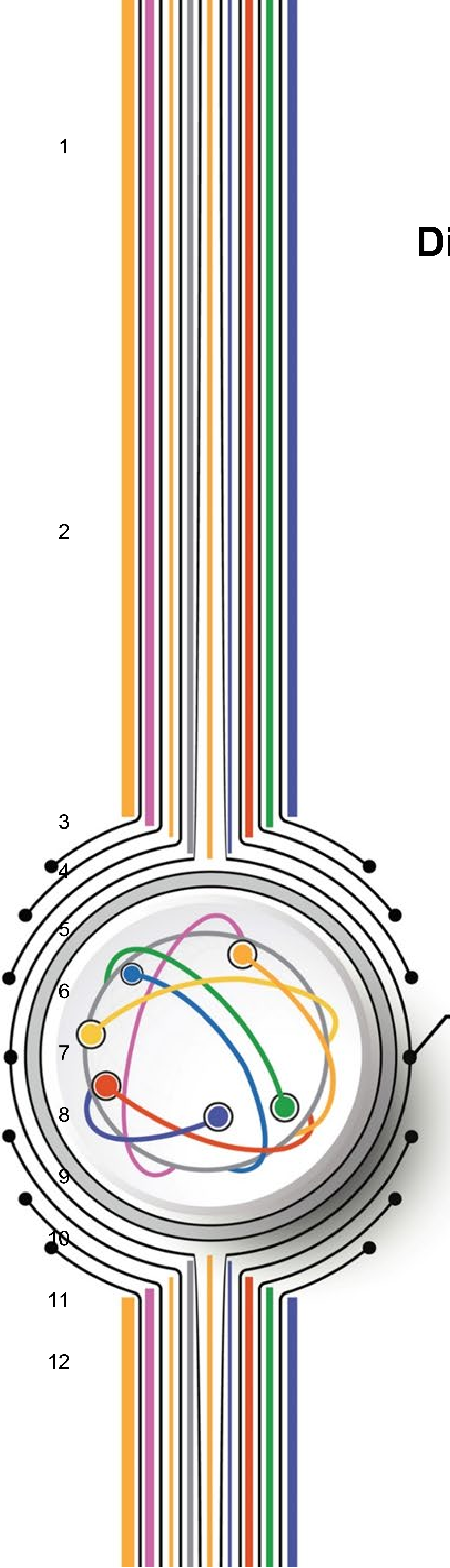
White Paper
Digital Product Conformity Certificate Exchange

Public Review Draft



UNECE
UN / CEFACT

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.

Acknowledgement

The UNECE Trade Facilitation Section and UN/CEFACT would like to express its gratitude to the experts who participated in the development of this paper: XXX (project leader), XXX (supporting Vice Chair and then Chair), XXX (Secretary UN/CEFACT, UNECE Secretariat), and XXX, XXX.

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

Simple, Transparent and Effective Processes for Global Commerce

UN/CEFACT's mission 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, and so 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 recognised 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

Foreword

XXX.

XXX

Director, Economic Cooperation and Trade Division

United Nations Economic Commission for Europe

Table of Contents

1 Executive Summary

The exchange of conformity assessment attestations between supply chain actors represents a critical element in modern global trade. The existing paper-based processes come with well-recognised problems. However, the necessary procedures, semantics and legal framework to enable transition to fully digitalised attestation systems have not been agreed.

This paper explores new possibilities that arise when framing the problem in terms of access to (rather than exchange of) conformity attestations. It also proposes the use of technology to link conformity attestations to physical product supply as a way to address existing problems. The paper also points to ways in which such framing may provide a natural structure for the future transition to fully digitalised systems, while noting that detailed exploration of such is outside the scope of this paper.

The findings are as follows:

1. There is a need for linking conformity attestations with physical product and to manage revision and issuing authority status.
2. The lack of any consistent process for exchange of conformity attestations is a barrier to interoperability.
3. Paper-based exchange of conformity attestations is inherently affected by legal ambiguities & exploitable loopholes which can exacerbate other process shortcomings.
4. There are gaps in the existing legal framework for cross-border data exchange. Therefore, any work towards digital exchange systems for conformity attestations must be made in the knowledge that the environment is ill-defined and likely to change, which could have implications for future choices of identifiers and specific digital technologies.
5. The critical data elements relating to conformity attestation exchange are dominated by identifiers and further work is needed to review the CEFACT data models having potential relevance to the identifiers of interest. It is further noted that established systems already exist for creating the types of linkages required to address the problem statement, including the use of globally unique identifiers.
6. Managing revision status is more complex than might first appear and a variety of incompatible approaches are being taken to address this. An important insight is that CABs (or parties acting on their behalf) are central to the process and that exchanging links to attestations may be more effective than exchanging attestations.
7. A set of complementary processes based on linked data can be expressed in generic terms that should serve to address the problem statement.
8. While the technology exists to achieve selective suppression of sensitive data, this cannot be consistently implemented due to the fractured way conformity attestations are currently exchanged. A more central role for CABs may make more consistent application of technology possible, from a process perspective.

A number of general principles are articulated that may serve as ‘guideposts’ for any future work to be undertaken. It is also acknowledged that whilst there remain some issues to be resolved, both the technology and systems necessary to address weaknesses in existing ‘analogue’ systems are available and that conformity assessment bodies can play a central role in a future digital trade ecosystem. The development of a CEFACT Business Requirements Specification (BRS) is recommended as a next step, to provide more detail and substance to the concepts explored in this paper. The opportunity for cooperation by relevant global bodies has also been highlighted, so that future developments may be approached in a manner that avoids splintered or siloed systems.

2 Introduction

This chapter serves as an introduction to the problem under consideration. Some clarification regarding the terminology used in this paper is also provided.

2.1 Terminology

The project deals with third-party testing, inspection and certification (TIC) conformity attestations, abbreviated as ‘conformity attestations’ within this paper.

The term ‘attestation’ covers any documented output of conformity assessment, including a certificate that describes the scope and standards against which products are certified, or a test report which specifies the outcomes of testing against a standard. Within this paper, all types of product tests and inspections are treated as relevant, however, the types of certification under consideration are limited to either management system or product certifications having relevance to the product in question.

2.2 Problem statement

TIC processes provide the backbone of global product and process conformity assurance. TIC provides an evidence-based approach to verify claims made about products including, but not limited to, quality, origin, safety, environmental and social impacts. International markets and consumers rely on a vast global ecosystem of TIC systems and services. Product conformity attestation exchange has historically relied upon the sharing of hard copy or facsimile electronic documents.

However, it can be difficult to verify paper-based conformity attestations and to ensure that claims made represent the current version of a genuine attestation and that those making the claims hold appropriate credentials to do so. As a result, products may be incorrectly accepted as fit for purpose, but include false, altered or non-current attestations, attestations with no clear link to a physical product shipment and attestations issued by parties not having the relevant authority.

These vulnerabilities are inherent to paper-based TIC systems and represent pitfalls for parties involved in weak compliance processes where a conformity attestation is accepted without questioning its legitimacy. The issues are especially challenging in the context of international trade, where both those making and receiving the claims are unknown to one another.

Given the sheer volume of conformity data that is associated with traded products, manual verification of all supplied product conformity evidence has never been possible. In consequence, manual verification has often been directed towards trading situations where trust has not yet been established or for high-risk products. The transition to digital systems carries potential for making the situation worse if digital verification of product conformity attestation is not adequately addressed.

This paper aims to discuss how product conformity attestations can be adapted to a paperless trading environment which optimises the advantages of digital technology while benefiting society by satisfying users and regulators that claims made about a product are true and transparent.

Unverified claims about a product regarding performance or other product attributes, such as environmental or social impact, serve little purpose in global trade. There is a need to ensure the capacity of international product conformity systems is fit for a digital world and has the utility to be applied across jurisdictions in the global supply chain.

2.3 Scope of this White Paper

This paper focuses on the exchange of conformity attestations pertaining to traded physical products. This conformity information may be requested by commercial parties, as well as public entities. The processes are part of the commercial procedures defined in the UN/CEFACT International Supply Chain Reference Model (ISCRM) and reflected in the UN/CEFACT BUY-SHIP-PAY (BSP) reference data models (RDM).

This paper explores the challenges and proposes principles to govern issuing conformity attestations and sharing these between supply chain actors from the private and public sector. These principles should ensure that conformity attestations are issued and shared in a manner which preserves verifiable connections to physical product delivery, while providing foundations for independent digital verification of the status of an issued attestation and the authority under which it was issued. Defining all data elements contained in conformity attestations (to enable digitalised exchange of content) is not regarded as necessary to achieve these outcomes but would introduce additional possibilities that are not considered in detail within this paper.

The paper does not consider conformity processes for which the applicable regulatory framework involves attestation types other than testing, inspection or certification. The development of uniform and harmonised attestation, in terms of layout and data sets, is also not specifically considered in this paper.

The paper points to concepts that could be applicable regardless of industry type, product type or geography and that would provide access to conformity data, at least in principle, to all types of users including supply chain actors.

The paper is framed particularly around the role of third-party testing, inspection and certification activities (refer 2.1 for detail), although it is considered likely that some of the principles and concepts will have at least some applicability to first- and second-party conformity activities (refer image on next page), as well as to forms of attestation other than testing, inspection and certification.

3 Exchange of conformity attestations

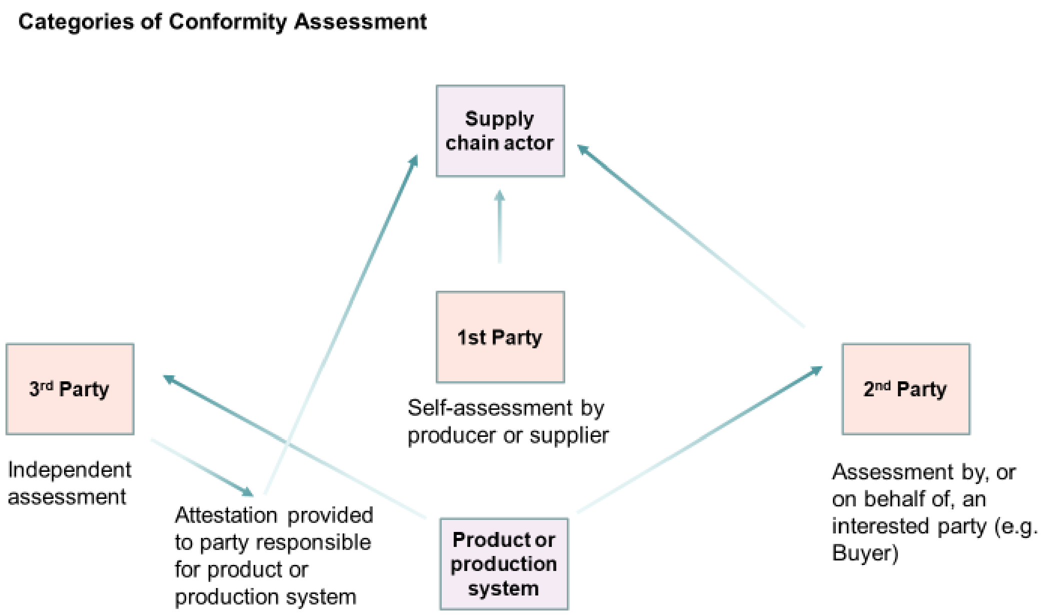
Conformity attestations arise from a set of processes, collectively known as conformity assessment, which can give substance to claims made about a product and to provide confidence in product selection. This chapter explores how conformity attestations are currently shared and points to some of the associated challenges.

3.1 Types of conformity attestations

The most common types of formal conformity assessment which result in conformity attestations are defined in ISO/IEC 17000:2020 Conformity Assessment - Vocabulary and general principles, as follows:

1. Testing – determination of one or more characteristics of an object of conformity assessment, according to a procedure
2. Inspection - examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements
3. Certification – third-party attestation related to an object of conformity assessment with the exception of accreditation

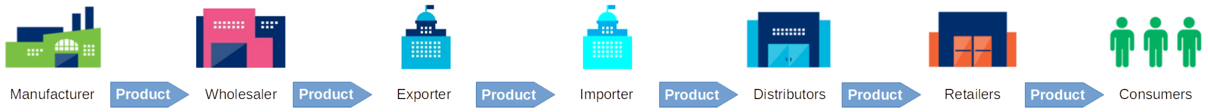
Conformity assessment processes are carried out by conformity assessment bodies (CABs), in accordance with standard methods and approaches. There are different categories of conformity assessment services: first party, second part and third party, depending on the relationship between the conformity assessment provider and the product of interest. This paper focuses solely on the exchange of third-party conformity attestations.


Categories of Conformity Assessment
Supply chain actor
1st Party
Self-assessment by producer or supplier
3rd Party
Independent assessment
Attestation provided to party responsible for product or production system
Product or production system
2nd Party
Assessment by, or on behalf of, an interested party (e.g. Buyer)

Finally, CABs may be accredited, or unaccredited, for any given conformity assessment activity. This distinction is important since CABs operate within a regulatory framework that is specific to a country or group or countries and to the particular product type in question. In some countries there exist accreditation laws requiring CABs to be accredited when assessing certain products. In addition, many governments only recognise conformity attestations from CABs accredited by bodies that are signatories to the global mutual recognition arrangements operated by the International Accreditation Forum (IAF) and the International Laboratory Accreditation Cooperation (ILAC). Therefore, the identity of the accreditation body (where applicable) is often an important data element in establishing the validity of an issued attestation. The use of such identifiers will be explored further in section 4.1.1.

3.2 Supply chain actors involved in exchange

Many different supply chain actors are potentially involved in the exchange of conformity attestations. Supply chain actors might seek to gain access to conformity attestations according to their role in the supply chain. Information typically passes along the chain from producer, to wholesaler, to exporter, to importer, to distributor, to retailer, to consumer and the different supply chain actors have different reasons for accessing conformity attestations.



- Except for the producer, other actors typically seek conformity attestations to guide their purchasing decisions
- except for the consumer, actors seek conformity attestations to enable them to demonstrate to the next actor in the supply chain that the goods intended for sale are fit for purpose.
- government agencies and authorised bodies in both import and export countries as well as transit countries often need to access attestation data for product categories subject to legislative requirements

In the specific case of raw materials or other product inputs, exchange of conformity attestations may only be necessary up until the point at which the materials or products are combined or transformed into new products. But even in such situations, purchasers of a finished product may have an interest and/or duty of care in establishing that all inputs to the product met certain criteria, the so-called tracing.

3.3 Challenges of existing system

Apart from fake product conformity attestations described by the TIC Council [footnote *TIC Council Anti-counterfeiting Committee White Paper, Falsified: Test reports and certificates, TIC Council publication, June 2020*], including genuine attestations that have been fraudulently altered, there are numerous other ways in which conformity claims can be mis-attributed. It is important to note that different processes for exchanging product conformity attestations along a supply chain vary considerably in terms of their vulnerability to specific modes of misuse or fraud. The most common integrity breakdowns in the exchange of conformity attestations might be summarised as follows:

1. Weak or no linkages between the claim and the subject of the claim

It can be difficult to establish whether a conformity attestation is linked to the physical product in question. One difficulty is to establish whether the attestation is linked to an individual item, a batch or a trade unit. Another is to establish whether such links are trustworthy and/or verifiable. For example, the outcome of a laboratory test generally pertains either to the sample as received or to a batch; however, it can be in the interests of some careless (or unscrupulous) suppliers to infer that the conformity attestation applies to the ongoing supply of the product (or even to a related, but different, product). The question of establishing linkages between conformity attestations and products applies equally in the other direction, that is, providing a means for reliable discovery of the conformity data associated with a specific product, batch or trade unit.

2. Managing ‘state changes’ (withdrawal/amendment/expiry) for an attestation

It is difficult to know if a conformity attestation is current, has been superseded or withdrawn. It is even more complex to know with certainty if a claim made in the past was current at the time the product was used. For example, the installation of a building product several years earlier may have been in accordance with a valid certification at the time, despite subsequent changes in standards or regulation.

Once conformity data has been captured within a supply chain, a key challenge is verifying such data at its source. For example, to track ongoing changes in the status of product conformity information as attestations are amended or withdrawn, or the associated credentials, authority, or standing of the holder change, noting that such changes are unlikely to be communicated to all interested parties. These issues arise whether the conformity attestation is of a traditional form or in the form of encoded data, so the solutions need to be applicable for both scenarios.

3. Issuing authority and jurisdictional relevance

It is necessary to identify the authority under which the issuer of an attestation is acting or was acting at the time of issuance. Authorisations granted to TIC bodies are usually specific to certain product types and assessment standards, which adds complexity to any validation process. A conformity attestation issued without an underpinning authority may be worthless in terms of addressing market access requirements or meeting consumer demands. Despite the existence of global mutual recognition arrangements for conformity assessment activities, it is not always straightforward.

The various challenges might be summarised as follows:

1. fake or altered conformity attestations
2. valid conformity attestations presented for products to which these do not relate (including reuse of attestations to support a larger amount of product than is warranted, or other models within a product family)
3. product certification marks applied to products without permission (including substitution of genuine product with fakes)
4. conformity attestations presented in circumstances where the authority of the issuing body is questionable or misrepresented
5. conformity attestation that reflects a different intended use than the purpose for which the product was sold
6. continued use of previously valid attestations or marks despite later restrictions coming into effect.

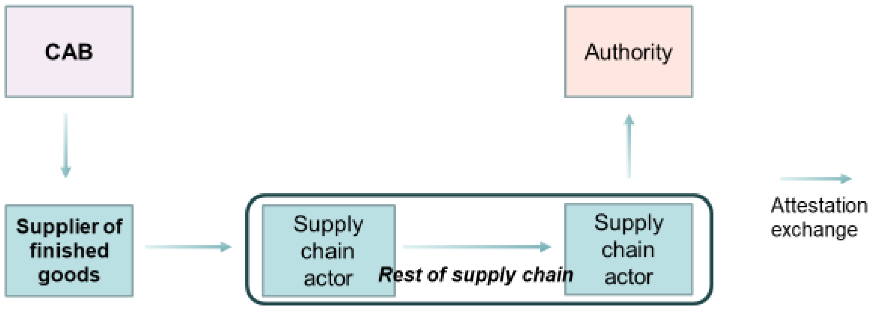
Finding 1: There is a need for linking conformity attestations with physical product and to manage revision and issuing authority status.

3.4 Conformity attestation exchange processes

Outside of the conformity assessment community, the processes by which conformity attestations are exchanged are not generally well understood. Conformity attestations are typically provided initially to the entity that commissioned the conformity assessment activity (commonly the producer or importer of a product). However, once generated, the exchange of the attestation between supply chain actors varies widely depending on the type of attestation, the type of product and the jurisdiction. A variety of existing processes are described and depicted in a simplified manner below (examples 1 to 5).

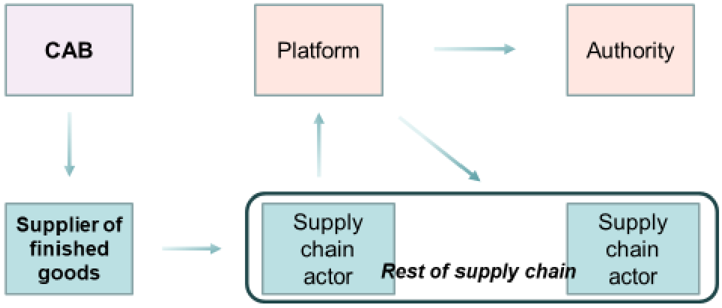
Example 1

The recipient of the conformity attestation directly forwards it (or otherwise makes available) to buyers or users of the product, who may then, in turn, make the information available to other parties within the supply chain. Establishing linkages to physical products generally involves the manual verification of data (typically by comparing parameters such as model type or batch number). This pattern of exchange is common for product categories, such as building and construction supplies, for which the involvement of governments is less central than for some food and health related areas.



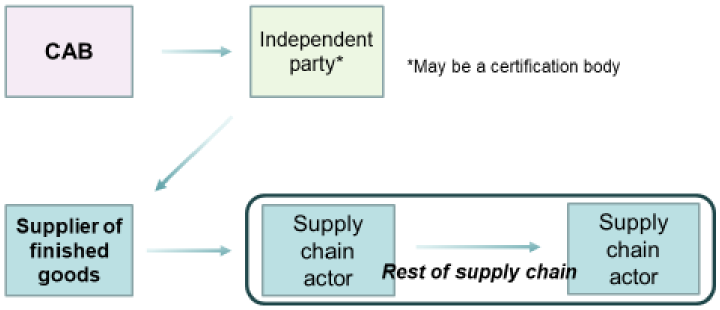
Example 2

The recipient of the conformity attestation (or subsequent supply chain actor) enters the attestation, or key information drawn from it, onto a data exchange platform and attests to any product links which are claimed to apply (with, or without, additional validation or oversight), such as may apply for some single window customs clearance systems.



Example 3

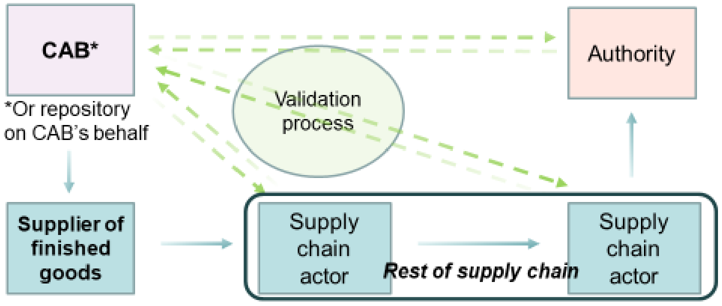
An independent party (which could be a regulatory authority, or product certifier) approves specific CABs to provide conformity details to a repository. Examples of this model can be seen applied in both the regulated space (such as testing of food imports) and the unregulated space (such as industry-operated product approval programs involving subcontracted testing).



Example 4

Providing for verification-at-source for a CAB-issued attestation, through processes that can include manual online verification or digital signing by public/private key encryption. This is emerging as a response by CABs seeking to protect their customers from fraudulent alteration of issued attestations. Although the technologies are not described, a TIC Council report has identified a number of verification databases established by major CABs [footnote *ibid, TIC Council, page 12*].

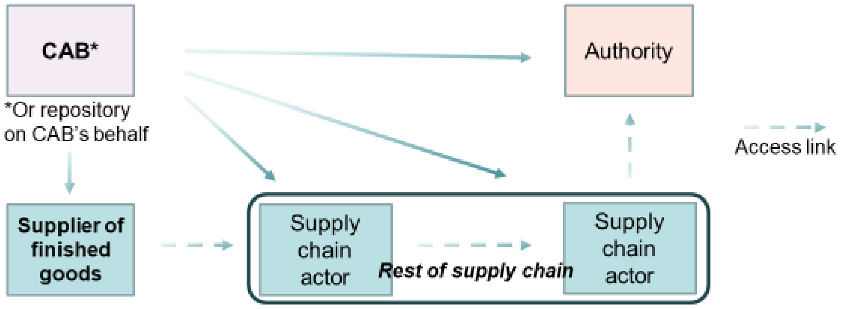
A recent proliferation of third-party digital signing services enabling implementation with little capital investment for document issuers, such as CABs, is another relevant development. A variation to this approach is where an authoritative body offers a validation platform on behalf of CABs, such as the Indian National Accreditation Board for Testing and Calibration Laboratories (NABL) portal, which is provided on behalf of its accredited test and calibration laboratories, or the International Accreditation Forum CertSearch platform, which is provided for management system certifiers globally.



Example 5

While not a common pathway at this time, some CABs that operate verification databases [previous ref] issue barcodes that encode a web address at which the corresponding conformity attestation can be viewed by any user, meaning that exchange of the attestation itself is no longer necessary, provided that the barcode (or other link) is conveyed by supply chain actors.

This pathway has features that are seen as valuable for some ideas explored in this paper and may be more easily adaptable to purely digital processes in the future, as described briefly within section 4.3.



It is important to realise that a genuine product supply chain normally involves processing and assembly operations and comprises a complex network of actors that will typically involve many CABs. Genuine supply chains are likely to contain a combination of the processes depicted above, possibly all of them, operating simultaneously.

This inherent complexity in the exchange process makes it difficult to model the flow of supply chain data and represents a barrier to achieving interoperability of exchange systems within a supply chain and, even more so, across different supply chains. One point which can be drawn from the examples above is, to the extent that data assurance and validation processes for conformity attestations exist, these revolve around CABs (or other parties acting on their behalf). This central role for CABs in data verification holds relevance for later sections of this paper, where the question of linking conformity attestations to physical product supply is considered.

For completeness, it can also be noted that there are cases in some regulatory systems where the authenticity or performance of a product can be established under a regulatory system without any reliance on conformity assessment. This can apply to innovative products for which there is no established standard, for example, products reflecting the outcome of an engineered solution for a specific building application. In these circumstances, attestation will likely be required to demonstrate compliance with the regulated requirements, but not of a type of attestation that is covered by the scope of this paper.

Additionally, some legislative frameworks, for some types of products, remove the need for further exchange of CAB outputs beyond a certain point in a supply chain, that is, the point at which a regulator, or other authority, takes control of product conformity. Examples of such legislative frameworks include some government-operated product approval schemes, approval of processing facilities (often food-related) by a competent authority, or sanitary and phytosanitary certification processes. Such processes for handling product conformity fall outside the scope of this paper (although exchange at earlier points along the supply chain, that is, before legislative control is established over the conformity data, could still be regarded as within the scope).

Finding 2: The lack of any consistent process for exchange of conformity attestations is a barrier to interoperability.

3.5 Legal considerations in cross-border exchange

The legal and regulatory context for the issuing and exchange of conformity attestations is constituted by national, regional, and international law, standards, and industrial good practices. Applied to cross-border exchange of attestations, there are three important aspects:

1. The combination of regulations, as found in World Trade Organisation (WTO) rules and regional or bilateral free trade agreements ('FTA') or national laws, as well as international standards and good practices which have been widely adopted by businesses.
2. The inter-operation of laws and regulations in multiple legal categories (such as authentication, consumer protection and data security).
3. Sets of government-to-business vertical regulations and business-to-business horizontal contractual agreements which, jointly, can provide trust and support for the traceability and integrity of conformity attestation exchange.

The WTO Technical Barriers to Trade (TBT) Agreement provides fundamental principles applicable to conformity assessment procedures to ensure that unnecessary obstacles to trade are not created [*footnote WTO TBT Agreement 3rd edition, Article 5.1.2*] and that confidentiality of information about products originating in a foreign country is respected in the same way as for domestic products and that legitimate commercial interests are protected [*footnote WTO TBT Agreement 3rd edition, Article 5.2.4*].

While noting the guidance in the above principles, there remain inherent legal uncertainties associated with existing systems for conformity attestation exchange. Disputes can arise over the availability or status of issued conformity attestations, for example:

1. Due to the risk of exposing commercially sensitive information (such as the identifier of suppliers), not all necessary information may be made available by parties in a timely manner, which can lead to incorrect decisions or disputes.
2. Outside certain legislated arrangements, the status of the issued conformity assessment data is typically subject to revision, yet there is a lack of recognized processes through which supply chain actors are notified of changes and no clear legal accountability for distributing this knowledge.
3. There may also be potential conflict of laws based on the localization of processing of conformity attestation data.

Where disputes arise regarding the availability, validity, relevance or status of conformity attestations, legal enforcement can be challenging, for reasons including:

1. The nature of sequential buy/sell contracts along a supply chain means that an end-user seeking legal remedy for product failure may need to pursue a series of consecutive legal suits that might dissuade the aggrieved party from seeking redress.
2. This environment of diluted accountability can also act to embolden parties to illegally alter data, to imply spurious connections between conformity assessment data and physical product, or to make dishonest claims regarding the authority under which conformity assessment data has been issued. In some economies, for some products, legislative frameworks exist to place an onus of accountability on each actor authenticating product claims and forwarding data that affects product compliance, but such arrangements are not widespread.
3. Enforcement may be further complicated by challenges arising from the conflict of laws between different jurisdictions.

What is needed is a robust framework for the digital exchange of conformity attestations that can respond to the legal complexities outlined above. Digital processes carry potential to mitigate many of these uncertainties through the exchange of data that is verifiably linked to both the product and the issuing authority.

Finding 3: Paper-based exchange of conformity attestations is inherently affected by legal ambiguities & exploitable loopholes which can exacerbate other process shortcomings.

3.6 Legal considerations applicable to cross-border digital interoperability

Measures to ensure exchange of, or access to, product conformity attestations should go beyond creating a digital representation of a document that is e-authenticated, e-signed and electronically shared through a recognised format and technology. They must ensure that all of the following outcomes are met:

1. establishing a match between conformity attestations and the physical product
2. verifying the authority and status of the certificate issuers
3. constant provision for verifying along the whole supply chain that an attestation is both genuine and reflective of the current issue status.

Achieving these outcomes in a digitalised setting presents legislative challenges, in at least in four areas:

1. Cooperation on conformity assessment procedures in digital trade
2. Digital legal identifiers

3. Data security and integrity
4. Balancing transparency and privacy protection

Existing cross-border provisions for conformity assessment procedures are generally not framed in the context of digital trade. Exceptions are the recently concluded Digital Economy Partnership Agreement (hereinafter 'DEPA'), concluded by Singapore, Chile, and New Zealand, on 12 June 2020 and effective for New Zealand and Singapore on 7 January 2021; the Singapore-Australia Digital Economy Agreement; and the Singapore-South Korea Digital Economy Agreement. These provisions are laudable, however, they are bilateral in nature and cannot establish the linkage and interoperability among multiple countries in the global supply chain.

Entity identifiers are an important element in discussion of conformity attestation exchange since the identity of commercial parties and CABs from different countries will need to be verified. However, few international trade agreements provide provisions for agreed legal identities. DEPA, the Singapore-Australia Digital Economy Partnership Agreement, and the Singapore-South Korea Digital Partnership Agreement are among the first international agreements to address this issue. All contain a similar provision suggesting that parties to the agreements promote the interoperability between their respective regimes for digital identities by fostering technical interoperability or common standards or recognition of each other's legal framework or regulatory effects. (viz., Article 7.1 of the DEPA, Article 29 of the Singapore-Australia Digital Economy Agreement, Article 14.30 of the Singapore-South Korea Digital Economy Partnership Agreement]. However, these provisions cannot bring benefits for commercial parties based outside these member states.

Cybersecurity and data protection are also key considerations in ensuring the security and integrity of conformity attestation data in future digital exchange systems. Leading FTAs such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), United States-Mexico-Canada Agreement (USMCA) and the Association of South-East Asian Nations (ASEAN) Agreement on Electronic Commerce recognise that cybersecurity threats undermine confidence in the global supply chain [e.g., Article 14.16 of the CPTPP, Article 19.15 of USMCA, and Article 8 of ASEAN Agreement on Electronic Commerce]. However, specific measures relevant to the digital exchange of conformity attestations are not defined at this time.

Finally, the exchange of conformity attestations in the global supply chain also requires a careful balance of transparency and privacy protection. Privacy should be guaranteed in respect to manufacturers and consumers. The latter may use their personal devices to scan a QR code on a product package or access a CAB website for conformity data. Privacy protection instruments in a digital context have been developed in multiple international fora and include the Organisation for Economic Cooperation and Development's (OECD) Privacy Guideline, the EU's General Data Protection Regulation (GDPR), Asia-Pacific Economic Cooperation's (APEC) Privacy Framework. In addition, relevant provisions can be found in other more general documents, for example, OECD, Digital Trade Inventory - Rules, Standards and Principles (page 19) and Article 4.2.3 of the DEPA. However, these instruments mostly provide principles and best-effort provisions, with detailed rules for privacy protection left to domestic laws, where significant inconsistencies can exist.

Finding 4: There are gaps in the existing legal framework for cross-border data exchange. Therefore, any work towards digital exchange systems for conformity attestations must be made in the knowledge that the environment is ill-defined and likely to change, which could have implications for future choices of identifiers and specific digital technologies.

4 Attestation information sharing technology

To make the required attestation information available to the various stakeholders in the supply chain, technological building blocks will be required to meet different requirements for the overall solution. The sections below in this chapter cover required building blocks identified during development of this paper.

4.1 Digital identifiers

4.1.1 Minimum data information

Conformity attestations contain a large number of data elements that can also vary considerably depending on the type of attestation. The scope of this White Paper is not the harmonisation of attestations or their data elements. The point made here is that it is necessary to identify a limited set of data elements that are fundamental to the exchange of these attestations:

1. Identifiers for the specific product/model
2. Identifiers (if applicable) for the batch, trade unit or individual item that is subject to conformity assessment
3. Identifier for each individual conformity attestation
4. Revision status of the attestation
5. Identifier for the issuing party (i.e., CAB)
6. Identity of the party (if applicable) under whose authority the issuing party is acting (e.g., accreditation body)

Existing reference data models, such as CEFACT Reference Data Models, WCO Data Model, contain harmonised data elements including identifiers for products, distributors, documents, etc. An in-depth review needs to identify applicable identifiers and from these RDM for the TIC sector and identify gaps in these data models. It is expected that some data elements require more granularity to be used for the TIC sector.

While examples are provided within this paper of suitable identifier types for products and attestations, these are intended to be illustrative of general principles, rather than prescriptive. No examples of specific identifier types for parties (such as CABs and accreditation bodies) are given in this paper, but there are several globally recognised alternatives that can be used and selecting a preferred option is beyond the scope of this paper.

In the following sections, several classes of identifiers are explored and these may offer suitable patterns for achieving verifiable digital exchange of conformity that is also linked to physical product flow.

4.1.2 Using identifiers to link data

The first issue to deal with is the necessity of identifying both the attestation and the physical product to which the attestation relates.

For product certification, the product identifier would normally refer to general production but, in the case of testing or inspection results, the product identifier may need to be specific to a single batch (or even to a logistics identifier if that became relevant, such as where a shipment might be tested). There exist global schemes for product identification *[footnote E Ganne and H Nuygen, Standards Toolkit for Cross-border Paperless Trade, Joint WTO/ICC publication, March 2022]*, which range from identifiers for general product categories, such as the Harmonized System developed for the classification of goods for customs processing (footnote https://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx) to identifiers that uniquely distinguish specific product lines from individual producers and even individual batches or lots of a given product, for which the Global Trade Identification Number (GTIN), compliant with ISO/IEC 15459-6 [footnote *ISO/IEC 15459-6:2014 Information technology - Automatic identification and data capture techniques - Unique identification - Part 6: Groupings*] is the most widely used example. Physically marking a unique product identifier on packaging and/or the product itself is standard practice for retail products (which typically incorporate a GTIN). Additional logistics identifiers *[footnote https://www.gs1.org/sites/default/files/docs/gs1_iso_brochure.pdf]* are available to uniquely distinguish logistical units (such as shipping containers), consignments and even individual product items and all based on the ISO 15459 series of standards. Where conformity attestations are related to a shipment, the use of a standard shipping mark, *[footnote https://unece.org/fileadmin/DAM/cefact/recommendations/rec18/rec18_ecetrd271e.pdf]* as described in the UNECE Recommendations 18, may provide a way to create further linkages.

There also exist global schemes for organisational entity identification (based on ISO standards), which is useful when seeking to specify an individual producer, possibly in conjunction with a particular production site, which may be identified with global schemes, based on ISO standards. In the case of quality, safety and environment management system certifications, the connection from the attestation to an individual product is meaningful, but it is indirect, since such attestations apply to the producer (specifically to the certified production sites), rather than directly to the product. Therefore, while such attestations should not directly reference product identifiers, references made within a conformity attestation to unique site locations should, in principle, provide a pathway for data linkages to be made with the physical product supply (potentially using concepts such as Linked Data).

There is also a requirement for identification of the attestation itself, since data connections to physical products must link to the specific attestations required to substantiate any claim about the product. While all CABs generally adhere to the principle of uniquely identifying issued attestations, these almost invariably rely on internally generated identifiers, which in turn require some sort of index or registry to uniquely establish a correlation between an attestation and a physical product. This might represent the starting point for defining business processes for linking conformity attestations to physical supply, which could be made available to any supply chain actor.

It is important to recognise that there are already very large numbers of attestations in existence. Furthermore, existing databases and services offered by Scheme Owners or Accreditation Bodies will not immediately start using a common globally unique identifier scheme. Therefore, global identifier schemes and existing identifier schemes will continue to co-exist, but need to transition from ‘analogue’ to digital. At the same time it is important to align to global identifiers used by the trading community, both private and public sector to avoid duplication. This White Paper therefore recommends using identifiers based on global data standards, like those provided by ISO or the United Nations. That said, there is scope for global identifiers to be used primarily for the exchanges of information across systems, whereas the existing identifiers might continue to be used as ‘intuitive’ identifiers for use by human beings. Furthermore, there is scope for decentralised architecture accessing objects such as verifiable credentials (VCs) to facilitate digital communication across different platforms, provided that a common understanding of entities and identifiers can be achieved (further insights may be gained from the UN CEFACT White paper *[footnote https://unece.org/sites/default/files/2022-06/010_Verifiable-Credentials-CBT.pdf]*

Different stakeholders will have different expectations about the data they would need to see related to a product. While this is not a problem for some types of attestation (i.e. those that are typically made freely available to supply chain actors), shortcomings can be revealed where access to attestation content is blocked to protect some of the content for commercial reasons. This challenge is considered further in section 4.4.

Finding 5: The critical data elements relating to conformity attestation exchange are dominated by identifiers and further work is needed to review the CEFACT data models having potential relevance to the identifiers of interest. It is further noted that established systems already exist for creating the types of linkages required to address the problem statement, including the use of globally unique identifiers.

4.2 Management of conformity data lifecycle

A conformity attestation, once issued, can change status over the period of its lifecycle in a way that depends upon the type of attestation. Digitalising status information in the context of conformity attestations warrants further investigation, since the existing definitions for certificate statuses found within UN/CEFACT e-Cert BRS Section 5.3.3, which reflect cross-border operations relating to export certificates, do not address the processes that typically apply within the TIC sector. In general, test, inspection and calibration outputs remain valid unless withdrawn by the issuing authority (e.g., as a result of replacement issued to correct an earlier error). Other types of attestations, such as product certificates, may have a defined period of validity (which may be subject to extension), although such attestations can also be suspended or withdrawn by the issuing authority (if the conformity is no longer guaranteed) or revised if the associated product is changed, requiring some form of reassessment. However, to complicate matters, individual Scheme Rules may define specific statuses applicable to certificates issued under that scheme.

It is therefore proposed that future work be undertaken to define a general set of statuses be developed applicable to conformity attestations, drawing upon existing UN/CEFACT definitions to the extent possible and with allowance for equivalent terms to be recognized against a given status (for example cancelled/withdrawn/revoked or revised/amended or issued/current) to accommodate divergences in language between Schemes.

In any case, up-to-date knowledge regarding the status of a conformity attestation is an inherent aspect of its validity and therefore needs to be available to market surveillance and regulatory authorities, customs authorities, importers, wholesalers and consumers. The required degree of transparency may depend on the requirements of the party requesting the conformity assessment, or applicable Scheme rules (where relevant) or, depending on the consequences of a status change, may also be subject to legislative requirements.

In general, accreditation requirements obligate CABs to inform the party to whom an attestation was issued (sometimes referred to as the certificate holder) of the fact that an attestation is no longer valid and may allow the body to choose its own appropriate communication channel. However, depending on the type of communication, this updated information may not be propagated along a supply chain to reach all interested parties, such as regulators and end-users.

There are various approaches used by issuing authorities to enable authentication of their attestations, many involving encryption processes based on public or private keys. Commonly known as 'digital signatures', these processes provide for authentication for the point in time when the conformity attestation was originally issued and represents a means of protection against alteration. The digital signature itself is a mathematical construct (a hashing algorithm) that remains functional until such time as the 'digital certificate' held by the signer may be revoked, however, they do not neatly handle changes in status of an attestation. There are other examples where issuing authorities, or certification scheme owners or other agencies make the current status of an attestation visible, through either a central database or central list, such as a revocation list.

An alternative is to consider the exchange of a link to an attestation, rather than the attestation itself, meaning that every instance of access will be directly to the authoritative version. Use of Linked Data and Digital Link Resolvers represents an example of such an approach that may be adaptable to a greater variety of situations, including the ability to link to a variety of related information in addition to the attestation itself. Digital Link Resolvers may be used as an "index" and accessed by little or nothing more than the globally unique identifier for an item/entity, which activates a reference/link to the online service that contains the Linked Data about that identifier. For a conformity attestation, the data held in the Digital Link Resolver may be limited to the unique attestation identifiers and the URL (plus the identifier used by the target online service). Certain decentralised methods, such as verifiable credentials mentioned in section 4.1.2, which can be exchanged and stored in 'digital wallets', may offer similar advantages while carrying the promise of additional control and security.

Regardless, one important principle when dealing with management of conformity data lifecycle is that the issuer of the attestation be recognised as retaining authority over the attestation, in order to provide certainty over the state (e.g., withdrawal, amendment, expiry) of an attestation over its valid lifetime.

Finding 6: Managing revision status is more complex than might first appear and a variety of incompatible approaches are being taken to address this. An important insight is that CABs (or parties acting on their behalf) are central to the process and that exchanging links to attestations may be more effective than exchanging attestations.

4.3 Patterns for conformity data access from physical identifiers

4.3.1 Physical identifiers

There exist a variety of processes by which identifiers can be placed on physical objects (such as products, or documents) that can be read by both humans and machines. Two technologies are dominant: Barcodes and Radio-Frequency Identification (RFID). Barcodes have more immediate relevance to this paper, among which there are two main approaches: Linear barcodes and two-dimensional (2D) barcodes. One advantage of 2D barcodes (a family which includes the commonly used QR Code) is that they contain sufficient space to capture many different data elements that can be read and interpreted in a single barcode-scan, using global data standards such as described in the GS1 Scan4Transport guidelines [footnote: https://www.gs1.org/industries/transport-and-logistics/scan4transport]. Furthermore, the capacity of the 2D barcodes allows stakeholders to include a Uniform Resource Identifier (URI), creating a digital link to the physical object, which is sometimes described as a 'digital twin' to that object.

2D barcodes placed on products can encode a link to the producer's own website, but the table below illustrates how a barcode can also encode the web location of a conformity attestation, with or without a central hosting organisation.

The barcode to the right encodes the link/URI https://resolver-dv1.gs1.org/253/871423175000060012051
The value following “253/” indicates a GS1 GDTI (871423175000060012051) which is a globally unique identifier. The first part of the address points to an external ‘index’ where an issuer may register that they have issued an attestation as well as the target URI where the attestation is located. Additional links to other information may be created within such an ‘index’ (refer section 4.3.2).

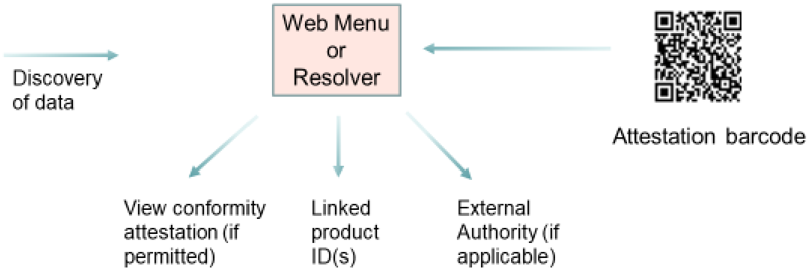
Alternatively, the issuer could simply encode direct links to their own web index of attestations. The identifiers used could leverage global identification systems, such as described in ISO/IEC 15418 *[footnote ISO/IEC 15418: 2016 Information technology — Automatic identification and data capture techniques — GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance]* or might be proprietary in nature (the latter could be based on syntax and semantics described in ISO 8000-115). *[footnote ISO 8000-115:2018 Data quality - Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements]*

4.3.2 Product and authorisation linkages from a conformity attestation

There are many examples *[footnote ibid, TIC Council, page 12]* of URI links made from conformity attestations to an issuing authority’s website. However, the accessible information has not normally extended to information about the associated products (ie, beyond the conformity details) and accessing linked data using such tools represents quite a new area of research. There appears to be no reason why testing laboratories, for example, could not record displayed product identification barcodes in issued attestations, and no reason why product certification bodies could not similarly record product identification codes along with the standards to which the product had been certified. Indeed, there are examples *[footnote Digitalisation of Product Certificates, Claims and Credentials, NATA/JAS-ANZ/GS1 joint publication, October 2022, page 21]* of encoding an ISO 15459 compliant identifier (specifically, a GTDI) into issued test reports to establish a digital link with the specific batch of product that is the subject of the test report.

This approach also points to a framework for enabling a user to establish the independently assessed competence (where applicable) of the body issuing the attestation, for which precedents do exist. The laboratory accreditation authority in India, NABL, currently promotes inclusion of a QR code on all reports issued by calibration and test laboratories, linking to the corresponding accreditation details hosted on the NABL website. Processes involving cryptographically verifiable digital signatures, referencing back to the appointed accreditation body, are also being actively developed by some national authorities.

Extending the general concept, within a setting based on accessing attestations (rather than exchange), a user wanting to view/verify the attestation will be accessing the application operated by the issuing body or other authority, so it should be possible to provide additional links to the credentials/competency of that issuing body.


Discovery of data
Web Menu or Resolver
Attestation barcode
View conformity attestation (if permitted)
Linked product ID(s)
External Authority (if applicable)

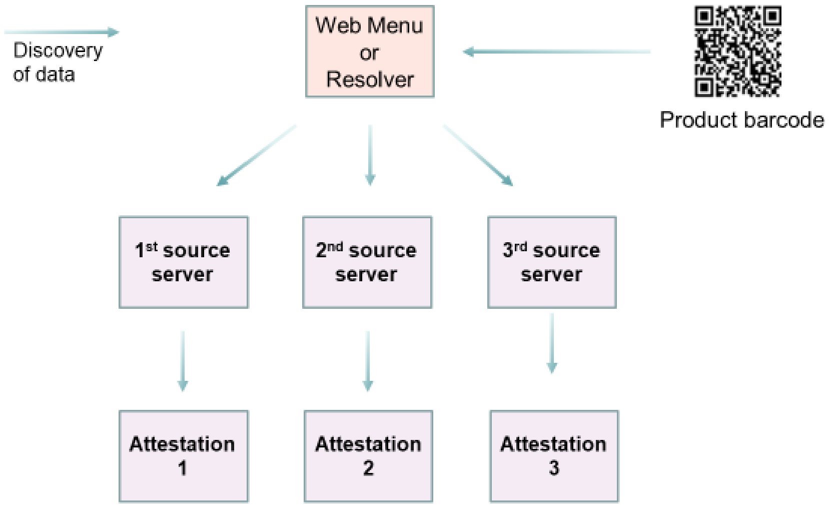
A web menu or resolver as depicted above might be operated by the CAB, or a third-party supply platform or even a national registry. For certificates that are made available publicly, the certificate itself does not need to be shared, only the barcode (or other type of link).

4.3.3 Conformity attestation linkages from product data

Linking to conformity attestations (at their source) from a product identifier represents a more challenging application, but is a logical extension of the ideas that have been presented earlier in this paper. It is also consistent with existing and emerging legislation in some jurisdictions aimed at increased transparency of linkages between product markings and the underpinning conformity assessment information.

The intention of enabling this type of data access is to place greater control in the hands of supply chain actors and consumers to verify a product's credentials when it is supplied, but also to enable industry practitioners to identify a product's attributes at the point of specification to ensure that it is fit for the intended use (which in many cases is also necessary to satisfy regulatory conformity requirements). The ability to ensure that the product, once selected, is digitally linked to its accompanying conformity attestations, enables a robust authentication process. This is even more important where components are being delivered for the purpose of assembly into a system, where establishing traceability can be especially challenging.

URIs, such as web addresses, are commonly encoded onto products or the product packaging, to link to repositories of information that may include conformity data associated with the product. Such URIs typically lead to the manufacturer's website but without subsequent linkages to independent data sources. This makes independent validation of the data difficult and perpetuates the challenge of establishing a defined connection between retrieved attestations and the physical product shipment of interest.



A web menu or resolver as depicted above might be operated by the manufacturer, or a third-party supply platform, or even a national registry.

Finding 7: A set of complementary processes based on linked data can be expressed in generic terms that should serve to address the problem statement.

4.4 Defining levels of digital information access

Section 4.1.1 dealt with the minimum data information needed to establish some key linkages to conformity attestations, in order to address the problem statement. However, potential patterns of data access that were described in the previous section were presented in terms of assuring maximum transparency of data to all supply chain actors. However, in reality, not all conformity attestations can be freely shared in this manner since they may contain protected commercial information, yet existing attestation exchange processes do not accommodate this functionality.

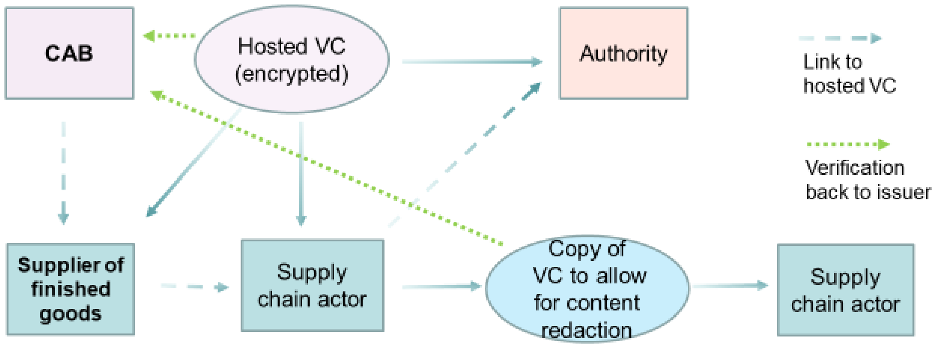
Digitalisation provides potential new ways of navigating this aspect. This concluding part of Section 4 will explore this matter from the perspective of harmonisation with other elements that have already been explored, noting that a full treatment of such a complex area falls outside the scope of this paper.

The minimum data information represented a set of data points that could be digitally associated with an attestation. However, this does not mean the remaining content of the conformity attestation must also be shared. Examples of digital interrogation, based on restricted data points, are quite widespread. In the transport area, these include Bills of Lading in the FIATA eFBL platform *[footnote https://www.efbl.fiata.org/efbl]* where certain limited data, such as date of issue, issuing party or issue status, is searchable to validate an issued document. In the same way, digital correlations can be established between a conformity attestation and real world processes/events, without necessarily exposing the human-readable attestation. But this is merely the start of a journey into full digitalisation.

Although outside the scope of this paper, defining data elements comprising the complete content of conformity attestations opens the possibility for sharing of data to an arbitrary level of discrimination, based on permission structures that reflect the underlying protocols for data encoding. Complete digital encoding has been demonstrated for calibration certificates according to ISO/IEC 17025 [footnote *Hackel, S. et al., The fundamental architecture of the DCC, Measurement: Sensors, Volume 18, 2021, 100354, doi: 10.1016/j.measen.2021.100354; see www.ptb.de/dcc for the most up to date information*] and is being developed for conformity assessments according to ISO/IEC 17065 of equipment in legal metrology as well as in the legally regulated area of explosion protection [footnote *Foyer, G. et al., in preparation; see https://www.qi-digital.de/en/digital-certificates for the most up to date information*]. Extensible Markup Language (XML) provides the technological basis for these initiatives.

There are other promising technologies which can build upon the digital advances just described. These might include the opportunity for verifiable credentials (VCs) encoding attestations that could be centrally hosted (and accessed from a private link) but which can also be copied and redacted as necessary to suppress sensitive information for subsequent supply chain actors, while retaining the inherent ability to be cryptographically verifiable by all parties as both a genuine and current attestation. This is likely to become an interesting area of future activity as decentralised approaches may offer solutions to the challenge of suppressing commercially sensitive information without degrading the exchange process.

Below is a schematic which shows one possible way redactable exchange might occur in future. Redaction is not needed for all attestations but the flexibility to implement such, when required, is key. The main point of this diagram is to highlight the structural similarities with the process highlighted as Example 5 in Section 3.4 , while also noting the expanded functionality that can be derived from decentralised digital exchange.


CAB
Hosted VC (encrypted)
Authority
Link to hosted VC
Verification back to issuer
Supplier of finished goods
Supply chain actor
Copy of VC to allow for content redaction
Supply chain actor

The ideas in this final Technology subsection illustrate that adoption of ideas presented in the paper (particularly the centrality of the CAB, or their nominated host, in validating attestations) may enable much more powerful tools to be deployed in future, in a way not presently possible due to the fractured nature of existing attestation exchange both within supply chains and across different supply chains.

Finding 8: While the technology exists to achieve selective suppression of sensitive data, this cannot be consistently implemented due to the fractured way conformity attestations are currently exchanged. A more central role for CABs may make more consistent application of technology possible, from a process perspective.

5 Findings and next steps

The analysis contained in the White Paper points to a number of findings that include challenges and ways of addressing the problem. These are summarised in this closing chapter, which also establishes several principles and an outlook for how its proposals can be taken forward.

5.1 Summary

The challenges associated with existing systems for conformity attestation exchange within supply chains are explained (Section 3.3) as arising largely from a lack of reliable linkages (that is, linking attestations to physical product, to the authority under which the attestation was issued and the revision status). The lack of any consistent mechanism for accessing conformity attestations (Section 3.4) or well-defined supporting legal arrangements (Section 3.6) are also seen as barriers to finding systematic and interoperable solutions.

A set of ideas are explored in Section 4 that outline possible ways of addressing the Problem Statement. Insights are provided (Section 4.1) as to how conformity attestations might be linked to physical product, using existing identifiers and widely used technology. The possibility of exchanging links to attestations, rather than the attestations themselves, is explored (Section 4.2) and this places CABs or their nominated host (such as a Scheme Owner or other authority) in a central role as both the source and the validating entity for conformity attestations. The concept is expanded (Section 4.3) to frame a potential system involving access to conformity attestations (rather than exchanging such), including the possibility of digitally linking to attestations from physical products that carry barcodes (or other identifiers). The suppression of commercially sensitive data, which can be required for some types of attestations, is considered in Section 4.4 where it is noted that the type of exchange structure described earlier in the paper might be adapted to address this issue as well, using existing technologies.

It is acknowledged that further work is needed to explore the application of technologies to attestation exchange (particularly in regard to the selective redaction of sensitive information). At the same time, the potential value to global supply chains warrants further investigation of the concepts presented.

The use of identifiers is a fundamental concept in this paper and it is recommended that further work be undertaken to identify applicable identifiers from relevant CEFACT RDM (and identify gaps in these data models, as it is expected that some data elements require more granularity to be used for the TIC sector). To the extent possible, the use of globally unique identifiers is also recommended, to simplify exchange of data among different platforms. Development of a CEFACT BRS is recommended as a priority, to bring a greater level of clarity to these concepts at an inter-governmental level.

5.2 Principles

Several principles have been identified that may support future efforts directed towards digital exchange of conformity attestations:

- Recognition of CABs as having authority over the content of their attestations and that URL links with issued attestations should digitally reference back to the CAB, or to a host acknowledged by the CAB (which could be a recognised national or international competent authority).
- Recognition that the authority of a CAB (where applicable) to issue attestations should be established by digital reference back to the appointed Accreditation Body, Scheme Owner or national or international competent authority.
- Prioritising awareness and adoption of interoperable international data standards to avoid splintering of verification processes into data silos.
- Supporting the adoption of globally unique identifiers for products and attestations as a way of simplifying the processes for data exchange.

5.3 Implications and outlook

Interest and demand for digital processes for accessing and verifying conformity attestations may increase as manual verification of attestations becomes less feasible in digital trade scenarios and as governments,their regulators and other supply chain stakeholders look for more effective and efficient tools to limit the incidence of non-conforming products entering the market. Opportunities also exist for regulators or Scheme Owners to specify the use of product identifiers in the resulting conformity attestations, as a way of strengthening trust in their own processes.

The key outcome from this paper is the unique position held by CABs for creating connections between conformity attestations to physical products and that CABs might be encouraged to provide URI links with issued attestations to enable connections with product to be digitally processable. Such voluntary processes could be implemented at the level of individual CABs, or delegated to Accreditation Bodies, or Scheme Owners (where applicable), national or industry level bodies, or for some types of attestations even at a global level.

For the avoidance of doubt, no suggestion is being made for the creation of centralised systems, beyond those currently in existence. Rather, an opportunity is being identified for indexing of existing databases.
It is considered that the Problem Statement could be addressed through an integrated ecosystem of CABs, leveraging existing product identifiers (to the extent available) and which might be encouraged through the globalised arrangements under which the conformity sector already operates.

Potential costs to CABs in introducing the capacity for capture of product linkages into attestations should be acknowledged. The extent of ongoing cost/impact may depend upon whether such information is applied only upon request from the client, or actively collected as a routine activity. There might also be cost involved in facilitating electronic access to attestations and associated product linkages, although many of the required structures may already exist, in the form of CAB, Scheme owner, Accreditation Body and other databases already established for the sharing of validated conformity information.

Research through National Quality Institutes or non-governmental organisations would be welcomed, to further test the concepts at a global level.   A further opportunity exists for engagement and harmonisation with CABs responsible for calibration of scientific measurement instruments (these CABs operate under the same ILAC accreditation framework as applies for testing), as well as closely related areas like trade measurement, where intensive work towards formalising digital certificate issuance is being undertaken by bodies such as Physikalisch-Technische Bundesanstalt in Germany.

Advancement of the ideas will require wide engagement with stakeholder groups internationally. Collaboration between relevant global bodies will be important to avoid the creation of splintered or siloed systems in future developments.

Appendix 1 - Some relevant technologies

The Table below provides a brief survey of some established and emerging technologies, including a brief description of each and a statement about why the technology might have relevance to the digital exchange of conformity attestations. It is noted that such a list represents a point in time and that technologies will continue to evolve.

Technology	**Description**	**Relevance to digital conformity**
JSON and JSON-LD	JSON is an IETF specification for a simple representation of digital data using Javascript notation *[footnote https://www.rfc-editor.org/rfc/rfc7159]*. JSON is the most popular representation for digital data in web services in use today. JSON-LD is a W3C specification for Linked Data *[footnote https://www.w3.org/TR/json-ld11/]*.	Given its simplicity, wide tools support, and popularity amongst web developers, JSON is a worthy candidate for digital conformity data representation. Example {"CertificateNumber" : "871423175000060012051”} JSON-LD semantic tagging allows verifiers to consistently extract the data they need at runtime, irrespective of variations in certificate structure and content. The key idea is that any data element in any JSON document can be linked to a global standard vocabulary definition. So, the consumer of a document containing JSON-LD can be confident of consistent meaning assigned to a term irrespective of the document type that contains it.
XML	Extensible Markup Language (XML) was developed by a working group formed under the auspices of the World Wide Web Consortium (W3C) in 1996 *[footnote www.w3.org/TR/xml/]* and has established itself internationally as a widely accepted data exchange format. Conversion to other data exchange formats such as JSON is easily done. Furthermore, many established markup languages such as MathML are based on and can directly be included within XML structured data.	XML was originally designed as a document format and is therefore well-suited for documents such as digital certificates. It has been extensively used in IT for over 20 years. XML syntax allows for the definition of secure, simple and complex data types and provides the means for an automated validation of data structures and properties through XML schema files. Namespaces, reference IDs, and attributes allow an easy integration of semantic meaning to data and linking with other metadata. Cryptographic processes can be applied robustly and securely to XML data structures.
PKI	Public key infrastructure is a generic term for a wide variety of protocols and algorithms that are based on the use of public and private key-pairs to digitally sign and encrypt documents in order to support secure and high integrity data exchange.	Product conformity attestations exist to provide trust to the marketplace. Digitalisation of conformity attestations without corresponding digitalisation of trust would be of limited value. Public Key cryptography and digital signatures provide a means for the integrity of the attestation to be maintained irrespective of where it is stored or how it is shared.

DID and VC	The W3C has defined standards for Decentralized Identity (DID) and Verifiable Credentials (VC). These specifications are built upon JSON-LD and PKI and underpin a new and highly scalable decentralised framework for sharing of high integrity digital data. DIDs allow parties in the supply chain to prove their identity, and VC is a standard way to express verifiable claims made by issuer parties about any subject party or product.	Most supply chains will cross multiple industries and geographies, each with one or several distinct supply chain systems and platforms. There will never be one system to rule them all and so for digital product conformity claims to follow goods throughout the supply chain a scalable solution such as VCs is needed. Like the chip in an e-passport, a conformity attestation VC is issued to the holder and travels with the products and can be verified manually or by systems. There is no dependency on shared platforms or technologies.
ZKP	Zero Knowledge Proofs represent a collection of cryptographic techniques for proving that something is true without revealing the underlying evidence.	Product conformity attestations may include commercially sensitive trader party and product information, along with the conformity results. ZKP provides the ability to share verifiable conformity claims without leaking sensitive information. There are some practical implementations associated with VC technology where ZKP is used for selective redaction or selective disclosure.
QR	A QR (Quick Response) is a two-dimensional (2D) barcode that is easily and cheaply printable on any product. Often the QR codes represent web URLs so that, when scanned by anyone with a smartphone, the user is taken to a website. QR codes can also embed further data, such as product specifications or secret keys.	QR codes provide a very effective means to bridge the paper-digital divide by supporting a hybrid model where links to digital conformity attestations can be printed on PDF certificates. This allows issuers to 'go digital' without dependency on consumer or verifier maturity.
Linked Data	Linked data is structured data which is interlinked with other data, so it becomes more useful, e.g., through semantic queries.	It builds upon standard web technologies such as hypertext transfer protocol (HTTP), Resource Description Framework (RDF) and URIs, but rather than using them to serve web pages only for human readers, it extends them to share information in a way that can be read automatically by computers. Part of the vision of linked data is for the internet to become a global database.
Digital Link Resolvers	Resolvers are online services based on Linked Data standards. These services 'resolve' identifiers to one or more sources of information about the identified item.	Resolvers can, for example, link a Product identifier to information about the product, including product conformity attestations to substantiate product claims. For hardware, they can link to things like instruction manuals and usage videos. At the same time, resolvers can link an identified item to information for business partners such as recall/revision status APIs, master data, (hazardous materials) handling instructions and much more.