

# Verifiable Credentials for Cross-Border Trade and Other Use Cases: Proposed Contributions by Singapore Infocomm Media Development Authority and Singapore Government Technology Agency



TradeTrust – A digital utility that comprises a set of globally-accepted standards and frameworks that connects governments and businesses to a public blockchain to enable trusted interoperability and exchanges of electronic trade documents across digital platforms.

## Current challenges of cross-border trade documents exchanges

Current cross-border trade documentation spans many documents and processes, and is a manual, time-consuming, and resource-intensive process for all stakeholders. The paper-based processes are still practiced today as there is currently no easy way to verify the accuracy and authenticity of the supporting trade documents via digital means. This results in inefficiency and delay as time required to process the paper-based documents for clearance may far exceed the actual time of physical movement of goods. According to a study<sup>1</sup> by McKinsey in 2022, documentation for a single shipment can require up to 50 sheets of paper that are exchanged with up to 30 different stakeholders.

## How does TradeTrust address these challenges

To address these inefficiencies, we have developed TradeTrust. TradeTrust, which is built upon OpenAttestation framework, comprises globally accepted standards and frameworks that allow governments and businesses to issue, verify and effect title transfer of electronic documents across different digital platforms seamlessly. TradeTrust can help to protect the trustworthiness of digital documents using cryptography and decentralised identifier (DID) for the verification of their authenticities and their provenances.

## What documents can TradeTrust support in their digitalisation

As a framework, TradeTrust is designed and developed to support the digitalization of two categories of documents used in Cross-Border Trade and Trade Financing processes. The first category is known as the Verifiable Document where the integrity or the trustworthiness of the document can be verified. Examples of such documents include the Certificates of Origin, Commercial Invoices and Packing Lists etc. The second category is Transferable document (or document of title) where it confers title ownership to an asset and the ownership can be transferred from one party to another. Examples of such documents include the negotiable Bill of Lading, Bill of Exchange, Warehouse Receipts and Promissory Notes etc. An electronic Bill of Lading (eBL) that is issued using the TradeTrust framework can be transacted by various commercial stakeholders in a fully decentralised manner, eliminating the need for all parties to be on a common digital platform.

## How are Selective Redaction and Decentralised Renderer functions used in TradeTrust and why are they useful

While TradeTrust facilitates the trusted exchange of digital documents across the different parties in cross-border trade processes, it is important to ensure that the holder of these documents have control over what information can be shared with other users. To support such flexibilities, TradeTrust adopts the **Selective Redaction** method and allows the holder of the digital trade document to redact information that are commercially sensitive (such as suppliers' or products' pricing) before sharing it with the next receiving party. TradeTrust also supports the concept of **Decentralised Renderer** of digital documents in order to allow the document issuers flexibility in designing the rendering functions according to their preference. The decentralised approach also helps to mitigate the risks of single point of failure (SPOF) when all documents rendering functions are consolidated under a common hardware infrastructure.

<sup>1</sup> <https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/the-multi-billion-dollar-paper-jam-unlocking-trade-by-digitalizing-documentation>



OpenAttestation –  
An Open-Source Framework  
for Verifiable Credentials

## Introduction

As the world moves away from paper documents and towards digital documents, it is important to ensure that digital documents are resistant to tampering and trust is preserved. OpenAttestation is an open-source framework developed by the Singapore Government Technology Agency to simplify the endorsement and verification of digital documents. In production since 2018, OpenAttestation has been implemented in various areas such as academic credentials, healthcare records, and cross-border trade.

The key features of OpenAttestation include:

- **Document integrity:** OpenAttestation ensures that the content of the document has not been modified since the document's creation, with the exception of data omitted using the built-in selective redaction mechanism.
- **Issuance status:** OpenAttestation checks that the document has been issued and that its issuance status is in good standing, i.e., it has not been revoked, for example. Currently, OpenAttestation supports two ways to issue documents: Decentralised Identifier (DID) Signing and Blockchain Smart Contracts.
- **Issuance identity:** OpenAttestation checks and returns the identity of the issuer primarily through the Domain Name System (DNS). It verifies that the issuing party in the document has provided some sort of proof that it is the same party as claimed by, for example, proving ownership over a domain by the ability to create a DNS record.

OpenAttestation has been listed in the [Digital Public Goods](#) registry by the [Digital Public Goods Alliance \(DPGA\)](#). DPGA is a multistakeholder initiative supported by the Norwegian Agency for Development Cooperation (Norad), United Nations Development Programme (UNDP), and UNICEF.

## Alignment with W3C Verifiable Credentials Data Model

OpenAttestation is aligned with the W3C Verifiable Credentials Data Model. As a framework with real-world implementation and production systems, our team hopes that OpenAttestation documents will be interoperable with other implementations of verifiable credentials and their related systems, including verifiers and wallets. We also hope to support greater adoption of verifiable credentials.

To this end, we have recently launched OpenAttestation v4 [<https://go.gov.sg/oa-v4>] which improves on interoperability with the W3C Verifiable Credentials Data Model [<https://www.w3.org/TR/vc-data-model/>].



OpenAttestation –  
An Open-Source Framework  
for Verifiable Credentials

## Proposed Contributions to W3C Verifiable Credentials Working Group

To improve interoperability and adoption, our team proposes the following contributions to the W3C Verifiable Credentials Working Group:

### 1. OpenAttestationMerkleProof2018 Signature Method for Selective Redaction

Selective redaction is a desirable property of verifiable credentials. OpenAttestation implements a lossy progressive selective redaction scheme, which allows it to be used in applications where a verifiable credential is passed along a chain of multiple verifiers and where privacy and data minimisation techniques are desired and/or required.

This proof method can be understood as a “hash of hashes” in which each property of the credential is salted and hashed. The output hashes are sorted, stored in an array, and hashed again to derive the target hash, which is akin to a digital fingerprint of the credential. To redact a property in the OpenAttestation Verifiable Credential, the obfuscated data is replaced by its corresponding derived hash. Obfuscation does not invalidate the proof property as the target hash is computed over all hashed key-value pairs in the credential, including obfuscated property hashes.

The Verifiable Credentials Data Model is proof format agnostic and does not normatively require any particular digital proof or signature format. As the OpenAttestationMerkleProof2018 Signature Method is being actively utilised by OpenAttestation implementations, our team believes that documenting the OpenAttestationMerkleProof2018 Signature Method as part of the Verifiable Credentials Data Model would be beneficial to implementers.

### 2. Decentralised Renderer

While the claims contained within verifiable credentials are machine-readable, they are not by default presented in a human-readable form. OpenAttestation implements a decentralised rendering protocol that presents the OpenAttestation verifiable credential in a human-readable format. Issuers create their own document schema and custom templates to render their OpenAttestation verifiable credentials. This decentralised renderer is publicly hosted as an endpoint.

When verifiers verify the OpenAttestation verifiable credential online, the OpenAttestation viewer then loads the decentralised renderer and uses it to display the OpenAttestation verifiable credential. This protocol enables document issuers to style their documents without code change to the different implementation of the document viewer, while managing the size of the credential.

### 3. Paper-Friendly Verifiable Credentials

OpenAttestation enables paper-friendly verifiable credentials that are suitable for use cases with uneven technological maturity, such as long cross-border supply chains. OpenAttestation verifiable credentials can be issued with a QR code which, when scanned with QR code reader such as a mobile phone, will direct the viewer to the OpenAttestation document viewer and load the OpenAttestation verifiable credential using the decentralised renderer.



OpenAttestation –  
An Open-Source Framework  
for Verifiable Credentials

### Use Cases

OpenAttestation has numerous use cases across a variety of sectors:

- **TradeTrust** builds upon the OpenAttestation framework to verify the authenticity and source of trade documents and for performing title ownership transfers of electronic transferable records.
- **OpenCerts** leverages the OpenAttestation framework to provide a convenient way for educational institutions to issue academic certificates, and for students to share their qualifications with prospective employers. It is used by all major post-secondary education institutions in Singapore.
- During the COVID-19 pandemic, OpenAttestation was used to issue tamper-proof pre-departure test and vaccination certificates (“**HealthCerts**”) for cross-border travel.
- Singapore’s Accounting and Corporate Regulatory Authority uses OpenAttestation to Issue Official Business Profiles and Certificates to registered companies.
- Singapore’s Immigrations and Checkpoints Authority uses OpenAttestation to issue long-term visitor visas.
- Start-ups have used OpenAttestation to issue transaction information about electric vehicle charging and carbon credits.



Scan here to view a verified  
digital copy of this brochure

For more Info, please visit:

[www.tradetrust.io](http://www.tradetrust.io)  
[www.openattestation.com](http://www.openattestation.com)

Contact us at:

[tradetrust@imda.gov.sg](mailto:tradetrust@imda.gov.sg)  
[openattestation\\_support@tech.gov.sg](mailto:openattestation_support@tech.gov.sg)