

# CAREC e-CERT Hub

Pilot Project on Electronic Exchange and Mutual Recognition  
of Product Conformity Certificates / Test Reports  
in the CAREC Region

## Kickoff Workshop

1–2 June 2026 · Incheon, Republic of Korea · TA-10730 REG



**ESCAP**  
Economic and Social Commission  
for Asia and the Pacific



# Session 5

Key Technical, Legal and  
Regulatory Issues

## S5-1. Aligning Key Issues — Six Issue Map

This session aligns the **technical, trust, legal, regulatory, and operational issues** required for CoC/TR electronic exchange, based on **Session 1 global practices and pre-kickoff questionnaire responses**.

<b>1. Document &amp; Data Standards</b>	<b>2. Signature &amp; Trust Verification</b>	<b>3. CAB Authority &amp; Scope</b>
Signed PDF · minimum metadata · document ID · HS/scope · validity alignment — common minimum dataset enables exchange despite differing national formats.	CAB digital signature · Public Key Registry · QR/authenticity link · certificate status - receiving countries may confirm document authenticity and issuing authority.	ISO/IEC 17065 · 17025 · regulator-driven designation · ILAC/IAF status - which CAB and which product scope is to be trusted shapes the pilot scope.
<b>4. Limits of Legal Acceptance</b>	<b>5. Data Lifecycle &amp; Security</b>	<b>6. Operating Rules</b>
e-document status · foreign e-signatures · TR/CoC acceptance · customs use - successful Hub verification should not be mistaken for automatic legal acceptance or customs clearance approval.	Temporary cache · metadata retention · audit logs · access control · cloud/VPN - data sovereignty, retention, and security requirements to be reflected in the Operational Arrangement and SOP.	SOP · exception handling · Focal Point · withdrawal · dispute handling - minimum rules to operate the 24-month pilot safely.

### ● Session Flow — How the Six Issues Are Aligned

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>▪ <b>Technical Standards (S5-2~10)</b></li> </ul>          | Hub concept · architecture · document/metadata standards · core functions · security   |
| <ul style="list-style-type: none"> <li>▪ <b>Trust Verification (S5-6, S5-7, S5-10)</b></li> </ul> | Public Key Registry · CAB authority · authenticity support modules                     |
| <ul style="list-style-type: none"> <li>▪ <b>Legal &amp; Regulatory (S5-11~14)</b></li> </ul>      | Phased approach · S1 case-based issue translation · e-Apostille analogy · check points |
| <ul style="list-style-type: none"> <li>▪ <b>Operations &amp; Rules (S5-15~17)</b></li> </ul>      | Stage 1 Pilot Operational Arrangement · indicative clauses · follow-up roadmap         |

## S5-2. Hub Concept — Trust Framework, Not a Repository

The CAREC e-CERT Hub is, in essence, **not a document store but a Trust Framework** that makes inter-institutional CoC/TR exchange reliable.

### ✗ The Hub is Not a Repository

- Not a permanent repository for original PDFs
- Not an original document management system for MRA · Pilot Operational Arrangement
- Not a CoC content review / audit system
- Not customs · single-window integration
- Not a simple file transfer or storage service

### ✓ The Hub is a Trust Framework

- Signed PDF + metadata routing · exchange
- Policy rules managed under the Pilot Operational Arrangement / SOP
- Authenticity check based on public keys · CAB status · audit logs
- Inter-agency exchange · status management · transaction tracking
- Trust based on public keys · CAB registry information

### ● Trust Framework

*A Trust Framework is a practical mechanism to confirm who issued the document, whether it is authentic, and under what scope it can be used.*

#### Technical Layer

**Public keys · digital signatures · verification**  
 → Confirms that the document has not been altered and was issued by a registered body.

#### Policy Layer

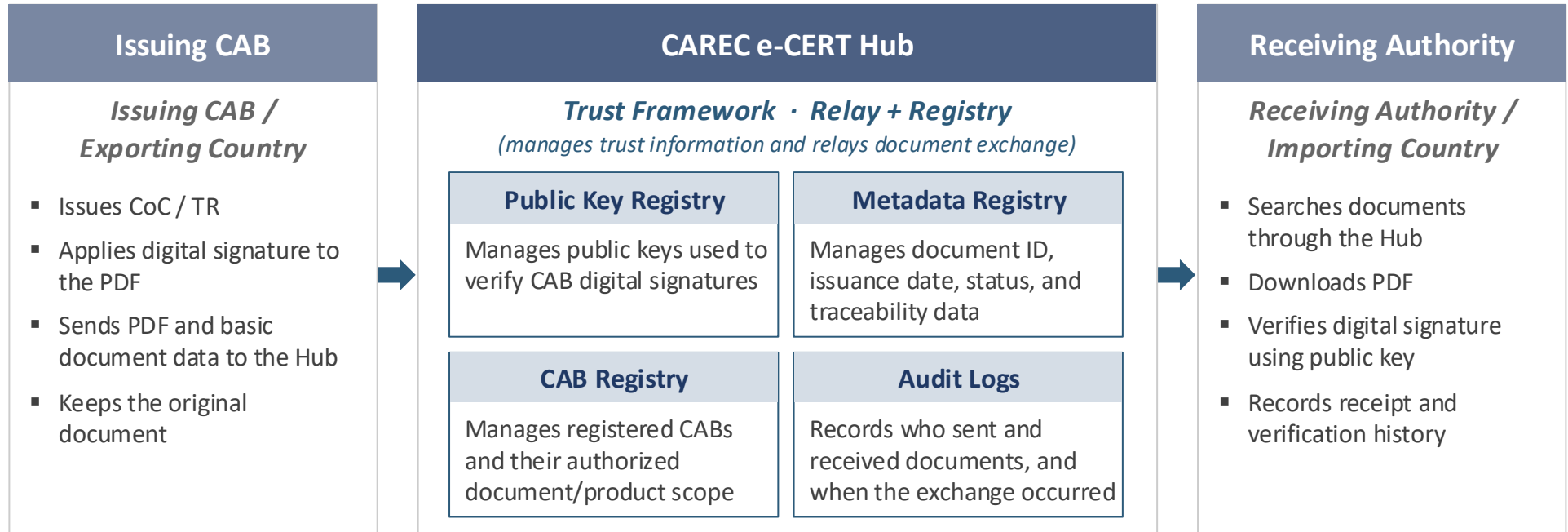
**SOP · CAB registration requirements · document scope**  
 → Defines in advance which institutions and documents can be exchanged.

#### Governance Layer

**ADB · KTNET · participating institutions · Pilot Operating Committee**  
 → Coordinates issues, consultations, and operational decisions during the pilot.

## S5-3. Technical Architecture Overview

The Hub is **not a repository for original PDFs**; it **manages trust information and relays document exchanges** so that authenticity and issuing authority can be verified.



### ● Two Architectural Layers

#### Trust Information Layer

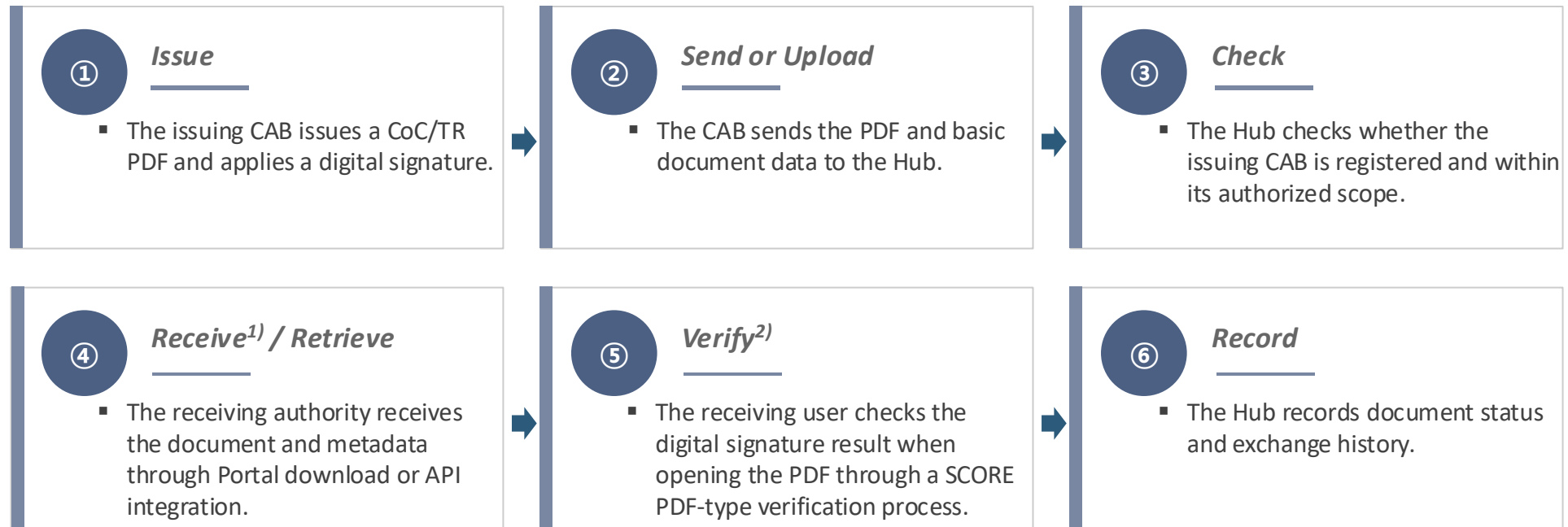
The Hub manages public keys, CAB information, document metadata, and exchange logs.

#### Original Document Layer

The signed PDF remains with the issuing CAB; the Hub only relays or temporarily caches it during the exchange.

## S5-4. CoC/TR Exchange and Verification upon PDF Opening

The pilot exchange is not a simple PDF transfer; it is a **six-step trust-checking process** where the Hub provides issuing-authority and public-key information, the receiving authority receives the document via Portal or API, and the digital signature result is checked when the PDF is opened.



1) **Note:** With API integration, the document can be delivered to the importing country's legacy system.

2) **Note:** The verification result is reference information; final acceptance follows the importing country's rules.

## S5-5. Common Document and Metadata Standards

For the pilot, a **hybrid approach using signed PDFs and a minimum metadata set** is more practical than full XML structuring.

### Limits of Full XML Structuring

*Applicable standards and test items vary by HS code · product - full XML structuring\* within the pilot is excessive.*

HS 0813	Dried fruit	Agricultural inspection standards
HS 8516	Heaters	IEC 60335 safety standards
HS 8517	Telecom equipment	EMC · safety standards
HS 6203	Clothing	Textile safety standards

**\* Reason: Multiple HS × national standard differences**  
**→ excessive XML schema standardization burden**

### Project Choice — Hybrid Approach

#### *Signed PDF + Minimum Viable Dataset (MVD)*

- **PDF (Original)**  
 Issuing CAB applies a digital signature to the PDF.  
 Detailed technical profile to be confirmed at design stage.
- **Metadata**  
 Issuing authority · HS code · issuance date — minimum common dataset
- **Public Key**  
 Pre-registered in the Hub Public Key Registry
- **Verification**  
 The receiving user checks the PDF signature result when opening the file; the Hub provides CAB authority, status, and public-key trust information.

**→ A common exchange structure that works despite HS-level differences**

## S5-6. Core Trust and Exchange Functions

The Hub **does not approve the document itself**; it **provides the trust information** needed to check who issued it, whether the signature is valid, and whether the CAB is authorized for the product scope.

### Document Exchange

Receives and shares signed PDFs and metadata through the Hub

- PUSH upload by the issuing CAB
- Search / retrieve by the receiving authority
- Status and history tracking

### Public Key Registry

Registers and manages CAB X.509 certificates used to verify digital signatures

- New certificate registration
- Certificate update / renewal
- Revocation

### Authenticity Support

Provides trust information used when the receiving user opens the PDF and checks the signature result

- Public key information
- CAB registration and validity status
- Audit log reference

### Policy & Scope Management

Manages which CAB is authorized to issue which document type for which product scope

- CAB authority mapping
- Product / document scope
- Approved CAB list

## S5-7. Hub Verification - In Scope vs Out of Scope

The Hub supports authenticity and authority verification, but does not substitute for product quality judgment, test result re-evaluation, customs clearance decisions, or legal acceptance.

### Supported / Provided by the Hub

#### *Trust-based functions managed by the Hub*

- **CAB Registration Status**  
Whether the issuing CAB is currently registered and active in the Hub
- **Public Key Validity**  
Whether CAB public keys are registered and within validity
- **Document Metadata Completeness & Consistency**  
Completeness and consistency of metadata records
- **Exchange Logs**  
Audit trail of all exchange events, accessible to participating institutions
- **Scope Mapping**  
Whether issuing CAB document types / product scope are registered

### Out of Scope for the Hub

#### *Decisions remaining with the importing authority*

- **Product Quality Itself**  
The Hub does not assess whether a product meets quality criteria
- **Technical Content of Test Results**  
The Hub does not re-evaluate or re-interpret test results
- **Customs Clearance Decision**  
Customs clearance decisions remain with national customs authorities
- **Legal Acceptance by the Importing Country**  
Import acceptance is decided under the importing country's rules
- **Full MRA Recognition**  
The Hub does not constitute a treaty-level mutual recognition agreement

## S5-8. Data Retention Model — Minimum Storage, Clear Responsibility

The pilot uses **Model A as the baseline**: original PDFs are **temporarily cached and deleted**, while metadata, verification evidence, PKI data, and audit logs are **retained under the Operational Arrangement and SOP**.

### Pilot Baseline: Model A — Hub-mediated exchange + temporary cache

<b>Model A</b> [Recommended for Pilot]	<b>Model B</b> [Not Recommended for Pilot]	<b>Model C</b> [Future Option]
<b>Temporary Relay</b> <ul style="list-style-type: none"> <li>• CAB → Hub temporary cache → Receiving Authority</li> <li>• PDF is deleted after receipt, as defined in the SOP</li> <li>• Minimizes storage and reduces data-sovereignty concerns</li> </ul>	<b>Long-Term Hub Storage</b> <ul style="list-style-type: none"> <li>• CAB → Hub long-term storage ← Receiving Authority</li> <li>• Strong traceability, but high data-sovereignty concern</li> </ul>	<b>Metadata-Only Reference</b> <ul style="list-style-type: none"> <li>• Hub stores metadata only; PDF remains on CAB server</li> <li>• Lightweight model, but requires CAB servers to be always available</li> </ul>

Note: Model A defines how the PDF is handled; the five data layers define what the Hub deletes, retains, and manages under the SOP.

### ● Five Data Layers under Model A — What is Deleted, What is Retained

L1	L2	L3	L4	L5
<b>Signed PDF</b> Temporarily cached, then deleted under the Pilot Operational Arrangement / SOP	<b>Metadata</b> Basic document information retained as defined in SOP	<b>Signature / Hash Evidence</b> Verification evidence retained for authenticity checks	<b>PKI Validation Data</b> Certificate, CRL, OCSP, TST data for long-term verification	<b>Audit Logs</b> Exchange history retained for traceability and accountability

## S5-9. Integration Options — API & Portal

The pilot supports **both API integration and Hub Portal access**, so each participating country can join according to its technical readiness, while deployment will be confirmed based on data protection and security requirements.

### Deployment Options

#### Option 1 · Public Cloud — priority option for pilot review

- **Example:** AWS Seoul / Azure / GCP
- **Build:** Fast (weeks-scale) | usage-based pricing
- **Scalability:** High (auto-scaling)
- **Data Sovereignty:** Region selection · access controls mitigate concerns

#### Option 2 · Private Cloud

- **Example:** Dedicated IDC · VPC isolation
- **Build:** Longer setup | fixed cost
- **Scalability:** More limited
- **Data Sovereignty:** Stronger direct control

### Integration Mode

#### Mode A · REST API Integration (for technically ready institutions)

- **Target:** CABs or agencies with system integration capacity
- **Function:** Automated PUSH registration and batch processing
- **Data:** Automated metadata synchronization
- **Tools:** OpenAPI 3.0 and Swagger Sandbox

#### Mode B · Hub Portal Manual Entry (baseline option for all participants)

- **Target:** All participating institutions, including portal-first users
- **Function:** PDF upload and metadata entry through the Hub Portal
- **Access:** 2FA login
- **Tools:** Multilingual UI planned, including English and Russian

## S5-10. Security · Digital Signature · Technical Profile

2FA, digital signature, and technical profile **serve different purposes**: user login security, PDF authenticity verification, and signature specification. They **do not replace legal acceptance or customs clearance decisions**.

<div style="text-align: center;"> <span style="font-size: 2em; font-weight: bold; border: 1px solid white; border-radius: 50%; padding: 5px 15px;">1</span> </div> <div style="text-align: center;"> <b>2FA</b>                      (Two-Factor Authentication)                 </div>	<div style="text-align: center;"> <span style="font-size: 2em; font-weight: bold; border: 1px solid white; border-radius: 50%; padding: 5px 15px;">2</span> </div> <div style="text-align: center;"> <b>Digital Signature</b>                      (Electronic Signature)                 </div>	<div style="text-align: center;"> <span style="font-size: 2em; font-weight: bold; border: 1px solid white; border-radius: 50%; padding: 5px 15px;">3</span> </div> <div style="text-align: center;"> <b>Technical Profile</b>                      (Signature Specification)                 </div>
<p><b>Portal access security</b></p> <hr/> <ul style="list-style-type: none"> <li>▪ <b>Purpose</b> Secures user login to the Hub Portal</li> <li>▪ <b>What it does</b> Confirms the user’s identity with password + OTP</li> <li>▪ <b>Not the same as</b> PDF digital signature</li> <li>▪ <b>Applied to</b> All Hub Portal users</li> </ul>	<p><b>PDF authenticity verification</b></p> <hr/> <ul style="list-style-type: none"> <li>▪ <b>Purpose</b> Verifies that the PDF has not been altered and was signed by the issuing CAB</li> <li>▪ <b>What it does</b> Allows the receiving user to check whether the PDF is unchanged and was signed by the registered CAB</li> <li>▪ <b>Not the same as</b> Portal login authentication</li> <li>▪ <b>Applied to</b> CoC/TR PDF issued by the CAB</li> </ul>	<p><b>Digital signature specification</b></p> <hr/> <ul style="list-style-type: none"> <li>▪ <b>Purpose</b> Defines the common technical rules for creating and verifying the digital signature</li> <li>▪ <b>What it includes</b> PADES · RSA-SHA256 · X.509 v3, etc.</li> <li>▪ <b>Not changed without</b> Joint agreement among participating institutions</li> <li>▪ <b>Confirmed at</b> Pilot design stage</li> </ul>

## S5-11. Why a Step-by-Step Approach

For the 24-month pilot, the realistic starting point is a **limited Pilot Operational Arrangement, not a Full MRA**. Trust can then be built **step by step through actual exchange and validation**.

### 24-Month Project Constraint

- The pilot should focus on what can be agreed, tested, and validated within 24 months.
- A formal MRA or legal mutual recognition may require country-specific diplomatic, administrative, or legislative procedures.

### Different Readiness Levels

- Participating countries have different levels of digital systems, CAB structures, and customs integration.
- A limited pilot allows all countries to participate without requiring full MRA readiness from the beginning.

### Trust Takes Time

- Trust cannot be created by technology alone.
- Testing and certification procedures, as well as legal acceptance by the importing country, require separate consultations.

### Start Small, Then Expand

- Session 1 global practices and selected MRA cases show that many recognition systems start with limited scope and expand gradually.

## S5-12. CAREC Pilot Issues Derived from Session 1 Global Practices

Session 1 global practices are **not models to copy directly**; they help identify the **document, trust, CAB, data, and operating issues that must be aligned** for the CAREC pilot.

<p><b>① Document &amp; Metadata Standards</b></p> <ul style="list-style-type: none"> <li>• <b>Common data and verification rules needed</b> → Signed PDF + MVD + API/Portal</li> </ul>	<p><b>② Legal Limits of Hub Verification</b></p> <ul style="list-style-type: none"> <li>• <b>Authenticity verification is not legal acceptance</b> → Hub verification is reference information; final acceptance follows importing-country rules</li> </ul>	<p><b>③ CAB Authority &amp; Product Scope</b></p> <ul style="list-style-type: none"> <li>• <b>CAB authority and product scope must be clear</b> → CAB Registry + Scope Annex</li> </ul>
<p><b>④ Temporary Cache · Logs · Retention</b></p> <ul style="list-style-type: none"> <li>• <b>Retention and security rules must be defined</b> → Operational Arrangement + SOP</li> </ul>	<p><b>⑤ Exceptions · Liability · Disputes</b></p> <ul style="list-style-type: none"> <li>• <b>Exceptions, liability, and disputes need operating rules</b> → Focal Point consultation + SOP</li> </ul>	<p><b>⑥ S1 → S5 Connection Principle</b></p> <ul style="list-style-type: none"> <li>• <b>S1 provides reference lessons</b> → Country conditions confirmed through Focal Points → Reflected in the Operational Arrangement, SOP, and annexes</li> </ul>

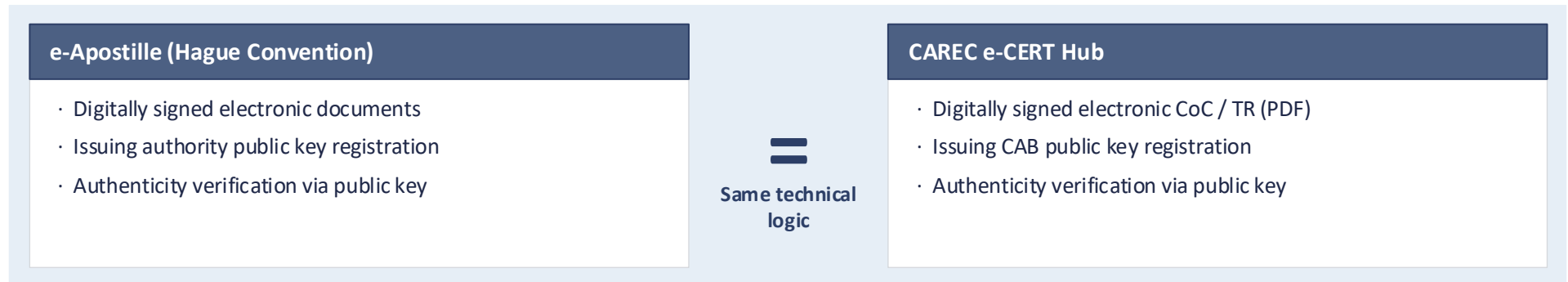
### ● Gradual Alignment Pathway — From Global Lessons to Pilot Operating Rules



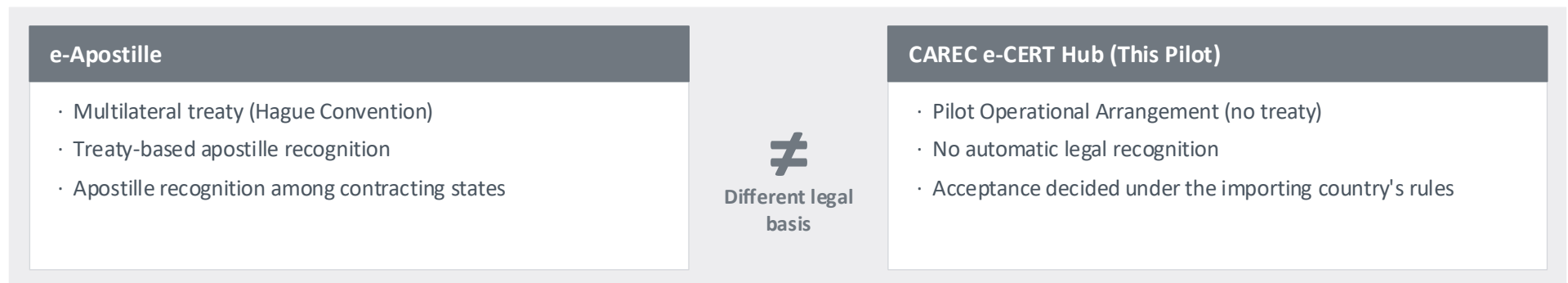
## S5-13. e-Apostille Analogy — Authenticity Logic Only

The e-Apostille analogy is **limited to public-key-based authenticity verification logic** and **does not apply as a legal recognition model** for the CAREC pilot.

✓ **APPLIES** — Public-key-based authenticity verification



✗ **DOES NOT APPLY** — Treaty-based legal recognition



**Conclusion — We borrow the verification logic, not the legal recognition effect.**

## S5-14. Legal & Regulatory Review Points

This review **does not decide legal feasibility upfront**; it **identifies the conditions and constraints that each country must confirm** for the Stage 1 Pilot Operational Arrangement.

### ● Six Review Questions

**Q1** Authorized signing institution / signatory?

Which institution and position can sign the Stage 1 Pilot Operational Arrangement under each country's internal process?

**Q3** Conflicts with existing MRAs or bilateral cooperation?

Does the pilot align with existing ILAC MRA, IAF MLA, APEC TEL MRA, or bilateral arrangements?

**Q5** Applicability of Rolling Signature?

Can countries sign sequentially, and what happens if one signature is delayed?

**Q2** Roles of NSB · AB · CAB · Customs?

How are standards, accreditation, CAB, and customs roles divided in each country?

**Q4** EAEU · WTO · data protection · e-signature variables?

What external legal, regulatory, data protection, or e-signature requirements must be considered?

**Q6** Clauses to include in the Pilot Operational Arrangement?

Which clauses are needed on liability, withdrawal, data protection, disputes, personal data, and governing law?

### ● How Results Will Be Used

**Pilot Operational Arrangement**

Refine clauses and annexes

**CAB List**

Confirm accreditation status and signing authority

**SOP Design**

Reflect country-specific constraints

**Data & Liability Clauses**

Reflect data protection and dispute-handling requirements

*Note: For discussion only — final positions are subject to each country's internal review and focal point consultation.*

## S5-15. Stage 1 — Pilot Operational Arrangement Details (Tentative)

The Stage 1 arrangement is a **limited administrative arrangement for safe pilot operation** — not a treaty, not a Full MRA, and not automatic legal recognition.

Stage 1 = Minimum administrative arrangement for safe pilot operation

### Administrative Arrangement

Administrative understanding, not an international treaty

### Authorized Institution Signing

Specific signatories and the method of giving effect to the arrangement are subject to each country's internal approval process

### 24-Month Limit

24 months from contract effectiveness; detailed dates aligned with the approved work plan; renewal requires mutual agreement

### Withdrawal Possible

60 days' prior written notice; no impact on other participating institutions

 **Not a treaty** · **Not a Full MRA** · **No automatic legal recognition**

## S5-16. Pilot Operational Arrangement — Indicative Clauses

The clause structure is a **discussion draft** that translates the pilot's legal, technical, data, liability, governance, and annex issues **into operating rules**.

A. Pilot Scope & Roles	B. Exchange & Trust Rules	C. Governance & Annexes
<p><b>1 Purpose &amp; Scope</b> Pilot purpose, participants, and document types</p> <p><b>2 Institutional Roles</b> ADB, KTNET, standards bodies, CABs, receiving authorities</p>	<p><b>3 Document Exchange Rules</b> Signed PDF, metadata, exchange flow, temporary cache</p> <p><b>4 Digital Signature &amp; Public Key Registration</b> CAB list, authority scope, certificates, public keys</p> <p><b>5 Data Protection &amp; Security</b> Retention, audit logs, access control, data protection</p>	<p><b>6 Liability &amp; Limits</b> No product-quality judgment, no customs decision, Non-Prejudice</p> <p><b>7 Duration · Withdrawal · Renewal</b> 24-month pilot, notice period, renewal possibility</p> <p><b>8 Dispute Handling &amp; Governance</b> Pilot Operating Committee, consultation, issue escalation</p> <p><b>9 Annexes</b> Product scope, CAB list, technical profile, SOP, metadata set</p>

**Note: Four pilot acceptance principles:** ① ILAC/IAF equivalence review, ② Designated authority, including regulator-driven designation, ③ Document-type flexibility (CoC / TR / both), ④ Non-Prejudice (importing country's law prevails)

## S5-17. Follow-up Roadmap — Beyond This Project

Stages 2 and 3 are **not project deliverables**; they are **optional follow-up pathways** that countries may review after pilot results are validated.

**⚠ Stages 2 and 3 are not direct outputs of this project — follow-up pathways for participating-country review after the pilot**



*Commitment level decreases from left to right — **only Stage 1 is delivered by this project.***

## S5 Key Messages

S5 concludes that the Hub should operate as a **Trust Framework**, and legal-regulatory issues should be **aligned gradually through the Stage 1 Pilot Operational Arrangement and SOP**.

### S5. Key Technical, Legal and Regulatory Issues

- 1 The Hub is a Trust Framework, not a repository**  
It supports signed PDF and metadata exchange, public keys, CAB authority checks, and audit logs under Model A.
- 2 Focus on Stage 1 — not a Full MRA**  
The pilot starts with a 24-month administrative arrangement; Stages 2 and 3 remain future options.
- 3 Avoid categorical legal claims**  
Legal feasibility, acceptance, and required procedures are subject to each country's internal review.

→ Next session (S6): Synthesis and Next Steps

Thank You · 감사합니다 · Rahmat · Спасибо · شكراً

— With participation and cooperation of 5 countries, opening a new chapter in CAREC digital trade together —



**ESCAP**  
Economic and Social Commission  
for Asia and the Pacific

**25**  
**CAREC**  
Central Asia Regional  
Economic Cooperation



**KOREA**  
e-Asia Fund