

# CAREC e-CERT Hub

Пилотный проект по электронному обмену и взаимному признанию сертификатов соответствия и протоколов испытаний в регионе ЦАРЭС

## Вводный семинар

1–2 июня 2026 г. · Инчхон, Республика Корея · TA-10730 REG



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



# Сессия 5

Основные технические, правовые и  
нормативные вопросы

## S5-1. Согласование ключевых вопросов — карта шести проблем

В рамках данной сессии согласовываются **технические, правовые, нормативные и операционные вопросы, а также вопросы доверия**, необходимые для CoC/TR, на основе **международных практик сессии S1 и ответов на предварительную анкету**.

<b>1. Стандарты документов и данных</b>	<b>2. Верификация подписи и доверие</b>	<b>3. Полномочия и охват ОПС</b>
Подписанный PDF · минимальные метаданные · идентификатор документа · ТН ВЭД/охват · согласование срока действия — общий минимальный набор данных обеспечивает обмен при различных национальных форматах.	Цифровая подпись ОПС · реестр открытых ключей · QR-код/ссылка для проверки подлинности · статус сертификата — принимающие страны могут подтверждать подлинность документа и полномочия органа-эмитента.	ISO/IEC 17065 · 17025 · назначение регулятором · статус ILAC/IAF — определение того, каким ОПС и по какому охвату продукции следует доверять, формирует рамки пилота.
<b>4. Пределы правового признания</b>	<b>5. Жизненный цикл данных и безопасность</b>	<b>6. Операционные правила</b>
Статус электронных документов · иностранные электронные подписи · протоколы испытаний/CoC принятие · таможенное применение — успешная верификация через Хаб не означает автоматического правового признания или одобрения таможенного оформления.	Временное кэширование · хранение метаданных · журналы аудита · контроль доступа · облако/VPN — требования к суверенитету данных, срокам хранения и безопасности подлежат отражению в операционном соглашении и СОП.	СОП · порядок работы с исключениями · национальный координатор · выход · урегулирование споров — минимальный набор правил для безопасной реализации 24-месячного пилотного проекта.

### ● Структура сессии — согласование шести вопросов

<ul style="list-style-type: none"> <li>▪ <b>Технические стандарты (S5-2–10)</b></li> </ul>	Концепция Хаб · архитектура · стандарты документов/метаданных · ключевые функции · безопасность
<ul style="list-style-type: none"> <li>▪ <b>Верификация доверия (S5-6, S5-7, S5-10)</b></li> </ul>	Реестр открытых ключей · полномочия ОПС · модули поддержки проверки подлинности
<ul style="list-style-type: none"> <li>▪ <b>Правовые и нормативные вопросы (S5-11–14)</b></li> </ul>	Поэтапный подход · трансляция вопросов на основе кейсов S1 · аналогия e-Apostille · контрольные точки
<ul style="list-style-type: none"> <li>▪ <b>Операции и правила (S5-15–17)</b></li> </ul>	Операционное соглашение по пилоту первого этапа · ориентировочные положения · дорожная карта последующих действий

## S5-2. Концепция Хаба — механизм доверия, а не репозиторий данных

CAREC e-CERT Hub по своей сути **представляет собой не хранилище документов, а систему доверия**, обеспечивающую надёжный обмен CoC/TR между учреждениями.

### ✗ Хаб — не хранилище

- Не является постоянным хранилищем оригинальных PDF
- Не является системой управления оригинальными документами для СВП · операционного соглашения
- Не является системой CoC контентного аудита
- Не является интеграцией с таможней / единым окном
- Не является просто сервисом передачи или хранения файлов

### ✓ Хаб — механизм доверия

- Подписанный PDF + маршрутизация метаданных · обмен
- Управление нормативными правилами в рамках операционного соглашения / СОП
- Проверка подлинности на основе открытых ключей · статус ОПС · журналы аудита
- Межведомственный обмен · управление статусом · отслеживание транзакций
- Доверие на основе открытых ключей · данных реестра ОПС

### ● Механизм доверия

*Под системой доверия понимается практический механизм, обеспечивающий подтверждение органа, выдавшего документ, его подлинности, а также допустимой области его применения.*

#### Технический уровень

Открытые ключи · цифровые подписи · верификация

→ Подтверждается, что документ не был изменен и выдан зарегистрированным органом.

#### Нормативный уровень

СОП · требования к регистрации ОПС · охват документов

→ Заранее определяется перечень учреждений и документов, допускаемых к обмену.

#### Уровень управления

АБР · КТNET · участвующие органы · Руководящий комитет

→ Обеспечивается координация вопросов, консультаций и операционных решений в рамках пилотного проекта.

## S5-3. Обзор технической архитектуры

Хаб не является хранилищем оригинальных PDF; посредством него **обеспечиваются управление доверительной информацией и передача документов** для целей проверки подлинности и полномочий выдающего органа.



### ● Два архитектурных уровня

#### Уровень информации о доверии

Посредством Хаба обеспечивается ведение открытых ключей, информации об органах по оценке соответствия, метаданных документов и журналов обмена.

#### Уровень оригинального документа

Подписанный PDF-документ сохраняется у выдавшего его органа по оценке соответствия, тогда как Хаб используется исключительно для передачи или временного кэширования документа в ходе обмена.

## S5-4. Обмен CoC/TR и верификация при открытии PDF

Обмен в рамках пилота — это не простая передача PDF, а **шестиэтапная процедура проверки доверия**, в ходе которой посредством Хаба предоставляются сведения об органе-эмитенте и открытом ключе, принимающий орган получает документ через портал или API, а результат цифровой подписи проверяется при открытии PDF.



*1) Примечание: При наличии API-интеграции документ может передаваться в действующую систему страны-импортера.*

*2) Примечание: Результат проверки носит справочный характер; окончательное принятие осуществляется в соответствии с правилами страны-импортера.*

## S5-5. Единые стандарты документов и метаданных

Для нужд пилота гибридный подход на основе подписанных PDF и минимального набора метаданных является более практичным, чем полная XML-структуризация.

### Ограничения полной XML-структуризации

*Применимые стандарты и испытываемые параметры различаются в зависимости от кода ТН ВЭД · продукции — полная XML-структуризация\* в рамках пилота избыточна.*

HS 0813	Сухофрукты	Стандарты агрохимического контроля
HS 8516	Обогреватели	Стандарты безопасности IEC 60335
HS 8517	Телеком. оборудование	ЭМС · стандарты безопасности
HS 6203	Одежда	Стандарты безопасности текстиля

**\* Причина: Различия в охвате ТН ВЭД × национальных стандартов → чрезмерная нагрузка на стандартизацию XML-схем**

### Выбор проекта — гибридный подход

*Подписанный PDF + минимально необходимый набор данных (MVD)*

- **PDF (оригинал)**  
Орган-эмитент применяет к PDF цифровую подпись. Подробный технический профиль подлежит определению на этапе проектирования.
- **Метаданные**  
Орган-эмитент · код ТН ВЭД · дата выдачи — минимальный общий набор данных
- **Открытый ключ**  
Предварительно зарегистрирован в реестре открытых ключей Хаба
- **Верификация**  
Пользователь на стороне получателя проверяет результат подписи PDF при открытии файла; посредством Хаба предоставляются данные о полномочиях ОПС, его статусе и доверенном открытом ключе.

**→ Единая структура обмена, работающая независимо от различий на уровне ТН ВЭД**

## S5-6. Основные функции доверия и обмена

Хаб не является инструментом одобрения документа; он предоставляет информацию о доверии, необходимую для проверки того, кто выдал документ, действительна ли подпись и уполномочен ли ОПС по данному охвату продукции.

### Обмен документами

Приём и передача подписанных PDF и метаданных через Хаб

- PUSH-загрузка органом-эмитентом
- Поиск / извлечение принимающим органом
- Отслеживание статуса и истории

### Реестр открытых ключей

Регистрация и управление сертификатами X.509 ОПС для верификации цифровых подписей

- Регистрация нового сертификата
- Обновление / продление сертификата
- Отзывы

### Поддержка проверки подлинности

Предоставляет информацию о доверии, используемую при открытии PDF принимающим пользователем и проверке результата подписи

- Данные открытого ключа
- Статус регистрации и действительности ОПС
- Обращение к журналу аудита

### Управление правилами и охватом

Управляет распределением полномочий ОПС по типам документов и охвату продукции

- Распределение полномочий ОПС
- Охват продукции / документов
- Перечень одобренных ОПС

## S5-7. Верификация через Хаб — процессы в рамках и вне рамок функций

Хаб предназначен для обеспечения проверки подлинности документов и полномочий органов, осуществляющих выдачу, однако его использование не предусматривает замену процедур оценки качества продукции, пересмотра результатов испытаний, таможенного оформления или юридического признания документов.

### Функции, поддерживаемые / предоставляемые Хабом

#### *Функции на основе доверия, управляемые Хабом*

- **Статус регистрации ОПС**  
Наличие действующей регистрации органа-эмитента в Хаб
- **Действительность открытого ключа**  
Наличие регистрации открытых ключей ОПС и их действительность
- **Полнота и согласованность метаданных документа**  
Полнота и внутренняя согласованность записей метаданных
- **Журналы обмена**  
Журнал аудита всех событий обмена, доступный участвующим органам
- **Соответствие охвату**  
Наличие регистрации типов документов / охвата продукции органа-эмитента

### Вне функций Хаба

#### *Решения, остающиеся за принимающим органом*

- **Качество продукции**  
Оценка соответствия продукции критериям качества в функции Хаба не входит
- **Техническое содержание результатов испытаний**  
Повторная оценка и интерпретация результатов испытаний в функции Хаба не входят
- **Решение о таможенном оформлении**  
Решения о таможенном оформлении остаются за национальными таможенными органами
- **Правовое признание страной-импортёром**  
Принятие при импорте осуществляется в соответствии с правилами страны-импортёра
- **Полное признание в рамках СВП**  
Хаб не является соглашением о взаимном признании на уровне международного договора

## S5-8. Модель хранения данных — минимальный объём, чёткое распределение ответственности

В рамках пилота в качестве базовой используется **модель А**: оригинальные PDF временно кэшируются и удаляются, тогда как метаданные, доказательства верификации, данные PKI и журналы аудита **сохраняются в соответствии с операционным соглашением и СОП**.

### Базовый вариант пилота: Модель А — обмен через Хаб + временное кэширование

#### Модель А [Рекомендуется для пилота]

##### Временная ретрансляция

- ОПС → временный кэш Хаба → принимающий орган
- PDF удаляется после получения в соответствии с СОП
- Минимизирует объём хранения и снижает озабоченность вопросами суверенитета данных

#### Модель В [Не рекомендуется для пилота]

##### Долгосрочное хранение в Хабе

- ОПС → долгосрочное хранение Хабе ← принимающий орган
- Высокая прослеживаемость, однако серьёзная озабоченность вопросами суверенитета данных

#### Модель С [Перспективный вариант]

##### Только метаданные

- Хранятся только метаданные; PDF остаётся на сервере ОПС
- Облегчённая модель, однако требует постоянной доступности серверов ОПС

*Примечание: В рамках Модели А определяется порядок обращения с PDF; пятью уровнями данных определяется, что подлежит удалению, хранению и администрированию в Хабе в соответствии с СОП.*

### ● Пять уровней данных в рамках Модели А — что удаляется, что сохраняется

L1	L2	L3	L4	L5
<b>Подписанный PDF</b> Временно кэшируется, затем удаляется в соответствии с операционным соглашением / СОП	<b>Метаданные</b> Основные сведения о документе сохраняются в соответствии с СОП	<b>Доказательство подписи / хэш</b> Доказательства верификации сохраняются для проверки подлинности	<b>Данные валидации PKI</b> Данные сертификата, CRL, OCSP, TST для долгосрочной верификации	<b>Журналы аудита</b> История обмена сохраняется для обеспечения прослеживаемости и подотчётности

## S5-9. Варианты интеграции — API и портал

Пилот поддерживает как API-интеграцию, так и доступ через портал Хаб, что позволяет каждой стране-участнице подключиться в соответствии со своим уровнем технической готовности; выбор варианта развёртывания будет подтверждён с учётом требований к защите данных и безопасности.

### Варианты развёртывания

**Вариант 1 · Публичное облако** — приоритетный вариант для рассмотрения в рамках пилота

- **Пример:** AWS Seoul / Azure / GCP
- **Развёртывание:** Быстрое (в течение нескольких недель) | оплата по факту использования
- **Масштабируемость:** Высокая (автоматическое масштабирование)
- **Суверенитет данных:** Выбор региона · средства контроля доступа позволяют снизить соответствующие риски

### Вариант 2 · Частное облако

- **Пример:** Выделенный ЦОД · изоляция VPC
- **Развёртывание:** Более длительное развёртывание | фиксированная стоимость
- **Масштабируемость:** Ограниченная
- **Суверенитет данных:** Более жёсткий прямой контроль

### Режим интеграции

#### Режим А · Интеграция по REST API (для технически готовых ОПС)

- **Целевая аудитория:** ОПС или ведомства с возможностями системной интеграции
- **Функция:** Автоматическая PUSH-регистрация и пакетная обработка
- **Данные:** Автоматическая синхронизация метаданных
- **Инструменты:** OpenAPI 3.0 и Swagger Sandbox

#### Режим В · Ручной ввод через портал Хаб (базовый вариант для всех участников)

- **Целевая аудитория:** Все участвующие органы, включая пользователей, работающих через портал
- **Функция:** Загрузка PDF и ввод метаданных через портал Хаб
- **Access:** Вход с двухфакторной аутентификацией (2FA)
- **Инструменты:** Запланирован многоязычный интерфейс, включая английский и русский языки

## S5-10. Безопасность · цифровая подпись · технический профиль

Двухфакторная аутентификация (2FA), цифровая подпись и технический профиль **выполняют различные функции:** безопасность входа пользователя, верификация подлинности PDF и спецификация подписи. Они **не заменяют правовое признание и решения о таможенном оформлении.**

<div style="display: flex; align-items: center;"> <div style="border: 1px solid white; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">1</div> <div> <p><b>2FA</b> (двухфакторная аутентификация)</p> </div> </div>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid white; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">2</div> <div> <p><b>Цифровая подпись</b> (электронная подпись)</p> </div> </div>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid white; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">3</div> <div> <p><b>Технический профиль</b> (спецификация подписи)</p> </div> </div>
<p><b>Безопасность доступа к portalу</b></p> <ul style="list-style-type: none"> <li>▪ <b>Цель</b> Обеспечивает безопасность входа пользователя на портал Хаб</li> <li>▪ <b>Назначение</b> Подтверждает личность пользователя посредством пароля + OTP</li> <li>▪ <b>Не то же самое, что</b> Цифровая подпись PDF</li> <li>▪ <b>Применяется к</b> Всем пользователям портала Хаб</li> </ul>	<p><b>Верификация подлинности PDF</b></p> <ul style="list-style-type: none"> <li>▪ <b>Цель</b> Подтверждает, что PDF не был изменён и подписан органом-эмитентом</li> <li>▪ <b>Назначение</b> Позволяет принимающему пользователю проверить, не был ли PDF изменён и был ли он подписан зарегистрированным ОПС</li> <li>▪ <b>Не то же самое, что</b> Аутентификация входа на портал</li> <li>▪ <b>Применяется к</b> PDF CoC/протокол испытаний, выданный ОПС</li> </ul>	<p><b>Спецификация цифровой подписи</b></p> <ul style="list-style-type: none"> <li>▪ <b>Цель</b> Определяет единые технические правила создания и верификации цифровой подписи</li> <li>▪ <b>Содержание</b> PADES · RSA-SHA256 · X.509 v3 и др.</li> <li>▪ <b>Не изменяется без</b> совместного согласования между участвующими органами</li> <li>▪ <b>Подтверждается на</b> этапе проектирования пилота</li> </ul>

## S5-11. Обоснование поэтапного подхода

Для 24-месячного пилота реалистичной отправной точкой является **ограниченное операционное соглашение, а не полноценное СВП**. Доверие выстраивается **поэтапно** — через фактический обмен и валидацию.

### Ограничения 24-месячного проекта

- Пилот должен быть сосредоточен на том, что может быть согласовано, протестировано и подтверждено в течение 24 месяцев.
- Формальное СВП или правовое взаимное признание может потребовать проведения специфических для каждой страны дипломатических, административных или законодательных процедур.

### Различные уровни готовности

- Для стран-участниц характерны различия в уровне развития цифровых систем, организации органов по оценке соответствия и интеграции с таможенными системами.
- Ограниченный пилот позволяет всем странам принять участие без необходимости обеспечивать полную готовность к СВП с самого начала.

### Доверие формируется постепенно

- Доверие не может быть создано исключительно технологическими средствами.
- Процедуры испытаний и сертификации, а также правовое признание со стороны страны-импортёра требуют отдельных консультаций.

### Начать с малого и расширяться

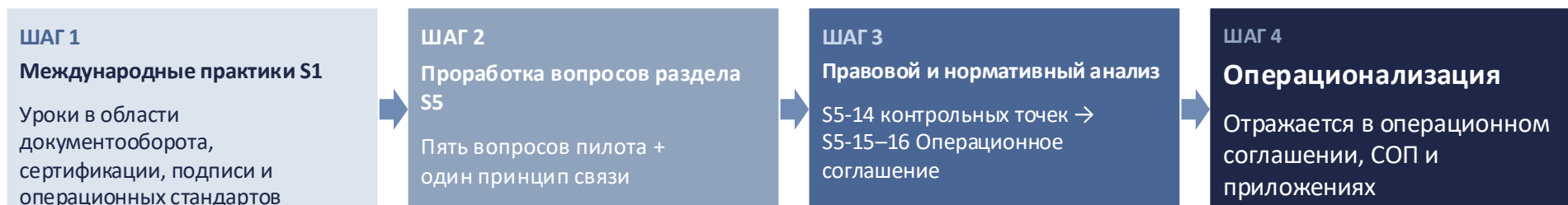
- Международные практики сессии S1 и отдельные примеры СВП демонстрируют, что многие системы признания начинаются с ограниченного охвата и постепенно расширяются.

## S5-12. Вопросы пилота ЦАРЭС, выявленные на основе международных практик сессии S1

Международные практики сессии S1 не являются готовыми моделями для прямого копирования; они помогают выявить вопросы в области документооборота, доверия, ОПС, данных и операционной деятельности, требующие согласования применительно к пилоту ЦАРЭС.

<p><b>① Стандарты документов и метаданных</b></p> <ul style="list-style-type: none"> <li>• <b>Необходимы единые правила верификации и работы с данными</b> → Подписанный PDF + MVD + API/портал</li> </ul>	<p><b>② Правовые пределы верификации через Хаб</b></p> <ul style="list-style-type: none"> <li>• <b>Верификация подлинности не равнозначна юридическому признанию</b> → Верификация через Хаб носит справочный характер; окончательное принятие осуществляется по правилам страны-импортёра</li> </ul>	<p><b>③ Полномочия ОПС и охват продукции</b></p> <ul style="list-style-type: none"> <li>• <b>Полномочия ОПС и охват продукции должны быть чётко определены</b> → Реестр ОПС + Приложение об охвате</li> </ul>
<p><b>④ Временное кэширование · журналы · хранение</b></p> <ul style="list-style-type: none"> <li>• <b>Правила хранения и безопасности подлежат определению</b> → Операционное соглашение + СОП</li> </ul>	<p><b>⑤ Исключения · ответственность · споры</b></p> <ul style="list-style-type: none"> <li>• <b>Исключения, ответственность и споры требуют операционных правил</b> → Консультации с национальными координаторами + СОП</li> </ul>	<p><b>⑥ Принцип связи S1 → S5</b></p> <ul style="list-style-type: none"> <li>• <b>В разделе S1 представлены ориентиры международной практики</b> → Условия стран подтверждаются через национальных координаторов → Отражаются в операционном соглашении, СОП и приложениях</li> </ul>

### ● Поэтапный путь согласования — от международных уроков к операционным правилам пилота



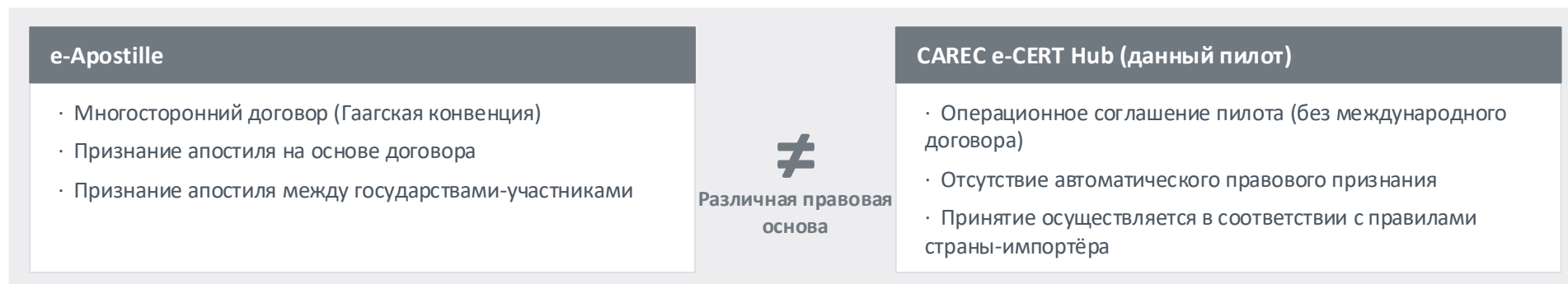
## S5-13. Аналогия e-Apostille — только логика верификации подлинности

Аналогия с e-Apostille **ограничена логикой верификации подлинности на основе открытых ключей** и **не распространяется на правовую модель признания** применительно к пилоту ЦАРЭС.

✓ **ПРИМЕНЯЕТСЯ** — Верификация подлинности на основе открытых ключей



✗ **НЕ ПРИМЕНЯЕТСЯ** — Правовое признание на основе международного договора



**Вывод — Используется логика верификации, но не эффект правового признания.**

## S5-14. Правовые и нормативные контрольные точки

В рамках данного анализа **не принимается предварительное решение о юридической реализуемости; определяются условия и ограничения, которые должны быть подтверждены каждой страной** для Этапа 1 Пилотного операционного соглашения.

### ● Шесть контрольных вопросов

**В1** Уполномоченный подписывающий орган / подписант?

Какой орган и должностное лицо уполномочены подписать операционное соглашение первого этапа в соответствии с внутренними процедурами каждой страны?

**В3** Противоречия с существующими СВП или соглашениями о двустороннем сотрудничестве?

Соответствует ли пилот действующим СВП ILAC, MLA IAF, СВП АРЕС TEL или двусторонним договорённостям?

**В5** Применимость последовательного подписания?

Могут ли страны подписывать последовательно и каковы последствия задержки одной подписи?

**В2** Роли органа по стандартизации · органа по аккредитации · ОПС · таможни?

Как распределены функции в области стандартизации, аккредитации, деятельности ОПС и таможни в каждой стране?

**В4** ЕАЭС · ВТО · защита данных · переменные в области электронной подписи?

Какие внешние правовые, нормативные требования, требования к защите данных или электронной подписи подлежат учёту?

**В6** Положения, подлежащие включению в операционное соглашение?

Какие положения необходимы в части ответственности, выхода, защиты данных, урегулирования споров, персональных данных и применимого права?

### ● Применение результатов

**Операционное соглашение**

Доработка положений и приложений

**Перечень ОПС**

Подтверждение статуса аккредитации и полномочий на подписание

**Разработка СОП**

Учёт специфических ограничений каждой страны

**Положения о данных и ответственности**

Учёт требований к защите данных и урегулированию споров

*Примечание: Только для обсуждения — окончательные позиции определяются по итогам внутреннего рассмотрения каждой страны и консультаций с национальными координаторами.*

## S5-15. Первый этап — детали операционного соглашения (предварительно)

Соглашение первого этапа представляет собой **ограниченную административную договорённость для безопасной пилотной эксплуатации** — не международный договор, не полноценное СВП и не автоматическое правовое признание.

### Этап 1 = Минимальная административная договорённость для безопасной пилотной эксплуатации

#### Административная договорённость

Административное взаимопонимание, а не международный договор

#### Подписание уполномоченным органом

Конкретные стороны, подписывающие соглашение, а также механизм придания ему юридической силы подлежат определению в рамках внутренних процедур утверждения каждой страны.

#### Срок действия: 24 месяца

24 месяца с даты вступления контракта в силу; конкретные сроки согласовываются с утверждённым планом работ; продление требует взаимного согласия

#### Возможность выхода

С предварительным письменным уведомлением за 60 дней; не влияет на другие участвующие учреждения

 Не является договором · Не является полноценным СВП · Не предполагает автоматического правового признания

## S5-16. Операционное соглашение — ориентировочная структура статей

Представленная структура положений носит характер **проекта для обсуждения** и предназначена для преобразования правовых, технических, информационных, управленческих вопросов, вопросов ответственности и приложений пилотного проекта в **операционные правила**.

А. Охват пилота и распределение ролей	В. Правила обмена и доверия	С. Управление и приложения
<p><b>1</b> <b>Цель и охват</b> Цель пилота, участники и типы документов</p> <p><b>2</b> <b>Институциональные роли</b> АБР, КТNET, органы по стандартизации, ОПС, принимающие органы</p>	<p><b>3</b> <b>Правила обмена документами</b> Подписанный PDF, метаданные, порядок обмена, временное кэширование</p> <p><b>4</b> <b>Цифровая подпись и регистрация открытых ключей</b> Перечень ОПС, охват полномочий, сертификаты, открытые ключи</p> <p><b>5</b> <b>Защита данных и безопасность</b> Хранение, журналы аудита, контроль доступа, защита данных</p>	<p><b>6</b> <b>Ответственность и ограничения</b> Отсутствие оценки качества продукции, таможенных решений, без ограничения национальных полномочий</p> <p><b>7</b> <b>Срок действия · выход · продление</b> 24-месячный пилот, срок уведомления, возможность продления</p> <p><b>8</b> <b>Урегулирование споров и управление</b> Руководящий комитет, консультации, эскалация вопросов</p> <p><b>9</b> <b>Приложения</b> Охват продукции, перечень ОПС, технический профиль, СОП, набор метаданных</p>

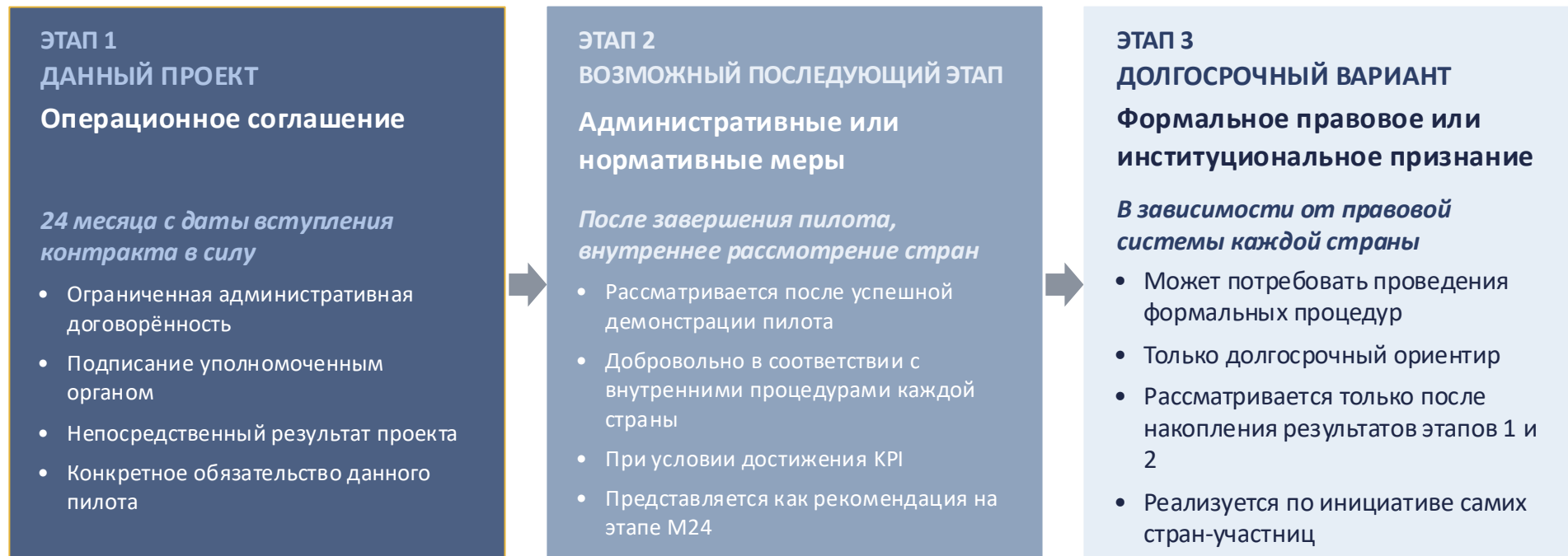
**Примечание: Четыре принципа принятия в рамках пилота:**

- ① Проверка эквивалентности ILAC/IAF,
- ② Уполномоченный орган, включая назначение регулятором,
- ③ Гибкость по типам документов (СоС / протокол испытаний / и то, и другое),
- ④ Без ущерба для национального законодательства (приоритет имеет законодательство страны-импортера)

## S5-17. Дорожная карта последующих действий — дальнейшее развитие за пределами проекта

Этапы 2 и 3 не входят в перечень проектных результатов и рассматриваются как возможные последующие направления, подлежащие рассмотрению странами после валидации результатов пилотного проекта.

**⚠** Этапы 2 и 3 не относятся к прямым результатам проекта и предусмотрены в качестве последующих направлений, которые могут быть рассмотрены странами-участницами после пилотного этапа.



Уровень обязательств снижается слева направо — **только этап 1 является результатом данного проекта.**

## Основные выводы раздела S5

В разделе S5 подчеркивается, что Хаб должен использоваться как **система доверия**, при этом правовые и нормативно-регуляторные вопросы **подлежат постепенному согласованию через Этап 1 Пилотного операционного соглашения и СОП.**

### S5. Основные технические, правовые и нормативные вопросы

1

#### Хаб — механизм доверия, а не репозиторий файлов

Обеспечивает обмен подписанными PDF и метаданными, управление открытыми ключами, проверку полномочий ОПС и журналы аудита в рамках Модели А.

2

#### Акцент на первом этапе — не на полноценном СВП

Пилотный проект начинается с 24-месячного административного соглашения; Этапы 2 и 3 сохраняются в качестве возможных последующих вариантов.

3

#### Следует избегать категоричных правовых формулировок

Правовая осуществимость, условия принятия и необходимые процедуры определяются по итогам внутреннего рассмотрения каждой страны.

→ Следующая сессия (S6): Итоги совещания и дальнейшие шаги

Thank You · 감사합니다 · Rahmat · Спасибо · شكراً

— Совместными усилиями пяти стран — к открытию новой главы цифровой торговли в рамках ЦАРЭС —



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

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



  
**KOREA**  
e-Asia Fund