

ПРАВИЛА ФЕДЕРАЛЬНОЙ
УПОЛНОМОЧЕННОЙ
ОРГАНИЗАЦИИ
(ПРАВИЛА ЕПСС УЭК)

Приложение № Од-10

Общие технические
спецификации

Спецификация
универсальной
электронной карты

Редакция 1.5.2 от 7.10.2011

Правила Федеральной уполномоченной организации установлены в соответствии с Федеральным законом от 27 июля 2010 года «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ и принимаемыми в соответствии с указанным федеральным законом иными нормативными правовыми актами.

Далее в тексте настоящего документа термин «Правила ЕПСС УЭК» означает Правила Федеральной уполномоченной организации в их значении, установленном в части 6 статьи 28 Федерального закона от 27 июля 2010 года «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ.

ОГЛАВЛЕНИЕ

Введение	5
1. Определения и сокращения	5
2. Общие положения.....	6
2.1. Состав носителей информации.....	6
2.2. Интегральная схема карты	6
2.3. Лицевая и оборотная стороны карты	6
2.4. Магнитная полоса карты.....	7
3. Требования к физическим характеристикам карты	7
3.1. Общие требования.....	7
3.2. Требования для карт с интегральной схемой с контактами	8
3.3. Требования для карт с интегральной схемой с бесконтактным интерфейсом.....	8
3.4. Требования для карт с магнитной полосой	9
4. Требования к интегральной схеме карты	9
4.1. Требования к аппаратной части интегральной схемы.....	9
4.1.1. Объем ПЗУ	9
4.1.2. Объем ОЗУ.....	9
4.1.3. Объем ППЗУ.....	10
4.1.4. Эксплуатационные характеристики памяти.....	10
4.1.5. Аппаратная поддержка генерации случайных чисел.....	10
4.1.6. Аппаратная поддержка криптографических алгоритмов	11
4.1.7. Диспетчер памяти.....	11
4.2. Требования к контактному интерфейсу	11
4.2.1. Размеры и расположение контактов.....	11
4.2.2. Электронные сигналы и протоколы передачи.....	12
4.3. Требования к бесконтактному интерфейсу	13
4.3.1. Размеры и расположение зон связи.....	13
4.3.2. Протоколы, форматы данных и процедуры восстановления.....	13
4.4. Требования к операционной системе.....	14
4.4.1. Межотраслевые команды для обмена.....	14
4.4.2. Элементы данных для межотраслевого обмена	14
4.4.3. Поддержка спецификации GlobalPlatform.....	15

4.4.4. Поддержка зарубежных криптографических алгоритмов	15
4.4.5. Поддержка российских криптографических алгоритмов.....	16
4.4.6. Поддержка виртуальной машины JavaCard	17
4.4.7. Уровень обеспечения безопасности.....	17
4.5. Требования к поддержке приложений	17
5. Требования к магнитной полосе карты	18
5.1. Применение магнитной полосы.....	18
5.2. Запись информации	18
6. Требования к графическому оформлению карты	19
6.1. Состав информации на лицевой стороне карты	19
6.2. Состав информации на оборотной стороне карты	19
6.3. Выполнение графической печати сторон карты	20
6.4. Защитные элементы	21
6.5. Графический дизайн карты	22
7. Прочие требования	30
7.1. Память, необходимая для размещения приложений.....	30
7.2. Начальное состояние интегральной схемы	31
7.3. Состав доменов безопасности.....	31
7.4. Главный домен безопасности	31
7.5. Дополнительный домен безопасности	31
7.6. Установка приложений	32

Введение

Документ раскрывает технические требования к универсальной электронной карте, в т.ч.:

- требования к носителям информации карты;
- требования к физическим характеристикам карты;
- требования к интегральной схеме карты (требования к аппаратной платформе, требования к операционной системе и пр.);
- требования к магнитной полосе карты;
- требования к графическому оформлению карты;
- прочие требования.

1. Определения и сокращения

В настоящем документе используются следующие определения и сокращения.

Держатель (заявитель, держатель карты УЭК) – пользователь универсальной электронной картой.

УЭК (карта УЭК) – универсальная электронная карта.

Специализированное устройство чтения и записи – интерфейсное устройство, обеспечивающие взаимодействие терминала с универсальной электронной картой для чтения и записи информации.

2. Общие положения

В настоящем разделе раскрываются требования к носителям информации универсальной электронной карты.

2.1. Состав носителей информации

Карта (заготовка) должна обеспечивать возможность размещения информации:

- на лицевой и оборотной стороне карты;
- в интегральной схеме карты;
- на магнитной полосе карты.

2.2. Интегральная схема карты

Карта должна быть оборудована интегральной схемой, для взаимодействия с которой должны присутствовать контактный интерфейс и бесконтактный интерфейс (дуальная карта).

Информация в электронном виде заносится в интегральную схему и считывается с нее специализированными устройствами чтения и записи через контактный или бесконтактный интерфейс.

Требования к контактному и бесконтактному интерфейсам взаимодействия с интегральной схемой приведены в настоящем документе.

2.3. Лицевая и оборотная стороны карты

Текстовая и графическая информация размещается на лицевой и оборотной стороне карты для возможности визуального считывания и использования в процедурах оказания услуг.

Требования к форме и способам размещения информации на лицевой и оборотной сторонах карты определяется настоящим документом.

2.4. Магнитная полоса карты

Информация в электронном виде заносится на магнитную полосу и считывается с нее с использованием специализированных устройств чтения и записи, обеспечивающих считывание информации с магнитной полосы.

Наличие на карте магнитной полосы является обязательным¹.

Размещение магнитной полосы на карте, характеристики магнитной полосы и кодирование информации на магнитной полосе осуществляются в соответствии с требованиями настоящего документа.

3. Требования к физическим характеристикам карты

3.1. Общие требования

Цель: обеспечить физическую (геометрическую, механическую, оптическую и т.п.) совместимость со специализированными устройствами чтения и записи и достаточные эксплуатационные свойства карты (прочность, устойчивость к воздействию агрессивных сред, температуры и т.д.).

Форма и физические (геометрические, механические, оптические и др.) характеристики карты должны удовлетворять требованиям стандарта Российской

¹ Обязательность данного требования продиктована вопросами совместимости с банковской инфраструктурой. В большей части банкоматов для обслуживания карты с использованием электронного приложения, размещенного в интегральной схеме, требуется наличие на карте магнитной полосы, персонализированной данными банковского приложения.

Федерации ГОСТ Р ИСО/МЭК 7810–2006 «Карты идентификационные. Физические характеристики» с учетом следующих особенностей:

- типоразмер карты – ID-1 (CR-80);
- материал изготовления – поликарбонат (слои белого поликарбоната с полиграфическим изображением под слоем лазероактивного прозрачного поликарбоната для изображения в градациях серого цвета, наносимого методом лазерного гравирования).

3.2. Требования для карт с интегральной схемой с контактами

Дополнительно к установленным выше требованиям физические (геометрические, механические, оптические и др.) характеристики карт на интегральных схемах с контактами должны удовлетворять требованиям стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7816-1–2002 «Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1: Физические характеристики».

3.3. Требования для карт с интегральной схемой с бесконтактным интерфейсом

Дополнительно к установленным выше требованиям физические (геометрические, механические, оптические и др.) характеристики карт на интегральных схемах с контактами должны удовлетворять требованиям стандарта Российской Федерации ГОСТ Р ИСО/МЭК 14443-1–2004 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия. Часть 1: Физические характеристики».

Антенна бесконтактного интерфейса интегральной схемы должна иметь полный (Class1) или сокращенный размер².

² Карта должна успешно проходить испытания в соответствии со стандартом ИСО/МЭК 10373-6 "Карты идентификационные. Методы испытаний. Часть 6: Карты ближнего действия".

3.4. Требования для карт с магнитной полосой

Дополнительно к установленным выше требованиям физические (геометрические, механические, оптические и др.) характеристики карт на интегральных схемах с контактами должны удовлетворять требованиям стандартов Российской Федерации:

- ГОСТ Р ИСО/МЭК 7811-2–2002 «Карты идентификационные. Способ записи. Часть 2: Магнитная полоса малой коэрцитивной силы»;
- ГОСТ Р ИСО/МЭК 7811-6–2003 «Карты идентификационные. Способ записи. Часть 6: Магнитная полоса большой коэрцитивной силы».

4. Требования к интегральной схеме карты

4.1. Требования к аппаратной части интегральной схемы

4.1.1. Объем ПЗУ

Цель: эффективно задействовать постоянную память (ПЗУ, ROM) интегральной схемы карты для того, чтобы максимально высвободить энергонезависимую перезаписываемую память (ППЗУ) карты для размещения приложений.

Интегральная схема карты должна обладать постоянной памятью (ПЗУ) в размере, достаточном для размещения операционной системы и обязательных федеральных электронных приложений. При этом размер постоянной памяти (ПЗУ) для размещения обязательных федеральных электронных приложений должен быть не менее 92 кбайт.

4.1.2. Объем ОЗУ

Цель: обеспечить для разработчиков приложений для универсальной электронной карты гарантированный уровень ресурсов оперативной памяти (ОЗУ, RAM).

Интегральная схема карты должна обладать оперативной памятью (ОЗУ) в размере, достаточном для того, чтобы предоставить доступную для приложения оперативную память в объеме не менее 2048 байт.

4.1.3. Объем ППЗУ

Цель: обеспечить приемлемый уровень ресурсов энергонезависимой перезаписываемой памяти карты (ППЗУ, EEPROM) для размещения приложений и данных.

Интегральная схема карты должна обладать перезаписываемой памятью (ППЗУ) в размере не менее 72 кбайт.

4.1.4. Эксплуатационные характеристики памяти

Цель: обеспечить возможность эксплуатации карты в течение всего ее срока действия.

1. Постоянная память (ПЗУ) и энергонезависимая перезаписываемая память (ППЗУ) интегральной схемы должна обеспечивать хранение записанной в нее информации в течение не менее 5 лет.

2. Энергонезависимая перезаписываемая память (ППЗУ) [электрически стираемое перепрограммируемое ПЗУ (ЭСПЗУ, EEPROM)] интегральной схемы должна обеспечивать возможность выполнения не менее 100000 циклов стирания/записи.

4.1.5. Аппаратная поддержка генерации случайных чисел

Цель: обеспечить защищенность выработки ключевых последовательностей.

Интегральная схема должна иметь аппаратный генератор случайных чисел.

4.1.6. Аппаратная поддержка криптографических алгоритмов

Цель: обеспечить высокую производительность криптографических операций для обеспечения приемлемого времени реакции карты при оказании услуг.

Интегральная схема карты должна иметь аппаратную реализацию на уровне криптографического сопроцессора:

- вычислений для алгоритма RSA;
- вычислений на эллиптических кривых для алгоритма ГОСТ Р 34-10-2001;
- вычислений для алгоритма DES;
- вычислений для алгоритма ГОСТ 28147-89;
- вычислений для алгоритма ГОСТ Р 34.11-94.

4.1.7. Диспетчер памяти

Цель: обеспечить контроль и управление доступом центрального процессора ко всем видам памяти микросхемы, а также защиту хранящейся в памяти информации.

В интегральной схеме карты должен присутствовать аппаратный диспетчер памяти (MMU).

4.2. Требования к контактному интерфейсу

4.2.1. Размеры и расположение контактов

Цель: обеспечить геометрическую совместимость со специализированными устройствами чтения и записи карт на интегральных схемах с контактами.

Размеры и расположение контактов для карт на интегральных схемах с контактами должны удовлетворять требованиям следующих документов:

- стандарт Российской Федерации ГОСТ Р ИСО/МЭК 7816-2–2002 «Карты идентификационные. Карты на интегральных схемах с контактами. Часть 2: Размеры и расположение контактов»;
- спецификация EMVCo «EMV Integrated Circuit Card Specifications for Payment Systems. Book 1: Application Independent ICC to Terminal Interface. Version 4.2, June 2008».

4.2.2. Электронные сигналы и протоколы передачи

Цель: обеспечить совместимость со специализированными устройствами чтения и записи карт на интегральных схемах с контактами на уровне электрических характеристик сигналов и протокола обмена данными.

Электронные сигналы и протоколы передачи для карт на интегральных схемах с контактами должны удовлетворять требованиям следующих документов:

- стандарт Российской Федерации ГОСТ Р ИСО/МЭК 7816-3–2006 «Карты идентификационные. Карты на интегральных схемах с контактами. Часть 3: Электронные сигналы и протоколы передачи»;
- спецификация EMVCo «EMV Integrated Circuit Card Specifications for Payment Systems. Book 1: Application Independent ICC to Terminal Interface. Version 4.2, June 2008».

Указанные выше требования должны выполняться с учетом следующих особенностей:

- тип протокола передачи – T=0 и T=1;
- максимальная скорость передачи данных – не менее 38400 бит/с.

При этом конкретный тип протокола передачи данных (T=0 или T=1) должен быть выбран при заказе партии карт.

4.3. Требования к бесконтактному интерфейсу

4.3.1. Размеры и расположение зон связи

Цель: обеспечить совместимость со специализированными устройствами чтения и записи карт на интегральных схемах с бесконтактным интерфейсом на уровне геометрических и электромагнитных характеристик.

Размеры и расположение зон связи, а также способы модуляции и кодирования битов для карт на интегральных схемах с бесконтактным интерфейсом должны удовлетворять требованиям международного стандарта ISO/IEC 14443-2 "Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 2: Мощность высокочастотного сигнала и сигнальный интерфейс".

4.3.2. Протоколы, форматы данных и процедуры восстановления

Цель: обеспечить совместимость со специализированными устройствами чтения и записи карт на интегральных схемах с бесконтактным интерфейсом на уровне протоколов, форматов данных и процедур восстановления.

Протоколы, форматы данных и процедуры восстановления для карт на интегральных схемах с бесконтактным интерфейсом должны удовлетворять требованиям международных стандартов:

- ISO/IEC 14443-3 "Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 3: Инициализация и антиконфликтность";
- ISO/IEC 14443-4 "Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 4: Протокол передачи".

Бесконтактный интерфейс интегральной схемы карты должен поддерживать протокол передачи – T=CL тип А и тип В. При этом конкретный тип протокола передачи данных (тип А или тип В) должен быть выбран при заказе партии карт.

Для обеспечения защиты от несанкционированного отслеживания экземпляра универсальной электронной карты с использованием радиочастотного интерфейса, при проведении процедуры антиколлизии в соответствии с ISO/IEC 14443-3 в качестве уникального номера карты (UID) рекомендуется использовать случайное число.

4.4. Требования к операционной системе

4.4.1. Межотраслевые команды для обмена

Цель: обеспечить совместимость карт на интегральных схемах с устройствами чтения карт на прикладном уровне.

Операционная система должна поддерживать общие (межотраслевые) команды для обмена с картой на интегральных схемах в соответствии с требованиями стандарта Российской Федерации «Карты идентификационные. Карты на интегральных схемах с контактами. Часть 4: Межотраслевые команды для обмена» ГОСТ Р ИСО/МЭК 7816-4–2004.

4.4.2. Элементы данных для межотраслевого обмена

Цель: обеспечить совместимость карт на интегральных схемах со специализированными устройствами чтения и записи на прикладном уровне.

Операционная система должна поддерживать элементы данных для общего (межотраслевого) обмена с картой на интегральных схемах в соответствии с требованиями национального стандарта Российской Федерации «Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6: Элементы данных для межотраслевого обмена» ГОСТ Р ИСО/МЭК 7816-6–2003.

4.4.3. Поддержка спецификации GlobalPlatform

Цель: обеспечить возможность управления контентом карты.

- Операционная система интегральной схемы карты должна соответствовать спецификации GlobalPlatform, определенной в документе «GlobalPlatform. Card Specification. Version» версии не ниже 2.2.
- Операционная система в соответствии с GlobalPlatform должна обеспечивать загрузку приложений в энергонезависимую память (EEPROM) интегральной схемы.
- Поддержка дополнительных доменов безопасности (SSD) для использования поставщиками приложений.
- Наличие механизма управления приложениями (Delegated Management, Delegated Management с DAP-верификацией).
- Для DAP-верификации должны поддерживаться следующие криптографические алгоритмы:
 - 3DES;
 - RSA;
 - ГОСТ 28147-89;
 - ГОСТ Р 34.10-2001.

Операционная система должна поддерживать следующие протоколы защищенного соединения с доменами безопасности:

- SCP02 (i='35');
- SCP10.

4.4.4. Поддержка зарубежных криптографических алгоритмов

Цель: обеспечить совместимость с криптографическими схемами, которые используются для оказания банковских услуг, за счет применения

криптографических алгоритмов, реализованных в карте УЭК и предназначенных для успешной работы банковского приложения.

Операционная система интегральной схемы карты должна иметь поддержку для реализации зарубежных криптографических алгоритмов:

- 3DES – время шифрования блока данных длиной 128 байт на ключе длиной 112 бит в режиме CBC-поряд - не более 20 мс;
- RSA (поддерживаемая длина модуля ключей: для проверки электронной подписи – не менее 1984 бит, для вычисления электронной подписи – не менее 1024 бита) – время формирования электронной подписи (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит – не более 250 мс; время проверки электронной подписи (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит - не более 100 мс;
- SHA1 – время формирования проверочного значения (свертки) сообщения (при длине 18 байт) – не более 30 мс.

4.4.5. Поддержка российских криптографических алгоритмов

Цель: обеспечить легитимность схем безопасности при оказании государственных и муниципальных услуг за счет применения российских криптографических алгоритмов.

Операционная система интегральной схемы карты должна иметь поддержку для реализации российских криптографических алгоритмов:

- ГОСТ Р 34.10-2001 – время вычисления электронной подписи не более 250 мс, время проверки электронной подписи не более 500 мс;
- ГОСТ 28147-89 – время преобразования не более 2 мс;
- ГОСТ Р 34.11-94 – время формирования проверочного значения (свертки) сообщения (при длине 32 байта) – не более 30 мс.

4.4.6. Поддержка виртуальной машины JavaCard

Цель: обеспечить возможность подключения приложений, функционирующих на разных интегральных схемах.

Операционная система интегральной схемы карты должна обеспечивать поддержку виртуальной машины JavaCard в соответствии со спецификацией JavaOS версии не ниже 2.2.1.

4.4.7. Уровень обеспечения безопасности

Цель: обеспечить приемлемый уровень безопасности размещения на карте информации и использования карты для оказания государственных и муниципальных услуг.

Карты на интегральных схемах (включая интерфейсы взаимодействия) должны обеспечивать в соответствии с документом "ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности" оценочный уровень доверия не ниже ОУД4.

4.5. Требования к поддержке приложений

Интегральная схема карты должна обеспечивать возможность размещения и использования обязательных федеральных электронных приложений.

Размещение иных электронных приложений осуществляется в пределах объема перезаписываемой постоянной памяти (ППЗУ, EEPROM), оставшегося после размещения обязательных федеральных приложений.

5. Требования к магнитной полосе карты

5.1. Применение магнитной полосы

Цель: 1) обеспечить возможность применения карты УЭК терминалах, чьи специализированные устройства чтения и записи настроены на обязательное присутствие магнитной полосы, которая содержит данные банковского приложения, 2) обеспечить возможность использования карты в случае, когда на оборотной стороне карты присутствует дополнительный логотип платежной системы.

Универсальная электронная карта должна содержать магнитную полосу на оборотной стороне карты, как это определено в физических требованиях к карте с магнитной полосой.

5.2. Запись информации

Цель: обеспечить совместимость со специализированными устройствами чтения и записи карт с магнитной полосой на уровне характеристик электромагнитных полей и способов кодирования данных.

Физические характеристики магнитной полосы, рабочие характеристики магнитного материала, кодирование и расположение дорожек для карты с магнитной полосой должны удовлетворять требованиям стандартов Российской Федерации:

- «Карты идентификационные. Способ записи. Часть 2: Магнитная полоса малой коэрцитивной силы» ГОСТ Р ИСО/МЭК 7811-2–2002;
- «Карты идентификационные. Способ записи. Часть 6: Магнитная полоса большой коэрцитивной силы» ГОСТ Р ИСО/МЭК 7811-6–2003.

На магнитную полосу должна записываться информация банковского приложения.

6. Требования к графическому оформлению карты

6.1. Состав информации на лицевой стороне карты

Универсальная электронная карта на своей лицевой стороне должна содержать следующие визуальные (незащищенные) сведения:

- логотип универсальной электронной карты;
- логотип платежной системы;
- логотип банка - эмитента банковского приложения;
- номер универсальной электронной карты³;
- трехзначный код проверки подлинности карты⁴.

6.2. Состав информации на оборотной стороне карты

На оборотной стороне универсальной электронной карты должны содержаться следующие визуальные (незащищенные) сведения (изображение в градациях серого цвета, наносимое способом лазерного гравирования):

- сведения о пользователе универсальной электронной карты:
 - фамилия;
 - имя;
 - отчество (если имеется);
 - пол;
 - дата рождения;

³ Номер универсальной электронной карты – изображение в градациях серого цвета, наносимое способом лазерной гравировки.

⁴ Код проверки подлинности карты (CVV2/CVC2), если он назначен для банковского приложения – изображение в градациях серого цвета, наносимое способом лазерной гравировки.

- страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования Российской Федерации;
- номер полиса обязательного медицинского страхования;
- фотография заявителя (в случае выдачи универсальной электронной карты по заявлению гражданина в порядке, установленном статьей 25 Федерального закона от 27 июля 2010 года «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ);
- образец подписи;
- срок действия универсальной электронной карты;
- номер банковской карты;
- номер производителя.

Также на оборотной стороне универсальной электронной карты должны содержаться следующие визуальные сведения:

- дополнительный логотип платежной системы (при его наличии);
- контактная информация уполномоченной организации субъекта Российской Федерации.

6.3. Выполнение графической печати сторон карты

Для изготовления изображения лицевой стороны карты должна использоваться офсетная печать с применением 5 красок:

- СМΥК, или 4 смесевые краски (Pantone);
- 1 краска – люминесцирующий под воздействием УФ излучения элемент), трафаретная печать (цветопеременный защитный элемент).

Для изготовления изображения оборотной стороны карты должна использоваться офсетная печать с применением до 4 красок:

- до 3 смесевых красок (Pantone), одна из которых должна быть с полутоновым эффектом;
- черный текст.

6.4. Защитные элементы

Универсальная электронная карта относится к защищенной полиграфической продукции и должна содержать ряд средств защиты от изменений (искажений) визуальной (графической) информации зафиксированной на лицевой и оборотной стороне:

- позитивные и негативные гильоширные элементы в офсетной печати;
- защитные полутоновые элементы, выполненные без растривания в офсетной печати на обороте (специальные технологии);
- микротекст (негативный высотой 230-250 мкм, позитивный высотой 150-200 мкм);
- элемент, выполненный оптически переменной краской (площадью ≤ 0.5 см²);
- элемент в верхнем левом углу, площадью ≤ 6.0 см², люминесцирующий под воздействием ультрафиолетового излучения;
- элемент в верхнем левом углу, выполненный краской со специальными свойствами для приборного контроля площадью ≤ 6.0 см²;
- буквенно-цифровая информация черного цвета, напечатанная прозрачной для инфракрасного излучения краской (оборот);
- плёночное покрытие с дифракционными голографическими элементами, обеспечивающее защиту поверхности карты от механических и физико-химических воздействий.

6.5. Графический дизайн карты

Графический дизайн лицевой и оборотной стороны универсальной электронной карты без указания областей элементов данных представлен на рисунке “Исходный макет”.

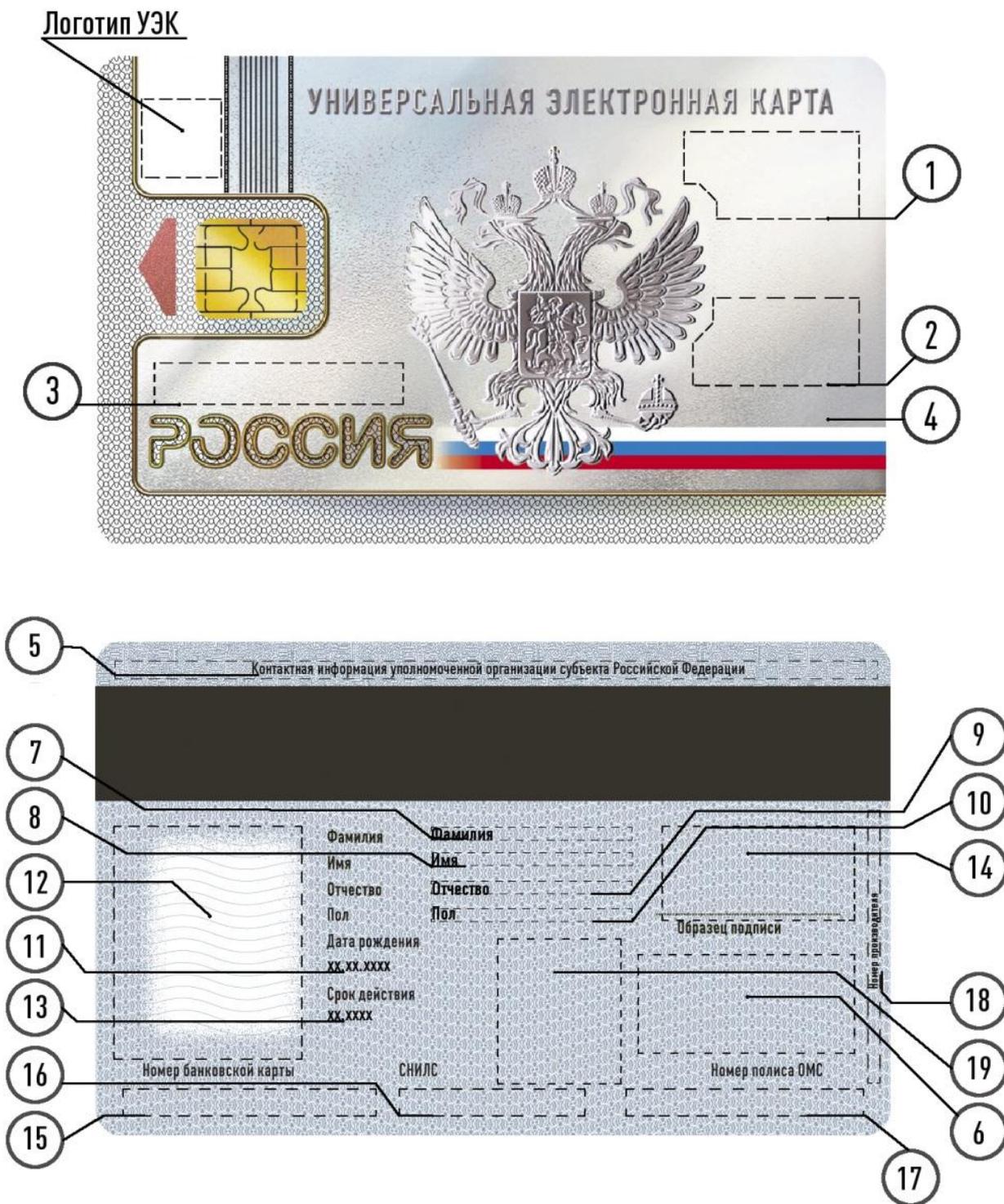
Графический дизайн лицевой и оборотной стороны универсальной электронной карты с указанием областей элементов данных представлен на рисунке “Макет графического оформления”.

Федеральная уполномоченная организация для изготовления заготовок универсальной электронной карты и их персонализации по запросу предоставляет центрам изготовления и центрам персонализации:

- графический дизайн лицевой и оборотной стороны карты в варианте, подходящем для изготовления заготовок универсальной электронной карты;
- шрифт для нанесения необходимых надписей на лицевую и оборотную стороны универсальной электронной карты.

Отступления от графического дизайна в части цвета, фона и шрифта не допускаются.

Исходный макет



Макет графического оформления



Обозначение	Наименование элемента данных	Положение и размеры поля размещения элемента данных ⁵	Примечания
1	Логотип банка – эмитента банковского приложения	<p><u>Положение:</u></p> <p>сторона карты – лицевая.</p> <p>отступ от правого края – не менее 3 мм</p> <p>отступ от верхнего края – не менее 7 мм</p> <p><u>Размеры:</u></p> <p>ширина – не более 20 мм.</p> <p>высота – не более 10 мм.</p>	<p>Детали изображения логотипа должны быть расположены на расстоянии не менее 1 мм от изображения герба</p>
2	Логотип платежной системы	<p><u>Положение:</u></p> <p>сторона карты – лицевая.</p> <p>отступ от правого края – не менее 3 мм</p> <p>отступ от верхнего края – не менее 26 мм.</p> <p>отступ от нижнего края – не менее 17 мм</p> <p><u>Размеры:</u></p> <p>ширина – не более 18 мм.</p>	<p>Детали изображения логотипа не должны быть ближе к изображению герба ближе, чем на 1 мм.</p>
3	Номер универсальной электронной карты	<p><u>Положение:</u></p> <p>сторона карты – лицевая</p> <p>отступ от левого края – 6 мм</p> <p>отступ от нижнего края – 15 мм</p> <p>выравнивание текста: по левой и по нижней границе</p>	<p>Шрифт DIN Condensed Normal.</p> <p>Первые 3 цифры и последняя цифра – 12 кегль, девять цифр номера 19 кегль.</p>

⁵ Допускается отклонение от указанных размеров не более чем на 0,5 мм.

4	Трехзначный код проверки подлинности карты	<u>Положение:</u> сторона карты – лицевая отступ от правого края – 3 мм отступ от нижнего края – 13 мм выравнивание текста: по правой и по нижней границе	Шрифт DIN Condensed Normal, 9 кегль.
5	Контактная информация уполномоченной организации субъекта Российской Федерации	<u>Положение:</u> сторона карты – обратная отступ от верхней границы магнитной полосы – 1 мм выравнивание текста: по центру карты и по нижней границе	Шрифт DIN Condensed Normal, 6 кегль
6	Дополнительный логотип платежной системы (при его наличии)	<u>Положение:</u> сторона карты – обратная отступ от правого края – не менее 4 мм отступ от нижнего края – не менее 8 мм отступ от верхнего края – не менее 34 мм <u>Размеры:</u> ширина – не более 23 мм.	Детали изображения логотипа не должны быть ближе к другим элементам ближе, чем на 1 мм.
7	Фамилия	<u>Положение:</u> сторона карты – обратная отступ от левой границы карты – 36 мм отступ от верхней границы карты – 20 мм выравнивание текста: по левой границе и по верхней границе	Шрифт DIN Condensed Normal, 8 кегль.
8	Имя	<u>Положение:</u>	Шрифт DIN Condensed Normal,

		сторона карты – оборотная отступ от левой границы карты – 36 мм отступ от верхней границы карты – 23 мм выравнивание текста: по левой границе и по верхней границе	8 кегль.
9	Отчество (если имеется)	<u>Положение:</u> сторона карты – оборотная отступ от левой границы карты – 36 мм отступ от верхней границы карты – 26 мм выравнивание текста: по левой границе и по верхней границе	Если есть, шрифт DIN Condensed Normal, 8 кегль.
10	Пол	<u>Положение:</u> сторона карты – оборотная отступ от левой границы карты – 36 мм отступ от верхней границы карты – 29 мм выравнивание текста: по левой границе и по верхней границе	Шрифт DIN Condensed Normal, 8 кегль.
11	Дата рождения	<u>Положение:</u> сторона карты – оборотная отступ от левой границы карты – 25 мм отступ от верхней границы карты – 36 мм выравнивание текста: по левой границе и по верхней границе	Шрифт DIN Condensed Normal, 8 кегль.
12	Фотография заявителя	<u>Положение:</u> сторона карты – оборотная отступ от левого края – 2 мм отступ от верхнего края – 20 мм	

		<p><u>Размеры:</u></p> <p>ширина – 20 мм.</p> <p>высота – 25 мм.</p>	
13	Срок действия универсальной электронной карты	<p><u>Положение:</u></p> <p>сторона карты – оборотная</p> <p>отступ от левой границы карты – 25 мм</p> <p>отступ от верхней границы карты – 41 мм</p> <p>выравнивание текста: по левой границе и по верхней границе</p>	Шрифт DIN Condensed Normal, 8 кегль.
14	Образец подписи	<p><u>Положение:</u></p> <p>сторона карты – оборотная</p> <p>отступ от правого края – не менее 4 мм</p> <p>отступ от верхнего края – не менее 19 мм</p> <p><u>Размеры:</u></p> <p>ширина – не более 20 мм.</p> <p>высота – не более 10 мм.</p>	
15	Номер банковской карты	<p><u>Положение:</u></p> <p>сторона карты – оборотная</p> <p>отступ от левой границы карты – 3 мм</p> <p>отступ от нижней границы карты – 2 мм</p> <p>выравнивание текста: по левой границе и по нижней границе</p>	Шрифт DIN Condensed Normal, 10,5 кегль.
16	Страховой номер индивидуального лицевого счета (СНИЛС) застрахованного	<p><u>Положение:</u></p> <p>сторона карты – оборотная</p> <p>отступ от левой границы карты – 30 мм</p> <p>отступ от нижней границы карты – 2 мм</p>	Шрифт DIN Condensed Normal, 10,5 кегль.

	лица в системе обязательного пенсионного страхования Российской Федерации	выравнивание текста: по левой границе и по нижней границе	
17	Номер полиса обязательного медицинского страхования	<u>Положение:</u> сторона карты – оборотная отступ от правой границы карты – 3 мм отступ от нижней границы карты – 2 мм выравнивание текста: по правой границе и по нижней границе	Шрифт DIN Condensed Normal, 10,5 кегль.
18	Номер производителя	<u>Положение:</u> сторона карты – оборотная отступ от правой границы карты – 2 мм отступ от нижней границе карты – 1мм ориентация текста – вертикальная, снизу вверх выравнивание текста: по нижней границе и по центру области от нижней границы карты до нижней границы магнитной полосы	Шрифт DIN Condensed Normal, 4 кегль.
19	Дублирующий портрет (опционально)	<u>Положение:</u> сторона карты – оборотная отступ – не менее 2 мм от любого элемента <u>Размеры:</u> ширина – не более 13 мм. высота – не более 17 мм.	Защитный элемент – плёночное покрытие с дифракционными голографическими элементами, обеспечивающее защиту

			поверхности карты от механических и физико- химических воздействий
--	--	--	---

7. Прочие требования

7.1. Память, необходимая для размещения приложений

Интегральная схема, которая будет использоваться для изготовления заготовок универсальных электронных карт, должна выбираться центром изготовления исходя из оценки объема памяти (ППЗУ и ПЗУ, совокупно), необходимого для размещения соответствующих приложений. Рекомендуемые оценочные значения расхода памяти составляют:

- системные данные (данные доменов безопасности и др.) – 5 Кбайт;
- идентификационное приложение (обязательное): загружаемый модуль – 25 Кбайт, обязательные данные – 10 Кбайт, данные дополнительных секторов данных – предварительно 10 Кбайт;
- банковское приложение (обязательное), данные банковского приложения:
 - если на оборотной стороне карты отсутствует дополнительный логотип платежной системы – 8 Кбайт;
 - если на оборотной стороне карты присутствует дополнительный логотип платежной системы – 14 Кбайт;
- иные приложения: в зависимости от спецификации и конкретной реализации соответствующего приложения.

7.2. Начальное состояние интегральной схемы

Интегральная схема, используемая при изготовлении заготовки карты УЭК, должна находиться в состоянии, допускающем создание доменов безопасности, соответствующих спецификации GlobalPlatform.

7.3. Состав доменов безопасности

При изготовлении заготовки универсальной электронной карты должны быть созданы и инициализированы домены безопасности:

- главный домен безопасности (Issuer Security Domain);
- дополнительный домен безопасности (Supplementary Security Domain) – только в случае, если персонализация заготовки карты будет выполняться отдельно от изготовления этой заготовки.

7.4. Главный домен безопасности

Главный домен безопасности должен иметь идентификатор (AID, Application Identifier), равный 'A000000432554543495344'.

При инициализации главного домена безопасности в него должны быть занесены следующие данные:

- учетный номер карты УЭК (Card Image Number);
- ключи⁶ домена безопасности.

7.5. Дополнительный домен безопасности

После своего создания дополнительный домен безопасности должен иметь идентификатор (AID, Application Identifier), равный 'A00000043255454353534431'.

⁶ Главный шифровальный ключ.

При инициализации дополнительного домена безопасности в него должны быть занесены следующие данные:

- ключи⁷ домена безопасности.

Владельцем дополнительного домена безопасности является центр персонализации карт.

Данные инициализации дополнительного домена безопасности содержатся в задании на изготовление заготовки карты УЭК, подготовленном ФУО по запросу Центра изготовления заготовок универсальных электронных карт.

7.6. Установка приложений

После инициализации доменов безопасности должны быть инициализированы обязательные приложения карты.

Если приложение карты записано в постоянную память карты (ПЗУ), должна быть выполнена его установка посредством соответствующего домена безопасности.

Если приложение отсутствует в постоянной памяти карты, посредством соответствующего домена безопасности должны быть выполнены:

- загрузка загружаемого модуля приложения в энергонезависимую перезаписываемую память карты (ППЗУ);
- установка приложения.

Установка приложений посредством дополнительного домена безопасности должна осуществляться с применением механизма делегирования полномочий по управлению контентом карты (Delegated Management), определенного спецификацией GlobalPlatform.

⁷ Дополнительный шифровальный ключ.