Malaysia 2024

The paper reviews the current challenges in unlocking cross-border data flows, and how interoperability of digital identity regimes using high level types of decentralized technologies can overcome this with active public-private partnerships. Main highlights include key factors for success for APEC to realize the potential of paperless trade through fostering cross-border interoperability of digital identity concepts beyond entities to physical products, as governments continue to evolve their regulatory stances to advance the region's shared goal of digital trust in trade.

APEC Business Advisory Council

Unlocking trade data flows with digital trust using interoperable identity technology

White Paper

ABAC Secretariat
www.abaconline.org

Acknowledgements

Working Group Participants

Adrian Ng, Country Representative for Global Legal Entity Identifier Foundation (GLEIF) Singapore

Ashley Ho, Compliance & Partnerships Manager, Trustana Singapore Pte Ltd

Avery Erwin, Head of Content, Chainlink Labs

Bertrand Chen, CEO of Global Shipping Business Network (GSBN)

Chaitanya Samprajan, Solutions Architect Lead, Affinidi Pte Ltd

Gao Fei, Blockchain Researcher, China Academy of Information and Communications Technology

Giriraj Daga, Director of Solutions Architect, Affinidi Pte Ltd

Henry Roxas, Business Development & Partnerships Lead, Affinidi Pte Ltd

Lee Chwee Beng, Director of Trade Operations, Trustana Singapore Pte Ltd

Li Jingxuan, Blockchain Researcher, China Academy of Information and Communications Technology

Mark Raynes, Head of Solutions, Chainlink Labs

Munetoshi Yamada, Executive Consultant/ Global Alliance Director, TradeWaltz

Niki Ariyasinghe, Head of Business Development APAC-MENA, Chainlink Labs

Pamela Mar, Managing Director of DSI, International Chamber of Commerce

Rebecca Xing, CEO of Trustana Singapore Pte Ltd

Satoru Someya, Managing Director and Head of CEO Office, TradeWaltz

Sowmya Ganapathi Krishnan, Head of Data and AI, Thoughtworks

Sukaasini Latch, Manager of Government Affairs and Transformation, SGTech

Sun Chiye, Blockchain Researcher, China Academy of Information and Communications Technology

Tang Wai Ying, Managing Director, Accenture Strategy & Consulting Singapore

Tat Yeen Yap, Managing Director of APAC, Co-sherpa of Asia Pacific Financial Forum (APFF)

Wayne Ang, Manager of Digital Trust, SGTech

Xue Tan, Head of Business Development, GLEIF Singapore

Yau Loong Aw, Senior Manager, Digital Trust and Government Affairs, SGTech

Observers

Chonraya Koomalayavisai, Deputy Director of External Affair and International Relation, Thai Bankers' Association

Indharatana Sriprajittichai, Subject Matter Expert, Thai Bankers' Association

Kajohnsak Manaviriyakul, Senior Vice President, Bangkok Bank PCL

Khanit Phatong, Advisor and CIO, Electronic Transactions Development Agency (EDTA)

Kobsak Duangdee, Secretary General, Thai Bankers Association

Krit Kamolnetrapisutt, Senior Product Exectuvie, National ITMX Co. Ltd.

Kukkong Ruckphaopunt, Senior Executive Vice President, Bangkok Bank PCL

Panumas Kaweechun, Senior Officer, Thai Bankers' Association

Parnkae Nandavisai, Subject Matter Expert - Trade Digitization, Thai Bankers' Association

Executive Summary

As the world becomes increasingly interconnected, the importance of secure and efficient cross-border trade has never been greater. Digitalization of cross-border trade referring to the digitalization of information flows required to support good and services crossing borders brings about innumerable benefits in improving supply chain visibility, reducing trading costs and increasing access to global markets. The flow of trade data is a critical component of this process where nations, especially regional economies in the Asia-Pacific Economic Cooperation (APEC) representing 21 economies, aim to promote inclusive and sustainable economic growth.

1. Spurred by the disruption of a global pandemic and promises of high efficiency & cost-savings, the race towards digitalization of cross-border trade is on

Digitalization of cross border trade, or paperless trade refers to the digitalization of information flows required to support goods and services crossing borders. The impact of digitalization on trade in today's fast-paced and interconnected post-pandemic world has given rise to digitally enabled business models for trade in goods and services that have traditionally been conducted through offline paper-based transactions. A report by International Chamber of Commerce (ICC) indicated that cross-border paperless trade facilitation could create $267 billion of additional exports by 2026, and digitalizing the trade ecosystem could create $6 trillion in extra exports by 2026.[1] Within Asia Pacific, the export value continues to be above Europe estimated at US $200 billion in exports of intermediate goods in 2021.[2] ICC report also revealed that current costs associated with trade at 3% could reduce to 0.7% by 2026 through digitalization of the trade ecosystem.[2] **It is evident that the opportunities and importance of digitalization of cross-border trade continue to grow in Asia Pacific.** The ensuing concerns of digitalization of trade are 1) legal environment, 2) lack of standards/ market fragmentation where individual nations are operating on their own and data is not interoperable with data localization requirements, and 3) lack of capacity. A critical issue that must be resolved to unlock the potential of trade digitalization is the adoption of a globally interoperable digital identity systems. Digital identity serves as a crucial foundation, since without an interoperable digital identity, data sharing lacks a verifiable trust element that will not accelerate the move from paper-based transactions dominating current international trade, to the use of electronic transactions for paperless trade. Digital identity enables secure electronic transmissions governed under international framework granting electronic transactions legal validity with no unjustified barriers of customs duties imposed on such transactions. Singapore is one of the early adopters of paperless trade among APEC economies with mandatory document requirements as early as 2014, along with Hong Kong, China, and the Republic of Korea[3]. These economies are well-equipped with the resources necessary to pioneer innovation and advancements. Such leadership will be instrumental in navigating the multifaceted regulatory landscape that governs cross-border trade digitalization throughout the region.

2. Challenges in digital trust where we believe development of portable, verifiable digital identities is critical

The success of cross-border trade digitalization is fundamentally built on the level of digital trust between businesses and governments, which is the confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner. The level of digital trust is shaped by the concerns and challenges in legal certainty of digital trade transactions, in the level of recognition of foundational and identifier standards and frameworks for interoperability, and in the nation's capacity to progress regulatory and institutional reform for businesses to leverage digital tools for data free flows with trust. The enabling tools and digital infrastructure for the facilitation of digital trust has its utmost challenges since trade itself involves various participants and roles in the supply chain process within different enabling policy environments of the region. The World Bank estimates that the digital economy contributes to more than 15% of global gross domestic product (GDP), and in the past decade it has been growing at two and a half times faster than physical world GDP. Despite the promising opportunity, the missed opportunity caused by the lack of digital trust is quantified to be 5%-point increase to an average of GDP per capita of $3,000 increase by The Digital Trust Index: the value of digital trust report[4]. The factors driving the trust gaps include personal experience of fraud, and not understanding what information can be trusted online. In cross-border trade context, the same challenges are noted in International Chamber of Commerce (ICC) Digital Standards Initiative's Trust in Trade Report[5], namely the lack of capacity and culture of data sharing posing barriers to digital trade amongst others. Regional economies and industry leaders have all identified the key to unlocking the success of digital trust implementation, **through digital identities.** All cross-border movement of goods, capital and people can be made more efficient, safe, and inclusive with the use of cross border digital identity systems. For instance, it can enable easier cross-border electronic transactions and better access to trade financing. At the economy level, the use of digital identity could generate more than 10% of additional GDP by 2030[6] as digital identity enables individuals to unlock value and benefit when they interact with firms and governments, thereby benefiting micro, small and medium enterprises and low socio-economic groups. Having the ability to be verified and authenticated to a high degree of

assurance while at the same time protecting user privacy and giving user access to their data, digital identity expands existing national identity regimes regardless of its level of maturity and implementation stage, consequently requiring less investment in new technologies especially for emerging economies. Mutual recognition of digital identity systems accelerates trade digitalization and market expansion as there's increasing number of trade transactions transiting to paperless trade. Bilateral digital economy agreements signed by APEC governments (see **Appendix 1**) are exploring the use of digital identities to promote interoperability of digital identity regimes, which underpins their belief in digital identity being one of the priority areas for increased digital standardization and baseline for cross-border trade. The APEC Digital Economy Steering Group's Global Benchmarking Study 2023 has identified that digital identity solution has the potential to automate manual processes and enable operational efficiencies, especially for businesses.[7] **Interoperability of digital identity regimes is the critical step towards advancement of digital identities that are portable**, allowing entities and users to own and manage their identities, thereby advancing the concept of self-sovereign identity (SSI) and breaking existing identity siloes to enable trust in digital trade across the global supply chain.

3. Stronger G2G and private sector initiatives are imperative, where large trading organizations and corporates can take the lead with endorsements from digital promotion agencies to promote interoperability of digital identity regimes.

For a variety of reasons, national digital identity schemes are proliferating in Asia. While this is a favorable development, showing nations' commitments to the digital economy, on a practical level and given the realities of cross border trade and payments, interoperability or mutual recognition is key, or as an alternative, interoperability with globally recognized schemes like the Legal Entity Identifier (LEI) under the Global Legal Entity Identifier Foundation (GLEIF). Cross-border digital identity systems may not mean the creation of a harmonized identity system but one that allows recognition and use of one jurisdiction's digital identity in another. It may not be similar, but it needs to be trusted i.e., recognized across borders, thereby surfacing the important basis of digital identity systems which is interoperability. For cross-border trade, recognition of an overseas supplier's digital identity can allow the buyer to obtain letter of credit from local banks to initiate the purchase transaction, and in another instance, digital identity with enhanced biometric data protected by digital certificate can be used for businesses to transact electronically without additional multi-layer verification systems. Digital identity concepts can also be applied to entities beyond a business – for example, to physical products or SKUs – where the benefits of interoperability can help to make data exchange in cross-border trade more efficient. As governments continue to evolve their regulatory stances, ensuring that goods such as F&B products or health-related products have trustable certifications will smoothen the operations for customs while increasing confidence.

Enabling policy environment, governmental involvement in setting strategies, regulatory complementarity and harmonization of standards will rightly guide and accelerate the implementation roadmap of interoperable digital identities in APEC region. That said, the capacity, readiness state of technological infrastructure and political agenda of governments are unique in their own jurisdiction, thus setting the varying pace of digital identity development in individual economies. This also presents fundamental challenges in interoperability and portability of digital identities across economies and uses across industry verticals. The importance of interoperability of digital identity systems to support cross border operations has been acknowledged at the EU level in the eIDAS (electronic IDentification, Authentication and trust Services) regulation which entered into force 2014. Several elements necessary to realize a global trade digital identity system are also being discussed in the context of the United Nations. UNCITRAL Working Group IV, for example, is working on a draft legislative text on identity management and trust services which includes cross-border aspects (i.e., legal recognition)[8].

It is clearly the case that implementation of digital identities by private sector players in cross-border trade transactions alone present mounting difficulties considering the foremost recognition of identity regimes that is necessary between exporting and importing economies, and involvement of governmental agencies including customs for approval and clearance of all goods and services. It presents the need for government-to-government (G2G) public sector initiatives in mutual recognition of digital identity regimes, in setting of harmonized standards and establishing the utility infrastructure for interoperable digital identities upon which applications for industry verticals can be built. The role of global non-profit organizations and regional trade associations is not independent in this trust paradigm as these organizations share the same objectives as their make-up of public authorities and/or business corporations to advance digital trade for the promotion of open economies through different forms. To overcome the differing pace, political and economic interests of the APEC economies, the role of these global non-profit organizations could be elevated to advance interoperability of digital identities through the setting of harmonized standards, protocols and implementation roadmap (e.g., cryptographic techniques) based on mutual understanding

and recognition from governments in the region. In parallel, private or corporate entities can begin with the implementation of digital identities for businesses and products in cross-border trade, complementing the efforts of global non-profits by providing evidence to the commercial benefits of portable and interoperable data.

4. Decentralized identity technologies, such as verifiable credentials (VCs) and decentralized identifiers (DIDs), coupled with interoperability protocols can complement the current Web3 infrastructure to enhance interoperability and digital trust

It is noted in the World Economic Forum White Paper that global trust worthiness is an important identity system principle for future supply chains, as this process of dynamically verifying counterparts through digital identity management and verification is a critical step in establishing trust and assurance for organizations participating in digital supply-chain transactions.9 As the number of digital services, transactions and entities grow, it is crucial to ensure that digitally traded goods and services take place in a secure and trusted network in which each entity can be dynamically verified and authenticated.

Web3 describes the next generation of the internet that leverages blockchain to “decentralize” storage, compute and governance of systems and networks, typically using open source software and without a trusted intermediary.With the new iteration of Web3 being the next evolution of digitalized paradigms, **several new decentralized identity technologies have become an increasingly important component to complement existing Web3 infrastructure for digital trade. Two key building blocks for a decentralized identity system include verifiable credentials (VCs) and decentralized identifiers (DIDs).**

VCs are an open standard for digital credentials, which can be used to represent individuals, organizations, products or documents that are cryptographically verifiable and tamper-evident. The important elements of the design framework of digital identities involves three parties – issuer, holder and verifier. This is commonly referred to the self sovereign identity (SSI) trust triangle. The flow starts with the issuance of decentralized credentials in a standard format. The holder presents these credentials to a service provider in a secure way. The verifier then assesses the authenticity and validity of these credentials. Finally, when the credential is no longer required, the user revokes it. This gives rise to the main applications of digital identities and VCs in **business credentials, product credentials and document identifiers** in the trade environment involving businesses, goods and services. In a typical transaction, the interoperability of business credentials for export and import between two economies, portability of product credentials for post-importation sales, and mutual trust in verified business and product credentials are the key factors for consideration in the implementation roadmap of high trust digital identities using VC towards the longer-term objective of accelerating trust in cross-border trade digitalization.

Similar to global trade, VCs are also decentralized in that there can be multiple issuers of digital credentials, holders/owners of these identities can share data peer to third parties in a peer-to-peer manner. This technology can complement existing trade systems as a cross-system digital identity solution, which allows parties to independently verify the identities of an individual or organization before transacting.

DIDs are a new type of identifier that refer to a subject, whether it's an individual, organization, product, or document etc. These DIDs are created and managed completely by a user (individual or organization), enable the owner to securely prove control over them and don’t contain any personal data. DIDs can be programmatically resolved to metadata required for independent and cryptographical verification , without having a direct relationship or checking with the issuer. This is highly relevant for global trade as stakeholders within a supply chain may rely on different systems, each with their own stand-alone digital identity solution. Having a common relationship with the same service provider for each system can be costly, complex and different to scale.

VCs and DIDs, when used together, form the building blocks to a decentralized identity solution, complemented by the inclusion of legal entity identifiers (LEI) within a standardized framework for digital identity and trust in digital interactions

The benefits of using DID and VC for digital cross-border trade are multifold, including time and resource efficiency in removing manual verification processes; achieving trustworthiness in source of data transmission; enhancing digital trust and data privacy where data has not been tampered with during transmission through the use of cryptographic mechanisms (public key and private key), selective disclosure and zero knowledge proof for third party authentication of user digital identity; allowing interoperability of data flows where DID and VC standards adopted by countries and industry verticals are based on global standards; safeguarding data security through decentralized and self-generated

DID compared to a centralized system vulnerable to cyberthreats; lastly granting entities and individuals control of their own identity compared to control via a third party centralized platform in current Web2 digital identity model while ensuring compliance with data protection laws of various jurisdictions.

5. Key factors for success

We recognize the increasing efforts of public and private sectors to advance the shared goal of digital trust in trade for open trade promotion within APEC economies and it is pertinent to consider the key factors for success in our efforts. Successful adoption of digital identities stems from the involvement and support of regional and local governments, and willingness of large non-profit organizations, standards bodies or trade associations in their capacity to step up and set regionally harmonized standards embracing the key components of high trust digital identities in their archetypes for different ecosystem players.

6. Call to action

For cross-border trade digitalization to become the de facto practice at scale regionally within APEC economies and enabling end-to-end trade digitalization across economies and platforms, present regulatory barriers in 1) legal environment, 2) lack of harmonized standards/ market fragmentation and 3) capacity to make available digital infrastructure must first be acknowledged. Strategic digital cooperation milestones within the APEC region shall be set through more active G2G promotion efforts focusing on interoperability of digital identities and their components to address the key challenges. The concomitant recognition of the role of large independent non-profit organizations in standards development and harmonization is necessary to support industry players in this trade paradigm to explore the applicability of high trust digital identities with VC across various trade digitalization scenarios. We also foresee numerous pilot opportunities when the economies in the APEC can start working together to recognize digital identity regimes in cross-border trade and services to drive interoperability and portability of credential types.

Concluding remarks

APEC Business Advisory Council (ABAC) Chair Mr. Kriengkrai Thiennukul, Chairman of the Federation of Thai Industries said at the ABAC meeting in November 2022, “It is critical that we enable the digital economy and promote digital transformation for resilience and growth, especially for MSMEs”. One of the priorities for the group include strengthening digital connectivity and advancing digital transformation to further facilitate trade, recognizing the progress made in digitalization of border clearance processes as well as developing and implementing paperless trade facilitation measures.[10]

APEC Ministers reaffirmed their commitment at APEC Trade Ministers Meeting 2023 to “accelerate the implementation of the APEC Internet and Digital Economy Roadmap, to support inclusive, sustainable and innovative economic growth, including the facilitation of e-commerce and advancing cooperation on digital trade. This is mainly through promotion of interoperable approaches approaches and the use of digital technologies to facilitate trade and investment.” [11]

IMDA Chief Executive, Mr Lew Chuen Hong, said in interviews that “Digital tech is a great multiplier”, and “the real role of the regulator is to build the foundations for trust, so that businesses, governments and consumers have the trust to innovate and co-create in the digital domain”.

SGTech Chairman, Wong Wai Meng quoted that “Trust is the basic hygiene that Singapore needs to tackle as the country’s digital economy continues to grow”, and “digital trust will put us in a favorable position”.

Section (1) Opportunities in enabling cross-border data flows

Enabling cross-border data flows for paperless trade is important for cross-border recognition of electronic data and documents for inclusive and sustainable intraregional trade facilitation. It represents an important, albeit hard-to-measure, component of international cross-border trade, and is set to accelerate on the back of businesses' reliance on digital technologies to increase trade efficiencies and productivity. Through this enablement, trade information can flow across borders through the whole operation of an international supply chain. Concomitantly, the rise of the digital economy over the past few decades and its enhanced role during the COVID-19 pandemic have highlighted digitalization as being not only one of the world's most powerful engines for growth and innovation, but also as a key part of developing resilient and sustainable twenty first-century economies.[12]

In APEC Report "Economic Impact of Adopting Digital Trade Rules" 2023[12], there has been research findings stating that the macroeconomic costs of forced data localization ranges between 0.7% and 1.7% of GDP, as it reduces trade, slows productivity, and increases prices for the affected industries. In addition, data localization has been associated with investment decreases of up to 4%, suggesting that constraints on cross-border data flows not only affect the digital sector itself, but also the broader economy.[14] Furthermore, the Digital Trade Openness Index (DTOI) findings revealed that 121 out of 210 trade pairs in APEC are still not covered by any of the listed 13 digital trade provisions in 2021, which strongly suggests that there are greater opportunities for APEC to strengthen regional digital trade infrastructures and the broader framework of the digital economy that will set the stage for the promotion of cross-border data flows.

a. APEC situation

APEC region is expected to enter a golden age for the development of digital trade over the next few years despite our geopolitical differences, with increasing growth in trade volume and transactions in the region, continuous improvement of digital infrastructures, and economies' commitment to implement the Regional Comprehensive Economic Partnership (RCEP) Agreement facilitating regional digital trade in the region. Evidently, digitalization of cross-border trade will bring about huge cost savings and efficiency gains to international trade, with estimates ranging between 15 to 45% in cost savings depending on the stage an economy has reached implementing paperless trade facilitation measures at the border, amounting to billions of dollars annually.[15]

Development levels of trade digitalization in APAC ranges from mature to development and early-stage markets, creating myriad of opportunities for the region to promote establishment of infrastructures based on regionally accepted standards, capacity building for small to medium sized enterprises utilizing jurisdictional digital trade infrastructures and a culture of data sharing to remove barriers to digital trade. Each economy has their own initiative or experimental framework being piloted for cross-border trade digitalization but there is slow headway given the lack of commonalities in legal frameworks for data standardization, policy environment and use of enabling technologies (see **Appendix 2** for the initiatives of individual economies). In cross-border trade digitalization, APEC region can be characterized in the following three areas:

i. Policy environment – Diverse regulatory environment such as the lack of unified adoption of the Model Law on Electronic Transferable Records (MLETR) developed by the United Nations Commission on International Trade Law (UNCITRAL), one of the instruments for enabling cross-border data flows for cross-border trade digitalization; and different jurisdictional certification requirements under the APEC Cross-border Privacy Rules (CBPR) system with different data localization restraints and no mutual recognition of CBPR certification outside APEC.[16] Based on the data of 22 selected economies, key regulatory barriers for cross-border digital trade in the APEC region are mostly related to infrastructure and connectivity policy more than in other areas as measured by the OECD DSTRI.[17]

ii. Business readiness: Business readiness for adoption of cross-border trade digitalization technologies is mutually dependent on the level of digital maturity of the jurisdiction. Major Asian economies can be mainly divided into mature markets, developing markets and early-stage markets in terms of their development level of digital trade. Among them, mature markets mainly include China, South Korea, Singapore and Japan; developing markets include Thailand, Malaysia, Indonesia, Vietnam and the Philippines; and early-stage markets include Myanmar, Cambodia, Laos and Brunei. This is considering multi-factors including per capita volume of transaction via e-payment and proportion of cross-border e-commerce in overall e-commerce which are individually less than 15%.[18]

iii. Technology: Technical readiness of APEC region is not high given the differing levels of digital maturity and localized approaches in implementing trade facilitation measures. Vietnam government has progressively worked on building ICT infrastructure for paperless trade and national single window interoperability, while Philippines Bureau of Customs has achieved much in business process reengineering towards adoption of paperless trade[19], but there are

no shared resources for technical capability building to fully maximize technology-enabled solutions in helping decrease the amount of budget spent as a region. There is a need for increased capacity for resource sharing and greater alignment with recognized international, open standards which could help to boost the economic benefits of cross-border trade digitalization, creating more economic value.

b. Cross-border data flows as a critical component of digital trade

Cross-border data flows encompass any transfer of data or information across boundaries, and in the cross-border trade context, it refers to any trade transaction-related information and documentation. With drastic growth in trade data movement, the importance of cross-border data flows would far outweigh the physical transfer of goods or provision of services. To progress towards cross-border paperless trade in the region, it is pertinent to consider cross-border data flows as a critical component in the development and harmonization of interoperable digitalization standards. Rather than diminish, data's value grows with repeated access and use due to accretion and network effects: the value of data increases as the volume and variety of data increase and as more users contribute to and have access to it.[20]

Notable widely used standards for cross-border data flows such as the exchange of electronic trade documents should be considered for participants in the trade value chain.[21] Current legislative gaps impede the progress of unlocking cross-border data flows for the digitalization of trade, such as the lack of unified adoption of the Model Law on Electronic Transferable Records (MLETR) developed by the United Nations Commission on International Trade Law (UNCITRAL). MLETR aims to bridge the gap in trade digitalization by addressing transferable documents and instruments where these documents require legal adaptation to ensure equivalence with electronic alternatives. MLETR is a model law that provides these needed adaptations. Widespread regional adoption of the MLETR in APEC holds the promise of coherence in the modernization and harmonization of regional policies on enabling cross-border trade data flows.[22]

To facilitate the free movement of data across borders, digital identity is the key. Being one of the foundational building blocks of digital economy recognized by jurisdictions, digital identity allows any individual, business and legal entity, authority and even physical goods and locations to be identified which enables them to assert and confirm unambiguously who they are in the digital realm. The APEC Business Advisory Council report on digital identity in APEC revealed findings from a study[6] that extending full digital ID coverage could potentially unlock up to $6.8 trillion for APEC economies, with more gains for emerging economies. A digital identity is made up of attributes including unique characteristics (e.g., company name, business registration date and number) that together make up a unique identity. A well-designed digital identity system potentially unlocks many benefits for individuals and companies in accessing public or private services such as receiving payments, enrolling in a program, opening a bank account, or sharing trade information and shipping status. It enables more seamless, trusted, secure, privacy-enhancing and efficient business and trade transactions, including leveraging the ability to identify physical objects and locations to streamline supply chains and increase trade efficiency with particular benefits for small to medium enterprises in financial inclusitivity.[23]

Suffice to say, digital identity is foundational and is the most important priority within the standards field. Without an interoperable digital identity, data sharing lacks a verifiable trusted element that will not accelerate the move from paper-based transactions dominating current international trade and transport to paperless trade using electronic forms made available by customs authorities. **Digital identification of businesses and documents embed the trust element in electronic transactions and complements the use of electronic contracts with authentication that makes digital transactions interoperable but in a more secure and efficient manner.** Digital identity could save 110 billion hours of work for public services, reduce business onboarding costs by up to 90 percent and payroll fraud savings of up to $1.6 trillion annually.[23]

c. APEC success in facilitating cross-border data flows for digital trade

APEC is unique in its composition and economies have their geopolitical focus and jurisdictional trade priorities. Despite that, efforts have been made to establish harmonized regulatory frameworks and data protection protocols to mitigate risks of cross-border data flows, such as the implementation of APEC cross-border privacy rules (CBPR) system, a government-backed data privacy certification for companies to demonstrate compliance with internationally recognized data privacy protections. Taking advantage of the economic diversity in the region, APEC is adopting a unique approach in setting regionally acceptable standards based on international benchmarks, thereby creating a more favourable regulatory environment to spur digital trade initiatives. Individual jurisdictions will have the

sovereignty to promulgate their own regulations that caters to their economic situation aligned with the centralized governance framework.

Within APEC, ASEAN has also successfully adopted a smaller-scale regional approach in establishing the ASEAN framework on digital data governance[24] and model contractual clauses for cross-border data flows, recognizing the importance of diversity for success and differing digital maturity levels. Japan has proposed the concept of "data free flow with trust" as an organizing principle for a global approach to data governance, which has won endorsement by both Group of 20 (G20) and G7 leaders. Evidently, establishing a strong centralized data governance framework with data protection protocols, and setting effective regulatory policies in areas related to data flows, data privacy, cybersecurity under the umbrella of privacy-enhancing technologies and interoperability of digital trade regimes is important to drive success towards trade digitalization. This could also involve setting up an institutional mechanism for promoting APEC cooperation on cybersecurity, digital trade rules and digital trade infrastructures within the ambit of thought-leadership statements and digital economy cooperation agreements.

Considering the diversity of APEC economies, there is no one-size-fit all solution obtained by unanimous agreement among all economies. This, however, does not limit early-stage markets to leverage on the strengths of APEC economies with high level of digital trade maturity, who could perform the role of an aggregator of digital trade domain knowledge. Aggregators for specific industries could set domain-level standards for data collection and aggregation for cross-border trade flows while considering regionally acceptable privacy standards, within a secure digital architecture that enables government-to-government (G2G) and business-to-government (B2G) permission sharing of trade information. **A step ahead will be the digital identification of trade data fields by sectors that can be authenticated, verified, not stored on a permanence logic through an interoperable digital architecture that grants access control to governments and trade parties. The future of the cross-border trade digitalization ecosystem is a combination of platforms run by both public and private sectors that are interconnected through common taxonomies, data standards and protocols so that electronic trade data can be interchanged. By moving from various standalone trade platforms to a heterogenous one, private enterprises and cross-border trade parties can have plug-in applications to this heterogenous digital architecture that bridges the interoperability of data across different systems handled by the individual governments.**

d. Broad challenges in unlocking cross-border data flows

APEC success in trade digitalization is crucial in the advancement of jurisdictional and regional economic development. Notwithstanding the opportunities of trade digitalization in making supply chains more robust and supporting economic growth, there are present challenges in APEC economies' adoption of relevant regional and international digital trade standards. In addition to the lack of a unified approach for legal recognition of electronically transferred documents and instruments for paperless trade, a key factor in unlocking cross-border data flows for trade digitalization, there is also the ensuing concern of digital trade between governments and businesses on digital trust, surrounding digital trade footprint on user identity and access. More specifically, user identity and access are correlated to data security and privacy concerns where cyber threats are set to outpace data protection and cybersecurity measures in APEC economies. Overall, robust technical and institutional capabilities within the whole of APEC are still lacking to parry data breaches which can erode business and consumer trust in the use of digital trade solutions. The geopolitical diversity of APEC also results in different levels of readiness amongst economies, who also find it challenging to transit from protectionist approaches to promoting cross-border data exchanges and have a regional strategy to make the most of enabling cross-border data flows for trade digitalization opportunities. In the ASEAN region, only a few countries have established mechanisms encouraging cross-border data flow with the purpose of stimulating innovation and economic growth. This is likely due to the challenges encountered by some countries in capturing value from data - including lower-levels of data connectivity, issues with foundational digital infrastructure, weaker data collection processes and abilities, limited data or digital literacy that stifles innovation, and a lack of access to high quality or large datasets.[25] Both governments and private enterprises have to balance between readiness versus eagerness to adopt enabling technologies to bring about the economic benefits of unlocking cross-border data flows.

In a published study[26], United Kingdom, United States of America and European Union ranked among the top 6 as the lead global economies in having an openness to embrace cross-border data flows with the right policy environment and participation in legal frameworks for data protection or cross-border privacy rules. There is, therefore, strong impetus for APEC economies in the region to endorse and implement cross-border data flow provisions and make trusted data sharing frameworks the default for cross-border trade.

Section (2) Challenges in digital trust and how interoperable digital identities has a role to overcome present challenges.

a. Low impetus for jurisdictional adoption and lacklustre public-private partnership to co-invest quickly into digital trust technology and interoperability.

It is widely acknowledged that securing digital trust among jurisdictions and businesses is the essence of driving digitalization of global trade, especially within APEC economies which are facing challenges in securing digital trust through the lack of effective interoperable digital identification regimes and digital transmission means. Considering the foremost challenges of digital trust, verification tools play a vital role in establishing trust in digital transactions. Within China and US[27], current developments on digital trust from respective governments and their strategic focus are all silos of their own, while efforts by corporate businesses in both economies breaking frontiers in related technology to strike a common standard between them is almost non-existent. In recent years, there have been significant developments around digital trust technology though surrounding privacy, security, and verification. Organizations needing digital trust applications increase their budgets to enhance digital trust through IT strategy/governance, security and digital transformation– 80% of over 2700 enterprises surveyed say digital trust is important, but only 12% have addressed it. Increasing private sector budgets reflect the fact that digital trust tops the agenda for resilience planning.[28] On the other hand, fewer APEC governments have a holistic strategy in their approach to a digital government[17] including having a jurisdictional data governance strategy[29], putting them far behind the private sector and APEC governments can certainly spend greater effort investing into their digital roadmap encryption, secure communication protocols, and data anonymization techniques to bolster privacy and enhance user trust. This will in turn enhance the ease of adoption for end-to-end digitalization of cross border trade documents that can result in potentially 2% increase in cross border business-to-business (B2B) trade volume in annual terms due to greater efficiency to conduct cross border trade[30]. If public private partnerships are more quickly sought out with greater efforts to foster ecosystem development for trust technologies in their own jurisdictions, it will help build more momentum towards a regional trust circle within APEC for digitalization of information flows required to support goods and services exchanges.

b. Importance of digital identity and key aspect for development of interoperable digital identities across jurisdictions is the wider adoption of verification technology and mutually recognized VCs

As acknowledged in regional and bilateral digital economy agreements, the key to unlocking the success of digital trust implementation is through digital identities. All cross-border movement of goods, capital and people can be made more efficient, safe, and inclusive with the use of cross border digital identity systems. For instance, it can enable easier cross-border electronic transactions and better access to trade financing. Mutual recognition of digital identity systems accelerates trade digitalization and market expansion as there's increasing number of trade transactions transiting to paperless trade. The wider usage of digital identities by corporates further extended to electronic transferable records will enable the entire supply chain to be transacted digitally, thereby increasing visibility, efficiency and propel cross-border trade digitalization. Digital identification embeds business trust in the digital trade environment and mitigates concerns on open data flows and open government data crucial for interoperability where commercial and non-commercial data can be securely shared and redistributed or published.

Apparently, the biggest hurdle remains interoperability between different jurisdictions. In cross-border trade context, there are still various verification scenarios using traditional paper materials instead of digital identification of documents, which comes with disadvantages and risks such as resource consumption cost, long processing time, risk of damage, loss and counterfeiting in addition to lack of interoperability. Secondly, trade requirements are not fully transparent between governments and businesses, which coupled with the lack of interoperable digital identity regimes will result in an incomplete information chain upstream and downstream of the trade chain. Thirdly, without interoperable digital identity regimes and unified verification mechanism, the cost of various forms of identification for businesses and trade documents is high with the combination of digital and paper-based trade documents in each transaction by trade lanes. Lastly as cited in the preceding paragraphs, the main challenge in interoperability between jurisdictions hinges on data security and privacy due to the lack of effective technical protection measures for personal privacy data and important data in cross border trade, and often, the use of a centralized jurisdictional platform to resolve this has its risk of single point of failure vulnerable to concerted cyberattacks. Data security, privacy and protection measures should be balanced with the number of data localization measures for interoperability to be fully realized, considering that ITIF reported the number of data localization measures implemented globally to have more than doubled in the past four years.[31]

The wider adoption of verification technology is crucial for the quick development of interoperable digital identities across jurisdictions. Self-service mutually recognized VCs can play a significant role in achieving this goal. These credentials allow individuals to manage and control their own digital identity information securely while enabling trade organizations to verify and trust that information in a permissioned controlled environment. Technologies such as digital signatures, blockchain, and secure authentication protocols are just tip of the iceberg to help enable secure and tamper-proof verification of identities, documents, and transactions. Given the geopolitical diversity of APEC, it is noteworthy to consider the pace of adoption by less developed economies that may be lacking the utility infrastructure and resources, and ensuring there is lesser burden of adoption placed on these economies who could be assisted through resource-sharing from lead economies. Jurisdictions with robust digital identity infrastructure and regime should also caution against eager adoption of new verification technologies resulting in non-standardization and silo industry practices. Organizations like the World Wide Web Consortium (W3C) are actively working on higher and new standards such as the VC Data Model and the Decentralized Identifiers (DIDs) specification and they are all worthy of considerations in application tools to enhance interoperable digital identities. Specific cross border trade use cases may include but are not limited to certificates of origins, Authorized Economic Operators (AEO) mutual recognition, documentary trade finance, product conformity, sanitary & phytosanitary certifications, CITES or endangered species trade permits, illicit contrabands detection and supply chain traceability for carbon emissions etc.[32]

c. Regulatory support, public awareness, and education to promote pilot projects between trading economies in APEC.

Governments in APEC can start by wanting to play a crucial role in providing regulatory support and raising awareness through framework of cooperations with its key trade partners to create an enabling environment for the adoption of mutually identifiable VCs regardless of current level of standardization across the region. Possible measures may include updating existing regulations, addressing legal and privacy concerns, and promoting the use of digital identities in various sectors within their own jurisdictions, such as healthcare, finance, and government services where speed of digitalization varies but can be driven in single direction. Taking the example of Singapore, Infocomm Media Development Authority (IMDA) and the National Research Foundation (NRF) launched the National Trust Centre to focus on R&D efforts for trust technologies and support talent development in this space, including Privacy Enhancing Technologies (PETs) that preserve data privacy while the data is being analyzed. Together with private sector incentivized to build trustworthy AI technologies surrounding secured trust mechanisms for cross border trade due to the R&D efforts conducted, Singapore government in turn became enabled to propose framework of co-operation with Malaysia in Digital Economy and Green Economy[33] where pilot projects between enterprises in both economies can participate into joint initiatives that help showcase the benefits and feasibility of mutually recognized VCs assisted by trade ministries of both governments. China in another instance has established the multi-layer legal framework for cross-border data flows under the legal framework of the Cybersecurity Law, Data Security Law and Personal Information Protection Laws of the People's Republic of China. The Cybersecurity Law first proposed the concept of important data and personal information, followed by the regulation of cross-border exchanges under the Data Security and Personal Information Protection Laws. This enables the storage of personal information within the jurisdiction, while processors of personal and non-sensitive business data required for overseas cross-border usage is efficiently processed through a structured security assessment with local businesses' consent.

With Singapore and China leading the region in setting up unique regulatory frameworks and policy environment mirroring the General Data Protection Regulations in the European region, they can set the stage for APEC economies and further encourage joint public-private collaborations tapping on utility infrastructures built by the government to accelerate exchange of cross-border data flows. These initiatives in turn help highlight the potential cost savings, increased security, and improved user experiences associated with adopting trust technologies and inevitably supports interoperability testing and certification programs with usage of different verification technology providers adhering to both parties defined standards. The piloting process will also help educate stakeholders and helps lay good foundations for the vision of achieving seamless interoperability goals across multiple jurisdictions within APEC for the longer term. Standardization and promoting open standards for VCs is essential but purely waiting for ready tools to share common data formats, single interfaced protocols and new technologies surrounding security frameworks to mature between private sector organizations will be too slow an approach and too costly in terms of lost opportunities. APEC Governments, technology companies, and industry organizations need to collaborate and form partnerships to drive the adoption of interoperable digital identities.

d. Interoperable digital identities replacing conventional means of "signing off" and taking references from other trading blocs.

Digital identities that are interoperable can eventually replace conventional means of "signing off" on traditional agreements and facts, which are necessary exchanges in trade of almost all cross-border scenarios. That said, digital identity requires standardization on all layers to become fully interoperable. Interoperability of data and alignment of parties' data infrastructure and practices to established standards for data sharing along the supply chain will allow digital trade documentations to become the de facto practice at scale. For instance, a cross-border trade transaction involving two corporate digital identities will need cross-border harmonization of identity standards and mutual recognition, on top of the usual technical requirements to successfully transact and ship the goods through their forwarders and other trade parties. Corporate digital identities are particularly challenging due to the complexity of corporate attributes and architectural setup based on their organizational relationships with customers. Moreover, different jurisdictions have different forms of legal entities, which may make it more difficult to harmonize across borders.

Collaborative efforts at digital partnership between jurisdictions are far in few between in terms of scale of actual success. So far pilot projects are restricting to the likes of cross border customs clearance and payment identities used for purposes of trade financing since limiting access to trade finance is a barrier to trade. For cross border payment, distributed ledger technology (DLT) when combined with other technologies, has the potential to significantly lower the cost of compliance.[32]

Know-your-customer utilities and digital identity can facilitate information-sharing and help reduce the cost of compliance, including with respect to anti-money laundering/combat finance terrorism (AML/CFT) regulations as well as sanctions-related control documentations. However, the use of new technologies in the field of the abovementioned compliance may be limited by broader issues, including the extent to which regulation would allow financial institutions to outsource customer due diligence to mitigate risks such as money laundering, financing terrorism, and other illicit activities. The challenge is on the lack of harmonized standards within APEC, even within the financing industry. As it stands, EU is advanced in their research stage on the use of wallet identity for cross-border payments within their region including AML/CFT and sanctions control respects and supported by EU legislation. For APEC, there's no available data that governments or private enterprises are being more advanced in wanting adoption of abovesaid technologies for these trade compliance considerations within the trade bloc as many jurisdictions are also still in early stage of implementing National IDM (see **Appendix 3** for the status in OECD nations).[34]

Notwithstanding, China is strengthening the research and application of new generation information technology to accelerate the empowerment of trade digitalization. The advancement of cloud storage and computing services support the rapid development of cross-border e-commerce and promotes digital transformation of service trade. The State Government has already embarked on the initial establishment of a blockchain infrastructure called Xinghuo Blockchain Infrastructure & Facility (Xinghuo BIF, Chinese name "星火链网") to enhance digital identity and boost digital economy, to complement the advantages of privacy computing and cross-border data collaboration and sharing. Their industrial internet identification resolution technology transforms the entire process of goods circulation into data circulation through digitization and informatization, providing a prerequisite for the digital transformation of trade. These are ground initiatives that show how APEC economies recognize the importance of trade digitalization through development of digital identities and interoperability of digital identity regimes, in alignment with the objectives of regional or bilateral digital economy agreements and cooperation *(see **Appendix 2** for more information on the regional and bilateral digital economy agreements).*

Even though there are various national identity regimes in individual APEC economies, they are mostly developed for either public sectors or local consumers and enterprises' use. The drive towards cross-border trade digitalization requires national identity regimes to transit to a harmonized cross-border digital identity regime where different regimes are interoperable and recognized in a trusted manner, thereby imposing minimal regulatory burden on enterprises.

e. Importance of interoperability of digital identity regimes

The COVID epidemic has also brought the APEC region closer to a digital society, which includes five elements: digital citizenship, digital lifestyle, digital business, digital identity and digital connectivity. The ability to prove businesses' identities is a fundamental component of economic development, and governments recognize the importance of implementing and deploying a national identity system to facilitate cross-border trade. Influenced by the geography and economic prosperity of the individual APEC economies, different approaches will be adopted in the design and degree of implementation of digital identity systems. However, it should also acknowledge its risks and

challenges including the right to privacy of personal and business data, cybersecurity risk of sensitive data being leaked, and whether business data could be used for government and/or commercial surveillance. Instead of dividing into countless different "identity islands" by different platforms and applications like current situation[35], an interoperable regional and global digital identity system importantly enables users to have own control of their digital/business identity and access to multiple platforms, thereby improving trade efficiency, privacy and security of data transmission and user experience. **A unified and interoperable digital identity regime is fundamental to the advancement of regional and global trade digitalization, through joint public and private sector cooperation.** Governments in the early stage of national digital identity implementation could conduct digital identity pilots with digitally mature APEC economies that have a robust national identity regime, while involving technology companies to improve the efficiency and inclusiveness of their current identity management systems. Private sector players involved in digital identity technologies could be motivated through governmental means to expand on their capabilities to improve and advance current cybersecurity risk management tools, under a standardized regulatory framework recognized and adopted by APEC economies which clearly define the roles, responsibilities of all parties involved, especially third parties with access to business and trade data in the cross-border trade chain.

Section (3) Enabling digital trust, interoperability and cross border data flows in trade using decentralized technologies and identity solutions

a. Technical challenges in designing digital identity systems for global trade

A natural starting point to solving interoperability is to first solve for digital identity. Digital identities could be related to not just individuals and organizations, but also products, systems, web pages and devices – anything that can be identified.

Traditionally, designing a stand-alone digital identity system starts with a set of questions to inform the technical requirements for a system. Common questions include:

- What is the objective of the digital identity?
- How do we establish trust?
- What are the policy design choices (e.g., roles, safeguards & assurances, etc.)?
- What is the appropriate governance framework?
- What is the appropriate information architecture typology?
- Where does the digital identity data reside?
- What are the appropriate credentials, identification & authentication factors?
- What are the relevant cybersecurity threats & failures?

Aligning global trade stakeholders on answering digital identity questions is a challenge in the context of global trade, as this involves multiple participants, across jurisdictions and heterogenous technology systems and differing requirements. Designing one digital identity system that meets all the needs for global trade participants and use cases is neither practical nor feasible.

Given many digital identity systems exist within existing and emerging trade systems, one area of focus is with regards to examining technologies that can complement existing and emerging trade systems. As trade is inherently decentralized, decentralized digital identity systems and how they may support enabling cross border data flows for global trade is an area of interest.

Designing a decentralized digital identity system in this context needs to balance different and at times competing requirements: discoverability, accessibility, privacy, trust, safety and consent. While several technologies exist, choosing ones that have a high-level of maturity, active and wide community based on industry standards is desirable.

b. High level types of decentralized technologies (non-exhaustive) that are relevant for cross border trade, it's role in enabling digital trust, criteria when it's relevant

DID and VCs have high relevancy in cross-border trade scenarios where there can be privacy-preserving and secure sharing of credentials (e.g., individuals, organizations, products, etc) to receiving customs authority in the context of cross-border trade. Each trade transaction is enabled by VCs and DIDs, which facilitates importing authority in the verification of exporter credentials as the basis for goods clearance. OpenID Connect for VC (OID4VC) in the same scenario facilitates the authorization-based information exchange between individual exporting companies with customs authorities in the issuance and presentation of the VC. It enables exporting companies to authorize receiving

customs authority in accessing their credentials, while authorities can independently verify the exporter's digital identity without having a direct relationship with the identity issuer.

Whereas decentralized identity solutions (using VCs, DIDs and OID4VC) enable issuance, presentation and verification of digital credentials, decentralized technologies like blockchain and DLT provide the digital infrastructure for the immediate sharing of underlying transactions and assets in each trade transaction on an immutable ledger that can be accessed by participants in a network. Interoperability protocols enable integration of decentralized identity solutions and different blockchain or DLT solutions to enable integration, orchestration, and abstraction of different protocols to enable ease of integration for Web3 networks which may need to connect with other Web3 infrastructure platforms.

These decentralized technologies are complementary and share similarities in establishing digital trust, preserving privacy while increasing efficiency and giving back user control of their DID in relation to product and business credentials.

#	Type of Digital Identity Technology	Brief Description	Role in enabling Digital Trust	Relevance Criteria	Examples
1	Decentralized Identifiers (DID)	DIDs are a new type of globally unique digital identifier, a string of characters that identify a resource or entity.TIndividuals and business entities can create and manage their own identifiers without relying on centralized authorities or intermediaries. DIDs, also known as SSI, are a fundamental building block for a new layer of decentralized digital identity and public key infrastructure for the internet, offering secure and private digital identity systems.	DIDs provide a decentralized and immutable way to verify and authenticate digital identities, enhancing trust by reducing the reliance on centralized authorities.	Relevant when trust needs to be established without reliance on central authorities or when users need full control over their identities.	A DID is a simple text string consisting of three parts: (a) a did URI scheme identifier, (b) the identifier for the DID method and (c) the DID method specific identifier. An example DID is: did:example:123456789abcdefghi
2	Verifiable Credentials (VC)	VCs are a fundamental component of the self-sovereign identity (SSI) framework and a key technology for securely and privacy-preserving identity verification on the internet. They provide a standardized way to prove identities via "bottom-up trust" without reliance on central authorities to digitally represent and	VCs are digitally signed attestations that enhance trust by allowing parties to verify the authenticity of claims made by an identity holder	Relevant when verifying the authenticity of claims or credentials is essential for cross-border trade.	Digital Identification Card, Digital Test Certificates, Digital Qualification Certificates

		exchange attestations or claims about an individual or organization			
3	Blockchain & Distributed Ledger Technology (DLT)	Blockchain and DLT is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.	A decentralized way for providing immediate, shared and transparent information on an immutable ledger that can be accessed by participants in a network.	Enables parties to be in sync about a shared state of facts. Allows for decentralized means of reaching agreement on a shared set of facts.	Useful for variety of industries, including financial service and digital trade which is inherently decentralized.
4	OpenID Connect for VC	Built on top of OAuth 2.0 and OIDC, OID4VC enables end users to directly present identity information to relying parties to enable end users more control over when and what information they are sharing and gain portability of their digital identity. This includes three standards related to authentication, VC issuance (OID4VCI) and VC presentation (OID4VP)	Leverages open standards for authentication and authorization. In the context of cross border trade, this can be useful to enable individuals or organizations to control the sharing of their digital identity, while allowing verifiers (e.g. counterparty or third party) to verify an identity without having a relationship with the issuer of the digital identity.	Relevant when different countries and systems have multiple issuers of identities across multiple siloed systems. Authorization will be required to specify access rights/ privileges to resources (e.g. digital identity). Authentication is the process of verifying the identity of a user or organization. Using OID4VC, a user or organization can prove their identity by providing their credentials, which can be cryptographically verified.	Useful for one-click sharing of VCs with consent. Since the protocol allows for dynamic, deferred VC issuance, user need not hold required VC in their wallet, well in advance. As a result, user experience is much better. This protocol also allows for authentication using a portable DID

c. What are the key design considerations to enable interoperability?

Digital identities have emerged as crucial enablers of trust in cross-border trade. Achieving seamless interoperability and portability of these digital identity solutions is paramount to fostering efficient and secure international electronic transactions.

This digital trust serves as a vital precursor to successful digital cross-border trade, as it ensures the legitimacy of parties involved and the authenticity of exchanged information.

Identity Standards and Formats: Adopting common global standards and data formats is pivotal to enable seamless interoperability across diverse networks without the need for intricate data transformations. When universally accepted formats are embraced, the sharing and interpretation of data become streamlined, ensuring efficient communication between different systems. This standardization promotes a cohesive ecosystem where data

can be readily understood and utilized across borders and industries, fostering smoother cross-border transactions, and enhancing overall operational efficiency.

Data Minimization and Consent: Vital not only for ensuring compliance with data protection laws like GDPR but also for building trust with customers and partners in cross-border trade. Fostering a privacy-conscious approach demonstrates commitment to respecting individuals' rights and can help organizations avoid legal and reputational risks associated with mishandling personal data in international trade transactions.

Security and Encryption: Plays a critical role in ensuring the confidentiality, integrity, and authenticity of data exchanged during cross-border trade. Protecting sensitive information, including digital identity, financial data, and trade secrets, is essential for compliance with data protection regulations and for building trust among trade partners. Prioritize security measures like encryption, hashing, and digital signatures to protect identity data during transmission and storage. Employ strong authentication methods, including multi-party computation.

Privacy by design: It is a proactive approach to data protection and privacy that involves considering privacy principles from the outset when designing systems, processes, and products. In the context of cross-border trade, where there may be exchange of personal and sensitive data, implementing Privacy by Design principles is essential for ensuring compliance with data protection regulations, building trust with customers, and minimizing the risk of data breaches.

Decentralized Identity: The capability to transition identities across jurisdictions seamlessly is a fundamental enabler of cross-border digital trade. The development of mechanisms that facilitate such seamless portability while maintaining the sanctity of data integrity and security is paramount. This innovation simplifies the complexities associated with changing regulatory landscapes and varying identity requirements across different regions. As individuals and businesses navigate international interactions, the capacity to seamlessly adapt their digital identities to new contexts fosters operational efficiency and bolsters trust among trade partners.

Ensuring the efficacy of cross-border digital identity solutions necessitates a comprehensive approach to identity lifecycle management. From initial registration to eventual revocation, an organized and structured process is essential. Robust identity lifecycle management processes encompass not only registration but also the issuance of credentials, mechanisms for revocation in case of compromise, and the eventual retirement of identities. Amid the dynamic evolution of digital identity, the management of identity attributes and credentials over time remains a critical consideration. Addressing these facets diligently results in a resilient ecosystem where identities are maintained, updated, and retired in a secure and controlled manner, safeguarding the overall integrity of cross-border trade operations.

Scalability and Performance: Crucial considerations for platforms involved in cross-border trade. These platforms facilitate international commerce, and their ability to handle increasing transaction volumes while maintaining responsiveness and reliability is essential.

Compliance and Auditing: To ensure the robustness of cross-border digital identity endeavors, the implementation of appropriate auditing and compliance mechanisms is needed. These mechanisms serve as vigilant guards, meticulously monitoring and enforcing adherence to established cross-border identity standards and regulatory frameworks. By meticulously tracking compliance, organizations can not only ensure the alignment of their practices with global norms but also bolster the trust of stakeholders by showcasing their commitment to secure and compliant operations. Additionally, having well-defined processes for handling instances of non-compliance and security incidents bolsters the resilience of cross-border digital identity ecosystems. Swift and well-coordinated responses to breaches or deviations from regulations contribute to the overall integrity and security of cross-border trade operations.

Legal interoperability: A pivotal facet of cross-border digital identity facilitation involves addressing the intricate landscape of legal frameworks and regulations. By navigating complexities like jurisdiction, liability, and dispute resolution, organizations can foster a cohesive environment where digital cross-border trade transactions unfold seamlessly. Striving for legal harmony in this context is essential not only for regulatory compliance but also for cultivating an environment where businesses and individuals can engage in cross-border interactions with clarity, confidence, and legal protection.

Collaboration and Governance: Forging a robust foundation for the interoperable identity ecosystem benefits from the establishment of governance models and collaborative frameworks that unite governments, private sector entities, and international organizations. This concerted effort serves as the cornerstone of effective management and maintenance, enabling the sustained functionality and evolution of the ecosystem. By harmonizing the interests and expertise of these diverse stakeholders, a cohesive governance structure is formed, facilitating collective decision-making, standards enforcement, and strategic direction. Governments can provide regulatory insights, private sector organizations contribute technical innovations, and international bodies can offer a global perspective, together cultivating an environment conducive to secure, seamless cross-border digital trade interactions. Through these collaborative frameworks, an interoperable identity ecosystem can be created.

d. The role of verifiable credentials (VCs) and decentralized identifiers (DID) to avoid fragmentation and "identity islands"

The success of realizing an interoperable regional and global digital identity system starts from jurisdictions' willingness to recognize and adopt international standards for digital identification. The W3C DID standard defines DID as a new type of identifier that enables verifiable, decentralized digital identity. A DID may refer to any subject, a person, organization, thing, data model, abstract entity, etc. as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.[36] Given that the identifiers are not controlled by a centralized platform, this approach to digital identification is also known as "Self-Sovereign Identity (SSI)" as envisioned by the Decentralised Identity Foundation.[37] An entity (person, organization, thing) may hold multiple context aware DIDs and associated cryptographic keys. Possession of keys allows the entity to prove ownership of that **DID. A DID is globally unique, based on four important properties:**

(1) Decentralization: A DID need not be issued and controlled by a centralized authority.
(2) Inherent persistency: A DID need not be stored at a centralized location. It is portable.
(3) Resolvability: A DID always resolves to a 'DID document'. DID document contains the information related to cryptographic keys and other metadata associated with the DID.
(4) Cryptographically verifiable: Using the cryptographic keys available in the DID document, A DID can be verified independently by any verifier.

Complementary to DID, a VC is defined in W3C VC standard as a "specification that provides a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable.[36] **A VC comprises of three key parts**:

(1) Metadata: Credential type (eg. Business registration VC), Issuer details (Eg. Issuer Name, Issuer DID etc), etc
(2) A set of one or more claims: e.g. Business name, Business type, establishment year etc
(3) Proof: cryptographically verifiable proof that the VC has not been tampered with (e.g., json web signature)

VCs are issued to a holder (usually the subject), who can present to any verifier without geographical limitation. VCs may reference a DID as the issuer and/or subject of a credential. See **Appendix 4** for figurative illustration of the interaction between decentralized identifiers and VCs.

Such a relationship between digital identifiers and VCs is beneficial to overcome above-mentioned challenges of interoperability of digital identity regimes for cross-border trade digitalization, only when there's well defined standards recognized as international standards for adoption. When trade data is exchanged across platforms or national trade single windows with export or import documentation identifiers issued as VCs differently, verification costs for governments around the world will become prohibitive, thereby limiting interoperability. Instead of dividing into countless different "identity islands" by different platforms and applications, interoperability has to work at two levels, one through technical interoperability and the other through semantic interoperability.

- **Technical interoperability** is concerned about consistent implementation of protocols like DID methods, cryptography suites, and so on. This is the domain of the W3C and the Internet Engineering Task Force and there are already some well documented standards and certification test services.

- **Semantic interoperability** is concerned with a common understanding of language. Standards are usually domain specific (i.e., health, education, supply chain, etc). Standard data models, data exchange structures and code lists, when used consistently, will mean that a certificate VC issued by one system will be readable and understandable by another.[36]

Although technical interoperability is a fundamental prerequisite for any successful implementation, it is not sufficient. It only guarantees that a credential issued by one platform will be verifiable by another. However, it does not confirm that both platforms understand the meaning of the claims in the credential. This kind of semantic interoperability issue sits at a level above the technical interoperability concerns, using standard vocabularies, specifically vocabularies expressed in JavaScript Object Notation for Linked Data or JSON-LD syntax and managed by a standards authority relevant to the business domain. JSON-LD requires vocabulary to be globally unique and referenceable with a permanent web URL. This is so that computers can understand the difference between similar terms managed by different authorities that might have different meaning. For most cross-border trade terminology, the semantic standards authority is UN/CEFACT with draft JSON-LD vocabularies. Since it is impractical to build a system that "understands" every term in the entire vocabulary, JSON-LD provides a concept called "@context" which represents a subset of one (or more) vocabularies.[36]

Given these considerations, the role of regional or global standards bodies and non-profit organizations is thus crucial in the setting of harmonized standards on interoperability, which can be used by APEC economies for cross-border trade use cases. For example, the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) and Extensible Markup Language (XML) Messaging are largely re-usable in VCs. The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) being the leading global standards body also publishes its semantic standards in format that is compatible with the VC technology so that they are easily usable by implementers around the world. Since there is already a full set of UN/CEFACT international trade data exchange subsets which define specific process areas such as invoicing, contracts, certificates, etc. and more in time to support uptake of DIDs and VCs on the international supply chain, APEC economies could already take these standards as formal recommendations in the implementation of digital economy agreements, and develop them into regional standards following more successful pilots between APEC economies of different digital maturity levels and technology companies.

e. How blockchain and distributed ledger technologies support verifiable data registries for DID and VC

DIDs and VCs do not require blockchain to work effectively. Any publicly accessible "verifiable data registry" can be used for storage. The registry must be publicly accessible because an issuer has no a-priori knowledge of who will be verifying. Any public register will work, provided it has sufficient integrity and durability for the VC/DID purpose for which it is used. See **Appendix 5** for the relationship between DID, VCs and the role of verifiable data registries, and the list of public data registries that can underpin a VC/DID ecosystem.[36] Among the categories of public data registries, there are public blockchains and side-trees which are pinned to a public blockchain on an occasional basis, in addition to non-blockchain ledgers like Distributed Ledger Technology (DLT) and the web. To enable inter-blockchain readability, there is also open-source global standard for chain-specific integrations while users can interact with any blockchain via a single interface, under a scalable architecture that is extendable and future-proof.

In essence, VCs and DIDs depend on publicly accessible data registries and not solely on blockchain technology. However, blockchain is one of the viable, highly-reliable solution for cross-border trade use cases. Some use cases may be suited to dedicated DLTs or side-trees pinned to public blockchains, such as DID for non-permanence transactions such as consignments that may find did:key or IPFS (did:ipld) to be a good choice.

f. Identification of national trust registries and making verifiable identity a national asset while incentivizing verifiable import data sets APEC up towards interoperability success

For cross-border trade digitalization, what is fundamental to the basis of technical and semantic interoperability is the establishment of a digital trade trust architecture in any economy, since the recognition of VCs at the end of the trade chain (e.g., importing economy) will only happen when there is trust in the issuer of VCs between economies. This is through the mutual identification of authoritative entities known as national trust registries within the APEC region, who could be government agencies administering local trade laws or national digital identification regimes, or other governance organizations such as national accreditation authorities. For example, the Ministry of Trade authorizes the chambers of commerce to issue preferential certificates of origin; the customs agency authorizes trained customs declarants to file import declaration; a national accreditation authority accredits laboratories to issue ISO-14000 or

other quality standards-based certifications for overseas product registration and exportation purpose. These are examples of national trust registries who issue the VCs making such claims (e.g., certificate of origin certifying the product is made in Philippines), which can then be verified in an importing economy presented with the VC. The role of national trust registries allows the verifier to confirm that not only is the VC valid but also that the issuer is authorized to make such claims and that the authority has not been revoked.

This foundational national digital trade trust architecture is implemented simply by empowering each trust registry to do digitally what they already do manually. As an implementation guidance, it is specified in UN/CEFACT's white paper on VCs for cross-border trade[36] that "every party in a national economy that receives some kind of accreditation or authority from a trust registry should be able to request that authority in the form of a digital VC so that they can link any VCs they issue to the trust registry that attests to their authority."

Additionally, authoritative entities who are administering national digital identities could provide a service for any authenticated constituent to self-issue an identity VC that links their self-sovereign identity to their national identity. This brings about the concept of making verifiable digital identities a national asset for cross-border trade digitalization to be realized. By doing so, it expands the use of national digital identity schemes currently limited to government use to individuals' and businesses' use cases where there is a need for them to provide their identity far more frequently in cross-border trade transactions.

Given that DIDs and VCs provide a means for a national economy to release the value of high integrity proof of national identity to constituents without any need for regulatory change or for any extension of identity federation to non-government or foreign parties, import authorities as national trust registries can help increase the trust of high integrity digital verification of import consignments by providing policy levers to incentivize exporters to issue VCs.[36] The other important implementation guidance specified by UN/CEFACT is the testbed where national trust registries identify and incentivize opportunities for streamlined import clearance when import documentation is supported by digital VCs issued from the exporting economy.

g. The role of DID methods in facilitating interoperability of digital identities

Since DID play a key role in the issuing and verification of linked credentials, where a key dependency is the cryptographically verifiable connection between the subject of one VC and the issuer of the next, there has to be standardization on the DID methods. A DID method is defined by a DID method specification, which specifies how a DID and DID documents are created, resolved, updated and deactivated.

The W3C DID specification is designed to allow market innovation to drive DID methods (e.g., did:key, did:web, did:ethr etc.). Whilst this is a good decision in principle, it has led to a proliferation of candidate DID methods. A overview of some of the common DID methods (non-exhaustive) are below:

	did:ebsi, did:polygon	did:web	did:key	did:keri
Root of Trust	Blockchain	Optionally anchored public keys & VCs on blockchain	Self-certifying	Key Event Receipts Log (Not blockchain)
Portability	Ledger locked	Tied to web domain	Portable	Portable
Reliability	High	Single point of failure is public domain	Keys cannot be rotated / revoked	High
Scalability	Low to medium	Medium to High	High	High
Operating Costs	Medium to High	Medium to Low	Low	Low
Suitability	Low-frequency, high trust apps	High-frequency, low trust apps	Low-impact use cases compatible with ephemeral credentials	Central Authority-controlled credentials needing high frequency, low cost, and good trust

h. Blockchain and distributed ledger interoperability using interoperable protocols

As examined in above sections, interoperability of digital identity regimes for cross-border trade digitalization is a critical success factor. The more independent decentralized systems, the more critical standards and interoperability becomes. Based on the semantic standards architecture for interoperability by UN/CEFACT, the goal of the framework should ensure that each jurisdiction's digital identification implementation for business identity and trade documents are interoperable with others using internationally standard vocabularies.

Economies in Asia Pacific have different digital identity solutions. Some are on traditional technology, while others are leveraging new technology i.e., blockchains. To enable economies with blockchain based solutions, and facilitate cross border trade follow, interoperability is key. To enable interoperability between these disparate blockchains, an **interoperability platform** is useful for enabling cross border data flows. Several open-source and proprietary interoperability frameworks can link networks built on heterogeneous distributed ledger technologies (DLT) and blockchain technologies and execute transactions spanning multiple networks to enable the flow of value and assets. Some of the more common examples include Chainlink's Cross-Chain Interoperability Protocol (CCIP) and Hyperledger Catci and Hyperledger Harmonia). See Appendix 5 on a cross-border payment use case using an interoperability protocol.

A key design tenet for these emerging interoperability platforms does not require modification to any existing DLT stack and operates purely at the contract- and-application layers.

Blockchain interoperability systems enable the transfer of information and digital assets between two blockchain or DLT networks and between blockchain or non-blockchain platforms (i.e., an interoperability platform). Some of the key architectural features needed to create a blockchain interoperability standard and provide users with guarantees include:

- Decentralized Security: Decentralization is key to ensuring there is no single point of failure and maximizing security and reliability. This can take the form of having decentralized networks made up of independent nodes for processing transactions and a defense-in-depth approach to security, ensuring checks and balances and multiple security checkpoints for increased resistance against tampering and downtime.
- Active Risk Management: Maintaining robust security requires external and independent monitoring, the ability to detect and halt suspicious activity, and configurable risk parameters to account for the different trust assumptions of stakeholders. Risk management is essential to all mission-critical systems, especially those that automate the transfer of value using data.
- Agnostic and Credibly Neutral Platform: An interoperability protocol must be independent of any specific blockchain technology stack if it is to support a wide range of blockchain technologies and future-proof itself to inevitable changes in the industry. Being agnostic and independent also ensures credible neutrality, meaning no party can gain an unfair advantage because it can't also serve as the administrator of the network.
- Universal Connectivity: Support for a wide range of heterogeneous systems is key to global collaboration. In practice, this entails being able to read data from and write data to EVM and non-EVM blockchains, public and private blockchains, layer-1 and layer-2 blockchain networks, centralized and decentralized VC databases, and other forms of distributed ledger technologies (DLTs). Furthermore, it must be easy for existing systems to interact without meaningful modifications, such as through APIs.
- General-Purpose Functionality: The ability to both exchange data and transfer value (e.g., tokenized assets) across blockchains and non-blockchain systems enables a broader set of workflows and creates more efficiencies. For example, there are a plethora of workflows that open up if the interoperability protocol can facilitate identity verification, and, upon approval, automatically trigger a subsequent action (e.g., payment for goods). This creates a streamlined process for global trade.

- Readily Available Network: The interoperability protocol should have a network of nodes that is readily available to users, as opposed to users having to construct their own networks each time they want to engage in a business relationship. This abstracts away the complexity of backend decentralized systems so users can conduct business in a more efficient manner.
- Open Code Base: Enabling all stakeholders to directly verify the source code of an interoperability solution will further increase trust in how it operates. It also encourages global collaboration around auditing the codebase and upgrading it to support emerging industry needs, ultimately creating higher security for everyone.
- Excellent Developer Experience: It's important for stakeholders to be able to integrate with the interoperability protocol through a simple interface. The interface should abstract away the complexity of the integration, monitoring, and the specifics of the destination blockchain (i.e., users should not care whether the destination is a similar tech stack or totally different).

Blockchain interoperability systems can complement decentralized identity systems. For example, these interoperability solutions enable the invocation of a verification function on a decentralized identity system located off-chain.

In order to better understand how cross-chain interoperability can support complex, multi-party workflows, consider the following example:

> A US company is buying goods from a manufacturer in Spain. Both organizations have accounts with banks in their respective countries and hold trade licenses issued by the relevant authorities in their respective jurisdictions.

Decentralized identity and blockchain technology can add value in this scenario by providing a means to verify relevant documents, define and manage contractual relationships, and automate key parts of the workflow without the need for a single, centralized point of trust or control.

Decentralized technologies are relevant as trade is also inherently decentralized and it's unlikely all parties will be using the same service provider, application, and, in practice, may face the challenge of bridging documents and managing key parts of the workflow across multiple heterogeneous networks to facilitate the trade end to end. In addition, today, all parties have to trust one another to not modify key information about the trade in their respective source systems after a contractual agreement has been signed.

A secure and credibly neutral means of transferring information and contractual assets across different network boundaries with the assurance that immutability of key elements is required. Consider the following arrangement:

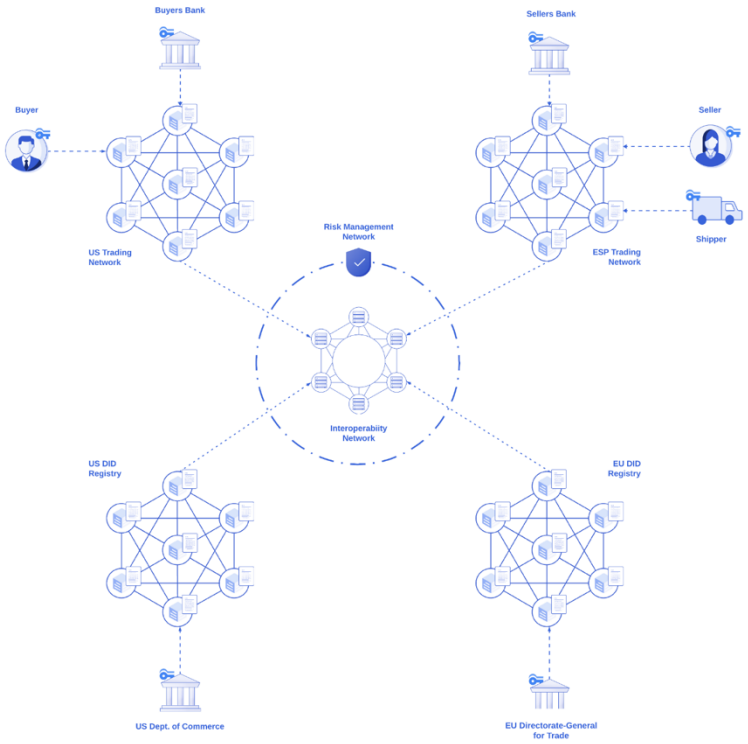


Figure 1 - Cross-Chain Interoperability in international trade

In the example above, there are four independent blockchain platforms, each built on (potentially) different underlying technology. However, with secure cross-chain interoperability in place, there is a means to issue, update, and exchange all relevant assets and manage contractual obligations and payment flows throughout the entire process without resorting to a single point of trust.

Asset	Technology	Cross-Chain Benefits
Trade Licenses	Verifiable Credentials	Allows a verifier (e.g., the seller) to retrieve the DID document containing the public key of the license issuer (e.g., U.S. Dept. of Commerce) from its corresponding DID which resides on a Verifiable Data Registry (VDR) on a different blockchain.
Trade Agreements	Multilateral Contracts	Allows a seller to establish an agreement with a buyer on a different blockchain platform and remain assured that all information remains in synchronization and in accordance with pre-agreed constraints.
Bills-of-Lading	Non-Fungible Tokens	Allows a shipping company to establish a bill-of-lading on their own blockchain platform that can be transferred to buyers, sellers, and their banks as a transaction progresses, irrespective of the chains they reside on.
Proof-of-Delivery	Non-Fungible Tokens	Allows a buyer to confirm receipt of goods, which then becomes an input for the

		automation of payments and can also be used in connection with dispute management processes.
Cash Payments	Fungible Tokens	Allows payments using tokenized cash to be made between buyers and sellers with bank accounts on entirely different blockchain platforms.

i. Select case studies of decentralized technologies and identity solutions being implemented in trade and beyond

An example of a distributed ledger technology and verifiable credential implementation includes the European Blockchain Services Infrastructure (EBSI), which uses Open ID for VC issuance (OID4VCI) and VC presentations (OID4VP), as detailed in **Appendix 6.** This approach allows individuals or organizations to own and share digital identity with third parties directly in a decentralized approach.

Another example is the cross-border blockchain infrastructure called Xinghuo Blockchain Infrastructure & Facility (Xinghuo BIF). In response to the potential EU carbon tariff on products exported to the EU, Siemens China partners with Xinghuo BIF to build global trusted digital platform tracking carbon footprint by utilizing DID and VC technologies. Also, Xinghuo BIF works with SAP to construct a DID-based blockchain network for interoperable digital identity, in this project SAP connects China's Xinghuo BIF, Microsoft's ION blockchain network and German's IDUnion blockchain network, for trusted data exchange. Currently Xinghuo BIF is working with GLEIF vLEI project, to include QVI(Qualified vLEI Issuer) in the Xinghuo BIF ecosystem, to enable real-time and automated authentication between counterparties in all industry sectors worldwide.

The Global Legal Entity Identifier Foundation (GLEIF) has also pioneered a new form of digitized organizational identity to meet the global need for automated authentication and verification of legal entities across a range of industries called the verifiable LEI (vLEI). By creating the vLEI, GLEIF is now answering to this urgent and unmet need of pioneering a multi-stakeholder effort to create a new global ecosystem for organizational digital identity. vLEIs are based on the Trust over IP Authentic Chained Data Container (ACDC) specification (based on the Key Event Receipt Infrastructure (KERI) protocol, both Internet Engineering Task Force (IETF) draft specifications). See **Appendix 7** on KERI protocol, and how through vLEI credentials can be issued in the context of engagement of persons with an organization which can be verified by the organization.

Another recognized framework allowing the portability of digital identities is the **Trust Over IP (ToIP)** which provides a framework and principles for creating and using VCs as a tool with digital identities. Importantly, ToIP-based VCs can incorporate revocation and expiration mechanisms. If a VC needs to be invalidated due to compromise or expiration, the issuer can revoke it, making it unverifiable. This capability enhances the trustworthiness and accuracy of the presented credentials, ensuring that relying parties can rely on up-to-date and valid information. ToIP can integrate LEIs which are globally recognized unique identifiers assigned to legal entities participating in financial transactions, allow for seamless linkage of digital identities and facilitates reliable and verifiable representations of legal entities in digital transactions.

For digitalization of trade documentation, Singapore for instance developed OpenAttestation[38] to enable documents issued with this technology to be cryptographically trustworthy and able to be verified independently. OpenAttestation provides the technology underpinnings of TradeTrust. It uses Domain Name System (DNS) to verify the identity while DID can be used optionally. The open attestation protocol (a compatible & interoperable extension of W3C VC) provides a very powerful mechanism to turn paper processes into digital processes without impacting stakeholders who stay with paper.

- VCs are issued as digital credentials just like any other VC. Each VC is encrypted with a unique key and stored at a public location.
- The issuer defines a "decentralized renderer" that can present the VC in human readable form just like the paper.

- A QR code on the human readable format includes the decryption key, the URL of the digital VC, the URL of a renderer, and the URL of any compatible hosted verifier service.

An example of how to support blockchain interoperability for payments is described in the archetype workflow in Appendix 5, which showcases how to securely transfer data and value between legacy systems (e.g. SWIFT) and other blockchain platforms. In future, VCs and DIDs can be used to support enabling a decentralized way of issuing, sharing and verifying digital identities independently each other, while enabling portability and composability of these digital identities.

Using this protocol, the trade document is passed around the supply chain as a human readable document with QR code, just like existing paper documents. Verifiers (e.g., any of the seven parties in the preferential certificate example) can work at any level of digital maturity. Each standard or framework serves a specific purpose, addressing different aspects of digital identity, authentication, authorization, and trust. Organizations and developers often combine these standards and frameworks based on their specific needs and use cases to build secure and reliable systems. There is a need for leading APEC economies to harmonize and agree on the DID methods for implementation within each industry domain in the region.

Section (4) Key factors for success

The ability to successfully foster cross-border interoperability of digital identity regimes for trade digitalization is highly dependent on the following five key factors to realize the potential of paperless trade (see **Appendix 8**):

(1) Development and alignment of harmonized standards, protocols and implementation roadmap for interoperable digital identification regimes and digital transmission means legally recognized, through the nomination of national trust registries, and active participation of large non-profit organizations, standards bodies, trade associations;
(2) Dedicated support of governments investing in interoperable digital identification regimes to unlock cross-border data flows, with active commitment of both the public and private sectors to work together in pilot implementation, and incentivizing the role of technology companies to improve the efficiency and inclusiveness of established and developing national identity management systems;
(3) Fostering public private partnerships in the development of trust technologies recognized regionally and advancing towards a regional trust circle within APEC, to bolster user trust in trade digitalization and enhance the ease of adoption for end-to-end digitalization of cross-border trade documents;
(4) Capacity building and provision of shared technological resources led by digitally mature economies for the region, under the establishment of legal frameworks recognizing electronic cross-border trade transactions; and
(5) Incorporation of high trust digital identities and VCs for secure cross-border data flows adopting structured security assessment and privacy-enhancing technologies that protects user privacy, data security and giving users control of their own identifiers, through an interoperable digital architecture that grants access control to governments and trade parties.

It is therefore pertinent to consider above key factors for success in our efforts to adopt and implement interoperable digital identification and verification solutions. The support of the public sector is crucial in setting the legal environment, governing frameworks and harmonized standards, alongside large organizations, standards bodies and non-profit trade associations lending their domain expertise and technological capabilities to unlock the potential of secure and open cross-border trade data flows.

Section (5) Call to action

Looking forward, cross-border trade digitalization in APEC is poised for further growth in tandem with its proliferating digital economy, driven by: businesses' reliance on digital trade technologies; the increasing adoption of digital identification and verification technologies for interoperability and cross-border trade efficiency gains; the growing demand for trade digitalization to achieve efficiency and cost-savings in trade processes; and the heightened awareness of data privacy-enhancing and data security risk mitigation measures to be incorporated in the use of trade digitalization technologies. Additionally, the stance of governments recognizing the importance of cross-border trade digitalization through digital economy agreements and regional frameworks for cross-border privacy rules and digital data governance are expected to present more opportunities for businesses in APAC to participate in a heterogenous digital trade architecture and be ready for the institutional opening-up of trade domains and cross-border lanes digitally.

For cross-border trade digitalization to become the de facto practice at scale regionally within APEC economies and enabling end-to-end trade digitalization across economies and platforms, the intricacies and complexities of present regulatory barriers in 1) legal environment, 2) lack of harmonized standards/ market fragmentation and 3) capacity to make available digital trade infrastructure must be successfully dealt with. Governments must support the establishment of an enabling environment that facilitates cross-border trade digitalization, including regulatory framework, norms and standards. Addressing barriers to participation in digital trade technologies will help low socio-economic groups and micro, small and medium enterprises to improve their digital skills, access cross-border trade opportunities online and promote inclusive and sustainable economic growth while enhancing competitiveness in the digital economy.

The capacity building of digital trade infrastructure for APEC region, and continued advancement of strategic digital cooperation milestones through more active G2G and G2B collaboration efforts focusing on interoperability of digital identities and VC technologies is the key to addressing these challenges. The concomitant recognition of the role of large independent non-profit organizations in standards development and harmonization is necessary to support industry players in this trade paradigm to explore the applicability of high trust digital identities with VC across various trade digitalization scenarios.

Building on the use cases presented in this paper, the next step forward for APEC is to

a. Set up an APEC Steering Committee with the participation of UN/CEFACT, the leading global standards body and large non-profit organizations (e.g., GLEIF) to develop a 3-year implementation roadmap on recognized semantic standards for interoperable digital identification regimes, and allocate project teams to publish JSON-LD vocabularies and context files for a positive list of cross-border trade documentation, summarily known as a small collection of terms for issuers (national trust registries) and verifiers (importing economies) to encounter in these credential types;
b. Develop annual grant schemes administered by public sector leads of national digital identities, trade and industry or government digital structures to incentivize private technology companies specializing in digital identification and VC technologies to seek financial opportunities for testbeds on interoperability of digital identities and digitally issued credentials for cross-border trade use cases;
c. Form or further expand on current National Digital Identity Working Group under the main regulatory agencies in trade and/or cybersecurity to issue projects to the private sector to develop high trust, high-value VCs, and mutually recognized interoperable digital identities;
    - Establish Working Group Stream 1 to discuss how organizational identity can be used such as credit rating of know your customer (KYC)/ anti-money laundering (AML) at banks
    - Establish Working Group Stream 2 to discuss how product identity can be used such as building a new track and trace system for logistical tracking
    - Establish Working Group Stream 3 to discuss how document identity can be used such as detecting tampered documents and/or duplicated use of a single document
d. Boost widespread adoption of the MLETR into statute law of individual economies by disseminating global best practices on enabling electronic trade documents at APEC forums, and form consensus on the development of a heterogenous digital trade architecture led by digitally mature economies open to plug-in applications by private enterprises and least digitally mature economies in the region;
e. Pledge funding and resources to provide capacity building programs to least digitally mature economies to upskill and replicate secure cross-border data flows adopting data security assessments and privacy enhancing technologies of digitally mature economies, anchored by the mutual identification of issuers (national trust registries) by trade domains in individual economies.
f. Embark on cross-border digital identity pilots to educate industry on new technologies and solicit feedback. These pilot initiatives hold the key to substantiating the practical viability of interoperability and portability of digital identities within real-world scenarios. By strategically selecting a small group of economies and goods, governments and organizations can meticulously examine the nuances of cross-border transactions and interactions, shedding light on potential challenges and opportunities. The involvement of diverse stakeholders in these pilot projects adds a layer of richness to the insights garnered. As various participants collaborate, their collective expertise aids in identifying potential bottlenecks, refining processes, and addressing emerging issues in a collaborative manner. The outcomes of these pilot endeavors inform the larger trajectory of cross-border digital identity implementation, enhancing its efficacy and preparing the groundwork for wider adoption.

With the United Kingdom, United States of America and European Union making significant progress in cross-border trade digitalization efforts through their openness to cross-border data flows, including efforts between EU and Singapore in affirming their commitment to deepen their bilateral relations with respect to digital trade, APEC entering

its golden age of trade digitalization must ride on the waves of digital transformation to realize the economic benefits of cross-border paperless trade, and actively promote and support pilot projects that drive interoperability of digital identity regimes and advancement of verification technologies. Fundamental to the success of APEC's cross-border trade digitalization efforts and digital economy commitments in this golden age is a unified regional approach in achieving interoperability and portability of digital identities using internationally standard vocabularies, in recognizing national trust registries, and in strengthening public private partnerships bolstered by the support of non-profit organizations, standards bodies and trade associations who help set regionally harmonized standards embracing key components of high trust digital identities in their archetypes for different ecosystem players.

Appendix 1

1. On 26 May 2022, GovTech Singapore signed a Memorandum of Cooperation (MOC) on Digital Government Transformation with Japan's Minister for Digital, Karen Makishima in Tokyo. The three-year agreement will focus on the exchange of knowledge and experience in areas including digital identity, artificial intelligence, cybersecurity, cloud services and even digital technologies to tackle the COVID-19 pandemic. On the National Digital Identity (NDI) front, for example, both countries will explore the mutual recognition of verified credentials for their residents' digital identities. This will benefit digital trade and people-to-people flows between both countries.[39]

Japan also seeks Singapore's experience in national digital ID rollout. The cooperation is based on a bilateral agreement which the two countries entered into last year with the main objective being to allow digital collaboration in different areas including digital identity, cybersecurity and related services.[40]

2. In 2022, a MoU was signed by the governments of the Philippines and Singapore that would allow each nation's digital ID to be recognized in the other's jurisdiction. The deal fits with a broader global trend of bilateral deals between nations to promote interoperability among digital identity and related systems.[41]

3. Governments of Singapore and the Republic of Korea (ROK) have signed the Korea-Singapore Digital Partnership Agreement (KSDPA), which aims to create seamless and secure data flows between the two countries' digital systems. The agreement includes 11 "modules," one of which covers digital identity interoperability.[42]

4. Singapore, New Zealand, and Chile have finalized negotiations for the Digital Economy Partnership Agreement (DEPA). The countries joined forces to address digital concerns such as electronic documentation in cross-border trade, personal data protection, and cybersecurity. For example, digital identity could be introduced to promote digital trade, while cutting down on document transit time for cross-border trade would reduce operating costs. At present, DEPA requires the mutual recognition of digital identities for products as the goal, enhances regional and global interconnection, and is committed to professional cooperation in policies and regulations, technical implementation and security standards related to digital identities.[43]

6. In 2022, the European Union and Japan concluded the EU-Japan Digital Partnership, the first digital cooperation initiative to advance economic growth and provide a safe and inclusive space to solve digital issues. This effort furthers the "Data Free Flow with Trust" agenda, aimed at facilitating safe and secure cross-border data flows. As part of the common vision, the Digital Partnership identified a number of key action items, such as "implementing concrete pilot projects in cutting-edge areas such as AI and digital identity".[44]

7. The European Union and Singapore announced that the EU-Singapore Digital Partnership will be formally signed and launched in 2023 and aims at reinforcing existing relationships between the European Union and Singapore in the digital realm to achieve sustainable economic growth. The range of digital issues the collaboration will focus on 6 areas and "digital identity" is regarded as one of the emerging technologies.[45]

8. On 30 January 2023, Ministry for Trade and Industry and Malaysia's Ministry of International Trade and Industry signed two Frameworks on Cooperation (FoC) in Digital Economy and Green Economy. Out of the focal areas, two are on Cross-border Data Flows and Digital Identities. (1) To support cross-border data flows, including the use of interoperable mechanisms for the protection of personal data, such as the APEC/Global Cross-Border Privacy Rules system and ASEAN Model Contractual Clauses ("MCCs") (2) Digital Identities: To promote exchanges and knowledge-sharing to facilitate the interoperability and development of our respective digital identity regimes, for both individuals and businesses. This includes efforts to support the development of the ASEAN Unique Business Identification Number ("UBIN").[46]9. The Korea-Singapore Digital Partnership Agreement (KSDPA) is Singapore's fourth Digital Economy Agreement (DEA), and the first with an Asian country. The agreement will deepen bilateral cooperation in the digital economy between both countries, by establishing forward looking digital trade rules and norms to promote interoperability between digital systems. This will enable more seamless cross-border data flows and build a trusted and secure digital environment for our businesses and consumers. Similarly, out of the focal areas, two are on promoting interoperability of digital identity regimes and enabling cross-border data flows to support digitally-enabled activities including for financial services.[47]

47. MTI Singapore website on KSDPA, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA

Appendix 2

Australia

On 11 May 2021, the Australian Government released its Digital Economy Strategy, a $1.2 billion investment to ensure Australia has the right policy settings, infrastructure and capability to support digital transformation. Through the Digital Economy Strategy, Australia is set to become a modern and top 10 digital economy and society.

The Digital Trade Strategy from the Department of Foreign Affairs and Trade provides a framework for Australia to maximise economic growth by shaping an enabling environment for digital trade. It guides Australia's practical action as a leader in digital trade, informing our work to develop digital trade rules to deliver commercial benefits and push back against digital protectionism. Specific to cross-border trade digitalization under the digital trade agenda, focal areas include electronic facilitation of trade, such as the acceptance of electronic trade documents and, possibly, the adoption of 'regtech' solutions as technology evolves; Transmission of data across borders as a business activity in its own right and to support other business activities.[48]

China Xinghuo

Xinghuo Blockchain Infrastructure & Facility (Xinghuo BIF, Chinese name "星火链网") is a permissioned public DID-native blockchain network, initiated by China Academy of Information and Communications Technology (CAICT). Xinghuo BIF is the largest-scale blockchain infrastructure in China, and it provides multiple services targets on different industries, include supply chain finance, traceability, carbon neutral, cross-border trade, web3 name etc.

The philosophy of Xinghuo BIF construction is that, builds Xinghuo BIF blockchain nodes in various countries, which are controlled and operated by trusted entities in each country. Every country's node follow the same governance principles and operating rules, including the governance rules of the trust registry in the digital identity field, and promote collaborative cooperation and development among multiple countries in digital economy through blockchain technology, and through DID technology, Xinghuo BIF provides countries with self-sovereign and interoperable digital identities, thereby promoting mutual recognition of digital identities among countries around the world, and promoting global application scenarios such as cross-border trade, green finance and carbon trading.

India

India's Open Network for Digital Commerce (ONDC) initiative was established by the Department for Promotion of Industry and Internal Trade (DPIIT) of Government of India to develop open e-commerce. It was incorporated on 31 December 2022.[49]

As it grows, it could influence digital commerce on a global scale by promoting cross-border trade and accelerating and democratising digital commerce across markets. However, there is room for ONDC to transform digital commerce beyond India's borders, through four key enablers in supporting international digital commerce, including seamless cross-border e-payment settlements and global cooperation.

Japan

Cutting-edge logistics technologies in Japan provide strong support for cross-border electronic trade. In addition to advanced information technology and other infrastructure in the early stages, Japan also relies on its effective management of cross-border logistics, and its efficient logistics information systems provide strong support for digital trade inside and outside of Japan. Logistics costs in Japan only occupied 5.38% of its sales volume in 2020.[50]

At present, Japan has great ascendancy in advancing green digital trade as its carbon dioxide emissions per unit of GDP are only 0.18kg, much lower than that of other RCEP member states. Meanwhile, Japan formulates and responds to environmental protection standards in trade based on strict principles and takes part in the signing of

48. Australia DFAT website, Digital Trade Strategy (April 2022), https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade/digital-trade-strategy
49. Indian Council on Global Relations Resilience and Inclusivity in Cross-Border Digital Supply Chains through Digital Services Trade and Investment, https://www.gatewayhouse.in/resilience-and-inclusivity-in-cross-border-digital-supply-chains-through-digital-services-trade-and-investment/#_ftnref4
50. Deloitte report on "Technology-empowered Digital Trade in Asia Pacific" https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/deloitte-launches-technology-empowered-digital-trade-in-asia-pacific-report-summary.html
51. MDEC Malaysia website https://mdec.my/malaysiadigital
52. Alpha beta publication, The Economic Opportunities of Digital Transformation and Google's Contribution (Oct 2021) https://accesspartnership.com/wp-content/uploads/2023/03/Malaysia-Digital-Transformation.pdf
53. MTI Singapore website on Digital Economy Agreements, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements

multiple environmental protection agreements so as to actively boost the green economy in regional trade digitalization.

Malaysia

Since its establishment in 1996, Malaysia Digital Economy Corporation (MDEC) and Malaysia Digital have driven digital transformation and adoption across the public and private sectors in Malaysia. Initiatives include the Malaysia Digital Status, where MDEC will award Malaysia Digital Status to eligible companies to participate and undertake any of Malaysia Digital's activities[51]; and working with Google to facilitate trade digitalization through public-private partnerships.[52]

Singapore

The Singaporean government actively promotes global digital trade. Singapore established rules on digital trade and economic cooperation on digital trade with multiple countries with the release of the Digital Economy Agreement (DEA) as it seeks to establish a digital trade framework in Asia and even the whole world. The digital trade cooperation framework built on the DEA enables Singaporean companies to connect with their overseas partners in digital trade more seamlessly, thus ultimately cutting down operational cost, increasing business processing efficiency, and making it easier for them to get access to overseas markets. At the same time, Singapore gives top priority to six aspects in the development of the DEA, namely artificial intelligence, Cross-Border Privacy Rules (CBPRs) of APEC, data innovation, Data Protection Trustmark (DPTM) certification, national electronic invoicing network, and digital transformation of SMEs, as a way to actively push forward the transformation of domestic companies. Currently, Singapore has signed relevant digital trade deals with many countries, including Chile, New Zealand, Australia, South Korea and the UK.[53]

TradeTrust was developed by Singapore's Infocomm Media Development Authority to provide a comprehensive digital solution to deal with key documents in international trade. It is a framework that comprises globally accepted standards connecting governments and businesses to a public blockchain. This enables trusted interoperability of electronic trade documents across digital platforms. Thus, TradeTrust is offered as a digital utility, with capability in tracing the source of digitally issued documents and verifying their integrity independently. Examples of use cases include validating the authenticity and provenance of government-issued documents, title transfers of electronic Billing of Lading and more.

South Korea

South Korea takes a leading position in digitalization among RCEP member states with the highest internet penetration rate (96.16%) in the region. Efficient and sophisticated digital infrastructure in South Korea can be mainly attributed to the support of the government for digitalization construction. The South Korean government has taken the lead in the transformation of digital government, and upgrades in the construction of a superior network has been a national strategy. It remains devoted to a ten-year national broadband construction from 1995, making use of powerful digital technologies to build e-government platforms for the public, and publicizing the practices to the whole country. The sophisticated infrastructure has provided excellent conditions for the development of digitalization of cross-border trade in South Korea.[50]

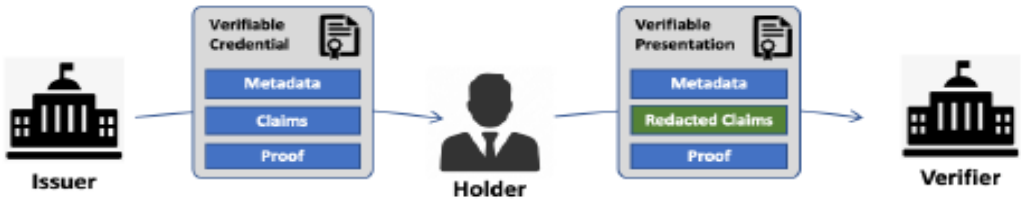
48. Australia DFAT website, Digital Trade Strategy (April 2022), https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade/digital-trade-strategy
49. Indian Council on Global Relations Resilience and Inclusivity in Cross-Border Digital Supply Chains through Digital Services Trade and Investment, https://www.gatewayhouse.in/resilience-and-inclusivity-in-cross-border-digital-supply-chains-through-digital-services-trade-and-investment/#_ftnref4
50. Deloitte report on "Technology-empowered Digital Trade in Asia Pacific" https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/deloitte-launches-technology-empowered-digital-trade-in-asia-pacific-report-summary.html
51. MDEC Malaysia website https://mdec.my/malaysiadigital
52. Alpha beta publication, The Economic Opportunities of Digital Transformation and Google's Contribution (Oct 2021) https://accesspartnership.com/wp-content/uploads/2023/03/Malaysia-Digital-Transformation.pdf
53. MTI Singapore website on Digital Economy Agreements, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements

Appendix 3

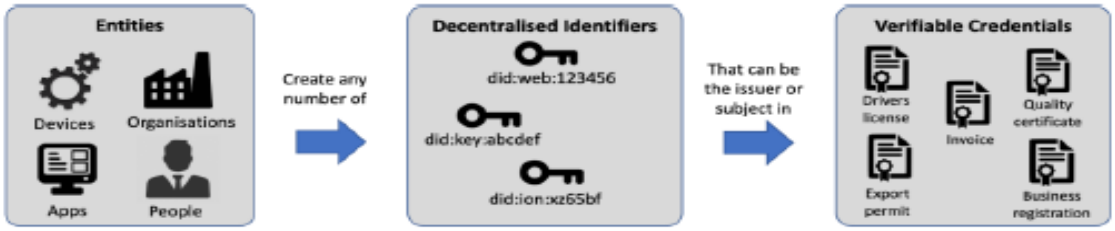
Estimated status of National IdM Strategy development and implementation

Stage	Development	Implementation
Not started or planning stage	Japan	Canada, Chile, Japan, United States
Early stage	United States, Chile, Slovenia	Germany, Australia, Luxembourg, New Zealand, Slovenia, Turkey
Ongoing	Canada, Luxembourg, Turkey	Austria, Denmark, Italy, Korea, Netherlands, Portugal, Spain, Sweden
Final stage	Australia, Germany	
Fully developed	Austria, Denmark, Italy, Korea, Netherlands, New Zealand, Portugal, Spain, Sweden	

Appendix 4



Verifiable Credentials



Decentralised Identifiers

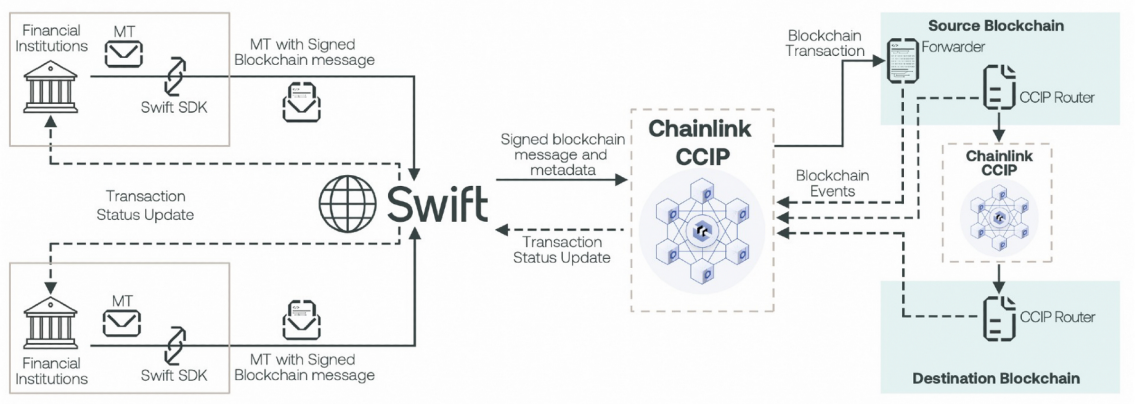
Source: https://www.tradetrust.io/static/uploads/white-paper-verifiable-credentials-CBT.pdf

Appendix 5

Case Study: Secure Blockchain Interoperability for Cross-Chain Interactions

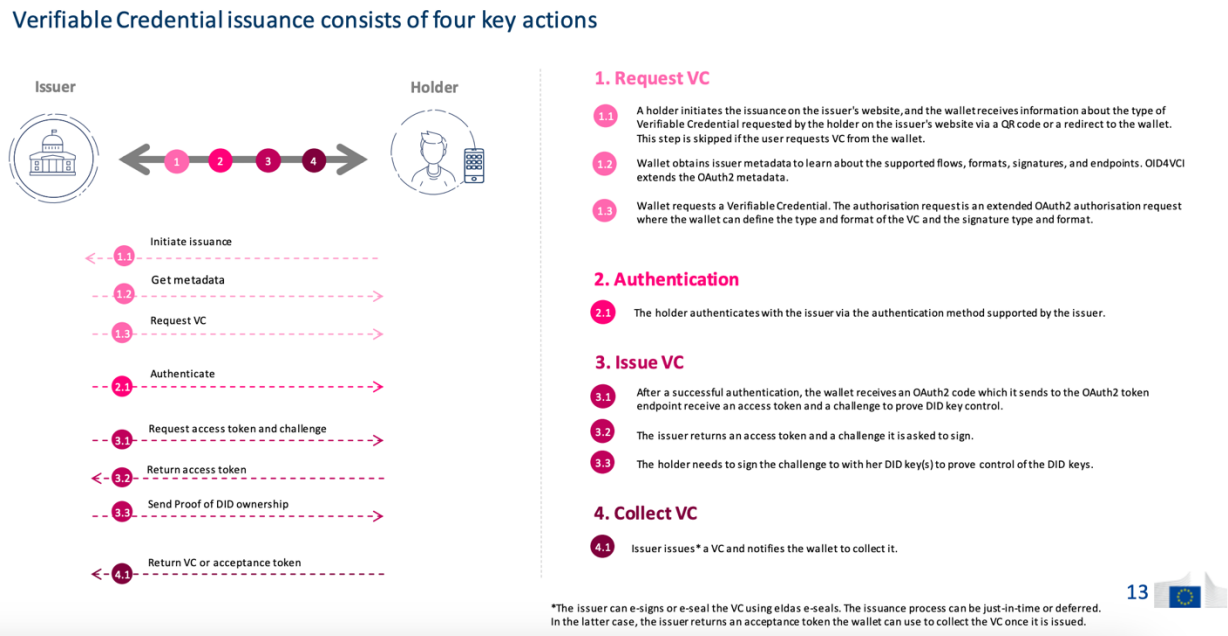
Secure cross-chain interoperability is key to orchestrating and verifying digital assets and credentials across existing infrastructure and blockchain networks. A recent blockchain interoperability collaboration between Swift and more than a dozen financial institutions and market infrastructures—including the Depository Trust & Clearing Corporation (DTCC), BNY Mellon, Citi, Euroclear, Clearstream, Australia and New Zealand Banking Group Limited (ANZ), BNP Paribas, Lloyds Banking Group, and SIX Digital Exchange (SDX)—demonstrated how firms can leverage their existing Swift infrastructure in combination with Chainlink to efficiently send data and instructions over a range of public and private blockchain networks.

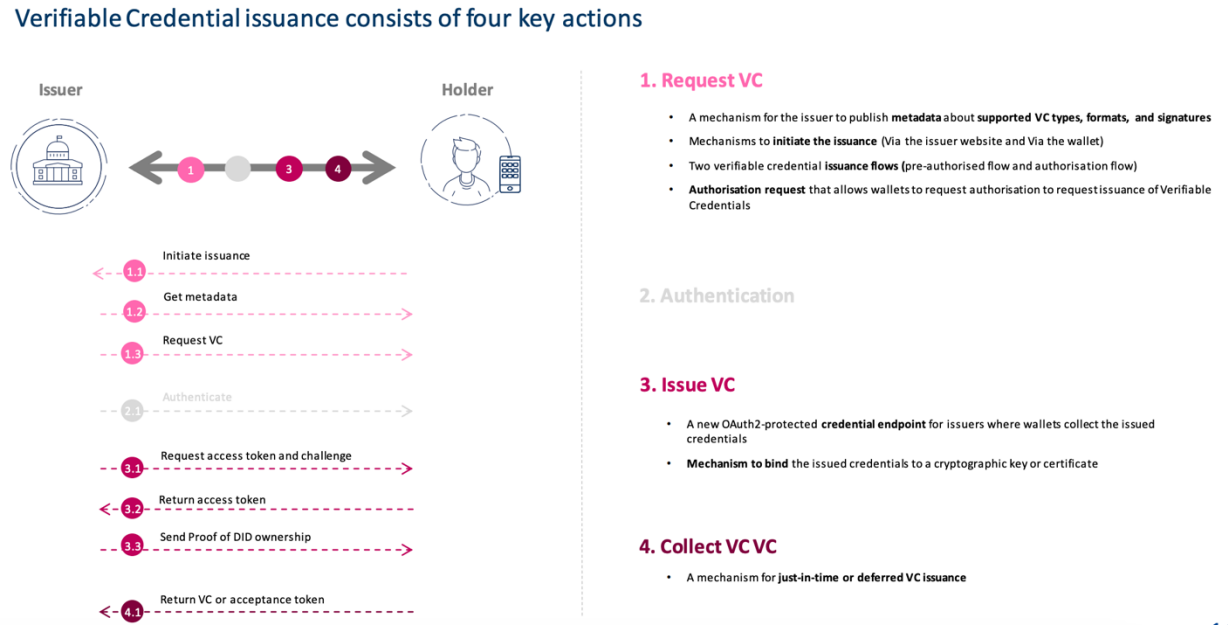
The Chainlink Cross-Chain Interoperability Protocol (CCIP) provided Swift with connectivity to and interoperability across public and private blockchains. CCIP is an open blockchain interoperability standard that utilizes a series of decentralized networks to facilitate data and token transfers across any blockchain, as well as provide existing systems with an abstraction layer to communicate across blockchains from a single interface.



Reference: https://www.swift.com/news-events/news/successful-blockchain-experiments-unlock-potential-tokenisation

Appendix 6 – How a verifiable credential (VCs) works with decentralized identifiers (DIDs)?

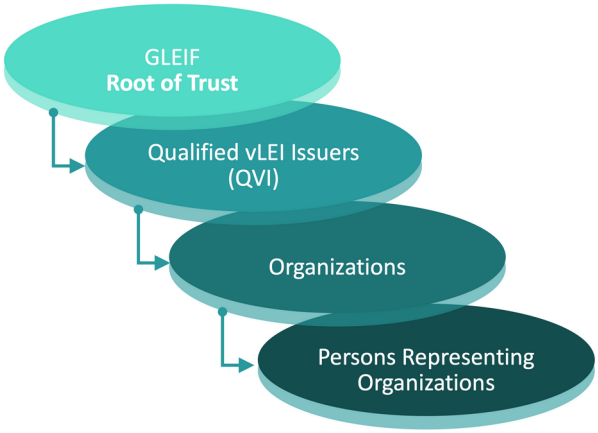




Source: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/600343491/Chapter%206%20-%20Open%20ID%20Connect.pdf?api=v2

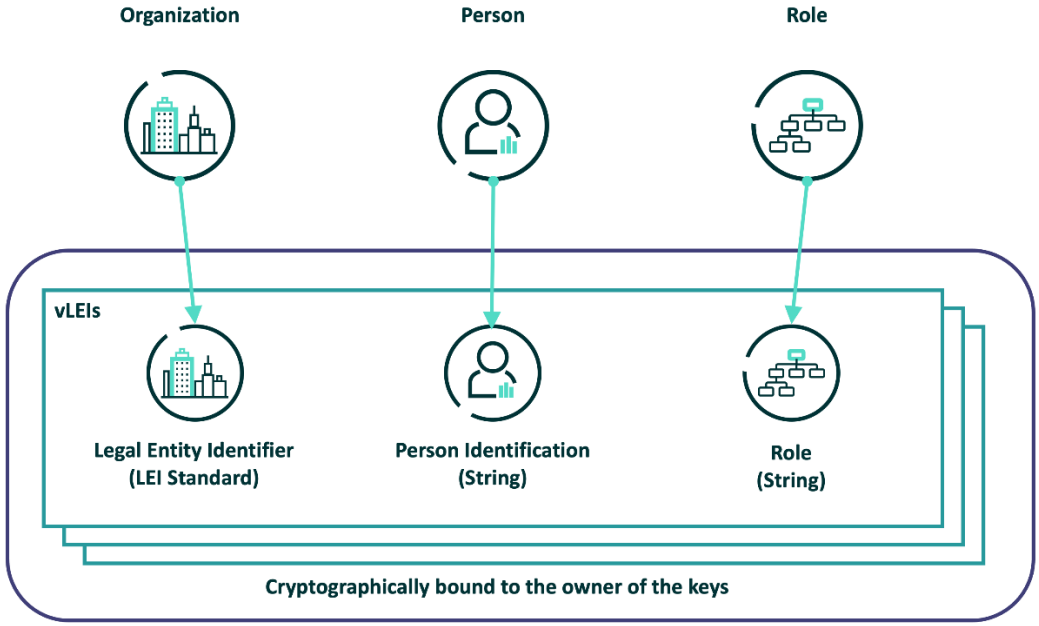
Appendix 7

The LEI as a VC – the vLEI Trust Chain



- GLEIF is the **Root of Trust**.
- Root **AID** (Autonomic Identifier) to establish the Root of Trust.
- Delegated **AID**s to issue vLEIs to its trusted network of Qualified **vLEI** Issuers (**QVIs**).
- **QVI**s are qualified to issue Entity and Role vLEI Credentials.
- Once a vLEI is issued to an Organization, vLEIs can be issued to Persons who represent Organizations either in official or functional roles.

By combining three concepts – the Organization's identity, represented by the LEI, a person's identity and the role that the person plays for the Organization, vLEI credentials can be issued.



Embedding the LEI in digital tools - Representing Organizations, Persons and Roles

vLEI Role Credentials issued to Persons whose **Official Organizational Roles** (ISO 5009 standard) that can be verified both by the organization as well as against one or more public sources, or through official documents obtained from the organization such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person. vLEI Role Credential issued by Legal Entities to Persons **in the context of the engagement** of those Persons with an organization which can be verified by the organization. Example:

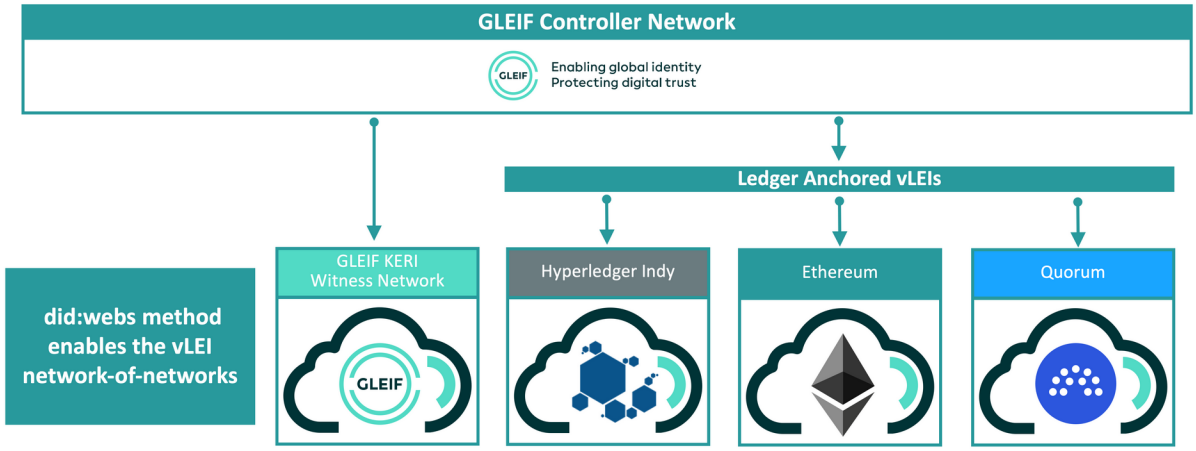
vLEI Role Credentials issued by an organization to its authorized suppliers:

- Requirements for use defined by the organization
- Could require authorized suppliers to submit invoices signed with their vLEI Role Credentials to eliminate presentation of fraudulent invoices

Chaining of the vLEI Credentials in the vLEI Trust Chain using ACDC credentials allows for the provenance of vLEIs to be traced back to GLEIF as both the Root of Trust for the vLEI Trust Chain as well as to the entity that ensures the operational integrity of the Global LEI System.

In December 2020, GLEIF announced its plans to create a fully digitized LEI service capable of enabling instant and automated identity verification between counterparties operating across all industry sectors, globally. Additionally, in December 2022, GLEIF announced the first suite of vLEI services to enable digital signing and automated verification of corporate caller IDs through proof-of-concept (POC) trials to be carried out by the first qualified vLEI issuer, delivering on GLEIF's plans to create a fully digitized LEI service capable of enabling instant and automated identity verification between counterparties operating across all industry sectors, globally.

The vLEI infrastructure is a network-of-networks of true universality and portability, developed using the KERI (Key Event Receipt Infrastructure) protocol. It supports the full range of blockchain, self-sovereign identity and other decentralized key management platforms. vLEIs will be hostable on both ledgers and cloud infrastructure supporting both the decentralization of ledgers plus the control and performance of cloud. Portability will enable GLEIF's vLEI ecosystem to unify all ledger-based ecosystems that support the vLEI.



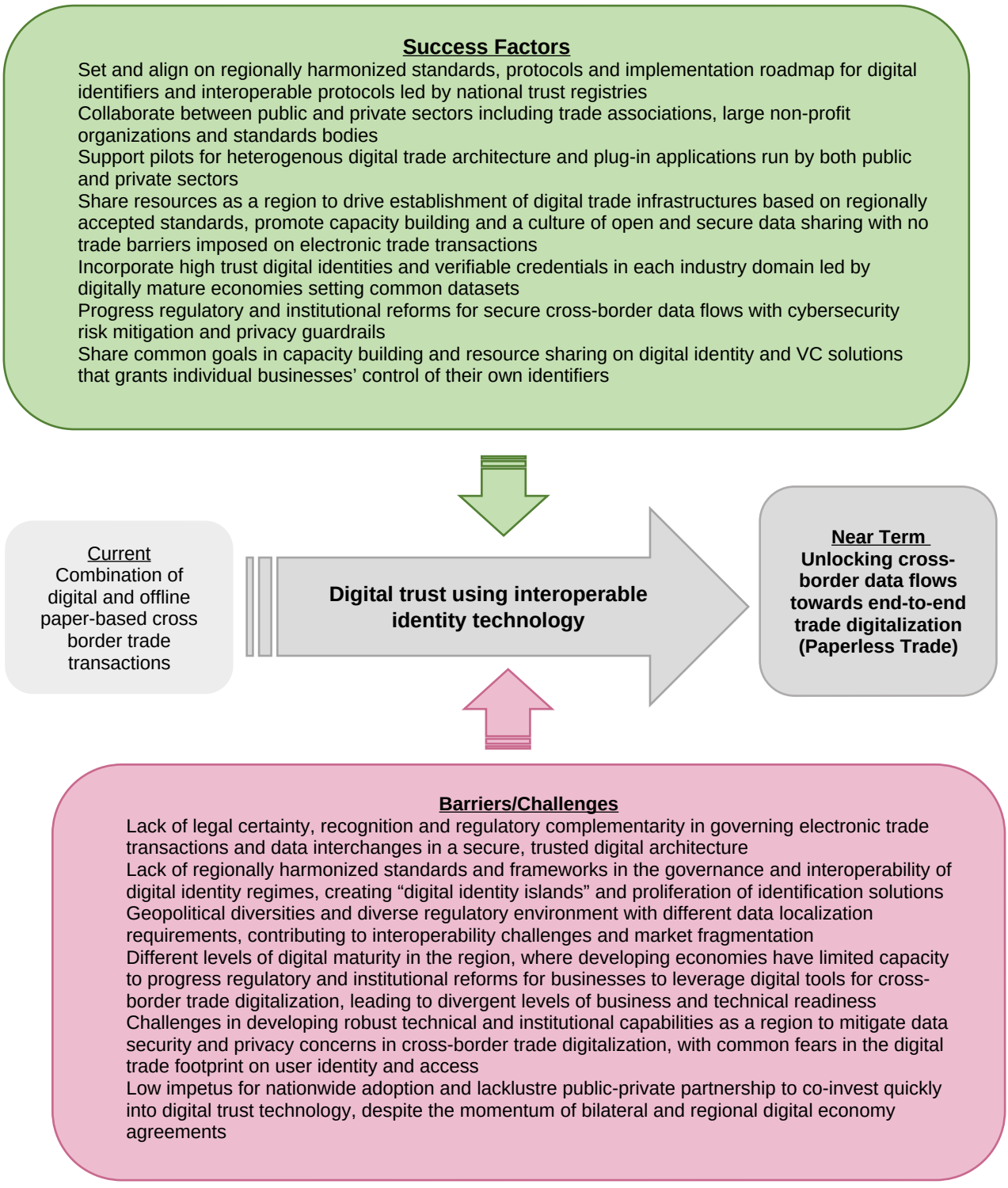
Network-of-networks True Interoperability, Portability and Scalability

vLEI network-of-networks based on KERI

Development of the capabilities needed for issuance, verification and revocation of vLEIs do not need to operate on blockchain or distributed ledger technology.

This would allow GLEIF to **connect to any blockchain or distributed ledger technology SSI network or cloud infrastructure** without the need for custom implementation, cost and overhead of operation.

Appendix 8


Success Factors
Set and align on regionally harmonized standards, protocols and implementation roadmap for digital identifiers and interoperable protocols led by national trust registries
Collaborate between public and private sectors including trade associations, large non-profit organizations and standards bodies
Support pilots for heterogenous digital trade architecture and plug-in applications run by both public and private sectors
Share resources as a region to drive establishment of digital trade infrastructures based on regionally accepted standards, promote capacity building and a culture of open and secure data sharing with no trade barriers imposed on electronic trade transactions
Incorporate high trust digital identities and verifiable credentials in each industry domain led by digitally mature economies setting common datasets
Progress regulatory and institutional reforms for secure cross-border data flows with cybersecurity risk mitigation and privacy guardrails
Share common goals in capacity building and resource sharing on digital identity and VC solutions that grants individual businesses' control of their own identifiers
Current
Combination of digital and offline paper-based cross border trade transactions
Digital trust using interoperable identity technology
Near Term
Unlocking cross-border data flows towards end-to-end trade digitalization (Paperless Trade)
Barriers/Challenges
Lack of legal certainty, recognition and regulatory complementarity in governing electronic trade transactions and data interchanges in a secure, trusted digital architecture
Lack of regionally harmonized standards and frameworks in the governance and interoperability of digital identity regimes, creating "digital identity islands" and proliferation of identification solutions
Geopolitical diversities and diverse regulatory environment with different data localization requirements, contributing to interoperability challenges and market fragmentation
Different levels of digital maturity in the region, where developing economies have limited capacity to progress regulatory and institutional reforms for businesses to leverage digital tools for cross-border trade digitalization, leading to divergent levels of business and technical readiness
Challenges in developing robust technical and institutional capabilities as a region to mitigate data security and privacy concerns in cross-border trade digitalization, with common fears in the digital trade footprint on user identity and access
Low impetus for nationwide adoption and lacklustre public-private partnership to co-invest quickly into digital trust technology, despite the momentum of bilateral and regional digital economy agreements

References

1. ICC, UK Report on G7 | Creating a Modern Digital Trade Ecosystem https://7703b98d-a40e-40b5-9a19-2340c0e85ea4.filesusr.com/ugd/0b6be5_c8f1719de362441f8277fcdf49240d86.pdf?index=true x
2. World Trade Statistical Review 2022 https://www.wto.org/english/res_e/publications_e/wtsr_2022_e.htm
3. ADB Working Paper Series on Regional Economic Integration No. 137 https://www.adb.org/sites/default/files/publication/152775/reiwp-137.pdf
4. World Economic Forum, The Digital Economy on Digital Trust website article: https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/
5. ICC Digital Standards Initiative Trust in Trade Report, 2023 https://www.dsi.iccwbo.org/_files/ugd/8e49a6_5a75a77950d7474da772bf9cfc2d985b.pdf
6. McKinsey Global Institute (2019), Digital Identification: A key to inclusive growth.
7. Achieving Harmonization of a Biometric ID Management Framework across APEC Economies: Global Benchmarking Study https://www.apec.org/publications/2023/03/achieving-harmonization-of-a-biometric-id-management-framework-across-apec-economies-global-benchmarking-study
8. United Nations Working Group IV: Electronic Commerce https://uncitral.un.org/en/working_groups/4/electronic_commerce
9. WEF White Paper Inclusive Deployment of Blockchain for Supply Chains Part 2 https://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf
10. 2022 APEC Ministerial Meeting https://www.apec.org/meeting-papers/annual-ministerial-meetings/2022/2022-apec-ministerial-meeting
11. Statement of the Chair-Ministers Responsible for Trade Meeting 2023 http://mddb.apec.org/Documents/2023/MM/MRT/23_mrt_jms.pdf#:~:text=We%20will%20strengthen%20physical%2C%20institutional%20and%20people-to-people%20connectivity,area%20connectivity%20through%20quality%20infrastructure%20development%20and%20investment
12. United Nations, Economic and Social Commission for Asia and the Pacific (ESCAP) (2017). Digital Trade Facilitation in Asia and the Pacific. Studies in Trade, Investment and Innovation. Sales No. E.18.II.F.10; Organisation for Economic Co-operation and Development (OECD) (2017). Digital trade. The impact of digitalisation on trade. Available at www.oecd.org/trade/topics/digital-trade/.
13. Economic Impact of Adopting Digital Trade Rules: Evidence from APEC Member Economies https://www.apec.org/publications/2023/04/economic-impact-of-adopting-digital-trade-rules-evidence-from-apec-member-economies
14. Matthias Bauer et al. (2014), The costs of data localization: Friendly fire on economic recovery, European Centre for International Political Economy (ECIPE). Available at: https://www.aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf
15. World Trade Report 2015 Speeding up Trade: Benefits and Challenges of Implementing the WTO Trade Facilitation Agreement. https://www.wto.org/english/res_e/publications_e/wtr15_e.htm.
16. APEC's Cross-border privacy rules system: A house of cards? by Graham Greenleaf, UNSW Australia http://classic.austlii.edu.au/au/journals/UNSWLRS/2014/42.pdf
17. ESCAP-OECD Asia-Pacific Digital Trade Regulatory Review 2022 https://repository.unescap.org/bitstream/handle/20.500.12870/4570/ESCAP-2022-RP-Asia-Pacific-digital-trade-regulatory-review.pdf?sequence=1&isAllowed=y
18. Deloitte report on "Technology-empowered Digital Trade in Asia Pacific" https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/deloitte-launches-technology-empowered-digital-trade-in-asia-pacific-report-summary.html
19. ESCAP, Readiness assessment for cross-border paperless trade (2022). https://www.unescap.org/our-work/trade-investment-innovation/trade-facilitation-digital-trade/paperless-trade
20. UNCDF: The role of cross-border data flows in the digital economy (June 2022) https://policyaccelerator.uncdf.org/s/EN-UNCDF-Brief-Cross-Border-Data-Flows-2022
21. ICC Standards Toolkit for cross-border paperless trade https://iccwbo.org/news-publications/policies-reports/standards-toolkit-for-cross-border-paperless-trade/
22. ADB, ICC publication on Digitalizing Trade in Asia needs Legislative Reform https://www.adb.org/sites/default/files/publication/704041/digitalizing-trade-asia-legislative-reform.pdf
23. Digital Identity in APEC: Deepening Trust, Inclusion and Interoperability in the Digital Economy https://www2.abaconline.org/assets/2022/Publications/Digital%20Identity%20Report.pdf
24. ASEAN framework on digital data governance https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf
25. UNDP Enabling cross-border data flow: ASEAN and beyond. https://www.undp.org/publications/enabling-cross-border-data-flow-asean-and-beyond
26. Data beyond Borders 3.0 https://www.salesforce.com/news/stories/data-beyond-borders-2023-report/

27. World Integrated Trade Solution statistics on East Asia and Pacific top 5 export and import partners https://wits.worldbank.org/CountrySnapshot/en/EAS
28. PWC Findings from the 2023 Global Digital Trust Insights https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
29. UNESCAP Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies https://collections.unu.edu/view/UNU:7760
30. Chapter 1 The impact of digital technologies on developing countries trade (Eddy Bekkers, Robert Koopman, Giulia Sabbadini and Robert Teh) https://www.wto.org/english/res_e/booksp_e/05_adtera_chapter_01_e.pdf
31. Information Technology & Innovation Foundation "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/
32. UNECE White Paper eDATA VCs for Cross Border Trade (September 2022).
33. MTI Singapore Factsheet on Frameworks on Cooperation in Digital Economy and Green Economy between Singapore and Malaysia https://www.mti.gov.sg/Newsroom/Press-Releases/2023/01/Factsheet-on-Frameworks-on-Cooperation-in-Digital-Economy-and-Green-Economy
34. OECD report on digital identity management https://www.oecd.org/sti/ieconomy/49338380.pdf
35. IGI Global, Identity Assurance in Open Networks https://www.igi-global.com/chapter/identity-assurance-open-networks/63082
36. UN/CEFACT White Paper eDATA Verifiable Credentials for Cross Border Trade https://www.tradetrust.io/static/uploads/white-paper-verifiable-credentials-CBT.pdf
37. Decentralized Identity Foundation https://identity.foundation/
38. Open Attestation Platform https://www.openattestation.com/
39. GovTech Singapore website (9 June 2022) https://www.tech.gov.sg/media/technews/govtech-partners-the-digital-agency-of-japan-to-push-digital-government-transformation
40. Kyodo news article: Singapore, Japan agree to cooperate in digitalization (24 June 2023) https://english.kyodonews.net/news/2023/06/edec18d271e2-singapore-japan-agree-to-cooperate-in-digitalization.html
41. PH-Singapore memorandum to advance digital cooperation: DICT https://www.pna.gov.ph/articles/1192927
42. MTI website on KSDPA, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA
43. New Zealand Foreign Affairs and Trade website on DEPA, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/#:~:text=The%20DEPA%20was%20signed%20in,basis%20of%20a%20draft%20framework
44. EC website, EU-Japan Summit: strengthening our partnership. https://digital-strategy.ec.europa.eu/en/news/eu-japan-summit-strengthening-our-partnership
45. MTI Singapore website on EU-Singapore Digital Partnership, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/EUSDP
46. MTI Press Release (30 Jan 2023), https://www.mti.gov.sg/Newsroom/Press-Releases/2023/01/Factsheet-on-Frameworks-on-Cooperation-in-Digital-Economy-and-Green-Economy
47. MTI Singapore website on KSDPA, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA
48. Australia DFAT website, Digital Trade Strategy (April 2022), https://www.dfat.gov.au/trade/services-and-digital-trade/e-commerce-and-digital-trade/digital-trade-strategy
49. Indian Council on Global Relations Resilience and Inclusivity in Cross-Border Digital Supply Chains through Digital Services Trade and Investment, https://www.gatewayhouse.in/resilience-and-inclusivity-in-cross-border-digital-supply-chains-through-digital-services-trade-and-investment/#_ftnref4
50. Deloitte report on "Technology-empowered Digital Trade in Asia Pacific" https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/deloitte-launches-technology-empowered-digital-trade-in-asia-pacific-report-summary.html
51. MDEC Malaysia website https://mdec.my/malaysiadigital
52. Alpha beta publication, The Economic Opportunities of Digital Transformation and Google's Contribution (Oct 2021) https://accesspartnership.com/wp-content/uploads/2023/03/Malaysia-Digital-Transformation.pdf
53. MTI Singapore website on Digital Economy Agreements, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements