

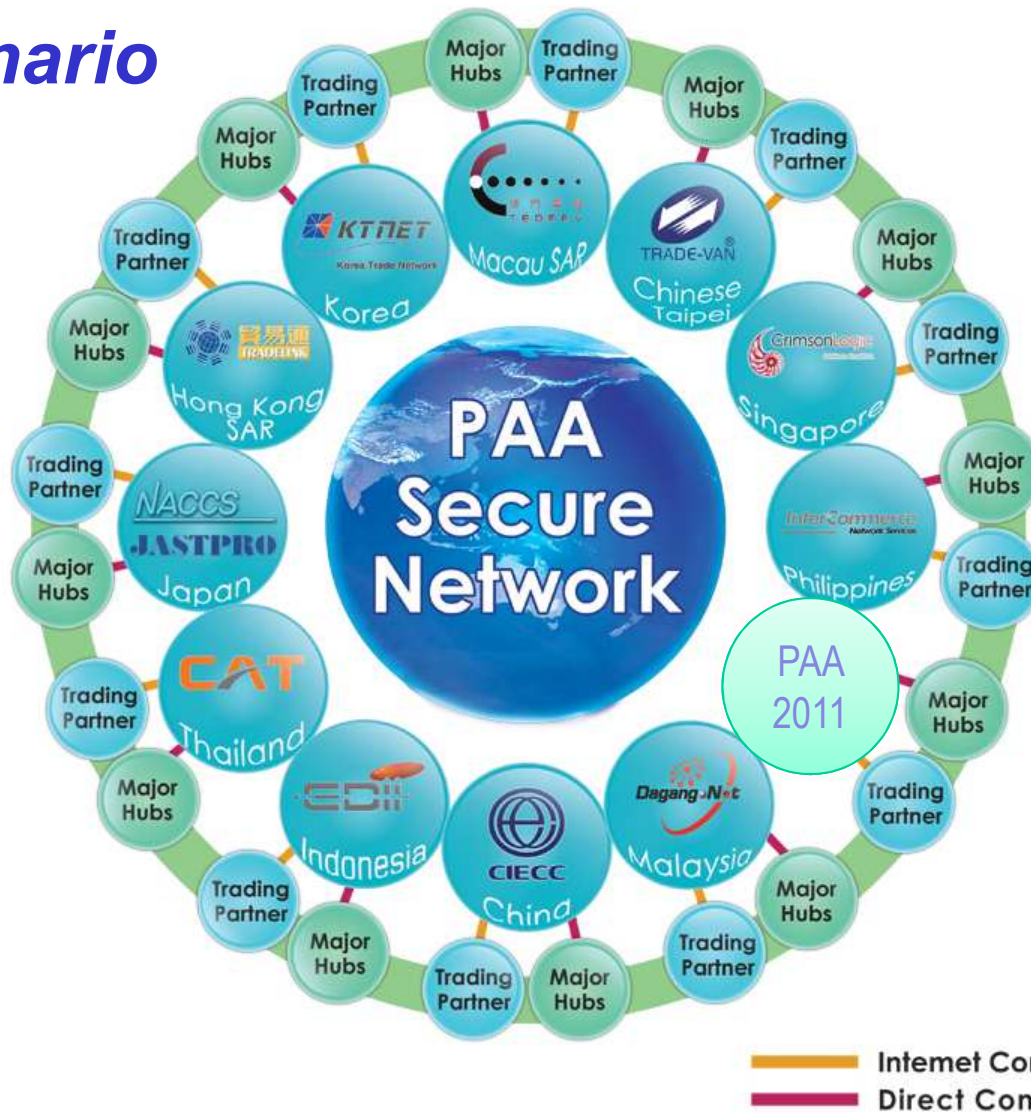


PAA & Global Paperless trade

Jay Kim
Korea Trade Network
Member of PAA
Oct, 2011 APTFF

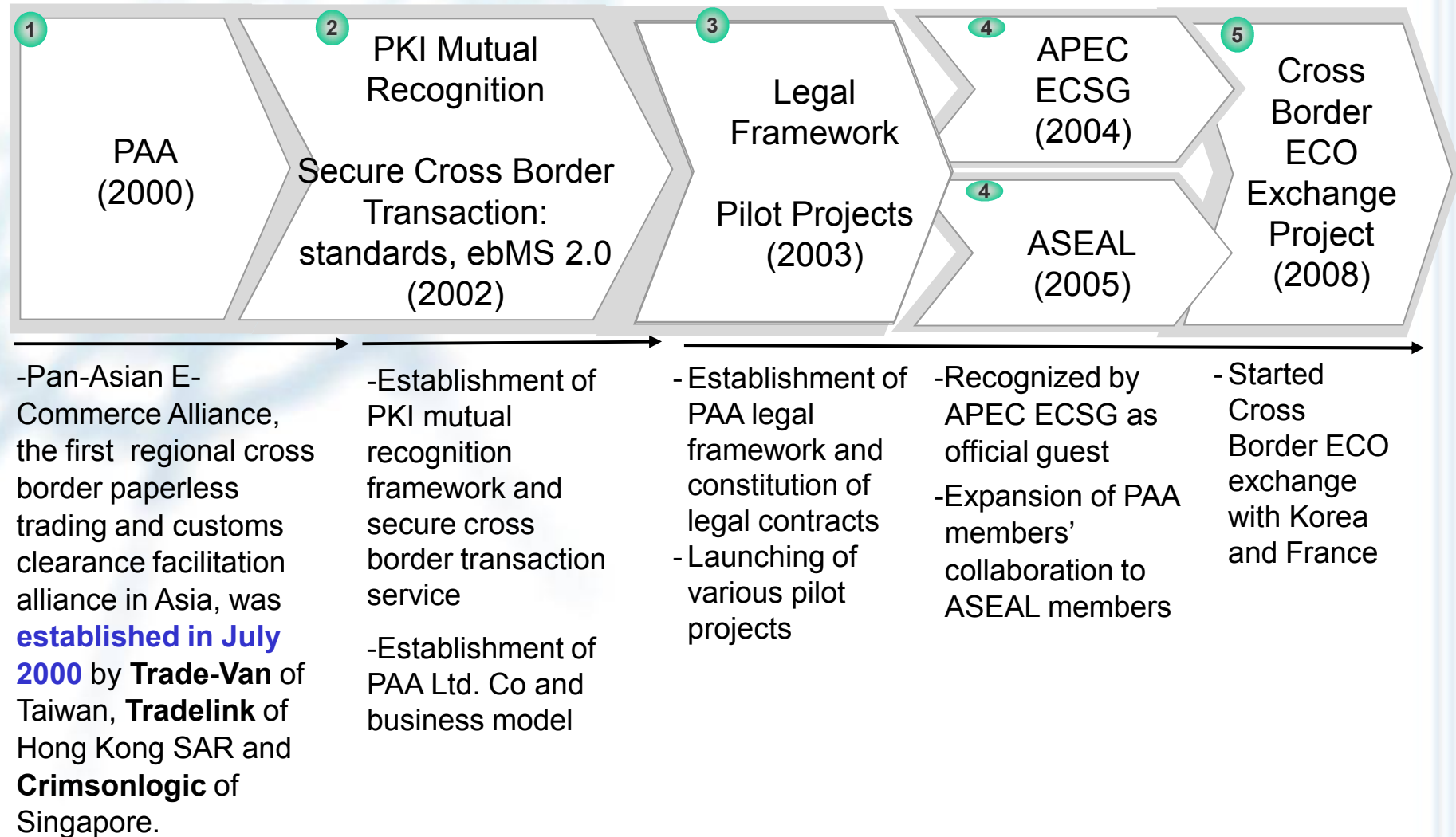
Single Window, Asian Connection

PAA Scenario



To promote and provide secure, trusted, reliable and value-adding IT infrastructure and facilities to enhance seamless trade globally

PAA Milestone



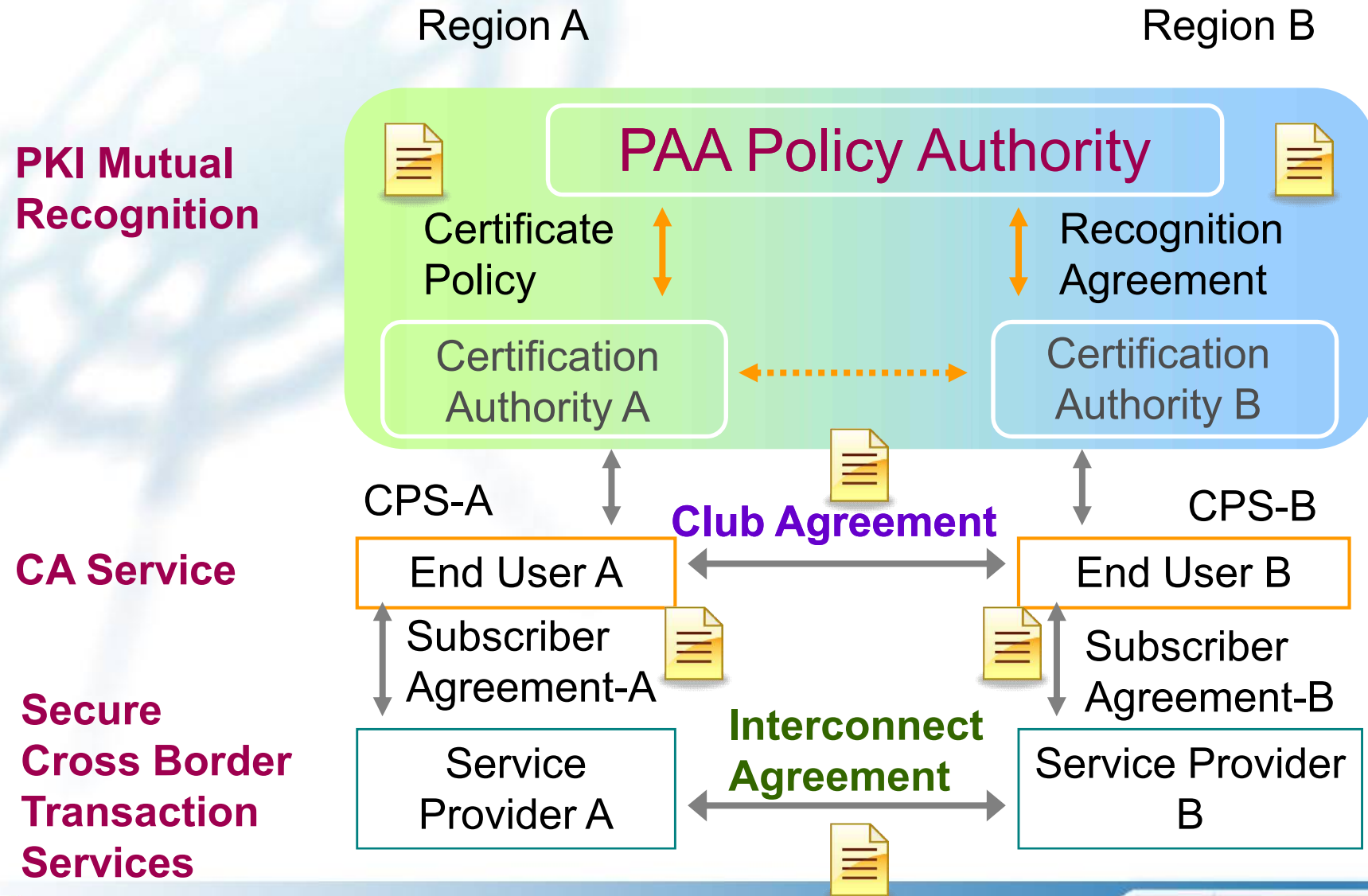
PAA's Achievements

- Has established robust legal framework which covers the liability of each parties, service level, dispute resolution process etc. for the exchange of digitally signed electronic documents
- Has developed PKI mutual recognition framework to support secure cross border transaction
- Has created message standards for both commercial and government related documents
- Has completed interconnectivity test among members using ebMS v2.0 messaging service handler
- Has created business model and charging scheme
- Has recruited users from different industries for various projects

PAA Projects

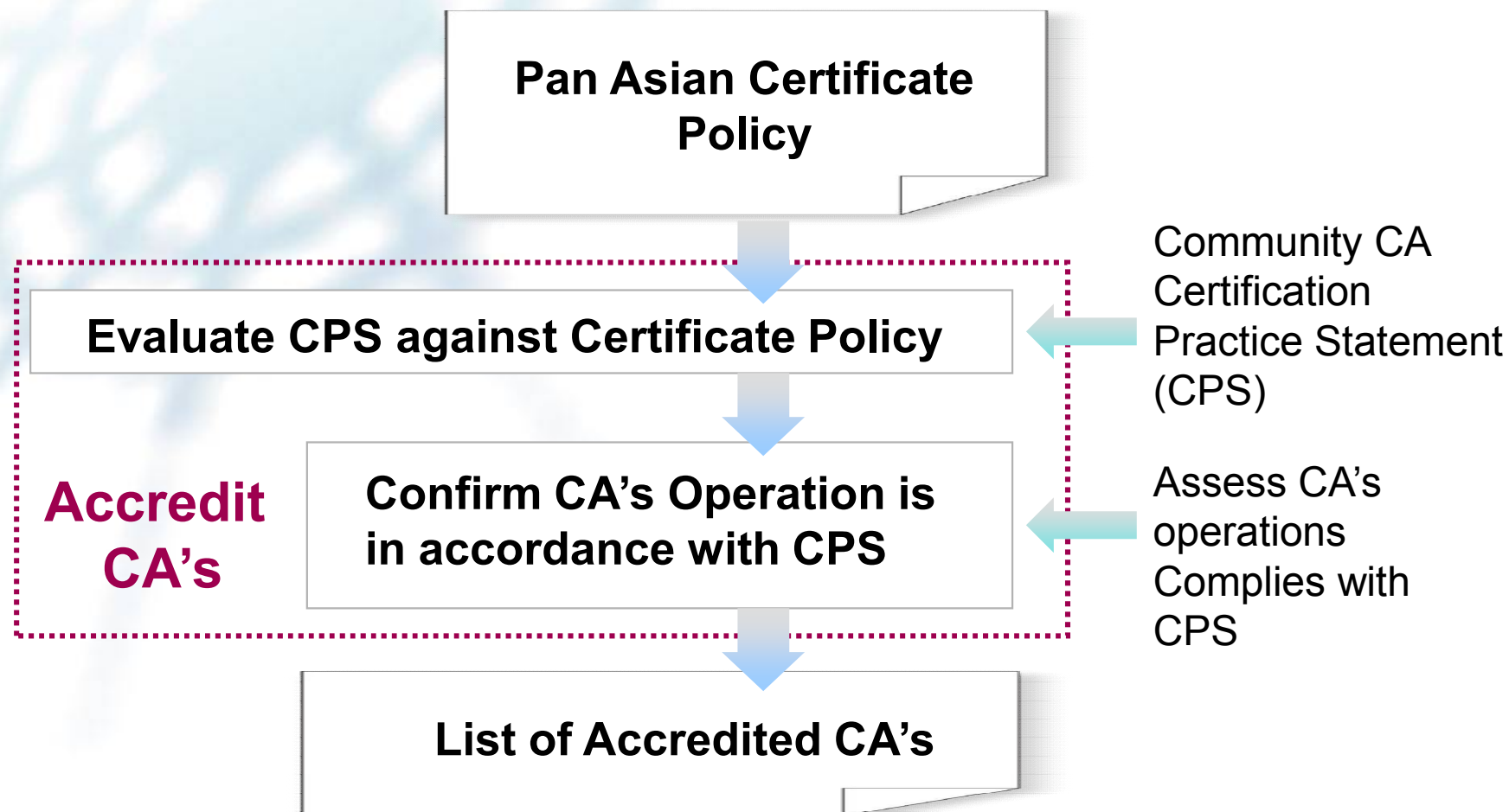
- **B2B Projects: Commercial Documents Exchange**
 - Electronic commercial documents (Purchase Order, Commercial Invoice, Packing List, Advanced Shipment Notice) exchanged in textile industry between Taiwan and Hong Kong
- **B2B2G Projects: Automated Manifest/Declaration Service**
 - Air Way Bill data from Taiwan, Hong Kong delivered to Korea to be generated into Korean Import Air Manifest
 - Air Way Bill, commercial invoice and export customs declaration data from Korea delivered to Taiwan to be generated into import declaration
- **ECO Project**
 - ECO exchange between Taiwan and Korea
- **Global Visibility Project**
 - Cross border container tracking between Asia and Europe

PAA Legal Framework



PKI Mutual Recognition

Pan Asian Certificate Policy Authority

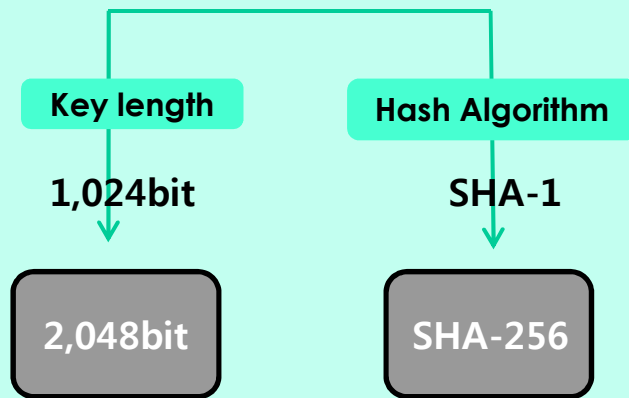


Upgrading Security Structure

For Authentication, Integrity, Confidentiality, Non-repudiation

- In Cryptography, SHA-2 designed by NSA and published in 2001 by US Federal information Processing Standard
- SHA-2 (no Collision found), SHA-1, 0 (collision and theoretical attack)

Upgrading Security Hash Function



In 2005, security flaws were identified in SHA-1

GeT*Mate 2.3.2 or above is required for a digital signature with SHA-2

* Key length upgrade

RSA / KCDSA 1024bit-> 2048bit

(Korea Certification-based Digital Signature)

•**ECDSA(Elliptic Curve Digital Signature Algorithm)163bit-> 224, 233bit** (recommended)

•**Hash Algorithm: SHA1(160bit)>SHA256(256bit)**

(recommended by National Institute of Standard and Technology, European Network of Excellence for Cryptology)

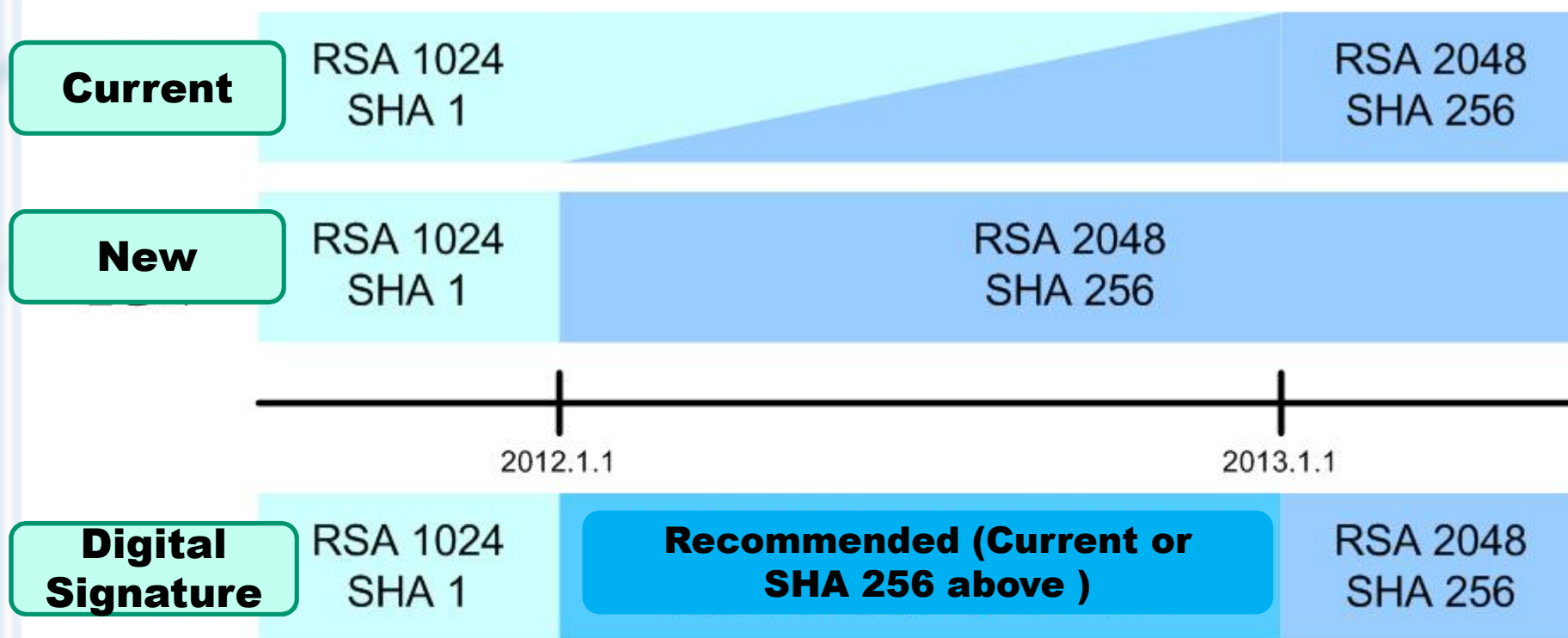
Recommendation for Key Management

* Key length upgrade (recommended)

- RSA / KCDSA 1024bit-> 2048bit (Korea Certification-based Digital Signature)

- ECDSA(Elliptic Curve Digital Signature Algorithm)163bit-> 224, 233bit

* Hash Algorithm: SHA1(160bit)>SHA256(256bit)



*Ministry of Public Administration and Security

[Rivest Shamir Adleman](#)



Copyright@2011 KTNET Reserved



Migration (SHA256) Survey

- **Does your current system support SHA-256?**

(If so, is the support version specific --explain. If not, what is the projected timeframe for support? Do you anticipate having beta test suites available for customers prior to general public release and configuration guidelines?)

- **How are we going to minimize the cost and the substantial impact for SHA-256 support ?**

(maintain backward compatibility for SHA-1 until the end of 2012)

- **What is required to conduct product testing, evaluation and procedures to ensure complete compatibility?**

(ie., general plan and milestones)

- **How are we going to address validating product claims of compatibility? (ie., certification)**

Supported Documents

- Purchase Orders
- Advance Shipment Notice
- Packing List
- Commercial Invoice
- Air Way Bill
- Bill of Lading
- Delivery Order
- Trade Declarations
- Electronic Certificate of Origin
- Shipping Order
- Processing Trade (China)



Case Study 1

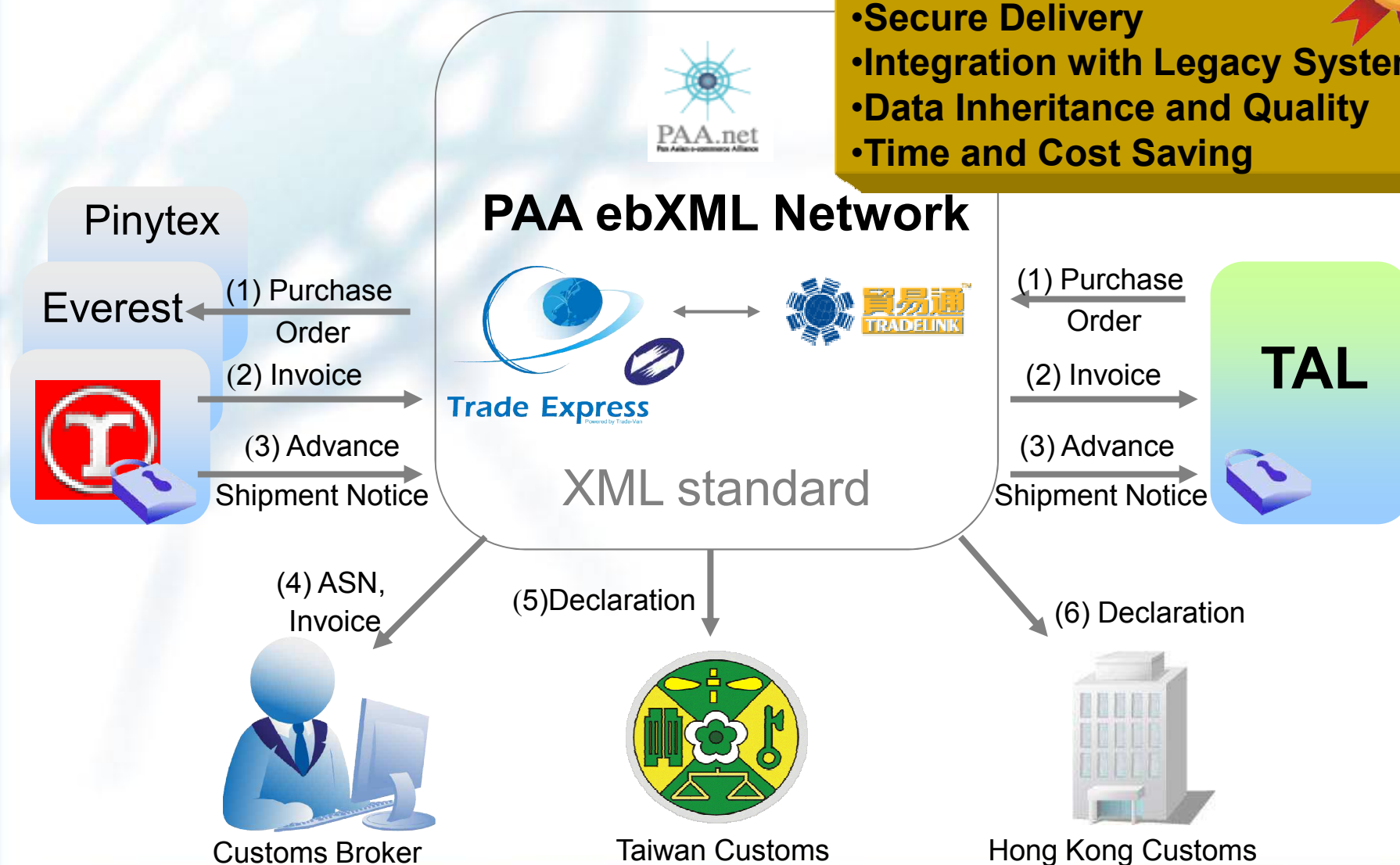
TAL

Major textile manufacturer in Hong Kong

TAL – Tai Yuen Cross Border Pilot via PAA

Guarantee

- Secure Delivery
- Integration with Legacy System
- Data Inheritance and Quality
- Time and Cost Saving

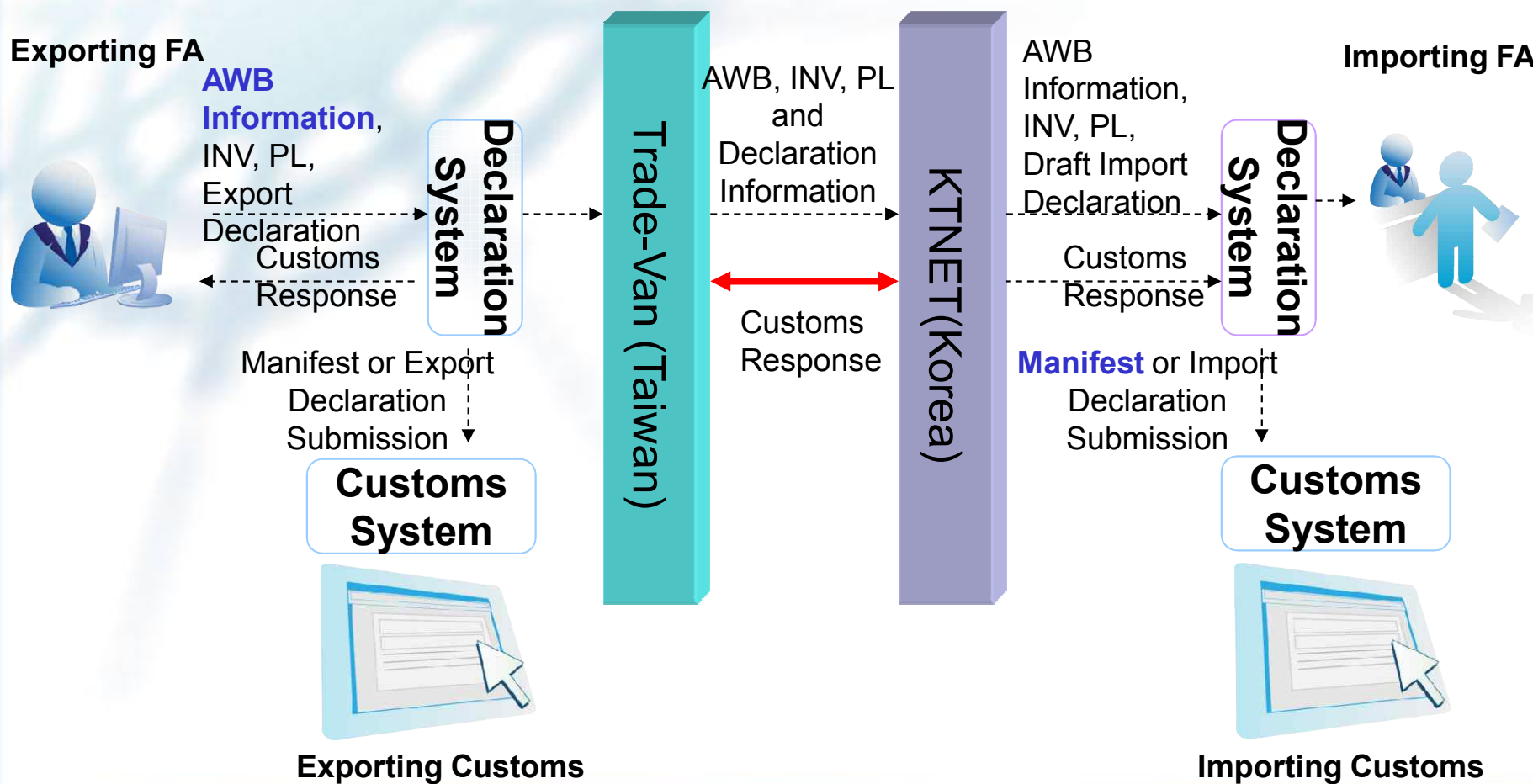


Case Study 2

Freight Forwarder

A new logistics management model

Extended Freight Forwarder Scenario



Monthly 3,000-4,000 live transactions!

The PAA Value Proposition

- EFFICIENT OPERATIONS – Trade **data can be reused** resulting in time savings in documents preparation
- REGULATORY INTEGRATION **-Integrated with Government services** (e.g. Trade Declarations) provided by PAA member
- ERROR FREE OPERATIONS – Automated reuse of trade data transmitted from trading partners result in **reduction of errors** caused by multiple data re-entry
- SECURITY - Secure electronic transaction with overseas trading partners – **no additional development** works or data mapping
- NEUTRAL RELIABLE PLATFORM – Common or **neutral** e-platform for **reliable** and **secure** document delivery
- STRONG PAA LEGAL FRAMEWORK - Backed by comprehensive contractual arrangement



Case Study 3

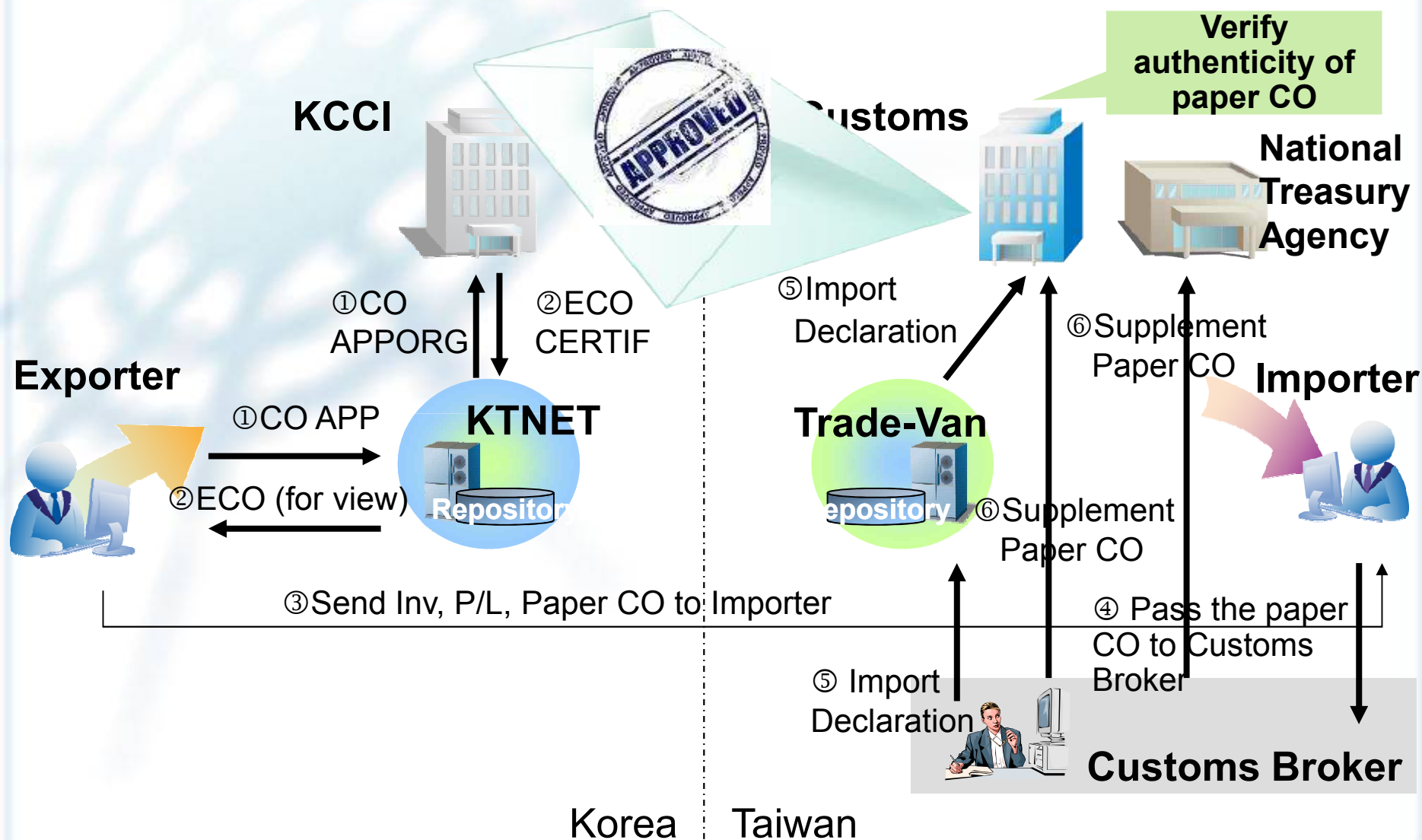
Electronic Certificate of Origin Exchange Project

A public and private partnership model

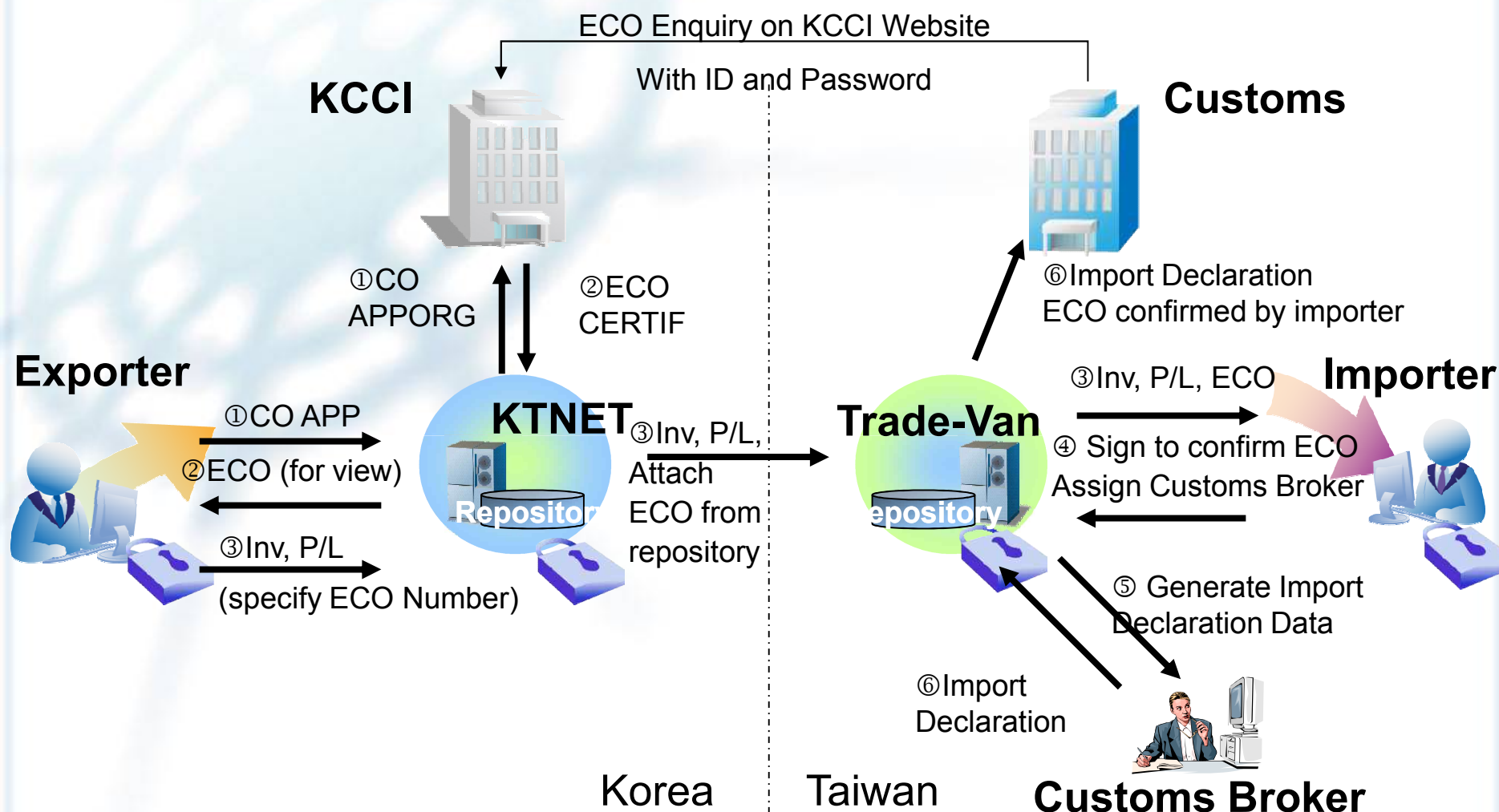
APEC Pathfinder Project

- ECO pathfinder is the most active **pathfinder project** under APEC ECSG
- A ECO project (an example of **Public Private Partnership**) between **MKE** (public sector), **KITA** and **KTNET** (private sector) of Korea and **BOFT, MOFA** (public sector), and **Trade-Van** (private sector) of Taiwan was initiated.
- ECO exchange model between Korea and Taiwan has been adopted by APEC member economies as a best practice for cross border paperless trading

Paper CO Scenario [Korea ▶ Taiwan]



ECO Scenario [Korea ▶ Taiwan]



New developments: cross border eSPS exchange

Benefits to Exporters/Importers

Exporter

- Save time and costs (*courier express US\$23*) in applying and sending over paper CO
- No need to get a stamp/seal on the CO from Taipei Trade Representative Office in Korea → save tremendous time (*in average 3 days*) and costs (*US\$17 per stamp, transportation cost US\$20-40*)
- Transmit cross border documents in a secure online environment
- Better service to their buyers

Importer

- Speed up customs clearance process
- Expedite cargo pick up → saving warehouse cost
- Guarantee of authentic CO

Expansion to Other Member Economies

- How do you start?
 - Readiness of domestic **ECO application system**
 - Readiness of digital signature law and PKI technology for secure data transmission
 - Secure exchange network and **PKI mutual recognition** framework to assure the authenticity of the electronic documents
 - **Domestic government's acceptance** of digitally signed electronic documents
 - Online ECO repository for inquiry and data validation if necessary

Conclusion

- PAA, the first regional alliance of service providers facilitating paperless trade, customs and logistics
- PAA is serving 150,000 organizations, representing almost all active trading enterprises in the Asian market
- Welcome to visit us at www.paa.net