Ростелеком
Больше возможностей

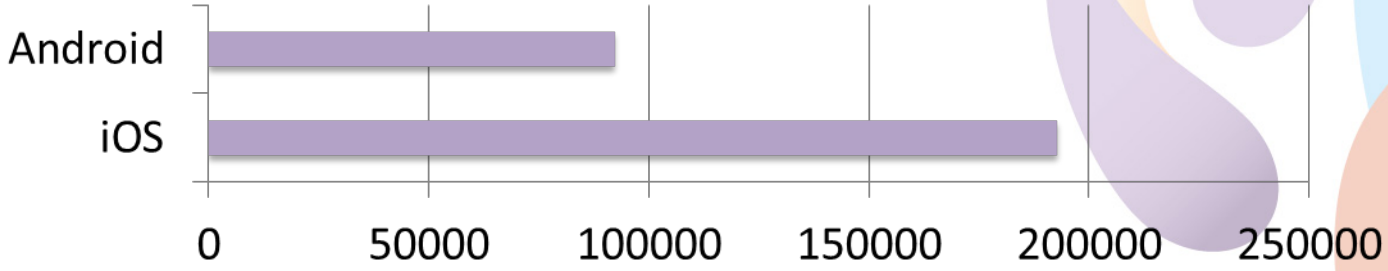
Использование удаленных механизмов ЭП при работе с мобильными устройствами

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

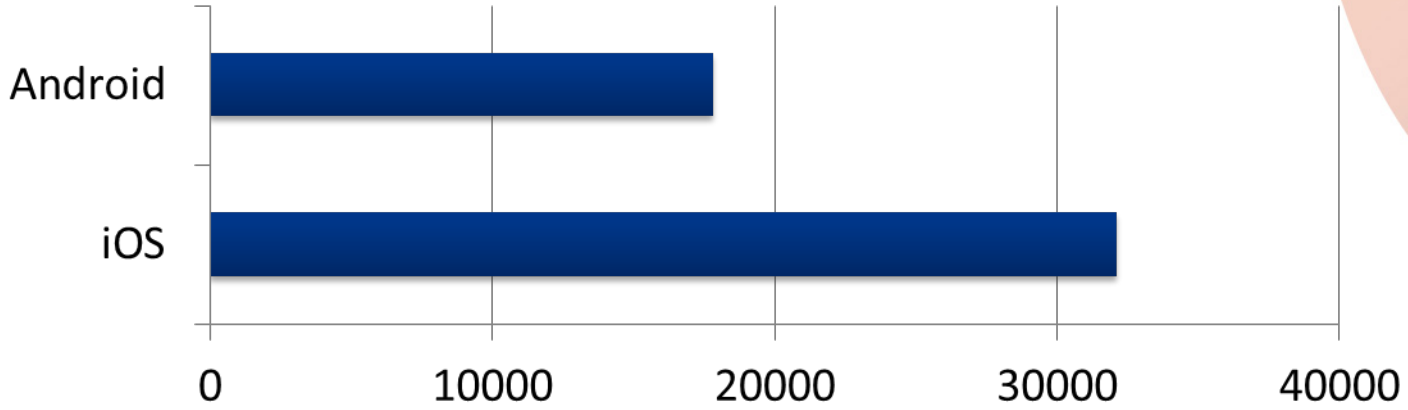
sochi.ru 2014

Интерес пользователей к приложениям «Госуслуги» за период март - август 2012

Количество скачиваний приложений (около 285 тыс.)

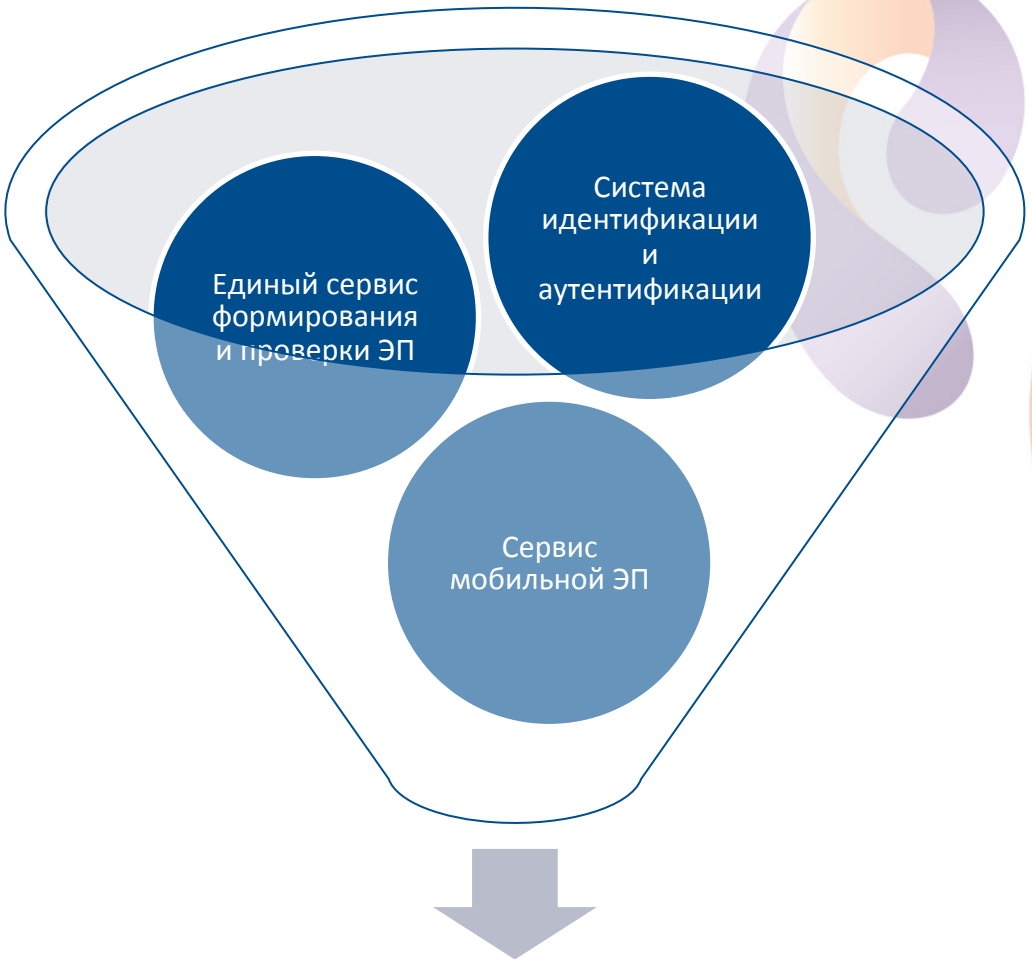


Количество активных пользователей СМУ (около 60 тыс.)



Ростелеком

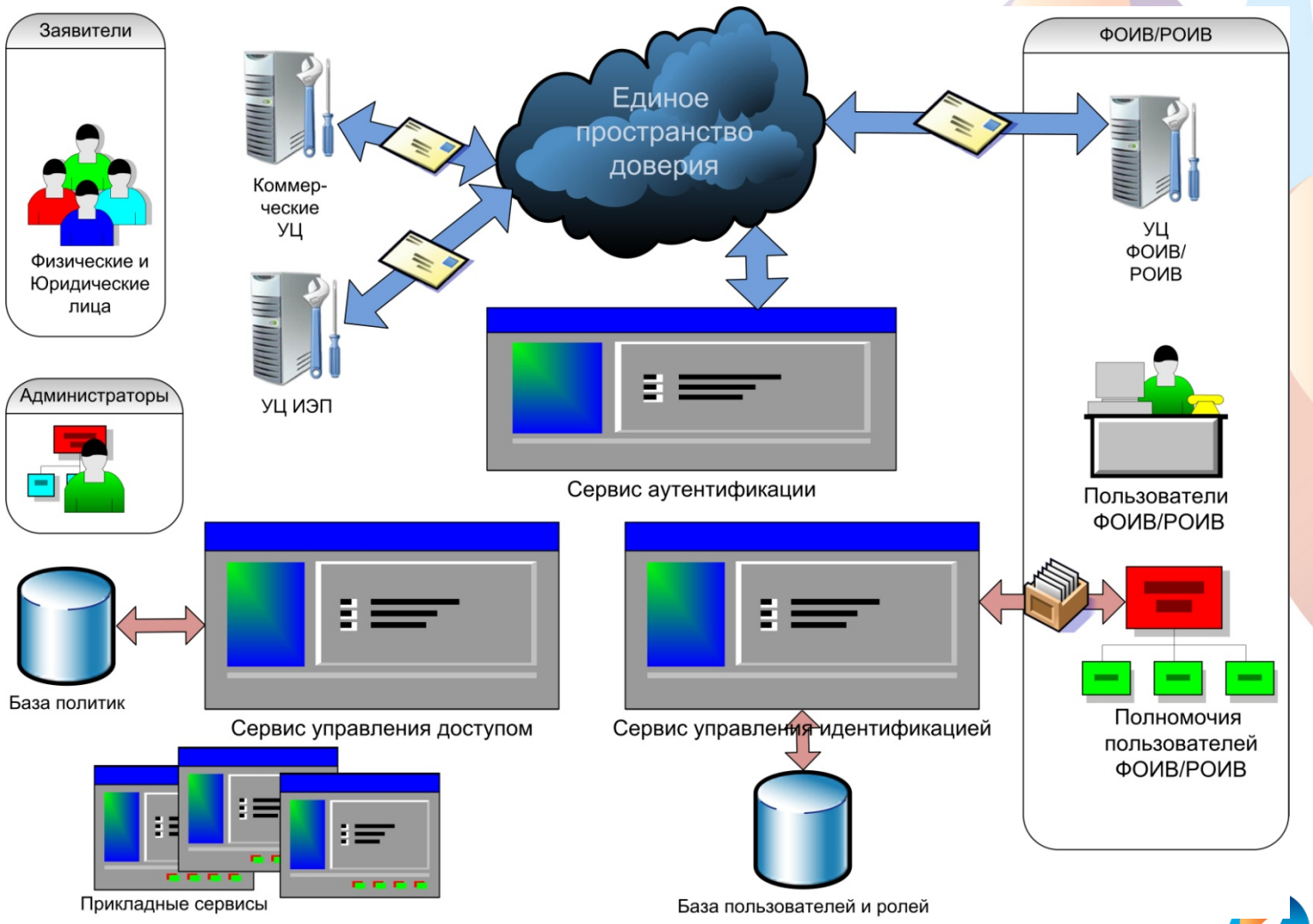
Базовые компоненты обеспечения использования ЭП в инфраструктуре электронного правительства



Инфраструктура обеспечения ЭП

Ростелеком

Система идентификации и аутентификации



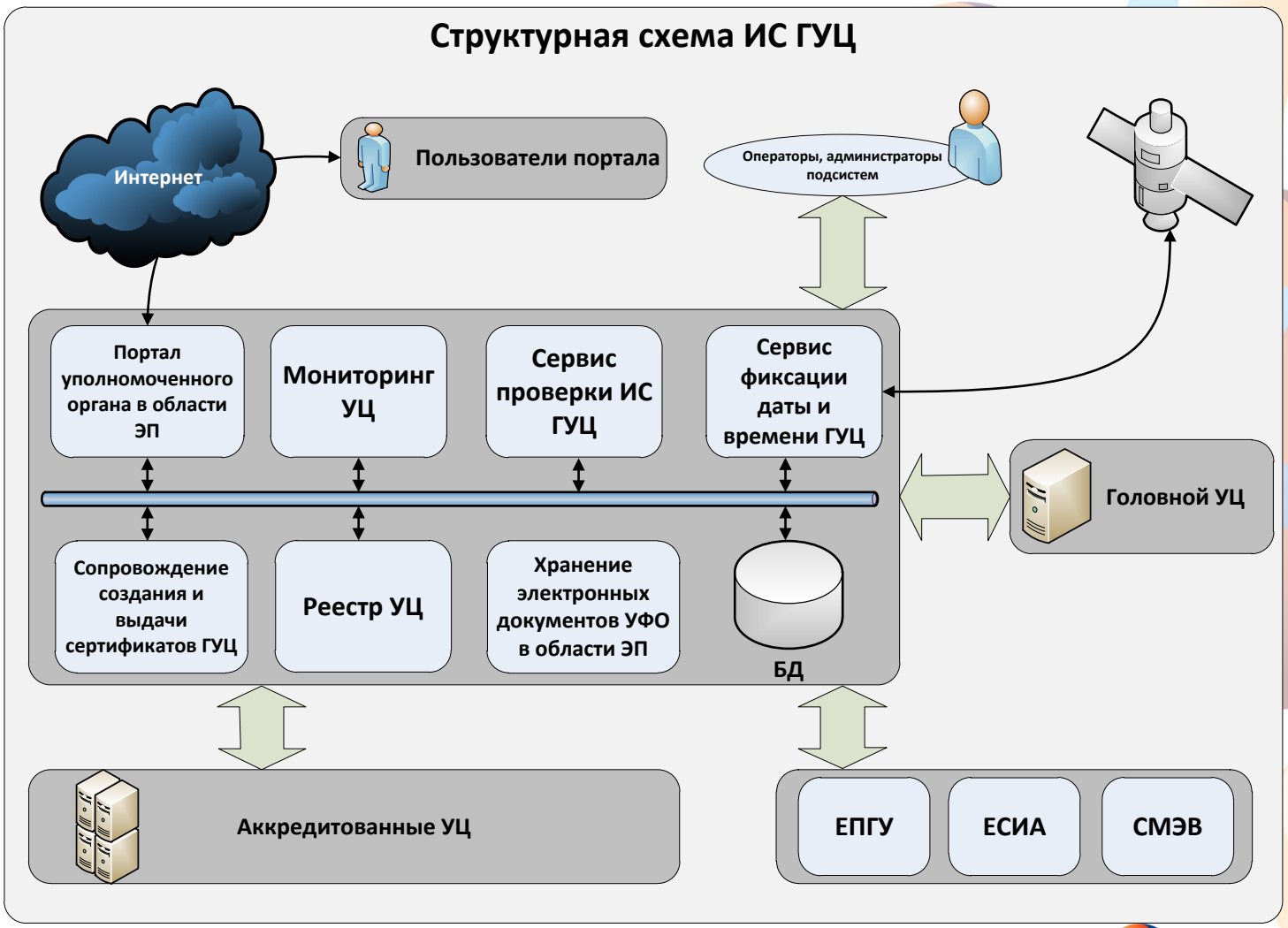
Ростелеком

Уровни достоверности пользователей

1	2	3	4
Регистрация через Интернет, подтверждение Email	Подтверждение личности по Почте РФ или в офисе регистрации. Верификация ФИО, ИНН, СНИЛС	Подтверждение личности в офисе регистрации.	Регистрация ДЛ ОИВ в соответствии с политикой Ведомства
Вход по паролю	Вход по паролю	Вход по ЭП, одноразовым паролям	Вход по ЭП, одноразовым паролям

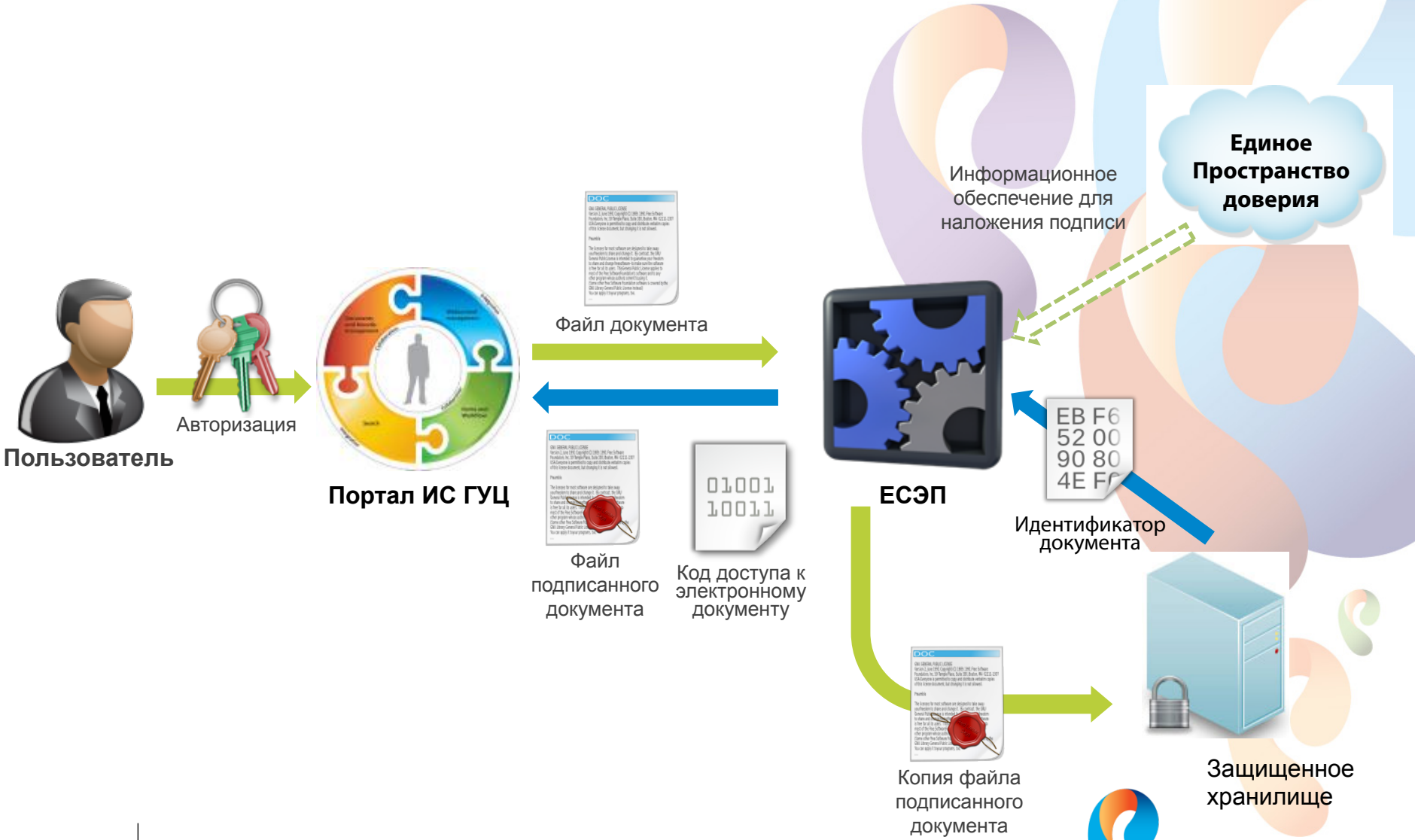
Ростелеком

Сервис формирования и проверки ЭП в ИС ГУЦ



Ростелеком

Электронная подпись as a service ИС ГУЦ



Создание сервиса поддержки мобильной ЭП

Цель работы

- Создание системы на базе УЦ Ростелекома, обеспечивающей предоставление услуги удаленной электронной подписи в интересах пользователей мобильных устройств и платформы облачных вычислений

Преимущества

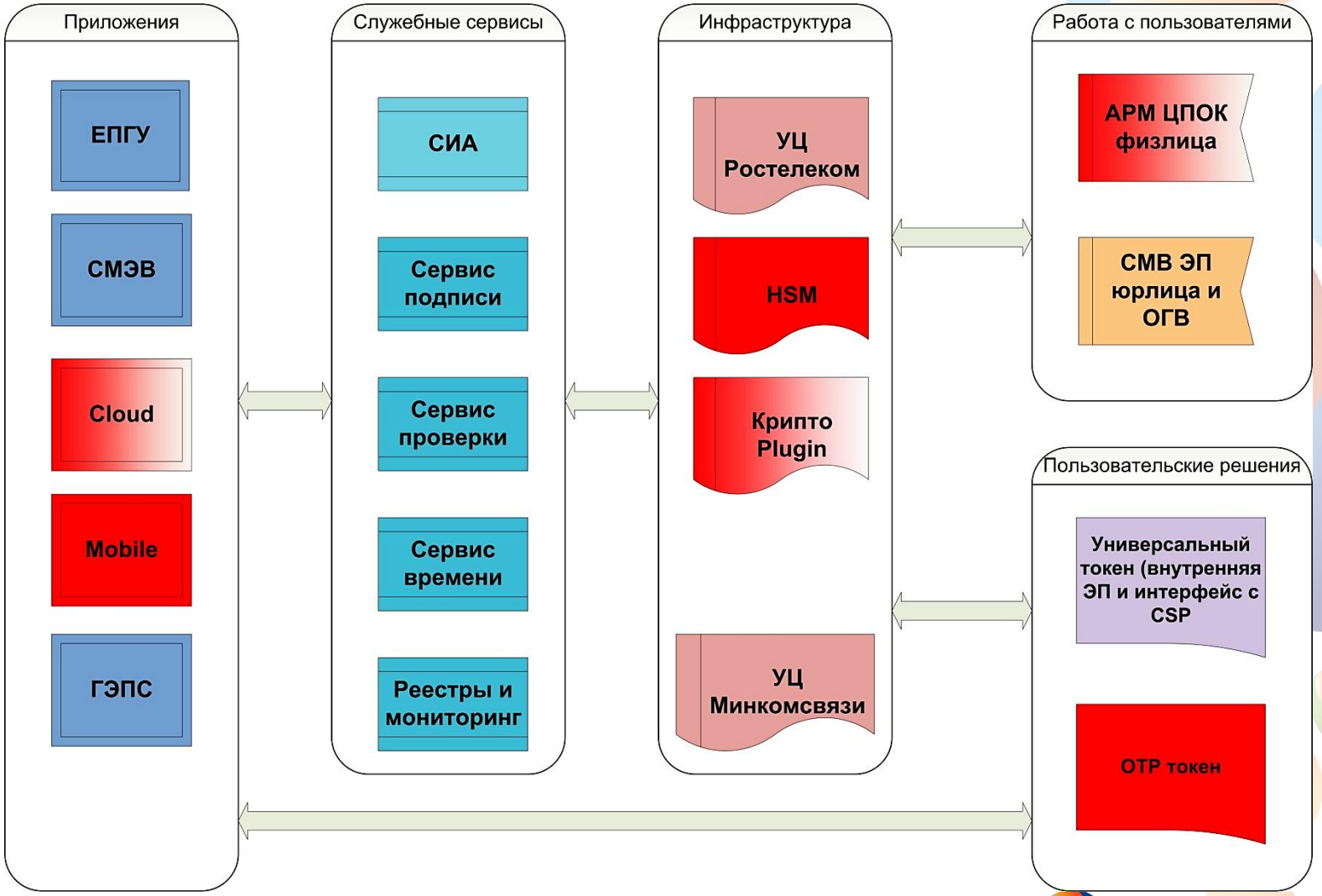
- Возможность централизованного хранения ключей и сертификатов
- Отсутствие требований по криптографии для конечных пользователей
- Возможность использования усиленной аутентификации в ЕСИА

Функции

- Аутентификация пользователей на основе одноразовых паролей
- Обеспечение доверенного доступа к централизованному хранилищу ключей
- Проведение операций ЭП при помощи хранимого ключа ЭП
- Проведение аутентификации пользователей с помощью хранимого ключа ЭП

Ростелеком

Область применения мобильной ЭП



Ростелеком

Задачи обеспечения ИБ при различных формах доступа

Компьютер

- Обеспечение взаимной идентификации и аутентификации пользователей с ПГУ
- Обеспечение ЭП запросов к ПГУ
- Обеспечение конфиденциальности передаваемых ПД
- Обеспечение контроля пользовательской среды
- Определение политик доступа в соответствии с типом услуги и способом доступа к ПГУ
- Аудит действий пользователей ПГУ

Мобильное устройство

- Аутентификация пользователя – по одноразовому паролю, сервера – средствами GSM/3G
- ЭП на стороне оператора (HSM)
- Конфиденциальность данных обеспечивается средствами GSM/3G и VPN между мобильным оператором и ГПУ
- Контроль пользовательской среды невозможен
- Контроль прав доступа осуществляется средствами мобильного оператора и средствами ИЭП (СИА и ПОИБ)

Инфомат

- Аутентификация пользователя по паролю, сервера – по VPN-ключу
- ЭП на внешнем устройстве (токене, карте)
- Конфиденциальность данных обеспечивается VPN туннелем
- Контроль пользовательской среды оператором инфоматов
- Контроль прав доступа и аудит осуществляется средствами ИЭП (СИА и ПОИБ)

Централизованное хранение ключей ЭП: плюсы и минусы

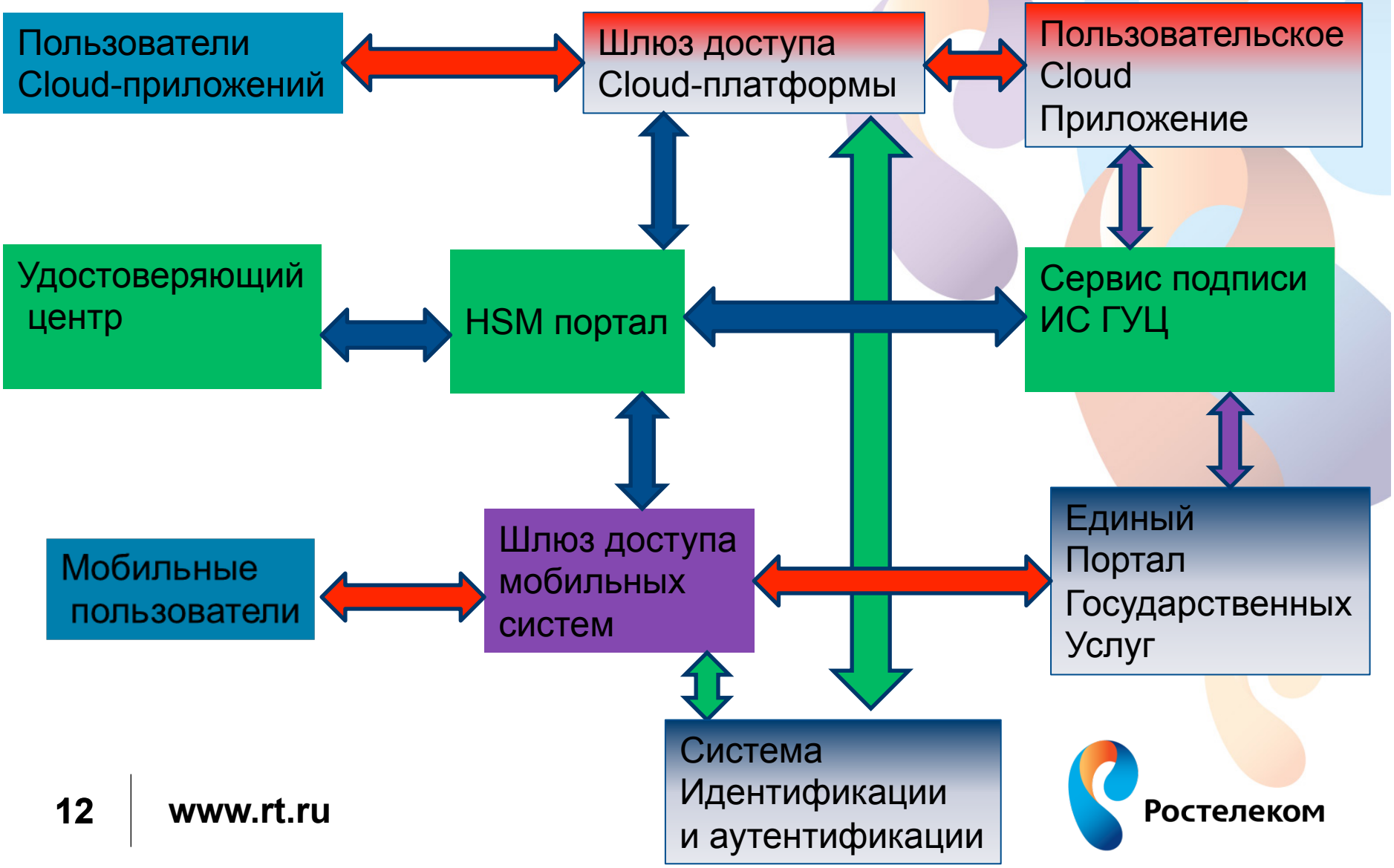
Локальное хранение ключей

- 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

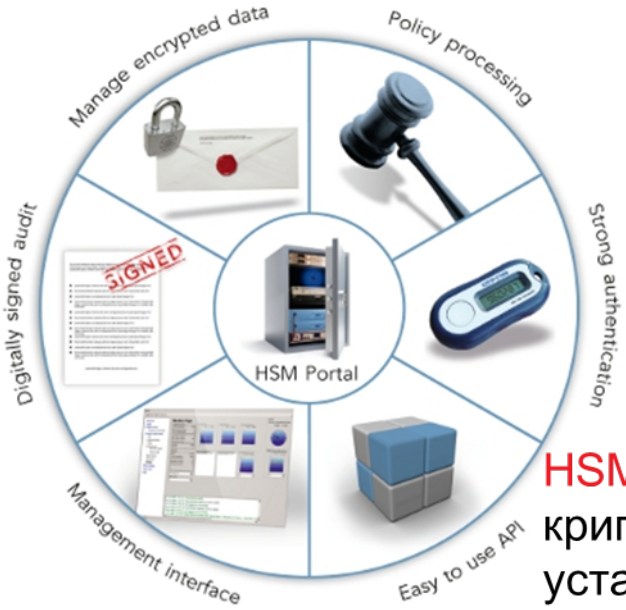
- Ключевой носитель контролируется оператором
- Дополнительная аутентификация на основе одноразовых паролей
- Возможность работы как с порталом, так и с мобильными приложениями
- Нет проблем с производительностью
- Проблема компрометации алгоритма одноразовых паролей
- Шифрование данных на уровне каналов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

Мобильная ЭП – интеграция с ЕСИА ИС ГУЦ и ЕПГУ



Ростелеком

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.

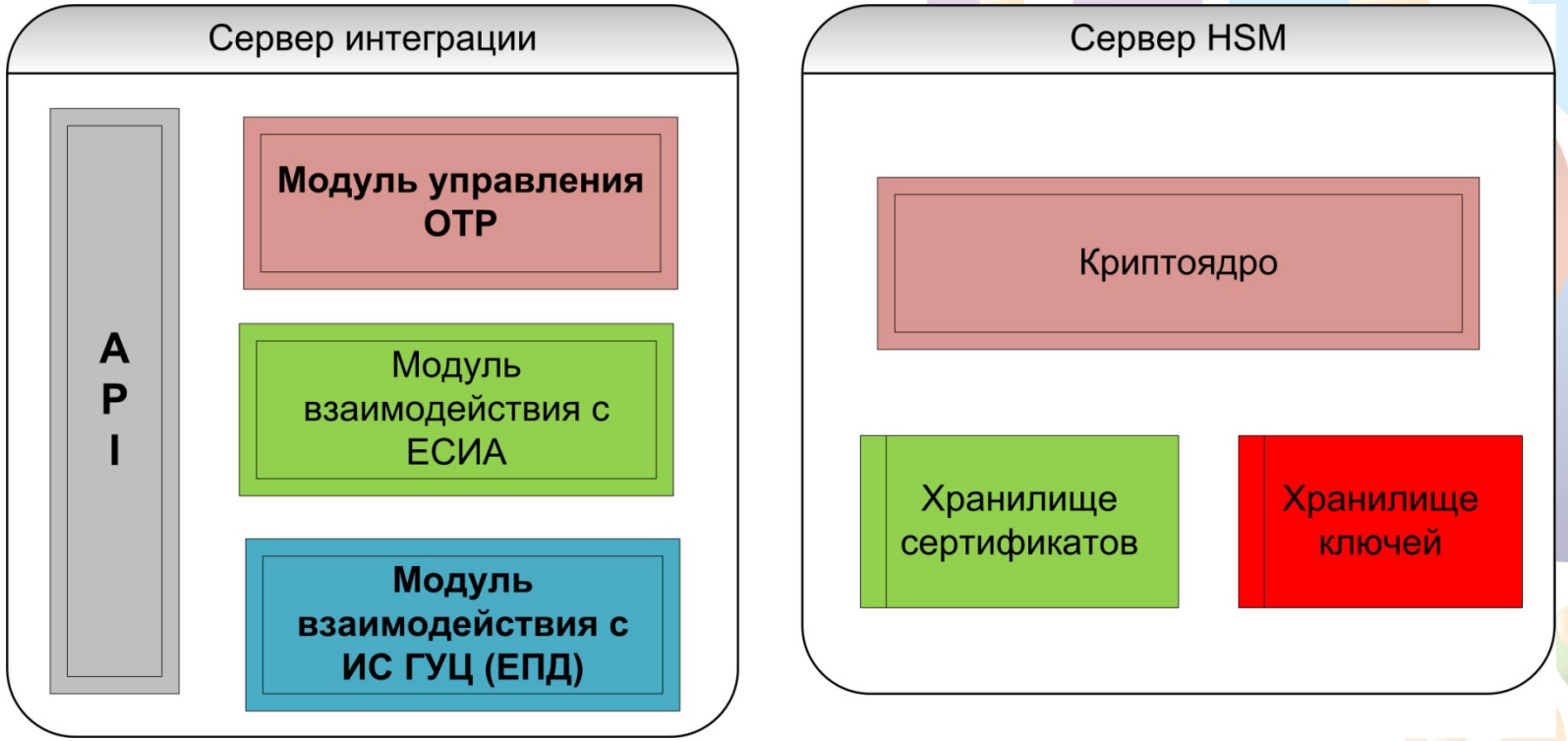
HSM Портал состоит из кластера криптографических серверов, которые устанавливаются между HSM (возможно не одним) и приложениями.

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.

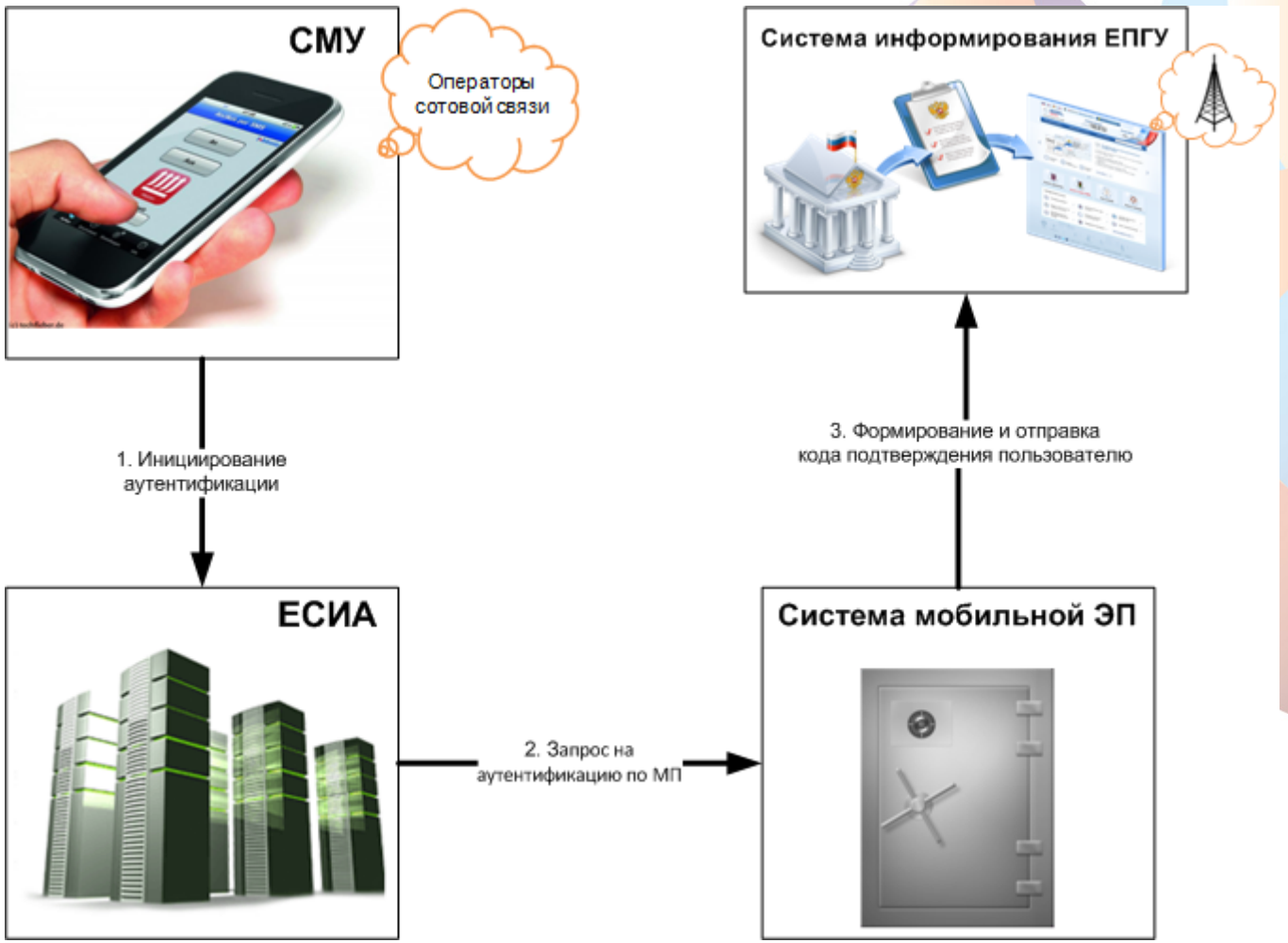
Ростелеком

Структура HSM портала



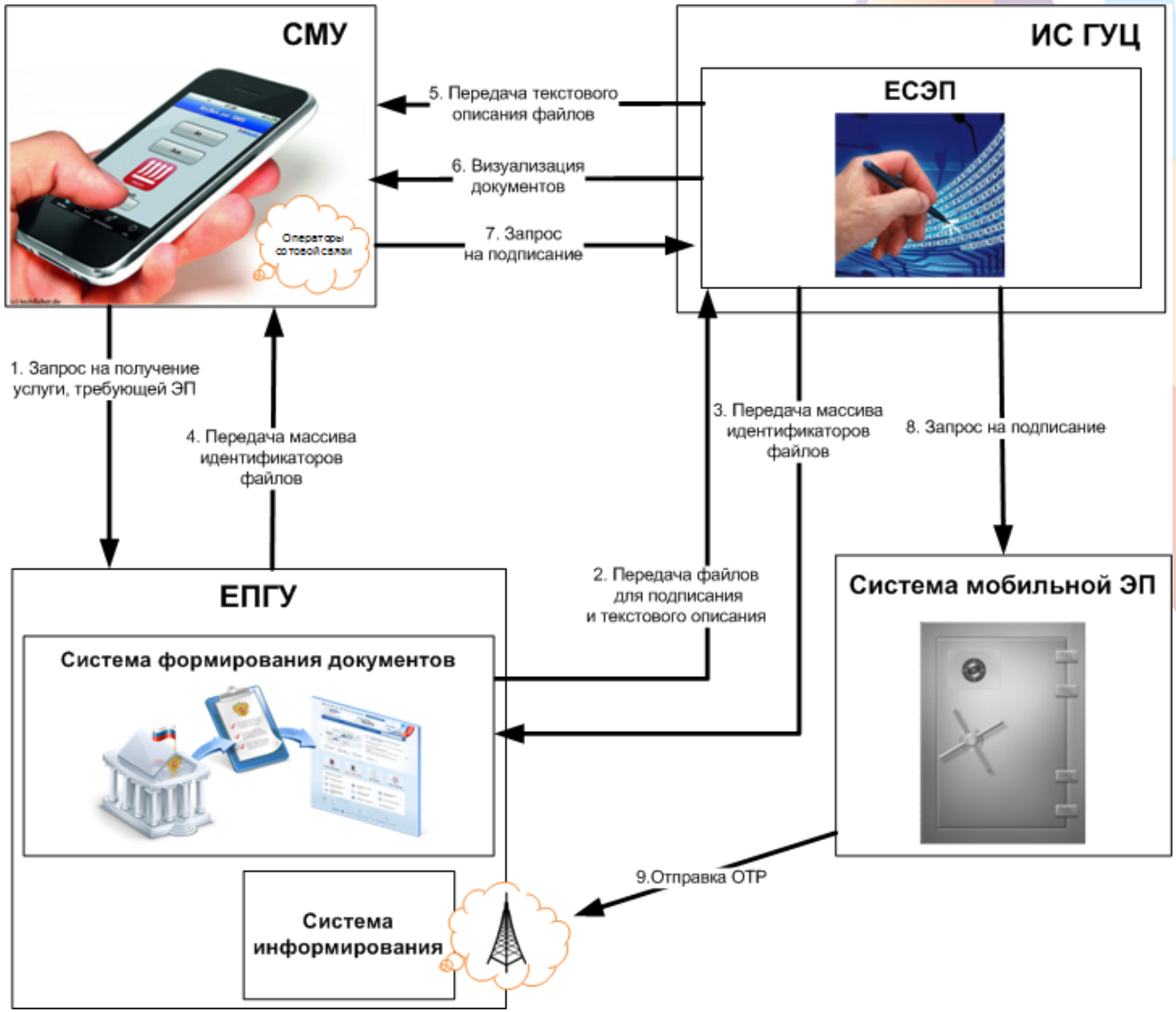
Ростелеком

Идентификация и аутентификация пользователей с использованием сертификата ЭП (фаза 1)



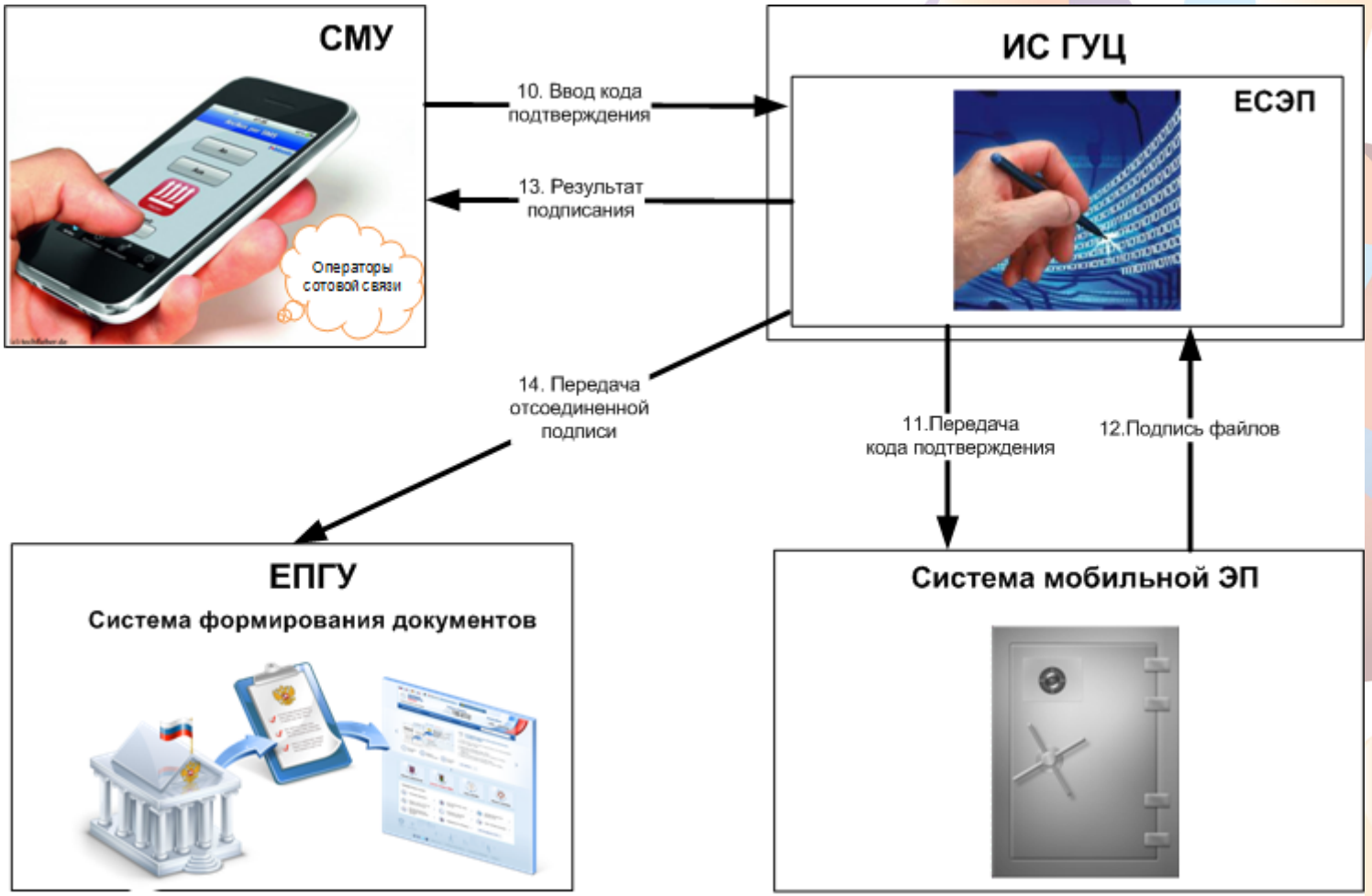
Идентификация и аутентификация пользователей с использованием сертификата ЭП (фаза 2)

Подача заявки на получение услуг с использованием сертификата ЭП (фаза 1)



Ростелеком

Подача заявки на получение услуг с использованием сертификата ЭП (фаза 2)



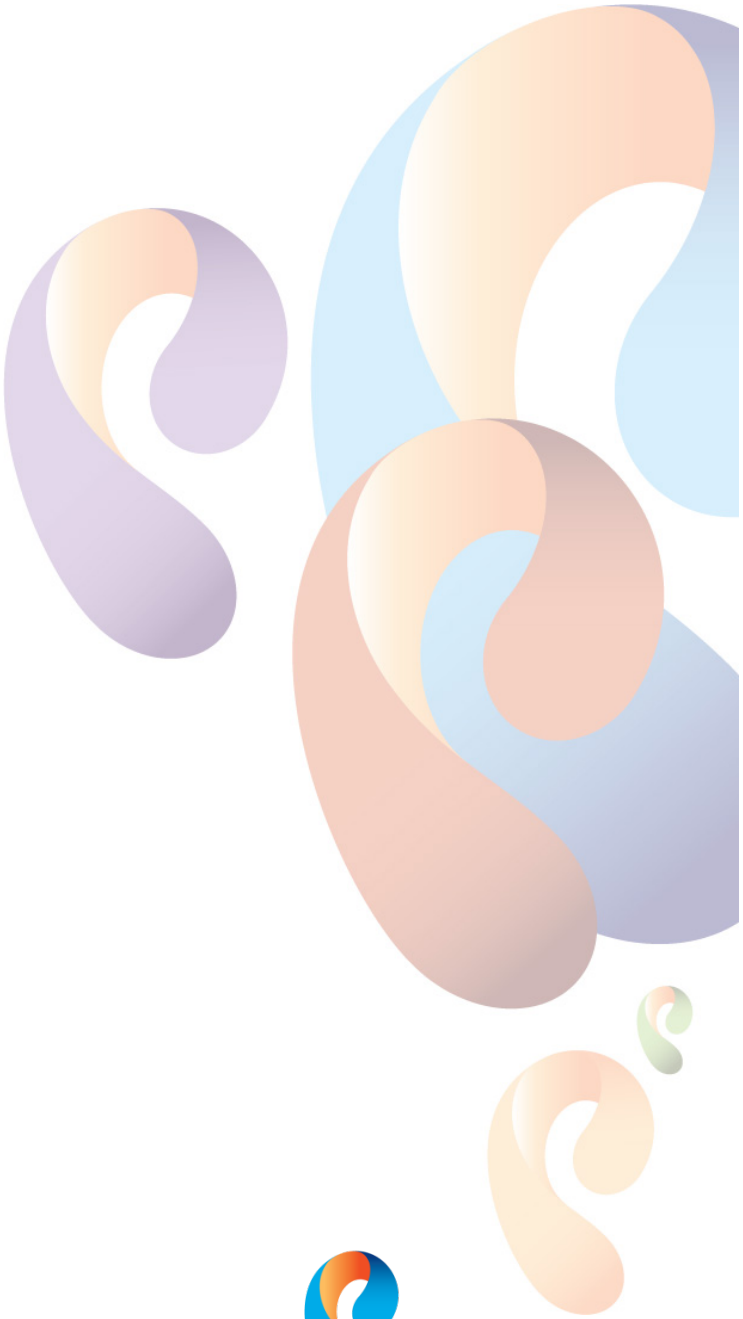
Ростелеком

Заключение

- Доступ к ЕПГУ с мобильных устройств необходим
- Сегодня Server side signature практически безальтернативна как для массового применения так и для облачных приложений
- Структура рисков мобильной подписи существенно отличается от традиционных и проявляется в различных уровнях достоверности
- Технически механизм аутентификации и подписывания реализован
- **В перспективе сервис позволяет разделить ЭП для аутентификации и ЭП для подписывания**

Ростелеком

СПАСИБО



Ростелеком