ЭЛЕКТРОННЫЙ ПАСПОРТ

ОСНОВНЫЕ КОНСТАНТЫ

А.Андреев

28 августа 2006 года наступил предварительный срок введения электронных паспортов в ЕС. Выдавать биометрические загранпаспорта начали и в некоторых регионах России. Но время, когда каждый гражданин РФ станет владельцем нового паспорта, соответствующего всем требованиям ICAO*, наступит еще не скоро. Однако уже сейчас вопросы внедрения системы электронных паспортов весьма злободневны. Как электронные паспорта будут работать за рубежом? А как у нас? Кто основные участники процесса внедрения новых паспортов? Какие эффективные технические решения уже приняты и будут работать в окончательном варианте системы электронных паспортов?

С ЧЕГО ВСЕ НАЧАЛОСЬ

Идея усовершенствования дорожных документов появилась еще в начале 90-х годов прошлого века. Но именно в начале 21 века она стала особенно популярной. Тому есть несколько причин: стремительное развитие информационных технологий, увеличение потока туристов, возросшая опасность террористических актов. Едва ли не основная причина повышенного интереса к паспортам нового поколения – борьба США с терроризмом и обновление требований ее программы безвизового въезда (Visa Waiver Program, VWP).

ТРЕБОВАНИЯ ICAO

Согласно "Дополнению к документу 9303: электронные паспорта" ICAO, электронный паспорт должен содержать встроенную микросхему бесконтактной карты (совестимую со стандартом ISO 14443). В карте хранится биометрическая информация пользователя в виде изображения лица в формате jpg или jpg2000. Данные дактилоскопических отпечатков пальцев или радужной оболочки глаза не обязательны. Кроме того, в бесконтактную карту необходимо ввести информацию о пользователе, записанную в машинно-считываемой зоне (MRZ – Machine Readable Zone). Все данные должны быть защищены электронной подписью (ЭЦП). Значение хэш-функции ЭЦП также содержится в памяти микросхемы. Необходимость передавать и хранить большой объем информации обусловило выбор ICAO в пользу микросхем бесконтактных карт. Для того чтобы данные правильно интерпретировались в машинно-считываемых дорожных документах (Machine Readable Travel Documents, MRTD), предложена логическая структура данных (Logic Data Structure, LDS), а для их защиты выбрали инфраструктуру с открытым ключом (Public Key Infrastructure, PKI).

ТРЕБОВАНИЯ К СТРАНАМ-УЧАСТНИЦАМ БЕЗВИЗОВОЙ ПРОГРАММЫ США

Безвизовая программа США, VWP, позволяет гражданам стран-участниц (всего 27 государств) въезжать на территорию США с туристическими или коммерческими целями сроком до 90 дней без получения визы. Чтобы воспользоваться преимуществами этой программы, въезжающим в страну необходимо иметь паспорта, которые могут считываться компьютером (начиная с даты выдачи 26.10.2005) и содержат цифровую фотографию владельца. Паспорта, выдаваемые с 26.10.2006, должны хранить биометрическую информацию.

Кроме участников VWP-программы, еще 40 стран планировали к концу 2006 года внедрить электронные паспорта. Если эта тенденции сохранится, то ежегодно только европейские страны-участницы программы будут производить около 25

* Международная организация гражданской авиации (International Civil Aviation Organization, ICAO). Ведущая организация по стандартизации процедур пересечения границ и норм авиаперелетов.

млн. паспортов нового поколения. Все они будут снабжены картами радиочастотной идентификации (Radio Frequency Identification, RFID).

БЕСКОНТАКТНЫЕ ПАСПОРТА: МОЖНО ЛИ ИМ ДОВЕРЯТЬ?

В чем достоинство бесконтактных карт? В первую очередь передача информации требует меньше времени по сравнению с контактными устройствами. Когда карта находится в пределах зоны действия считывающего устройства, связь не зависит от расположения паспорта относительно этого устройства. Это также позволяет ускорить процесс верификации личности. Было решено использовать в электронных паспортах пассивные RFID-метки малого радиуса считывания. Подобные радиометки соответствуют стандарту ISO 14443 "Identification cards, – Contactless integrated circuit(s) cards – Poximity cards" и успешно применяются в сфере банковских услуг и контроля доступа. Они состоят из индуктивной рамочной антенны и микросхемы и не имеют собственного источника питания (рис.1). Такие метки могут крепиться на подложке для получения радиочастотной этикетки (RFID label) или же их встраивают в пластиковую карточку.

Рис.1. Схема бесконтактной карты

В бесконтактных картах стандарта ISO 14443 используются ВЧ-транспондеры на частоту 13,65 МГц с дальностью действия 10–20 см. Устройство чтения состоит из антенны, передатчика и декодера. Оно не только излучает сигнал на несущей частоте, но и принимает отраженный сигнал карты, периодически сканируя пространство на предмет его обнаружения. При попадании метки в магнитное поле, которое создает сигнал считывающего устройства, в антенне метки индуцируется переменный ток (рис.2). Микросхема бесконтактной карты содержит выпрямитель и стабилизатор, преобразующие индуцированный ток в постоянный ток питания. Устройство чтения излучает АМ-сигнал. После приема микросхемой метки сигнал поступает на вход демодулятора и в блок выделения несущей. С выхода блока исходит тактовый сигнал с частотой 13,56 МГц. После декодирования и обработки данных метка связывается с устройством чтения посредством модуляции нагрузки (load modulation) антенны с поднесущей частотой сигнала 847,5 кГц. Устройство чтения выделяет поднесущую частоту сигнала метки и декодирует информацию.

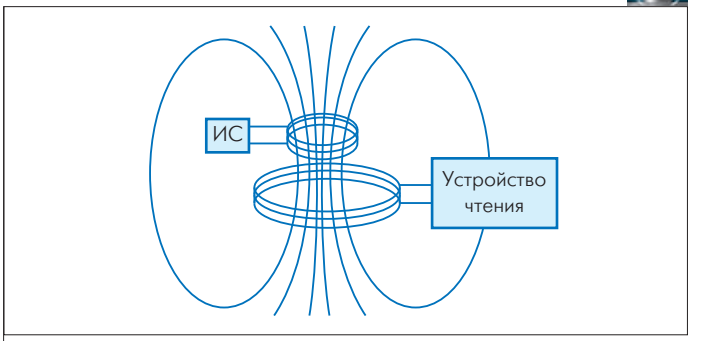

Рис.2. Индуктивная связь бесконтактной карты и устройства чтения

Каковы дополнительные преимущества бесконтактных карт на частоту 13,56 МГц? Дальность взаимодействия мала, поэтому невозможно считывать информацию дистанционно. Применение бесконтактных карт в странах, где одновременно вводятся электронные визы и паспорта, не вызовет дополнительных трудностей, поскольку в рамках стандарта ISO 14443 определен антиколлизионный протокол передачи данных.

Срок сохранения данных в микросхемах бесконтактных карт превышает 10 лет, а за их неприкосновенность отвечает целый набор средств безопасности. ICAO рекомендует использовать инфраструктуру открытых ключей – современную систему криптографической защиты, применяемую повсеместно для сохранения конфиденциальности и целостности информации. В криптосистеме PKI открытым ключом пользователя можно шифровать одновременно документ и значение его хэш-функции. Любые изменения документа приведут к изменению значения его хэш-функции. Расшифровав с по-

Таблица 1. Длина цифровой подписи в паспортах нового поколения

Алгоритм цифровой подписи	Размер подписи, бит	
	сертификационного центра страны	производителя паспорта
Алгоритм ассиметричного шифрования, RSA	3072	2048
Эллиптический алгоритм DSA (Elliptic Curve Digital Signature Algorithm)	256	224

мощью открытого ключа пользователя документ и значение хэш, а затем сравнив хэш с рассчитанным значением документа, можно убедиться в неприкосновенности переданной информации. Система PKI состоит из ПО серверов центра сертификации, ПО конечных пользователей и собственно аппаратного обеспечения, например бесконтактных карт. Центр сертификации заверяет аутентичность открытого ключа пользователя своей электронной цифровой подписью (ЭЦП). Пользователь ставит цифровую подпись, используя свой секретный ключ. Подлинность подписи подтверждает сертификат его открытого ключа, выданный сертификационным центром. Используемые алгоритмы цифровой подписи приведены в табл.1.

Устройство чтения проверяет ЭЦП производителя электронного паспорта и государства. Эту процедуру называют методом *пассивной авторизации.*

Инфраструктура с открытым ключом и ее поддержка RSA-микропроцессорами обеспечивают сохранность и неизменность данных, записанных в микросхему бесконтактной карты. Правда, это не гарантирует защиту от несанкционированного чтения и копирования информации. Чтобы предотвратить нелегальный доступ к персональным данным паспорта любого бесконтактного устройства чтения, в США обсуждают возможное применение так называемой *клетки Фарадея* (Faraday shield). Такая "клетка" – аналог идеального полого проводника. Ее формируют с помощью проводящих материалов или их сплавов. "Клетка", в которую, как в чехол, помещается паспорт, блокирует любое внешнее поле. Индуцированные внешним полем заряды перераспределяются по поверхности оболочки, блокируя его влияние. "Клетка Фарадея" используется как эффективное экранирующее покрытие кредитных карт и RFID-паспортов. Подобное защитное покрытие уже имеют электронные обложки паспортов США. В продаже также появились защитные чехлы (рис.3).

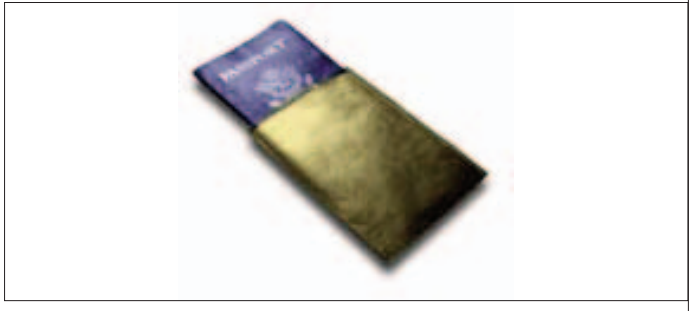

Рис.3. Защитный чехол для RFID-паспорта

Чтобы сохранить конфиденциальность информации паспортов, в странах ЕС и в США утвердили так называемый *базовый контроль доступа* (Basic Access Control, BAC) в качестве обязательной меры безопасности (согласно рекомендации ICAO – желательной). BAC использует разновидность PIN-кода. Обмен информацией между бесконтактной картой и считывающим устройством инициирует ключ, записанный в машинно-считываемой зоне паспорта (рис.4). Для этого электронный паспорт должен быть физически открыт и видим устройству оптического распознавания знаков. Таким образом, дистанционно получить доступ к информации микросхемы бесконтактной карты невозможно. Тестирование доказало работоспособность BAC. Однако время обмена данными между электронным паспортом и устройством чтения при этом возрастает вдвое.

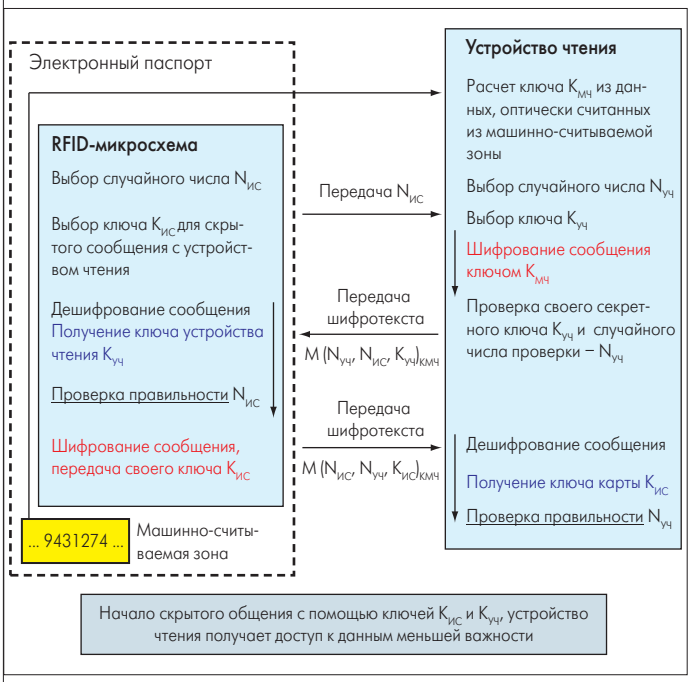

Рис.4. Схема работы системы базового контроля доступа (BAC)

Для предотвращения дупликации электронных паспортов некоторые страны внедряют дополнительную методику *активной авторизации*. С ее помощью можно проверить подлинность предъявляемого электронного паспорта, предотвратить замену его микросхемы, копирование данных. Такая методика – своеобразная альтернатива системе BAC. При активной авторизации считывающий терминал в качестве запроса формирует случайное число, микросхема подписывает запрос собственной ЭЦП, подтверждая свою подлинность. Однако инфраструктура распределения открытых ключей в подобной системе достаточно сложна. Каждый паспорт получает два ключа: открытый и собственный секретный пользователя. При этом открытый ключ хранится в цифровом документе, а секретный – в защищенной памяти микросхемы карты.

В перспективе для защиты дополнительной биометрической информации потребуется *расширенный контроль досту-*

Таблица 2. Сравнение электронных паспортов различных государств

Страна	Способ внедрения RFID-метки	Срок действия (для совершеннолетних/ несовершеннолетних)	Производитель микросхемы, емкость памяти	Цена, (для совершеннолетних/ несовершеннолетних)
США	В заднюю обложку	10	NXP* 64 Кбайт Infenion 64 Кбайт	120 долл.
Великобритания	В заднюю обложку	10/5	NXP 72 Кбайт	142/92 фунтов стерлингов
Бельгия	В заднюю обложку	5	NXP 72 Кбайт	41/71 евро
Дания	Поликарбонатная страница	-	Gemplus** 64 Кбайт	150/350 датских крон
Финляндия	Поликарбонатная страница	5	-	37,50 евро
Германия	Поликарбонатная страница	10/5	NXP 72 Кбайт Infenion 64 Кбайт	37,50/59 евро
Исландия	Вкладыш в обычный бумажный паспорт	-	-	81 фунт стерлингов
Голландия	В заднюю обложку	5	NXP 72 Кбайт	49,33 евро
Норвегия	Поликарбонатная страница	5	Gemplus* 64 Кбайт	87 фунтов стерлингов
Швеция	Поликарбонатная страница	5	Gemplus* 64 Кбайт	29/43 евро
Австралия	В центральную страницу	-	NXP 72 Кбайт	150 долл.
Новая Зеландия	Поликарбонатная страница	-	Philips 72 Кбайт	123 фунта стерлингов
Сингапур	Поликарбонатная страница	-	Philips 64 Кбайт	37,02 долл.
Австрия	Поликарбонатная страница	5	NXP 72 Кбайт	69 евро
Франция	В обложку	-	NXP 72 Кбайт	41 фунт стерлингов
Таиланд	В заднюю обложку	5	NXP 72 Кбайт	-

*NXP – в прошлом – отделение Philips Semiconductor компании Philips Royal.
**Компания Gemplus не только разрабатывает для своих карт собственные микросхемы, но и сотрудничает с ведущими производителями микропроцессоров. Скорее всего, в электронных паспортах Gemplus используются микросхемы NXP или Infineon.

па. Возможны следующие варианты реализации этой методики. Владелец паспорта вводит в считывающее устройство PIN-код. Либо сравнение производится исключительно на карте, содержащей образец биометрических данных, полученных у пользователя при проверке. Или же проверяющая сторона (устройство чтения) применяет специальный открытый ключ, заверенный сертификационным центром и удостоверяющий правомерность такого контроля.

Если правильно реализовать описанные способы защиты, данные, записанные в бесконтактную карту, будет невозможно ни скопировать, ни изменить, ни подделать. Нужно только внедрить карту с микросхемой в паспорт.

НА ЧЕМ ВСЕ ДЕРЖИТСЯ И СКОЛЬКО СТОИТ?

Оснащение главного идентификационного документа бесконтактной картой с микросхемой и антенной ставит производителей паспортов перед новой проблемой. Обычная бумага не предназначена для хранения такой карты и ее защиты. Необходимы новые материалы и механизмы включения карт в паспорт. Существует два решения. Первое, используемое в России, – применение пластиковой (поликарбонатной) страницы с персональными данными и вмонтированной бесконтактной картой. На RFID-карту (антенна, микросхема и подложка) наносится слой поликарбоната, а поверх него – ламинирующее покрытие. Через это покрытие лазерной гравировкой записываются персональные данные. Подобная пластиковая страница с микросхемой очень прочна и надежна. Второе решение – это внедрение антенны и микросхемы в заднюю обложку паспорта. При этом внешний вид и буклет традиционного паспорта сохраняются. Срок службы большинства обычных паспортов – 10 лет. Что же касается паспортов нового поколения, следует помнить о незрелости технологии и возможных изменениях всей паспортной системы. С другой стороны, логично предположить, что срок действия электронных документов окажется выше. Кроме того, стоимость традиционных бумажных документов в среднем вдвое ниже электронных. Таким образом, с учетом пятилетнего срока действия, затраты потребителей увеличиваются в четыре раза. Тем не менее, многие страны, вопреки рекомендациям ICAO о десятилетнем сроке электронных паспортов, устанавливают пятилетний срок (табл.2).

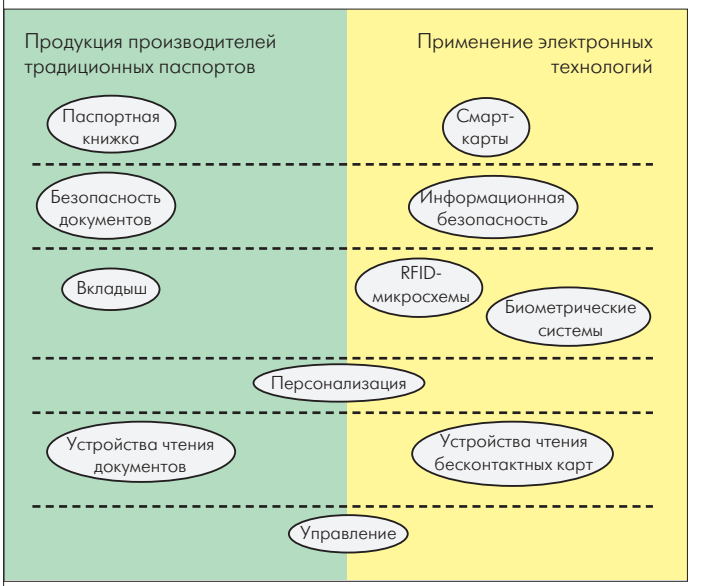

Рис.5. Дополнительные этапы производства электронных паспортов

ПРОИЗВОДСТВО ЭЛЕКТРОННЫХ ПАСПОРТОВ: КТО НА НОВЕНЬКОГО?

Появление электронного паспорта привело к решительным изменениям в сфере производства защищенных документов. Раньше эта отрасль контролировалась несколькими корпорациями, владеющими традиционными средствами защиты ценных документов (специальные чернила, водяные знаки и пр.). Теперь же в авангарде находятся компании, наиболее эффективно использующие электронные технологии. Цепочка производства становится все более сложной (рис.5), поэтому ни одна компания не может осуществить все ее этапы. Это ведет к новым альянсам и резкому расширению компаний. Подобные структурные изменения не только обеспечивают прибыльность производства бесконтактных карт, но и позволяют компаниям реализовывать большее число этапов производства паспортов. Как следствие – растут государственные заказы.

Корпорация Gemalto (Нидерланды) была образована в результате слияния таких крупных производителей средств идентификации и защиты данных, как Axalto и Gemplus International S.A. В июне 2006 года Gemalto стала основным игроком на рынке электронных паспортов. Годовой доход корпорации составил 2,2 млрд. долл. По итогам 2005 года Gemplus возглавляла производство смарт-карт как по прибыли, так и по общему объему поставок. Продукция Gemplus применяется в системах идентификации, мобильных средствах связи, банках, беспроводных сетях и здравоохранении. В 2005 году потенциал компании в области ценных документов и поликарбонатных карт возрос за счет приобретения финского производителя смарт-карт и средств печати документов с высокой степенью защиты Setec. В зависимости от конкретных требований Gemplus использует и микросхемы крупных полупроводниковых производителей – NXP, Siemens, Hitachi. Но в отличие от других поставщиков бесконтактных карт, компания разрабатывает и собственные микросхемы, которые по ее заказу выпускают эти же полупроводниковые фирмы. Например, в последней Java-карте компании Gemplus используется микроконтроллер фирмы NXP семейства SmartXA с ЭСРПЗУ емкостью 64 Кбайт, выполненный по 0,18-мкм технологии.

Самый крупный контракт у фирмы Setec – более 100 млн. евро. Согласно контракту, Setec производит национальные электронные паспорта Швеции. Правительство Норвегии в рамках программы внедрения национальных биометрических паспортов выплатит компании Setec 30 млн. евро. Для национальных электронных удостоверений личности Финляндии Setec предоставляет новое решение с поддержкой языка Java. Новые карты будут оснащены ОС Java Card™ и более мощной микросхемой с памятью объемом 64 Кбайт фирмы NXP. Напомним, что одним из участников программы введения российских биометрических паспортов является компания Axalto, также входящая в концерн Gemalto. Для США Axalto выпускает RFID-вкладыши, считывающие устройства и ПО, а также электронные обложки (как и для новых французских паспортов).

Таким образом, сегодня корпорация Gemalto участвует в программах внедрения электронных паспортов Дании, Норвегии, Португалии, Польши, России, Сингапура, Словении, США, Франции, Финляндии, Швеции и Чехии. Для электронных обложек польских паспортов Gemalto должна ежегодно поставлять 1,5 млн. RFID-вкладышей (inlays).

Средства сбора биометрической информации, переносные станции верификации и снятия отпечатков пальцев производит компания Motorola. Ее продукция предназначена для идентификации личности по трех- и двухмерному изображению лица, отпечаткам ладони и пальцев. Отдельно стоит отметить мобильные станции идентификации-верификации личности в пунктах пограничного контроля. Связь такой станции с сервером базы данных обеспечивают протоколы APC0265; TETRA; COPD; GSM/GPRS; CDMA; интерфейс Ethernet RG45. Продукция Motorola задействована в национальной системе электронных паспортов Норвегии. В своих решениях Motorola не всегда опирается на собственную аппаратную базу, предоставляя лишь ПО, интерфейсную и протокольную части систем.

Фирма Viisage (США) изначально ориентировалась исключительно на биометрические технологии. Однако, несмотря на негативное финансовое положение (2005 году ее убытки оценивались в 3 млн. долл.), она взяла курс на производство RFID-меток, смарт-карт и альтернативных биометрических технологий. Для этого Viisage в 2004 году приобрела крупнейшего европейского производителя систем распознавания личности по цифровой фотографии – компанию ZN Vision Technologies. Кроме того, Viisage за 50 млн. долл. купила фирму Trans Digital Technologies (TGT) – специалиста в области печати с высокой степенью защиты данных и поставщика паспортов по заказу правительства США. Покупка мирового лидера на рынке средств удостоверения подлинности документов компании Image Automation (iA) позволила фирме Viisage проводить экспертизу аутентичности документов с использованием развитой системы баз данных. Следующим шагом компании стала установка линии изготовления микросхем бесконтактных карт с интерфейсом iAthenticate. В итоге Viisage обладает технологиями регистрации, персонализации, авторизации и проверки достоверности документов, а также биометрическими технологиями. Результатом недавнего слияния с компанией Identix (США)* стала система распознавания личности по нескольким биометрическим характеристикам. ПО фирмы Viisage для распознавания изображения лица пользуются Министерство обороны США, система

* Слияние Viisage Technology и Identix Incorporated привело к созданию объединенной компании, которая с 29 августа 2006 года носит название L-1 Identity Solutions.

пограничного контроля аэропорта Берлина, средства идентификации крупных отелей и казино. Программные средства фирмы Viisage используются в электронных паспортах США, Пакистана и Австралии.

Существует компании, которые не могут выполнять все этапы внедрения электронных паспортов, однако являются лидерами в своих отраслях. Например, компания Datacard Group (США), крупнейший производитель пластмассовых идентификационных карт. Среди ее клиентов – 120 стран. Предлагаемые принтеры идентификационных карт и устройства персонализации позволяют производить карты с высокой степенью защиты данных. Компания предоставляет специальные программные средства, систему идентификации, устройства считывания биометрических данных: отпечатков пальцев, цифровой фотографии. Несмотря на отсутствие собственной технологии RFID-микросхем, Datacard участвует в паспортных программах Голландии, Израиля и Таиланда.

Лидер биометрической отрасли – компания Cognitec (ФРГ) – производит, возможно, лучшие системы распознавания личности по цифровой фотографии лица и соответствующее ПО. С 1995 года Cognitec выпускает системы контроля доступа на основе цифровых фотографий. В 2002 году результаты тестирования систем автоматического распознавания личности по фотографии лица FRVT (Face Recognition Vendor Test) подтвердили лидерство компании Cognitec в этой технологии. С 2005 года Cognitec в рамках австралийской паспортной программы поставляет системы сбора биометрических данных и ПО для персонализации паспортов, системы верификации и ПО для систем пограничного контроля. По этому же контракту Cognitec производит ПО для проверки качества изображения фотографий в паспортах.

ВЫБОР МИКРОПРОЦЕССОРОВ: ПОЕДИНОК РАВНЫХ

Компаниям-производителям бесконтактных карт невыгодно налаживать собственное полупроводниковое производство. Обычно они покупают готовые решения. Для электронных паспортов – микросхемы стандарта ISO 14443. Монополист на этом рынке – компания NXP, поставляющая до 80% микросхем всех электронных паспортов. Технология микропроцессоров с интерфейсом MIFARE компании NXP полностью совместима с ISO 14443 и признана стандартом в области бесконтактных карт. Правительство США выбрало NXP как одну из двух компаний-поставщиков RFID-микросхем. Семейство 32-разрядных микроконтроллеров SmartMx компании предназначено для карт, используемых в паспортных программах Голландии, Бельгии, Франции, Австрии, Германии и др. Микроконтроллер P5CT072 этого семейства первым из микросхем для электронных паспортов сертифицирован на соответствие стандарту безопасности CC уровня EAL5+ (Common Criteria Evaluation Assurance Level). Микроконтроллер изготовлен по усовершенствованной 0,18-мкм КМОП-технологии с пятислойной металлизацией. Для крип-

тографической защиты предусмотрены сопроцессоры, реализующие алгоритмы 3-DES и AES, и ускоритель шифрования FameXE для алгоритмов PKI. Срок хранения данных – 20 лет. Память рассчитана на 500 тыс. циклов записи. Микроконтроллер с тройным интерфейсом поддерживают контактные (ISO 7816 и USB 2.0) и бесконтактный (ISO/IEC 14443) интерфейсы. Сейчас NXP работает с правительствами 28 стран.

Основной конкурент NXP – компания Infineon. Более 20 лет работы в области микросхем с высокой степенью защиты данных принесли компании 38% этого сектора мирового рынка. Всплеск интереса к RFID-картам побудил компанию Infineon выпустить серию новых микросхем для бесконтактных карт стандарта ISO 14443. Это – 16-разрядные микроконтроллеры 66CxxxP серии SLE, выполненные по 0,22-мкм технологии. Они работают с основными бесконтактными (ISO 14443 A, B; Felica) и контактными интерфейсами. В контроллер бесконтактной карты модели SLE 66CLX641P входят ЭСРПЗУ емкостью 64 Кбайт, 136-Кбайт ПЗУ, 5 Кбайт ОЗУ. Контроллер, оптимизированный для банковских систем и устройств идентификации личности, поддерживает алгоритмы шифрования 3DES, RSA и ECDSA.

Микросхемы компании Infineon используются более чем в 30 национальных и здравоохранительных программах, например в картах общего доступа Министерства обороны США. В рамках российской паспортной программы Infineon заключила договор с заводом "Микрон" на передачу и внедрение 0,25-мкм технологии микросхем. Эти микросхемы с энергонезависимой памятью емкостью 64 Кбайт планируется использовать в первой серии российских биометрических паспортов. 21 августа 2006 года правительство США объявило, что компания Infineon станет одним из двух поставщиков микросхем для американских электронных паспортов. Подобное решение было принято и в Германии.

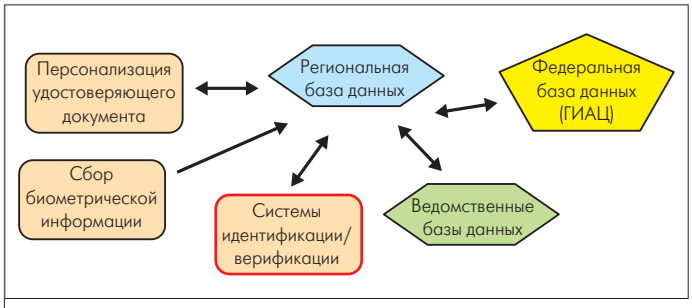

Рис.6. Упрощенная структура национальной паспортной системы

ЧТО В РОССИИ?

Анализ производителей электронных паспортов и их компонентов свидетельствует: основная тенденция многих государств – привлечение к проведению программ зарубежных компаний, в том числе поставщиков микросхем и устройств персонализации. При этом допускается закупка не только конкретной технологии (RFID-микросхем или защищенных карт), но и услуг по разработке всей инфраструктуры системы. Речь идет о проработке протоколов и сетей связи, ПО для взаимодействия структурных узлов, оборудования автоматизированных рабочих мест паспортных служб, системы серверов баз данных, средств пограничного контроля и моделей их взаимодействия. На базе бюджета государственной программы формируется аппаратная база и средства защиты данных. При этом используются технологии компаний NXP, Viisage и др. Пример общей структуры национальной паспортной системы приведен на рис.6.

В России не существует промышленного гиганта, способного взять на себя все этапы создания электронного паспорта нового поколения. Первоначально в целях национальной безопасности планировалось задействовать исключительно российские разработки. Например, разработку средств распознавания биометрических данных должно проводить НПО "Информация". Но уже для производства вкладыша с микросхемой привлечен иностранный производитель. Тендер, организованный Гознаком, выиграли НТЦ "Атлас" и компания Axalto. Механизм крепления поликарбонатной страницы в паспорт и печати паспортной книжки с высокой степенью защиты взял на себя Гознак. Для RFID-этикетки (вкладыша) желательна отечественная микросхема. К сожалению, предприятие "Микрон" обладает только технологией производства 0,8-мкм микропроцессоров. Поэтому для оснащения линий

производства микросхем на гибких носителях был заключен договор с компанией Infineon. Кроме того, с французкой компанией STMicroelectronics было достигнуто соглашение о передаче технологии производства кристаллов с топологическими размерами 0,18 мкм. Подобный технологический переход потребует не только денежных, но и временных ресурсов. Поэтому первые партии российских паспортов будут оснащены микросхемами компании Infineon.

Денежные инвестиции в развитие национальной паспортной системы огромны. Так, на покупку новой технологии микропроцессоров будет затрачено 10 млн. евро, не считая затрат на реорганизацию производства. Впрочем, с подобными тратами столкнулись и страны, планировавшие введение новых паспортов к 26.10.2006. Технология – лишь часть программы введения электронных паспортов. Необходимо законодательно утвердить процедуры регистрации и проверки персональных данных, протестировать совместимость паспортов и устройств чтения, отладить инфраструктуру управления открытыми ключами. И, самое главное, принять единую спецификацию требований к ПО, содержимому чипов, каналов связи, сетей, серверов, всех узлов инфраструктуры паспортной системы.

ЛИТЕРАТУРА

1. Keesing Journal of Documents & Identity: the world of secured documents in a single magazine. www.keesingref.com/kjd/.
2. http://www.nxp.com/index.html.
3. http://www.infineon.com.
4. http://www.setec.com.
5. http://www.gemplus.com.
6. http://www.axalto.com
6. http://www.rfidjournal.com.
6. Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards. – In Application note ATmega.
7. Euro smart Recommendations for European Electronic visa and passport. – In Eurosmart contribution to European Union regarding ePassports and eVisa, – October, 2004.
8. **Kugler D.** Security Mechanisms of the Biometrically Enhanced (EU) Passport. – In 2nd International Conference on the Security in Pervasive Computing. 04.07.2005.
9. **Павлов И., Потапов А.** Контроль подлинности документов, ценных бумаг и денежных знаков – Техносфера, 2006.

Компании AMD и Hynix врываются в первую десятку мировых производителей полупроводниковых приборов

Согласно предварительной оценке ведущих мировых производителей полупроводниковых приборов, проведенной аналитической фирмой iSuppli , в список 10 ведущих полупроводниковых компаний 2006 года впервые войдут компании Advanced Micro Devices (AMD) и Hynix Semiconductor (см. таблицу). Это обусловлено в первую очередь устойчивым ростом мирового рынка полупроводниковых приборов, который, в соответствии со скорректированной оценкой фирмы iSuppli, в 2006 году возрастет по сравнению с предыдущим годом на 9% (вместо ранее предполагавшихся 7,8%) и составит 258, 5 млрд. долл.

Ожидается, что доходы AMD за 2006 год увеличатся на 90% – с 3,9 млрд. долл. в 2005 году до 7,5 млрд. долл. Благодаря этому компания займет в списке десяти ведущих фирм седьмую позицию вместо 15-й в 2005-м. Столь резкое увеличение объема продаж объясняется ростом спроса на микропроцессоры компании, в первую очередь двухядерных микросхем. Доходы компании от продажи микропроцессоров в 2006 году увеличатся на 37,5%. Но более ощутимый вклад в увеличение доходов AMD принесло приобретение этой фирмой в октябре 2005 года изготовителя графических микросхем – компании ATI Technologies.

В 2006 году доходы производителя микросхем памяти – фирма Hynix – на рынке полупроводниковых приборов, согласно оценкам iSuppli, составят 7,4 млрд. долл. против 5,6 млрд. долл. в предыдущем году (прирост в 32,5%). В результате Hynix в 2006 году займет восьмую позицию в списке десяти ведущих полупроводниковых фирм вместо 11-й позиции в 2005-м. Это обусловлено успешной продажей микросхем ДОЗУ и флэш-памяти NAND-типа. Так, продажи компанией микросхем ДОЗУ увеличатся на 1,8 млрд. долл., флэш-памяти NAND-типа – на 770 млн. долл. Рост продаж ведущего мирового поставщика микросхем памяти – компании Samsung Electronics – будет более скромным – 1,77 млрд. долларов.

Вследствие агрессивной борьбы за первенство на рынке микропроцессоров, приведшей к снижению цен на эти микросхемы, доходы от их продаж в 2006 году сократятся на 6,6%. Это привело к тому, что в 2006 году доходы компании Intel сократились на 11,6%. Правда, следует отметить и уменьшение спроса и на ее флэш-памяти NOR-типа. В результате, по данным iSuppli, доля Intel на рынке полупроводниковых приборов составит 12,1%. Помимо Intel, в 2006-м снизились доходы компаний Renesas Technology и NEC, входивших в 2005 году в список десяти ведущих полупроводниковых фирм.

www.eetimes.eu

Рейтинг		Фирма	Доход		Изменение дохода, %	Доля на рынке, %
2005 г.	2006 г.		2005 г.	2006 г.		
1	1	Intel	35466	31359	-11,6	12,1
2	2	Samsung Electronics	17210	19207	11,6	7,4
3	3	Texas Instruments	10745	12832	19,4	5,0
4	4	Toshiba	9077	10166	12,0	3,9
5	5	STMicroelectronics	8801	9931	11,8	3,8
7	6	Renesas Technology	8266	8221	-0,5	3,2
15	7	Advanced Micro Devices	3917	7471	90,7	2,9
11	8	Hynix	5560	7365	32,5	2,8
9	9	NXP	5646	6221	10,2	2,4
10	10	Freescale Semiconductor	5598	6059	8,2	2,3