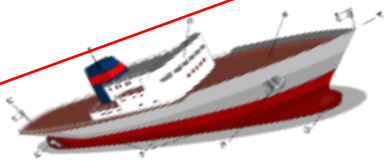
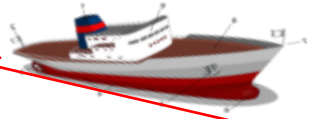
E-Signature Issues in Cross-Border Single Window: A comparative analysis of Australia, the UK and China

Ms. Hemali Shah
Department of Business Law and Taxation
Monash University
Australia

Import-Export of commodities between countries



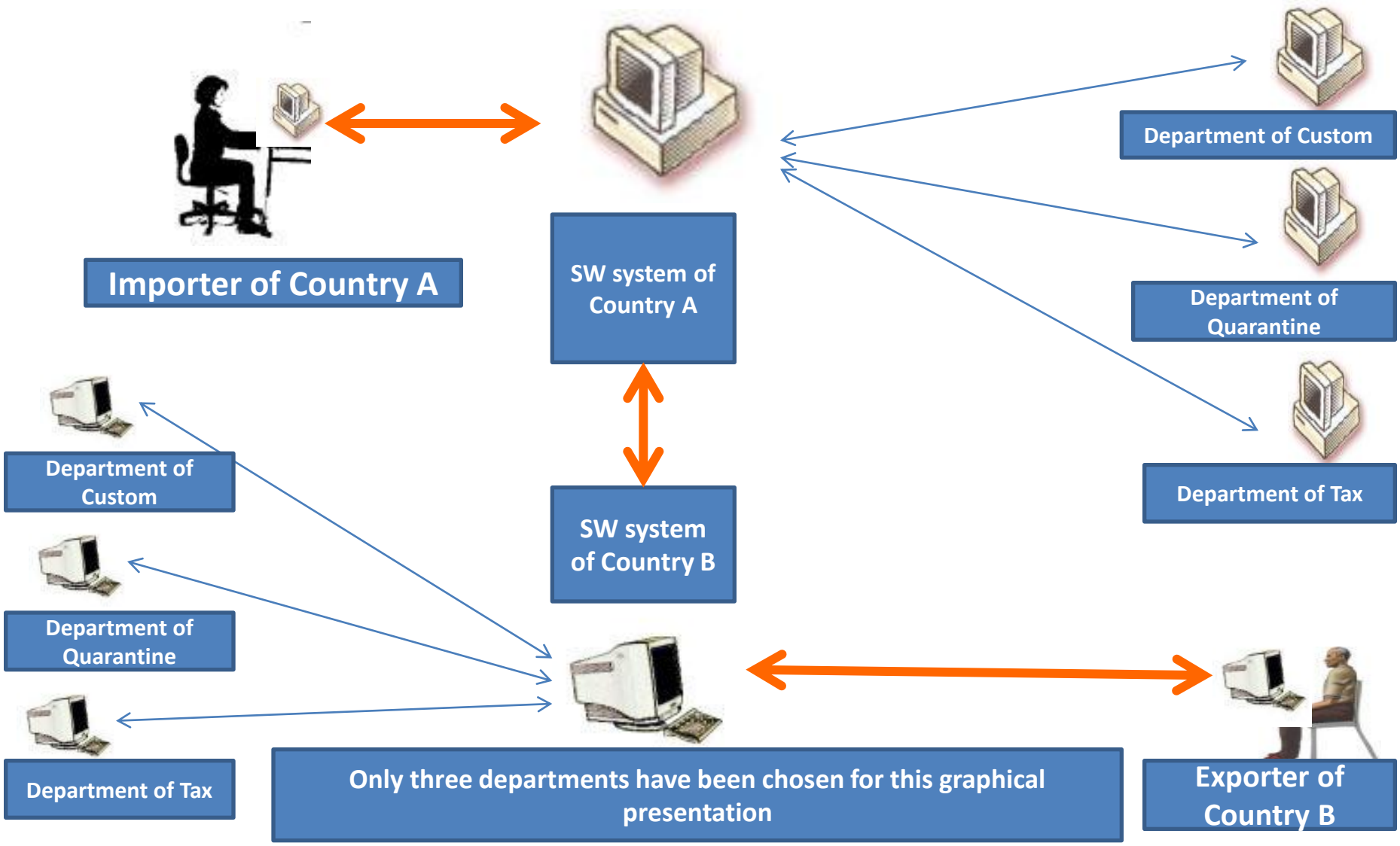


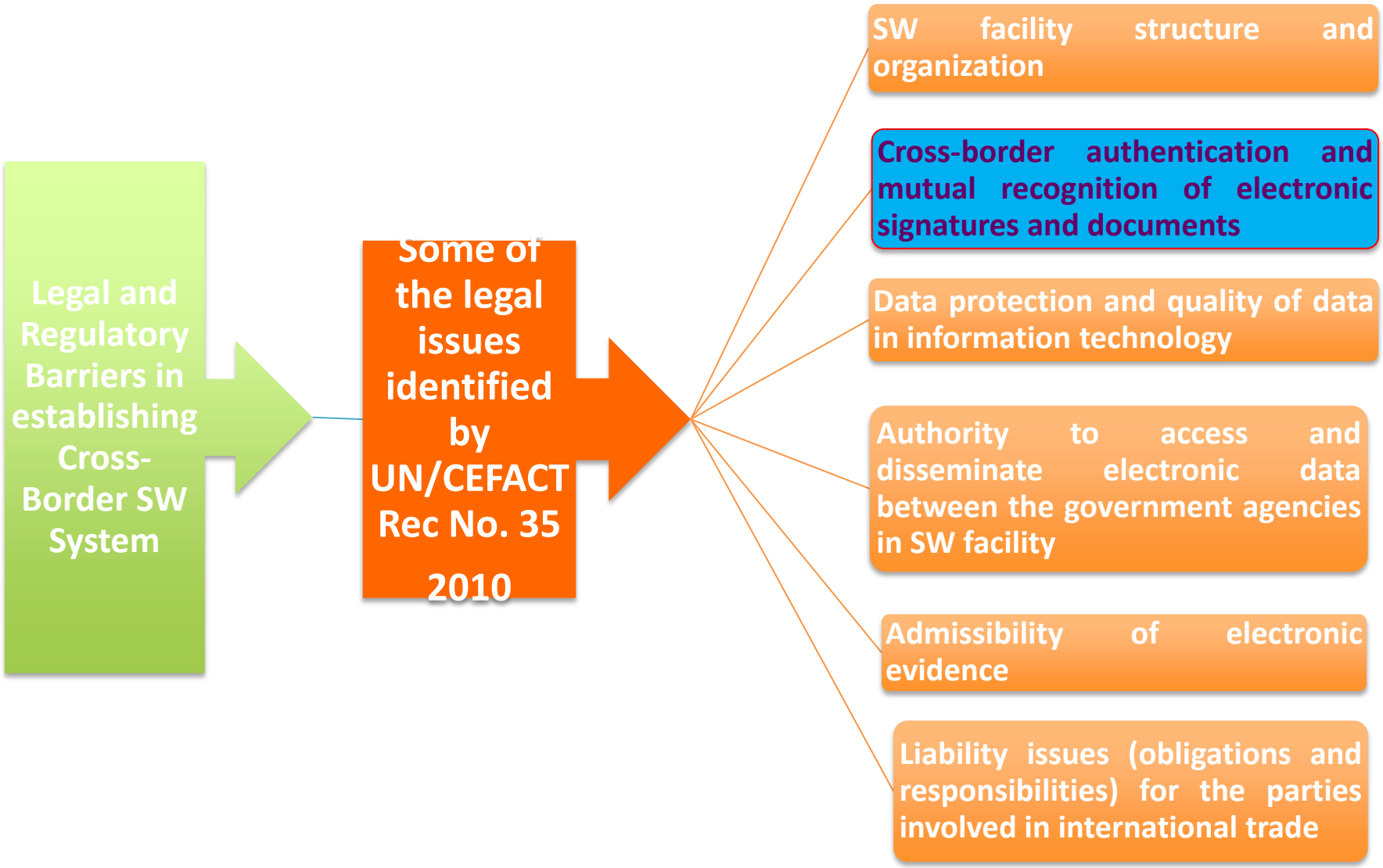
- Average cross-border transaction involves
  - 27 to 30 different parties,
  - 40 documents,
  - 200 data elements (30 of which are repeated at least 30 times) and the re-keying of 60 to 70 per cent of data at least once.
- Obtaining the necessary permits for import and export can take many weeks and sometime months in some economies. (Ministry of Foreign Affairs and Trade, 'Paperless Trading: The Potential of the APEC Paperless Trading Initiative', *Green Advertising,* 2001).
- Customs and Border Protection of Australia works collaboratively with **over forty** Commonwealth, State and Territory agencies and regulators.

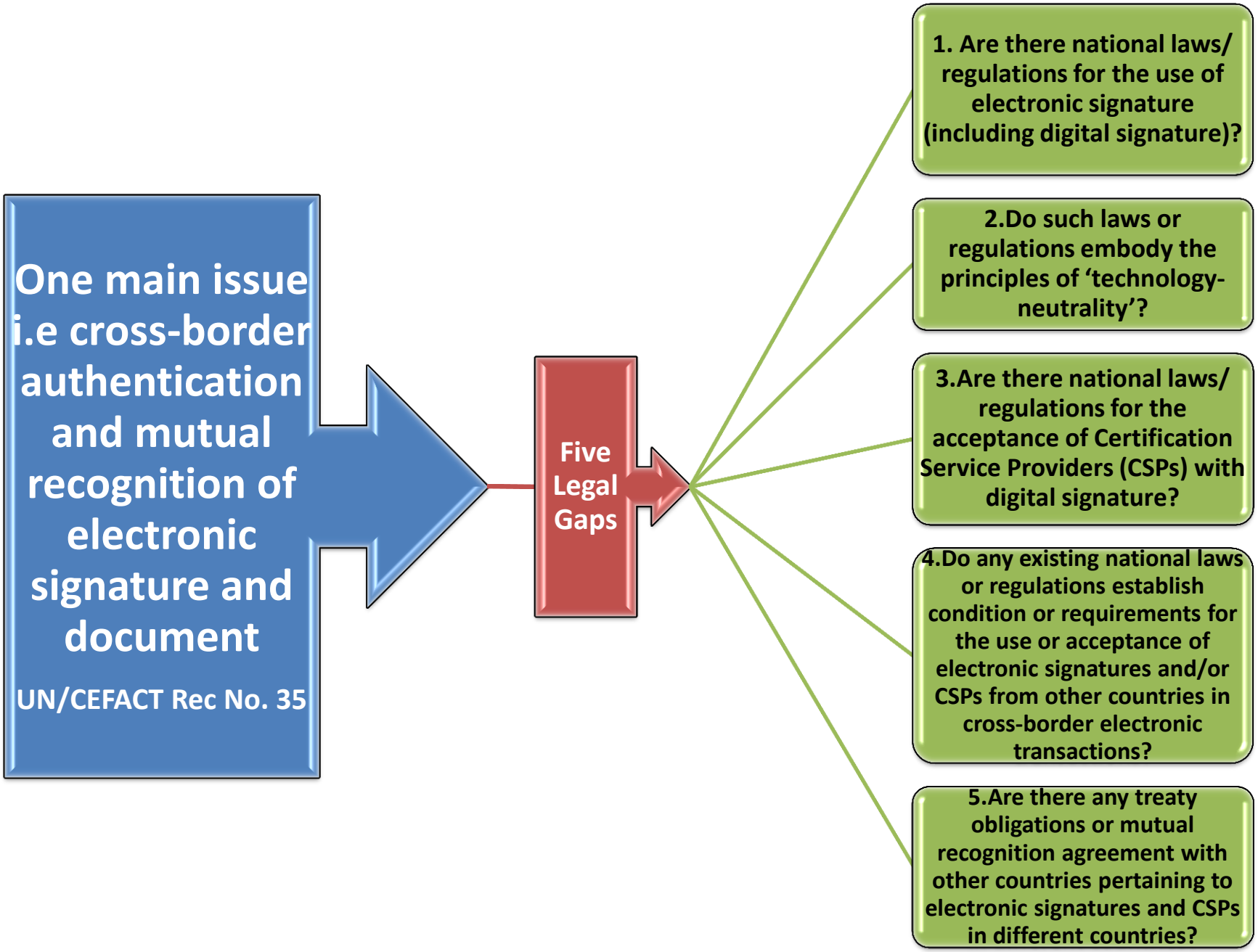
What is Single Window

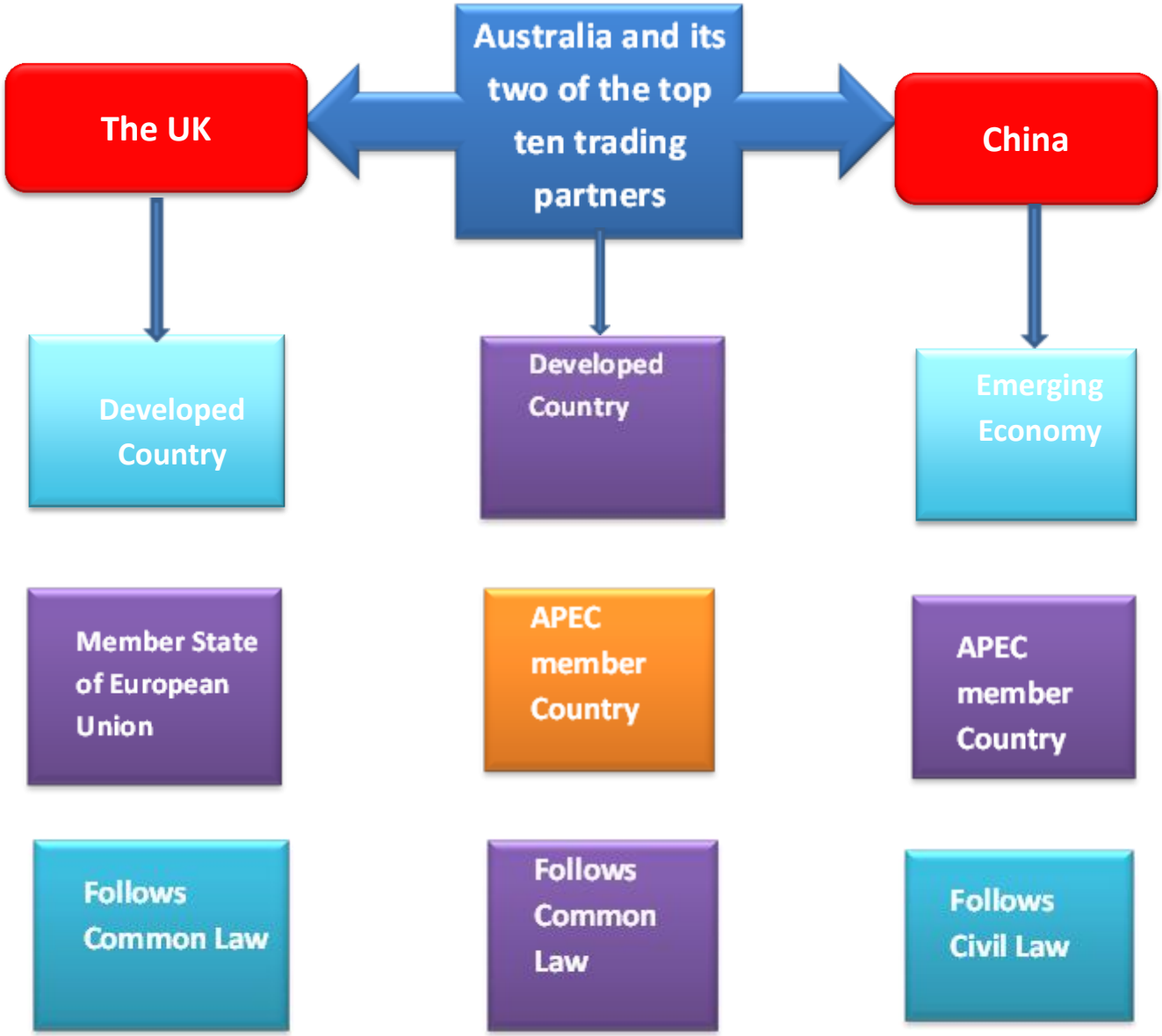
Single Window (SW) is a facility that allows parties involved in trade and transport to lodge standardized information and documents (mostly in electronic form) with a **single entry point** to comply with all import, export, and transit related regulatory requirements and if there is electronic information, individual **data elements should only be submitted once**. (UNECE, *UN/CEFACT Recommendation No. 33 Establishing Single Window to enhance the efficient exchange of information between trade and government,* ECE/TRADE/352 (July 2005), 3).

Graphical presentation of a Cross-Border single automated SW system




Legal and Regulatory Barriers in establishing Cross-Border SW System
Some of the legal issues identified by UN/CEFACT Rec No. 35 2010
SW facility structure and organization
Cross-border authentication and mutual recognition of electronic signatures and documents
Data protection and quality of data in information technology
Authority to access and disseminate electronic data between the government agencies in SW facility
Admissibility of electronic evidence
Liability issues (obligations and responsibilities) for the parties involved in international trade


One main issue i.e cross-border authentication and mutual recognition of electronic signature and document
UN/CEFACT Rec No. 35
Five Legal Gaps
1. Are there national laws/ regulations for the use of electronic signature (including digital signature)?
2.Do such laws or regulations embody the principles of 'technology-neutrality'?
3.Are there national laws/ regulations for the acceptance of Certification Service Providers (CSPs) with digital signature?
4.Do any existing national laws or regulations establish condition or requirements for the use or acceptance of electronic signatures and/or CSPs from other countries in cross-border electronic transactions?
5.Are there any treaty obligations or mutual recognition agreement with other countries pertaining to electronic signatures and CSPs in different countries?


Australia and its two of the top ten trading partners
The UK
China
Developed Country
Developed Country
Emerging Economy
Member State of European Union
APEC member Country
APEC member Country
Follows Common Law
Follows Common Law
Follows Civil Law

What is Electronic Signature?

- **Electronic Signature is a technology neutral term and refers to a process whereby a person (signer) can electronically sign an electronic record.**
- **Examples of Electronic Signatures are:**
- **1) Password or PIN**
- **2) typed name at the end of e-mail**
- **3) biometric based signature (finger print, retina scan, iris scan, signature dynamics, voice recognition, keystroke dynamics, DNA etc)**
- **4) digital signature (public key cryptography).**

Digital Signature (DS)

- DS uses Public Key Cryptography.
- It contains two keys:
  - Public Key and Private Key.
- Private key is secret to the user just like your PIN or password and public key is public in nature and can be found as a person's name in a telephone directory.

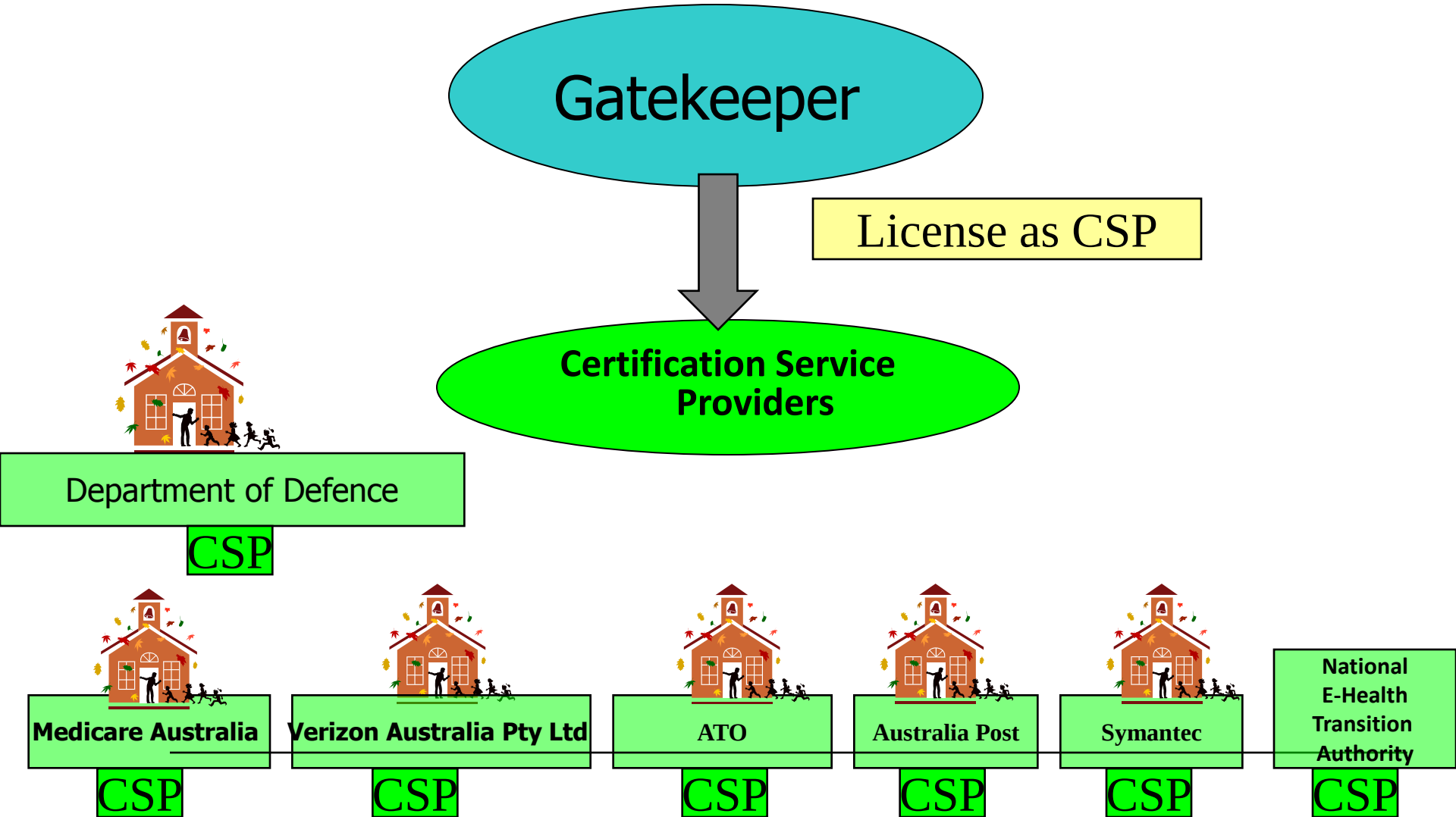
Bodies that issue digital signature certificate.

- Certification Service Provider (CSP): issue electronic ID certificate known as ‘digital certificate’ to ensure that the digital signature belongs to the signatory.

- A digital signature certificate (an electronic certificate) containing name, organisation details and other details to a subscriber.

- Note it is the CSP that links the public and private key pair to an individual/subscriber.

Who issues Digital Signature Certificate in Australia?



Three different regulatory approaches to e-signature worldwide

- **Digital Signature approach.**
  - Only digital signature is legally valid.
    - Nepal's *Electronic transaction and digital signature act 2004*
- **Two-prong approach.**
  - All types of electronic signatures are valid but special status to digital signatures.
    - India's *Information Technology Act 2000*
- **Minimalist approach.**
  - All types of electronic signatures are valid. No special status to digital signatures.
    - Australia's *Electronic Transaction Act* 1999 (Cth)

1. Legal Gap: Are there national laws or regulations providing requirements for the use of electronic signature (including digital signature)?

	Australia	**UK**	**China**
	Yes	Yes	Yes
Act and Regulation in force	*Electronic Transaction Act 1999* (Cth) (ETA) and the *Electronic Transaction Regulations 2000* (ETR)	*Electronic Communication Act 2000* (UK) c7 (ECA) and *Electronic Signatures Regulations 2002* (ESR)	*Electronic Signature Law* (ESL) and *Administrative Measure on Electronic Certification Service* (AMECS)
Legal requirements for the use of electronic signature (including digital signature)	Section 10	Section 7(2) and Section 7(1)	Article 14 should be read in conjunction with Article 2.
Legal effect of documents/communication shall not be denied solely on the ground of its electronic form.	Section 4 and section 8.	Section 7(1)	Article 3

2. Legal Gap: Do such laws or regulations embody the principles of ‘technology-neutrality’?

	Australia (ETA and/or ETR)	UK (ECA and/or ESR)	China (ESL and/or AMECS)
Prima facie	Yes	Yes	Yes
Technology-neutrality provisions of the Act and/or Regulation	Section 10 of the ETA	Section 7(2) of the ECA	Article 2 of the ESL
Other provisions of the Act or Regulation offering favourable legal presumption to certain technology exhibiting special features	No	Section 2 of the ESR provides standards for an ‘advanced electronic signature’ i.e. digital signature	Article 13 of the ESL provides standards for a ‘reliable electronic signature’ i.e. digital signature
After analysis	Technology-Neutral	Two-prong	Two-prong

3. Legal Gap: Are there national laws or regulations regarding the use and/or acceptance of CSPs with digital signature?

	Australia	**UK**	**China**
Licensing regime	Voluntary	Voluntary	Compulsory
Who provides licence/ accreditation to the CSPs?	*Gatekeeper*	*tScheme*	Ministry of Information Industry (MII)
Provision in the Act or Regulation regarding CSPs	No express provision. However,	Section 7(1) of the ECA	Article 16

4. Legal Gap: Do any existing national laws or regulations establish condition or requirements for the use or acceptance of electronic signatures and/or CSPs from other countries in cross-border electronic transaction?

Australia	**UK**	**China**
No	**No**	**Yes**
ETA & ETR do not provide express condition or requirement	Neither ECA nor ESR provides explicit condition or requirement	Article 26 of the ESL provides detailed requirement.
The inclusion or exclusion of evidence relating to foreign digital signature certificate will be a matter of procedure, rules and court's ex-post facto rationalization	Evidentiary value of foreign digital signature certificates will be determined by judicial procedure and rules	ESL recognizes a foreign CSP certificate provided it satisfies the requirements laid down in Article 26
AGIMO--*Gatekeeper* policies and criteria to be an appropriate basis for identifying standards for cross-recognition with non-*gatekeeper* PKI	*tScheme* will co-operate with equivalent organisations across Europe and elsewhere with a view to extending co-operation and mutual	Approval of the responsible department of the MII

5. Legal Gap : Are there any treaty obligations or mutual recognition agreement with other countries pertaining to electronic signatures and CSPs in different countries?

Australia	UK	China
No	No	No

Australia, UK and China do not have any particular treaty or MOU that recognizes the use of electronic signatures and CSP with other countries.

Findings

- All three countries have a national law for the use of electronic signatures.
- Prima facie, they appear technology-neutral. However, only Australia has a ‘technology-neutral’ legislation.
- Regarding the national laws and regulations for the use and acceptance of CSPs with digital signatures, Australia, UK and China have separate regimes making cross-border recognition of digital signatures difficult.
- The *United Nations Convention on the Use of Electronic Communications in International Contract 2005* (the Convention) aims to enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts. Countries should adopt this Convention.
- In the absence of a treaty obligation for mutual recognition of digital signatures and CSPs, it is almost impossible to have any cross-recognition of CSPs/digital signature.