eData Management Domain Discussion – 41st UN/CEFACT Forum

Vice Chair

Tahseen Ahmad Khan

Domain Coordinator, eData Management

Kaushik Srinivasan

Date

October 3, 2023

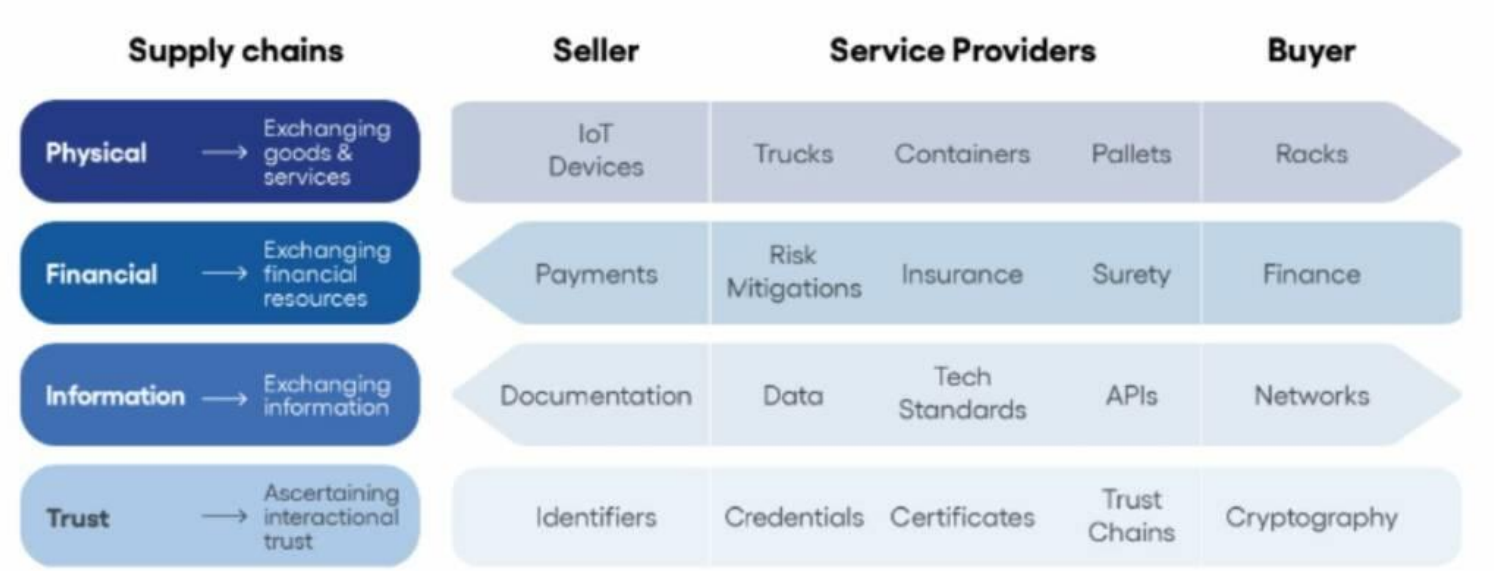
Trusted Third Party Services

- Cross Border Trade results in exchange of a number of documents such as Shipping documents, electronic bid document in e-Tendering process, Certified copies of incorporation and other documents
- Key Challenges include
  - Establishing authenticity of documents and data
  - Reliably identifying parties to the transaction
  - Mutual recognition of data and documents exchanged
- Trusted Third Party service providers such as Trust Service Providers, Timestamping Authorities and eNotaries act as important enablers in enhancing digital trustworthiness allowing parties to complete electronic transactions
- As data and documents get exchanged cross border, standardization and harmonization of above services is required for trade facilitation

In this context, “Zero Trust” is emerging as an important principle

Transition to Zero Trust

- A recent report * by ICC DSI highlighted four key layers of a supply chain: physical, financial, information and trust layers

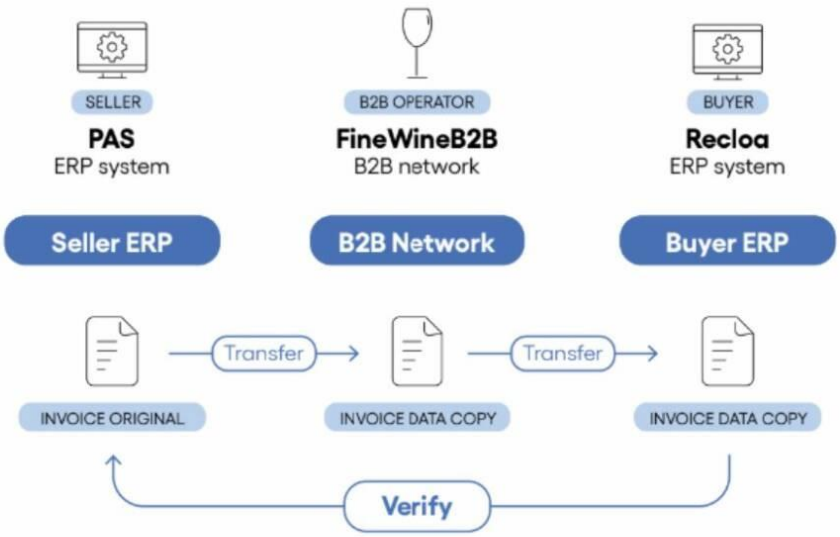


Report emphasized the need for technological interoperability to allow trusted data elements to flow seamlessly from one party to another

* https://www.tradefinanceglobal.com/posts/icc-dsi-releases-trust-in-trade-report-exploring-technological-mechanisms-to-establish-digital-trust/

Transition to Zero Trust

- Trade encompasses a broad range of actors – traders, financiers to shipping carriers
- To derive full value, an asset like a letter of credit created in one system needs to pass through multiple other systems before it reaches final destination where it needs to be verified against the originally created data



Data verifiability becomes a critical aspect of data exchange and this is where concepts like zero trust focusses on permission/identity based resource access

Transition to Zero Trust

- What is Zero Trust?

Given that we are running projects around Digital ID, Verifiable Credentials, it is essential to establish a guidance on what zero trust means in the context of trade

Transition to Zero Trust

- Concept of Zero Trust in the context of trade
  - Based on the principle of “Never Trust, Always Verify”
  - Security structure revolves around providing access to electronic data beyond individual organizations to external stakeholders that are part of a supply chain
  - Need to centre access privileges based on resources accessed and not around users
  - In the context of trade, the goal would be evolve a trust layer that accompanies the information layer which will support aspects of verifiability & traceability, legal compliance, and auditability

Next Steps

- Evaluate participation at launching a new project that focusses on highlighting
  - Role of Zero Trust in Cross Border Paperless Trade
  - Data Security aspects in sharing and providing access to information for internal/external stakeholders in electronic data exchange
  - Importance of trust layer in electronic data exchange including linkages to Digital ID, Verifiable Claims
  - Need and role of trusted third parties including eNotaries

Conclusion

Next Steps

- Action Items
  - Work on ongoing projects
    - Digital ID Standardization for Trade
    - Data Governance for Trade Facilitation
  - Evaluate Launch new projects
    - Trusted Third Party Services, E-Notarization and Zero Trust

UNECE

UN / CEFACT

Thank you