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

28th Plenary meeting
10-11 October 2022
Hybrid (virtual and Geneva in-person) meeting
Solving International Trade Challenges with Emerging Web Technologies

Three major challenges have obstructed global trade and supply chain digitization:
1. Global identification of trade parties
2. Establishing and maintaining trust at the distance
3. Mutual understanding and common semantics

An emerging technology stack is proving to solve these challenges by applying cryptography and international and W3C web standardization:
1. JSON Linked Data
2. Decentralized Identifiers
3. Verifiable Credentials
The heterogeneous environment of international trade makes it particularly difficult to ensure that the meaning of data is understood. When I say "x", might it be understood as "歪", or perhaps "ζ"?

This is at the core of UN/CEFACT! The Buy-Ship-Pay model is the global dictionary for terms in trade.

However, until recently using UN/CEFACT terminology still relied on:

- Out-of-bounds vocabulary agreement,
- Human interpretation, mapping source data into UN/CEFACT terms,
- Another human's interpretation, mapping UN/CEFACT terms to a target model,
- Breaking legacy API agreements.
Challenge 2: Global Trade Identification

The prevalent "2nd generation" digital identification is based on federation. There are large Identity Providers, especially for personal identification.

- Commercial organization identifier registries do exist, but are not commonly used for federated authentication.
- State-governed Identity Providers do exist, but are almost entirely recognized within that country.
- A federated approach does not scale: everyone recognizing everyone else’s Identity Providers is an exponentially complex problem.

Even if it was possible, the Identity Provider model in unattractive because:

- The 3rd party Identity Provider gains trade secret insights
- Granting an identifier monopoly tends to not benefit users
- Centralization entails a single point of failure

The problem extends beyond Parties: products, shipments, orders, consignments, devices, equipment, etc. GS1 and BIC are noteworthy successful identifier registries in some of these domains, but for identifiers not authentication.
Spanning cultures, political environments and jurisdictions, makes it hard to establish and maintain trusted business relationships in international trade. Trust today in large part rides on personal relationships, which are costly and fragile.

Even assuming a trusted relationship, how can you be sure that a set of claims are in fact representing the business partners intention? We are used to signed paper documents, backed by international law. PDFs is the intuitive way to "digitize", but is a mirage:

- Does not enable automation
- Data security based on human judgement

Commercial platforms approach this challenge by signing into a walled-off contractual environment which:

- Is limited to a particular part of the business process
- Is not globally scalable
- Trust is lost when data leaves the platform
JSON Linked Data

http://this

http://that
JSON Linked Data is a standard for overlaying normal API JSON with RDF in a non-breaking manner. This is done by literally adding a context to the raw data. This defines the types and identifiers of the data by use of web URIs.

For example, a "consignment" attribute would be defined as https://vocabulary.uncefact.org/Consignment.

JSON-LD enables:

- When the data sender is explicit about the meaning of data, no further interpretation is needed downstream. Interpret once, understand everywhere.

- Explicit semantics and standard syntax makes the data directly machine readable. For example, RDF fits directly into data graph which enables advanced data analysis.

You can try expanding a JSON-LD file here.
Decentralized Identifiers
Decentralized Identifiers are based on the model that the controller of an identity keeps a private key which is used for authentication, assertions and other use cases.

All DIDs resolve to a DID Document, which include the corresponding public key. This way, anyone can verify that an entity claiming to control a given identifier indeed holds its private key.

This removes the need to map between multiple identity provider representations; the DID is essentially its own Identity Provider.

Sample DID Document for did:web:transmute.industries

You can try resolving it yourself [here](https://didid.org/security/suitec/jws-2020/v1).
Verifiable Credentials
Verifiable Credentials is a standard data model which defines:

- Identification of the data issuer.
- The data subject about which assertions are made.
- Cryptographic proof which binds the data to the issuer.

Verifiable Credentials are based on two basic use cases:

- The issuer issues the Verifiable Credential.
- The verifier verifies the Verifiable Credential presented by its holder.

The Verifiable Credential may change hands many times over, just like physical and digital document are passed around. But at any point through out the supply chain, its content can be verified.

I may not know a foreign business partner well enough to trust it. But if the business partner can present suitable credentials from a trustworthy entity, trust is enabled.

Trust Graphs can be established, enabling completely automated processing of trustworthy branches – and manual focus on new relationships.

You can try verifying a Verifiable Credential here.
The DID+VC model is increasingly gaining traction. Many nation states are nearing production support as a means to digitization.

The UN/CEFACT vocabulary is essential for bringing the rich BSP semantic model for trade to modern web environment. Proper terms are the essential to verifiable data expressed with well-defined semantics.

Nis Jespersen is a Solution Architect at Transmute and editor of the UN/CEFACT JSON-LD Web Vocabulary project.

nis@transmute.industries

github: @nissimsan