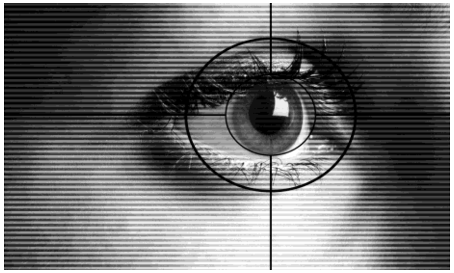
Authentication Technologies

Authentication

- The determination of **identity**, usually based on a combination of
  - –something the person has (like a smart card or a radio key fob storing secret keys),
  - –something the person knows (like a password),
  - –something the person is (like a human with a fingerprint).



Something you are

human with fingers and eyes

Something you have

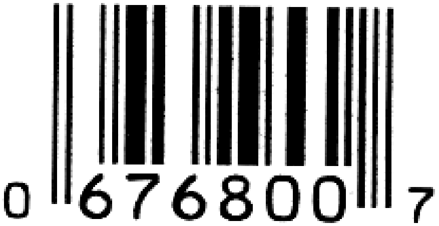
radio token with secret keys

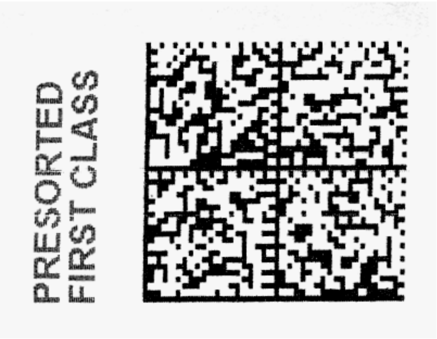
Something you know

password=ucIb()w1V
mother=Jones
pet=Caesar

Barcodes

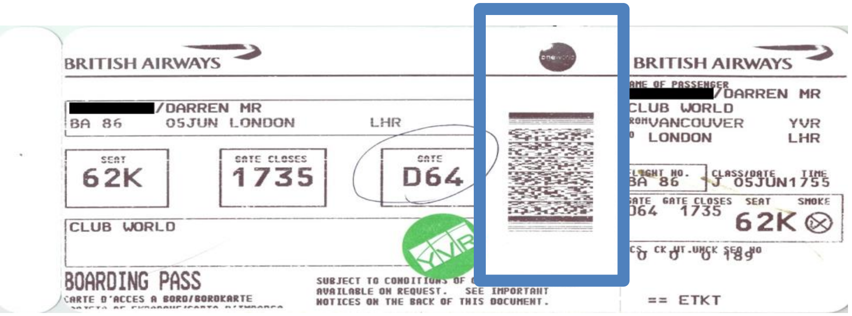
- Developed in the 20th century to improve efficiency in grocery checkout.
- First-generation barcodes represent data as a series of **variable-width, vertical lines** of ink, which is essentially a one-dimensional encoding scheme.
- Some more recent barcodes are rendered as **two-dimensional patterns** using dots, squares, or other symbols that can be read by specialized optical scanners, which translate a specific type of barcode into its encoded information.





Authentication via Barcodes

- Since 2005, the airline industry has been incorporating two-dimensional barcodes into boarding passes, which are created at flight check-in and scanned before boarding.
- In most cases, the barcode is encoded with an internal unique identifier that allows airport security to look up the corresponding passenger's record with that airline.
- Staff then verifies that the boarding pass was in fact purchased in that person's name (using the airline's database), and that the person can provide photo identification.
- In most other applications, however, barcodes provide convenience but not security. Since barcodes are simply images, they are extremely easy to duplicate.



BRITISH AIRWAYS

[redacted]/DARREN MR
BA 86 05JUN LONDON LHR

SEAT 62K
GATE CLOSES 1735
GATE D64

CLUB WORLD

BOARDING PASS
CARTE D'ACCES A BORD/BORDKARTE

SUBJECT TO CONDITIONS OF
AVAILABLE ON REQUEST. SEE IMPORTANT
NOTICES ON THE BACK OF THIS DOCUMENT.

BRITISH AIRWAYS
AME OF PASSENGER
[redacted]/DARREN MR
CLUB WORLD
ROM VANCOUVER YVR
O LONDON LHR

FLIGHT NO. BA 86
CLASS/DATE J 05JUN
TIME 1755
GATE D64
GATE CLOSES 1735
SEAT 62K
SMOKE ⊗
CS CK WT.UNCK SEQ NO
0 0 0 189

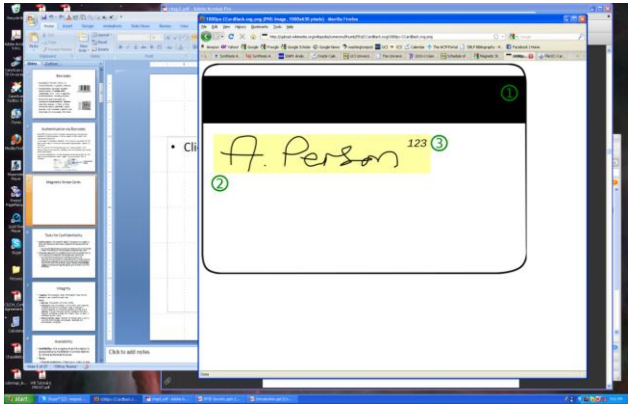
== ETKT

Two-dimensional barcode

Public domain image from http://commons.wikimedia.org/wiki/File:Bpass.jpg

Magnetic Stripe Cards

- Plastic card with a magnetic stripe containing personalized information about the card holder.
- The first track of a magnetic stripe card contains the cardholder’s full name in addition to an account number, format information, and other data.
- The second track may contain the account number, expiration date, information about the issuing bank, data specifying the exact format of the track, and other discretionary data.



Public domain image by *Alexander Jones* from http://commons.wikimedia.org/wiki/File:CCardBack.svg

Mag Stripe Card Security

- One vulnerability of the magnetic stripe medium is that it is easy to read and reproduce.
- Magnetic stripe readers can be purchased at relatively low cost, allowing attackers to read information off cards.
- When coupled with a magnetic stripe writer, which is only a little more expensive, an attacker can easily clone existing cards.
- So, many uses require card holders to enter a PIN to use their cards (e.g., as in ATM and debit cards in the U.S.).

Smart Cards

- **Smart cards** incorporate an integrated circuit, optionally with an on-board microprocessor, which microprocessor features reading and writing capabilities, allowing the data on the card to be both accessed and altered.
- Smart card technology can provide secure authentication mechanisms that protect the information of the owner and are extremely difficult to duplicate.

Circuit interface

Public domain image from http://en.wikipedia.org/wiki/File:Carte_vitale_anonyme.jpg

Smart Card Authentication

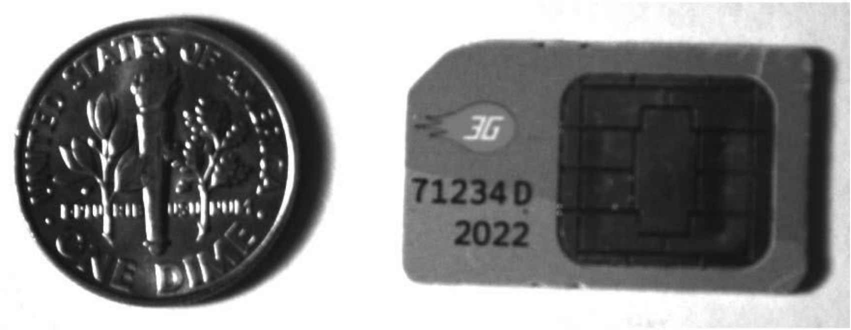
- They are commonly employed by large companies and organizations as a means of strong authentication using cryptography, US government CAC cards, e.g.
- Smart cards may also be used as a sort of “electronic wallet,” containing funds that can be used for a variety of services, including parking fees, public transport, and other small retail transactions.

PCMCIA Card Authentication

- These have active circuits powered when plugged into a computer or PCMCIA card reader
- Often these have cryptographic algorithms and keys stored on them, which can only be accessed through a limited interface
- Example: Fortezza cards with public key certificates and private key(s) encrypted with Skipjack

SIM Cards

- Many mobile phones use a special smart card called a **subscriber identity module card (SIM card).**
- A SIM card is issued by a network provider. It maintains personal and contact information for a user and allows the user to authenticate to the cellular network of the provider.



SIM Card Security(1)

- SIM cards contain several pieces of information that are used to identify the owner and authenticate to the appropriate cell network.
- Each SIM card corresponds to a record in the database of subscribers maintained by the network provider.
- A SIM card features an **integrated circuit card ID (ICCID),**
- which is a unique 18-digit number used for hardware identification.

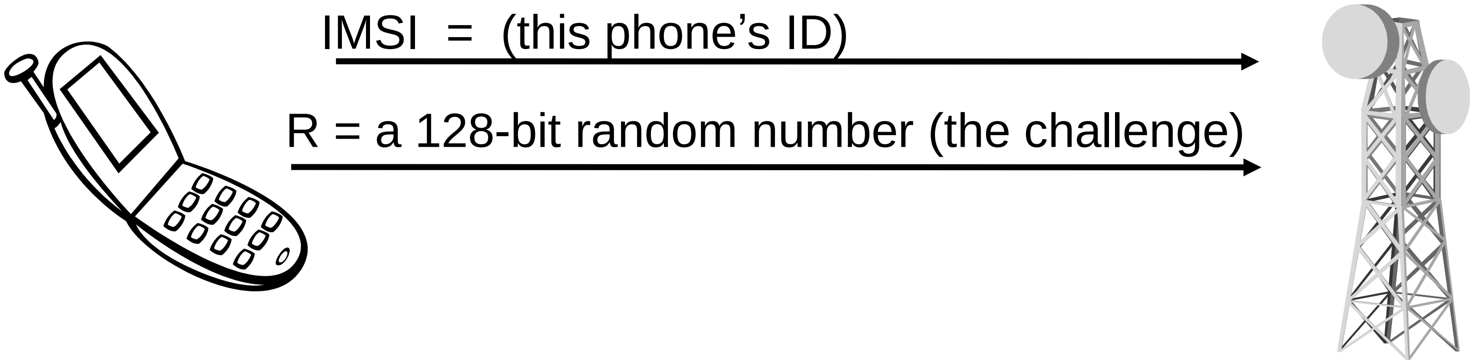
SIM Card Security (2)

- Next, a SIM card contains a unique **international mobile subscriber identity** (**IMSI),** which identifies the owner’s country, network, and personal identity.
- SIM cards also contain a 128-bit **secret key.** This key is used for authenticating a phone to a mobile network.
- As an additional security mechanism, many SIM cards require a PIN before allowing any access to information on the card.

GSM Challenge-Response Protocol

1.When a cellphone wishes to join a cellular network it connects to a local **base station** owned by the network provider and transmits its IMSI.

2.If the IMSI matches a subscriber’s record in the network provider’s database, the base station transmits a 128-bit random number to the cellphone.



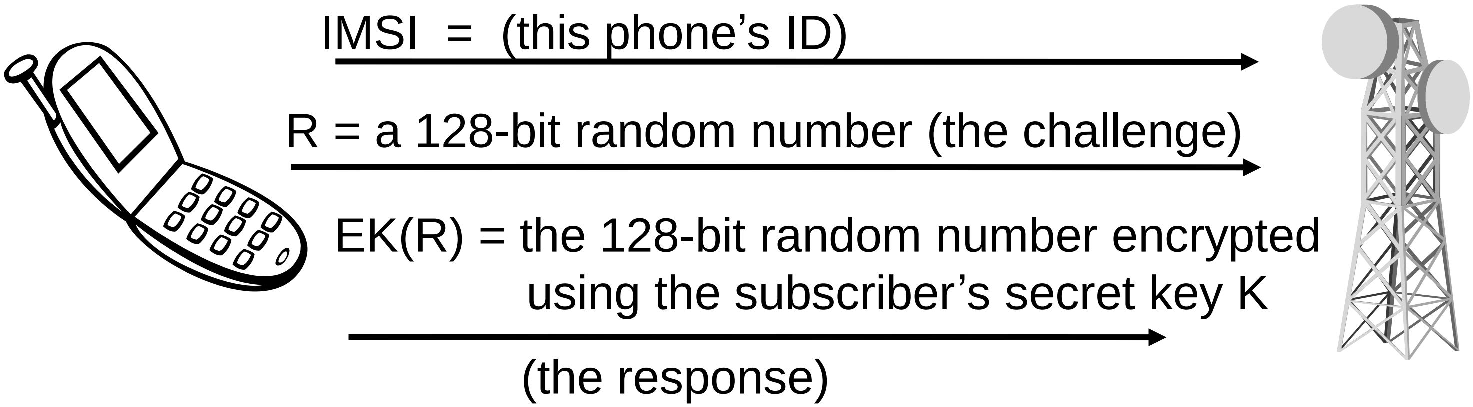
IMSI = (this phone’s ID)

R = a 128-bit random number (the challenge)

GSM Challenge-Response Protocol

1.This random number is then encoded by the cellphone with the subscriber’s secret key stored in the SIM card using a proprietary encryption algorithm known as **A3,** resulting in a ciphertext sent back to the base station.

2.The base station then performs the same computation, using its stored value for the subscriber’s secret key. If the two ciphertexts match, the cellphone is authenticated to the network and is allowed to make and receive calls.



IMSI = (this phone’s ID)

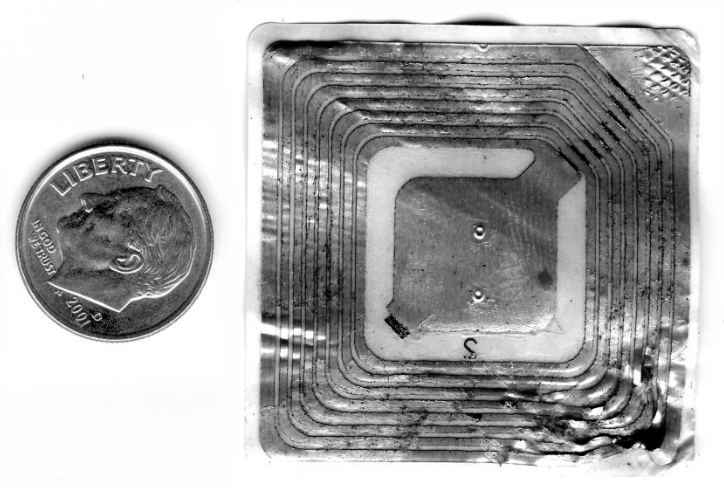
R = a 128-bit random number (the challenge)

EK(R) = the 128-bit random number encrypted using the subscriber’s secret key K

(the response)

RFIDs

- **Radio frequency identification, or RFID,** is a rapidly emerging technology that relies on small transponders to transmit identification information via radio waves.
- RFID chips feature an integrated circuit for storing information, and a coiled antenna to transmit and receive a radio signal.



RFID Technology

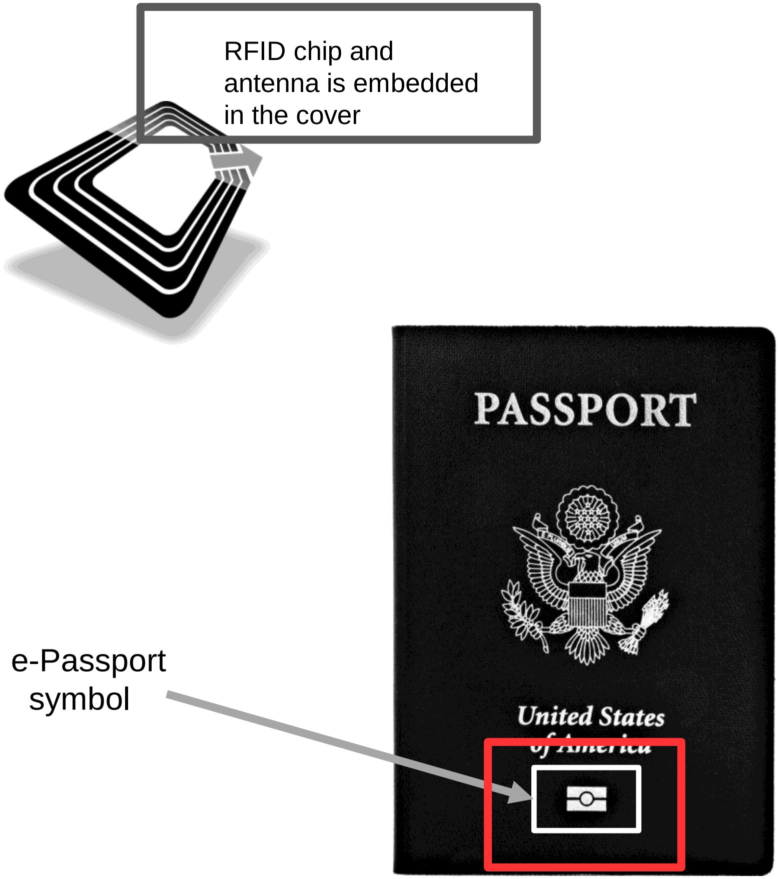
- RFID tags must be used in conjunction with a separate reader or writer.
- While some RFID tags require a battery, many are passive and do not.
- The effective range of RFID varies from a few centimeters to several meters, but in most cases, since data is transmitted via radio waves, it is not necessary for a tag to be in the line of sight of the reader.

RFID Technology

- This technology is being deployed in a wide variety of applications.
- Many vendors are incorporating RFID for consumer-product tracking.
- Car key fobs.
- Electronic toll transponders.
- Logistics tracking.

Passports

- Modern passports of several countries, including the United States, feature an embedded RFID chip that contains information about the owner, including a digital facial photograph that allows airport officials to compare the passport's owner to the person who is carrying the passport.



RFID chip and antenna is embedded in the cover

e-Passport symbol

Passport Security

- All RFID communications encrypted with a **secret key.**
- Often secret key is passport number, holder’s date of birth, and expiration date, in that order.
  - All of this information is printed on the card, either in text or using a barcode etc.
  - While this secret key is intended to be only accessible to those with physical access to the passport, an attacker with information on the owner, including when their passport was issued, may be able to easily reconstruct this key, especially since passport numbers are typically issued sequentially.

Biometrics

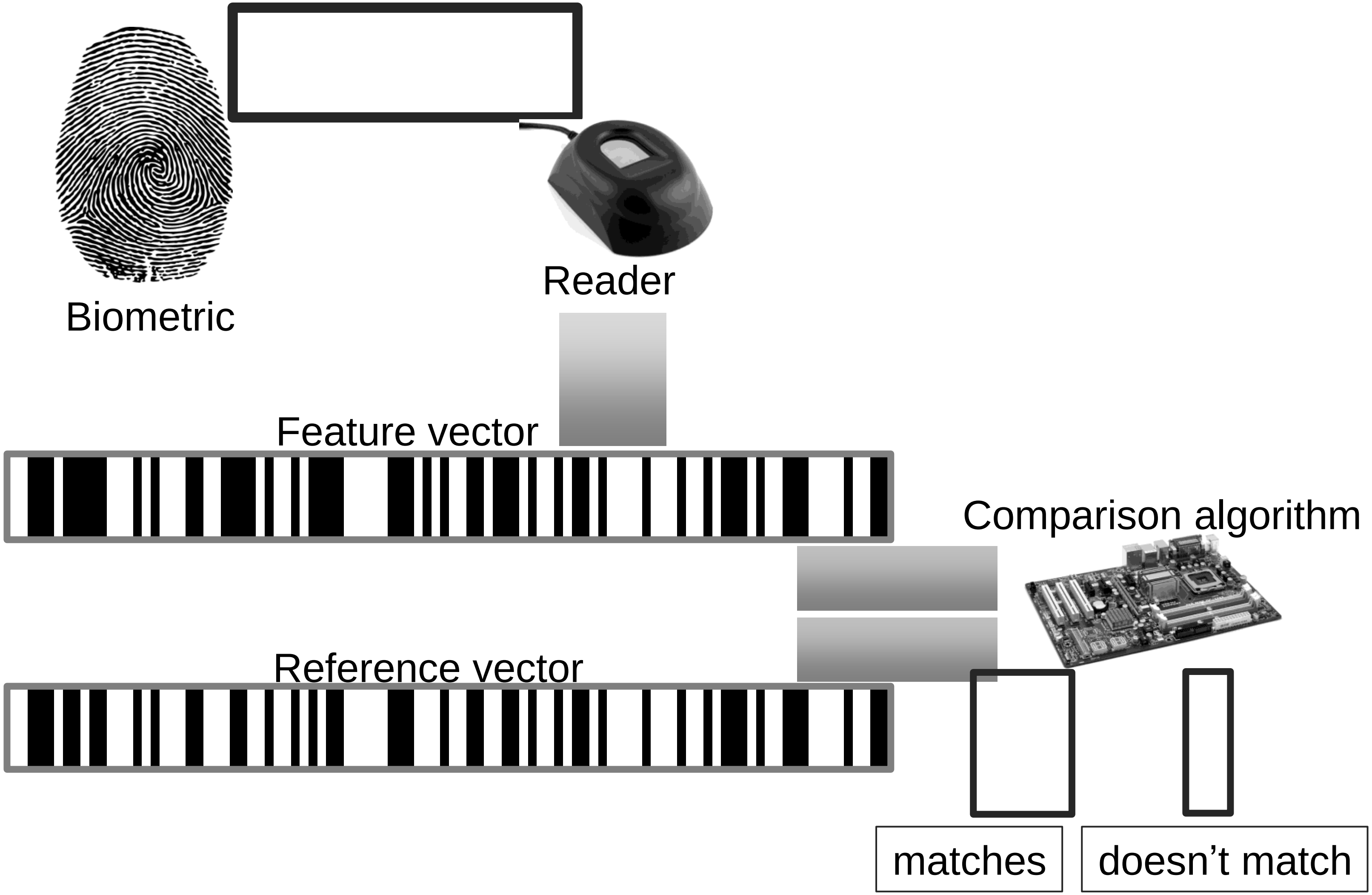
- **Biometric** refers to any measure used to uniquely identify a person based on biological or physiological traits.
- Generally, biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before granting access.

Image from http://commons.wikimedia.org/wiki/File:Fingerprint_scanner_in_Tel_Aviv.jpg used with permission under the Creative Commons Attribution 3.0 Unported license

Requirements for Biometric Identification

- **Universality.** Almost every person should have this characteristic.
- **Distinctiveness.** Each person should have noticeable differences in the characteristic.
- **Permanence.** The characteristic should not change significantly over time.
- **Collectability.** The characteristic should have the ability to be effectively determined and quantified.

Biometric Identification



Biometric

Reader

Feature vector

Comparison algorithm

Reference vector

matches

doesn’t match

Candidates for Biometric IDs

- Fingerprints
- Retinal/iris scans
- DNA
- “Blue-ink” signature
- Voice recognition
- Face recognition
- Gait recognition
- Let us consider how each of these scores in terms of universality, distinctiveness, permanence, and collectability…

Public domain image from
http://commons.wikimedia.org/wiki/File:Fingerprint_Arch.jpg

Public domain image from
s.jpg

Public domain image from
http://commons.wikimedia.org/wiki/File:CBP_chemist_reads_a_DNA_profile.jpg