

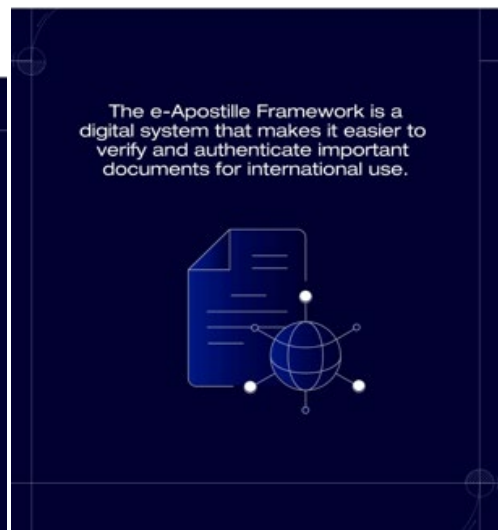
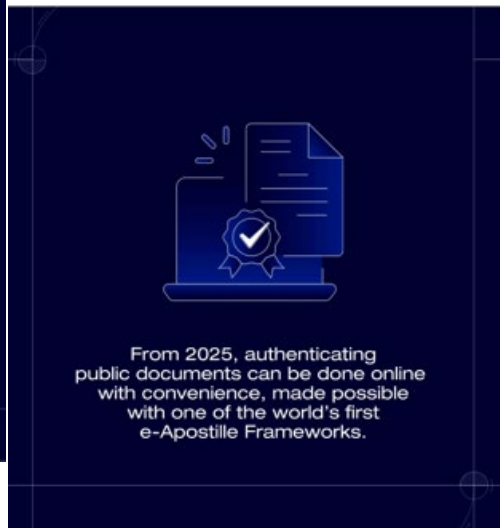


Singapore's E-Apostille Framework with Verifiable Credentials

Introduction to Singapore's e-Apostille Framework

Significance of Singapore E-Apostille Framework

- Singapore Academy of Law (**SAL**) and Infocomm Media Development Authority (**IMDA**) signed an MOU on 12 Sep 2024 to jointly develop an **open-source e-Apostille Framework** designed to digitalise the legalisation process of public and private documents.
- **One of the world's first** in the application of verifiable credential technology to the apostille process.
- The framework leverages on the **World Wide Web Consortium (W3C) Verifiable Credentials** standards to ensure globally interoperability, and further enhances the efficiency, security and reliability of document authentication.



W3C Verifiable Credentials 2.0: Data Model Standard

The **World Wide Web Consortium (W3C)** is the main international standards organisation for the World Wide Web.

For Verifiable Credentials, W3C has led the developments to establish a global standard. This standardization aims to facilitate the seamless creation, accessibility, and verification of credentials across various contexts and applications.

The **W3C Verifiable Credential Data Model 2.0** lays down the fundamental guideline governing two key aspects.

1. **Data Model:** How data should be structured and represented.
2. **Securing Mechanism:** How data should be signed and verified.

DATA MODEL

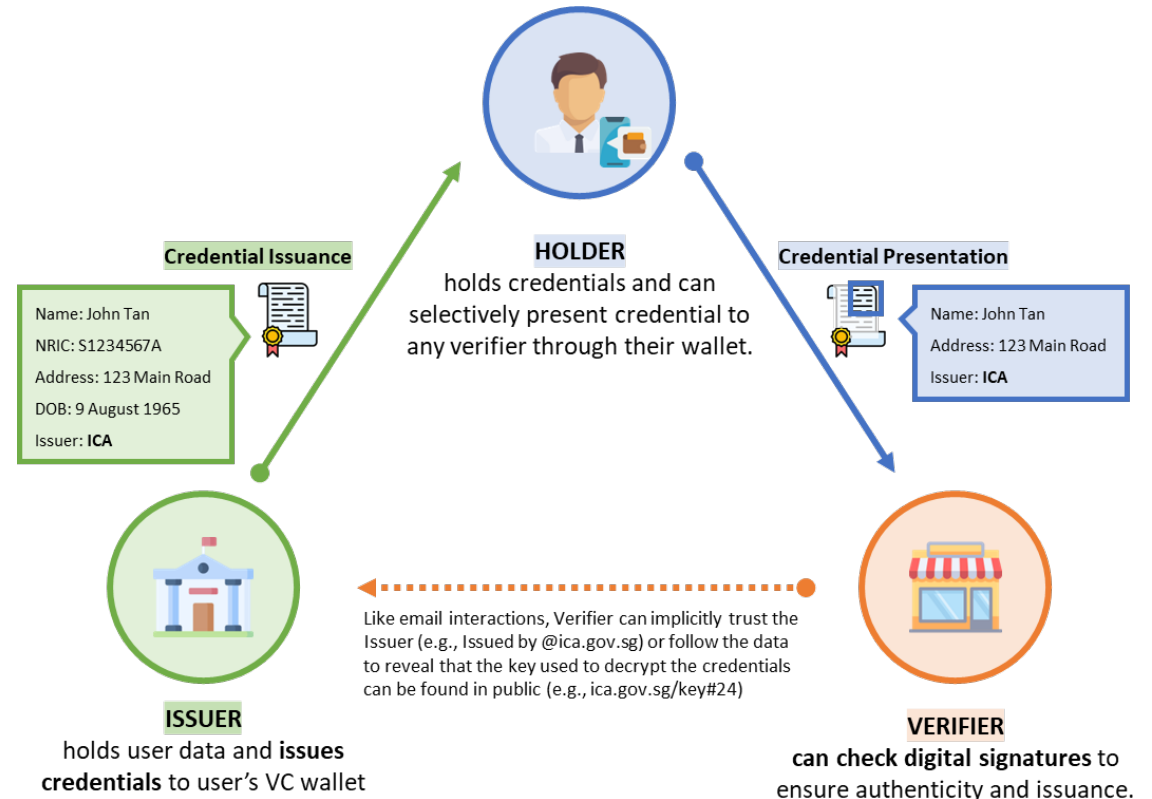
- W3C VC2.0 JSON Schema

SECURING MECHANISM

- BBS 2023
- ECDSA v1
- EdDSA v1
- JOSE & COSE

Source:
1. [W3C VC 2.0 Data Model](#)
2. [W3C VCWG Specifications](#)
3. [W3C VC 2.0 Securing Mechanism](#)

By establishing the standard for communicating VCs, a decentralised ecosystem can be developed where any **Verifier** can verify that the credentials presented by a **Holder** is legitimate, without being directly connected to the **Issuer**.



EU has passed legislations for the use and acceptance of EUDI wallet for VCs for both public and private sectors in all the EU member states.

Feb
2024

EUDI Wallet passed after receiving major support from ongoing Large-Scale Pilots across 250 public/private orgs, 25 Member States + Norway, Iceland & Ukraine.

EU Digital Identity (EUDI) Wallet to become law.

- Parliament gave its final green light (Feb 29th, 2024) to the regulation with 335 votes to 190, with 31 abstentions.
- EU Member States **must offer all citizens** an EUDI Wallet and Digital Identity Credential by **Q2 2026**.
- **Obligation for public sector and private sector businesses to accept EUDI Wallet and their credentials. (e.g., KYC, Age-Checks)**
- **Online platforms under the EU Digital Markets Act, must accept EUDI-Wallets for user authentication**, including social networks, search engines, and marketplaces with significant influence in EU.

Potential to tap onto this physical/digital infrastructure changes by EU to enable functionalities hard to obtain by SG market alone through our Digital Identity system. (e.g., Cross-Border Recognition, KYC for FB/YT, Age Check for Netflix/Restricted Goods)

Ongoing Large-Scale Pilots

<https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>



<https://www.dc4eu.eu/outputs/>
Timeline: Apr 2023 – Apr 2025

Lead: **Spain**

Consortium: 23 EU Members + Ukraine
Participants: 35 Public + 40 Private Org
Pilot Sector: **Education and Social Security**



<https://www.digital-identity-wallet.eu/>
Timeline: Aug 2022 - 2025

Lead: **Germany + France**

Consortium: 17 EU Members + Ukraine
Participants: 50 Public + 80 Private Org
Pilot Sector: **Gov Services, Bank Account, SIM, Driving License, eSignature, ePrescription**



<https://eudiwalletconsortium.org/>
Timeline: Early 2023 - 2025

Lead: **Sweden**

Consortium: 18 EU Members + Ukraine
Participants: 15 Public + 40 Private Org
Pilot: **Travel Credentials, Payments, Digital ID**



<https://www.nobidconsortium.com/>
Timeline: May 2023 - 2025

Lead: **Norway**

Consortium: 8 EU Members
Participants: 5 Public + 15 Private Org
Pilot: **Retail Payments**

<https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home>

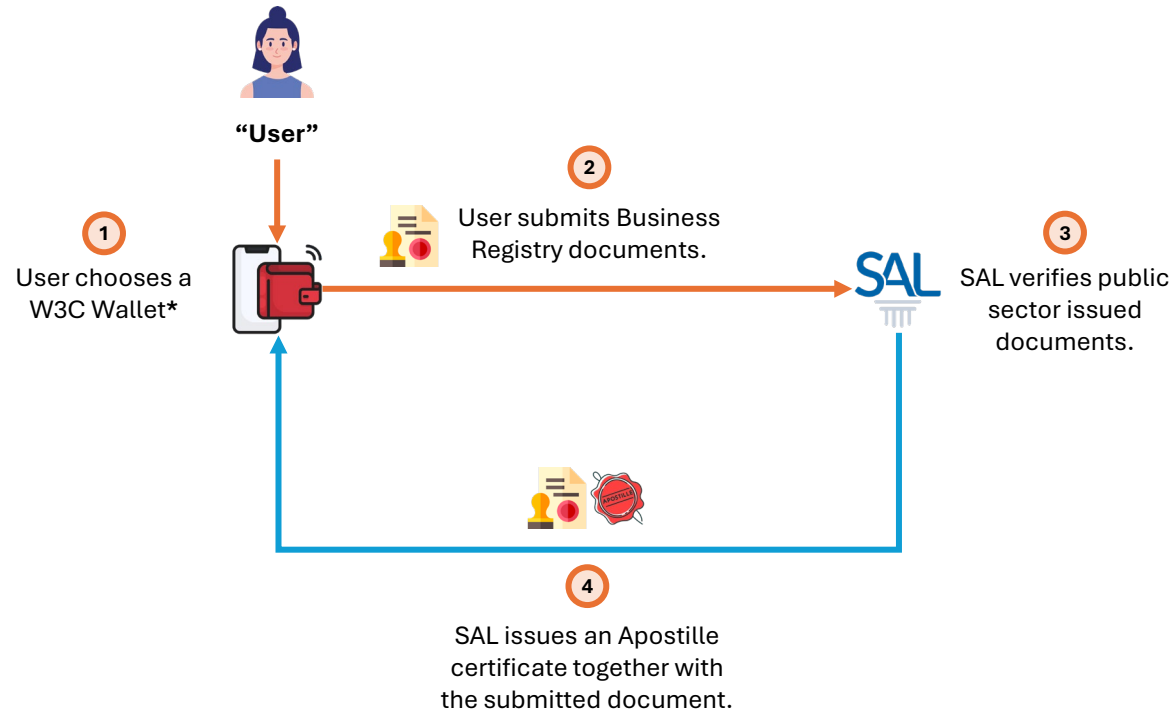
Key Features of e-Apostille Framework

- Built on top of **W3C VC**, enables an apostille to be issued in digital form which bears a digital signature with a digital certificate. Like a normal apostille, it authenticates the origin of a public document that will be used abroad.
- Verifiable credentials (VC) are **tamper-resistant digital credentials** that can be shared by the user with any party in a **decentralised** manner which enhances **scalability and interoperability**.
- Key Features include:
 - **Decentralised architecture** → Reduce concentration risk/ liability for Govt, increase user privacy/ control over data, more scalable
 - **Based on global standards** (e.g., W3C, ISO) → More interoperable
 - **Flexibility to onboard** public and private sector data → More utility for users
 - **Flexibility to selectively disclose** identity attributes → Increase user privacy/ control over data

Issuance and Utilization for e-Apostille Documents

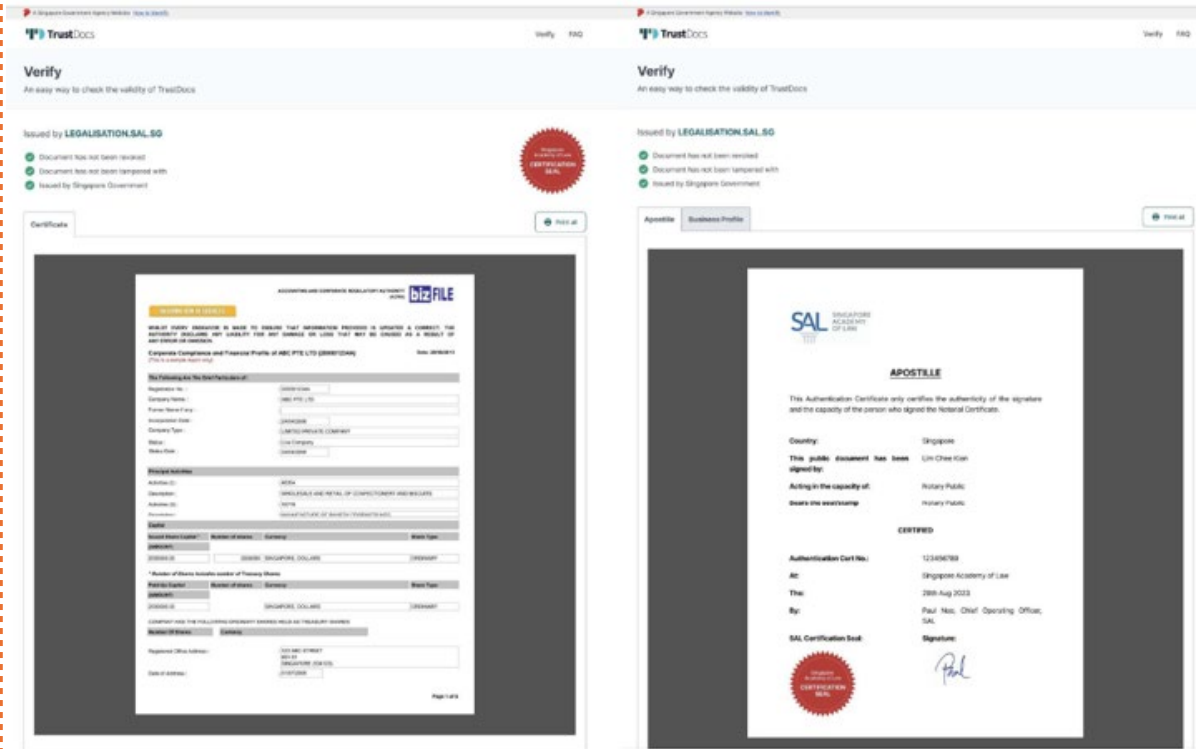
Issuance of e-Apostille Documents

Singapore Academy of Law (SAL), is the designated Competent Authority for apostillation of documents in SG. SAL will verify public sector-issued OA/W3C documents and affix an Apostille certificate for overseas use.



Utilising the e-Apostille Documents

Apostille simplifies legalisation and authentication of documents so they can be recognised internationally by 127 countries under the Hague Convention, providing an alternate route for overseas doc acceptance.

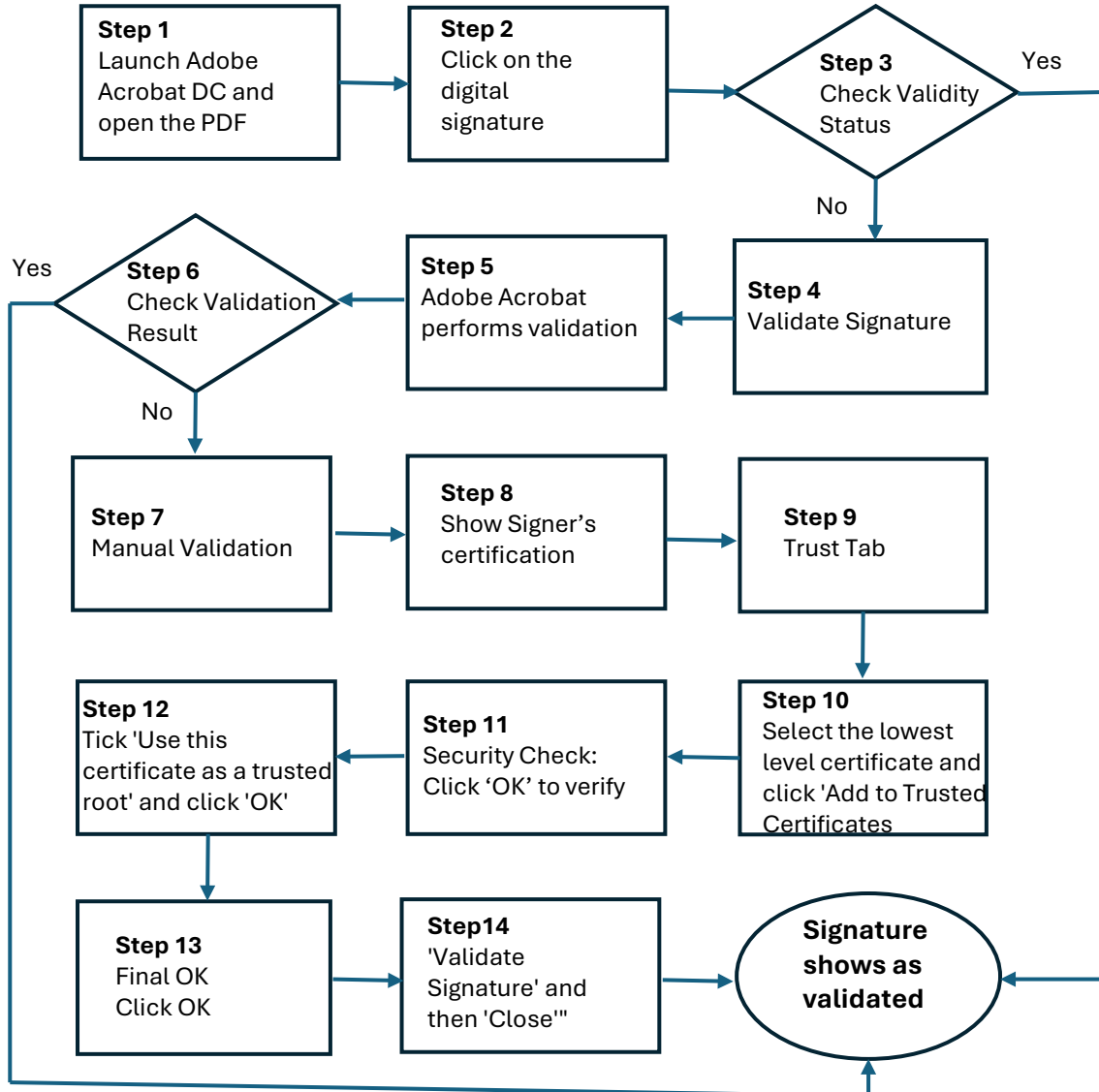


Background on Singapore's Apostille: <https://www.mlaw.gov.sg/news/press-releases/2021-01-19-singapore-accedes-to-the-apostille-convention/>

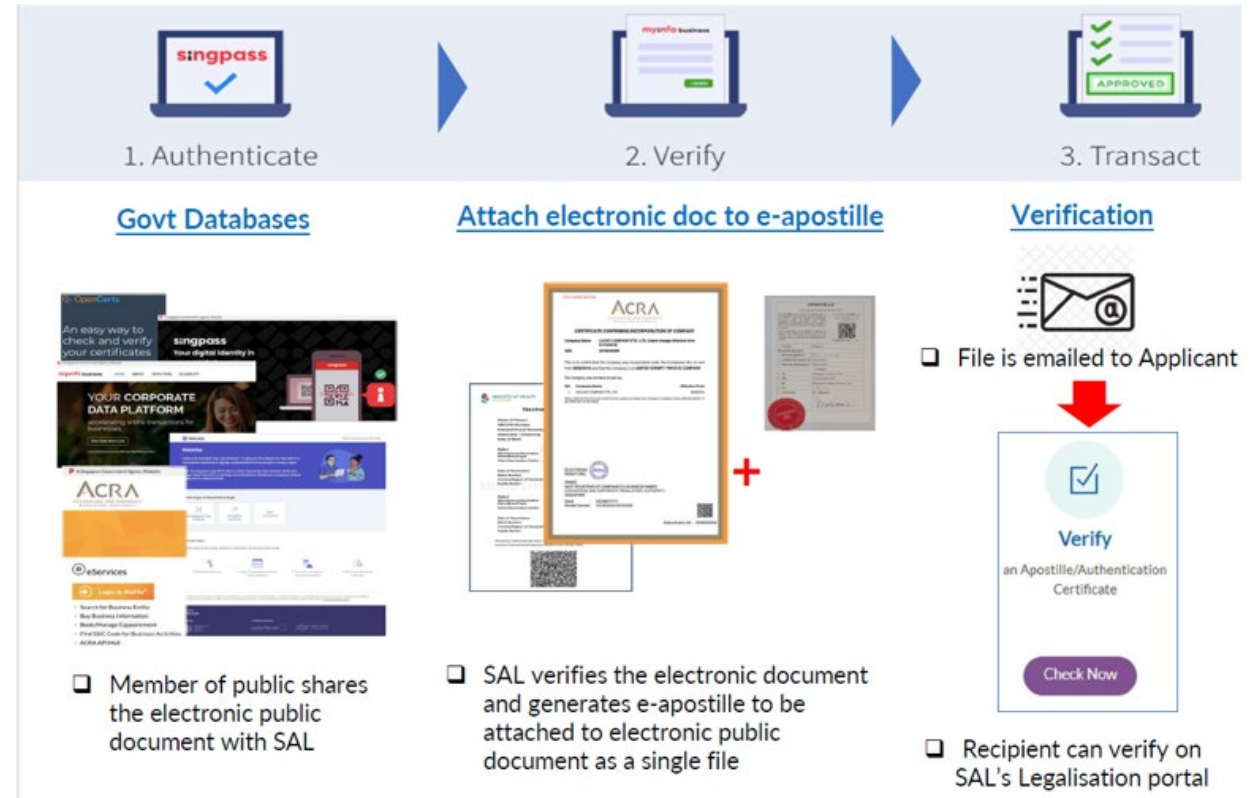
Comparing a Signed PDF vs a Verifiable Credential (VC) e-Apostille

Process for Verifying: a Signed PDF vs a Verifiable Credential (VC)

PDF with Digital Signatures



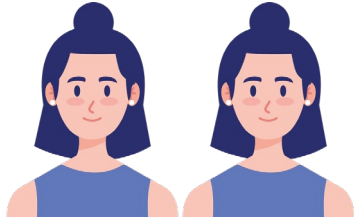
Verifiable Credential



Benefits of using the W3C e-Apostille Framework over traditional pdf format based Apostilles

Steps	Limitations of Paper and PDF	W3C Verifiable Credential
Automated and Real-time verification	<ul style="list-style-type: none"> Requires manual steps and specific software which can be time-consuming and prone to human error 	<ul style="list-style-type: none"> The document's integrity, validity and issuer identity can be easily authenticated with just a simple click on a provided link, or automatically in real-time by systems, reducing the need for manual intervention
Scalability for Large Scale Operations	<ul style="list-style-type: none"> Handling large volumes of digitally signed PDFs or paper can be cumbersome and resource intensive. 	<ul style="list-style-type: none"> Highly scalable, allowing for the efficient issuance and verification of thousands of documents
Decentralised Verification and Authentication	<ul style="list-style-type: none"> Centralised systems are often required to manage and verify digital signatures, which can be a single point of failure and target for attacks 	<ul style="list-style-type: none"> VC support decentralised authentication and verification, allowing individuals or companies to manage their verifiable documents in digital wallets.
Revokable	<ul style="list-style-type: none"> Issued paper or PDF documents cannot be revoked 	<ul style="list-style-type: none"> Issued paper or PDF documents cannot be revoked

Benefits of e-Apostille Framework with Verifiable Credential:



Individuals

- **Convenience:** No need to visit SAL's service counter.
- **Time-Saving:** Avoid long queues for document authentication.
- **Online Upload:** Submit documents via the SAL Legalisation Portal (www.legalisation.sal.sg).
- **Quick Delivery:** Receive digital Apostille certificate via email within minutes after verification and payment




Businesses

- Gain from a streamlined system that supports over 900 daily transactions, enhancing cross-border trade.
- Recipients can easily verify the following with a click on the link in the Apostille email or integrate into automated workflows:
 - **Document Integrity:** Check if the document content is unchanged.
 - **Issuance Status:** Verify the document's validity (not revoked).
 - **Issuance Identity:** Confirm the issuing party's identity.


For more information, please reach us at:

Thank You



INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

Ken-Wei Chng
Deputy Director, Digital Utilities
Programme Office



INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

Melinda Tan
Manager, Digital Utilities

