



**PKI Cross Border Interoperability:
Pan Asian E-commerce Alliance (PAA)
Mutual Recognition Scheme**

Andrew Cheng
Tradelink Electronic Commerce Limited

Thursday
22 July 2004

Agenda

- ◆ Highlights of Tradelink
- ◆ Cross Border PKI
- ◆ Pan-Asian E-Commerce Alliance (PAA)
- ◆ Secure Cross Border Transactions
- ◆ PAA Mutual PKI Recognition
- ◆ Current Status
- ◆ Future Direction



Tradelink's Mission

- ◆ To help Hong Kong **maintain its international competitiveness** through the use of Electronic Commerce
- ◆ To jump start HK's **adoption of Electronic Commerce**

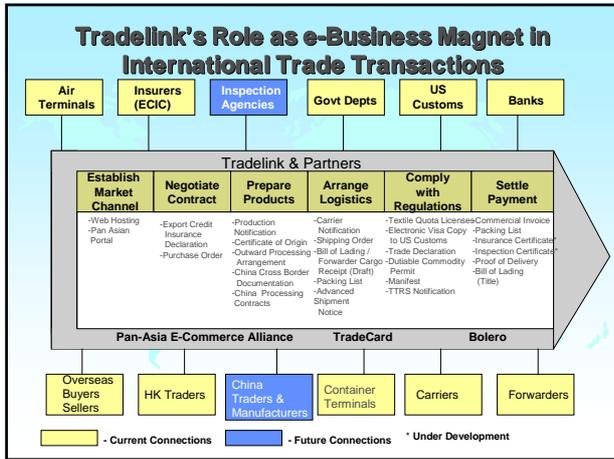
3

Tradelink's Electronic Services

Trade Related Government Services as the Basic Building Block

All Traders	Textile Traders & Manufacturers
<ul style="list-style-type: none"> ◆ Import & Export Declaration ◆ Certificate of Origin ◆ Dutiable Commodities Permit ◆ Shipping Order Service ◆ Trader Documentation Service for Regional/Global Trade ◆ China Processing Trade/Cross Border Documentation Service 	<ul style="list-style-type: none"> ◆ Restrained Textile Export Licence ◆ Carrier Notification and Electronic Visa Copy to US Customs ◆ Production Notification ◆ Textile Trader Registration Scheme (TTRS) Notifications
<h3 style="margin: 0;">Forwarders & Carriers</h3> <ul style="list-style-type: none"> ◆ Carrier Notification ◆ Shipping Order/AMS/ACI ◆ Manifest ◆ Textile Trader Registration Scheme Notifications 	

4



PKI (e.g. Hong Kong)

Legislation

Electronic Transactions Ordinance (Cap. 553) - enacted on 5 Jan 2000

Applications

- Tradelink's Services
- DTTN
- HKJC e-Betting services
- e-Banking (corporate)
- Corporate (email, document management, access controls)

Certification Authorities

CA Recognition Office (CARO)

- **Digi-Sign**
- **HiTRUST**
- **Postmaster General**

Users

- Personal
- Corporate
- Device
- Local
- Overseas

6

Cross Border PKI

- ◆ **Technical**
 - Cross Certification
 - Bridge CA
 - Certificate Trust List
 - Application support?
- ◆ **Legal**
 - Digital Signature Law

7

Pan-Asian e-Commerce Alliance (1)

Established in July 2000, aims to secure cross border electronic services for efficient global trade and logistics

Members	Number of Customers
CIECC (China)	10,000
KTNet (Korea)	25,000
CrimsonLogic (Singapore)	25,000
Trade-Van (Taiwan)	15,000
Tradelink (Hong Kong)	53,000
DagangNet (Malaysia)	2,000
TEDMEV (Macau)	2,000
TEDI Club (Japan)	_____
	132,000

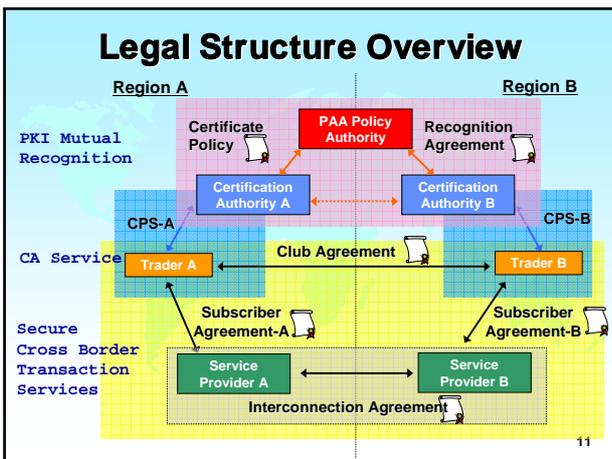
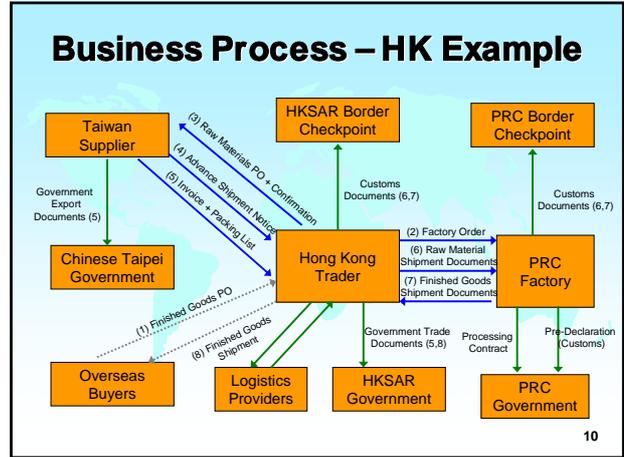
8

Pan-Asian e-Commerce Alliance (2)

◆ Initiatives

- Secure Cross Border Transactions
 - ◆ Document Supported: Purchase Order, Invoice, Packing List, Advanced Shipment Notice, Bill of Lading, Pre-Declaration
 - ◆ Cross border data sharing related to import and export declarations
- Mutual Recognition of Public Key Infrastructure
- Pan Asian Portal and e-Market Place
- Logistics Tracking
- Financial Services

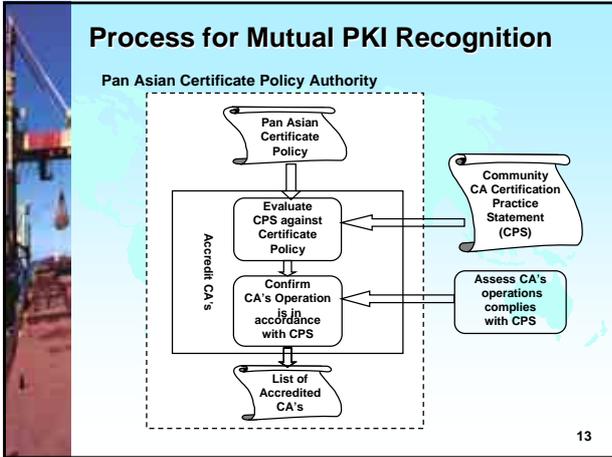
9



PAA Mutual PKI Recognition - Approach

- ◆ Pragmatic approach to drive cross border trade
- ◆ Establish comparative level of trustworthiness
- ◆ Establish Pan Asian Certificate Policy Authority to set criteria for PAA CA/CPS recognition
- ◆ Authentication of Identity of Individuals/ organizations so as to establishing non-repudiation for cross border trade
- ◆ Adherence to “good practice” while being flexible to allow for local requirements/variations

12



- ### PAA Mutual PKI Recognition - Current Status
- ◆ **Established Policy Authority (Jan 2001)**
 - ◆ **Established Pan Asian Certificate Policy (Nov 2001)**
 - ◆ **Recognized CAs**
 - Digi-Sign (Hong Kong) (Jan 2002)
 - TWCA (Taiwan) (Jan 2002)
 - Netrust (Singapore) (May 2002)
 - TradeSign (Korea) (Aug 2002)
 - GFACA (China) (Feb 2003)
 - JETS (Japan) (Feb 2003)
 - ◆ **Certificate Trust List distributed among PAA members**
- 14

- ### PAA Secure Cross Border Transactions - Current Status
- ◆ **Secure Cross Border Transactions**
 - Hong Kong - Taiwan (Buyer & Suppliers)
 - Taiwan - Korea / Japan (Buyer & Suppliers)
 - Taiwan - Singapore/ Malaysia (Freight forwarders)
 - Taiwan - China (HQ & Manufacturers)
 - Korea - Japan (Buyer & Suppliers, Title documents)
- 15

- ### Future Direction
- ◆ **Online Certificate Status Protocol**
 - ◆ **Global Certificate Service**
 - ◆ **Others**
- 16

Certificate Validation

- ◆ **Certificate Revocation List (CRL)**
- ◆ **Issued periodically (e.g. once every 8 hours)**
- ◆ **Size grow in time**
- ◆ **Force CRL may affect CRL publication schedule**
- ◆ **End user's responsibility to go through CRL**
- ◆ **Multiple CAs => Multiple CRLs**

17

Online Certificate Status Protocol (1)

- ◆ **OCSP**
 - OCSP responder (aka Validation Authority) collects Certificate Status from CA
 - End User queries status of a certificate
 - OCSP returns status of the certificate
- ◆ **No CRL downloads**
- ◆ **No need to search through CRL**
- ◆ **No CRL delay (CA dependent)**
- ◆ **Can Serve multiple CAs (local & overseas)**
hence single point of contact
- ◆ **Remove End user's burden**

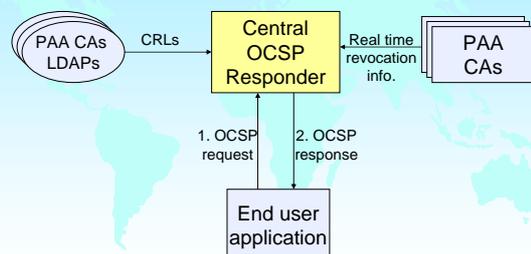
18

Online Certificate Status Protocol (2)

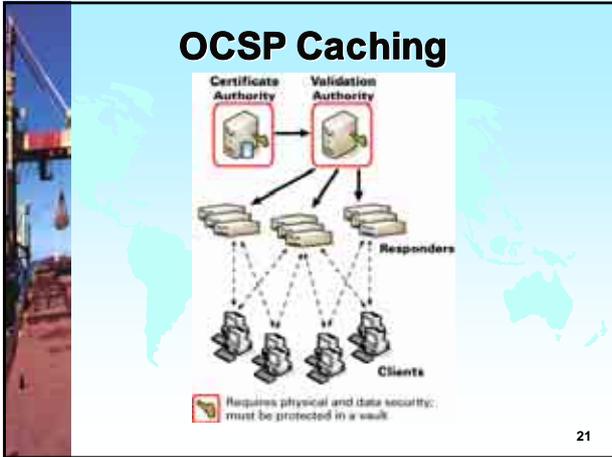
- ◆ **Considerations**
 - Suitable for online only!
 - Turn around time
 - Cost
 - o CRL - free
 - o OCSP - per transaction (typical)
 - Application support

19

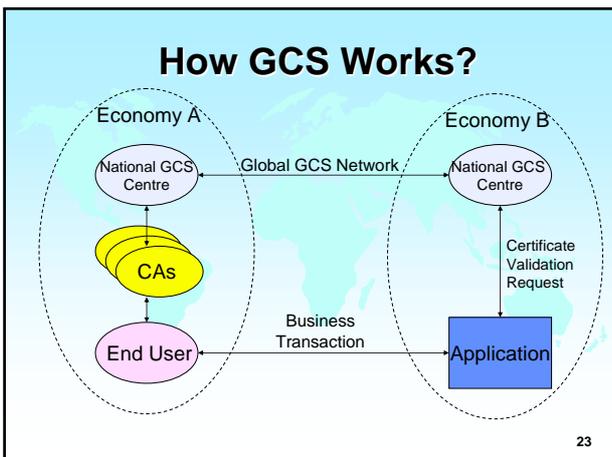
PAA OCSP



20



- ### Global Certificate Services
- ◆ OCSP only solves half of the problem
 - ◆ Global Certification Service
 - One national GCS centre per member economy
 - National gateway for all certificate related services
 - Business model similar to the relationship with the bank
- 22



- ### Why GCS? (1)
- ◆ Delineated liability boundaries in complex transactions
 - ◆ Single contact point for certification of transactions
 - ◆ Reduces management overhead in maintaining & establishing global relationships with third parties
 - ◆ Simplified legal framework (Application and local GCS centre in same jurisdiction)
 - ◆ Deposit an overseas cheque into the local bank
- 24

Why GCS? (2)

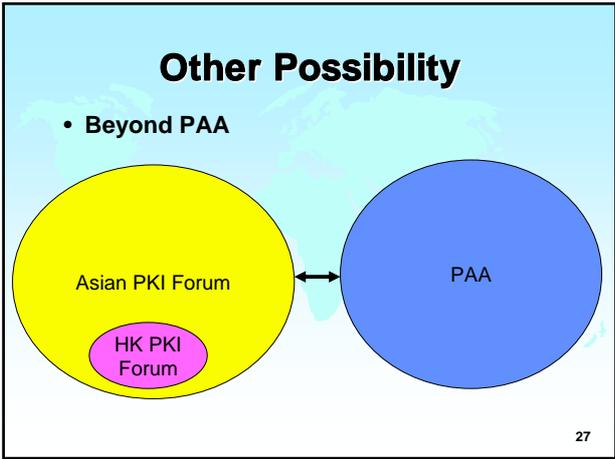
- ◆ Only need to deal with one local GCS
- ◆ Protected by local government regulation
- ◆ Single certificate to access broader global services
- ◆ Globally recognised certificate

25

GCS Model

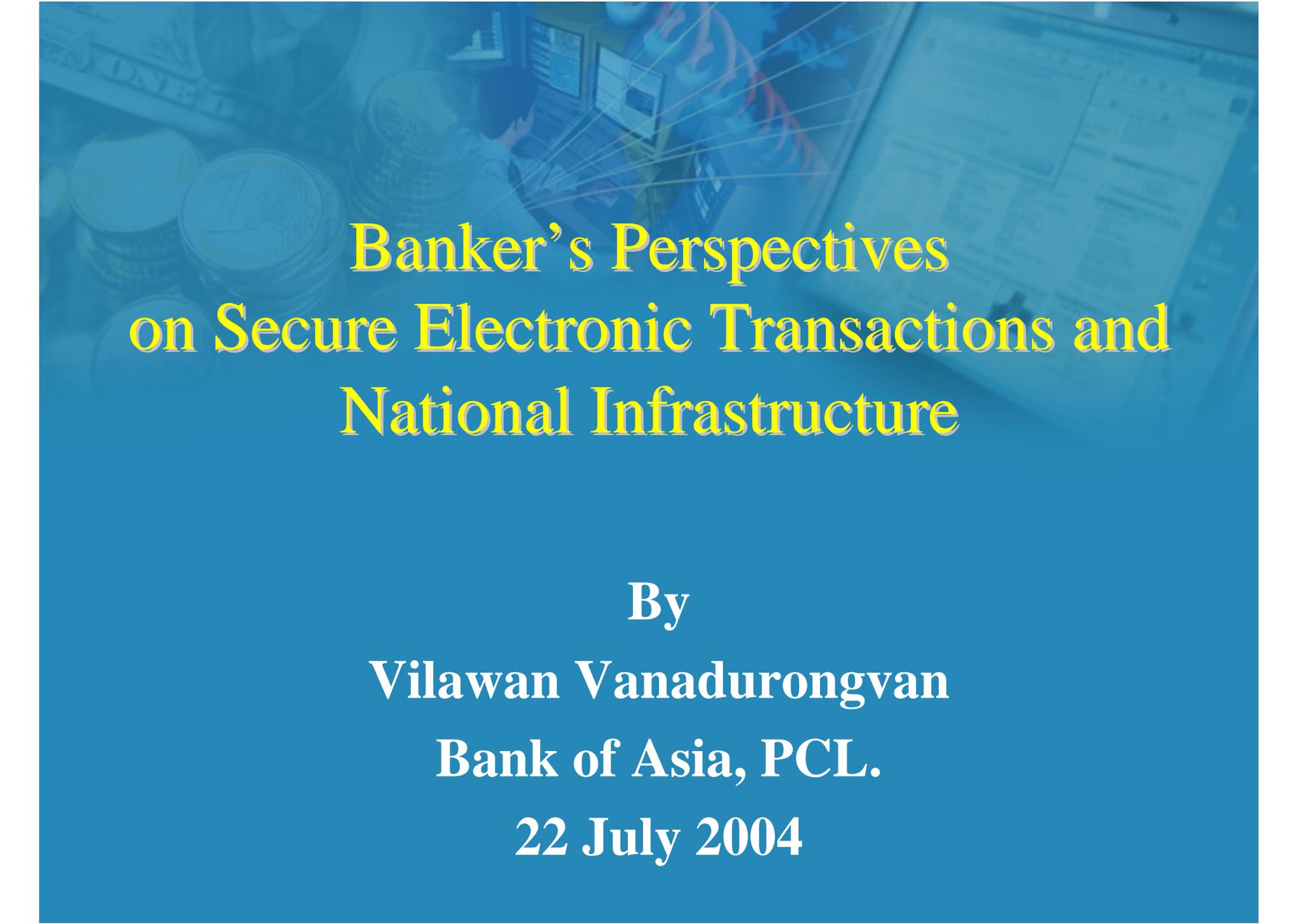
- ◆ National GCS centre as a trusted gateway provides a national single point of certification for all the subscribing CA's and the enterprises connected using public networks
- ◆ GCS Global Network
 - Full peer-to-peer network with local point of presence in each country (i.e. National CGS centre)
 - Each centre operates under the full jurisdiction & laws that are applicable for their host country

26



TRADELINK

Spearheading Hong Kong's Development of
Electronic Commerce



**Banker's Perspectives
on Secure Electronic Transactions and
National Infrastructure**

By

Vilawan Vanadurongvan

Bank of Asia, PCL.

22 July 2004

Security Concerns & E-Business

- Security concerns do not block the progress as much as initially fear.
- E-Business does not have to be 100% risk-free and fraud-free to be profitable.
- e-Business can still grow to a certain extent by ensuring that the “Rewards” outweigh the “Risks”.

Example: Verified by VISA

- *Verified by VISA (VbV)* can successfully mitigate credit card fraud for e-Commerce Merchants and card holders.
- Some E-Business decide to delay using VbV when

Loss in Sale with VbV > Risk in Fraud without VbV

- *VbV is expected to be effective and widely used when VISA will make Verified by VISA mandatory worldwide in 2005.*

Payment System & Security

Payment System

= Instruments + Procedures & Rules

Security Decisions:

- How much should be invested in hardware & software for security?
- How much security should appear in procedure / rules?

10 BIS Core Principles for Systematically Important Payment Systems (SIPS)

- Address ways to manage legal risks, credit risks, and liquidity risks in SIPS (payment system which can cause domino effect that led to financial crisis if something goes wrong).
- Address that SIPS need rules and procedures to manage the risks & foster understanding about system's impact on each financial risks.
- Address that SIPS must be practical and efficient and their governance arrangement should be effective, accountable, and transparent.

Levels of security in e-Business

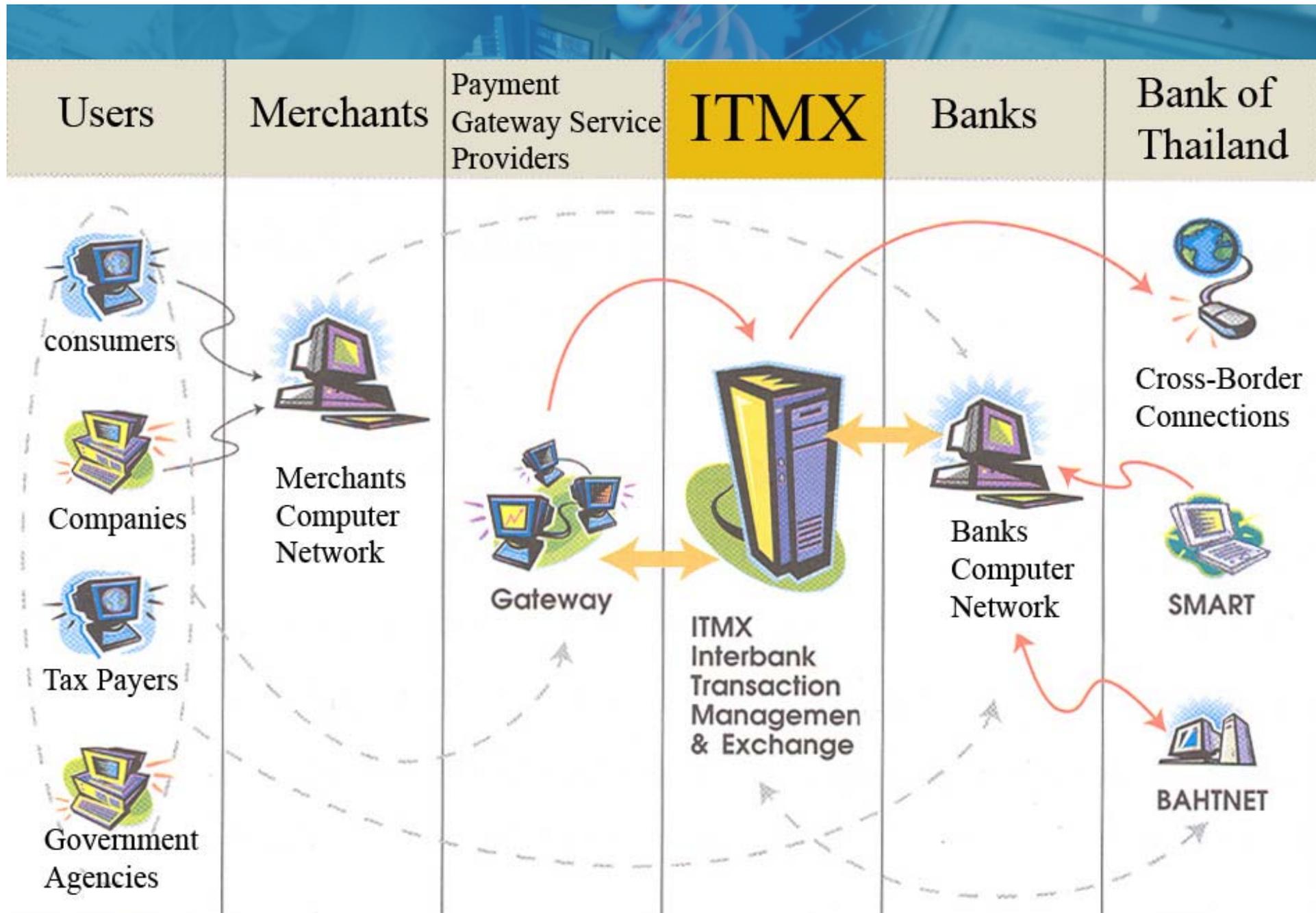
- **Local Level:**
 - With e-Business customers of one bank.
- **National Level:**
 - With e-Business customers of any bank in a country.
- **Regional level:**
 - With e-Business customers of any bank in any country within the region.

Local Level:

- **Banks in THAILAND began to offer e-Commerce Service years before Cabinet approved E-Commerce Law.**
- **B2C**
 - **Transaction amount is not high.**
 - **Level of Risks are acceptable.**
- **B2B**
 - **Businesses signed contracts with bank**
 - **Businesses must have accounts within the same banks to do fund transfer.**
- **Implement security that meets International Standard BUT PKI are not widely used**

National Level:

- *E-Business Growth:*
 - *Need to allow InterBank Transfer in large sum across banks within Thailand to do e-Commerce transaction.*
 - *Need PKI.*
- *Payment 2004: A Road Map for Thai Payment System.*
 - **Interbank Transaction Management and Exchanges (ITMX)**



Regional Level (APEC)

Several issues to address

- e-Commerce legislation for APEC region to help settle disputes in-court or out-of-court.
- **PKI IS A MUST but its acceptance depend on ACCOUNTABILITY of CA.**
 - How much liability CA are willing to accept for their mistakes when transaction amount is in million U.S. Dollars?
 - How much fee e-Business is willing to pay to make CA accountable?