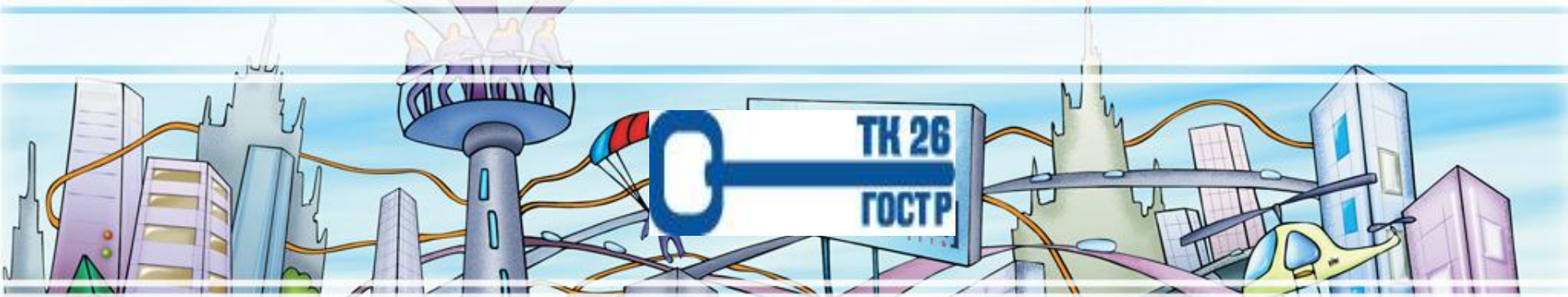
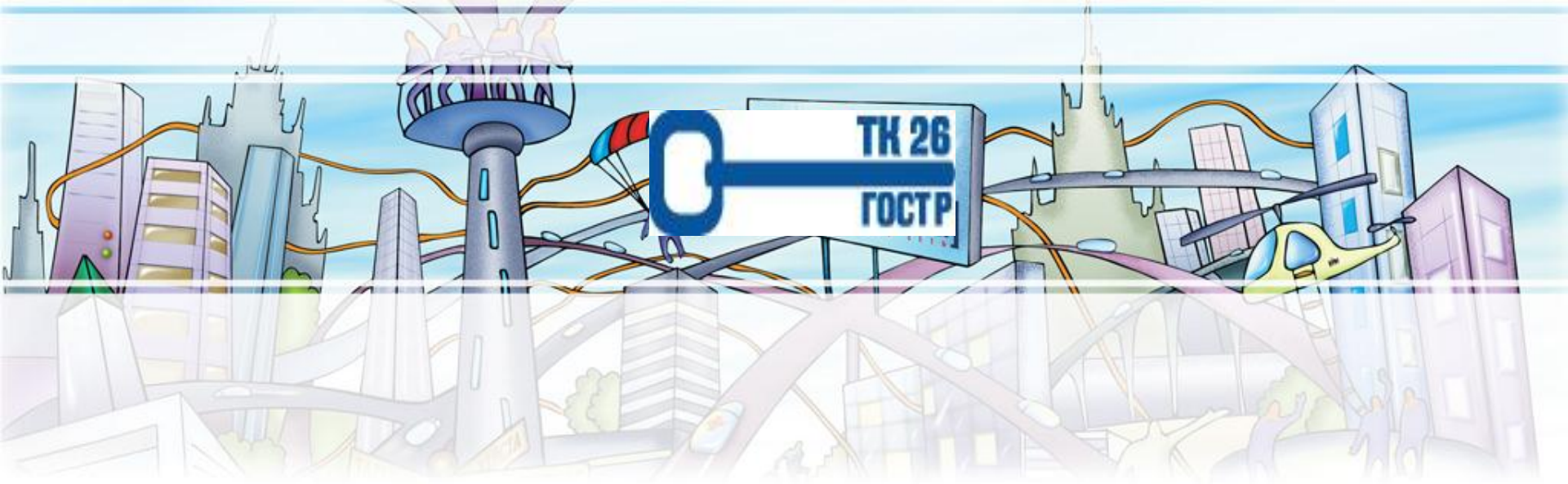


Задачи совместимости PKI-решений отечественных производителей, используемых при предоставлении государственных услуг, или Криптографический роуминг

Секретариат технического комитета по стандартизации «Криптографическая защита информации»



Цели стандартизации шифровальных (криптографических) средств

РОСТЕЛЕКОМ

Общие особенности проектов ИЭП

Масштаб - проект должен обеспечивать работу сотен систем по всей территории РФ

Динамика – проект реализуется в предельно короткие сроки

Массовость – услуги должны предоставляться всем

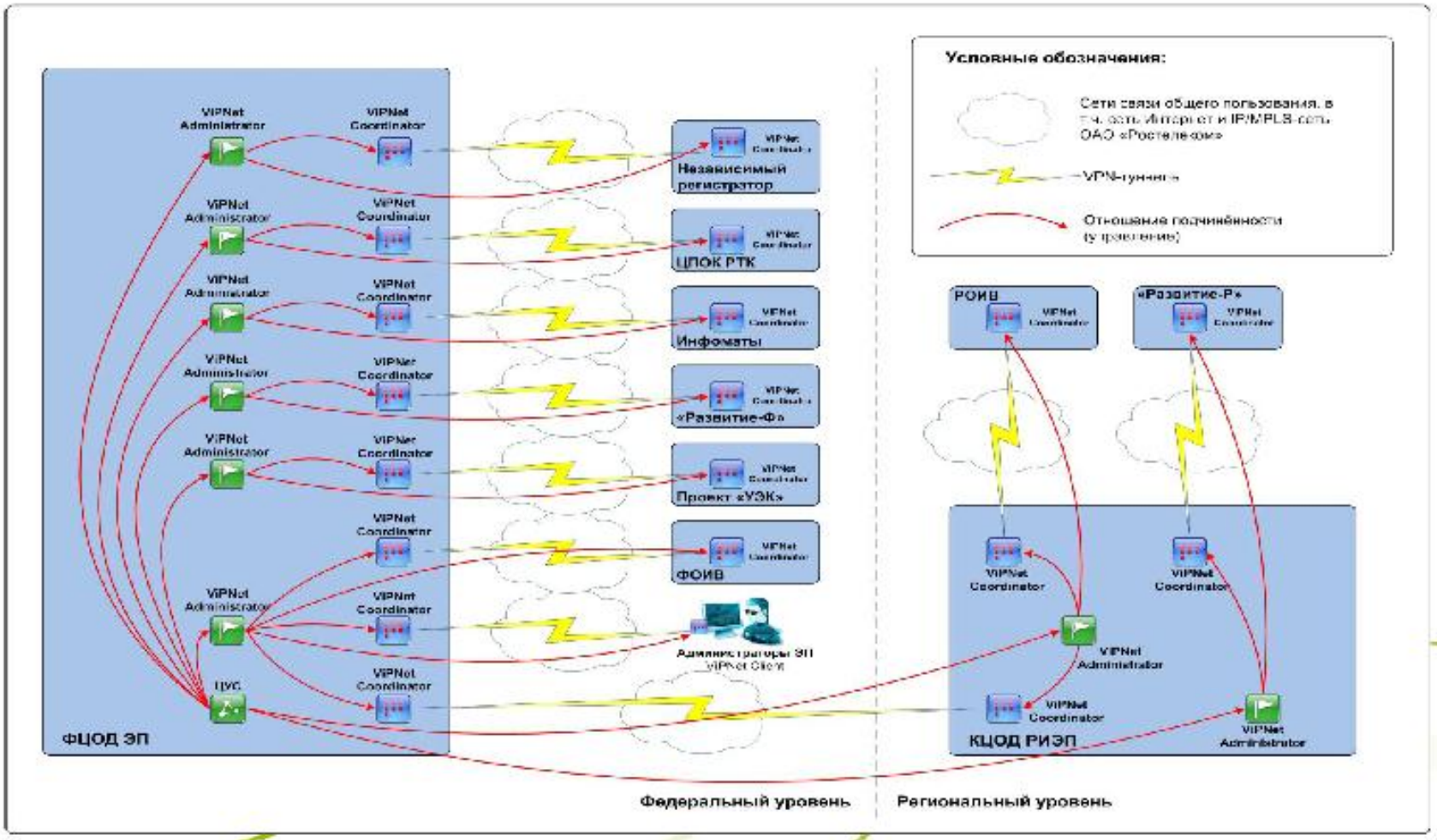
Неоднородность – проблемы информационного неравенства и отсутствия стандартизации

Проблемы с нормативным обеспечением

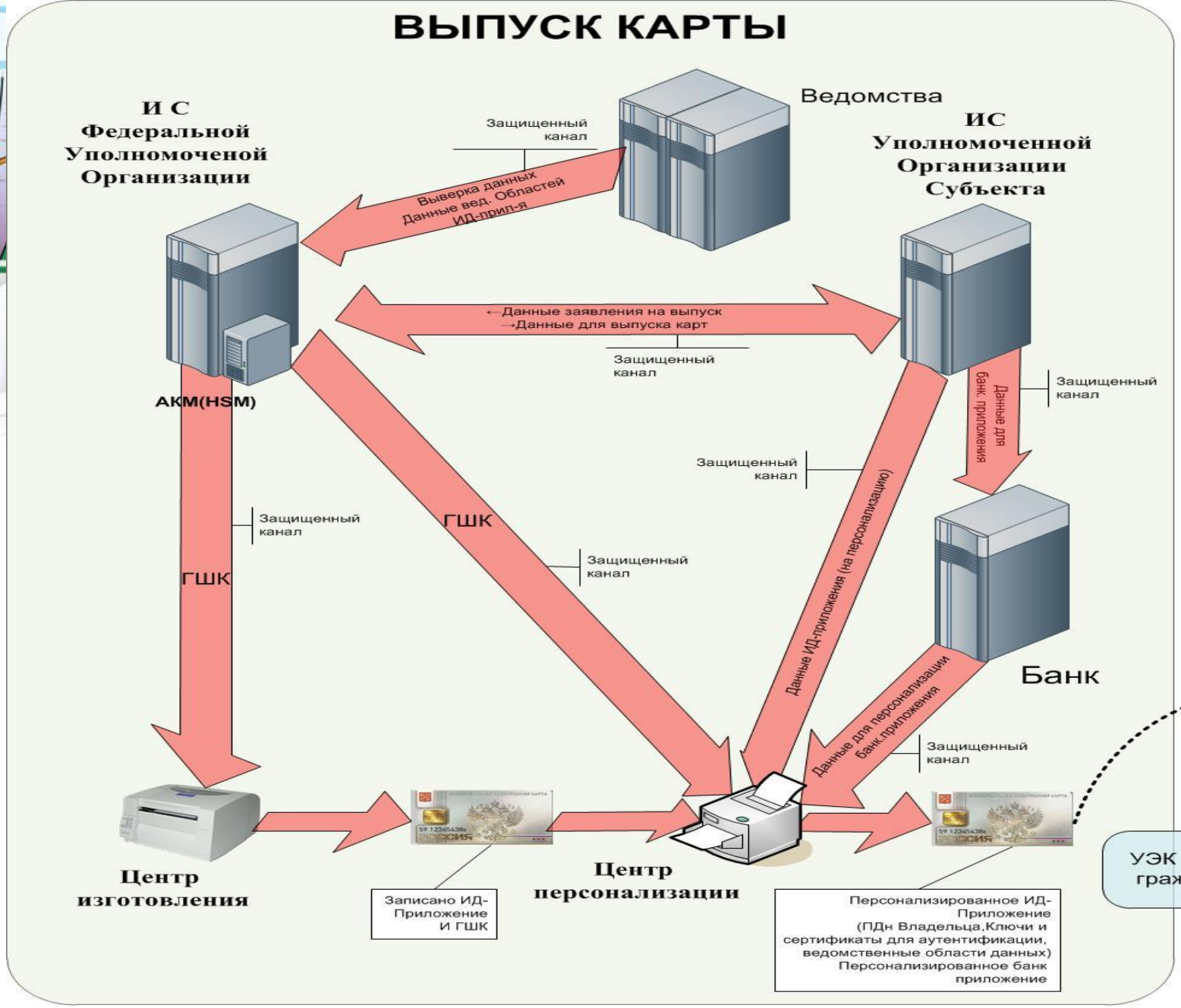
Из доклада И.А.Трифаленкова

РОСТЕЛЕКОМ

Целевая структура защищенной сети передачи данных



Из доклада И.А.Трифаленкова

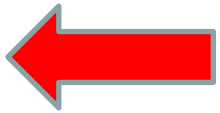

ВЫПУСК КАРТЫ
И С Федеральной Уполномоченой Организации
Ведомства
ИС Уполномоченной Организации Субъекта
Защищенный канал
Выверка данных
Данные вед. Областей
ИД-прил-я
←Данные заявления на выпуск
→Данные для выпуска карт
Защищенный канал
АКМ(HSM)
Защищенный канал
Данные для банк. приложения
Защищенный канал
ГШК
Защищенный канал
ГШК
Защищенный канал
Данные ИД-приложения (на персонализацию)
Банк
Данные для персонализации банк.приложения
Защищенный канал
Центр изготовления
Записано ИД-Приложение И ГШК
Центр персонализации
Персонализированное ИД-Приложение (ПДн Владельца,Ключи и сертификаты для аутентификации, ведомственные области данных) Персонализированное банк приложение
УЭК выдана гражданину

Обслуживание карты (госуслуги – общая технология)

Принципы создания ИБ ИЭП

Развитие нормативной базы как часть проекта

Сочетание отечественных и международных стандартов



Применение промышленных решений

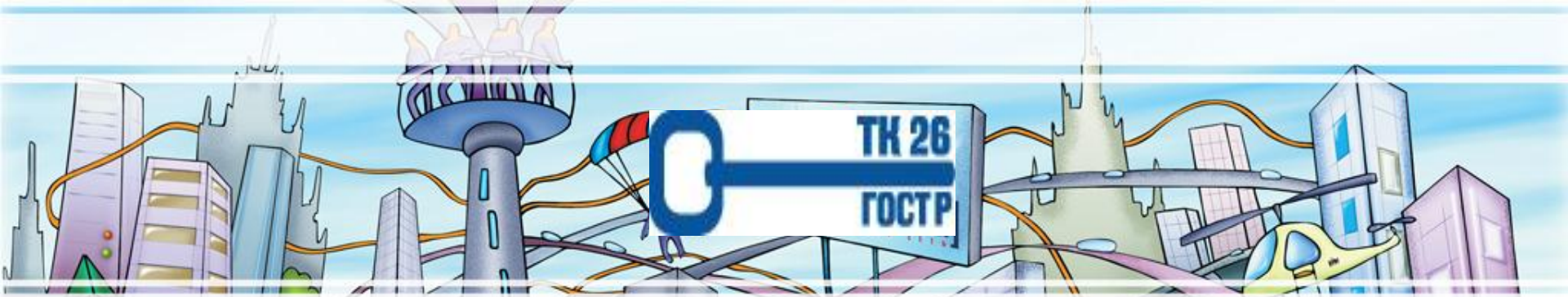
Процессно-ориентированный подход

Широкая кооперация производителей и исполнителей работ

Из доклада И.А.Трифаленкова

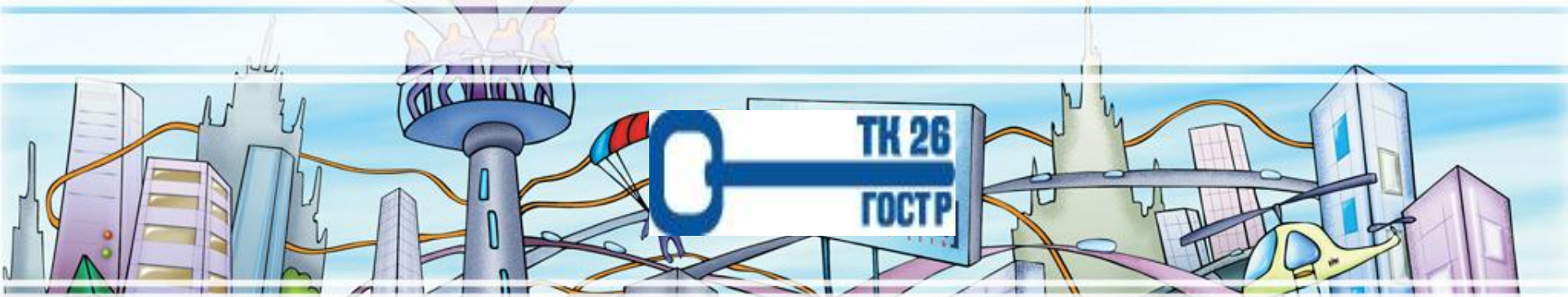
Стандартизация СКЗИ обеспечит:

- *рациональное использование ресурсов за счет взаимозаменяемости и интероперабельности криптографических (шифровальных) средств и их технической и информационной совместимости;*
- *сопоставимость результатов исследований (испытаний) СКЗИ на соответствие требованиям информационной безопасности за счет единства измерений и проведения анализа характеристик продукции (работ, услуг);*
- *качество исполнения государственных заказов за счет унификации технических требований к СКЗИ.*



Интероперабельность (Interoperability):

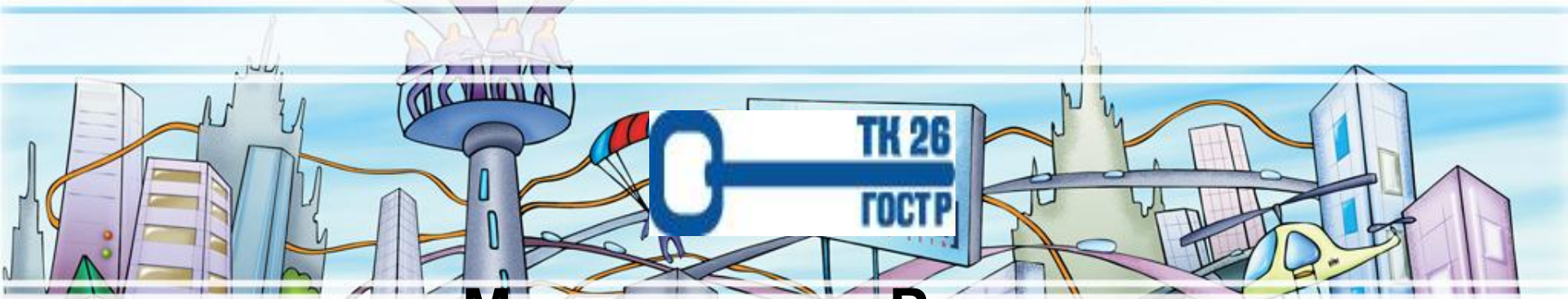
- *Интероперабельность (технологическая открытость) – свойство или возможность различных систем и организаций работать совместно (inter-operate).*



Интероперабельность криптографических (шифровальных) средств:

- *Исключается необходимость перешифрования защищаемой информации, ее переподписывания и т.д.*
- *В ИТКС исчезают участки , на которых информация оказывается потенциально незащищенной.*

Сохраняется и развивается общее криптографически защищенное информационное пространство

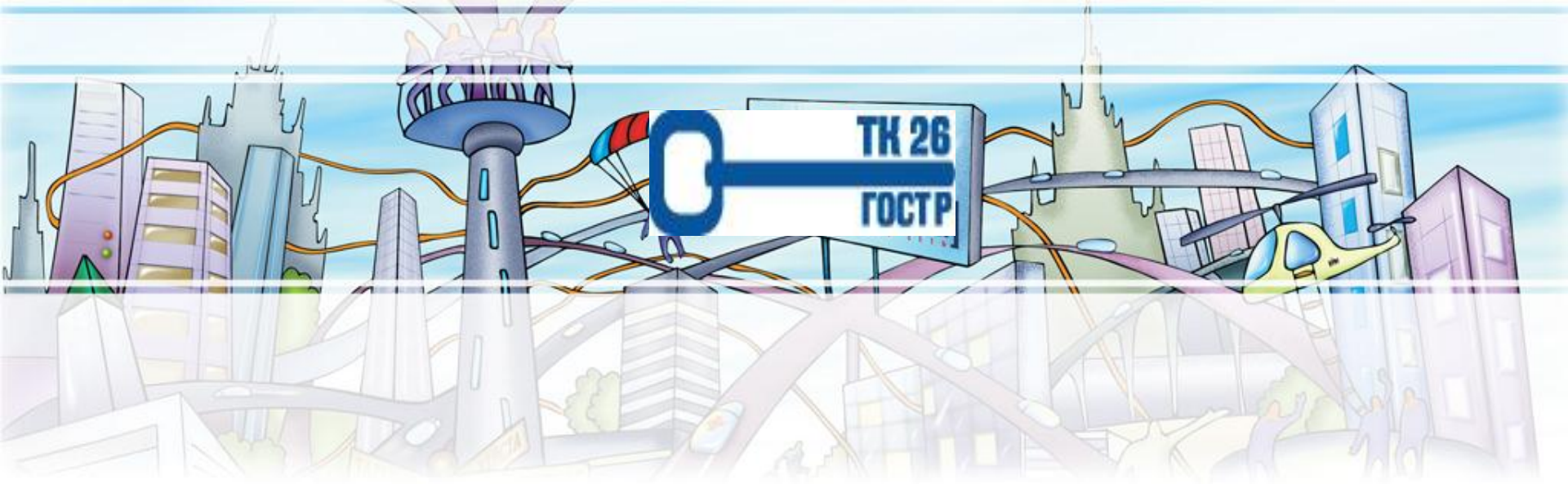


Минкомсвязи России

Приказ от 23 марта 2009 г. № 41«Об утверждении требований к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров ОГИЦ»

10. Требования к алгоритмам и стандартам, используемым для обеспечения информационной безопасности в подсистеме УЦ ОГИЦ.

Для выполнения криптографических преобразований должны использоваться алгоритмы, устанавливаемые государственными стандартами Российской Федерации



Практические потребности в интероперабельности

На национальном уровне:

Защищенные АСИО

- *Электронное правительство;*
- *УЭК;*
- *МЭДО;*
- *СМЭВ;*
- *национальная платежная система ;*

и др.

На региональном уровне:

Защищенные АСИО:

- *СНГ, в т.ч. погранслужб, полиции и т.д.*
- *ЕВРАЗЭС;*
- *ШОС;*
- *ОДКБ;*
- *АТЭС;*

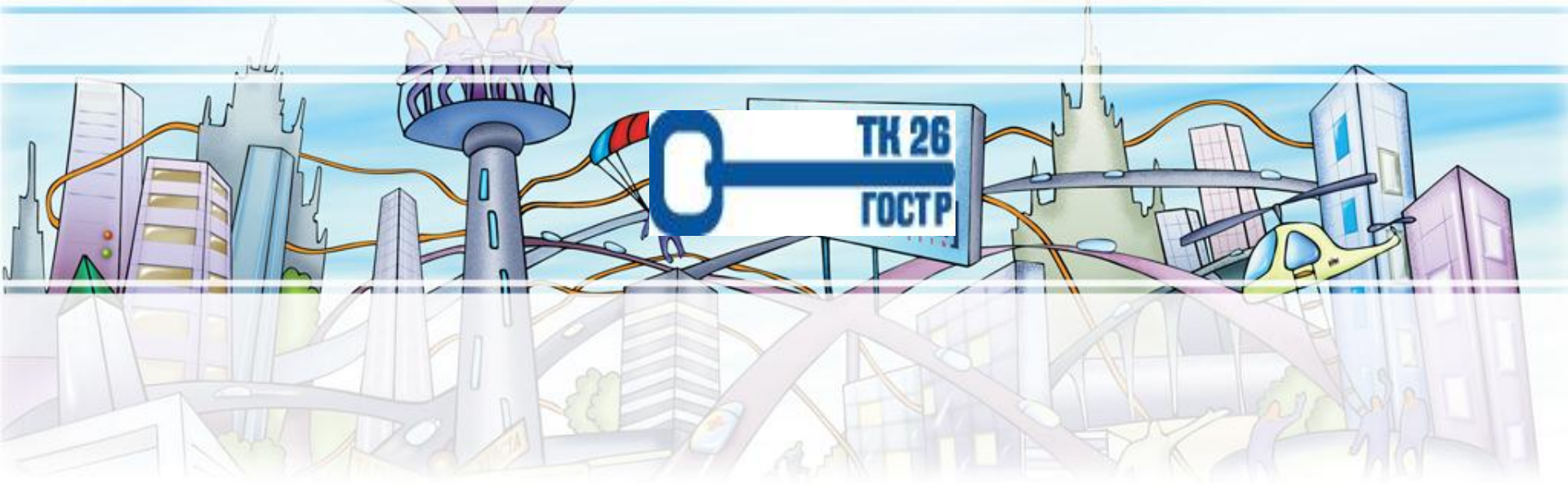
и др.

На международном уровне:

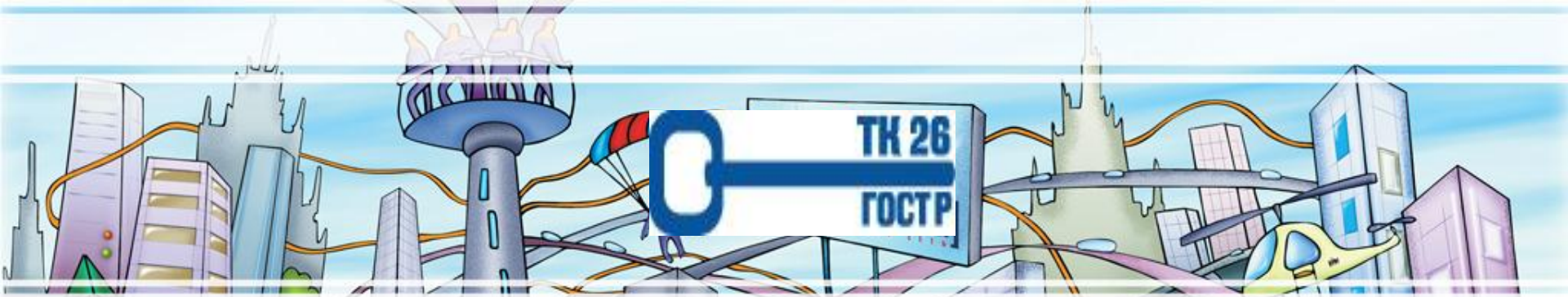
Трансграничное взаимодействие.

Паспортно-визовые документы нового поколения (ПВДНП)

•*защита и проверка персональных данных, включая биометрические данные.*



Российская национальная система стандартизации в области криптографии



Росстандарт

GOST R

Технический комитет по стандартизации «Криптографическая защита информации»

В ТК 26 представлены органы и организации (*более 50-ти*), к компетенции которых отнесена защита информации с использованием криптографических методов, имеющих опыт в организации разработок образцов шифровальных (криптографических) средств

Расширение стандарта PKCS#11

Расширение стандарта RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) российскими криптографическими алгоритмами.

В 2009 г. опубликована новая версия PKCS #11 v2.30, включающая ГОСТ 28147-89 и другие российские алгоритмы.

Использование стандарта PKCS#12

Использование стандарта *RSA Security Inc. PKCS #12 Personal Information Exchange Syntax Standard совместно с* российскими криптографическими алгоритмами.

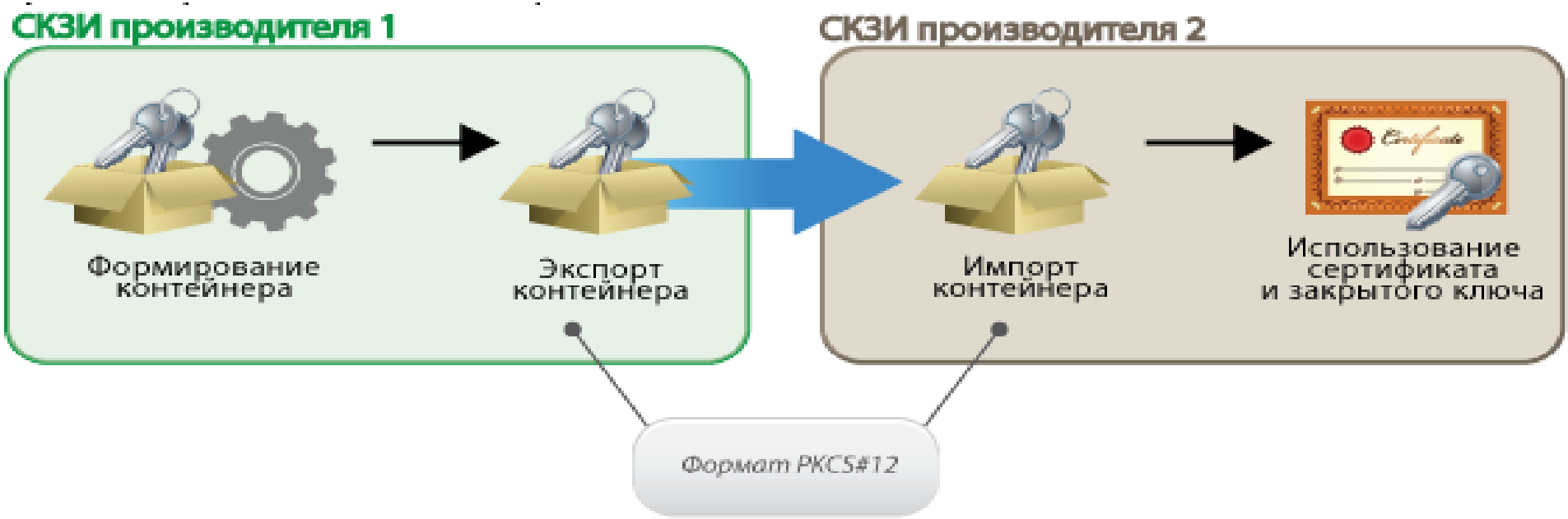
Позволяет создать т.н. транспортный контейнер ключей пользователя для организации получения госуслуг, например, при помощи универсальной электронной карты.

Документ проходит экспертизу в ФСБ России.

Использование стандарта PKCS#12

Регион 1 (Ведомство 1)

Регион 2 1 (Ведомство 2)



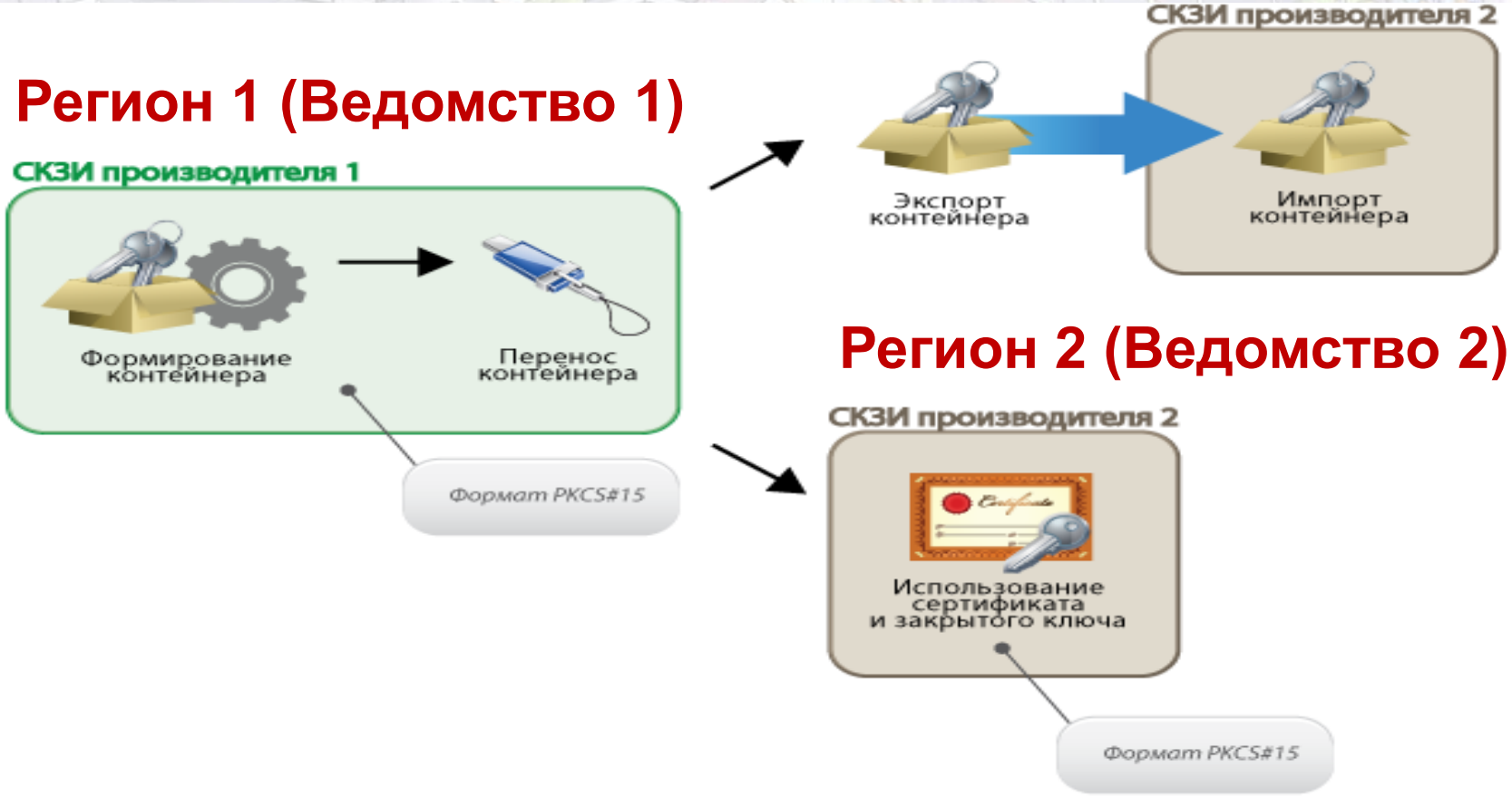
Использование стандарта PKCS#15

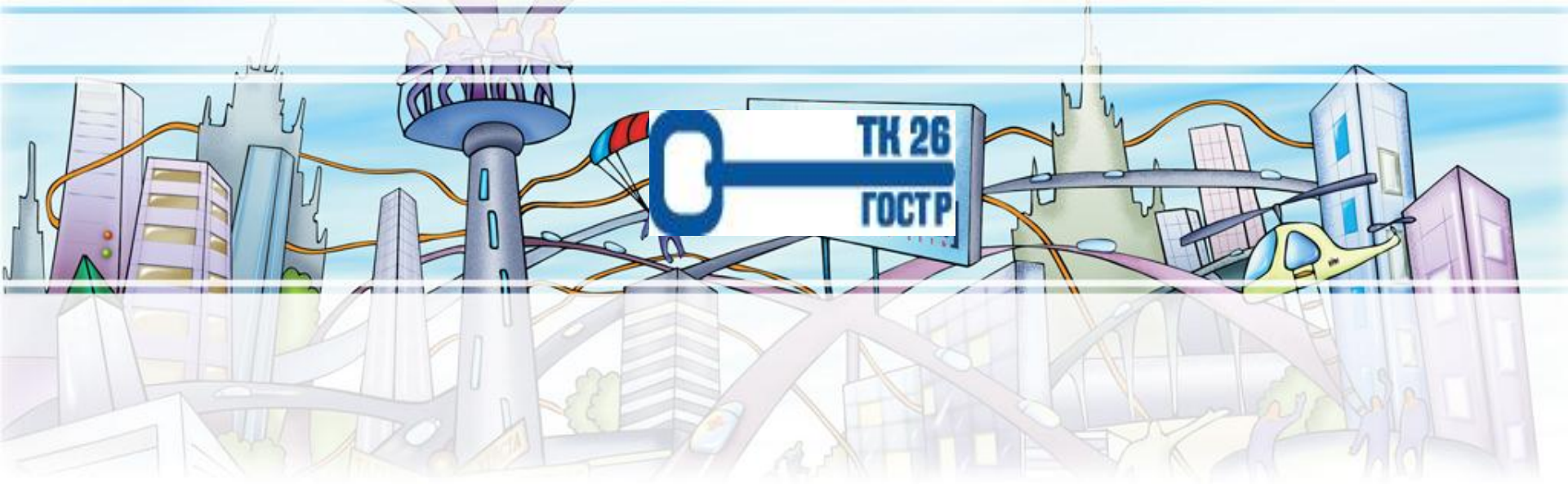
Использование стандарта *RSA Security Inc. PKCS #15 Cryptographic Token Information Format Standard совместно с* российскими криптографическими алгоритмами.

Позволяет создать т.н. контейнер хранения ключей пользователя для получения госуслуг, например, при помощи универсальной электронной карты.

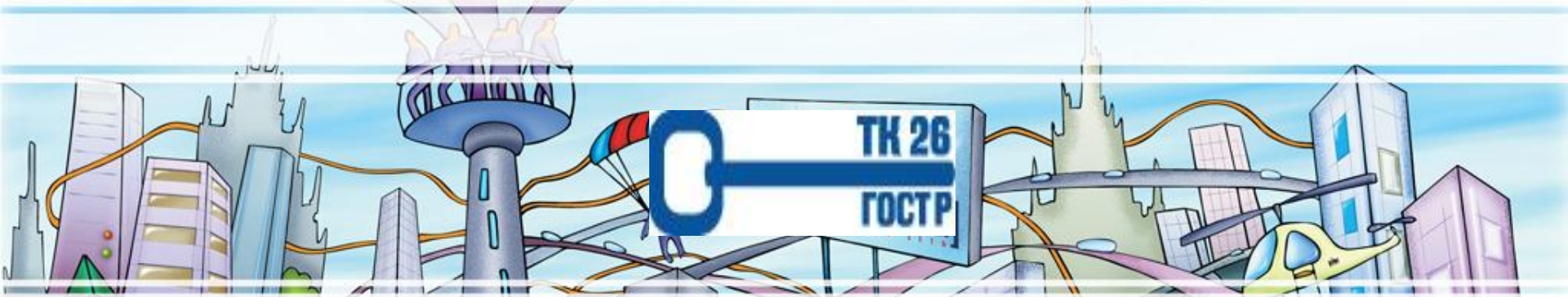
Документ уже прошел экспертизу в ФСБ России.

Использование стандарта PKCS#15





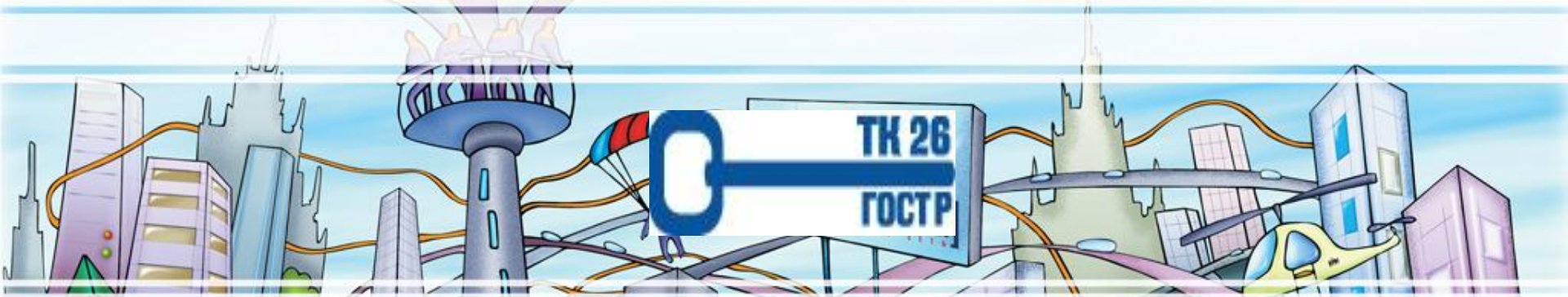
В заключение



European Interoperability Framework for European Public Services (EIF)

Version 2.0

This document is a work in progress

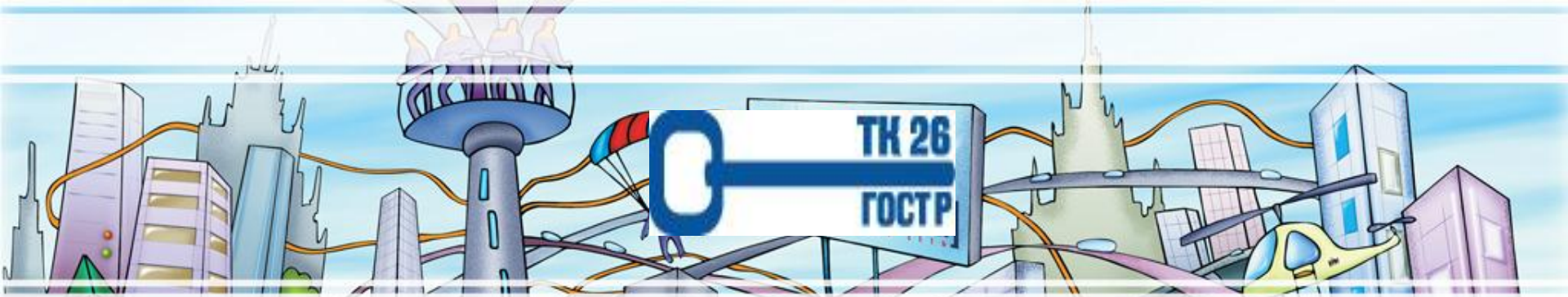


Целью Европейской рамочной совместимости (EIF) является:

• обеспечение и поддержка предоставления европейских общественных услуг путем обеспечения трансграничного и межсекторального взаимодействия;

• направление усилий государственных администраций в плане предоставления европейских общественных услуг предприятиям и гражданам;

• дополнение и связь воедино различных национальных рамочных систем взаимодействия (NIF) в Европейском пространстве.



Рекомендация 23.

Общественные органы должны активно участвовать в деятельности по стандартизации, которые имеют отношение к их нуждам.

GOST R

Благодарим за внимание!

ОАО «ИнфоТеКС»

Секретариат технического комитета по стандартизации «Криптографическая защита информации»

Тел. +7 (495) 737 61 92

tc26@infotecs.ru

www.tc26.ru