Ростелеком
Больше возможностей

От ЕПД к ИС ГУЦ – состояние и перспективы единого пространства доверия

И.А.Трифаленков, начальник отдела ИБ проекта «Информационное общество»

sochi.ru 2014

Единое пространство доверия – сегодня и завтра

Состояние на начало 2012

Создана информационная система, оказывающая реальный набор услуг:

Реестр УЦ

Проверка электронной подписи

Мониторинг функционирования УЦ и соответствия требованиям МКС

Разработан комплект нормативных документов и регламентов для работы в условиях ФЗ-63

Проведена модернизация ПАК Головного удостоверяющего центра

Основные мероприятия 2012

Формирование Информационной системы головного УЦ на основе ИС ЕПД и УЦ МКС на инфраструктуре Ростелекома

Построение иерархии удостоверяющих центров с обеспечением единых правил взаимодействия

Создание сайта уполномоченного органа

Формирование новых сервисов для информационной системы в составе

- Сервиса постановки электронной подписи;
- Сервиса точного времени и подтверждения

Проведение тематических исследование и аттестация Информационной системы головного УЦ по требованиям регуляторов

Результат

Предоставление полного набора услуг, связанных с установкой и проверкой ЭП в рамках инфраструктуры Ростелекома

Управление процессом выдачи сертификатов ЭП для любых организаций и граждан

Создание адекватной нормативной базы для управления процессами использования механизмов ЭП

Ростелеком

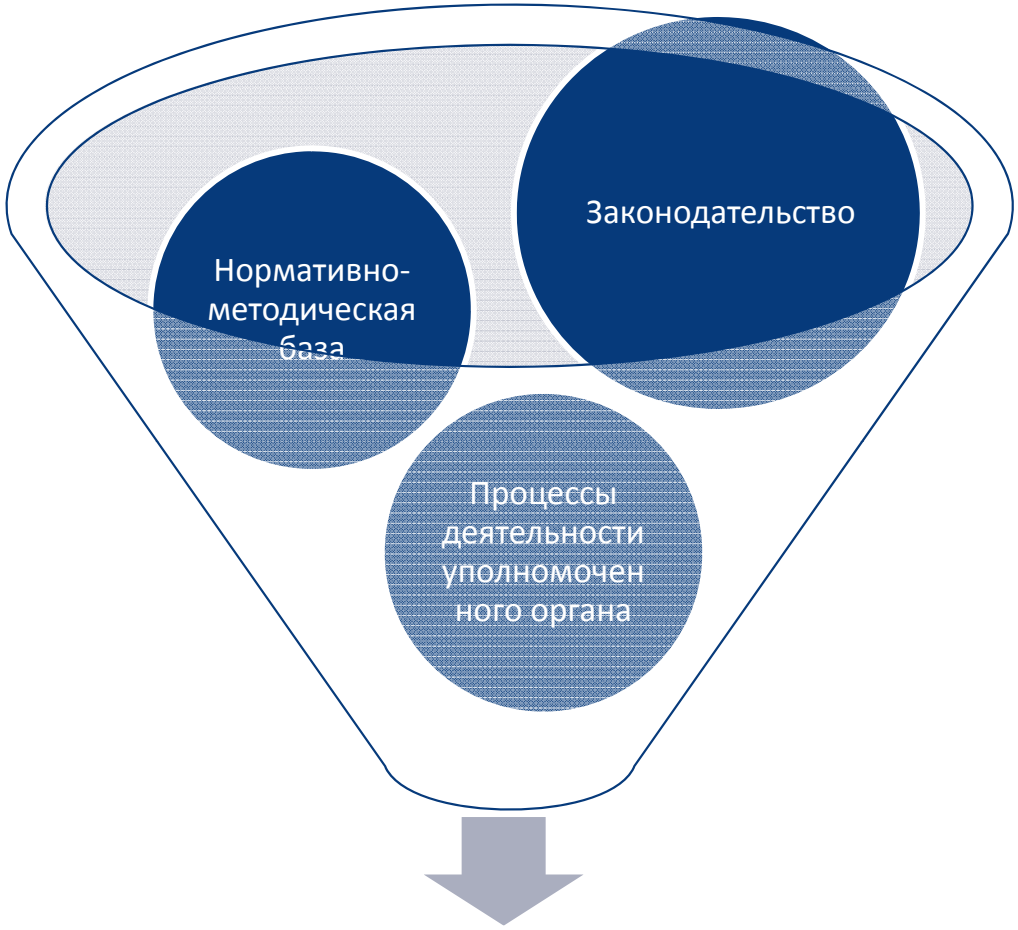
Что такое ЕПД – изменение концепции

ЕПД – это совокупность нормативных и организационно-технических условий, обеспечивающих техническую возможность и юридическую значимость действий граждан, организаций и государственных органов по установлению доверия электронным подписям при обеспечении информационного взаимодействия

ИС ГУЦ – это совокупность информационных систем, обеспечивающих предоставление услуг, связанных с постановкой и проверкой квалифицированной электронной подписи, а также автоматизация деятельности уполномоченного органа в области электронной подписи

Ростелеком

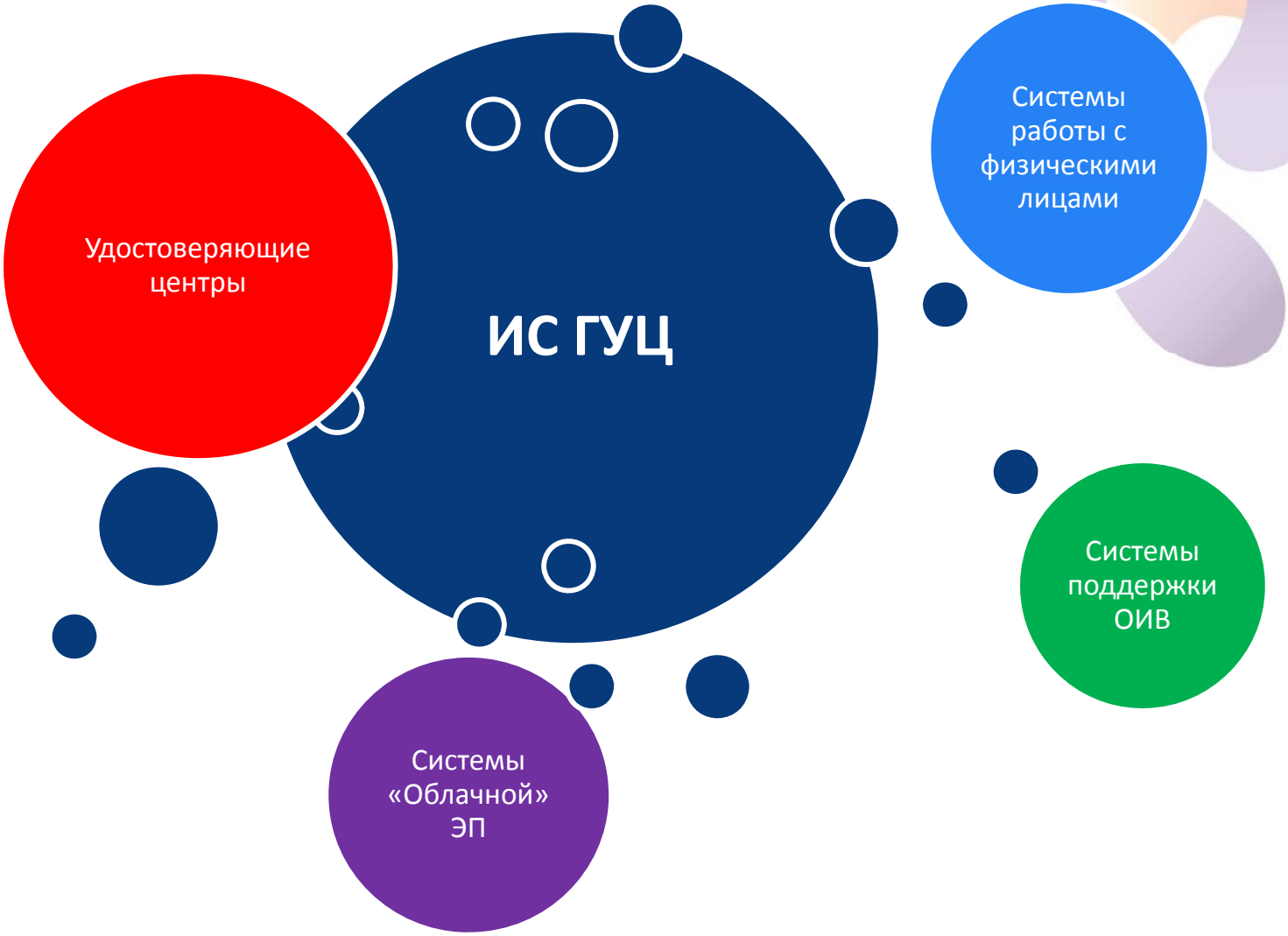
Информационная система головного удостоверяющего центра



Информационная система головного удостоверяющего центра

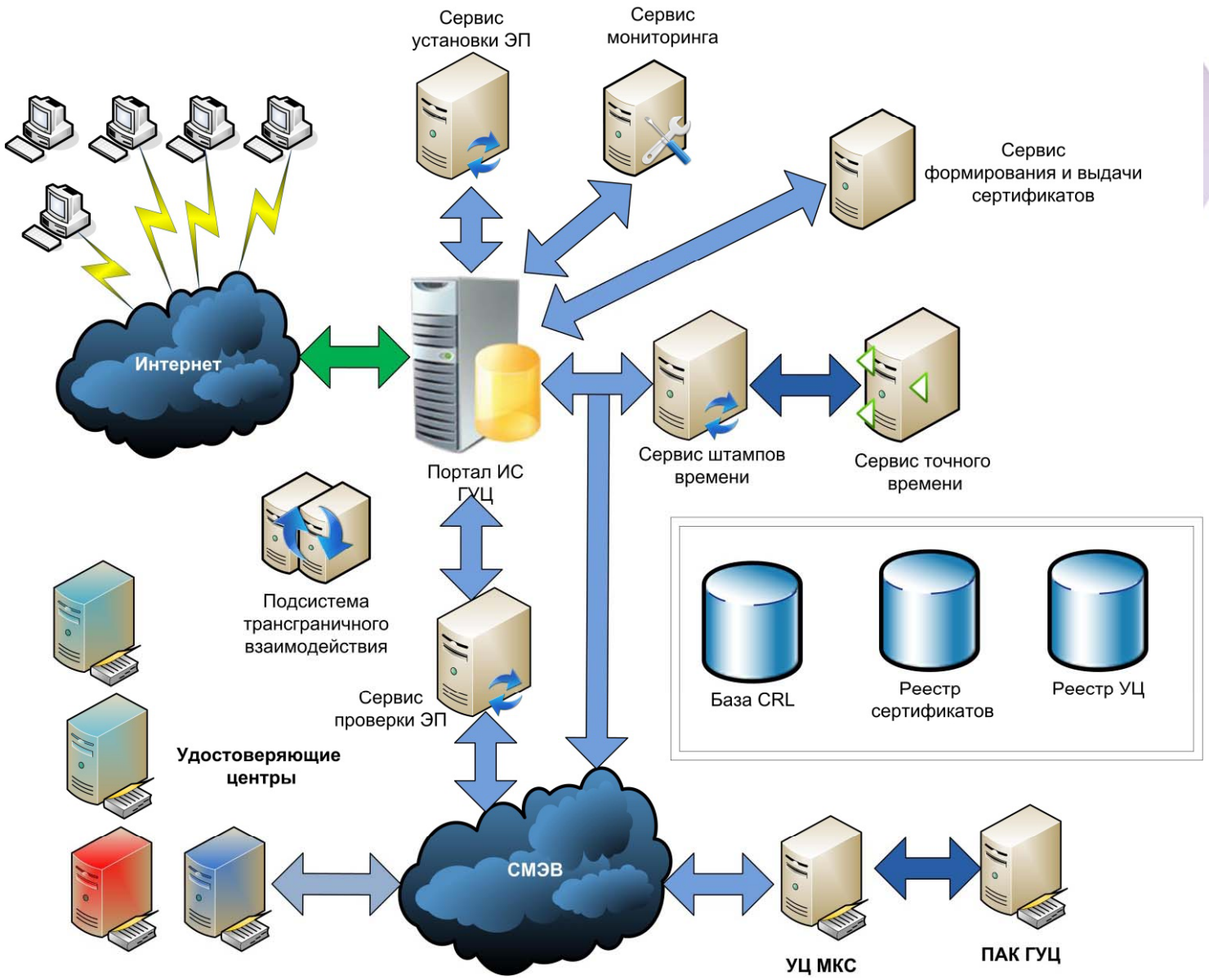
Ростелеком

Информационная система головного удостоверяющего центра и другие системы



Ростелеком

Состав и структура ИС ГУЦ



Ростелеком

ЕПД - Нормативная база 2011 года

Виды электронной подписи, используемой органами исполнительной власти (постановление №111 от 09.02.2012)

Порядок использования электронных подписей при обращении за получением государственных и муниципальных услуг

Порядок и правила мониторинга удостоверяющих центров, входящих в ЕПД

Порядок и правила применения удостоверяющими центрами сервиса проверки СНИЛС и ИНН в процессе выдачи сертификатов

Порядок и правила обеспечения фиксации единого времени и даты при подписании электронных документов

Правила присоединения удостоверяющих центров

Порядок и правила взаимодействия удостоверяющих центров, входящих в ЕПД для организации взаимного признания и проверки электронных подписей

Ростелеком

ЕПД - Нормативная база 2012 года

Методические рекомендации по функционированию системы аккредитованных УЦ с ГУЦ, описание технологического процесса взаимодействия различных УЦ в системе аккредитованных УЦ;

Инструкция и методики на перенос БД пользователей, БД сертификатов, сохранение юридической значимости сертификатов, выпущенных ФУЦ, на ГУЦ;

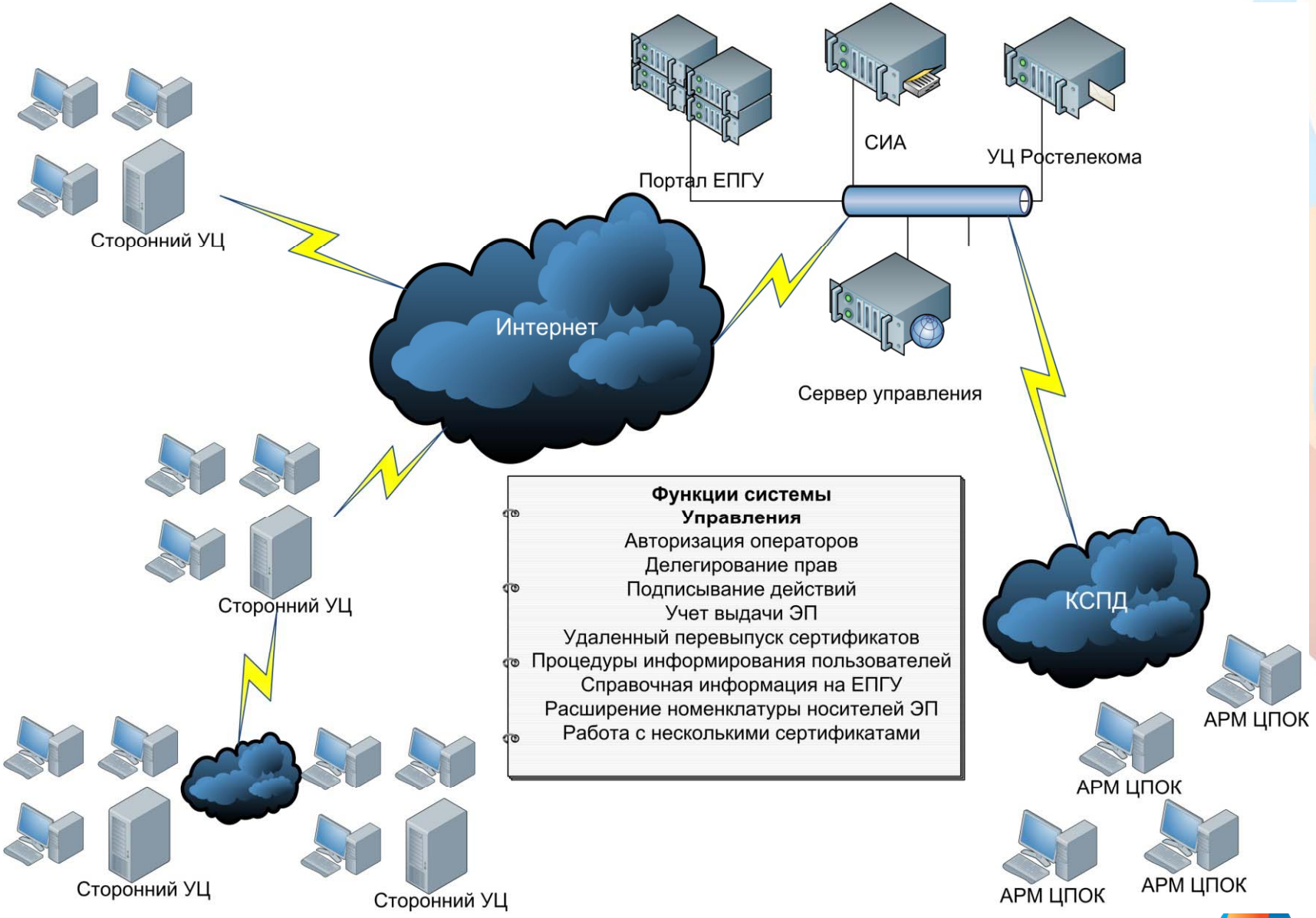
Инструкции по формированию и выдачи квалифицированных сертификатов аккредитованным УЦ;

Методологии и описание технологического процесса деятельности Головного удостоверяющего центра на основе ИС ГУЦ

Нормативно-техническая документация функционирования Головного удостоверяющего центра

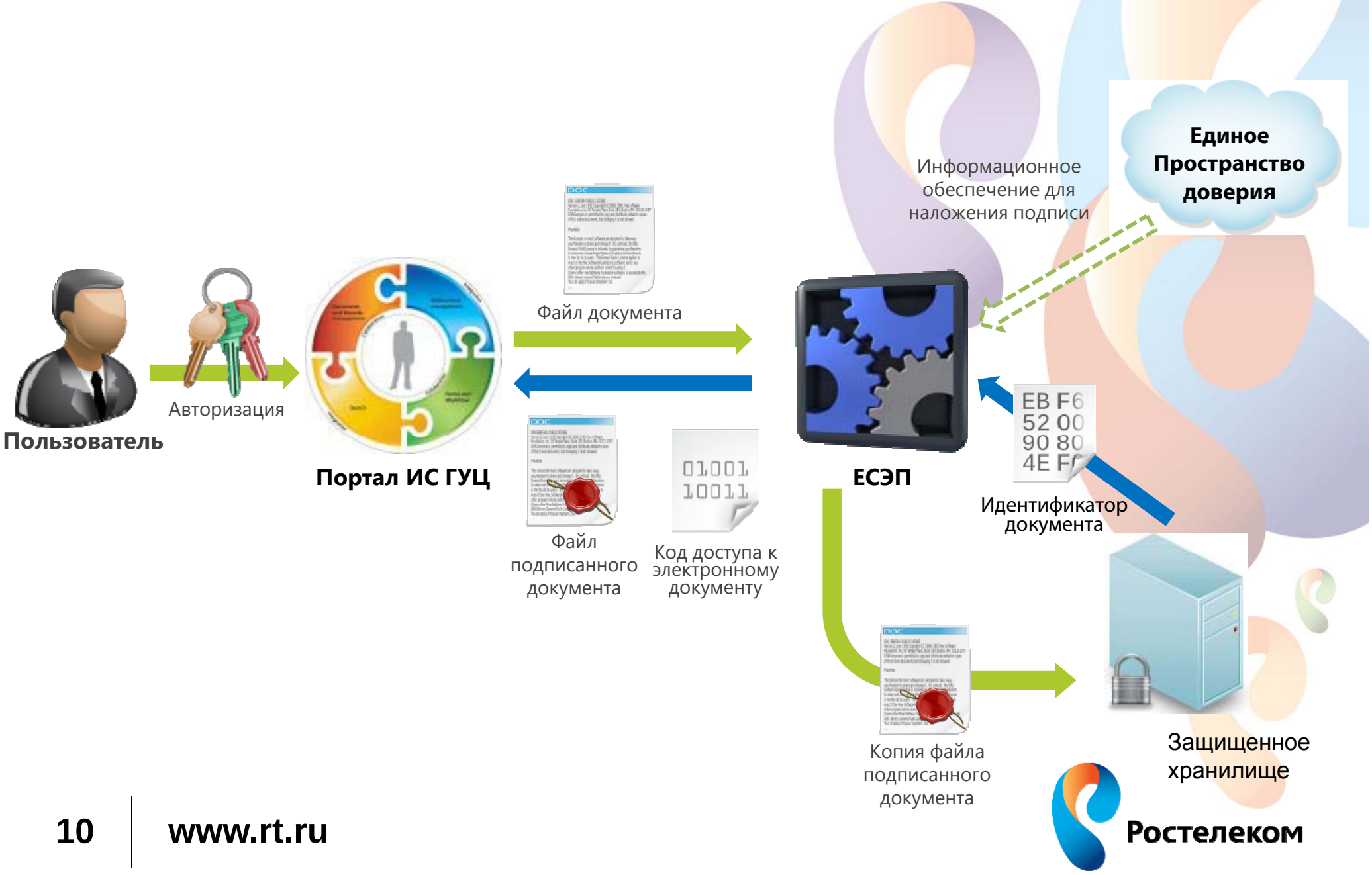
Ростелеком

Система регистрации пользователей ЕПГУ

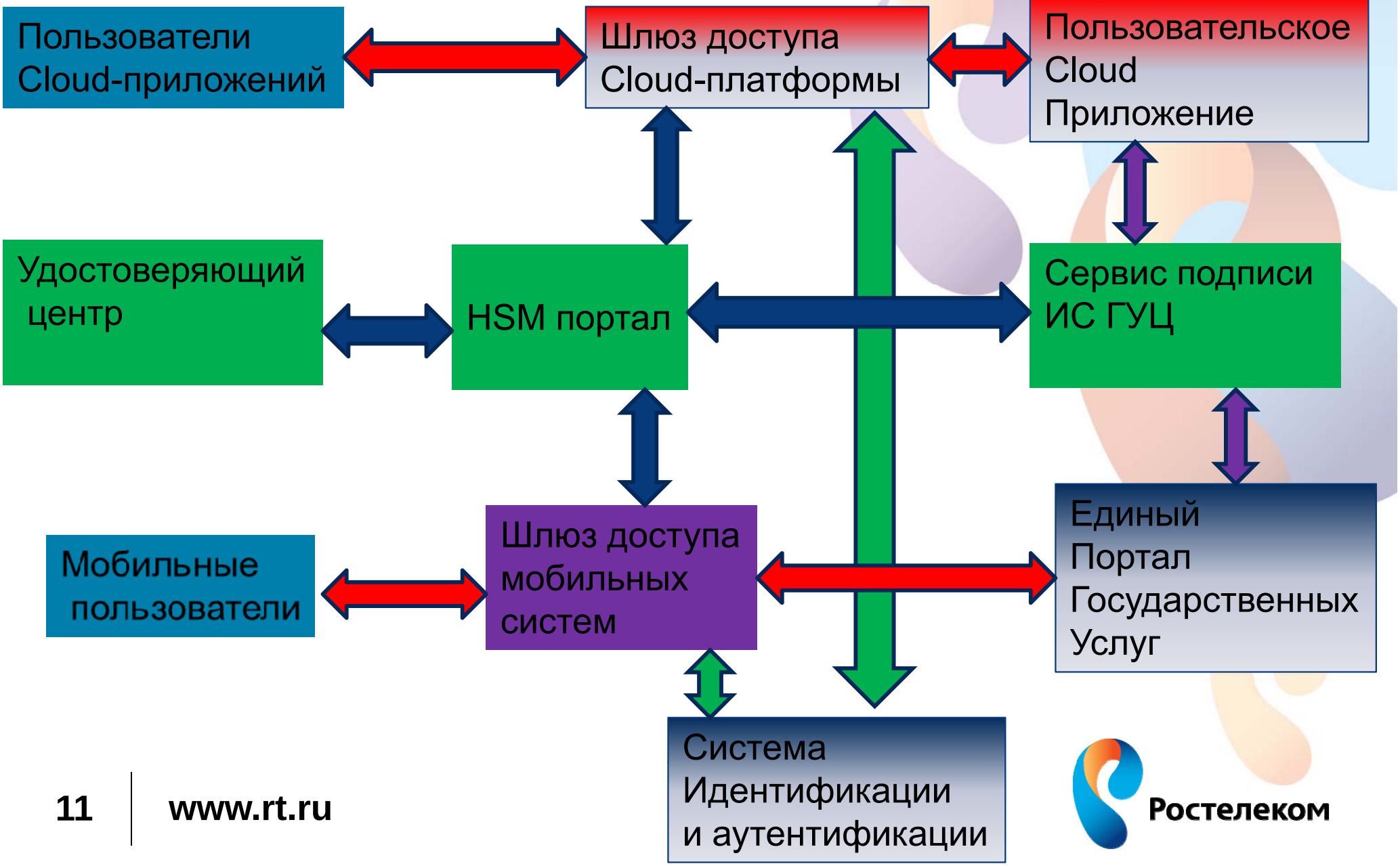


Ростелеком

Электронная подпись as a service ИС ГУЦ



Система мобильной электронной подписи



Ростелеком

Сервис мобильной электронной подписи

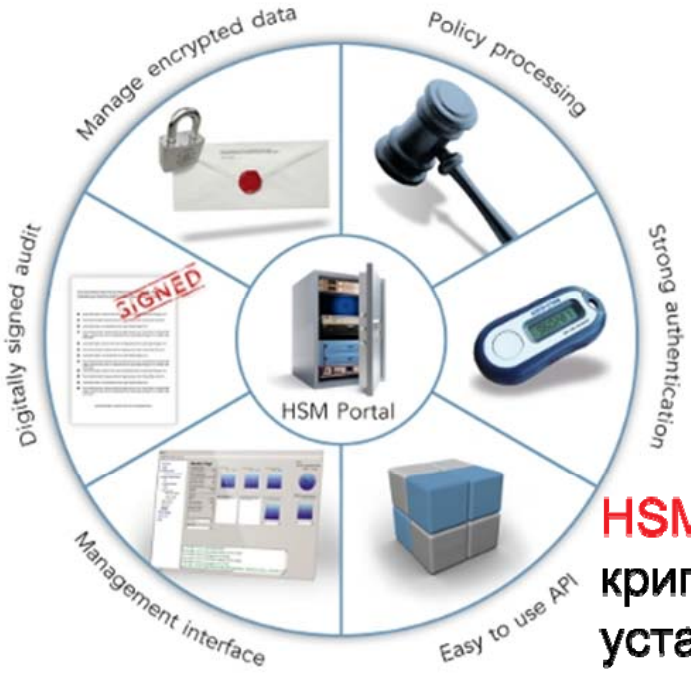
Локальное хранение ключей

- Ключевой носитель контролируется пользователем
- Единый механизм аутентификации на основе сертификатов ЭП
- Работа с приложениями портала
- Проблема компрометации ключей
- Необходимость дополнительного шифрования данных
- Наличие сертифицированных решений уже сейчас
- Применение решения снижает производительность ПГУ
- Необходимость контроля корректности использования ключевого носителя – защита клиентского места

Централизованное хранение ключей

- Ключевой носитель контролируется оператором
- Дополнительная аутентификация на основе одноразовых паролей
- Возможность работы как с порталом, так и с мобильными приложениями
- Проблема компрометации алгоритма одноразовых паролей
- Шифрование данных на уровне каналов
- Решения по HSM либо в стадии сертификации либо имеют проблемы при масштабном применении
- Нет проблем с производительностью

HSM портал как ядро сервиса мобильной ЭП



HSM Portal – аппаратное решение для использования криптографии в режиме сервиса, предоставляющее возможности виртуализации и эластичного доступа к криптографическим ресурсам.

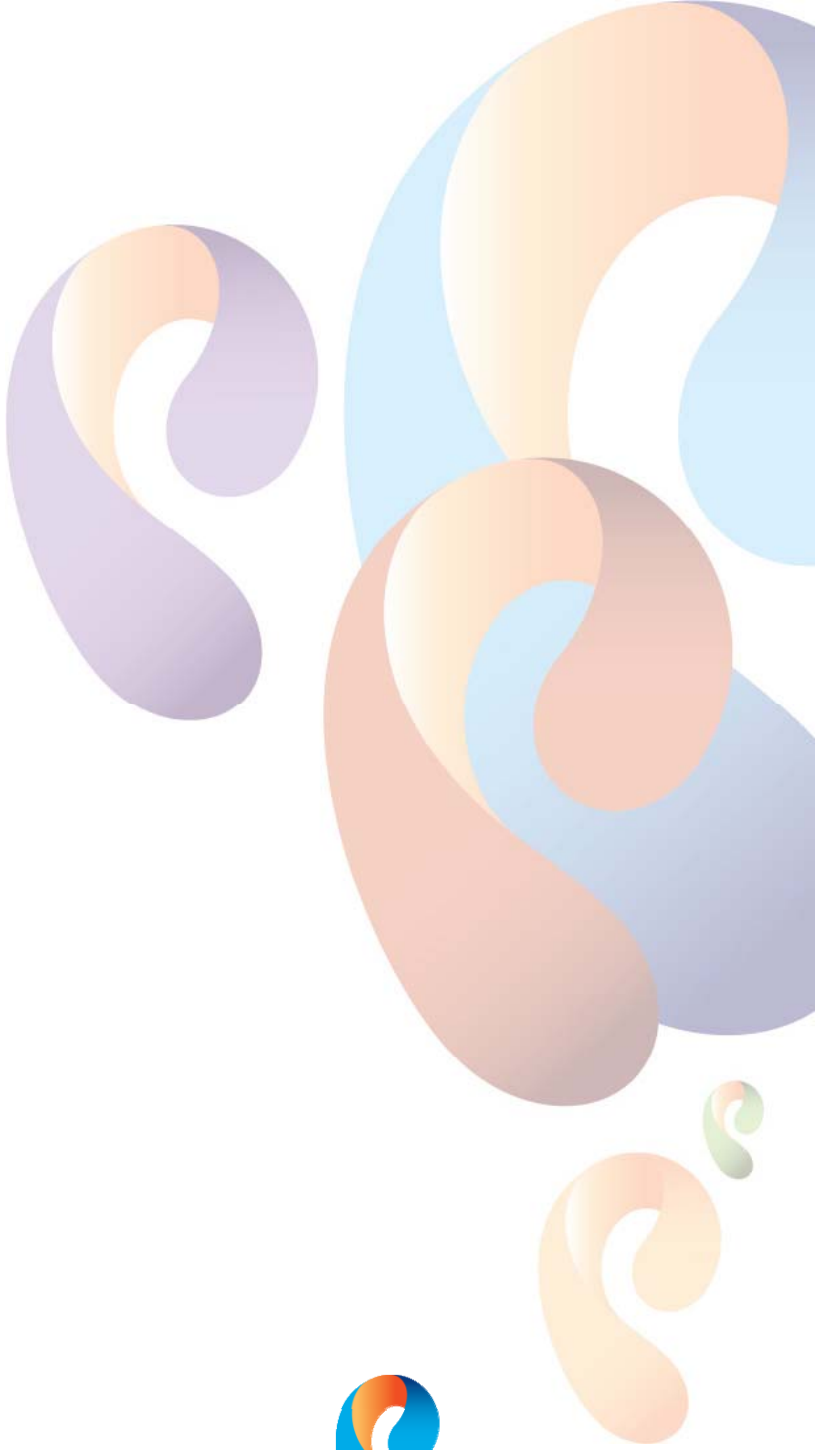
HSM Портал состоит из кластера криптографических серверов, которые устанавливаются между HSM (возможно не одним) и приложениями.

Криптографические сервера конфигурируются с панели управления с учетом политики управления (безопасной) и политикой мониторинга.

Криптографические параметры для приложений управляются с единой системы управления с применением высокоуровневых языков.

Ростелеком

СПАСИБО



Ростелеком