



Обеспечение безопасности в системе документов, удостоверяющих личность (Аспекты введения биометрии в проездные документы)

Милан Штерба

**Ведущий консультант,
Государственный сектор
НР Центральная и Восточная
Европа, Ближний Восток и
Африка**

E-mail: milan.sterba@hp.com

Александр Бражников

**Менеджер по развитию
бизнеса**

**Государственный сектор НР
Россия**

E-mail:
alexander.brazhnikov@hp.com



Содержание

Введение в проблему биометрического паспорта

Решения и стандарты по биометрическим паспортам

Биометрические технологии

Безопасность в системе обычного паспорта

Воздействие биометрии на процессы работы с заявлениями на паспорт, выдачи и использования паспортов

Подход компании HP к «end-to-end» решению по биометрическому паспорту

Выводы

Биометрический паспорт - введение

Цели



В сентябре 2001 Совет безопасности ООН единогласно принял широкомасштабную резолюцию 1373 по антитерроризму, в которой.



- “2. Также решено, что все государства будут:
“(g) Предупреждать передвижение террористов или террористических групп путем организации эффективного пограничного контроля и контроля за выпуском документов удостоверяющих личность и заграничных паспортов, и **усилению мер по пресечению подделок, фальсификаций или мошенничества с документами удостоверяющими личность**
- “3. Все государства призваны:
“(a) Найти пути интенсификации и **ускорения обмена оперативной информацией** особенно касательно: передвижений террористов или террористических сетей; **фальшивых или поддельных паспортов**; проникновений в армию, использования взрывоопасных материалов и коммуникационных технологий террористическими группами; угрозы от оружия массового поражения

Международные акции

- Программа **US-VISIT** предусматривает, что иностранные граждане, путешествующие в США, подлежат идентификации путем сканирования **отпечатков 2-х пальцев и цифровой фотографии лица (PDF)**, сделанных в момент пересечения поста пограничного контроля для идентификации граждан
- США требует от 27 стран безвизового пространства с **26 октября 2005 года начать выпуск** машиночитаемых паспортов повышенной прочности и содержащие биометрические данные владельца паспорта
- **Европейский Парламент** 2 декабря 2004 года проголосовал за предложение о включении в паспорт изображения лица в качестве биометрического идентификатора. Страны-участницы должны обеспечить исполнение решения **в течение 18 месяцев после утверждения технических требований**

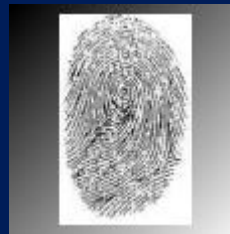
Цели введения биометрии в проездные документы?

- Усиление **однозначного соответствия** между биометрическими параметрами их носителя и их копией в документе
- Снижение риска **фальсификации** документа
- Увеличение **безопасности** при их производстве и повышение **достоверности** процессов проверки личности
- **Комфортность и безопасность** для самого носителя документов при их проверке или в случае их утери и т.д.
- **Автоматизация** процесса идентификации личности
- Повышение вероятности выявления **«нежелательных»** персон

Биометрические технологии – сегодня и завтра



2-мерное (2D)
изображение лица
(Граждан/Преступников)



Отпечаток пальца
(Граждан/Преступников)



3-мерное (3D)
изображение лица



ДНК



Голос



Геометрия руки



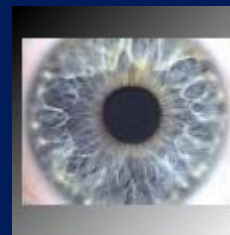
Венозный
рисунок
пальца



Ухо



Подпись



Радужка глаза



Какую биометрию использовать?

Распознаваемый биопризнак	Применимость	Использование	Точность образа	Надежность	Частота ошибок	Причины ошибок
Отпечаток пальца	✓	✓	●●●●	▶▶▶	1 из 500+	Сухость кожи, загрязнения, возраст
Лицо	✓	✗	●●●	▶▶	Нет данных	Изменение цвета, возраст, очки, волосы
Геометрия руки	✓	✗	●●●	▶▶	1 из 500	Повреждение руки, возраст
Голос	✓	✗	●●	▶	1 из 50	Шум, погода, простуда
Радужка	✓	✓	●●●●	▶▶▶	1 из 131,000	Обесцвечивание
Сетчатка	✓	✓	●●●●	▶▶▶	1 из 10,000,000	Контактные линзы
Подпись	✓	✗	●●	▶	1 из 50	Изменение со временем
Машинопись	✓	✗	●	▶	Нет данных	Усталость, повреждение руки
ДНК	✓	✓	●●●●	▶▶▶	Нет данных	Ошибок нет

Источник: Национальный центр государственного судопроизводства США 2004



Какую биометрию использовать?

Распознаваемый биопризнак	Уровень безопасности	Стабильность во времени	Признаваемость пользователем	Раздражимость при снятии	Простота в использовании	Низкие затраты
Отпечаток пальца	■ ■ ■	▶ ▶ ▶	◆ ◆	В небольшой мере	● ● ●	▼
Лицо	■ ■	▶ ▶	◆ ◆	Нет	● ●	▼
Геометрия руки	■ ■	▶ ▶	◆ ◆	Нет	● ● ●	✗
Голос	■ ■	▶ ▶	◆ ◆ ◆	Нет	● ● ●	▼
Радужка	■ ■ ■	▶ ▶ ▶	◆ ◆	Нет	● ●	✗
Сетчатка	■ ■ ■	▶ ▶ ▶	◆ ◆	Высокая	●	✗
Подпись	■ ■	▶ ▶	◆ ◆	Нет	● ● ●	▼
Машинный	■ ■	▶	◆ ◆ ◆	Нет	● ● ●	▼
ДНК	■ ■ ■	▶ ▶ ▶	◆ ◆	Чрезвычайная	●	✗

Источник: Национальный центр государственного судопроизводства США 2004

Действующие международные стандарты



- Документы группы ИКАО по биометрическим паспортам, вошедшие в новую (6-ю) редакцию издания Doc9303:
 - Введение бесконтактного чипа в машиносчитываемые проездные документы (МСПД)
 - Внедрение биометрии в МСПД версии 2.0 (MRTD 2.0)
 - Использование **цифрового фото** как **обязательного** биопараметра
 - Использование отпечатков **пальцев и радужки глаза** в качестве **дополнительных** биопараметров
 - Архитектура открытых ключей для МСПД, дающая доступ к бесконтактному чипу только на чтение
 - Технический доклад по логическая структурам данных (LDS)
- Соответствующие ISO/IEC стандарты:
 - ISO/IEC 14443 по бесконтактным близкодействующим картам вместе с ISO/IEC 7816-4 Команды, применяемые в картах, и протоколы связи
 - ISO/IEC 19794 Биопризнаки пассажиров и обмен биометрическими данными

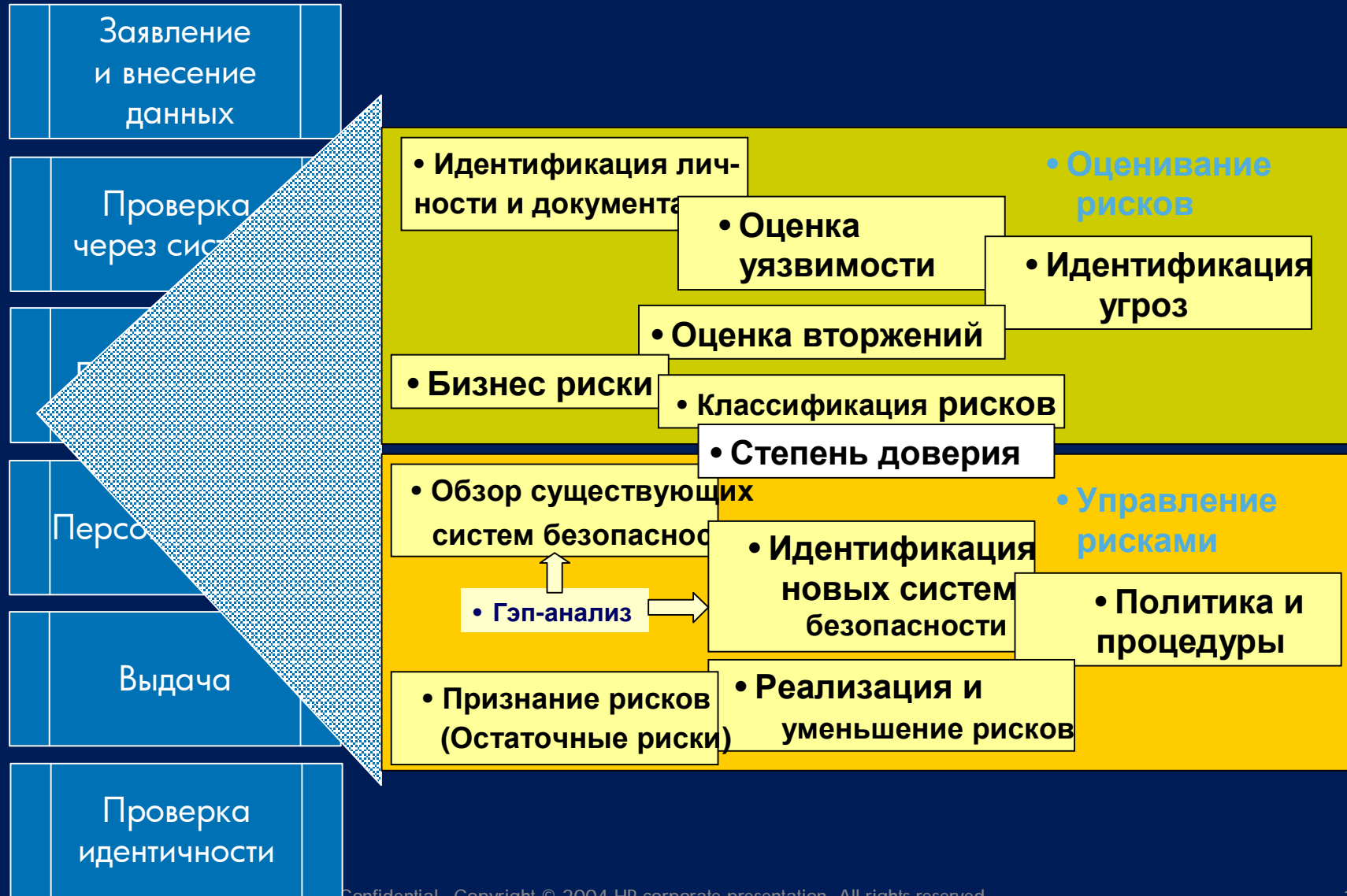
Деятельность HP по стандартизации и сертификации в безопасности



- HP является активным участником в более чем 150 международных органах по стандартизации включая IEEE, ITU, ISO, ANSI, NISO
- HP - особенно активный участник следующих органов по вопросам безопасности
 - Internet Engineering Task Force – безопасность сетей, управление системами и сетями
 - BioAPI Consortium – биометрические интерфейсы (ISO/IEC 19794)
 - WWW Consortium – безопасность Web-сервисов
 - Trusted Computing Platform Association – безопасность компьютерных систем
 - PKI Forum – взаимодействие архитектур ключей с открытым доступом
 - The Open Group – безопасная архитектура, управление электронной идентификацией, активное предотвращение потерь
 - Object Management Group – безопасность распределенных систем

Безопасность в системе обычного паспорта

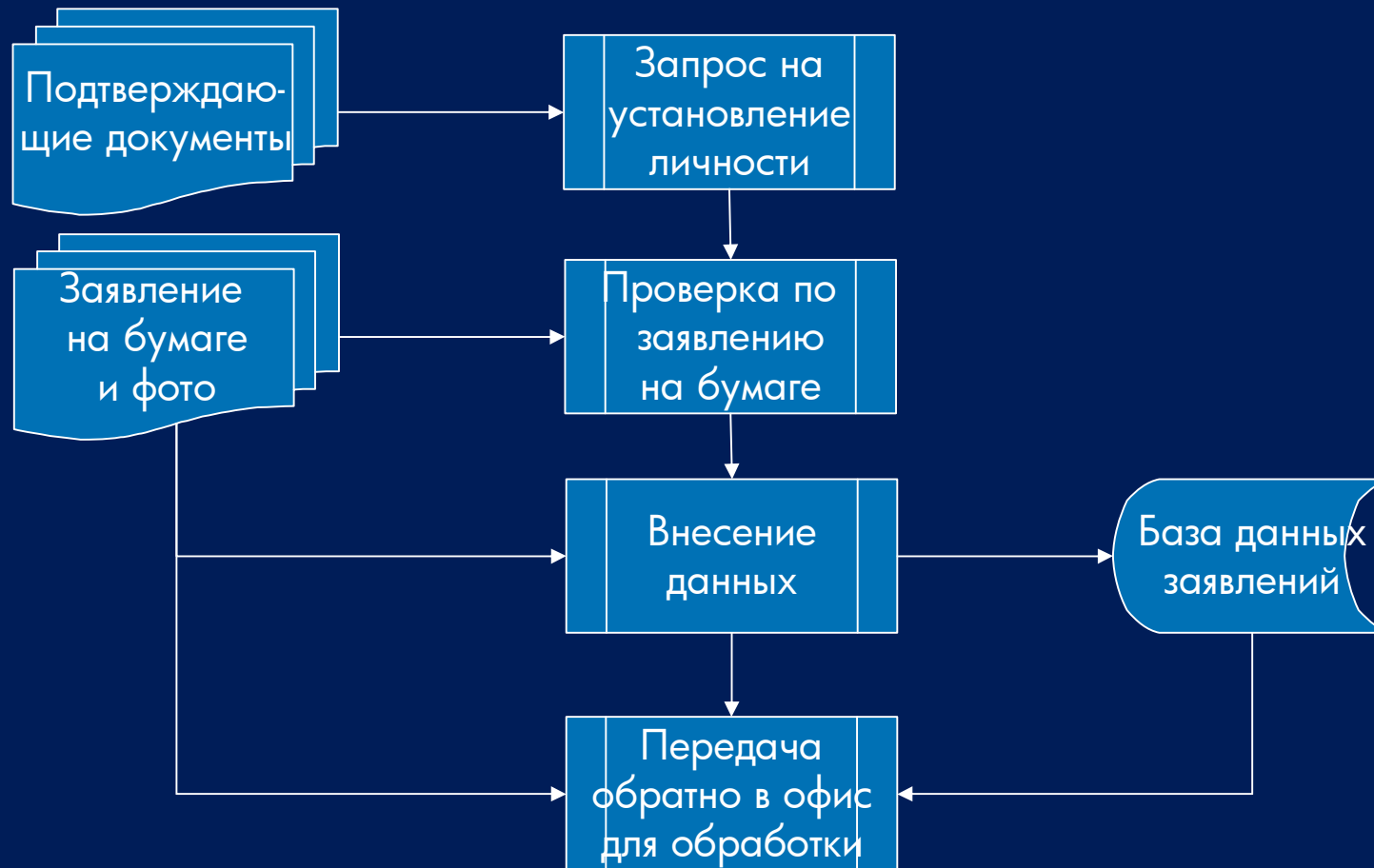
Основные процессы, связанные с паспортом, и их безопасность



Каковы основные риски?

- Подделка или изменение подлинного паспорта криминальными и другими структурами, которые нуждаются в новых документах по идентификации личности и гражданства
- Получение паспорта обманным путем, используя подложные или украденные документы
- Воровство и заполнение бланков заявлений на выдачу паспорта
- Должностные преступления сотрудниками авторизованных государственных органов по выдаче паспортов (внутренние мошенничества).

Пример 1 - Обработка заявлений для обычного паспорта



Пример 2 - Издание обычного паспорта



В чем состоит проверка документа и идентичности



- Действительный ли это документ? Не подделан ли он как-либо?



- Тот ли вы, кого представляет документ? Соответствуют ли ваши идентификационные признаки документу?



- Если «нет», то кто вы?
- Связаны ли с вашей реальной персоной какие-либо особые действия/запросы?

Идентификация в обычном случае

- Подлинный документ?
 - Признаки безопасности классического документа (классы I, II, III)
 - Списки утерянных или украденных документов и другие специальные списки и базы данных
 - Официальные каталоги и базы данных по подлинным документам и их признакам
 - Физический осмотр документа
- Соответствует ли персоне?
 - Сравнение с фотографией
 - Другие физические характеристики, описанные в документе
 - Информация о визе
 - Наблюдение за поведением предъявителя
 - Другие обстоятельства (сопровождающие, багаж и т.д.)
 - Зондирование вопросами
 - Специальные списки и уведомления



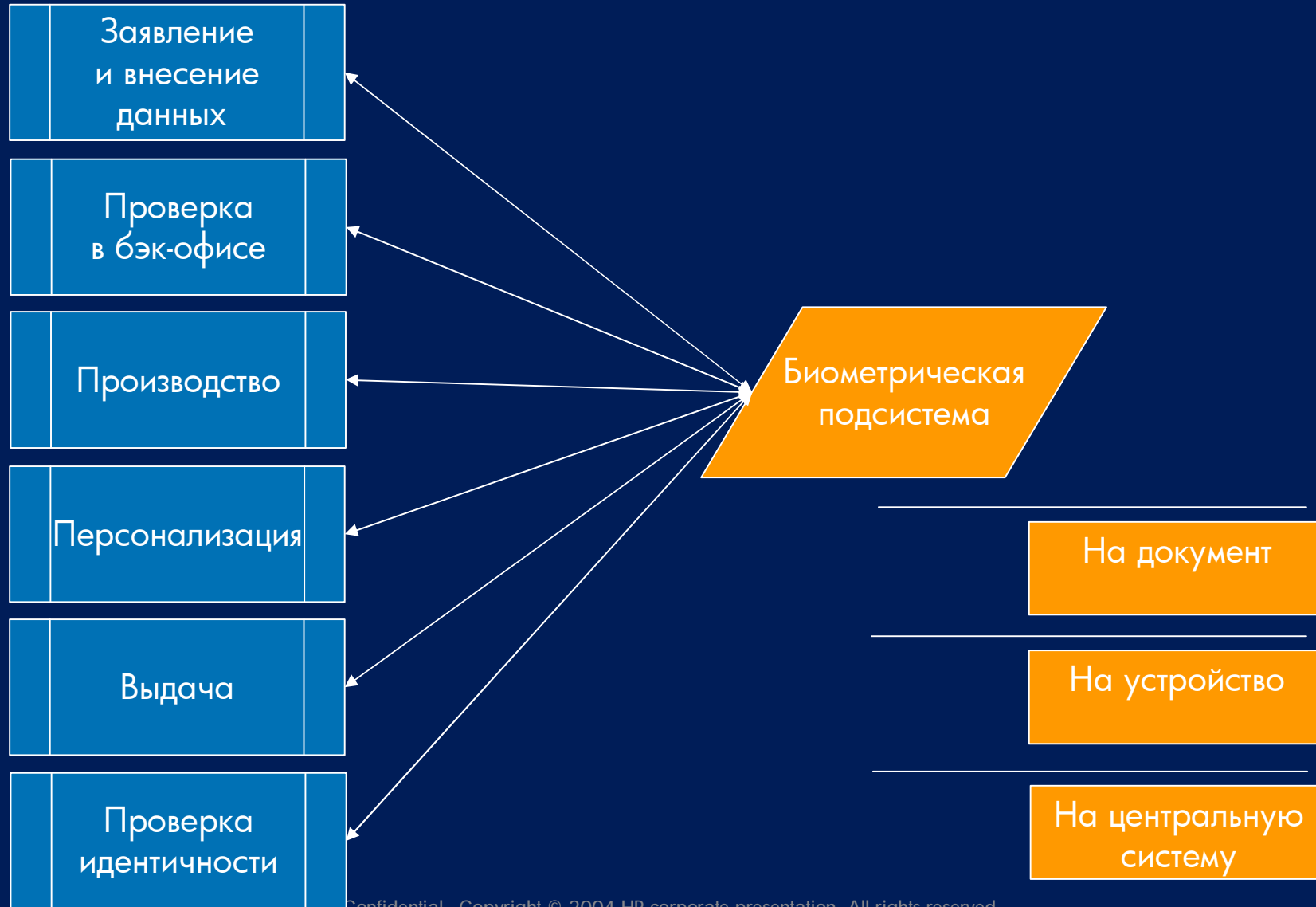
Что вносит
биометрия в
системы
проездных
документов

Влияние биометрии на паспортную систему



- Из-за введения электронного чипа все данные должны собираться в электронном виде
- Введение однозначной физической связи между физическими характеристиками владельца паспорта и самим документом (один или более биопараметров)
- Использование дополнительных цифровых возможностей защиты (PKI, цифровая подпись)
- Возможность создания независимых биометрических баз данных, позволяющих проводить идентификацию всех персон по внесенным о них данным даже без самого документа

Влияние на связанные с паспортом бизнес процессы



Пример 1 – Обработка заявлений для биометрического паспорта



Пример 2 - Издание биометрического паспорта



Подходы к процессу биометрической проверки/идентификации



Цифровое фото
Отпечаток пальца
Радужка ...



Персональные данные :

- Демографические данные
- Биометрические данные
- Другие
- Электронная подпись всех данных уполномоченным центром

Проверка 1:1 по документу

- Безопасное (за подписью) хранение и восстановление данных
- Проверка по кодированному чипу

Проверка 1:1 на устройствах:

- Восстановление текстовых данных
- Сканирование отпечатков пальцев
- Сопоставление детальной выборки

Он-лайн идентификация 1:n

- он-лайн идентификация 1:n по отношению к центральной биометрической системе

Влияние биометрии на безопасность в паспортной системе в целом



Основные риски также как и подход к их предотвращению и уменьшению остается тем же самым

Каковы основные риски?

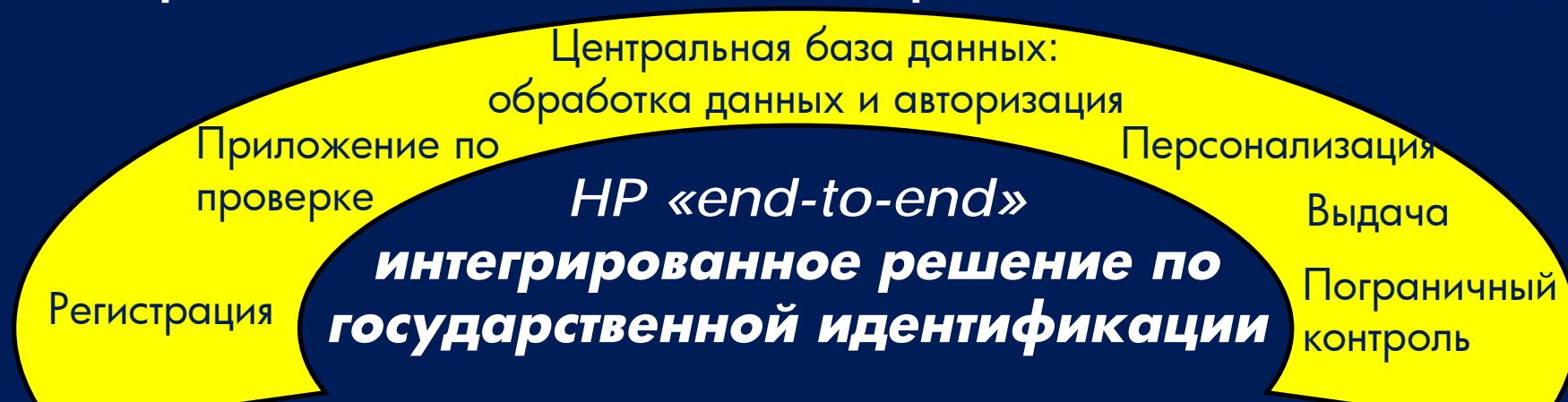
- Подделка или изменение подлинного паспорта криминальными и другими структурами, которые нуждаются в новых документах по идентификации личности и гражданства
- Получение паспорта обманным путем, используя подложные или украденные документы
- Воровство и заполнение бланков заявлений на выдачу паспорта
- Должностные преступления сотрудниками авторизованных государственных органов по выдаче паспортов (внутренние мошенничества).



Тем не менее, используя биометрию, мы имеем более совершенный инструментарий для борьбы с ними. В то же время мы также сталкиваемся с некоторыми новыми рисками!

Подход компании
НР к «end-to-end»
решению по
биометрическому
паспорту

Открытый подход HP к решению



Интегрированные технологии партнеров

Бланки документов

- Буклеты (бумага, пластик)
- Смарт-карты и чип-паспорта
- Биометрические стикеры

Биометрия

- AFIS (АДИС)
- Распознавание радужки
- Распознавание по лицу
- Проверка «1:1»
- Идентификация 1:n

Персонализация

- Лазерная гравировка и другие высокотехнологические методы защиты
- Кодирование чип-модуля

Международные стандарты

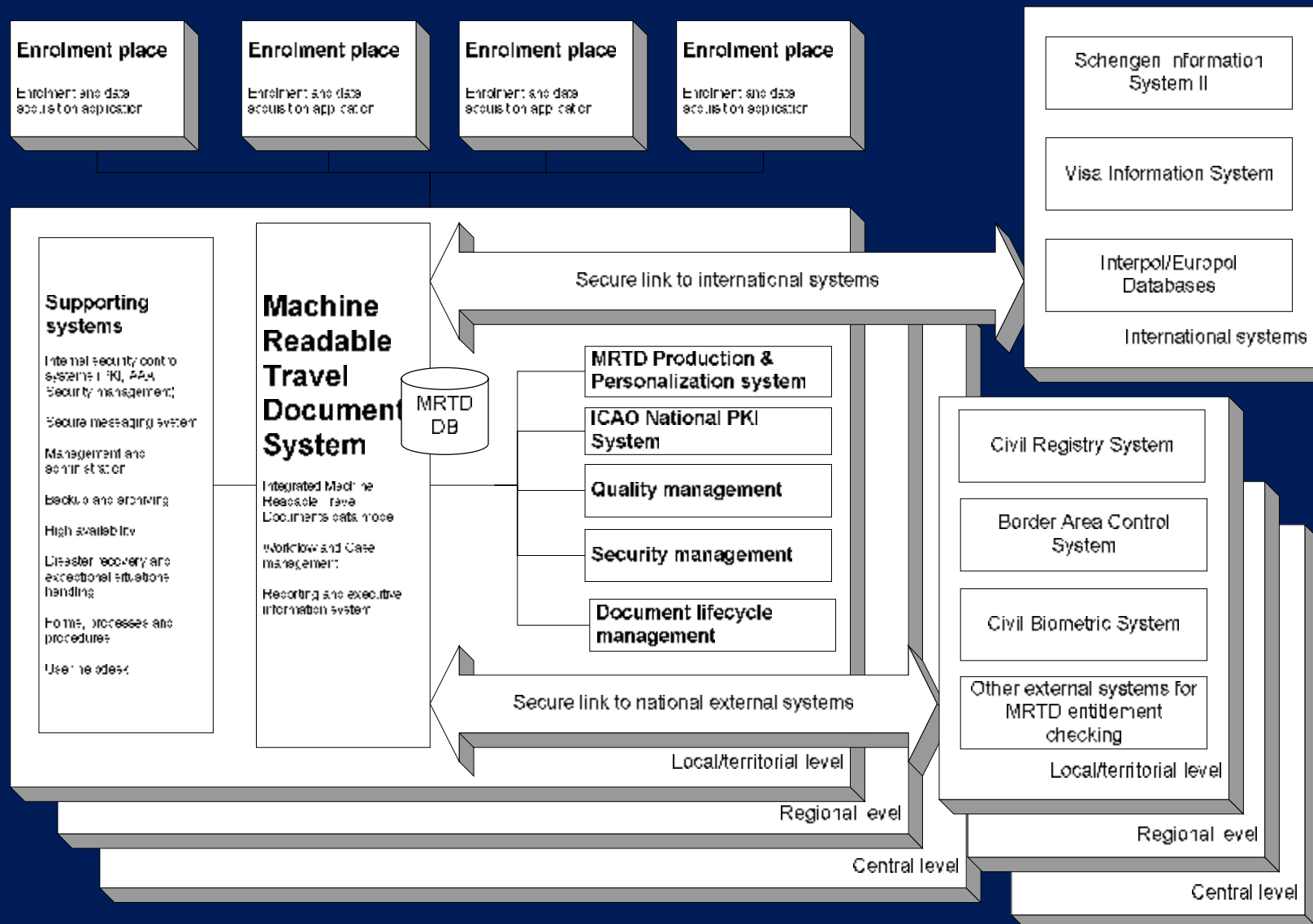
HP «end-to-end» система управления безопасностью

HP ИТ инфраструктура и ее обслуживание

HP экосистема защищенного биометрического паспорта



Организация защищенной инфраструктуры всех компонентов и интерфейсов паспортной системы



Управление жизненным циклом паспорта и обеспечение безопасности



Поставка HP решений для систем документов, удостоверяющих личность



Компания HP предлагает интегрированную унифицированную и высокотехнологичную защищенную платформу, позволяющую персональным идентификационным данным непрерывно перетекать от устройств к базам данных, из пограничной среды к центральным федеральным системам.

Федеральная транспортная сеть

Пограничная зона



Приложения/Данные

- Защита подключений
- Пограничные службы
- Национальные ID программы ID удостоверения водителя
- Борьба с подделками
- Централизованные системы идентификации
- Анализ стоп-листов

INFRASTRUCTURE

Беспроводные/проводные порты подключения

- Защита
- Аутентификация
- Регистрация пользователей
- Сжатие информации
- Поддержание рабочей сессии
- Наличие голосовой связи
- Синхронизация

ACCESS

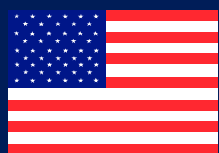
Порты сетевого провайдера

- Защищенные соединения, мобильные подключения, оптимальная маршрутизация

Устройства мобильного доступа

- Ноутбуки
- Карманные ПК
- Планшетные станции
- Мобильные телефоны
- Читающие устройства

Проекты HP по электронным удостоверениям личности (паспорта, ID-карты) по всему миру



США - водительские удостоверения в штатах Флорида и Мэриленд, карты с идентификацией по радужке для тюрем, система задержания преступников в Атланте, система учета преступников и фактов задержания в штате Аризона



Болгария – заграничные паспорта, национальные ID-карты и водительские удостоверения



Польша - национальные ID-карты, заграничные паспорта и водительские удостоверения



Италия – системы национальных ID-карт, обеспечения безопасности и биометрические системы



Израиль – широкий спектр документов: национальные паспорта Израиля, водительские и военные удостоверения, карты для голосования, свидетельства о рождении, женитьбе, смерти

другие

Разработка системы предоставления услуг Электронным правительством Гонк-Конга, Чешский государственный регистр страхования здоровья, государственный центр персонализации Словакии, карты с идентификацией по радужке для тюрем...

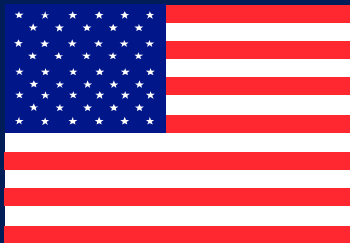
Некоторые последние акции компании HP в сфере международной безопасности



Шенгенская информационная система (фаза II) и визовая информационная система для стран Шенгена в совместном консорциуме с компанией Стериа



Недавно стартовал проект по биометрическому паспорту в Новой Зеландии



Компания HP активно участвует в реализации системы нескольких ключевых проектов по программе US VISIT и большим федеральным биометрическим системам



HP-инструментарий по безопасности I

- Проверенные инфраструктурные решения HP (сервера, системы хранения данных, сети)
- Безопасные системы баз данных
- HP решение PKI
- HP решение управления доступом
- Биометрические системы на базе HP
- HP мониторинг безопасности, инструменты управления и администрирования на базе HP OpenView
- Специальные характеристики безопасности документов, специальные устройства и поставки партнеров
- Системы персонализации со специфичными функциями безопасности

HP-инструментарий по безопасности II

- Методологии и инструменты
- Сертифицированные эксперты (PMP, CISA, CISSP, CISM)
- ISO 9001/2002 сертификация генерального исполнителя проекта
- Сервисы по восстановлению и поддержка критически важных бизнес процессов
- Курсы по безопасности, обучение и служба поддержки
- Сервисы по безопасности (от стратегии безопасности до управления инцидентами)
- Сертификация на CMM 5 разработки программного обеспечения HP
- Готовность к независимому аудиту другой компанией
- Тесное партнерство с лидирующими международными компаниями в сопутствующих областях IT и безопасности документов
- Сертифицированная партнерская сеть в России

Выводы

- НР имеет большой опыт практической работы в международных комитетах, тесные контакты с правительственными структурами и соответствующими организациями
- НР имеет соответствующие ресурсы – проект менеджеры и консультанты с сертификацией
- НР имеет практический опыт внедрения национальных систем документов персональной идентификации
- Как ведущий поставщик информационных технологий и услуг НР предлагает сквозное «end-to-end» решение
- Совместно с глобальными и локальными партнерами НР готова внедрять безопасную национальную систему документов персональной идентификации

Выводы

- **Качество данных** в паспортных регистрах является определяющим фактором, в этом плане HP предоставляет:
 - Мощные высококачественные системы/инструменты для массовых систем ввода данных высокой пропускной способности
 - Подготовленный и мотивированный персонал
 - Ориентированные на качество процессы, проектные команды и инструменты
 - Высококачественные биометрические системы, проверенные в крупномасштабных проектах
- **«End-to-end»** интегрированные системы контроля безопасности
 - Объединяющие все процессы и подсистемы
 - Управление на всех стадиях жизненного цикла документов, удостоверяющих личность
- Соответствие высоким **стандартам** и **совместимость** с международными системами
 - Документы, удовлетворяющие всем требованиям с широким признанием на международном уровне
 - Документы, способные существенно упростить возможность перемещения российских граждан через границы различных государств



«Российская Федерация может быстро стать одной из ведущих стран, внедряющих системы проездных документов нового поколения, и определить темпы внедрения таких систем в других государствах. Опыт компании HP, ее персонал и технологии могут оказать существенную помощь чтобы это произошло к назначенному сроку – Октябрь 2006 года»

Джим Гантьер

**Директор отделения международной компании
Hewlett-Packard по решениям для
правительства**