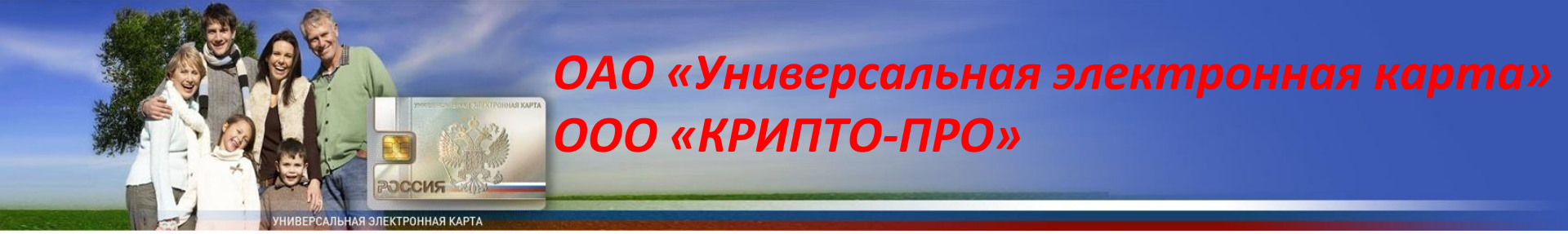


ОАО «Универсальная электронная карта»

ООО «КРИПТО-ПРО»

Общие принципы обеспечения безопасности информации при выпуске и обслуживании универсальной электронной карты

От ООО «КРИПТО-ПРО»

Попов Владимир Олегович к.ф.м.н. Начальник отдела

От ОАО «Универсальная электронная карта»

Звейник Владимир Карлович Начальник управления безопасности

2011

Назначение УЭК

- *Универсальная электронная карта – это унифицированная общенациональная масштабируемая инфраструктура доставки государственных, региональных, муниципальных и коммерческих услуг гражданам в электронном виде.*
- *Универсальная электронная карта – это общенациональный сервис удостоверения личности гражданина как в очной, так и в электронной форме, а также формирования его электронной подписи средствами карты.*
- *Универсальная электронная карта – это национальная платежная система.*
- *Универсальная электронная карта – это открытая инфраструктура для унифицированного подключения большого количества поставщиков электронный услуг и сервисов.*
- *Универсальная электронная карта – это безопасный и удобный доступ гражданина ко всем нужным ему услугам в любом регионе, в любом устройстве (банкомат, инфомат, телефон, персональный компьютер и т.п.), в любое удобное время и в любом режиме (он-лайн или офф-лайн).*

Содержимое карты

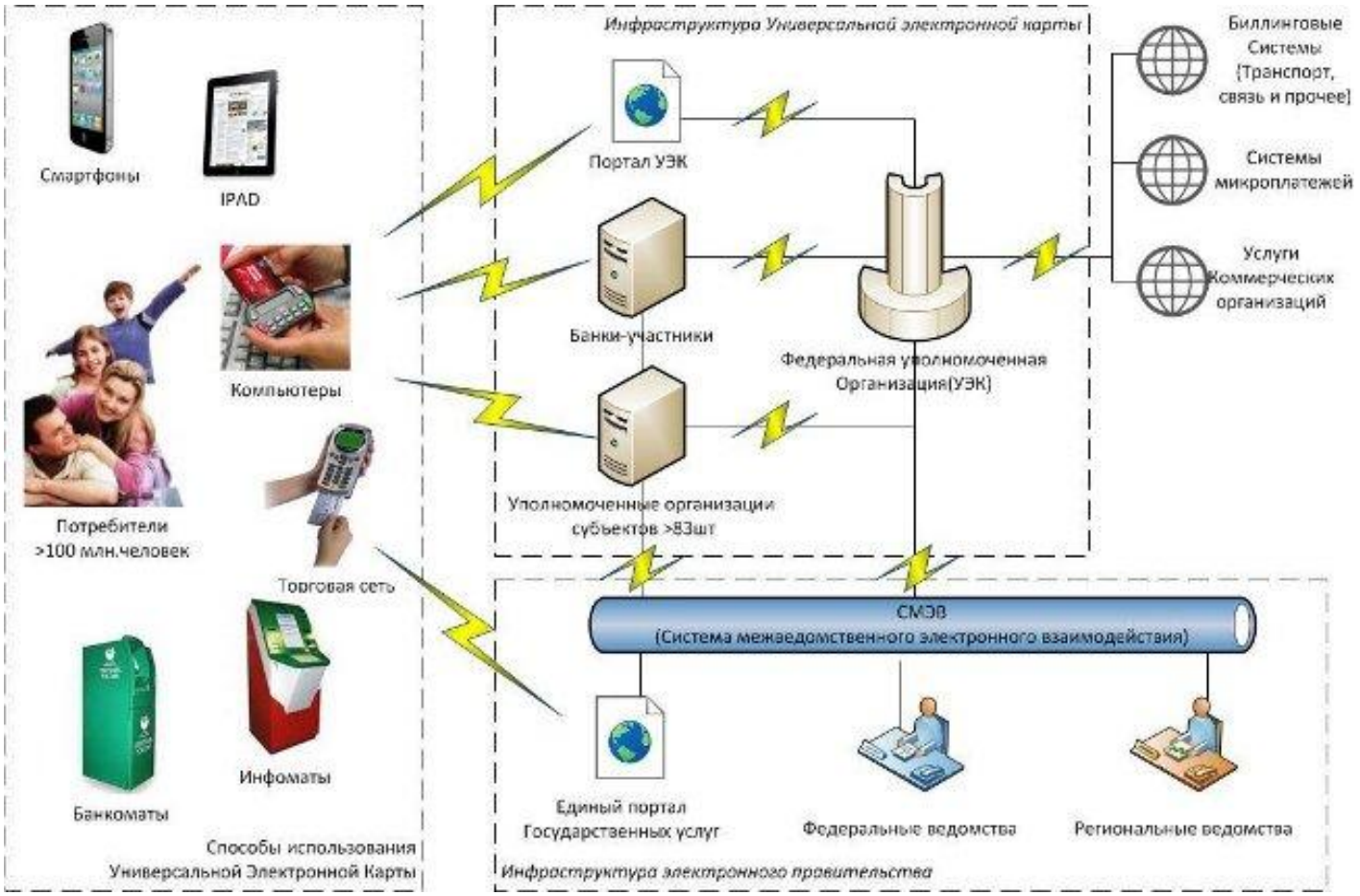
Федеральная часть:

- Единое идентификационное приложение
  - Идентификационная область
  - Область эмитента приложения (ФУО)
  - Область ПФР
  - Область ФОМС
  - Области других федеральных поставщиков услуг
- Единое транспортное приложение
- «Личный кейс» (дисконтные купоны, электронные билеты, карты лояльности)
- Прочие приложения федерального уровня
- Банковское приложение

Региональная часть:

- Региональные транспортные приложения
- Прочие приложения регионального уровня

Инфраструктура УЕК



Инфраструктура универсальной электронной карты должна активно взаимодействовать с создаваемой инфраструктурой электронного правительства.

Участники системы

Системообразующие участники:

- Уполномоченные организации субъектов
- Федеральная уполномоченная организация
- Банки-эмитенты платежного продукта
- Операторы каналов обслуживания
- Поставщики услуг

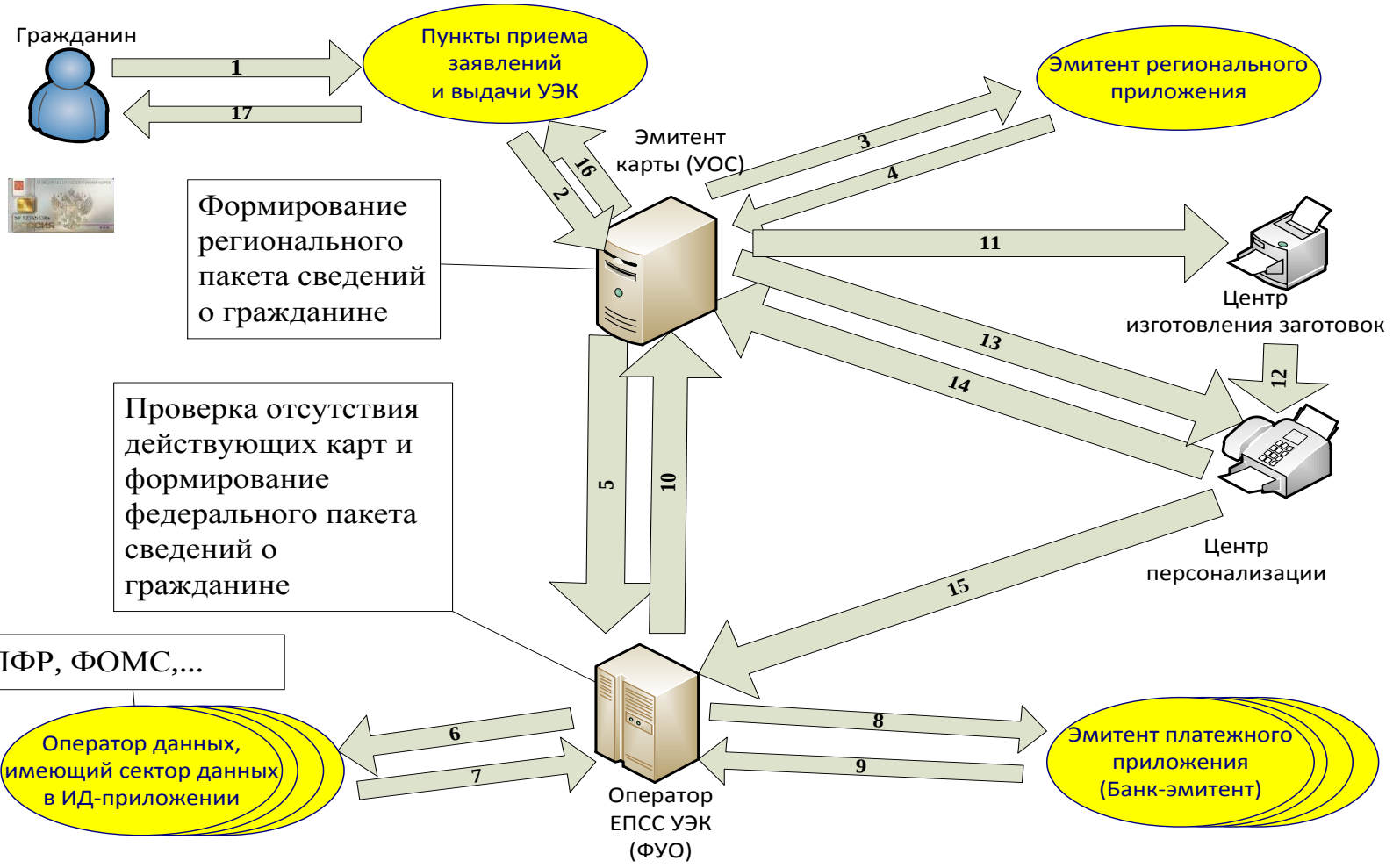
Обеспечение эмиссионного процесса:

- Пункты приема заявлений
- Пункты выдачи карт
- Центры изготовления заготовок
- Центры персонализации заготовок

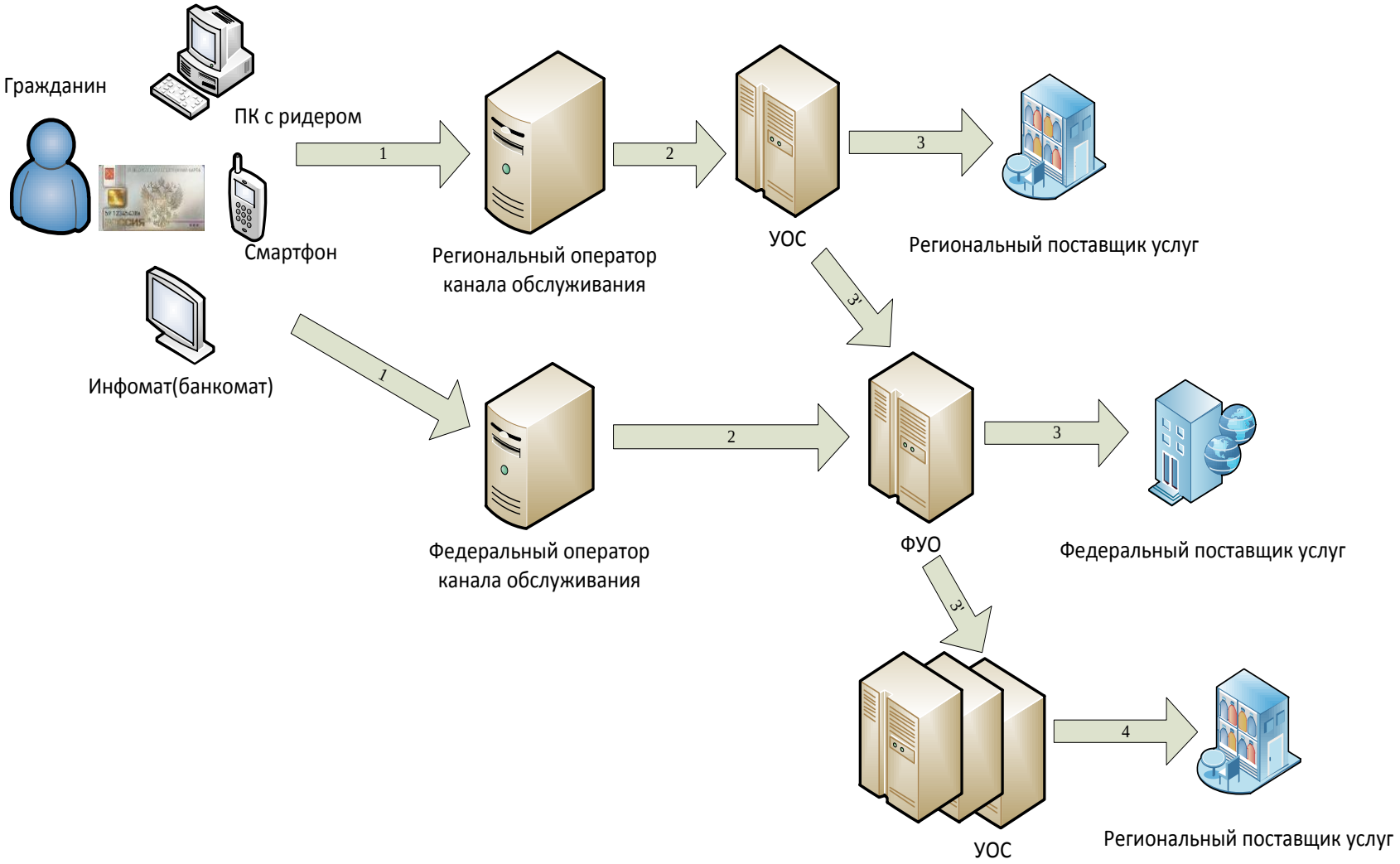
Технологическое обеспечение:

- Операторы каналов связи
- Центры обработки данных
- Удостоверяющие центры
- Операторы УОС
- Логистические операторы

Выпуск карты



Обслуживание карты



Механизмы защиты

Механизмы защиты в ЕПСС УЭК:

- Взаимная аутентификация карты и терминала (сертификаты открытых ключей);
- Аутентификация гражданина-владельца карты при получении данных с карты (карта+ПИН);
- Аутентификация криптограммы с запросом на услугу в ИС ФУО (симметричные ключи);
- Авторизация запроса на услугу перед поставщиком услуги со стороны ФУО (ЭЦП);
- Защита ведомственных блоков данных в соответствии с ведомственными требованиями;
- Шифрование передачи данных в каналах связи.

Данные УЭК

Универсальная электронная карта содержит следующие визуальные (незащищенные) сведения:

- Фамилию, имя и (если имеется) отчество пользователя универсальной электронной картой
- Фотографию заявителя (в случае выдачи универсальной электронной карты по заявлению гражданина в порядке, установленным законом)
- Номер универсальной электронной карты и срок её действия
- Контактная информация уполномоченной организации субъекта Российской Федерации
- Страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования Российской Федерации

Защита персональных данных

Согласие на обработку персональных данных

Включено в заявление гражданина на выдачу карты, составлено в соответствии с требованиями Закона «О персональных данных» и содержит пункт о том, что:

- Персональные данные обрабатываются посредством
- следующих действий: сбор; систематизация; накопление;
- хранение; уточнение (обновление, изменение);
- использование; передача информации для обеспечения
- выпуска, выдачи и обслуживания универсальной
- электронной карты и электронных приложений;
- обезличивание; блокирование; уничтожение.

Принципы обеспечения безопасности

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечены еѐ (их) конфиденциальность, доступность и целостность.

• Конфиденциальность: свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

• Целостность: неизменность информации в процессе ее передачи или хранения.

• Доступность: свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

• Модель угроз, модели нарушителей, требования по защите данных на всех этапах жизненного цикла карты разрабатываются и согласовываются с ФСБ.

•Управление рисками и «Правила ЕПСС УЭК» (подготовлены Федеральной уполномоченной организации в соответствии со статьей 28 Федерального закона от 27 июля 2010 года «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ).

•При решении задач по обеспечению информационной безопасности будут реализованы требования по конфиденциальности, доступности и целостности информации.

Принцип законности в обеспечении безопасности

Федеральные законы Российской Федерации

- «Об информации, информационных технологиях и о защите информации» (от 27 июля 2006 г. № 149-ФЗ)
- «О коммерческой тайне» (от 29 июля 2004 г. №98-ФЗ)
- «О персональных данных» (от 27 июля 2006 г. №152-ФЗ)

Управление ключами и сертификатами

Система управления ключами и сертификатами (включает ИОК) - существенные требования :

- поддержка международных стандартов в части инфраструктуры открытых ключей (RFC);
- поддержка международных стандартов карточной индустрии (7816, Global Platform, DES, RSA);
- поддержка российских стандартов криптографии ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.

Некоторые этапы

30 ноября 2010	- разработана основная НПБ
30 декабря 2010	- готова спецификация ИД-приложения
01 марта 2011	- опубликованы требования и типовая архитектура УОС
30 марта 2011	- готово ИД-приложение
30 мая 2011	- выпуск Правил ФУО
01 июля 2011	- начало присоединения участников
30 сентября 2011	- опытный запуск всех систем ФУО
01 декабря 2011	- боевой запуск 100% систем ФУО и пилотных субъектов РФ

GlobalPlatform – архитектурная база УЕК

Card Spec v2.1.1.pdf - Adobe Acrobat Pro Extended

File Edit View Document Comments Forms Tools Advanced Window Help

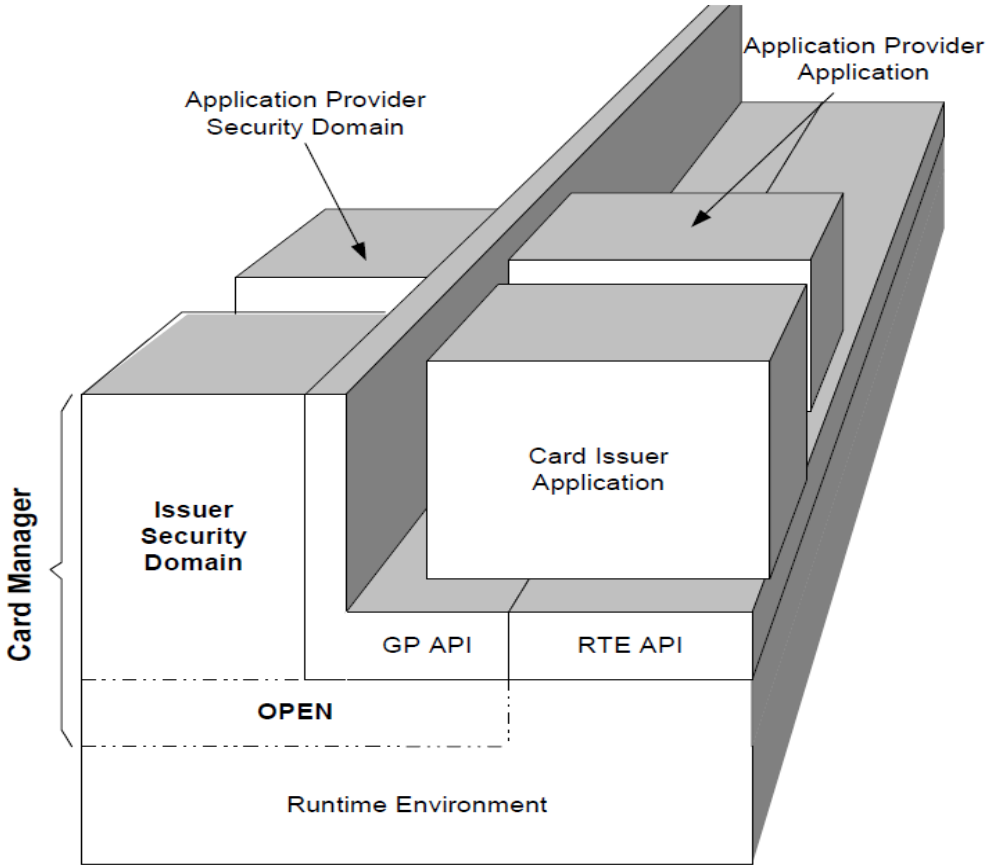


Figure 3-1: GlobalPlatform Card Architecture

All applications shall be implemented in a secure runtime environment that includes a hardware-neutral Application Programming Interface (API) to support application portability. GlobalPlatform does not mandate a

Пример представления услуги с помощью УЕК

Универсальная электронная карта обеспечивает юридическую значимость процесса дистанционного взаимодействия гражданина с организацией, предоставляющей услугу.

Система управления ключами и сертификатами

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

- Генерация 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 сегментов системы используются внешние УЦ:

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

EMV и предложения ООО УЕК по алгоритмам

EMV определяет основные аспекты жизненного цикла интеллектуальной карты и её окружения в платёжной системе

- Персонализация карты
- Криптографические алгоритмы и протоколы (симметричная –DES, ассиметричная –RSA)
- Интеграция с терминальным оборудованием

ООО УЕК определяет аналоги криптографических алгоритмов и протоколов на базе российских стандартов.

Ключевые системы

Симметричные ключи

Алгоритмы: 3DES, SHA1

ГОСТ 28147-89, 34.11 94

Идентификация карты на всех этапах жизненного цикла карты:

- изготовление
- персонализация
- инициализация идентификационного приложения
- идентификация карты при выполнении операций приложения

Ключевые системы
Асимметричные ключи

Алгоритмы: RSA, SHA1

ГОСТ 34.10 2001, 34.11 94

КриптоПро PKI

Поддержка технологической аутентификации карты с использованием улучшенной электронной подписи

Задачи ООО “КРИПТО-ПРО”

Разработка систем управления ключами:

КриптоПро HSM

российские стандарты, СКЗИ КриптоПро CSP + расширения УЕК

RSA, 3DES, SHA1 + расширения УЕК (EMV)

Уровень защиты КВ2

КриптоПро HSM клиент

PKCS#11, MS CryptoAPI v.1.0, 2.0

Управление и доступ к HSM

Опционально: PKCS#11, MS CryptoAPI v.1.0, 2.0

СКЗИ КриптоПро CSP+ расширения УЕК,

RSA, 3DES, SHA1+ расширения УЕК (EMV)

Уровни защиты КС1-КС3, КВ2.

Спасибо за внимание!

Попов Владимир Олегович

vpopov@cryptopro.ru