Аутентификация и идентификация

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов)

Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору.

Аутентификация

Односторонняя

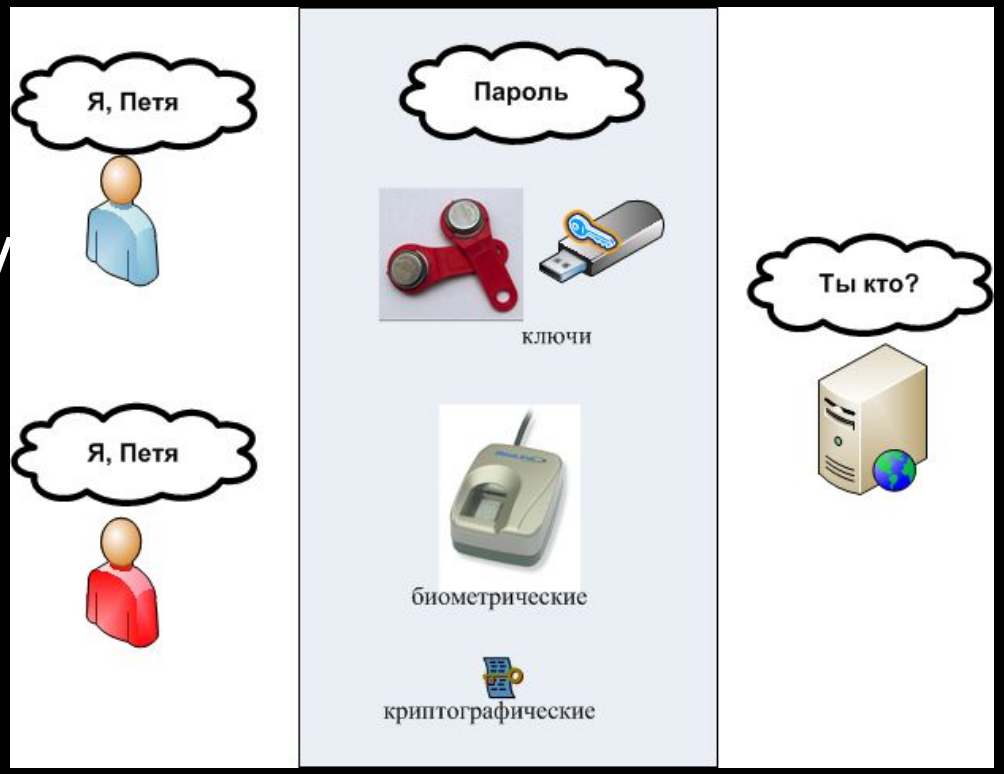
Двусторонняя

Аутентификаторы:

- нечто, что знает субъект (пароль, личный идентификационный номер, криптографический ключ и т. п.);
- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.)

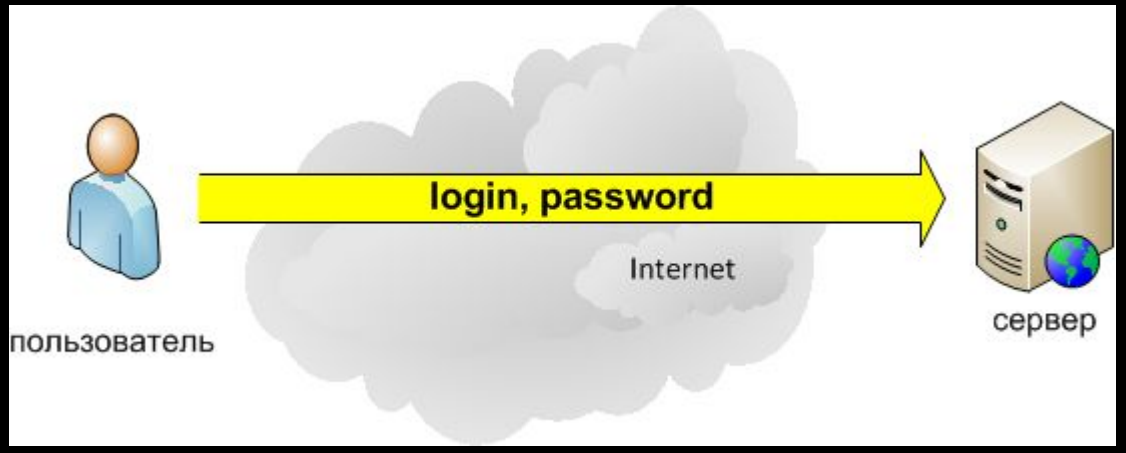
Программно-технические способы реализации идентификации и аутентификации:

- пароли;
- с использованием хеш-функции;
- на основе шифрования с открытым ключом;
- сервер аутентификации Kerberos;
- биометрия;
- идентификационные карты и электронные ключи



Парольная идентификация/аутентификация

- клиент посылает имя и пароль серверу
- сервер сверяет присланный пароль с паролем в своем хранилище



Парольная идентификация/аутентификация

Достоинства:

Простота и привычность

Недостатки:

- может быть перехвачен злоумышленником;
- БД стандартных паролей можно найти в Интернете;
- Программы-взломщики;
- подсмотреть (например, с помощью оптических приборов),
- сообщить другу/подруге (если секрет знают двое – это уже не секрет),
- записать на бумажке и приклеить.

Меры, позволяющие повысить надежность парольной защиты:

- наложение технических ограничений (программы - генераторы паролей (ключей));
- ограничение доступа к файлу с паролями;
- удаление резервных копий файлов с паролями;
- использование защищенных протоколов обмена ключами ;
- ограничение числа неудачных попыток входа в систему;
- управление сроком действия паролей, их периодическая смена, использование сеансовых ключей;
- удаление паролей, уволенных или лишенных полномочий пользователей.

Сеансовый (сессионный) ключ – ключ, используемый абонентами в рамках одного сеанса (сессии, раунда) общения.

- Использование сеансовых ключей позволяет ограничить размер ущерба при компрометации ключа.

Обмен ключами:

- ключ вырабатывается одним из абонентов и высылается второму;
- совместная выработка ключа абонентами;
- ключ вырабатывается и предоставляется абонентам третьей стороной.

Идентификация/аутентификация с использованием хеш-функции.

- Хеш-функция – легко вычислимая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение, фиксированной длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.
- При идентификации/аутентификации пользователь вводит пароль, а по каналу связи высылается его хеш-образ.
- Проверяющая система сравнивает введенный хеш-образ с образом, хранящемся в ИС для этого пользователя и в случае их совпадения разрешает доступ.

Протокол идентификации/аутентификации на основе шифрования с открытым ключом

Протоколы на основе:

- алгоритмов RSA,
- схемы Фейге-Фиата-Шамира,
- Эль-Гамаля,
- Шнорра

Сервер аутентификации Kerberos

- Kerberos – программный продукт, присутствующий во многих ОС.
- Есть открытая сеть и субъекты C и S.
- Каждый субъект обладает секретным ключом.
- Чтобы субъект **C** мог доказать свою подлинность субъекту **S** (без этого **S** не станет обслуживать **C**), он должен не только назвать себя, но и продемонстрировать знание секретного ключа.
- Система Kerberos представляет собой доверенную третью сторону (т.е. сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Протокол Kerberos

Идентификационные карты и электронные ключи

- карты с магнитной полосой;
- контактные смарт-карты и USB-ключи;
- бесконтактные RFID-карты.

Карты с магнитной полосой

	Кодировка символов	Максимальное количество символов	Плотность записи
Дорожка 1	7 бит (буквы, цифры и служебные символы)	79	210 bpi
промежуток			
Дорожка 2	5 бит (цифры и служебные символы)	40	75 bpi
промежуток			
Дорожка 3	5 бит (цифры и служебные символы)	107	210 bpi

1 дорожка была предназначена для банковских карт, и до конца прошлого века большинство карт имело только одну эту дорожку.

2 дорожка задействована для хранения исключительно числовых данных, за счет чего она имеет меньшую длину и меньше шансов повреждения данных.

3 дорожка в банковской сфере не используется и предназначена карт прочих систем (например, дисконтные карты)

- Задача банка, выпустившего карту – это аутентификация карты в ходе ее использования (процесс доказательства того, что данная карта выпущена банком, авторизированным на это соответствующей платежной системой).

Аутентификация карты:

- Чтение данных карты,
- Терминал отправляет их через банк-эквайер и платежную систему банку-эмитенту.
- Эмитент на основании данных карты определяет ее подлинность.

Контактные смарт-карты и USB-ключи

- Смарт-карта - карта со встроенной микросхемой.
- Помимо модуля памяти, содержит микропроцессор и операционную систему.
- Назначение смарт-карт - одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.
- Различают **контактные** и **бесконтактные.**

Информационные объекты, хранящиеся на смарт-карте, используются для обеспечения защиты:

- аутентификация участвующей стороны по паролю (проверка введенного PIN-кода);
- аутентификация участвующей стороны по ключу (аутентификация с использованием шифрования с открытым ключом);
- аутентификация данных (обеспечение целостности хранимых или пересылаемых данных с использованием криптографической контрольной суммы или ЭЦП);
- шифрование данных (обеспечение конфиденциальности хранимых или пересылаемых данных).

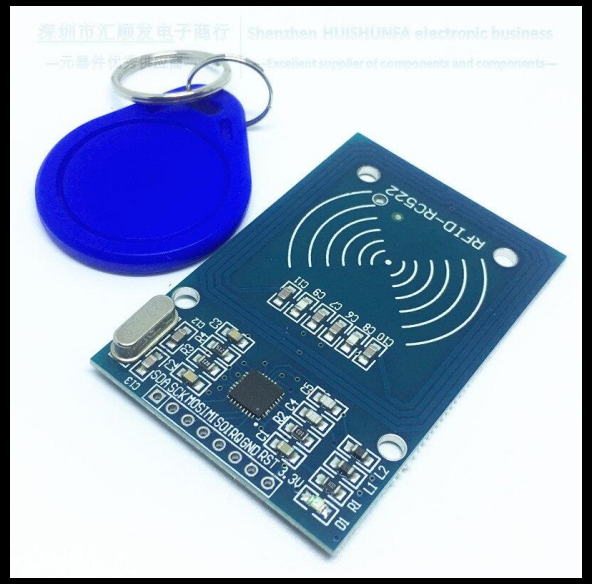
Контактные смарт-карты с USB-интерфейсом

- усовершенствование процесса аутентификации (двухфакторная аутентификация)

- шифрование данных на серверах, ноутбуках и рабочих станциях;
- обеспечение защиты персональных данных;
- защита электронной почты и в системах электронного документооборота;
- безопасность финансовых операций в системах дистанционного банковского обслуживания (ДБО);
- внедрение ЭЦП и заща документов в системах сдачи электронной отчетности через Интернет;
- обеспечение защиты корпоративного сайта в Интернете.

Бесконтактные RFID-карты

- RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) - способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах RFID-метках.



RFID-чип состоит из двух частей:

- микрочип, который хранит и обрабатывает информацию,
- антенна для приема и передачи сигнала.

Тег содержит конкретный уникальный серийный номер для одного конкретного объекта.

На таком чипе может храниться практически любая информация, например, ФИО владельца, время посещения тех или иных заведений или же информация о товаре (размер, цвет, цена) и т.д.

Классификация RFID-систем:

по дальности считывания:

- ближняя идентификация (до 20 см);
- средней дальности (от 20 см до 5 м);
- дальней идентификации (свыше 5 м);

по рабочей частоте:

- - диапазона LF (низкая частота) - 125 .. 134 кГц;
- - диапазона HF (высокая частота) - 13.56 МГц;
- - диапазона UHF (ультравысокая частота) - 860 .. 960 МГц;
- - диапазона SHF (сверхвысокая частота) - 2.4 ГГц;

Классификация RFID-систем:

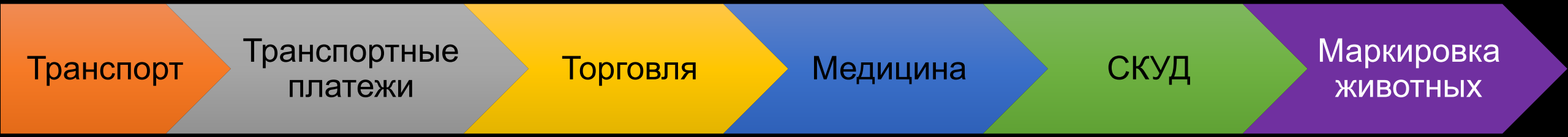
по типу используемой памяти:

- RO (англ. Read Only) - данные записываются только один раз при изготовлении;
- WORM (англ. Write Once Read Many) - содержат идентификатор и блок однократно записываемой памяти;
- RW (англ. Read and Write) - содержат идентификатор и блок многократно перезаписываемой памяти;

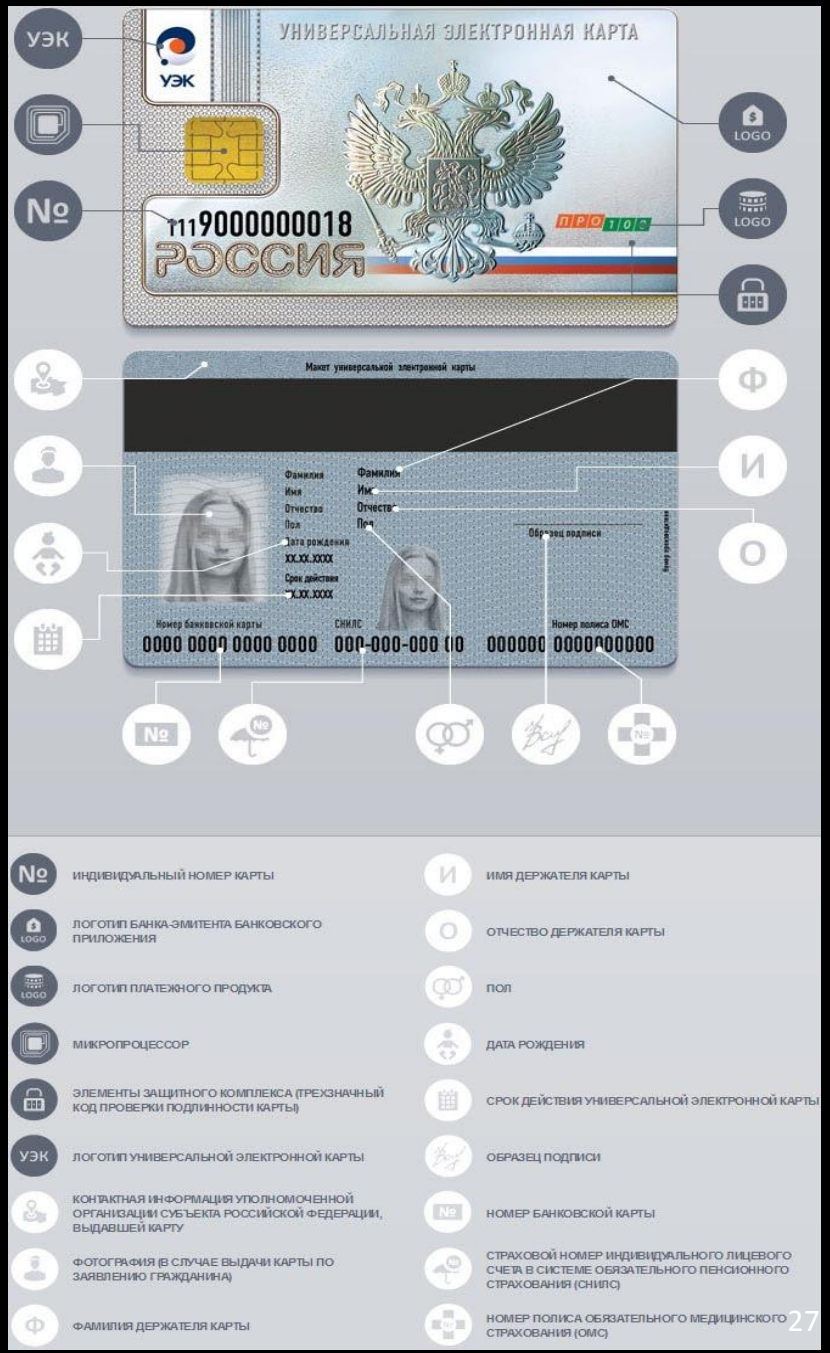
по источнику питания:

- пассивные. Не имеют встроенного источника питания. Дальность действия меток составляет 1-200 см (ВЧ-метки) и 1-10 метров (СВЧ-метки);
- активные. Имеют собственный источник питания. Дальность действия меток до 300 м;
- полупассивные.

Сфера применения



Универсальная электронная карта (УЭК) - российская пластиковая карта, объединяющая в себе идентификационное и платежное средство



Идентификация/аутентификация с помощью биометрических данных

Биометрические характеристики

Статические

- Код ДНК
- Форма кисти руки
- Сетчатка глаза
- Рисунок и форма пальца
- Геометрия или термограмма лица
- Выдыхаемый воздух

Динамические (поведение)

- Голос
- Сердечный ритм
- Роспись
- Походка
- Работа на клавиатуре

Комбинированные

Стандарты на машиносчитываемые проездные документы (МСПД)

определяют три способа биометрической идентификации:

- по изображению лица,
- пальцев
- радужной оболочки глаз.

Биометрический загранпаспорт содержит:

- бесконтактную пассивную карту RFID ближнего радиуса действия (до 10 см), соответствующую типу A или B стандарта ГОСТ Р ИСО/МЭК 14443 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия»).

Данные на карте защищены с помощью технологии контроля доступа BAC (Basic access control), которая позволяет произвести чтение данных только после ввода номера паспорта, даты рождения владельца и даты окончания действия паспорта.