ФЕДЕРАЛЬНАЯ УПОЛНОМОЧЕННАЯ ОРГАНИЗАЦИЯ

УНИВЕРСАЛЬНАЯ
ЭЛЕКТРОННАЯ
КАРТА

Проект УЭК: средства криптографической защиты информации

РусКрипто, 2012

Оператор проекта ЕПСС УЭК

ЕПСС УЭК - совокупность организаций, взаимодействующих по Правилам ЕПСС УЭК, обеспечивающих реализацию Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» в части, связанной с универсальной электронной картой.

Федеральная уполномоченная организация - ОАО «Универсальная электронная карта» (ФУО ОАО «УЭК») - координатор и оператор проекта по внедрению универсальной электронной карты (Распоряжение Правительства РФ от 12.08.2010 № 1344-р):

- ✓ Организует взаимодействие уполномоченных организаций субъектов
- ✓ Управляет порталом коммерческих услуг
- ✓ Ведет единый реестр карт и приложений (федеральных, региональных, муниципальных)
- ✓ Координирует эмиссию универсальных электронных карт.
- ✓ Является оператором российской платежной системы ПРО100

Приложения УЭК

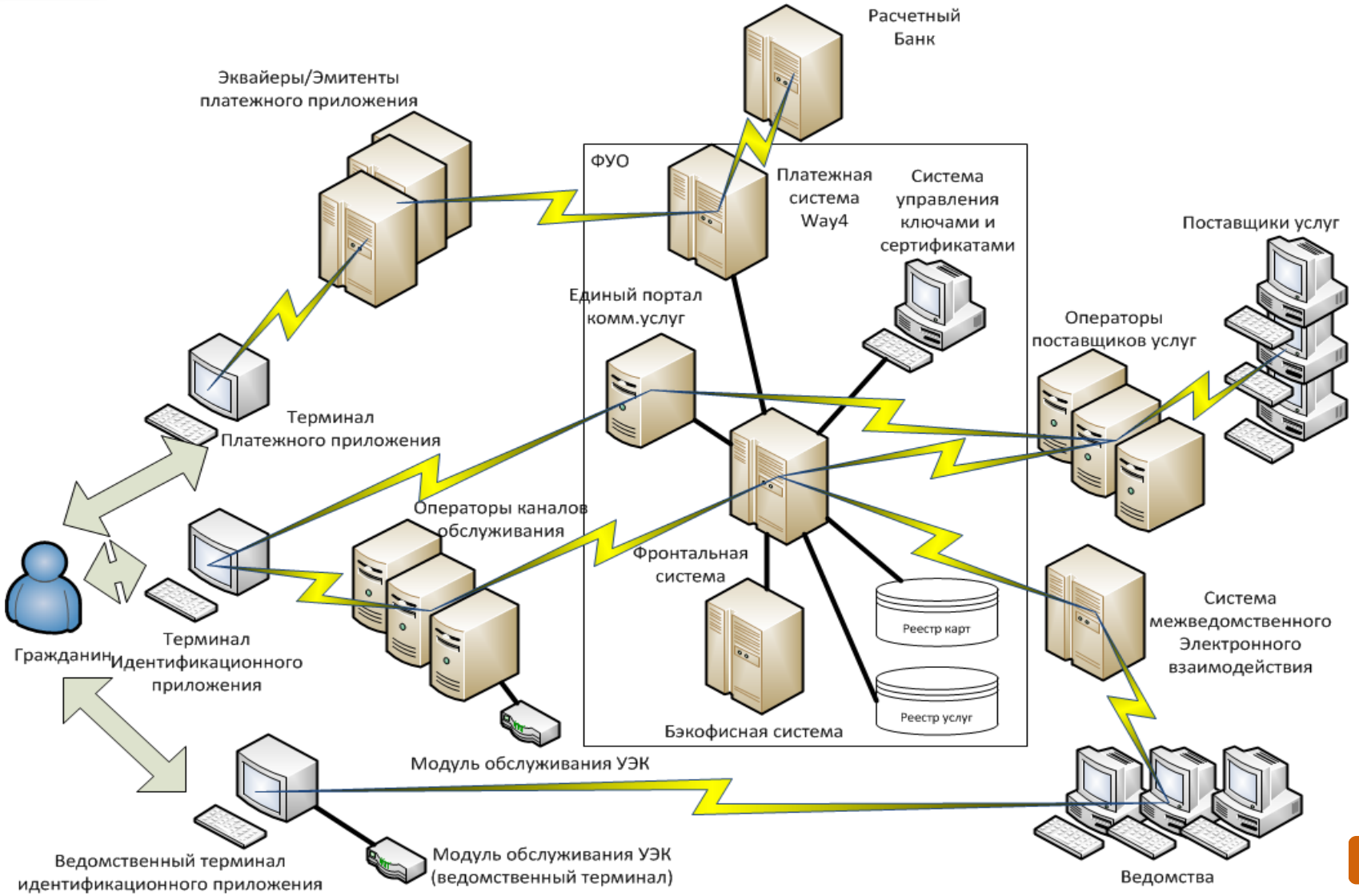
Универсальная электронная карта включает два обязательных федеральных приложения (ID и Банковское), а также может содержать региональные приложения, что позволяет оказывать широкий спектр услуг гражданам, формируя индивидуальные пакеты

Федеральная часть

Региональная часть

Единое ID-приложение	ПРО100		
ID-данные	Банковское приложение	Единое транспортное приложение	Прочие приложения
Область данных			
Область данных			
Область КЭП			
Региональное транспортное приложение	Прочие региональные приложения		

ЕПСС УЭК


Расчетный Банк
Эквайеры/Эмитенты платежного приложения
ФУО
Платежная система Way4
Система управления ключами и сертификатами
Поставщики услуг
Единый портал комм.услуг
Операторы поставщиков услуг
Терминал Платежного приложения
Операторы каналов обслуживания
Фронтальная система
Гражданин
Терминал Идентификационного приложения
Реестр карт
Система межведомственного Электронного взаимодействия
Реестр услуг
Бэкофисная система
Модуль обслуживания УЭК
Ведомственный терминал идентификационного приложения
Модуль обслуживания УЭК (ведомственный терминал)
Ведомства

Класс СКЗИ в ЕПСС УЭК

Компонент ЕПСС	Класс СКЗИ (требования ФСБ РФ)
Универсальная электронная карта	**КС3**
ИС ФУО (внутренний контур)	**КВ2**
ИС ФУО (при взаимодействии с ЦИ и ЦП)	**КВ2**
ИС ФУО (при взаимодействии с УОС, ОКО, …)	**КС3**
ИС Уполномоченной организации субъекта РФ	**КС3***
ИС Центра изготовления (внутренний контур и связь с ФУО)	**КВ2***
ИС Центра персонализации (внутренний контур и связь с ФУО)	**КВ2***
ИС Оператора канала обслуживания (для канала между терминалом и серверной частью ИС ОКО)	**КС1***
ИС Оператора канала обслуживания (при взаимодействии с ФУО и др.)	**КС3***

* Окончательное определение класса СКЗИ – на основе частной модели угроз и нарушителя для конкретной ИС с учетом особенностей функционирования и необходимости обеспечения общего уровня защиты

Механизмы защиты

- Управление контентом карты защищенным образом
- Аутентификация картой терминала
- Аутентификация гражданина-владельца карты
- Аутентификация ИД-приложения
- Электронная подпись держателя УЭК
- Защищенный канал между терминалом и ПУ
- Аутентификация терминалом ПУ
- Шифрование передачи данных в каналах связи

Управление контентом карты

- Главные шифровальные ключи (ключи главного домена безопасности) УЭК предназначены для управления составом приложений УЭК и их состоянием.
- Наличие ГШК в УЭК - обязательно. Для каждого экземпляра УЭК - уникальный ГШК.
- Управление составом приложений - только с применением ГШК. ГШК не используются в целях, отличных от управления составом приложений УЭК и их состоянием.
- Порядок изготовления ГШК – согласован с ФСБ
- До 30 сентября 2012 г. допустимо применение зарубежной криптографии при выпуске карт.

Аутентификация терминала

- ✓ Механизм аутентификации терминала является обязательным и применяется в отношении обслуживающего терминала во всех случаях использования ИД-приложения
- ✓ Алгоритмы: RSA|ГОСТ
- ✓ ИД-приложение:
  - ✓ проверяет цепочку сертификатов терминала
  - ✓ убеждается - терминал владеет соответствующим закрытым ключом
  - ✓ проверяет сроки действия каждого сертификата
  - ✓ получает сведения о полномочиях терминала из сертификатов открытых ключей
- ✓ По результатам аутентификации терминала между ИД-приложением и терминалом устанавливается канал для защищённого обмена сообщениями (сеансовый ключ, выработанный с применением ключей аутентификации)

Аутентификация держателя

Виды ПИН-кодов:

- основной ПИН (ПИН1) – право Держателя использовать карту УЭК;
- ПИН электронной подписи (ПИН2) – разрешение держателя карты УЭК на формирование квалифицированной электронной подписи;
- код разблокировки ПИН (КРП) – возможность держателю карты УЭК разблокировать заблокированный ПИН1 или ПИН2.

Требования по длине ПИН-кода:

- основной ПИН – от 4 до 8 цифр;
- ПИН электронной подписи – от 6 до 8 цифр;
- код разблокировки ПИН – 8 цифр.

Аутентификация ИД-приложения

Обеспечивает получение ОКО/ПУ подтверждения от ФУО факта подлинности УЭК:

- В процессе ФУО получает информацию, позволяющую подтвердить применение УЭК для оказания услуги, подтверждает достоверность УЭК и идентифицирует держателя.
- Аутентификация возможна в двух режимах:
  - в режиме 'online' запрос направляется в ИС ФУО. Используются алгоритмы симметричной криптографии (DES/ГОСТ).
  - в режиме 'offline' запрос направляется МО. Используются алгоритмы асимметричной криптографии (RSA/ГОСТ).
- В результате ФУО (явно, через ИС ФУО, или посредством МО) предоставляет ОКО документ результата аутентификации, заверенный своей подписью.

Электронная подпись

Формирование квалифицированной электронной подписи держателя УЭК.

- ✓ Вычисление осуществляется ИД-приложением при оформлении запроса на оказание услуги в терминале. Перед вычислением терминал (криптопровайдер на нем) должен убедиться, что:
  - ✓ механизм электронной подписи держателя карты УЭК подключён (присутствует квалифицированный сертификат ключа проверки подписи);
  - ✓ срок действия квалифицированного сертификата является действительным.
- ✓ Проверка электронной подписи держателя карты УЭК осуществляется ПУ при проверке запроса на оказание услуги.

Защищенный канал с ПУ

Обеспечивает конфиденциальность данных при обмене терминала и ПУ в ходе оказания услуги (абонентское шифрование):

- запрос на оказание услуги;
- ответ на запрос оказания услуги.

Используется сессионный ключ, формируемый для каждого случая оказания услуги.

Предполагает выполнение следующих процедур:

- настройка защищённого канала;
- защищённая передача запроса на оказание услуги;
- защищённое получение ответа на запрос на оказания услуги.

В зависимости от выбора ПУ могут применяться:

- ГОСТ Р 34.10.2001, ГОСТ 28147-89;
- RSA, DES.

Аутентификация терминалом ПУ

Обеспечивает контроль достоверности данных, полученных в ответе на запрос оказания услуги.

Включает процедуры:

- формирование ПУ ЭП ответа на запрос оказания услуги;
- проверка терминалом ЭП ответа на запрос.

Положительный результат проверки ЭП ПУ:

- свидетельствует о неизменности данных ответа;
- удостоверяет, что ответ отправлен именно этим ПУ.

Система управления ключами

Система управления ключами и сертификатами ЕПСС УЭК обслуживает технологические процессы выпуска и обслуживания карт:

- Генерация ключей главного домена безопасности (главных шифровальных ключей) карт для управления контентом карты;
- Генерация ключей для взаимной аутентификации технических компонентов ЕПСС УЭК (ИД-приложения, терминалов, систем операторов каналов обслуживания);
- Генерация транспортных ключей для обмена защищаемой информацией между техническими системами ЕПСС УЭК.

Для отдельных функциональных элементов системы используются внешние УЦ:

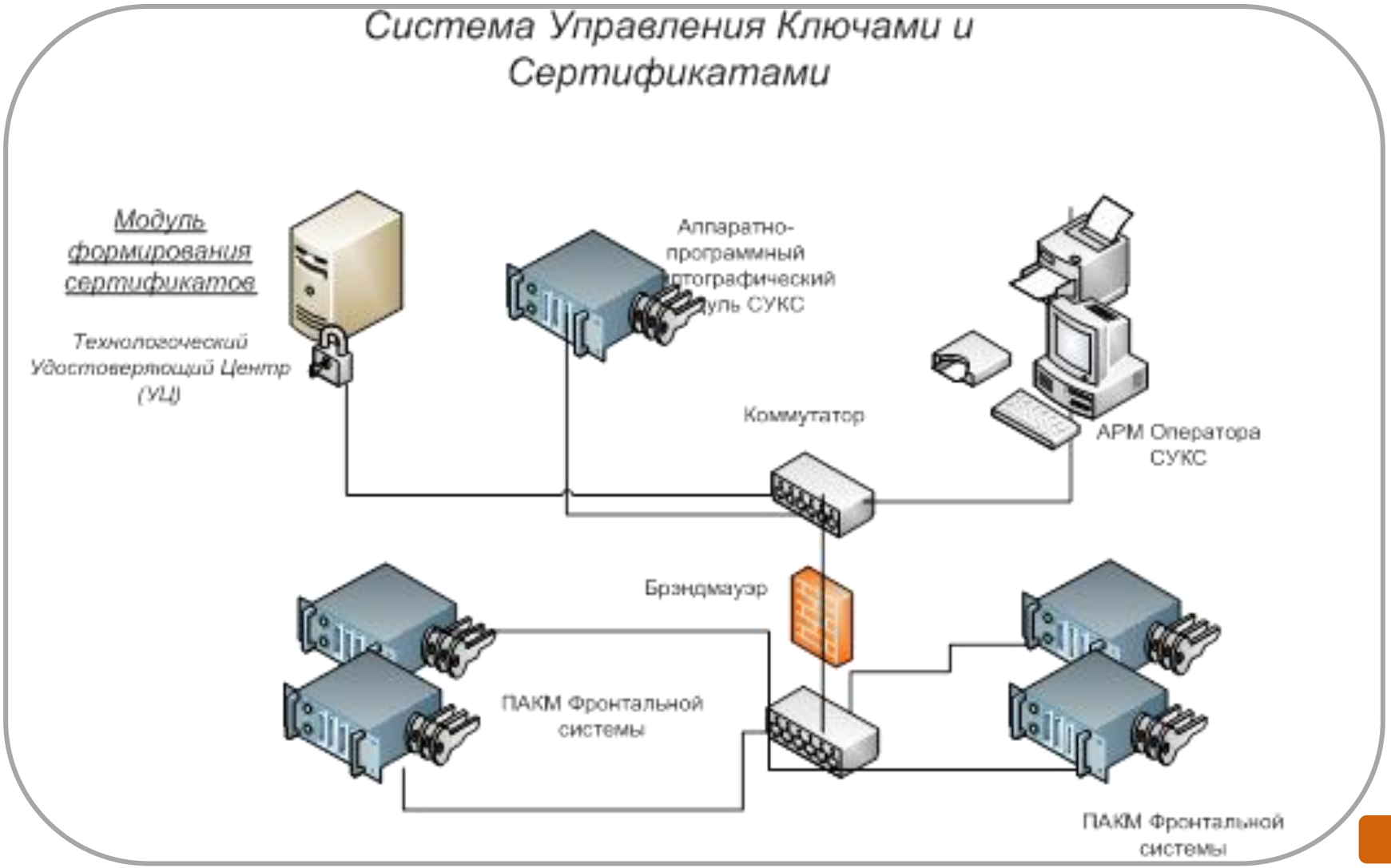
- УЦ Системы электронного документооборота участников ЕПСС УЭК;
- УЦ для выдачи сертификатов электронной подписи гражданина.

Система управления ключами

Существенные требования к данной системе:

- поддержка международных стандартов в части инфраструктуры открытых ключей (форматы сертификатов x.509, CVC);
- поддержка международных стандартов карточной индустрии (в первую очередь речь идет о группе стандартов 7816, Global Platform и применении зарубежной криптографии DES, RSA – в последующем – только в платежном приложении);
- поддержка российских стандартов криптографии ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, включая рекомендованные ФСБ России параметры криптоалгоритмов.

Система управления ключами

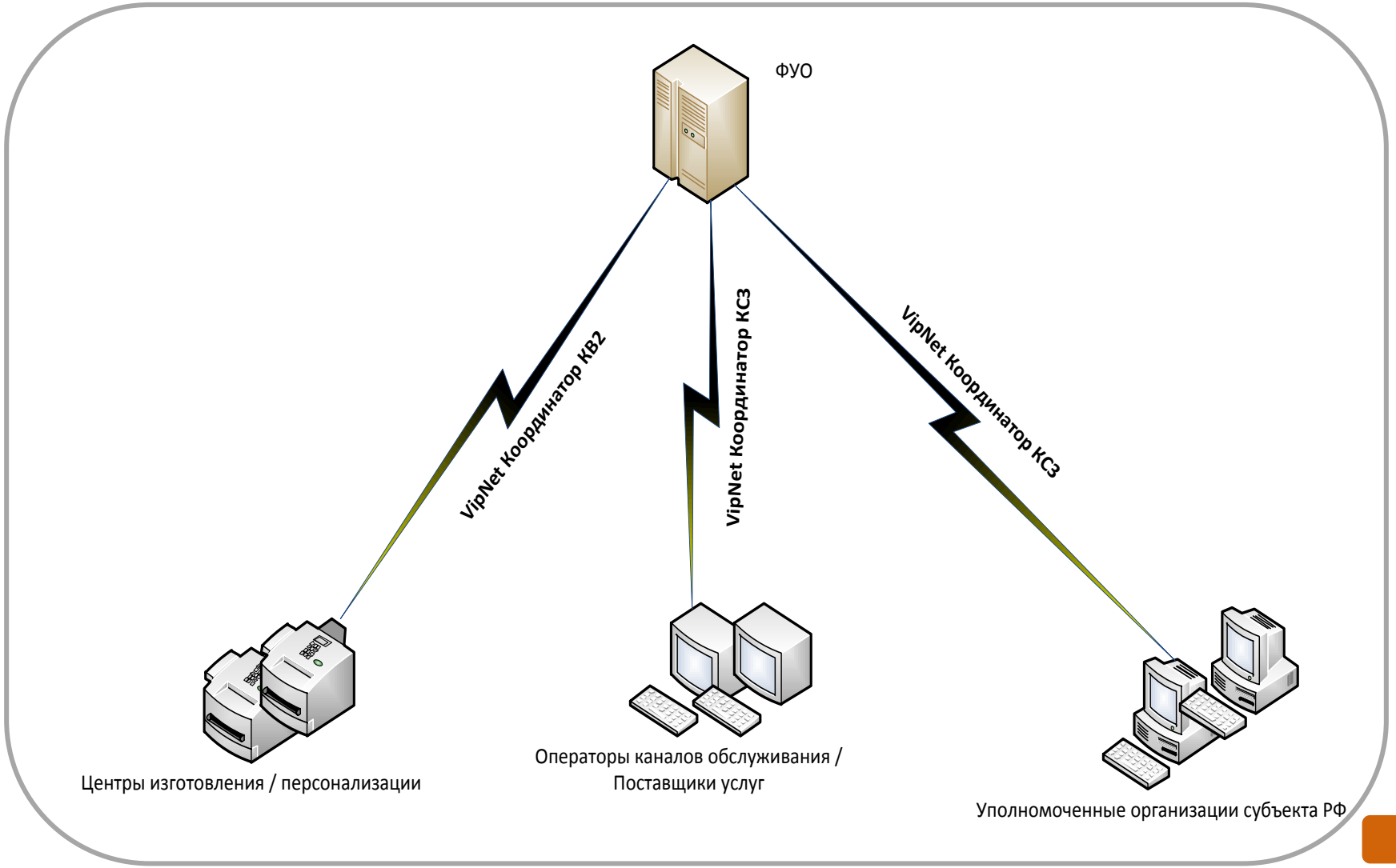


Внешние поставщики услуг

- Внешний документооборот (между участниками ЕПСС УЭК) – привлекается внешний УЦ, выбранный на конкурсной основе (Такском).

- Ключи и сертификаты для функции квалифицированной подписи держателей карт УЭК – предусматривается возможность гражданина обратиться в любой аккредитованный УЦ (оснащенный средствами криптографической защиты информации, умеющими работать с картой УЭК).

Защита каналов с Участниками



Статус проекта

- Разработано федеральное идентификационное приложение, включающее область данных ФОМС, ПФР, ЭП
- Запущена опытная эксплуатация всех информационных систем ФУО, включая инфраструктуру ПРО100
- Разработаны типовые решения для автоматизации УОС совместно с рядом ИТ-интеграторов
- Министерством связи и массовых коммуникаций РФ подписано соглашение о подключении ОАО «УЭК» к СМЭВ
- Чипы производителей прошли тематические исследования.

Контактная информация

Азин Дмитрий Вячеславович
начальник отдела по защите коммерческой тайны и персональных данных
Azin-dv@uecard.ru

Федеральная уполномоченная организация - открытое акционерное общество «Универсальная электронная карта»

119021, Москва, улица Тимура Фрунзе дом 11, стр. 15

Тел./Факс: +7 495 777 13 27

E-mail: info@uecard.ru

www.uecard.ru

Федеральный контакт-центр : 8 800 775 77 77

БЛАГОДАРИМ ЗА ВНИМАНИЕ!