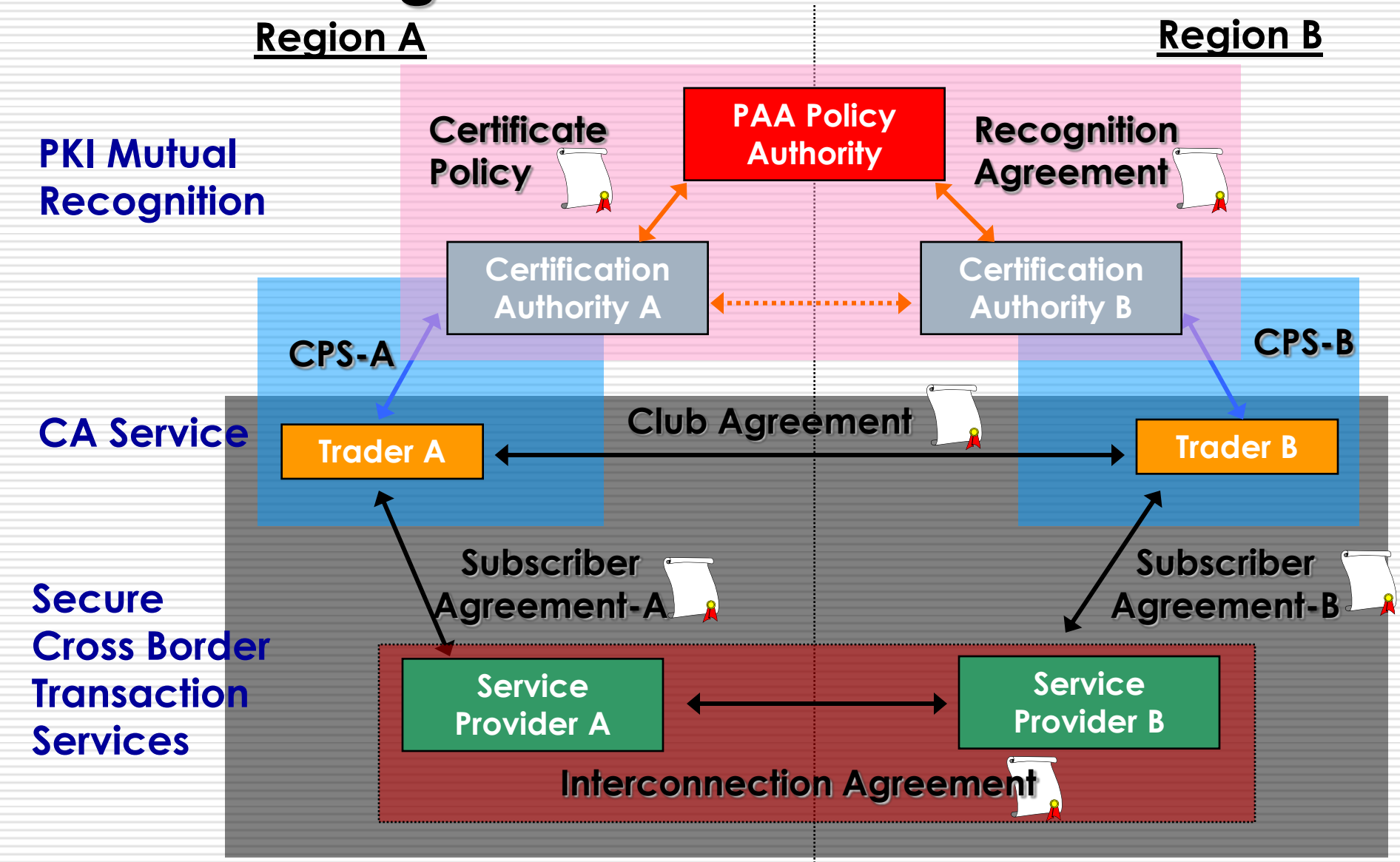
PAA
PKI Mutual Recognition Framework

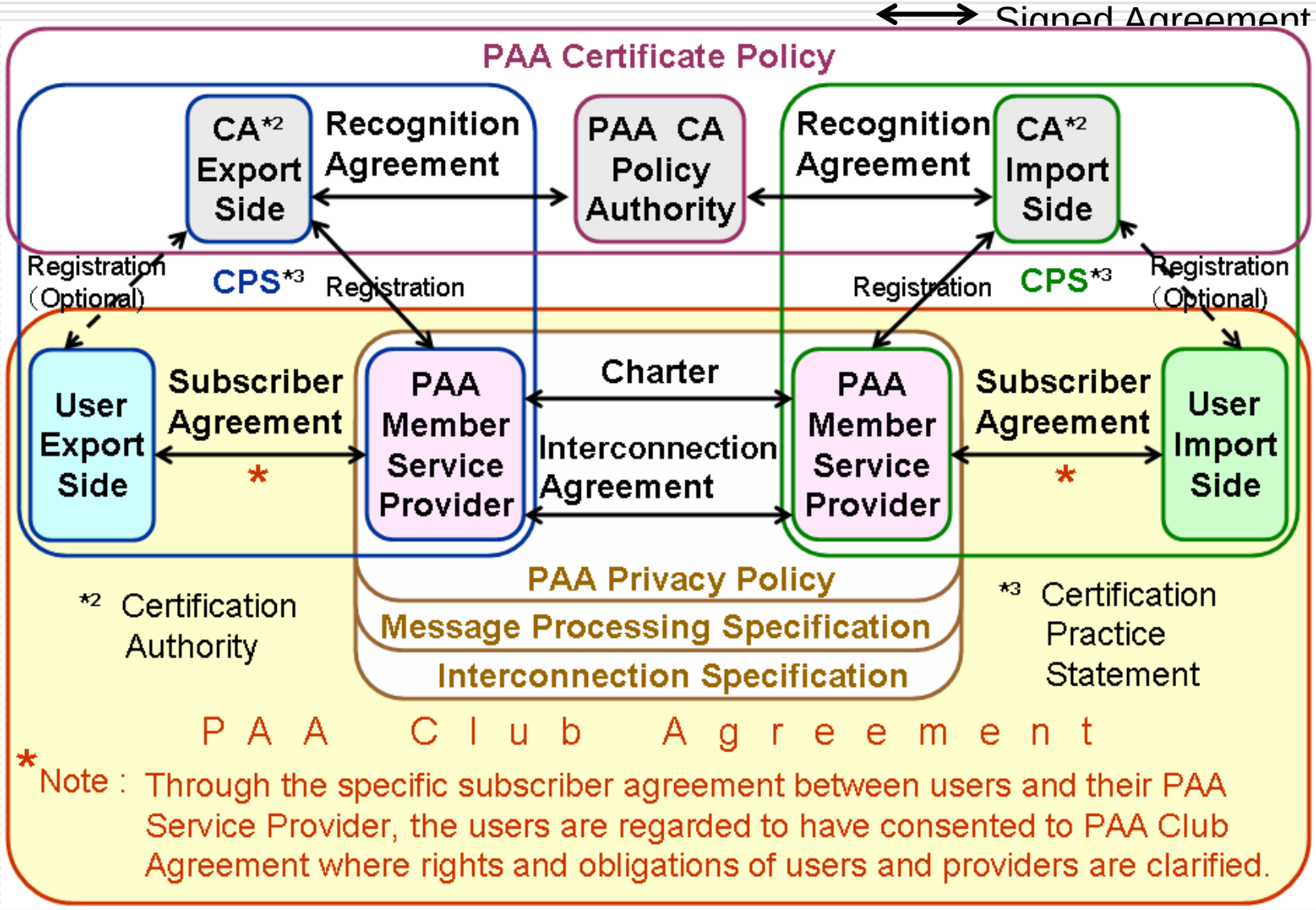
Agenda

- Overview of the Framework
- Components of the Framework
- How It Works
- Other Considerations
- Questions and Answers

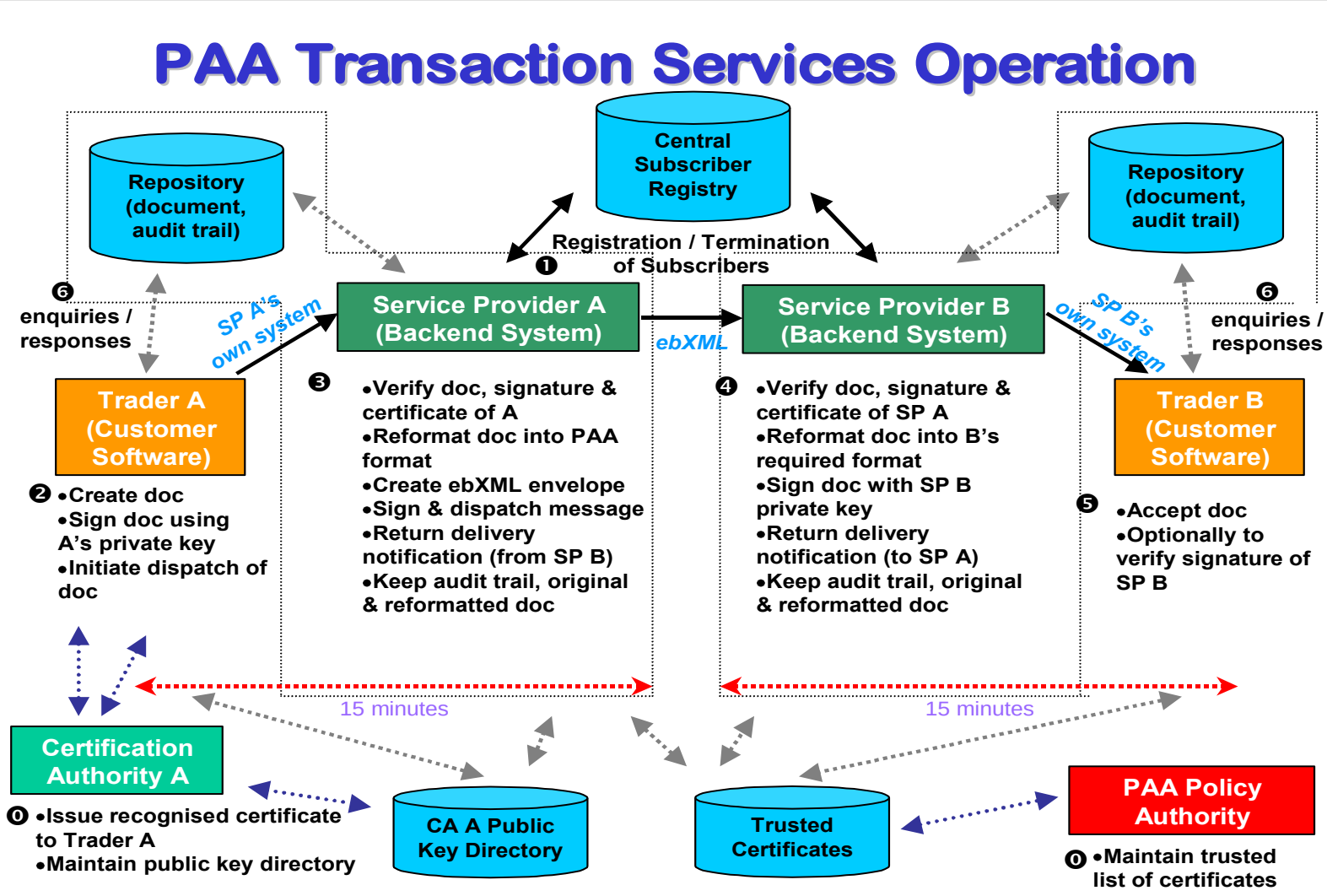
Legal Structure Overview



PAA Legal Framework for Cross-border Transaction Service



PAA Transaction Service Operation



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

Components of the Framework

A. PAA Policy Authority

- Established in Jan 2001
- The Authority's Terms Of Reference define the scope of responsibilities
- Define a common PAA Certificate Policy (CP)
- Define a procedure for the recognition of CPS of CA against this CP
- Define a procedure for the change management for the CP and the recognition procedure
- Administer the recognition and change management procedure

Components of the Framework

B. PAA Certificate Policy

- Define a set of rules as minimum and common criteria for recognition
- For use within the PAA domain and trusted by the PAA members
- CPS of a CA seeking recognition is assessed against this CP
- Sit on top of a CPS that cover different aspects (policy, legal, operational, technical)

Components of the Framework

C. Recognition Procedure

- 1. Initial recognition
  - Submit supporting documents (e.g. sponsor letter from PAA member being the user/relying party of the certificate, CPS, external assessment report, test report, etc) to the Authority
  - Review the documents by the Authority's PKI experts
  - Produce recommendation report by the experts

If recommendation is accepted, the Authority will

- sign recognition agreement with the CA
- publish the CA's information to the Authority's official web site
- add the CA to the Certificate Trust List (CTL) to be distributed to PAA members

Components of the Framework

C. Recognition Procedure

- 2. Renewal of recognition
  - Similar to initial recognition
  - Every two years
  - Some supporting documents are not required unless there are changes
  - The Authority's official web site will be updated to indicate renewal
  - Latest assessment report will also be published

Components of the Framework

C. Recognition Procedure

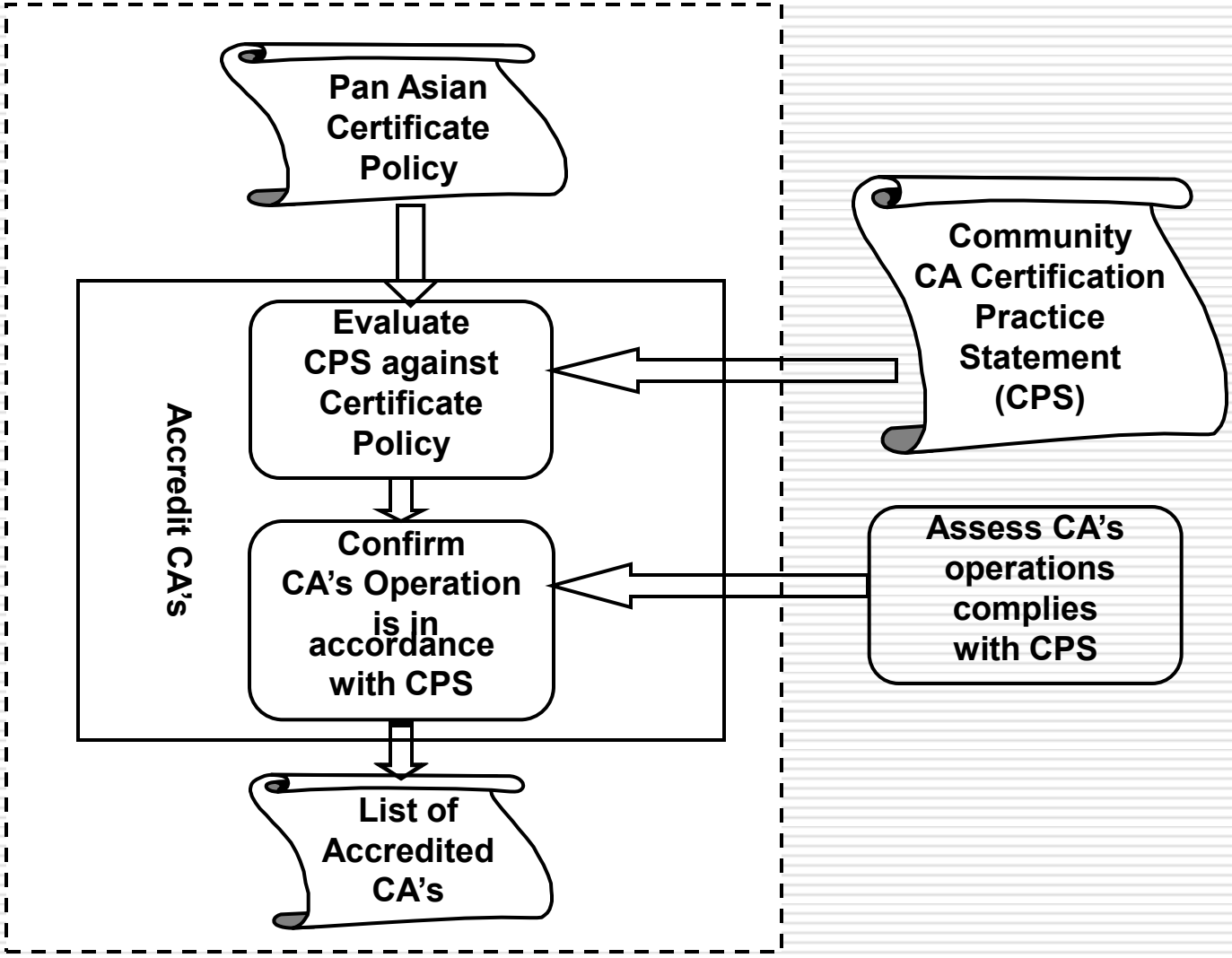
- 3. Revocation of recognition
  - The Authority's official web site will be updated to indicate revocation
  - CTL will be updated to remove the revoked CA

How It Works

Let's see how it works by examining the following:

- Establish the trustworthy framework by the PAA Certificate Authority
- Trust the framework by the members of PAA
- How the trust is established in PAA transactions

Process for Mutual PKI Recognition – Certificate Policy Authority



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

Certificate Authority (CA) related documents

PAA has Certificate Policy Authority Ltd. to authorize CA of each economy as Conforming CA that complies the common standard required as CA of PAA, leveling their Certification Practice Statement (CPS) etc.

(1) Certificate Policy

- Common Certificate Policy prepared by the Certificate Policy Authority that contains the set of rules that govern the issuance and use of digital certificates, and indicate the applicability of the certificates to the communities within PAA.
- It specifies Audit procedure, Revocation, Records archival and Certificate & CRL (Certificate Revocation List) Profiles, etc.
- This is the basis of the Mutual Recognition of Public Key Infrastructure that form a part of conditions for periodical assessment of CA, and each CA will need to ensure that their CPS complies with this Certificate Policy.

(2) Certificate Policy Authority Terms of Reference

This document is to facilitate the process of mutual recognition of the Public Key Infrastructures adopted by each PAA Service Provider under Certificate Policy.

(3) CA Recognition Agreement

- Agreement between Certificate Policy Authority Ltd. and each Certificate Authority contracted by PAA Service Provider in each economy.
- Under this agreement Certificate Policy Authority recognize that the applicant CA is a conforming or accredited CA of PAA.
- Frequency of assessment to have, fees and other details are defined in this Agreement.

(4) CA / CPS (Certification Practice Statement) Recognition Procedure

This document defines the procedure to be used by the Certificate Policy Authority to give recognition to the individual Certification Practice Statement (CPS) and Certificate.

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

1. Studies were carried out on the following:

- PAA members' security requirements (authentication, non-repudiation, message integrity, confidentiality)
- The legal framework of different countries regulating CA practices (other ref: Report On Legal Issues in Cross Border E-Commerce Transactions by Asia PKI Forum –Appendix 3A)

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

1. Studies were carried out on the following:

Mutual Recognition - CPS Comparison Framework

Item	Major Components	Korea : TradeSign (CA), KTNET (ASP)	Hong Kong : Digi-Sign (CA), Tradelink (ASP)	Taiwan : TaiCA (CA), TradeVan (ASP)	Singapore : ID.Safe (CA), SNS (ASP)
	General Provisions				
1.	Standards for CPS	Internet X.509 PKI Certificate Policy and Certification Practices	Based on the framework in the Code of Practice. The framework is in turn based on the IETF RFC 2527 standard.	Internet X.509 PKI Certificate Policy and Certification Practices (IETF RFC 2527)	Internet X.509 PKI Certificate Policy and Certification Practices
2.	Obligations	CA obligations, RA obligations, Subscriber obligations, Relying Party obligations, Repository obligations	CA obligations, Subscriber obligations, Relying Party obligations, Repository obligations	CA obligations, RA obligations, User obligations, Relying Party obligations, Repository obligations	ID.Safe obligations, CA obligations, RA obligations, Subscriber obligations, Relying Party obligations, Repository obligations
3.	Liability Per Certificate	Depending on grade of certificate and applied business transaction. 100 times of annual subscription fee. Omission resulting from negligence or breach of reasonable care and skill. General liability in Jan 2001.	Max HK$1.5 million per certificate to cover errors, omissions resulting from negligence or breach of reasonable care and skill.	Responsible for error or omissions: B2B Certificate : Max. NT$ 250,000	Limitation of liability may vary and are described within relevant contractual documents. In general S$5000 per certificate.
4.	Arbitration	Appoint arbitrator if failing to resolving a technical dispute within 7 days Mediation by Korea Commercial Arbitration Board in case of domestic problem and by NewYork arbitration committee	Resolve within days from date of notice Mediation in accordance with Mediation Rules Arbitration in accordance with Domestic Arbitration Rules	Apply to registration authority first Taiwan local district court	Mediation Appoint arbitrator if failing to resolving a technical dispute within seven days
5.	Refund Policy	Not applicable.	Not applicable.	Within 7 day is free(may refund)	Not applicable.
6.	Publication and Repository	CPS, certificates, subscriber list, CRL, CA public keys	CPS, certificates, subscriber list, CRL, CA public keys	Certificates, revoked certificates, CA certificates, Root CA certificate, cross certify certificates	CPS, certificates, revoked certificates, notices of suspension and expiry
7.	X.500 Directory	24 hours a day, 7 days a week	24 hours daily except 2 hours	24 hours a day, 7 days a week	24 hours a day, 7 days a

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

1. Studies were carried out on the following:

- International standards / guidelines on PKI (e.g. Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce published by eSecurity Task Group of APEC TEL Working Group)

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

2. The following aspects were explored and considered:

- CA has to be licensed / governed / recognized under its local jurisdiction
- Keys should only be used for digital signature but not for encryption (i.e. keys for encryption are out of scope, separate keys for signing and encryption is needed)
- Maintain a Certificate Trust List for approved CA (why? how?)

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

2. The following aspects were explored and considered:

- Face-to-face identity authentication of subscriber needed?
- Explore OCSP to provide certificate status information (timeliness, single point, simplify the retrieval)
- Limitation of liability and the reliance limit of certificates (trading vs financial)

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

2. The following aspects were explored and considered:

- The governing law to be agreed upon for interpretation and enforcement
- The compliance audit process (part of the requirement for recognition)
- Privacy and confidentiality policy (e.g. ID card numbers stored in the certificate should be encrypted)

Establish the trustworthy framework

A. Defining the PAA Certificate Policy

2. The following aspects were explored and considered:

- Subject name (DN) on a certificate must not be blank
- Central key generation and end user key generation (secure delivery vs proof of possesion of private key)
- Maximum validity period of certificate (e.g. 3 years)

Trust the framework

What next if we have the trustworthy framework in place?

- CA of different regions seek recognition from this framework
- The Authority publishes its list of recognized CAs in the CTL
- PAA members obtain and trust the CTL
- By the chain of trust, the digital signature generated by certificates issued by CAs under the CTL are trusted by the PAA members (both local and foreign to the CA)