicit goods and revenue leakage goes un-detected. At a global scale, the volumes will be much higher with the greatest volumes likely to occur where there is the greatest opportunity for criminal gain – which means developed economies will face higher proportion of illicit goods imports whilst developing economies will face higher duty evasion.

Customs authorities have a variety of tools to assist with risk targeting and thereby increase seizure rates. However, access to more detailed and higher integrity supply chain information is key. There is also a trend towards risk assessing the trading entities rather than only the consignment information. This is facilitated through schemes like the WCO Authorised Economic Operator (AEO) framework where customs authorities distinguish between known and trusted traders (who face less inspections and faster clearance) and unknown or un-trusted traders (where greater analysis and inspections may yield better seizure rates).

One challenge with any scheme that reduces inspections on trusted operators is to ensure that the consignee/consignor really is the trusted operator. A common practice used by smugglers is to masquerade as trusted parties (aka "piggybacking") to avoid inspections. Accordingly, any entity-based compliance schemes can only work well when there is high confidence in the identity of traders. Since most import declarations are lodged by agents and not the importer, there is usually no direct authentication of importer identity. Worse still, the exporter / consignor in the other country is often identified with little more than a claimed trading name and is un-verifiable in the importing jurisdiction.

The duty evasion problem is exacerbated by the fact that most import declarations are self-assessments of duty payable made by the importer or their agent. Manual auditing of supporting documentation such as commercial invoices is expensive and, to a determined duty evader, may not help because the invoices themselves are easily faked.

A future "nirvana" for customs authorities would draw on digitally verifiable trade and transport documents such as the digitally signed commercial invoice from the offshore supplier and the electronic bill of lading from transport service providers. Trader identities in both countries would be cryptographically verifiable and actual consignment/shipment information drawn from the source of truth, making piggy backing and duty evasion much more difficult. When based on global standards (such as UN/CEFACT documents and data models) and when coupled with Artificial Intelligence (AI) based analysis of commercial data (for example, to auto-classify tariff codes), there is a plausible future where a customs authority might say "just give me your digital invoice and I'll tell you how much duty to pay".

Decentralised identifiers (DIDs) provide a uniquely scalable way to provide cross border identity assurance and verifiable credentials (VCs) provide a significant increase in the integrity of trade documents such as commercial invoices. This document provides guidance for regulators on the use of DIDs & VCs to achieve increased border compliance.

[40] https://www.abf.gov.au/importing-exporting-and-manufacturing/trade-and-goods-compliance/goods-compliance-update

2.6 Some solutions exist but are hard to scale

Digital data exchange and cryptographic processes such as signatures are far from new technologies. The sceptical reader may well ask "So what's new? Why are verifiable credentials different?". This section contrasts the decentralised (verifiable credentials) architecture to two other architectures for digital data exchange, highlighting the challenges and advantages of each.

Peer to peer architecture. In this model, messages are exchanged over a secure pipe between two parties. This is the typical EDI model for B2B (Business-to-Business), G2G (Government to government), G2B (Government to Business) and other data exchange. The two parties exchange security tokens to identify each other and these are used to secure the physical connection. All parties are technologically mature and must make some investment to setup their connections. This model works well for high volume exchanges between a small number of parties that already know and trust each other. It is more difficult for low maturity participants and does not easily accommodate third parties that need access to the same data.

Shared hub architecture. In this model, all parties connect to a central data hub and exchange data with the hub. Typical examples are trade single windows or port community systems. Data exchange can be either manual (via a user interface) or automated via APIs (Application Programming Interface). In all cases, each party must register with the hub and receive an identity token. This model works well when the hub represents an existing identifiable community where the hub has a natural monopoly so that each party can complete most of their business on a single hub. It does not scale well for processes that cross geographic or industry sectors because no single hub has such a large footprint (it would be an un-natural monopoly if it did). The consequence of attempting to implement a hub architecture across borders and sectors is usually a "plethora of platforms" where participants would need to pre-register with an infeasibly large number of platforms to get their job done.

Decentralised architecture. In this model, trade documents are self-issued as "verifiable credentials" by traders (e.g., invoices, way bills) or issued by a competent authority (e.g., certificates & permits) to the trader who stores them in their own systems. Less mature issuers & holders may use hosted apps and wallets. The documents are digitally signed by the issuer using an identity created and owned by the issuer (a.k.a self-sovereign identities). The digital documents typically also have a human friendly view that looks like the paper equivalent (but with a QR code that links to the encrypted digital version). The documents are exchanged via any convenient method (email attachment, portal upload, API automation, even as a QR printed on the corresponding goods). The exchange method is not important because the security is built into the document itself. Any party that receives a document can verify its integrity and confirm the identity of the issuer. There is no dependency between issuer and verifier. This model works well for long supply chains where each party "just does their job". There are no centralised hubs nor any need for EDI connections.

A useful analogy for the decentralised architecture is the e-passport. It is a credential issued to a holder (citizen) by a trusted authority (a government). The chip in the e-passport contains the biometric and biographic data of the holder and is digitally signed by the issuing government. The holder travels with his/her passport, presenting it whenever identity verification is requested. Advanced verifiers such as border authorities can operate smart-gates that extract the data, verify the signature, and compare the photo of traveller with that on the chip. Less mature verifiers such as hotel check-in clerks can just look at the paper document and, if they have a suitable phone app, also verify the chip data. A verifiable credential is like an e-passport, but for any trade document.

The unique scalability feature of verifiable credentials is the decoupling between issuer and verifier. Issuers can just go 100 per cent digital at any time of their choosing without any dependency on other stakeholders to invest in Electronic Data Interchange (EDI) connections or register on hubs. Verifiers can stick to paper-centric processes or can upgrade to automated data extraction and verification at any time of their choice.

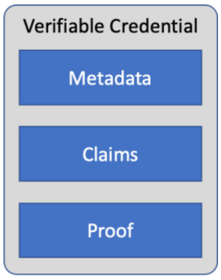
3 VERIFIABLE CREDENTIALS

3.1 What is a verifiable credential?

The World-Wide-Web Consortium (W3C) Verifiable Credential (VC) standard[41] says:

> *Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.*

A VC has three key parts:



A standard header that contains information like the credential type (e.g., a degree certificate), issuer identity (e.g., Oxford University), subject identity (e.g., John Smith), issue date (e.g., July 1990).

A set of one or more claims (e.g., that John has a first class honours in electrical engineering).

A cryptographically verifiable proof that the VC has not been tampered with and the issuer (and optionally the subject) are who they say they are.

A VC is issued to a holder (who is also usually the subject), who can present it to any verifier.

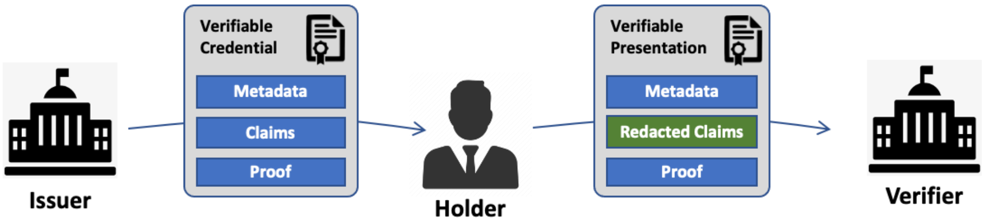


Figure 7 - Verifiable Credentials

VCs have some very important features:

- **Decentralised**. Without question, the most important feature of a VC is that it removes any dependency on centralised systems such as hubs or marketplaces or social network platforms. Just like your passport or driver's license, a VC is issued to the holder who keeps it in their (digital) wallet. A verifier to whom a VC is presented can confirm authenticity without any need to contact the issuer.
- **Paper compatible.** Because VCs are essentially digital versions of existing paper documents, they can be used with minimal impact to existing business processes. Indeed, VCs can be implemented as QR codes on paper documents. This means that digital transformations of entire economies can happen easily and incrementally alongside existing paper processes.
- **Privacy preserving.** A VC holder can choose (via "selective redaction") to present only a subset of claims to a verifier. For example, a driver's license holder can present only birth date as proof of age without revealing sensitive information like home address. Similarly, in commercial supply chains, parties can present verifiable quality claims (e.g., "is organic") without revealing commercially sensitive information such as pricing.
- **Cryptographically secure.** Unlike paper documents that are easily forgeable and difficult to verify if suspected to be fake (verifiers need to contact issuers that may not be easily contactable), VCs are nearly impossible to fake and can be verified easily and automatically. So rather than manually checking a subset of documents, verifiers can automatically check every document. Accessibility to services like trade finance can be improved when lenders can automate verification processes.

[41] https://www.w3.org/TR/vc-data-model/

3.2 What is a decentralised identifier?

The World-Wide-Web Consortium (W3C) Decentralised Identifiers (DID) standard [42] says:

> *Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.*

The key words in that definition are "*as determined by the controller of the DID*". The key idea is that the identifiers are not issued or controlled by any centralised platforms (like social networks) but rather by the owner. This approach to identity is also known as "Self-Sovereign Identity (SSI)" as envisioned by the European Union SSI programme[43] and the Decentralised Identity Foundation (DIF)[44].

Any entity (person, organisation, thing) can self-issue any number of identifiers (DID) and associated cryptographic keys that allow the entity to prove ownership of that DID. VCs may reference a DID as the issuer and/or subject of a credential.

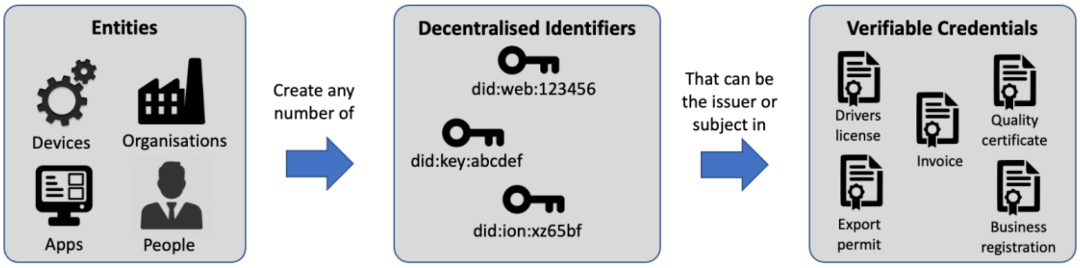


Figure 8 - Decentralised Identifiers

DIDs are globally unique and have four important properties:

- **Decentralized**: there is no central issuing agency.
- **Inherently persistent**: do not require the continued operation of an underling organization.
- **Cryptographically verifiable**: it is possible to prove control of the identifier.
- **Resolvable**: it is possible to discover further information about the identifier.

The W3C has documented some interesting use cases[45] that help to explain how the key technical features of DIDs can be combined in different ways to deliver some valuable business outcomes. For example:

- A customs authority can issue an Authorised Economic Operator (AEO) certificate as a VC to an exporter's DID so that the exporter can then digitally prove their AEO status to any verifier.
- A freight forwarder can create a DID for a consignment which can be used by any party in the supply chain to discover further data about the consignment and verify the data integrity.

Technically, a DID is a string of characters starting with "did", followed by a did method (which tells the consumer how to interpret the DID)[46], and then an identifier that is unique for a given method. E.g.:

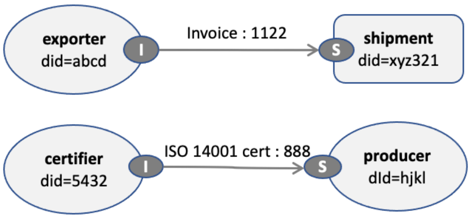
- did:**web**:abf.gov.au
- did:**key**:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
- did:**ion:**EiD3DIbDgBCajj2zCkE48x74FKTV9_Dcu1u_imzZddDKfg

The W3C standards deliberately allow market innovation in the development of different did methods which, although a valuable principle, has led to some proliferation and consequent confusion about which did method to use for what purpose. Some guidance is provided in Appendix A of this paper.

[42] https://www.w3.org/TR/did-core/
[43] https://www.eesc.europa.eu/sites/default/files/files/1._panel_-_daniel_du_seuil.pdf
[44] https://identity.foundation/
[45] https://www.w3.org/TR/did-use-cases/
[46] https://www.w3.org/TR/did-rubric/

3.3 What is a trust graph?

A single verifiable credential allows an issuer to make one or more verifiable claims about a subject.



For example, an exporter might issue a commercial invoice for a given shipment of goods as a VC. A verifier can be confident that the invoice was issued by the identified exporter and hasn't been tampered with. Similarly, a certifier can issue an ISO-14000 environment certificate to an identified producer which can be presented to any party for digital verification of ISO certification.

These uses are valuable in themselves, but credentials can be chained together to create "trust graphs" that release much greater value. The connections that make up the graph can be explicit (e.g., a credential includes a link to another credential) or implicit (e.g., the same DID appears in two separate credentials). Consider the example below, in which nodes represent DIDs and links are VCs.

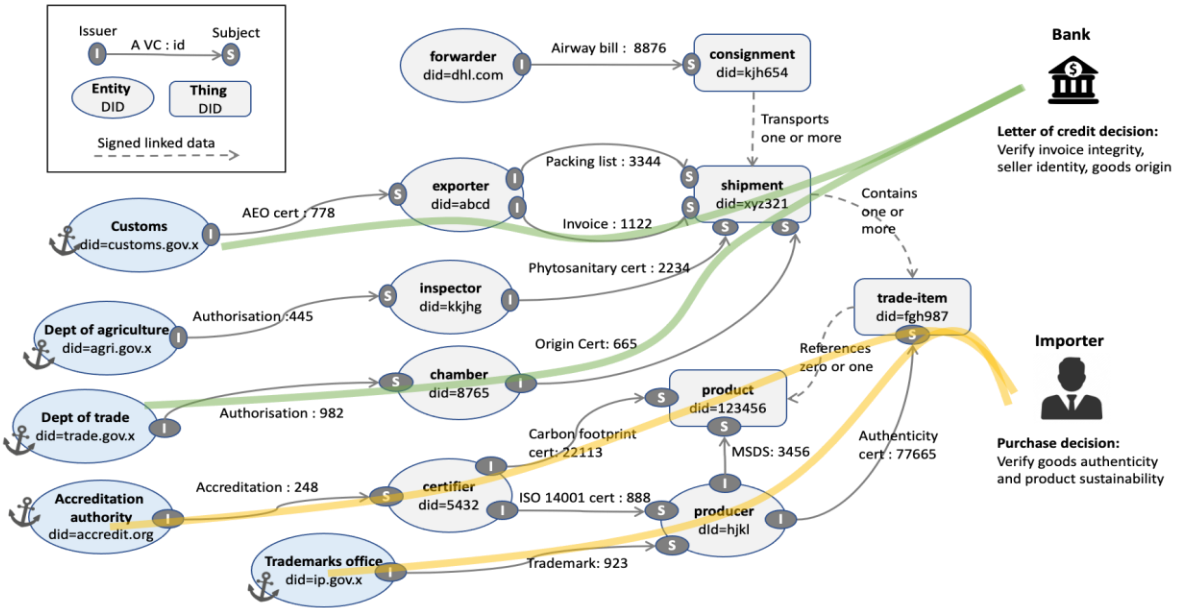


Figure 9 - Sample trust graph

- A Bank is presented with a commercial invoice VC issued by an exporter did:abcd for shipment did:xyz321. The bank verifies the document to confirm it was issued by did:abcd and hasn't been tampered with. The bank uses the did method to get further information and retrieves a linked VC issued by the customs agency that confirms the Authorised Economic Operator (AEO) status. The bank confirms that preferential certificate of origin VC references the shipment did:xyz321 as the subject. The bank now has enough information to automate the decision to issue a letter of credit.
- An importer finds a trade-item did:fgh987 (similar to a serial number) either on a packing list or possibly by scanning a QR on the shipped item. The did:fgh987 references and authenticity VC issued by the producer together with a verifiable attestation from the trademark office that the producer did:hjkl is the owner of the trademark on the item. The importer can also trace a link to the product and its carbon footprint certification. These verifiable quality claims give the importer confidence to strike up a supply agreement with the producer.

There is no dependency on centralised platforms or databases. A verifier can enter the graph at any point by being presented with a VC and then following links – like finding the end of a string and pulling on it to see what is connected. Because VCs are paper friendly whilst still containing digital data, there is no dependency on verifier technical maturity. The bank can use its computers to fully automate the verification and decision whilst the importer might follow links embedded in QR codes using their mobile phone. Privacy and confidentiality concerns are mitigated because information can be redacted so that (for example), verifiers can confirm country of origin or the carbon footprint of a product without knowing pricing or the names of suppliers in the value chain.

3.4 What is a trust anchor?

A VC provides cryptographic proof that a given claim was made by an identified issuer about an identified subject. But the value of that proof depends on how well the verifier knows and trusts the issuer. For example, a driver's license VC issued by a well-known .gov issuer needs no further proof to be trusted. But many supply chain VCs don't have this quality. An animal health inspection certificate issued by John Smith is of little value unless there is evidence from the well-known food health regulator (e.g., the department of agriculture) that John Smith is indeed authorised to make such claims. In most economies the trust anchors are government agencies and accreditation authorities. The trust graph in the previous section shows five examples of claims from relatively unknown parties that are anchored to a claim from a trusted party.

The role of trust anchors is to issue digital credentials to their community members that the members can use to make their own credentials more trustworthy. For example, a national companies register that issues paper or PDF company registration certificates can now issue them as VCs so that the company can, in-turn prove its identity to any verifier. A fundamentally important advantage of the decentralised architecture of VCs and DIDs is that there is no need for any direct relationship between the issuer (e.g., the companies register) and the verifier who, for cross border trade scenarios, is most likely in another country. Here's how it works

1. A member of a regulated community (e.g., a company director) creates a DID and associated public/private key-pair using the software of their choice.
2. The member authenticates to the trust anchor service (e.g., companies register) as they would normally do when interacting with the regulator / trust anchor.
3. The member presents evidence that they are the owner of the DID (a digital signature using the DID private key) that the trust anchor can verify using the public key.
4. The trust anchor issues a VC with the member DID as subject - that contains relevant claims (e.g., that the DID subject is indeed an authorised officer of company XYZ).
5. The member (i.e., the company) can now leverage this regulator attested digital identity as part of any normal business.
6. For example, the company issues a commercial invoice with their DID as the issuer. The invoice VC includes a link to the company registration VC.
7. The invoice recipient can now verify the invoice VC (yes, it was issued by the company DID and hasn't been tampered with) and the registration VC (yes, the government regulator confirms that the same DID is Company XYZ.
8. If company XYZ is de-registered, the regulator can revoke the registration VC. Immediately after revocation, any verification of the original VC will result in failure.

It is important to re-emphasise that the trust anchor is only doing their normal business of issuing certificates, permits, registrations, licenses, etc. to their members – just doing it digitally. There is no relationship between the trust anchor and verifiers. The digital credentials are also paper-compatible – for example they can be made available as a QR link on the paper or PDF certificate. Whether the member makes use of the digital credential for downstream proofs is up to the member.

This means that trust anchors can begin to empower their community members simply by issuing digital VCs to complement existing paper/pdf processes, starting immediately. For example, a business registration authority may decide to make business registration certificates to all businesses in an economy available as digital VCs. Uptake may start slowly but the cost is low, and the value is high so most likely the market will quickly find innovative ways to leverage the trusted assertions.

3.5 What about blockchain?

Blockchain is a poorly understood technology that has attracted a remarkable amount of hype due to its use for crypto-currencies. That has led to an explosion in blockchain based platforms that claim some magical trust enhancement just because a blockchain is part of the system.

Verifiable Credentials and Decentralised Identifiers **do not require** blockchain to work effectively. What they do require is access to a public “verifiable data registry”. The registry must be publicly accessible because an issuer has no a-priori knowledge of who will be verifying. Any public register will do provided it has sufficient integrity and durability for the VC/DID purpose for which it is used.

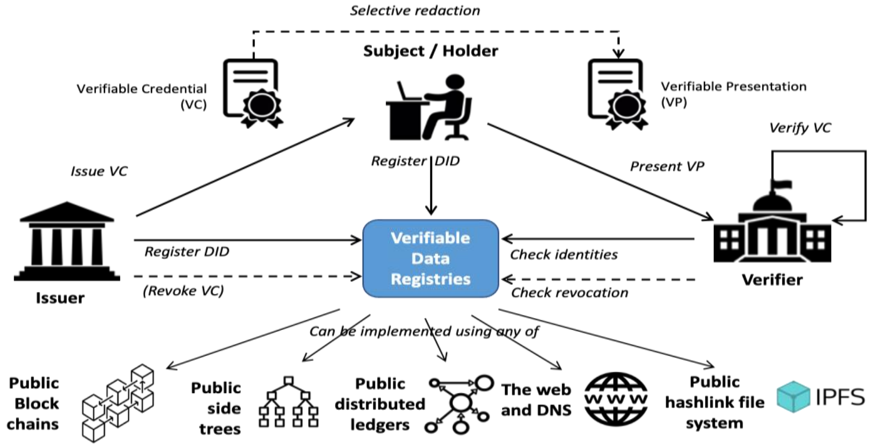


Figure 10 - VCs and the role of verifiable data registries

There are at least 5 categories of public data registries that can underpin a VC/DID ecosystem.

- Public blockchains such as Bitcoin and Ethereum are perhaps the best known. However, they are primarily cryptocurrency systems, and have very low performance (transactions per second) and could incur very high costs. They are generally not fit for purpose for VC/DID systems.
- Public side-trees are high-performance, low-cost networks that are “pinned” to a public blockchain on an occasional basis. Examples include ION network (layered on Bitcoin) and element-did (layered on Ethereum). These are much more cost effective and very functional but potential users should evaluate long term governance and funding of such networks, especially for long lived VCs.
- Public distributed ledgers are non-blockchain ledgers that are designed specifically for decentralised identity purposes. They are very high performance, low cost and well suited to VC/DID usage. However, like side-trees, the potential user should consider the long-term open governance and sustainability of the public Distributed Ledger Technology (DLT). Examples include the IOTA Foundation and Hadera Hashgraph.
- The web itself is a public register and can be used for VC/DID. In this case the identity is strongly linked to the Domain Name System (DNS) of the DID holder. Furthermore, there is an obligation for the issuer to host data on their public website that is highly available and very long term persistent. The web as a public register is best suited to large organisations and governments with well-known domains.
- The InterPlanetary File System (IPFS) is a global, public, high performance, decentralised file-store protocol with the unique feature that data, once stored, cannot be changed without changing the identifier (which is also the location) of the file. Unlike DLTs, IPFS files can be deleted and does not support smart contracts. However, the features of IPFS would make it an excellent candidate for high volume, shorter lived DIDs for things like consignments, shipments, etc.

In short, VCs and DIDs do not depend on blockchain and certainly not on cryptocurrencies. They do depend on publicly accessible data registries and there are several viable, high-performance, low-cost options. The best option most likely depends on the use case. Trust anchors may consider using their own websites (did:web or did:dns). DIDs for shorter lived “things” such as consignments may find did:key or IPFS (did:ipld) to be a good choice. Some use cases may be suited to dedicated DLTs or side-trees pinned to public blockchains.

3.6 Where does UN/CEFACT fit in?

Centralised platforms such as the major social networks attract billions of users to the same software package. When sharing data, the exchange is happening inside the same platform and so interoperability and data standards are of little concern. Decentralised systems on the other hand, when successful, will involve thousands of software systems servicing millions of independent issuers, subjects, and verifiers. One of the biggest barriers to successful uptake is interoperability. If thousands of universities issue their degree certificates as VCs but all do so differently, then verification costs for employers around the world will become prohibitive. Similarly, if thousands of chambers of commerce around the world all issue Certificates of Origin VCs differently then verification costs for importing authorities will be high. Well defined standards can solve this problem.

Interoperability needs to work at two layers.

- **Technical interoperability** is concerned about consistent implementation of protocols like DID methods, cryptography suites, and so on. This is the domain of the W3C and the Internet Engineering Task Force (IETF) and there are already some well documented standards and certification test services.
- **Semantic interoperability** is concerned with a common understanding of language. Standards are usually domain specific (i.e., health, education, supply chain, etc). Standard data models, data exchange structures and code lists, when used consistently, will mean that a certificate VC issued by one system will be readable and understandable by another.

For the international trade & transport business domain, UN/CEFACT is the leading global standards body. As the world moves towards paperless trade through decentralised architectures then consistent use of semantic standards will become a critical success factor. Fortunately, language moves more slowly than technology and so the semantics already defined by UN/CEFACT for earlier technologies. For example, the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) and Extensible Markup Language (XML) Messaging are largely re-usable in Verifiable Credentials. The main task for UN/CEFACT is to publish its semantic standards in format that is compatible with the VC technology so that they are easily usable by implementers around the world. There are two key activities.

1. Publish the UN/CEFACT international supply chain reference data model and code lists as JSON-LD vocabularies. This is needed because JSON-LD is the preferred technical representation for data in Verifiable Credentials. JSON-LD is perfectly suited for describing graphs of linked data and so is the natural representation for the trust graphs described in section 3.3.
2. Use the subsets of vocabulary elements developed by UN/CEFACT project teams for each credential type (e.g., Certificate of origin, bill of lading, etc) and publish a JSON-LD profile (as a @context file) and schema for each. This is very helpful for implementers because the entire global supply chain vocabulary will contain thousands of terms whilst a specific credential type will use only a few dozen. A @context file is essentially a way to say, "here's the small collection of terms from that large vocabulary that you can use (issuers) or expect to encounter (verifiers) in this credential type".

There is already a full set of UN/CEFACT international trade data exchange subsets which define specific process areas such as invoicing, transport contracts, certificates etc. A JSON-LD project will enable these to be published as JSON-LD vocabularies and context files. It is planned that UN/CEFACT standards will be ready in good time to support global uptake of VCs and DIDs in the international supply chain.

UN/CEFACT also issues best practice guidelines as either white papers[47] or formal recommendations[48]. This document is an example of guidance material and is issued as a UN/CEFACT white paper.

[47] https://unece.org/trade/uncefact/guidance-material
[48] https://unece.org/trade/uncefact/tf_recommendations

4 IMPLEMENTATION GUIDANCE

This chapter is designed for the policy maker that has read and understood the potential of verifiable credentials for cross border trade and seeks to prepare an implementation business case for their jurisdiction. We present several principles and strategies to guide implementation decisions. We also provide a template implementation roadmap that can assist with implementation planning.

4.1 Choose interoperable technology

In a centralised architecture that is dominated by a few large platforms there is little need for interoperability standards because the platforms *are* the standards. However, in the decentralised world of verifiable credentials there are thousands of issuers and millions of verifiers using multiple different software tools of their choice. In such an environment, standards-based interoperability is fundamentally important. An issuer that provides credentials that others cannot verify is serving no useful purpose. At the technology level, the standards are the W3C Verifiable Credentials (VC) and Decentralised Identifiers (DID) specifications. However, within those standards, there is considerable flexibility around cryptography algorithms and DID methods and so it remains entirely possible that two software products that claim to conform to the W3C standards may not be interoperable.

The solution to this interoperability problem is a robust test and certification framework where each software provider proves that their products are interoperable with others.

1. First, by testing their product against the W3C self-service test suite[49] that confirms conformance with the minimum common suite.
2. Next, by participating in multi-vendor interoperability tests (a.k.a "plug-fests") where each product is conformed to be interoperable with several other products.

The US Department of Homeland Security (DHS) has recognised the importance of interoperability and has been supporting interoperability plug-fests[50] for several years. New products are always welcome to participate. In future, some other interoperability test from may emerge but in the meantime, the US DHS sponsored plug-fest is the one that is attracting the highest vendor participation.

The implementation guidance policy on technical interoperability is:

> Choose any technology platform you like so long as it has successfully completed an interoperability plug-fest and is committed to continue to do so as new test cases emerge.

4.2 Use standard vocabularies

Although technical interoperability is a fundamental pre-requisite for any successful implementation, it is not sufficient. It confirms that a credential issued by one platform will be verifiable by another. However, it does not confirm that both platforms understand the meaning of the claims in the credential. For example, consider a sanitary & phyto-sanitary (SPS) certificate VC that defines the fumigation chemicals used for a consignment of cherries.

- Issuer says "fumigant":"methyl-bromide"
- Verifier expects "pesticide":"bromomethane"

A human may know that a fumigation uses a pesticide (and so "fumigant" is equivalent to "pesticide") and that bromomethane is commonly known as methyl-bromide. But, without smart AI, the digital verification will fail. This kind of semantic interoperability issue sits at a layer above the technical interoperability concerns described in the previous section. The solution is to use standard vocabularies. Specifically, vocabularies expressed in JSON-LD syntax and managed by a standards authority relevant to the business domain. The

[49] https://github.com/w3c-ccg/vc-api-test-suite
[50] https://lists.w3.org/Archives/Public/public-credentials/2021Mar/0101.html

reason JSON-LD is important is that the vocabulary terms must be globally unique and referenceable with a permanent web URL. This is so that computers can understand the difference between similar terms managed by different authorities that might have different meaning. Ideally, vocabularies maintained by the relevant global authority should be directly referenced. In the cherry fumigation example:

"Fumigant":https://www.fao.org/fao-who-codexalimentarius/codex-texts/dbs/pestres/pesticide-detail/en/?p_id=52

For most cross-border trade terminology, the semantic standards authority is UN/CEFACT, and a draft JSON-LD vocabulary can be found at https://service.unece.org/trade/uncefact/vocabulary/uncefact/

The reader may note that the UN/CEFACT buy-ship-pay vocabulary is very large. It is impractical to build a system that "understands" every term in the entire vocabulary. For this reason, JSON-LD provides a concept called "@context" which represents a subset of one (or more) vocabularies.

Each VC type (e.g., an SPS certificate) should have a @context reference that tell implementers "Here's the subset of that big vocabulary that you need to support, if you want to issue or verify this VC type". If no such context file exists for a given VC type, then an implementer may need to participate in an international standards forum to help create one. Any regulator may initiate a UN/CEFACT project to do exactly that by simply proposing the project to the UN/CEFACT bureau and getting at least three heads of delegation (i.e., country representatives) to agree to it.

The implementation guidance policy on semantic interoperability is:

> For cross border trade document semantics, use the UN/CEFACT JSON-LD vocabulary and use the correct @context file for your verifiable credential type. If an appropriate @context file does not yet exist, then launch a new project to create one.

4.3 Identify & empower your trust anchors

As described in section 3.4, verifiers in importing countries should not need to know or be expected to know how delegated authorisations work in exporting countries. One of the first steps in establishing a digital trust architecture in any economy is to identify the national trust anchors to which VC issued by authorised / accredited parties can be linked. These will often be government agencies but may also be other governance organisations such as national accreditation authorities. For example:

- A customs or trade agency accredits chambers of commerce to issue preferential certificates of origin.
- An agriculture or food health agency accredits inspectors to issue sanitary / phytosanitary certificates. It typically also accredits auditors to issue certificates to food processing establishments such as abattoirs.
- An intellectual property authority issues trademarks to businesses that legitimately own the trademark.
- A national accreditation authority accredits individuals or organisations to issue ISO-9000 or ISO-14000 or other quality standards-based certifications.

These are examples of national trust anchors. When a verifier in an importing country is presented with a VC that contains important quality claims (e.g., "this consignment of cotton is certified organic") then the verifier must be able to confirm not only that VC is valid but also that the issuer is authorised to make such claims and that the authority has not been revoked.

This foundational national digital trust architecture is implemented simply by empowering each trust anchor to do digitally what they already do manually.

The implementation guidance policy for trust anchors is:

> Every party in a national economy that receives some kind of accreditation or authority from a trust anchor should be able to request that authority in the form of a digital verifiable credential so that they can link any VCs they issue to the trust anchor that attests to their authority.

4.4 Make verifiable identity a national asset

Just like road and rail networks or electricity grids, verifiable identity is a national asset. Millions or billions of transactions within a national economy require evidence of identity.

- Registering a new bank account;
- Enrolling a new supplier or customer;
- Requesting a letter of credit for a cross border trade;
- Making a payment or sending an invoice.

The degree of identity verification depends on the risk of the transaction. For banking, a new account opening to a previously unknown customer typically requires in-person identity checks where the person presents proof of identity documents such as passports and drivers licenses. In other cases, such as enrolling a new B2B supplier it may be sufficient just to present a business registration certificate. In all cases there is a balance between the degree of effort (and cost) to confirm identity and the risk of a fraudulent enrolment.

At the same time many nations have implemented (or plan to implement) national identity schemes for individuals and businesses. Often these schemes are limited to government use. That is, they are useful for citizens and businesses to identify themselves to government but cannot easily be used to identify themselves to other citizens or businesses – especially those in other countries. And yet, most individuals and businesses need to prove their identity to other citizens and businesses far more frequently than they do to government.

One way to leverage a national identity scheme so that it can be used by non-government entities is to allow non-government relying parties (e.g., banks, e-commerce sites etc.) to offer a social network style “login with your government ID” to their sites. This is called “federated identity” and works the same way as “login with google / Facebook” etc. However, it can be challenging to determine the policy and security settings to allow this kind of identity federation within an economy – and almost impossible across borders. Furthermore, even if the federation is allowed, it becomes quickly impractical to use across borders. Using federated identity, an exporter in one country proves their identity to an importing regulator in another country by “logging in with” their national identity to the foreign government site. An exporter that exports to 20 different export markets would end up with 20 different offshore registrations, possibly in 20 different languages.

VCs and DIDs provide a means for a national economy to release the value of high integrity proof of identity to constituents without any need for regulatory change or for any extension of identity federation to non-government or foreign parties. They also provide an identity verification method that is far more convenient for the identity holder. The mechanism is fairly simple.

- Any person or business creates one or more DIDs – as many as needed to separate concerns (e.g., different DIDs for personal and business use).
- Users login to their government identity site in the usual way.
- Users prove ownership of their DID (e.g., did:key:123456) to the government site.
- The government site issues an “identity VC” that links the DID to a public identity such as business registration number.
- The user can now issue any document (e.g., an invoice) as a VC signed with their DID and linked to the government issued identity VC.
- Any verifier onshore or offshore can now confirm the identity of the issuing party.

The implementation guidance policy for identity as a national asset is

> Provide a service for any authenticated constituent to self-issue an identity VC that links their self-sovereign identity (DID) to their national identity.

4.5 Protect privacy & confidentiality

Many trade documents contain commercially sensitive information such as pricing. Even those without pricing but with identified consignee / consignor information can be used by third parties to infer customer / supplier lists. Any VC use case (e.g., traceability / transparency) that requires commercial entities to expose sensitive information is likely to fail.

Uptake therefore demands that issuers can choose how much information to reveal in any VCs they issue. In some cases, issuers may also need to redact information on upstream VCs that they receive (e.g., from their suppliers) before passing them on (e.g., to their buyers). This ability to selectively redact information is especially important for traceability & transparency use cases where parties near the end of a long chain can trace product information back to primary producers. Sustainability concerns, for example, can be met when a product is supported by verifiable environmental or social responsibility claims without necessarily knowing the identity of each party in the chain.

The W3C VC standard does not define a specific mechanism for hiding sensitive information in VCs, but some common approaches are emerging that may, in future, become standards.

- The BBS+ protocol is used to create so-called “Zero Knowledge Proofs” (ZKPs) where, for example, a holder of a driving license with a birth date can prove to a verifier that they are over 18 without presenting any specific details from the license.
- The Open Attestation “selective redaction” protocol allows data to be removed from VCs without impacting the overall integrity of the VC (i.e., a holder can selectively hide data but can’t add or change any data). This is particularly useful for many cross-border trade use cases.

The implementation guidance policy for privacy & confidentiality protection is:

> Ensure that any VCs issued by authorities can be selectively redacted by the holder.

4.6 Incentivise verifiable import data

Much of the policy guidance has been about issuers of verifiable credentials. However, from an import border compliance perspective, the key interest of customs authorities is as a verifier of import documents. High integrity digital verification can help increase trust in import consignments and allow customs / quarantine authorities to focus risk and compliance activities on lower integrity consignments.

For importing authorities to have digital import documents to verify, the exporting nation must issue them. In order to provide a business motivation for exporters to increase digital integrity, importing authorities should consider what policy levers might be available to incentivise exporters to issue VCs. For example:

- Faster import clearances;
- Lower import clearance fees;
- Reduced inspections;
- Simpler under-bond movements.

The implementation guidance policy for import incentives is:

> Identify and incentivise opportunities for streamlined import clearance when import documentation is supported by digital verifiable credentials issued from the exporting nation.

4.7 Minimise change impact on others

The international supply chain includes a lot of stakeholders, many of which handle or use the same document. Often the issuer of a document does not know who the final verifier will be. For example, a preferential certificate of origin:

- Is usually issued by a chamber of commerce to an exporter under authority of the exporting trade or customs agency;
- Passed from exporter to freight forwarder together with other export documentation;
- Sent to the importer by freight forwarder (or exporter);
- May be passed to a financial institution by the importer to support a letter of credit;
- Is given to an import customs broker by the importer;
- Is provided to the importing customs authority by the import broker – to obtain a concessional duty rate.

That's up to seven entities that handle the certificate. If digitisation of the certificate requires all stakeholders to change their established practices, then any digitisation effort is likely to fail. Therefore, digitisation processes must remain "paper friendly" so that, if any of the multiple stakeholders is not ready for change then business can continue without impact.

The open attestation protocol (a compatible & interoperable extension of W3C verifiable credentials) provides a very powerful mechanism to turn paper processes into digital processes without impacting stakeholders who stay with paper.

- VCs are issued as digital credentials just like any other VC. Each VC is encrypted with a unique key and stored at a public location.
- The issuer defines a "decentralised renderer" that can present the VC in human readable form just like the paper.
- A QR code on the human readable format includes the decryption key, the URL of the digital VC, the URL of a renderer, and the URL of any compatible hosted verifier service.

Using this protocol, the trade document is passed around the supply chain as a human readable document with QR code, just like existing paper documents. Verifiers (e.g., any of the seven parties in the preferential certificate example) can work at any level of digital maturity.

1. They can just inspect the human readable document, with no change to previous practice;
2. They can scan the QR with a mobile device, be taken to the hosted verifier service, which will retrieve the VC, decrypt and verify it;
3. They can automate the QR reading, retrieve the digital VC and decrypt it (ignoring the hosted verifier and rendering template) and do their own digital verification and extract all VC data for use within their systems.

In this way, with the same issued document, different consumers can very their behaviour from zero change to full digital integration.

The implementation guidance policy for minimising change impact is:

> Recommend use of paper friendly extensions to VC standards (such as Open Attestation) in order to facilitate digital uptake in complex supply chains by supporting verifiers at any level of digital maturity.

4.8 Be compatible with existing legal frameworks

This section is a minor variant on the previous section. Some regulators have quite prescriptive legislation about trade documents that may need to be changed in order to support digitisation. In such cases, there could be scenarios where issuers would need to know in advance which nations can support digital documents and which still need paper. Issuers in exporting nations that need to accommodate these differences in importing nation regulation will face increased complexity. The complexity is worsened when some verifiers prefer digital VCs (e.g., the bank that wants to automate the letter of credit process) whilst the importing nation demands paper. In such cases issuers may need to issue both paper and digital.

This variation in national regulatory environments with regard to digital documents is another reason to use a paper friendly protocol such as open attestation. It is very rare that an importing regulator would not accept the same document they've always accepted, except with a QR code in the corner.

The implementation guidance policy for legal framework compatibility is:

> Recommend use of paper friendly extensions to VC standards (such as Open Attestation) in order to facilitate digital uptake even when legal frameworks in other nations are not yet ready for digital documents.

4.9 And go 100 per cent digital

The single biggest obstacle for any nation to digitise cross border trade documents is the readiness of recipients to process digital documents. Any strategy that requires separate bilateral agreements and implementation projects for every digital exchange will lead to very slow progress.

Using VCs and Open Attestation in particular allows this dependency to be decoupled. Issuing nations can just issue all certificates, permits, licenses, etc. as digitally verifiable documents with confidence that counter parties that may not yet be ready technically or legally can still process the human readable version as before.

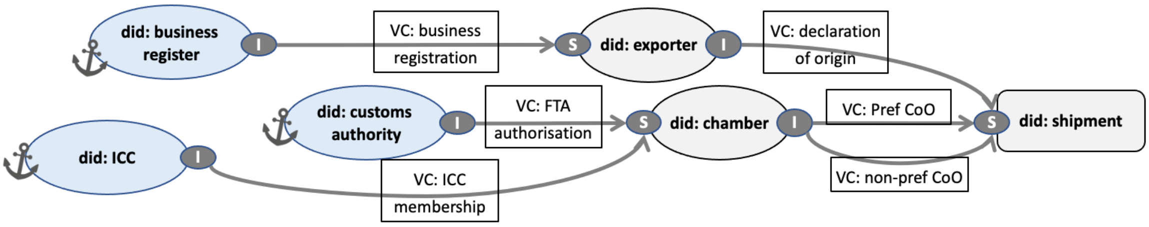
The implementation guidance policy for going 100 per cent digital is:

> Implementers should consider issuing all cross-border documents as paper friendly digital verifiable credentials (e.g.; open attestation files) as soon as practical and without any dependencies on counter-party readiness.

5 ANNEX A: USE CASE SCENARIOS

5.1 Certificates of Origin

VCs can digitise one of the most ubiquitous paper documents in cross-border trade – origin certificates.



The problem

Certificates of Origin attest to the country of origin of goods (i.e., where they were produced). A non-preferential certificate is usually required to support trade finance applications or to comply with import market regulation. They are issued to exporters on a per-consignment basis by a chamber of commerce in the exporting jurisdiction. A preferential certificate of origin is specific to a Free Trade Agreement (FTA) and is used to claim concessional duty rates. They are issued either by the customs authority or by an authorised delegate. Some FTAs allow exporters to self-declare origin criteria via a Declaration of Origin (DoO), although that privilege sometimes requires an advance ruling from the importing customs authority.

Certificates of Origin in their various forms are one of the most ubiquitous examples of cross border paperwork and so are an ideal target for digitisation. Some electronic solutions exist but face challenges.

- PDF certificates are easy to fake and so many verifiers still demand original paper with signatures and wet seals. Not only is this costly but, if lost in the post, shipments can be held up at borders.
- An international register has been established by the International Chamber of Commerce (ICC) so that PDF CoOs can be verified as genuine. It's a good initiative but requires that issuers update the register. When a verifier does not find an entry, it is not possible to know whether the CoO is fake or just not registered.
- Any electronic solution must accommodate the reality that CoOs are used by multiple parties in the supply chain that currently expect paper (or PDF) copies.

The solution

In a VC based solution to digitising origin claims, certificates and declarations would be issued as VCs but the digital version would also be accessible via a QR on the paper / PDF version so that the same certificate can support different verifier technical maturity. Some verifiers may simply scan the QR with their phone. Others may integrate with their systems and consume the full certificate data. Furthermore, each certificate would include a link to the trust anchor that confirms the issuer's authority.

- Non-preferential CoOs would be issued by chambers of commerce and would include a link to a VC issued by the ICC that confirms that the specific chamber is an accredited ICC member.
- Preferential CoOs would be issued by any authorised organisation (e.g., a chamber of commerce) and would include a link to the authorisation VC issued by the exporting customs authority.
- Declarations of origin would be issued by any exporter and would include a link to a business identity claim from the exporting regulator – typically a national business register.

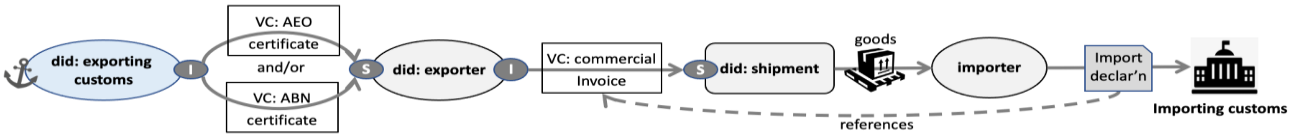
In all cases the subject of the certificate is the shipment about which the origin claim is made. In this way, any verifier can confirm that the origin claim is valid and that it is issued by an authorised and identified entity. The open attestation protocol (see appendix) is well suited to this blended paper/digital model.

A longer-term opportunity

In the longer term, verifiable supply chain traceability as described in section 4.10 may make origin certificates redundant as the evidence of origin would be verifiable through supply chain traceability.

5.2 AEO Mutual Recognition

VCs provide a scalable and very high integrity digital solution to the Authorised Economic Operator (AEO) mutual recognition challenges.



The Problem

As customs authorities around the world seek to improve efficiency and reduce risk, there is an increasing focus on risk assessing the trading **entity** rather than the consignment. The AEO[51] is part of the WCO SAFE[52] suite of standards and provides a model for authorities to assess and pre-quality certain trader and service provider businesses so that subsequent import/export transactions can be streamlined. It's a successful idea and most countries (including all large economies) already have an AEO scheme. However, AEO schemes face some challenges.

- They are domestic schemes that establish trust between a regulator and a trader in the same country. But a cross-border consignment involves both a domestic party (e.g., importer) and international party (e.g., exporter). Some regulators [53] have established mutual recognition frameworks to address this problem.
- But, as described in the lessons learned section of the WCO mutual recognition guide[54], IT system integration and automation are a big challenge. Exchanging AEO lists between regulators is hard to scale as the Mutual Recognition Arrangement/Agreement's (MRA's) scale as there would be a many-many (n-squared) integrations requirement.
- Some regulators have published lists of AEOs. This can be considered an authoritative list but, as a public register is very susceptible to piggy-backing – a fraudulent practice where an unscrupulous trader pretends to be a trusted trader to reduce seizure risk of illicit goods. Public lists can confirm that a given business is an AEO, but not that the counterparty in a trade really is that AEO.
- Whilst AEO schemes are primarily targeted at streamlined regulatory compliance, there is an opportunity to improve trust and hence facilitate trade if an AEO can prove their status to their customers as well as to regulators. Several good examples are described in this BTI paper[55].

The Solution

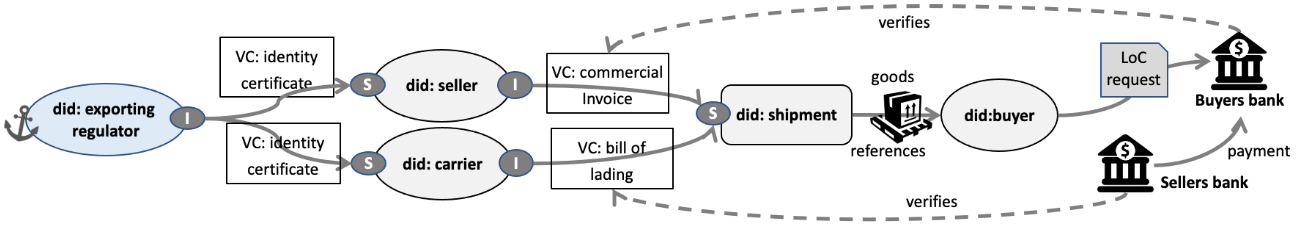
Rather than attempt to establish bilateral AEO list exchanges which, even if successful would not prevent piggybacking and would not facilitate commercial market facilitation of AEO status, regulators should simply issue all AEO certifications as digital verifiable credentials to subject DIDs controlled by the AEO party.

1. Domestic AEOs would create a DID (this could be facilitated by the regulator) and prove ownership of the DID to the regulator – who would then issue an AEO VC to that DID as the subject.
2. The AEO can create a verifiable presentation to prove their AEO status to any interested party (e.g., a bank offering trade finance). Furthermore, the AEO can issue trade documents such as commercial invoices using their DID as the issuer. Overseas counter-parties such as importers and importing authorities can then verify invoice integrity and, by verifying the linked AEO certificate, confirm that the invoice was indeed issued by the AEO.
3. At any time, the issuing regulator can revoke AEO status and any subsequent attempts by any verifier to confirm AEO status will fail - yielding a revoked status.

This solution prevents piggybacking, facilitates commercial uses of AEO status, and avoids the need for complex cross-border G2G data exchange frameworks.

[51] https://tfig.unece.org/contents/authorized-economic-operators.htm
[52] http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/frameworks-of-standards/safe_package.aspx
[53] https://ec.europa.eu/taxation_customs/mutual-recognition-and-cooperation-other-government-authorities_en
[54] http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/aeo-mra-strategy-guide.aspx
[55] https://www.uh.edu/bti/research/ecommerce-shi/bti-ecommerce-finalreport-24feb21-released.pdf

5.3 Documentary trade finance



The Problem

Trade finance is a crucial element for cross-border trade, which facilities the movement of goods across borders. While the US $5 trillion trade finance market[56] relies on long-standing practices and procedures used by banks and traders, a lack of trust and transparency among all parties in the trade ecosystem is still an issue today[57]. One consequence could be genuine businesses are unable to receive financing[58]. Some key challenges faced by the trade ecosystem includes:

- With cross-border trade, it is difficult for a bank to validate the identity of the trade parties (e.g., beneficiary) as many of them will be geographically distanced. Some banks will only work with trusted parties to address the issue.
- Digital documents may be fake[59]. If the bank is able to validate that the document comes from the expected issuer (e.g., an electronic bill of lading from a Maritime Transport Operator) and that the document has not been tampered with, it will be better able rely on it.
- Documentary Trade Finance is commonly used in international trade to provide an economic guarantee from a creditworthy bank to a seller of goods. It is still largely paper-based[60] and hence largely subject to manual processing. This makes the process slow, cumbersome, expensive and not without error. Digitisation efforts to date have been siloed in nature. This results in a fragmented landscape that requires many parties to use multiple systems to serve different business partners. Since different trading parties will undertake digitalisation efforts at different times (e.g., a recent survey by the International Chamber Commerce shows that roughly 40 per cent of responding banks said that digitalization was not an immediate priority[61]) so interoperability with paper is still necessary.

The Solution

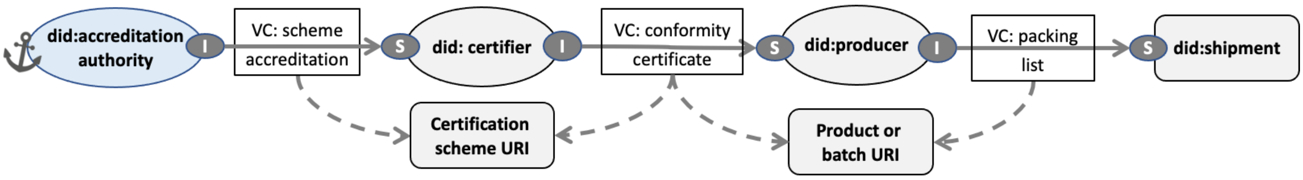
One way to better serve the needs of users in the trade finance ecosystem, is to bridge the systems provided by different systems and platforms, in that a single set of electronic trade documents can be read and validated by the different systems.

1. The issuers of trade documents would first create a DID and be registered as an authorised issuer with the relevant government authority.
2. With their DID as the issuer, they will be able to issue electronic documents (e.g., a packing list or a invoice). The DID will be recognised and accepted by different systems and users only need to keep a single DID to use with the different systems. Users can issue the trade document/s with its file signature being recorded elsewhere to ensure the recipient that the document/s has not been tampered with (e.g., when a party receives the trade documents, they are able to validate the issuer's identity and the authenticity of the document).
3. Cross-border parties will also be able to check on the document's latest status (e.g., whether it has been revoked).

[56] https://iccwbo.org/media-wall/news-speeches/icc-opens-consultation-on-draft-global-standards-for-sustainable-trade-and-trade-finance/
[57] https://www.wto.org/english/thewto_e/coher_e/challenges_e.htm
[58] https://iccwbo.org/content/uploads/sites/3/2018/05/icc-2018-global-trade-securing-future-growth.pdf
[59] https://iccwbo.org/publication/global-survey/ (Global Survey for 2020)
[60] https://blogs.adb.org/blog/can-pandemic-help-end-paper-chase-hobbling-international-trade
[61] https://blogs.adb.org/blog/more-just-money-digital-technologies-can-help-narrow-trade-finance-gap

5.4 Product Conformity

VCs can add integrity to a currently very paper-centric product conformity testing & certification process.



The problem

There are thousands of international schemes and conformity assessment processes involving tests and inspections that result in the issuance of conformance certificates. There are also mutual recognition agreements in place between countries such that certification processes in one country are recognised in others. Most certificates are generated on paper or PDF, and it is difficult to verify the currency of credentials and the status of issuing bodies. Misuse or falsification of certificates is relatively easy. This lack of transparency is challenging the integrity of national product conformity processes in a digital world.

Even legitimate documents can be misused. A test certificate, for example, generally pertains to a specific batch/shipment; however, it can be in the interests of suppliers to spuriously infer that the certificate applies to the ongoing supply of the product. Also, a certificate in current circulation may have ceased to be valid because associated credentials, authority, or standing of the certificate holder have changed.

International product conformity infrastructure is mature and well organised. Digitalisation of systems is inevitable however there is a risk, that a multitude of incompatible approaches may evolve. Any digital transformation in the sector must accommodate physical document as well as digital credentials exchange as legislative reforms will inevitably be slower than the uptake of verifiable credentials solutions.

The solution

As shown in the trust graph, a linked set of VCs can establish a verifiable chain of trust from a batch identifier in a shipment to the product conformity certificate that is issued by an accredited certifier or lab. Open attestation is a type of VC that can provide a seamless glide path from current paper-based product conformity processes, to a fully digitised process, allowing both to co-exist during a lengthy transition.

A key integrity measure is the link between physical product flow and product conformity information (i.e., that the certificate is really about the goods in the shipment). The International Organization for Standardization / The International Electrotechnical Commission (ISO/IEC) based identifiers (e.g., GS1 GTIN) of products being tested encoded in standardised data carriers (QR codes or RFID) and attached to physical products provide a means to establish this key link.

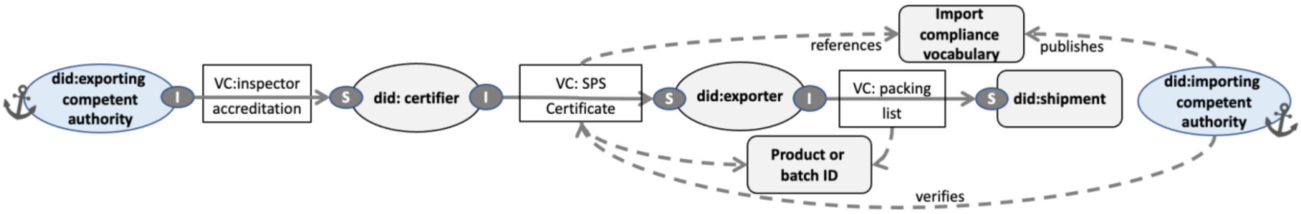
An implementation roadmap

Initial implementation efforts should focus on empowering international and national accreditation authorities and certification scheme owners to issue accreditations as VCs using standardised (JSON-LD) vocabularies. This is a necessary step to help the much larger group of certifiers to issue interoperable conformity certificates. Issuing the certificates as open attestations allows paper and digital versions to coexist.

This future will likely see regulators and other requiring evidence that credentials are used (viewed or checked) rather than just presented. Larger linked data graphs may be used to allow conformity certificates to be linked together throughout complex supply chains such as cotton bale to garment or lithium mineral to electric vehicle – thereby facilitating end-to-end product sustainability verification.

5.5 Sanitary & Phytosanitary (SPS) Certificates

VCs, together with well-defined compliance vocabularies, can provide a highly scalable and low-cost way to automate and digitise cross border sanitary & phytosanitary (SPS) certificates.



The problem

As a population health and biosecurity measure, most national regulators define commodity specific safety rules for the import of food into their countries. Exporters must provide certificates with each shipment that confirm compliance with food safety rules. Exporting regulators often act as the trusted authority and assist their exporters by maintaining commodity and country specific rules (for example this AU page[62] about exporting apples to Japan). Sometimes inspections and certificates of food processing establishments (e.g., abattoirs) are also required. The compliance framework is paper intensive, complex, and costly for both the exporting jurisdiction (to ensure country/commodity compliance) and importing jurisdiction (to verify each shipment). Any mis-alignment can result in food imports being delayed or lost to decay or disposal.

Current solutions

There are some existing solutions to the digitisation of food safety certificates and all offer improvements to paper based compliance, but each also has some limitations.

- UN/CEFACT has defined a government-to-government digital exchange standard called SPS e-Cert[63]. There have been several successful implementations over the last decade, there are two key scalability constraints. One is that both governments must have funded projects to become ready and capable to exchange digital data. The second is that, when third-party visibility of certificates is required, a paper copy is still required because the digital copy is strictly Govt to Govt.
- IPPC has developed a phytosanitary hub[64] that allows issuers to publish certificates for authorised verifiers to access. The hub offers some improvements over G2G exchange because less mature participants can access manually without ICT investment. However, the hub is limited to phyto (plant) certificates and, like any centralised hub model, has difficulty identifying and authorising verifiers (e.g., transit authorities and brokers) who may not be known to the issuing authority.

One difficulty for any digitisation model is whether the issuer and the verifier have the same understanding of the meaning of claims such as fumigation chemical type. Paper processes can rely on humans to read and understand claims even if spelled differently. Automated processes need well defined digital vocabularies.

A better way forward

A VC based solution, ideally using paper-friendly protocols such as Open Attestation, offers improvements

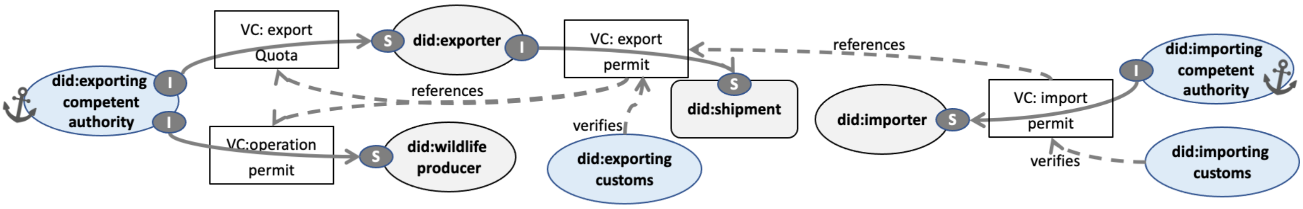
- Issuers can go 100 per cent digital without dependency on verifier maturity.
- Transit countries can easily verify certificates.
- Border authorities can verify certificates issued by the competent authorities.
- The identity and accreditation of issuers is assured.
- VC digital claims can be matched to competent authority vocabularies for automated processing.

Finally, if the product and transport identifiers are also managed as a DID then there can be a strong connection between the certificate and the actual goods being shipped, mitigating risks of shipping goods that weren’t the subject of the certificate.

[62] https://micor.agriculture.gov.au/Plants/Pages/Japan_JP/Apples.aspx
[63] https://unece.org/trade/uncefact/ecert
[64] https://www.ippc.int/en/ephyto/

5.6 CITES Permits

The International Convention for Trade in Endangered Species[65] (CITES) governs trade in banned (Appendix 1), endangered (Appendix 2) and country specific (Appendix 3) plants and animals. The highest volume is Appendix 2 trade in products made from endangered species (e.g., snake-skin shoes).



The problem

The process is necessarily complex. Exporters must only trade in allowed species from certified sustainable producers. Exporters are typically granted annual quotas by competent authorities and then draw down on those quotas with self-issued export permits. Importers must obtain import permits from their authority which must include an attached export permit from the exporting authority. Border agencies are often not connected to the competent authority and so are unable to verify quotas or permit validity at the point of export/import. Some competent authorities face years of paper-work backlog in their reporting obligations under the CITES convention. CITES permits have proven difficult to digitise due to the decentralised multi-stakeholder and multi-national nature of the problem.

The Solution

A VC based decentralised architecture offers the best opportunity to solve what is, by nature, a decentralised problem. A plausible solution is described by the trust graph at the top of this page.

- The competent authority audits producer operations against species specific sustainability criteria and issues an operations permit VC.
- Exporter requests an export license in the form of an approved quota for a given species and is granted a quota by the competent authority.
- Exporter self-issues an export permit VC for a specific shipment of goods made from a specific species. The permit is linked to both the quota VC and the operations VC.
- Exporting border authority verifies the export permit VC (and linked VCs) and grants clearance to export the shipment.
- Importer presents the export permit VC to the importing competent authority and requests an import permit VC.
- Importing competent authority verifies the export permit VC (and linked VCs) and issues the import permit.
- Importing customs authority verifies the import permit VC and grants clearance to import.
- Both competent authorities have automated issuing, compliance verification including quota management, and can also automate their international reporting obligations under CITES.

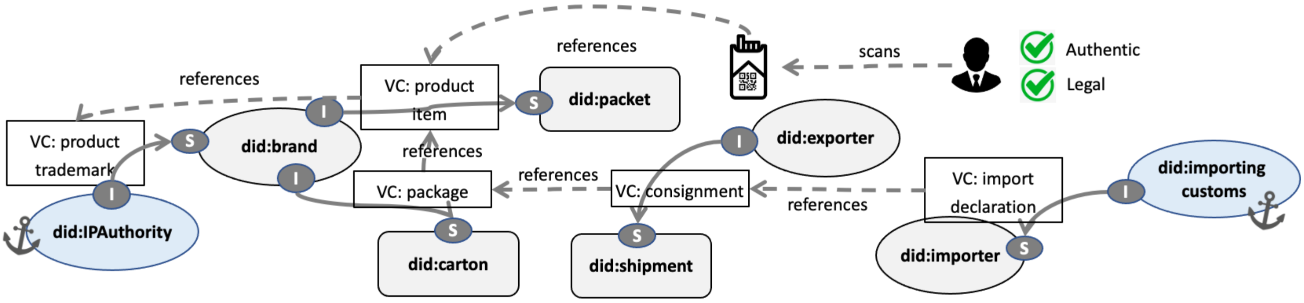
Illegal trade in endangered species becomes more difficult – thereby meeting the intent of the CITES convention. Although fully illegal trade (i.e., that where both production and consumption operate in illegal markets) will bypass CITES reporting obligations whether they are paper or digital, a significant proportion of illicit trade is produced illegally but then sold through legal markets (see UNODC report on wildlife crime[66]). Digitally verifiable integrity and traceability will make the sale of illegally produced wildlife in legal markets much more difficult.

[65] https://cites.org/eng/disc/text.php

[66] https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf

5.7 Illicit Tobacco

Although this use case is specifically about illicit tobacco, the pattern would apply equally to other kinds of counterfeiting and tax evasion counter-measures.



The problem

As described in section 2.3, counterfeiting and trade in illicit goods represents around 2.5 per cent of all international trade with an annual value of at least $500 billion. A large proportion of this trade is sold into licit markets and so, if buyers and consumers are equipped with appropriate verification tools, they can help to distinguish genuine from counterfeit goods. A key problem that must be solved with any solution to counterfeiting is that there must be a strong link between the physical goods and the digital evidence. There are several different attack vectors to mitigate

- Counterfeit goods may include unique identifiers embedded in QR codes, but they are fake and like to a fake site that looks like the real brand. So, verifiers see something that looks real but isn't.
- Counterfeit may goods include real identifiers embedded in QR codes that have been copied from a genuine article. Verifiers see a real site verification, but it is not for the physical product they've purchased.
- The goods are genuine but have been smuggled to avoid high domestic taxes (e.g., cigarettes).

The solution

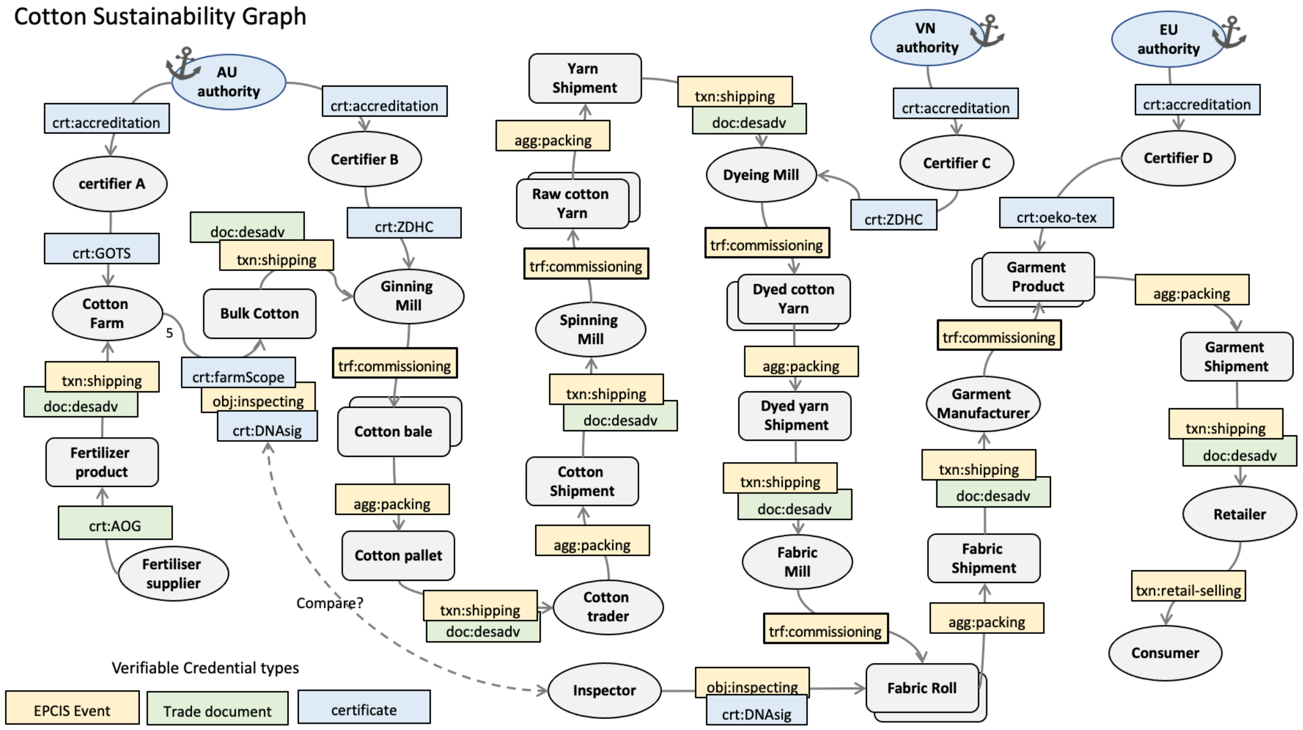
The trust graph shows how a Verifiable Credentials based solution can solve the problem.

- A national IP authority issues a VC to subject (brand) which attests that the subject is the legitimate owner of the relevant trademark.
- The brand (possibly through delegated manufacturers) issues a conformity VC for every product instance (i.e., each pack of cigarettes) and adds a unique QR to each pack.
- The brand issues a similar conformity VC for each carton with unique QR and list of contained packs. The VC for both carton and pack are linked to the product trademark VC.
- An exporter issues a VC representing a cross border consignment of cigarettes which lists all cartons in the shipment. The consignment VC could also link to higher level aggregations such as a box full of cartons.
- The importer lodges an import declaration to customs that references the consignment VC and pays duty. The customs authority follows VC links to establish the complete set of imported packs.
- The cigarettes are distributed within the import market.
- A buyer picks up a pack and scans the QR with a domestic verifier app with verifies that the cigarettes are genuine (by following the link to the IP authority trademark) and that they are legal (by checking against the customs authority list of duty paid packs.

Counterfeit goods will fail validation against a trusted IP authority. Genuine goods that have not been duty paid will fail validation against the customs list of duty paid packs.

5.8 Supply chain traceability

The cotton sustainability trust graph below is by far the most complex that has been presented in this document and serves to give a clear visual indication of the complexity of the cotton supply chain from grower through ginner, spinner, fabric mill and garment manufacturer through to retailer and consumer. The critical minerals supply chain from lithium mine to electric vehicle would follow a similar pattern. As described in section 2.4, supply chain traceability is the key to address accelerating environmental, social, and geopolitical sustainability concerns.



Any traceability platform that attempts to integrate such a complex supply chain into a single platform is bound to fail when faced with the multitude of commercial, geographical, sectoral, and geopolitical boundaries. Only a decentralised architecture can solve a decentralised problem as complex as end-to-end supply chain traceability. The interested reader can follow this particular use case in more detail on the UNECE sustainability project GitHub: https://github.com/uncefact/sustainability. The key features of the solution are:

- Each step in the supply chain is represented by a very simple and very consistent "event" data structure based on a subset of the GS1 EPCIS standard. This simple model has the effect of harmonising complex variations across all the stakeholders.
- Each party is identified with a DID that may be self-issued or may be issued by a traceability platform of their choice.
- Each event is represented as a VC and includes links to the previous step VC. It also includes links to supporting documents such as certificates and trade documents.
- Certificates (organic etc.) and trade documents are also represented as VCs but need only minimal structured metadata – so that they can be easily created from traditional PDF certificates.
- A simple boot-strapping protocol allows any party in the graph to start issuing and verifying credentials whilst others are brought along gradually via email and hosted apps.
- The International Trade Centre (ITC) standards map is used to harmonise the semantics of sustainability claims across hundreds of different sustainability standards.
- At any step in the chain, a verifier can follow the chain of credentials as far back as required.

6 ANNEX B: TECHNICAL GUIDANCE

This appendix is designed to support implementers with detailed technical information. Since such information is typically fast changing, this appendix provides only a summary of each topic and then a link to a UN/CEFACT project site that is maintained with the latest relevant information.

6.1 UN/CEFACT JSON-LD Vocabulary Management

As described in section 4.2, interoperability is a critical success factor for decentralised architectures. The more independent decentralised systems, the more critical standards and interoperability becomes.

UN/CEFACT has developed a semantic interoperability framework for verifiable credentials as shown in the diagram below. The goal of the framework is to ensure that your implementations are interoperable with others. That is, that you can verify VCs issued by others and that others can verify VCs issued by you.

All information is maintained on the UN/CEFACT GitHub at https://github.com/uncefact

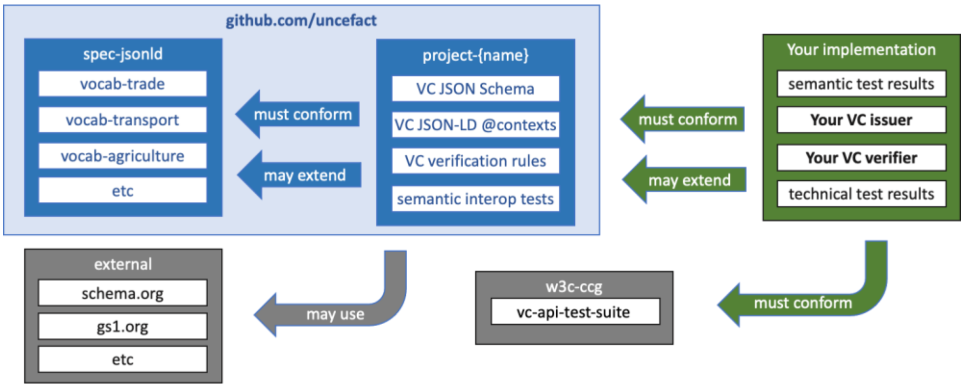


Figure 11 – Semantic standards architecture

- Interoperability starts by using international standard vocabularies. UN/CEFACT manages a suite of vocabularies organised by business domain (trade, transport, agriculture etc.).
- An international standard for given VC type such as a CITES permit or a certificate of origin is created through a UN/CEFACT project. The project must conform to the domain vocabularies and may, where relevant, draw upon recognised external vocabularies such as a pesticide list maintained by FAO or a species list maintained by CITES.
- The project will create standard credential structures (as JSON Schema), relevant vocabulary subsets (as JSON-LD @context files), verification business rules specific to the credential type, and finally a suite of self-service interoperability tests.
- The project repository contains all materials necessary for your implementation to be interoperable. Your implementation must successfully complete all interoperability tests before being listed as a certified interoperable system.

6.2 Linked VCs & trust rules

All VC use cases in this document include a “trust-graph” diagram that shows the relationships between VC types and actors (identified by DIDs). A key assumption in the trust architecture is that verifiers will follow linked credentials to reach the “trust anchors” that add integrity to the system. However, there is not yet strong consensus in the VC implementer ecosystem on how best to express the links and how verifiers should interpret them. This presents several risks to the trust architecture

- Issuers may link their VCs to a trust anchor, but verifiers may not be able to follow the links.
- Malicious issuers may define links to genuine trust anchors that are not relevant to the use case which verifiers may mis-interpret.

- Some trust graphs may require verifiers to check additional business rules - for example that the species listed in a CITES permit must be included in the species list in the linked operations permit.

The verification of a linked set of credentials therefore depends on consistent technical implementation of links and the correct evaluation of a number of credential specific business rules by verifiers.

The UN/CEFACT repository https://github.com/uncefact/spec-vclinks provides further guidance for implementers on the use of linked credentials and the verification of trust graphs.

6.3 Links to physical goods

The integrity of digital data is of much reduced value in cross border trade if it cannot be tied unambiguously and provably to the physical shipment of goods and be discoverable from the physical item. For example, a digitally verifiable product conformity certificate may be verified confidently but if it describes different goods than those in the shipment then it serves no useful purpose.

There are several mechanisms to link physical goods to credentials with different degrees of maturity and integrity.

- GS1 Digital Links provide a simple but powerful mechanism to link the existing very large ecosystem of 2-d barcoded products to digital data. It is very likely that a new ISO standard will formalise the principles of GS1 Digital Link so that it can be applied to other identification schemes, especially those that, like GS1’s, are based on ISO/IEC 15459. These standards underpin the growing use of 2D symbols, including QR codes, to sit alongside and then replace the traditional 1D barcode.
- DNA fingerprinting provides a mechanism to link bulk agricultural produce (e.g., grains or carcasses) to the related digital claims.
- Tamper-evident IoT (Internet of Things) sensors can read Radio Frequency Identifiers (RFIDs) on products, allowing strong links to corresponding digital claims.
- Several more advanced unique item identifier schemes based on DIDs (with associated public/private keypairs) can be linked to corresponding digital claims to prevent counterfeits.

The UN/CEFACT repository https://github.com/uncefact/spec-physicallinks provides further guidance for implementers on the use of physical product and consignment links for high integrity trade.

6.4 DID method guidance

Decentralised identifiers (DIDs) play a key role in the issuing and verification of linked credentials. As described in section 5.2 about AEO mutual recognition, a key dependency is the cryptographically verifiable connection between the subject of one VC and the issuer of the next.

The W3C DID specification is designed to allow market innovation to drive DID methods (e.g., did:key, did:web, did:ethr etc.). Whilst this is a good decision in principle, it has led to a proliferation of candidate DID methods – a total of 134 methods are listed in https://w3c.github.io/did-spec-registries/#did-methods at the time of writing this document. This proliferation presents a challenger for implementers. Which methods should be used for which purpose? Which methods are sufficiently stable and trustworthy for production implementations? The short answer is that only a small handful of the 134 methods are suitable for implementation.

The UN/CEFACT repository https://github.com/uncefact/spec-didmethods provides further guidance on this question.

6.5 Open Attestation and Tradetrust

Singapore developed OpenAttestation (see https://www.openattestation.com/) to enable documents issued with this technology to be cryptographically trustworthy and able to be verified independently. OpenAttestation provides the technology underpinnings of TradeTrust (see https://www.tradetrust.io) which is an open framework adapted for global trade practices to help the typically long chain of business partners achieve the ultimate objective of fully digitalising their business processes even across borders. Given the complexities of cross-border trade, success needs a multi-prong yet holistic approach. As such, with OpenAttestation providing the technology foundations, TradeTrust adds aspects such as acceptance by the global trade community and governments on the methods of document digitalisation as well as alignment on policy stances through G2G arrangements such as Digital Economy Agreements. These efforts have resulted in the following W3C verifiable credentials-related features being implemented:

- The Decentralised document rendering protocol enables users to choose their own document schema format, and to customise the look and feel of the trade documents produced.
- Selective Redaction provides a convenient method for intermediaries in the supply chain to hide sensitive data, which is critical for some use cases in the trade and traceability domains.
- The Title Transfer feature supports electronic transferable records and is designed to be compliant to the requirements laid out in UNCITRAL’s Model Law on Electronic Transferable Records (2017).
- The QR Code feature enables users to choose using paper or digital workflows, depending on their circumstances thus allowing issuers to execute digitalisation with minimal dependency on verifier technical capabilities.

The UNCEFACT repository https://github.com/uncefact/spec-tradetrust provides additional guidance on the effective use of TradeTrust.