Некоторые вопросы безопасности связанные с использованием универсальных электронных карт

Матвеев Сергей Васильевич

Пензенский филиал
ФГУП «НТЦ «Атлас»
440026, г. Пенза, ул. Советская, д. 9.
Телефон: (8412)56-39-16, 56-33-97.
E-mail: atlas@sura.ru.
Сайт: www.atlas.sura.ru

Основные нормативные акты определяющие появление универсальной электронной карты гражданина

- Федеральный закон Российской Федерации от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".
- Распоряжение Правительства 1344-р "Об организации предоставления государственных и муниципальных услуг с использованием универсальной электронной карты"

Сроки реализации проекта УЭК

30 июля 2010 г.	Вступление в силу Федерального закона №210-ФЗ
12 августа 2010 г.	Распоряжение Правительства №1344-р
1 июля 2011 г.	Дата начала предоставления государственных и муниципальных услуг в электронном виде (согласно Федеральному закону №ФЗ-210,)
1 января 2012 г.	Начало выдачи универсальных электронных карт гражданам на основании заявлений
1 января 2014 г.	Начало выдачи универсальных электронных карт гражданам, не подавшим заявление на получение такой карты и не написавшим отказ от получения карты

Функционал универсальной электронной карты

УЭК должна обеспечивать

- идентификацию пользователя универсальной электронной картой в целях получения им при ее использовании доступа к государственным услугам и услугам иных организаций
- получение государственных услуг в системе обязательного медицинского страхования
- получение государственных услуг в системе обязательного пенсионного страхования
- получение банковских услуг

Содержимое УЭК
Визуальная составляющая

- Внешний вид

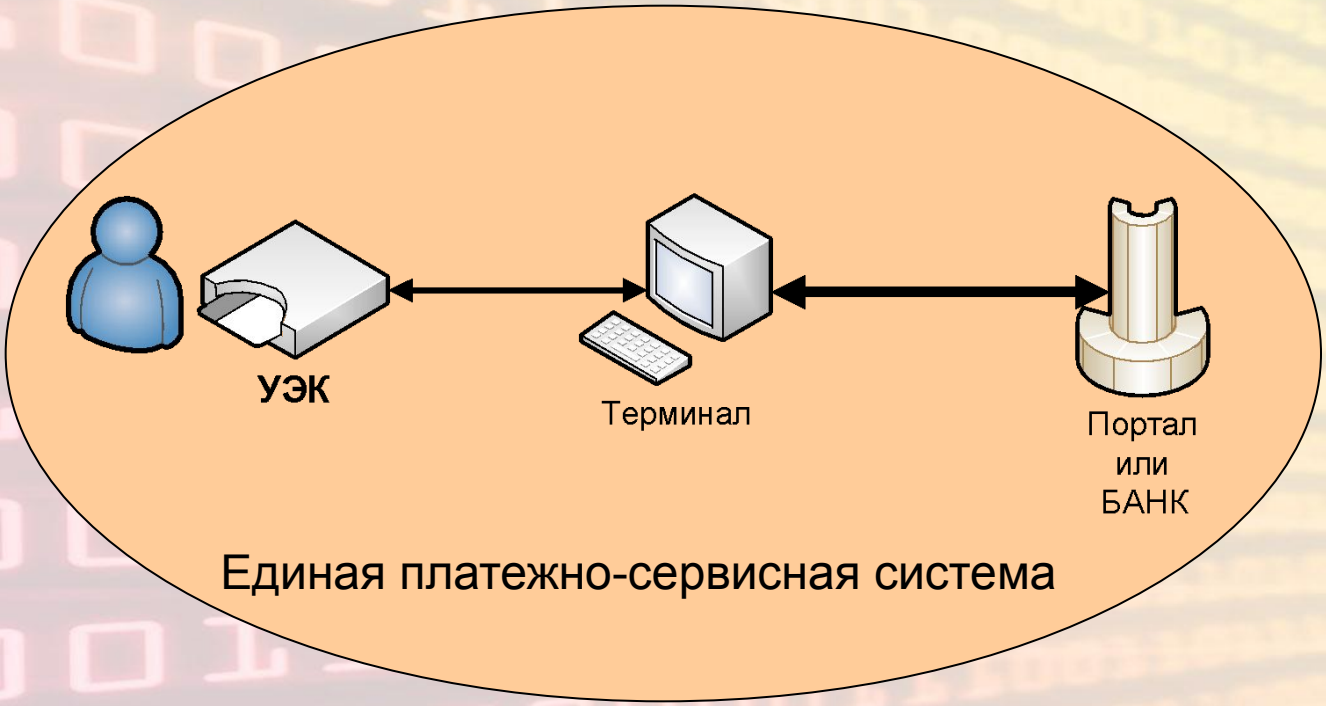
Визуальные данные

- фамилия, имя и (если имеется) отчество
- фотографию заявителя (в случае выдачи универсальной электронной карты по заявлению гражданина)
- номер универсальной электронной карты и срок ее действия;
- контактную информацию уполномоченной организации субъекта Российской Федерации;
- страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования Российской Федерации.

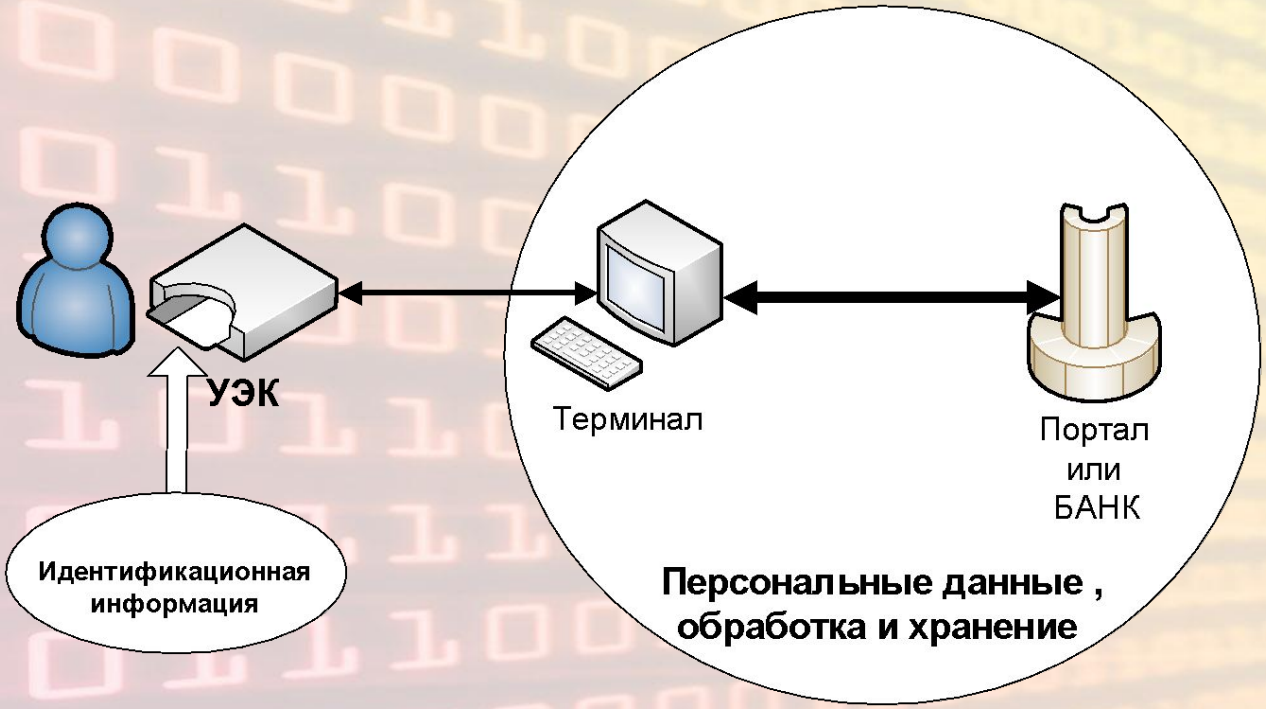
Содержимое УЭК
Электронная составляющая

- Данные
  - Визуальные данные в электронной форме
  - Дата и место рождения
  - Пол пользователя
- Приложения
  - Идентификационное
  - Платежное
  - Иные приложения

Упрощенная схема использования УЭК



Персональные данные при использовании УЭК



Режимы доступа к Единой платежно-сервисной системе с использованием УЭК

	чтение справочной информации	чтение информации пользователя	изменение данных пользователя
Без аутентификации и предъявления пароля	+	-	-
успешное предъявление пароля (ПИН-кода)	+	±	-
успешная аутентификация УЭК устройством доступа	+	+	±
успешная аутентификация УЭК устройством доступа и успешное предъявление ПИН	+	+	+

Функции безопасности решаемые средствами УЭК

Функции УЭК:

- Ограничение доступа к карте
- Аутентификация при доступе к государственным услугам
- Обеспечение безопасности платежей
- Разграничение доступа между приложениями карты

Функции безопасности решаемые средствами УЭК

Функции УЭК	*Чем обеспечиваетс*	*На чем основано*
Ограничение доступа к карте	Операционная система УЭК	Спецификация «GlobalPlatform. Card Specification»
Аутентификация при доступе к государственным услугам	Идентификационное приложение	ГОСТ 34.10-2001 ГОСТ 28147-89
Обеспечение безопасности платежей	Платежное приложение	Продукт ПРО100 на основе банковского приложения M\CHIP4 (MASTERCARD)
Разграничение доступа между приложениями карты	Операционная система УЭК	Спецификация «GlobalPlatform. Card Specification»

Аутентификация при использовании УЭК

Существуют следующие механизмы аутентификации:

- на основе паролей
- аутентификация с использованием симметричной криптосхемы
- аутентификация на основе ассиметричной криптосхемы

Государственные стандарты в сфере криптографической защиты информации необходимые для реализации функций безопасности УЭК

- Утвержденные
  - ГОСТ Р34.10-2001 (ЭЦП)
  - ГОСТ Р34.11-94 (Хеш-функция)
  - ГОСТ 28147-89 (шифрование)

- Разрабатываемые в рамках ТК26 «Криптографическая защита информации»
  - Формат хранения/чтения закрытых ключей в системах PKI
  - Применение схем с одноразовыми паролями

Спасибо за внимание!

Матвеев Сергей Васильевич

Пензенский филиал
ФГУП «НТЦ «Атлас»
440026, г. Пенза, ул. Советская, д. 9.
Телефон: (8412)56-39-16, 56-33-97.
E-mail: atlas@sura.ru.
Сайт: www.atlas.sura.ru