

BIOMETRICS : The Good, the Bad and the Ugly

LIMOS / 04 Mars 2020 13h30-15h30

AGENDA

- **Introduction**
  - Fundamental principle
- **The Good: it works!**
  - The biometric market : notebook, smartphone, governmental, payment…
  - Standards : governmental, industrial
  - Some modalities : fingerprint, face, eye, hand…
- **The Bad: it doesn't always work…**
  - Accuracy : definition, threshold, testing
  - Security : aliveness detection, cryptography
- **& The Ugly:**
  - Privacy

INTRODUCTION TO BIOMETRICS

WHAT IS “BIOMETRICS”?

- **The automated recognition of individuals based on their biological and behavioral characteristics**

INTRODUCTION TO BIOMETRICS

BIOMETRIC CHARACTERISTICS

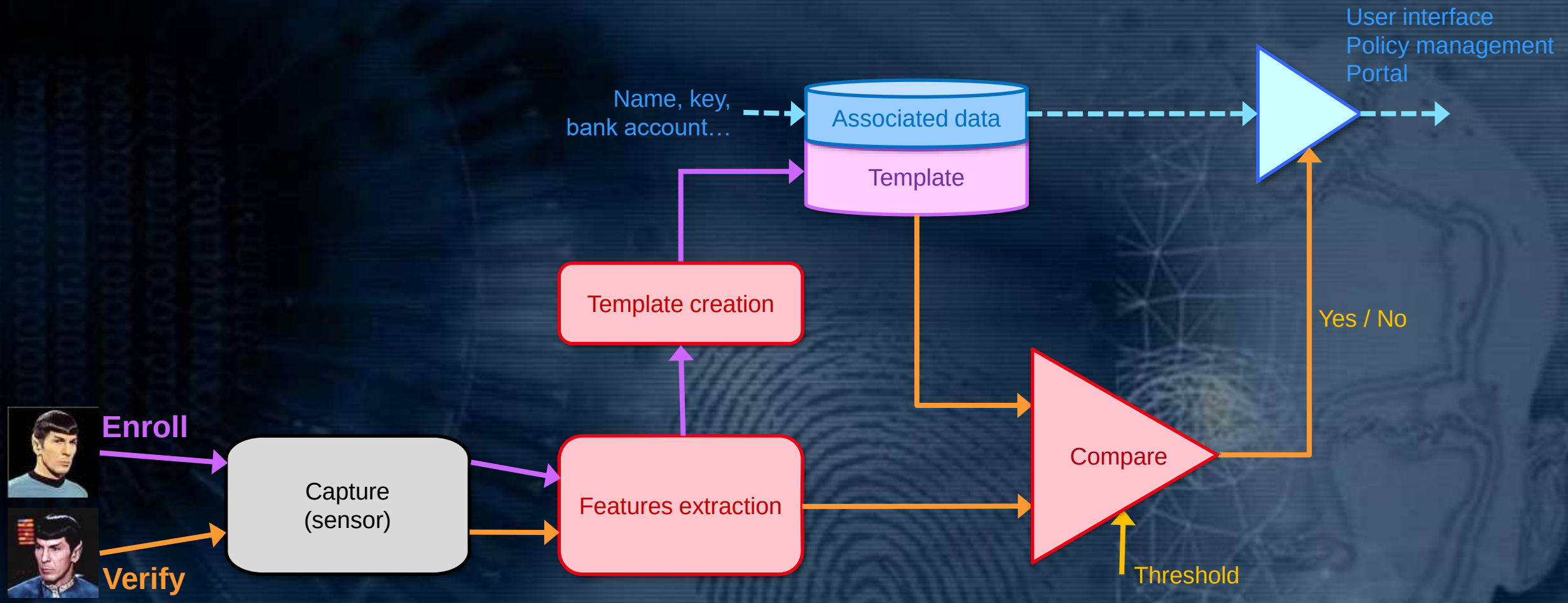
BIOLOGICAL

- Eye (iris, retina)
- Finger (print, geometry, nail)
- Hand (geometry, knuckle, palm, vein)
- Face (2D, 3D, visible, IR)
- Voice
- Retina
- DNA
- Miscellaneous: odor, earlobe, sweat pore, lips…

BEHAVIORAL

- Signature
- Keystroke
- Voice
- Gait

INTRODUCTION TO BIOMETRICS
CONCEPTUAL DIAGRAM OF A GENERAL BIOMETRIC SYSTEM



INTRODUCTION TO BIOMETRICS
BIOMETRIC PROCESSES

- **Enrollment**
  - User features extracted and stored in database
- **Verification (1 to 1)**
  - Are you who you say you are?
  - User features compared to template in database for claimed identity (only)
- **Identification (1 to n)**
  - Are you in my database? If so, who are you?
  - User features compared to multiple templates in database

INTRODUCTION TO BIOMETRICS
DESIRABLE QUALITIES OF BIOMETRIC FEATURES

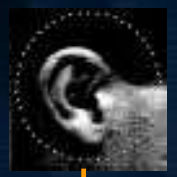
- **Robust**
  - Stable and repeatable, time-invariant
  - Difficult to spoof
- **Distinctive**
  - “Unique” amongst a population
- **Accessible – easy to use**
- **Acceptable – non-intrusive**

BIOMETRIC MODALITIES

DNA

keystroke dynamics

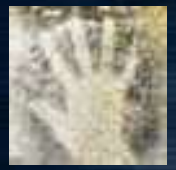
skin spectrum



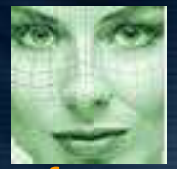
ear shape
ear canal

dental

hand
finger
geometry



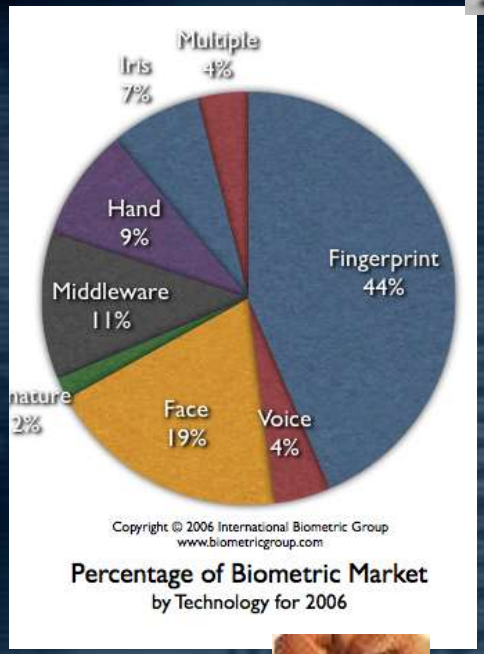
signature

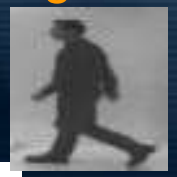


face

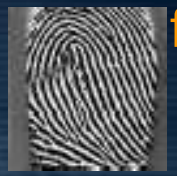
iris

retina



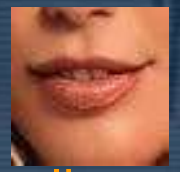


gait

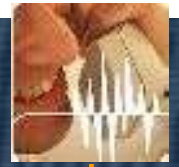


fingerprint
palmprint
pores

vein

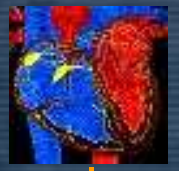


lips



voice

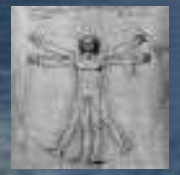
fingernail



pulse

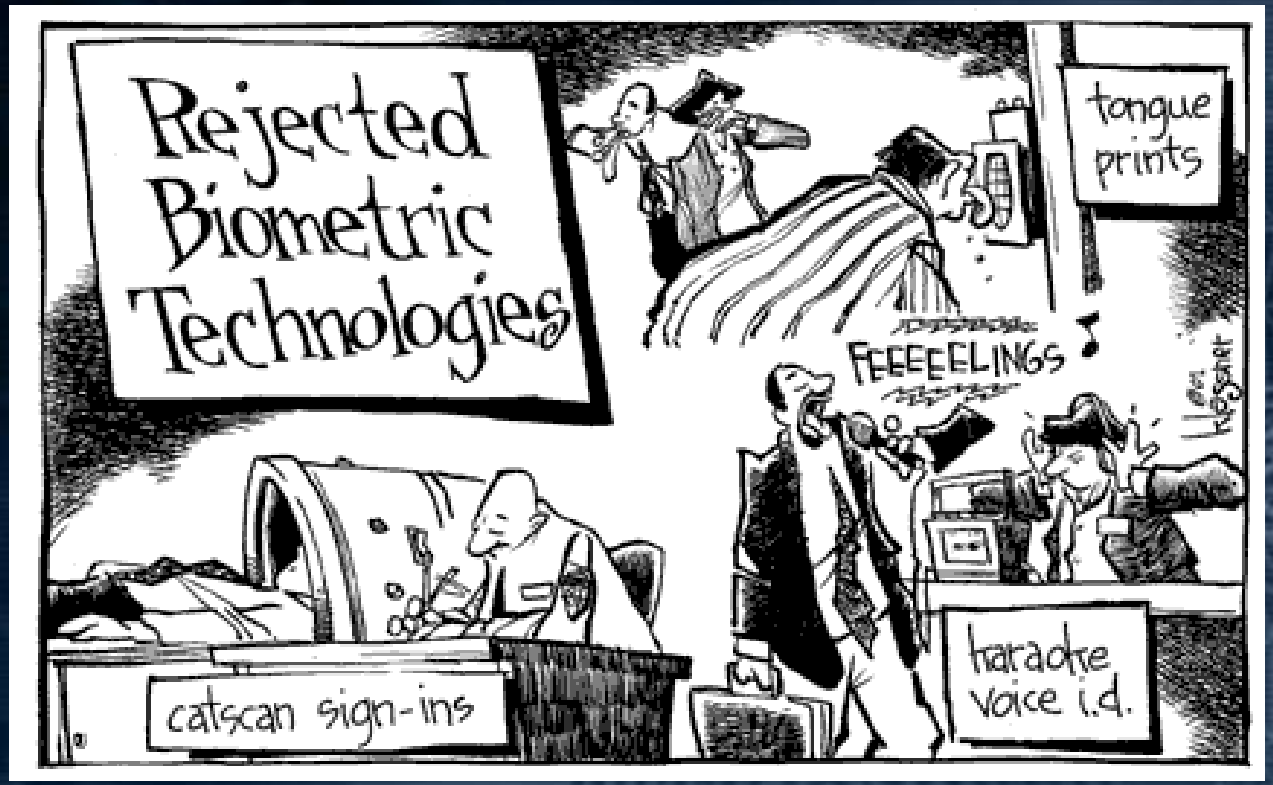
mouse
dynamics

tapping



odor
head resonance
knuckle creases
finger wrinkles
bioelectric field
Skin impedance
Hand pressure profile
Bone sound transmission
Eye movement tracking
Dynamic Grip Recognition
Corneal surface topography
3D Finger surface
EEG, Frontal Sinus
Nose, Butt
Skull sound,
Androgenic hair, …

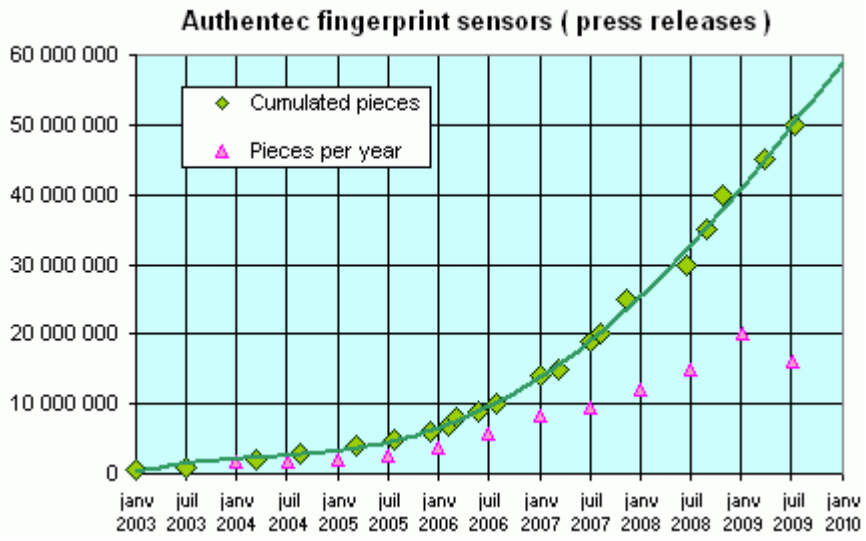
MODALITIES

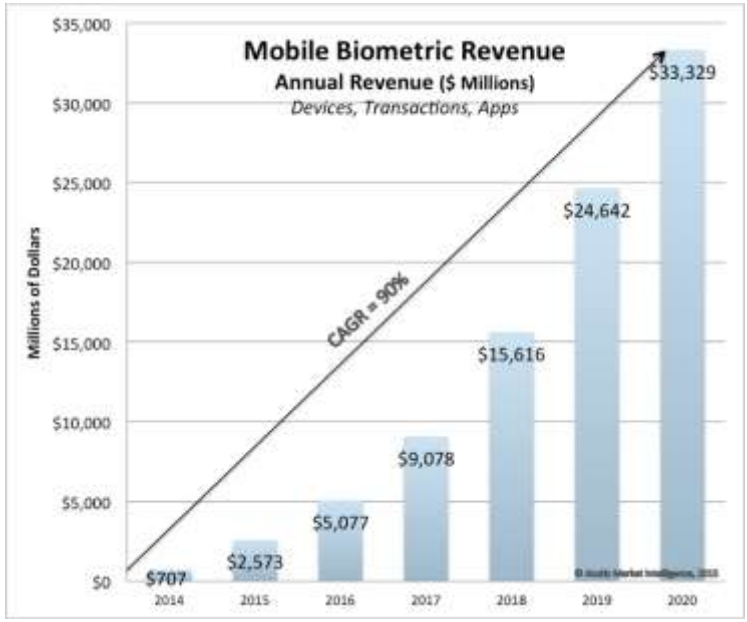

Rejected Biometric Technologies
tongue prints
FEEEEELINGS
catscan sign-ins
haraohre voice i.d.

THE GOOD : IT WORKS!

- **Many successful applications to date**
  - Commercial
  - Government
  - Civil

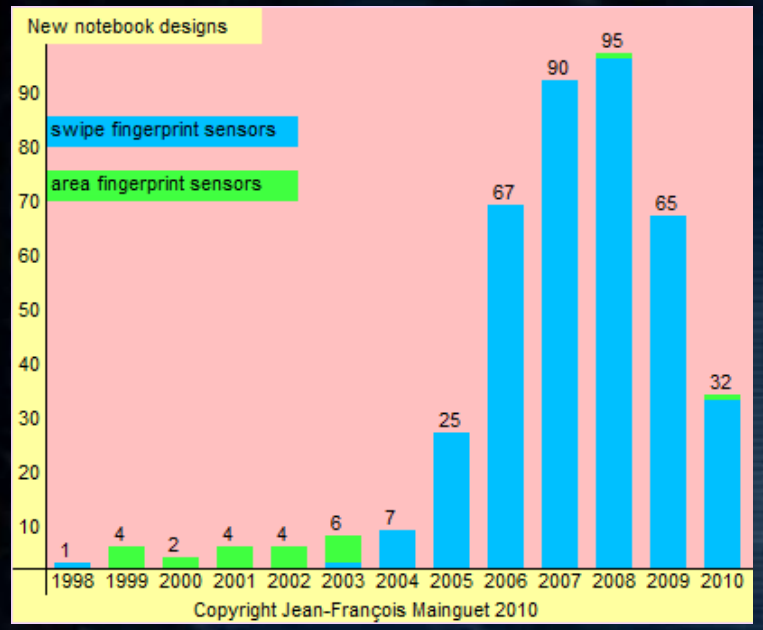
THE GOOD : IT WORKS!
THE BIOMETRIC MARKET

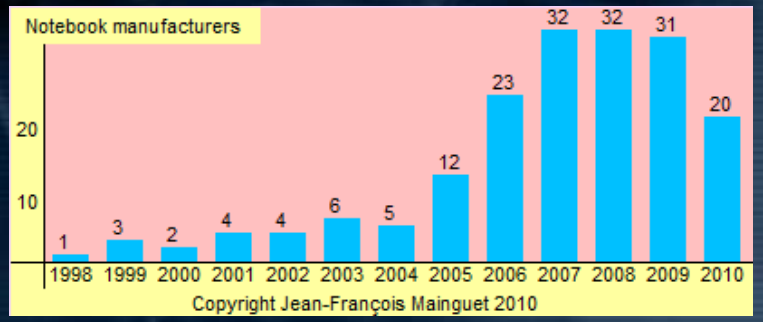




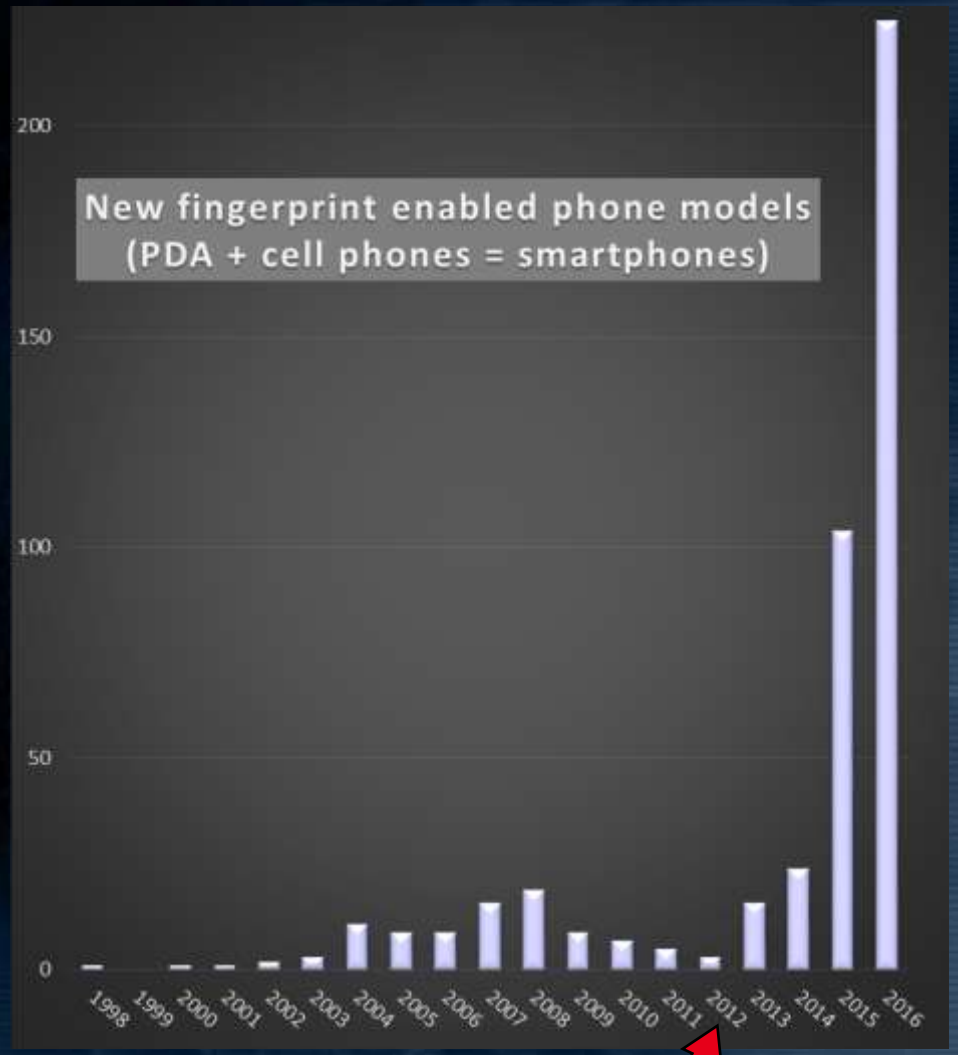
THE GOOD : IT WORKS!
THE FIRST REVOLUTION

NOTEBOOK COMPUTERS





THE GOOD : IT WORKS!
THE SECOND REVOLUTION



July 2012:
Apple buys
Authentec

THE GOOD : IT WORKS!
APPLICATIONS

Desktop phones 2005

Watch 2001

Pen 2004

Hard Drive 2002

Printer 2006

USB flash disks 2002

Mouse 1999

Keyboard 1999

THE GOOD : IT WORKS!
APPLICATIONS PHYSICAL STORAGE

Safe 2002

Key bank 2007

Fridge

Briefcase 2004

Locker 2004

Padlock 2005

Portable safe

THE GOOD : IT WORKS!
APPLICATIONS ACCESS CONTROL

Door lock 2004

Elevator 2004

Garage 2007

Turnstile

Airline check-in 2006

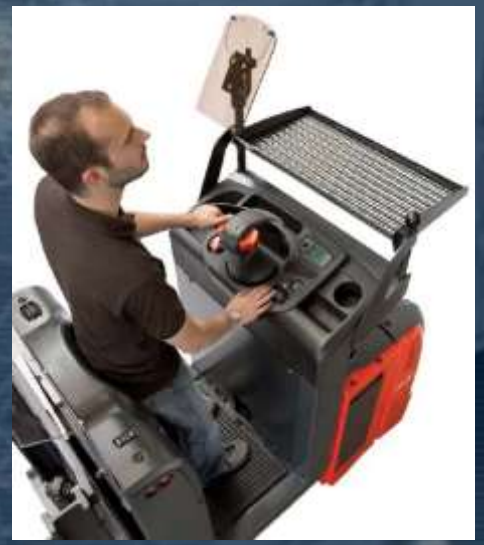
THE GOOD : IT WORKS!
APPLICATIONS VEHICLE

Bike 2001

Boat 2009

Car, truck 1999

Lift truck 2006



THE GOOD : IT WORKS!
APPLICATIONS SERVICES

Remote control 2008

Washing machine 2005
(your turn)

Coffee 2010

Cloakroom 2008

Lighter 2016

Thermostat 2005

THE GOOD : IT WORKS!
APPLICATIONS PERSONEL MANAGEMENT

Time attendance

Driving school

Night-Club Access

THE GOOD : IT WORKS!
APPLICATIONS

Kindergarten

School lunch
School bus

School exams 2007

Library

THE GOOD : IT WORKS!
APPLICATIONS GUN

THE GOOD : IT WORKS!
APPLICATIONS ELECTRIC SWITCH

INDUSTRY

THE GOOD : IT WORKS!
APPLICATIONS MEDICAL

Drug dispenser 2008

Marijuana vending machine 2008

Medical slate 2007

THE GOOD : IT WORKS!
APPLICATIONS MONEY

ATM

→ Integrated in the smart card?

WiFi casino

Set top box (movies) 2013

Vending machines

THE GOOD : IT WORKS!
APPLICATIONS

E-PAYMENT

- **Paying with your finger:**
  - Shopping
  - At home
  - With your cell phone …
- **US: Pay-By-Touch: 3 million enrollees Oct 2006 : died**
- **Shanghai : started October 2007**

- **Apple Pay (2014, iPhone 6)**
- **PayPal / Samsung**
- **Alibaba (80% of e-commerce in China) / Alipay : started 2015**

THE GOOD : IT WORKS!
APPLICATIONS

SEASON TICKET HOLDERS, AIRPORT

DisneyWorld (Florida)
Two-finger geometry (circa 2000)
replaced by fingerprints in 2006

Busch Gardens
(Tampa, Florida)
Hand geometry

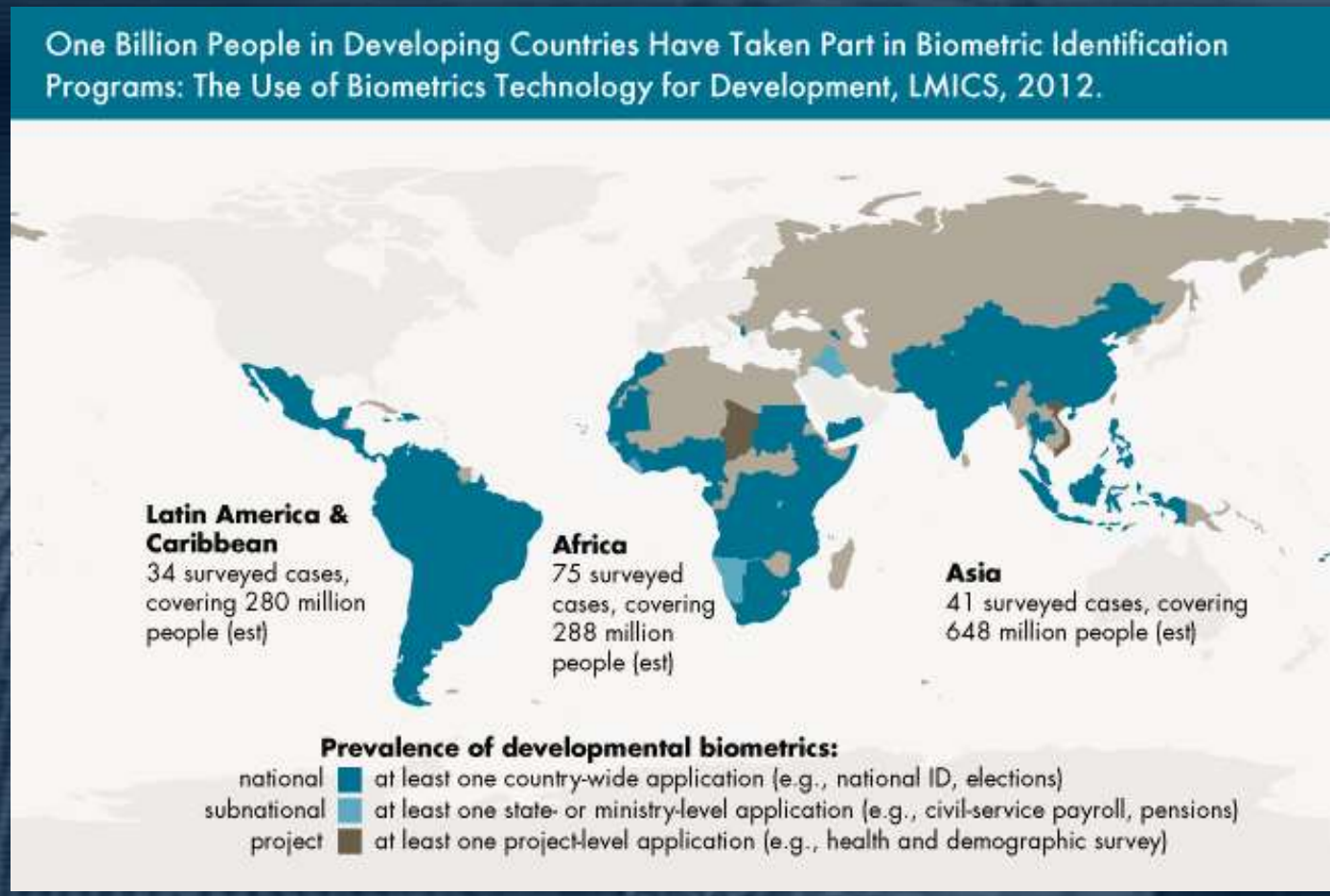
Privium
Schipol airport

Hanover Zoo (Germany)
Facial recognition
(camera behind mirror)
Works better for children
than fingerprint

THE GOOD : IT WORKS!
APPLICATIONS

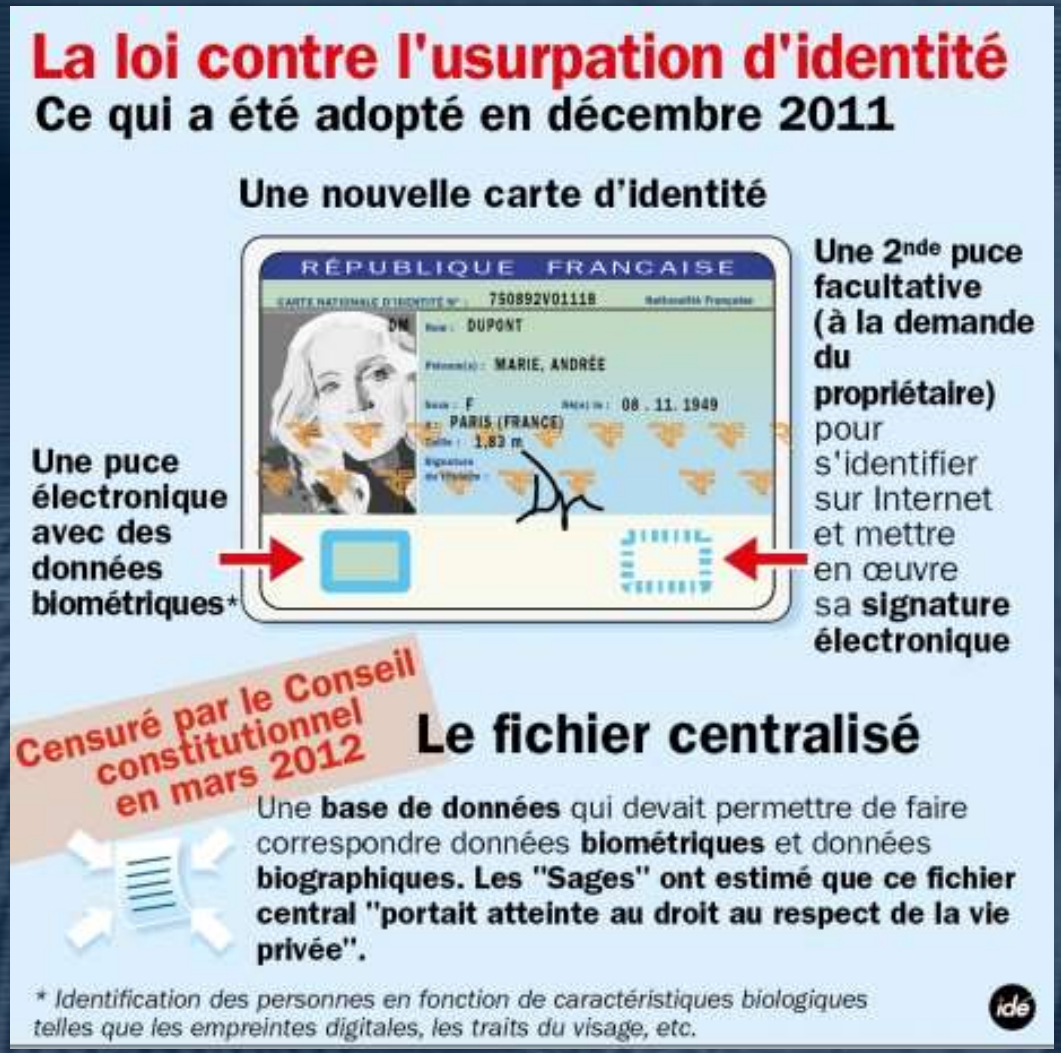
GOVERNMENTAL APPLICATIONS

India is enrolling the full population (fingerprint, iris, face):
1 billion in 2016



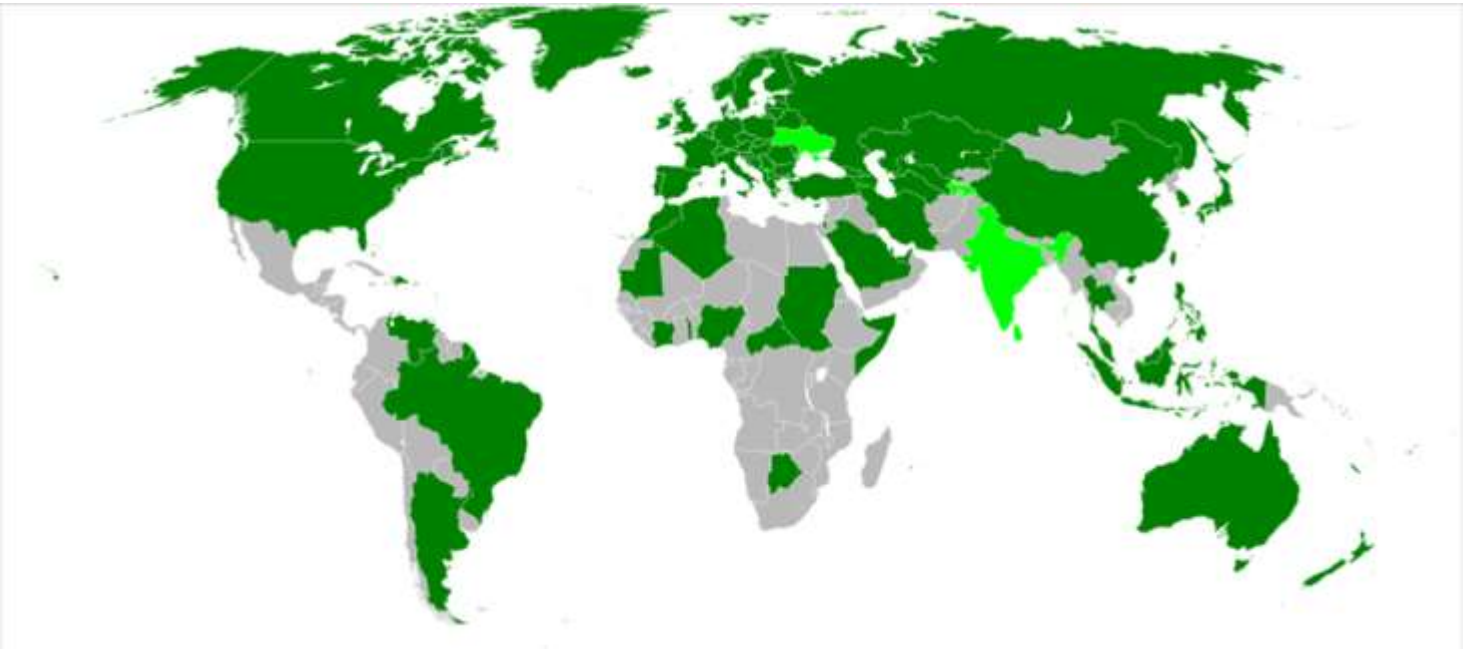
THE GOOD : IT WORKS! APPLICATIONS

NATIONAL SCALE DEPLOYMENTS



E-PASSPORTS

- Needs for more secured travel documents
- Contactless smart card chip inside the passport containing a copy of the written data
- Requested by USA, standards from the ICAO
- Today: face, future: fingerprint, iris



▶ The contactless chip can be integrated into either the cover page or the data page.

THE GOOD : IT WORKS!
APPLICATIONS

IMMIGRATION

- **Biometric data collected from travelers**
  - When they apply for a visa
  - When they arrive for entry
- **OBIM / US Visit: as of**
  - As of February 2007:
    - Over 76 million visitors processed at US air, sea and land ports of entry
    - Over 1,762 known criminals and immigrant violators intercepted
  - 2010: IDENT contains 108 millions subjects
  - 2012: 825000 entries from 375000 individuals: 0.2% of the IDENT database.
- **Fingerprint collection started in Japan in November 2007**
- **Eurodac**
  - Centralized fingerprint database for asylum seekers

Hong-Kong immigration control
(Lok Ma Chau border control)

THE GOOD : IT WORKS!
APPLICATIONS

LAW ENFORCEMENT, MILITARY

- **Biometric databases:**
  - USA / FBI: IAFIS, now NGI
    fingerprint: 77 million records (2014)
    criminals: 2 hours, civil: 24 hours
  - Australia NAFIS (Crimtrac 2013)
    6.3M fingerprints / 3.7M individuals
    837000 DNA records
  - UK: 5.5M fingerprints, 3.4M DNA
  - France: FAED 4.8M fingerprint individuals, 2.5M DNA
  - Interpol: 189k fingerprints, 140k DNA from 69 countries (2013)

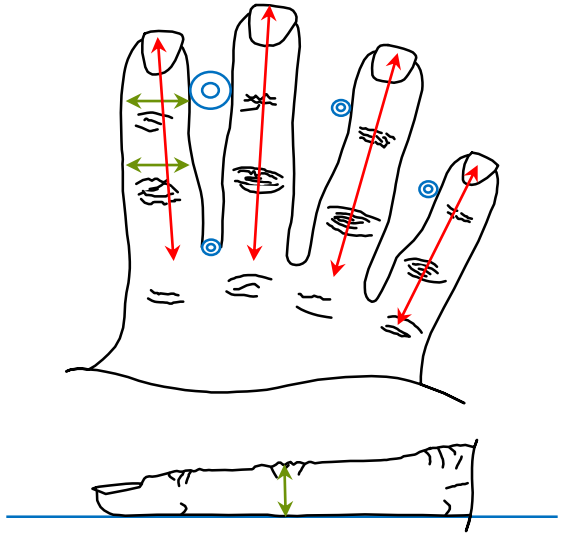
- **More and more US counties are buying biometric material for law enforcement**

THE GOOD : IT WORKS!

- **Focus on some modalities**
  - Hand (oldest automated biometric modality)
  - Face
  - Iris
  - Fingerprint

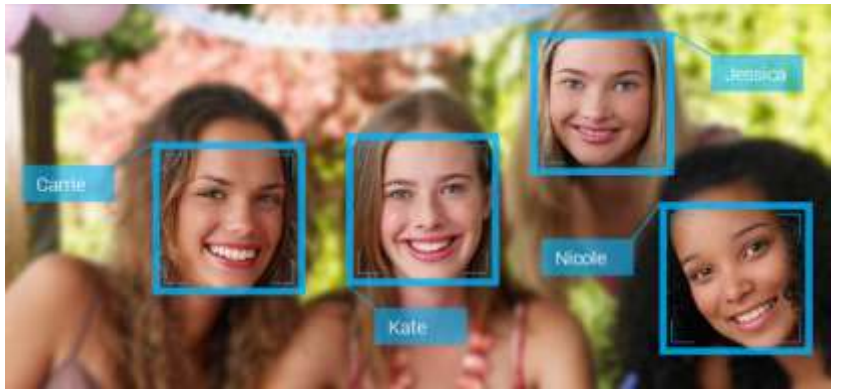
HAND GEOMETRY BASICS

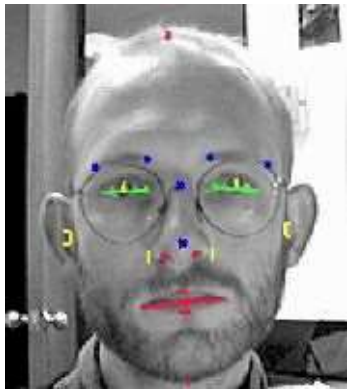
- Camera captures top and side view image of hand
- Geometrical characteristics of hand silhouette stored in a 9-byte template
- Oldest automated biometric modality



FACE RECOGNITION BASICS

- **Based on geometrical characteristics of the face**
- **Many 2D, 3D, visible, infrared products available**
- **Many different types of recognition algorithms**
  - Local Feature Analysis
  - Eigenface or Principal Component Analysis
  - 3D Morphable Models
  - 2D/3D, etc.
- **Pose, expression, lighting, background**
  - generally a challenge
- **Standards help enhance recognition results**

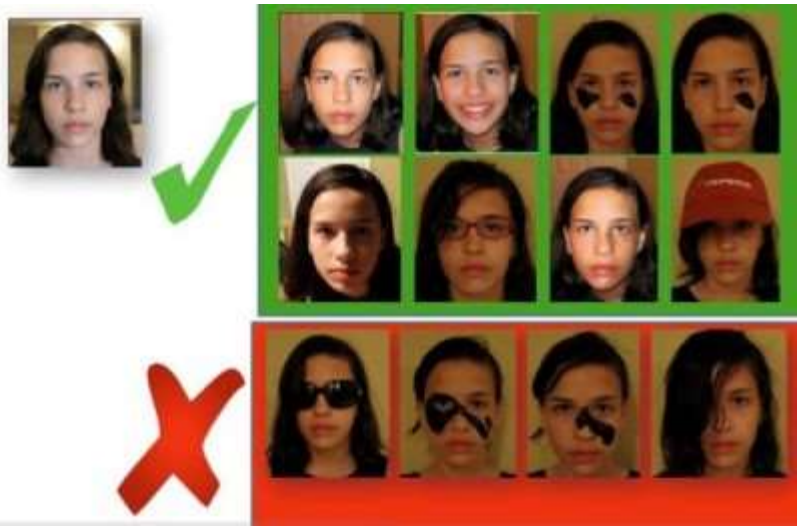


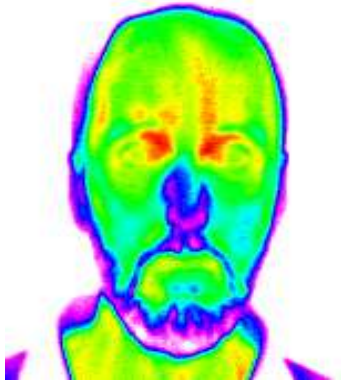


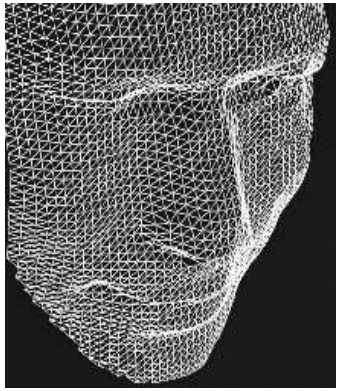
(a) Jennifer Grey

(b) pose (c) illumination (d) expression

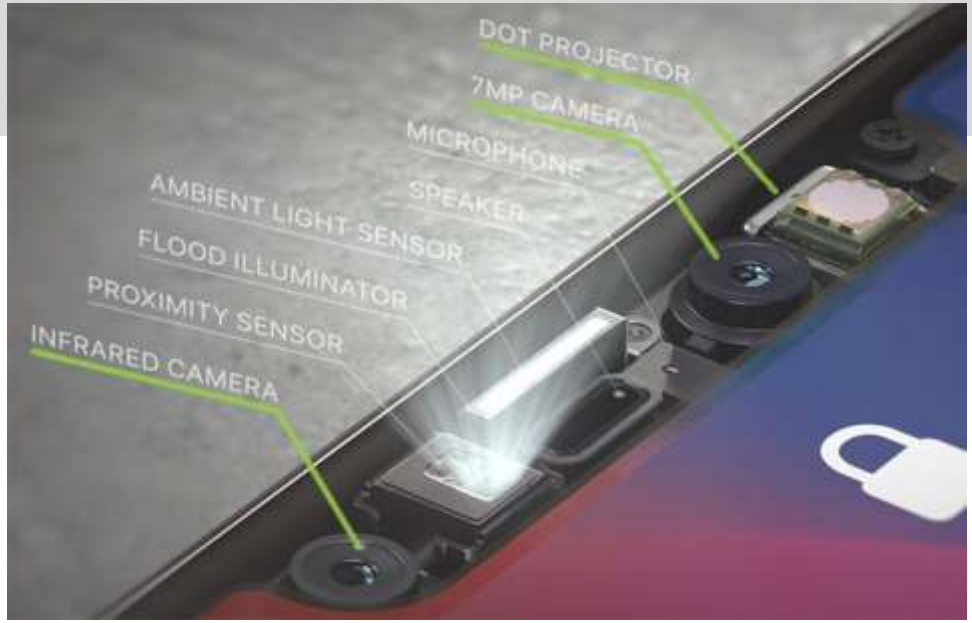
(e) plastic surgery (f) aging (g) makeup







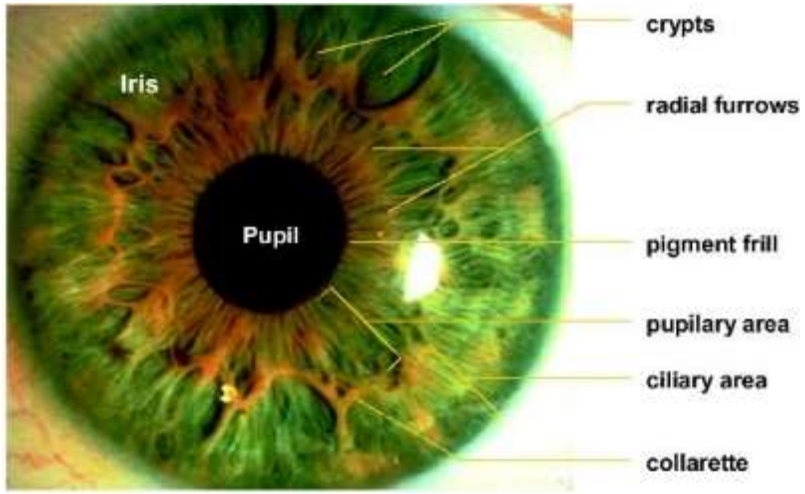
FACE RECOGNITION & SMARTPHONES + 3D

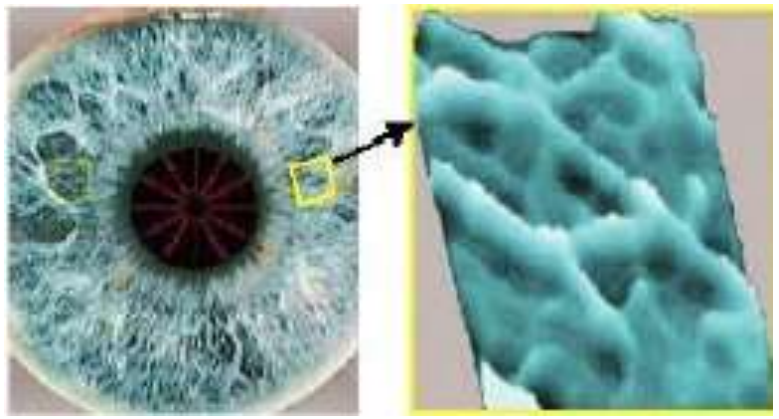


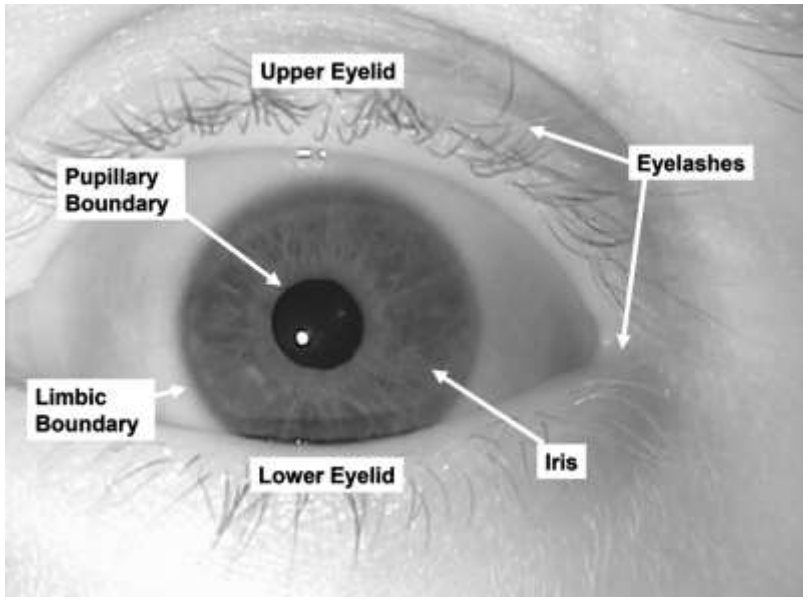
- **iPhone X (2017), XS (2018)… now with « Face ID »**
- **New:**
  - Fully & only near infrared
  - 3D recognition
  - Announced as 1/1’000’000 accuracy
- **Followers:**
  - Xiaomi
  - Oppo
  - Vivo
  - Huawei Mate 20 Pro (nov 2018)
  - Qualcomm + AMS
  - Google Pixel 4

IRIS RECOGNITION BASICS

- **Iris images captured in the near infrared bandwidth**
- **Iris "structure" recognized**
  - Iris color is not used
- **Do not confuse with:**
  - Retina, eye vein, corneal topography, periocular (facial area next to the eye)

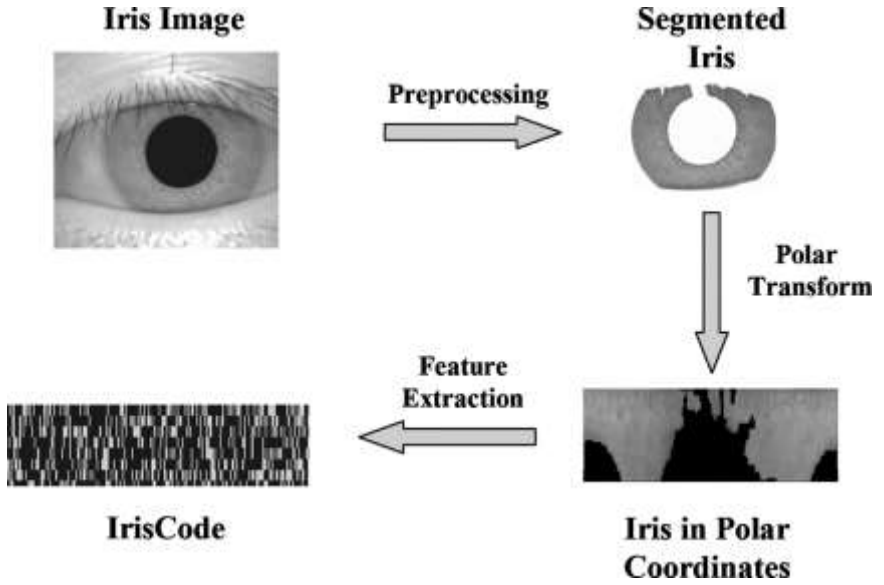


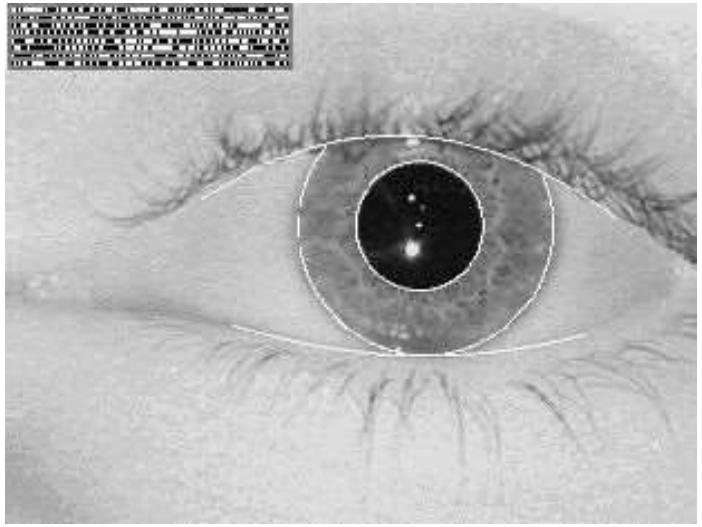




IRIS RECOGNITION BASICS

- **Most systems use Prof. John Daugman's recognition algorithm**
  - The iris structure is encoded in an "Iriscode"
  - Very good algorithm performance
- **Acquisition is a problem**
  - Capturing a moving target not easy
  - Focus and reflections are a challenge
  - Dark iris localization is difficult
  - Obscured by eyelashes, reflection, lenses





IRIS RECOGNITION BASICS

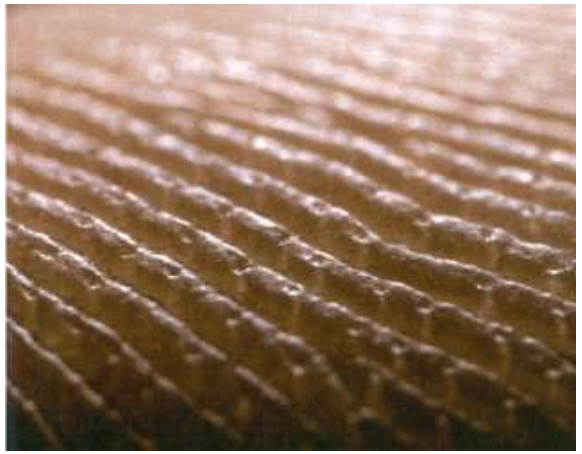
- Many products on the market
- “Iris on the move”

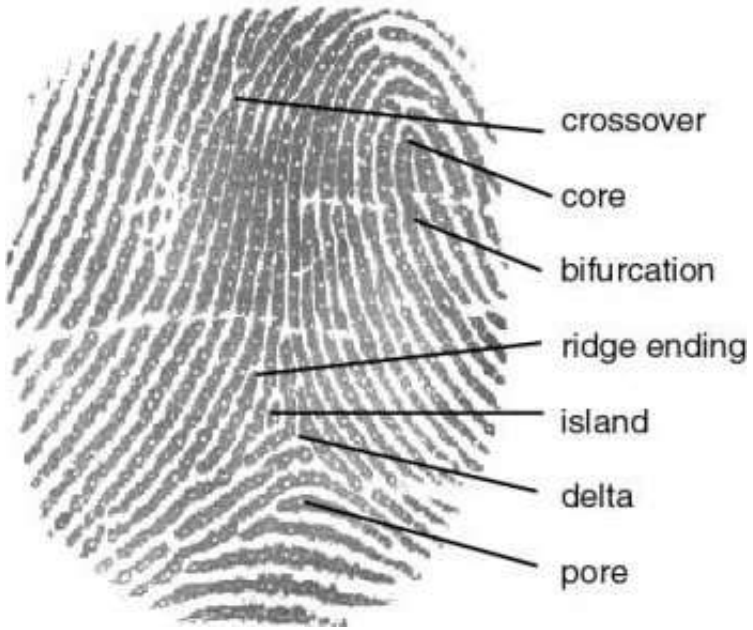
FINGERPRINT BASICS

- **What is a fingerprint?**
- **Types of capture**
- **Types of fingerprint sensors**
  - Optical
  - Electro-optical
  - Capacitive / RF
  - Pressure
  - Thermal
  - Ultrasonic
- **Algorithm basics**

FINGERPRINT BASICS
WHAT IS A FINGERPRINT?

FINGERPRINT BASICS
WHAT IS A FINGERPRINT?

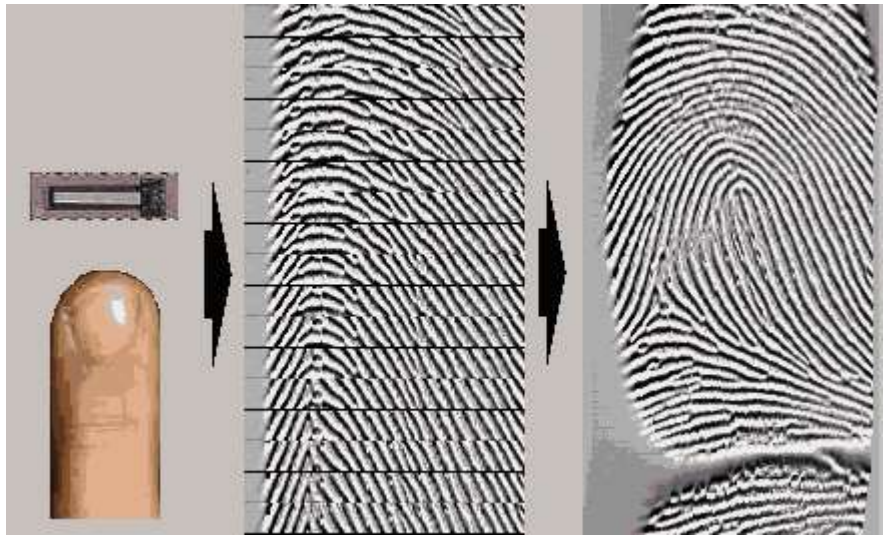




- **Skin on finger consists of friction ridges with pores (sweat glands)**
- **Ridge discontinuities are minutiae points**

FINGERPRINT BASICS
TYPE OF CAPTURE

- **Static: the user just touches the sensing area**
- **Sweep: the user sweeps their finger across the sensing area**
  - Advantage for silicon sensors: less area = less expensive



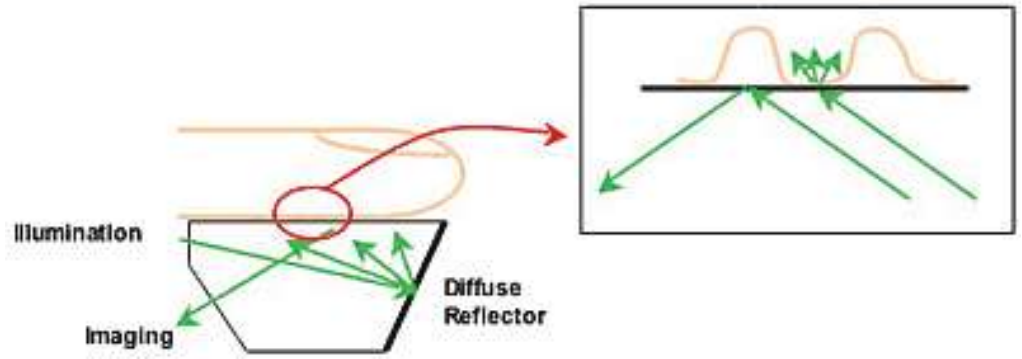
FINGERPRINT BASICS
TYPES OF FINGERPRINT SENSORS

- **Optical**
  - Reflection FTIR
  - Direct image
    - Structured light
    - Pinhole
  - Transmission
  - OCT
- **Electro-Optical**
  - Piezo-led
  - Emissive polymer
- **Ultrasound**
- **Capacitance**
  - Passive
  - Active (RF field)
- **Pressure**
  - Piezo
  - Conductive membrane
  - Tactile (MEMS)
- **Thermal**
  - Passive
  - Active
- **Combination (whenever possible)**
  - Silicon, TFT (glass)
  - Static, swipe
  - Contact, contactless

FINGERPRINT BASICS
FRUSTRATED TOTAL INTERNAL REFLECTION

- Finger illuminated on one side of prism with a LED
- Light reflected by air (fingerprint valleys)
- Light absorbed/scattered by skin (fingerprint ridge)
- Other side of prism transmits the image through a lens to a camera

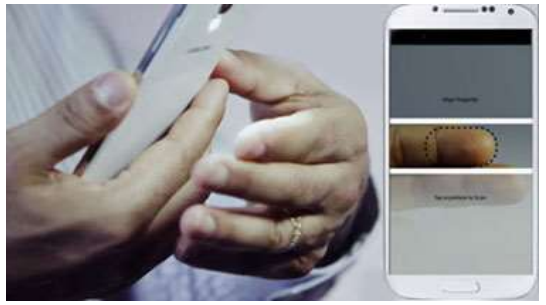
- Many clever variations on this theme



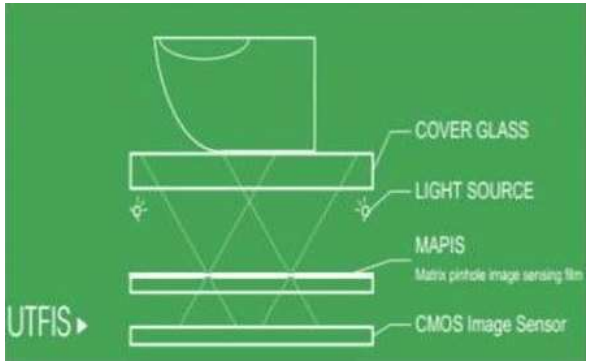
FINGERPRINT BASICS
DIRECT IMAGES

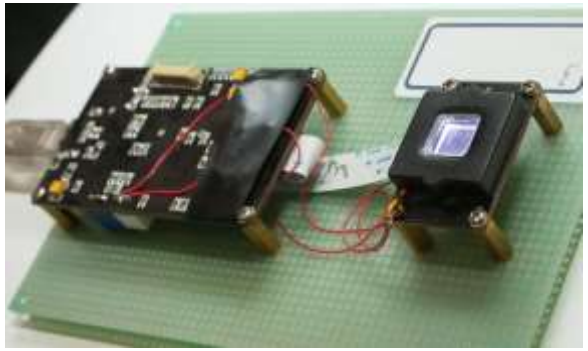
- Camera
- Structured light illumination
- Pinhole





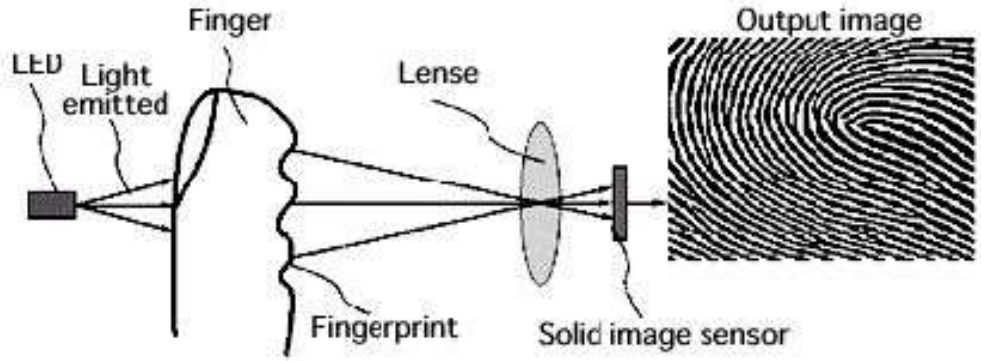


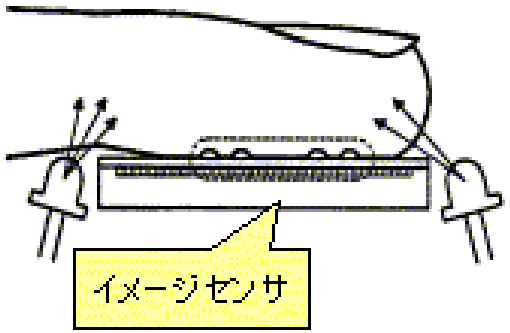



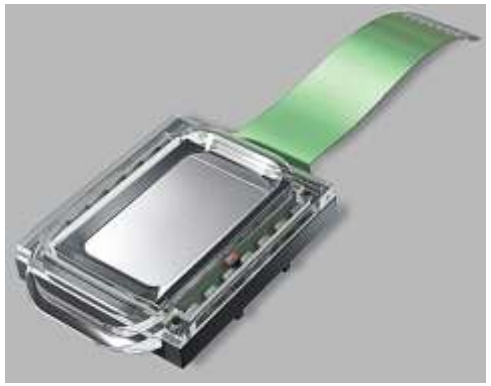


OPTICAL TRANSMISSION SENSOR

- **Image light transmitted through the skin or finger**

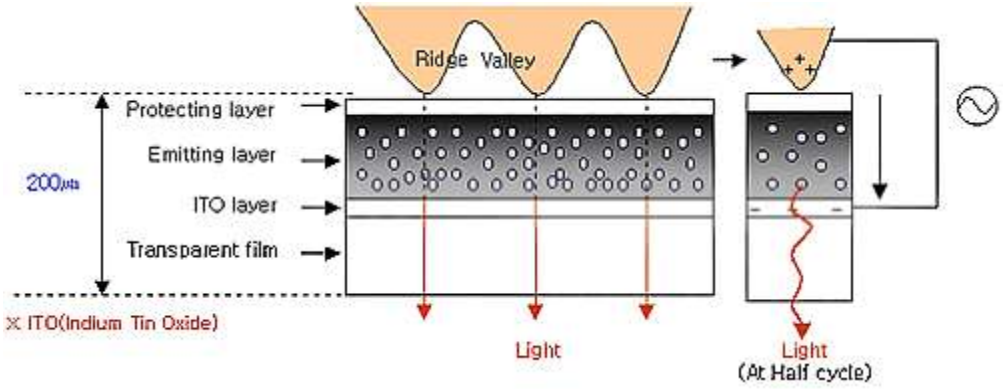


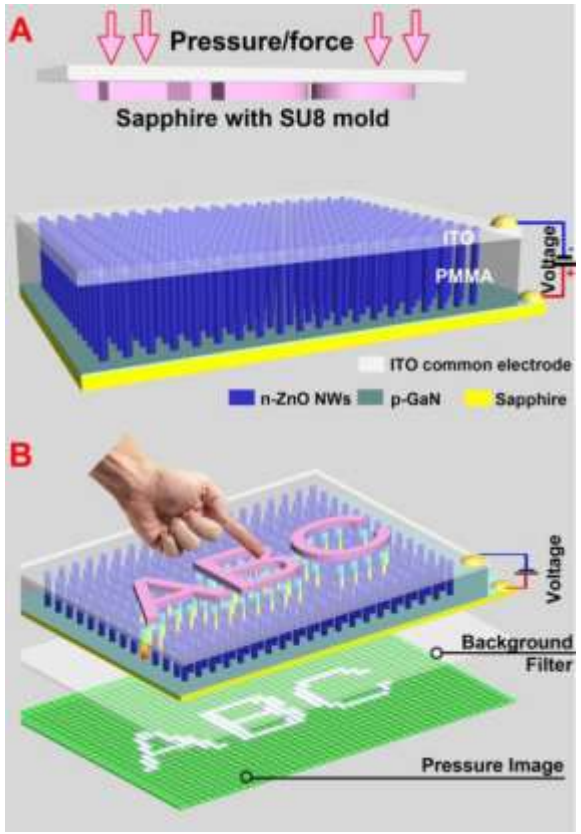




FINGERPRINT BASICS
ELECTRO-OPTICAL

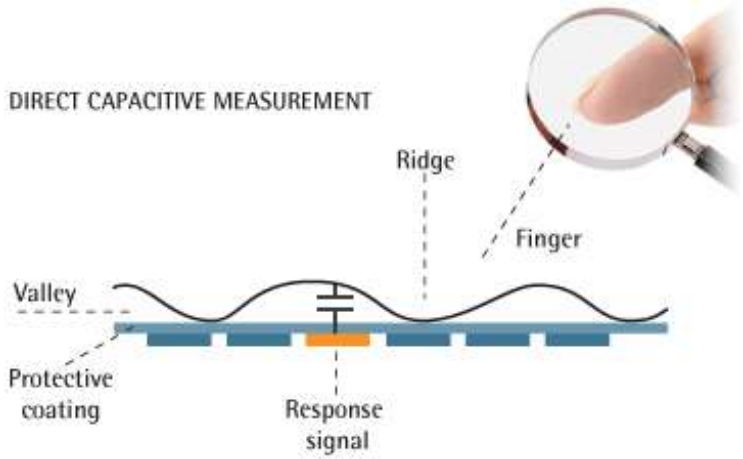
- A polymer emits light when properly powered
- A variation is proposed with a piezoelectric nanowire LED array

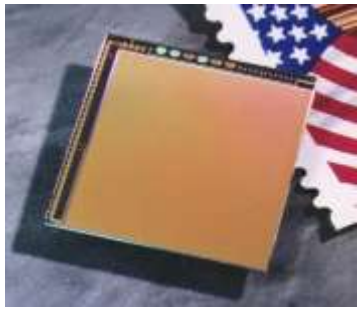




CAPACITANCE SENSOR, PASSIVE

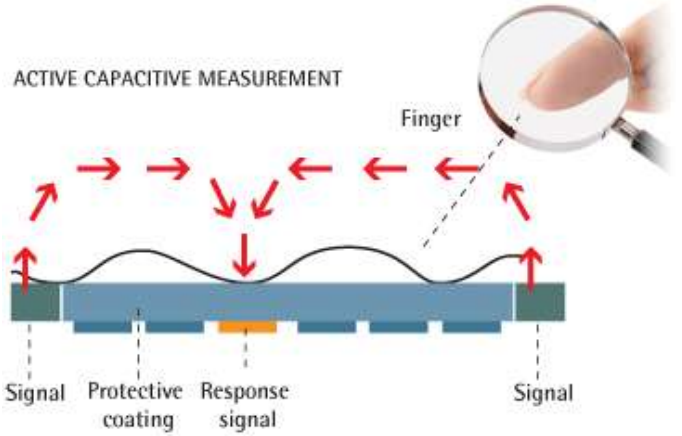
- Fingerprint valleys and ridges vary thickness of air dielectric layer, which modulates effective capacitance





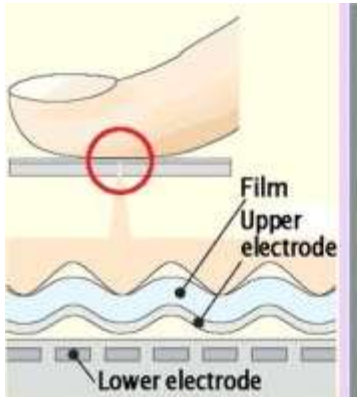
CAPACITANCE SENSOR, ACTIVE = RF FIELD

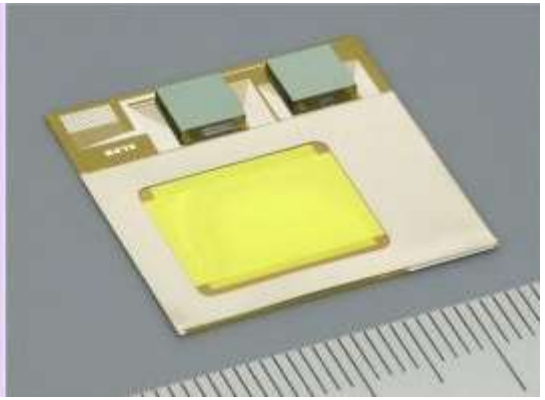
- RF signal sent into the skin and read at pixel level
- Signal crosses the coating via a capacitor

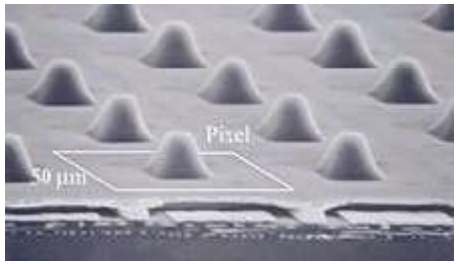


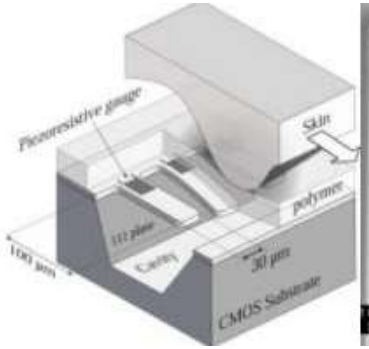
FINGERPRINT BASICS
PRESSURE

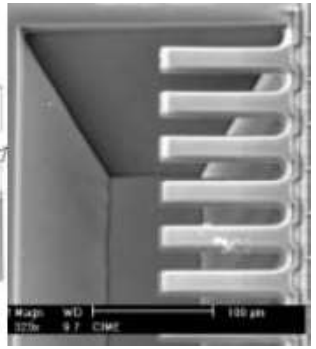
- Piezo
- Conductive membrane
- Tactile (MEMS)

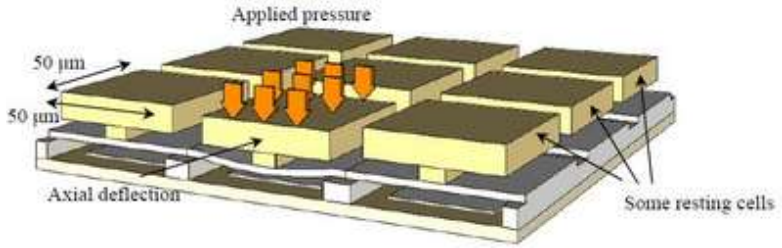


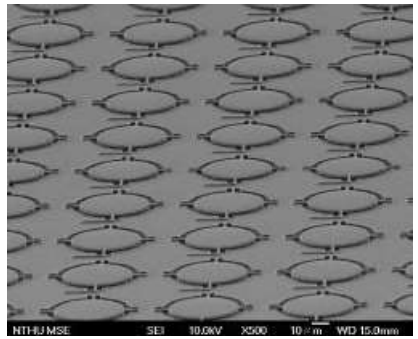






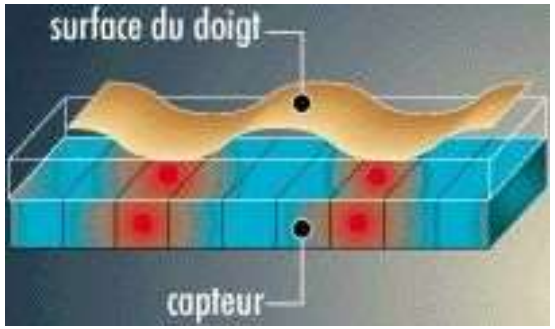






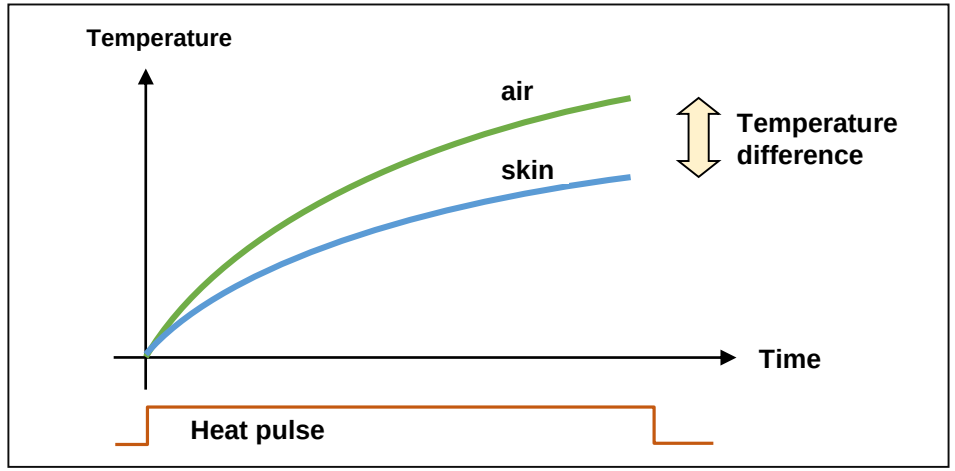
THERMAL PASSIVE

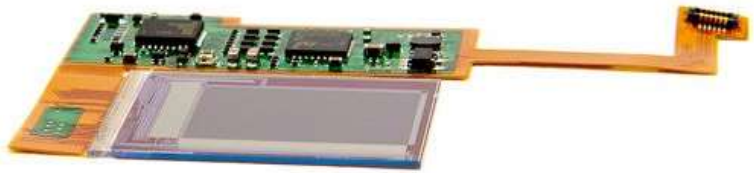
- Thermal exchange between the skin and the pixels



THERMAL ACTIVE

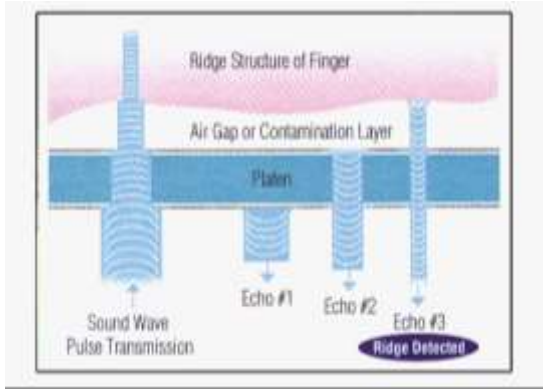
- A heat pulse is sent
- Skin will capture some heat, more than air: final temperature is lower

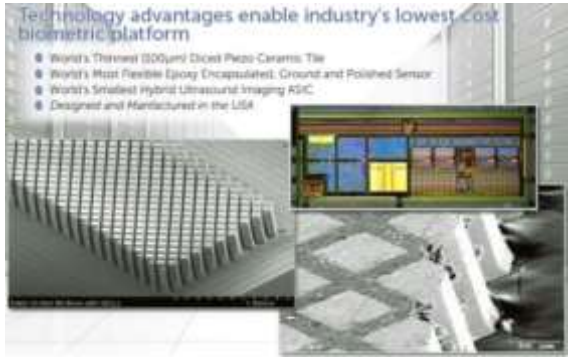


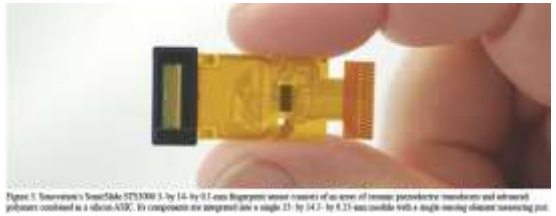


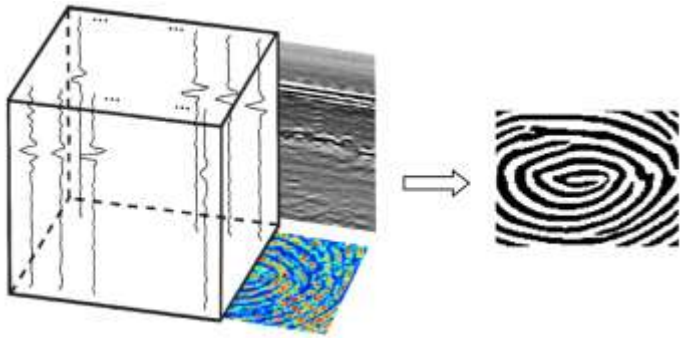
ULTRASOUND

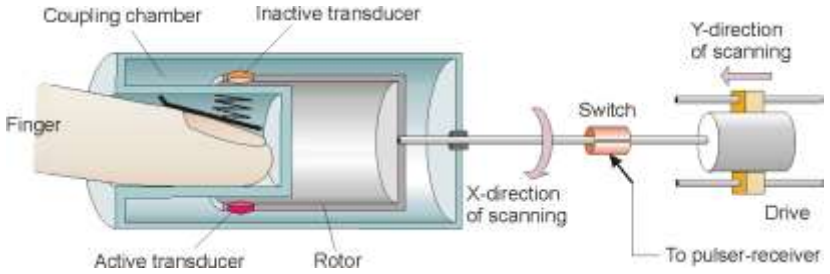
- **Piezoelectric layer**
  - Polymer
  - Ceramic











FINGERPRINT BASICS

THE GOOD : IT WORKS!

- **Standards**
  - Governmental / international big push after the 9/11 event by the ICAO / e-passport
  - Industrial associations

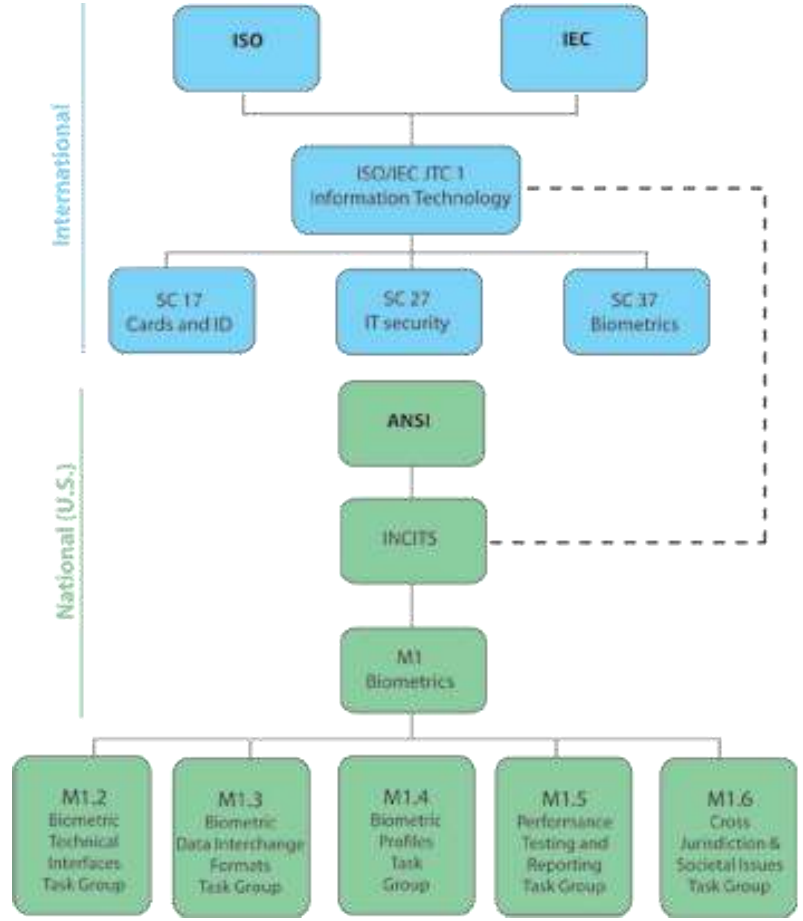
INTERNATIONAL / US ORGANISATION

- **FBI Appendix F**
  « Electronic Fingerprint Transmission Specification » 1999
  https://www.fbibiospecs.cjis.gov/IAFIS

- **ISO/IEC JTC 1 SC37 Biometrics**
  http://www.iso.org/iso/iso_technical_committee.html?commid=313770

- **INCITS M1 (ANSI)**
  http://standards.incits.org/a/public/group/m1

- **BioAPI Consortium (Biometric Application Programming Interface) published as an ISO standard in 2005**



ASSOCIATIONS

- IBIA International Biometrics & Identification Association
  https://www.ibia.org/
- FIDO (Fast IDentity Online) Alliance (formed in July 2012)
  https://fidoalliance.org/
- IEEE Standard for Biometric Open Protocol
  https://standards.ieee.org/standard/2410-2019.html
- OASIS Biometrics Technical Committee
  https://www.oasis-open.org/committees/biometrics/charter.php

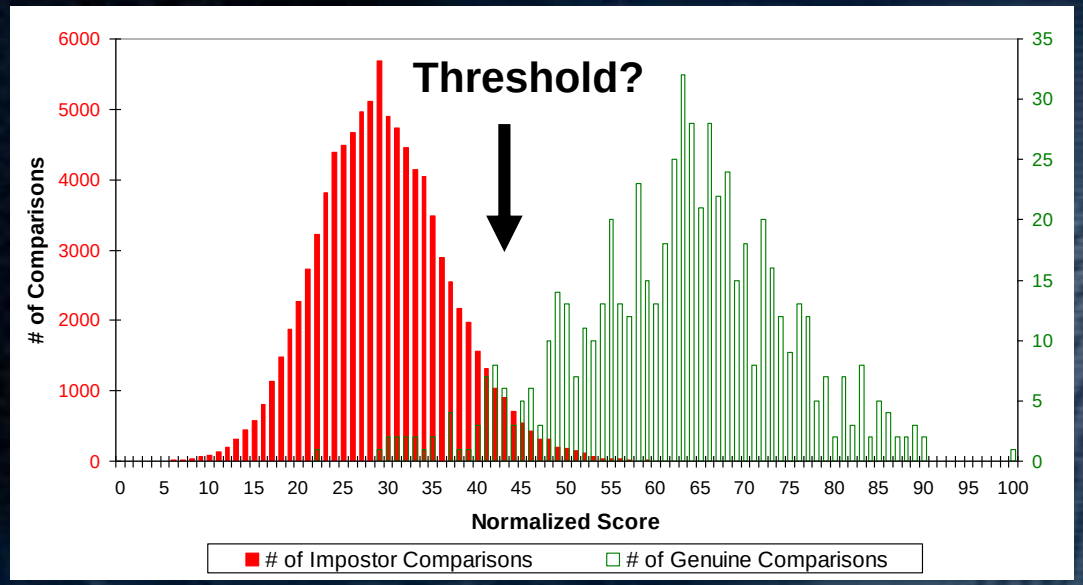
FIDO : ACCREDITED BIOMETRIC LABORATORY LIST

LOGO	COMPANY NAME ▲	COUNTRY	ACCREDITATION LEVEL	ISSUED DATE	
BCTC	Beijing Unionpay Card Technology Co., Ltd（Bank Card Test Center)	P.R.CHINA	• Biometric	6/17/2019	Details
elitt leti	ELITT/Leti CEA	France	• Biometric	5/1/2019	Details
FIME	FIME	France	• Biometric		Details
iBeta QUALITY ASSURANCE	iBeta, LLC.	USA	• Biometric	7/18/2018	Details
idiap	Swiss Center for Biometrics Research and Testing Idiap Research Institute institute	Switzerland	• Biometric	4/15/2019	Details
TTA 한국정보통신기술협회 Telecommunications Technology Association	Telecommunications Technology Association (TTA - biomteric)	South Korea	• Biometric	9/3/2019	Details
TÜVIT TÜV NORD GROUP	TUV Informationstechnik GmbH	Germany	• Biometric	11/27/2019	Details

(Feb 2020)

THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

Accuracy



Security:
- Cryptography
- Aliveness detection

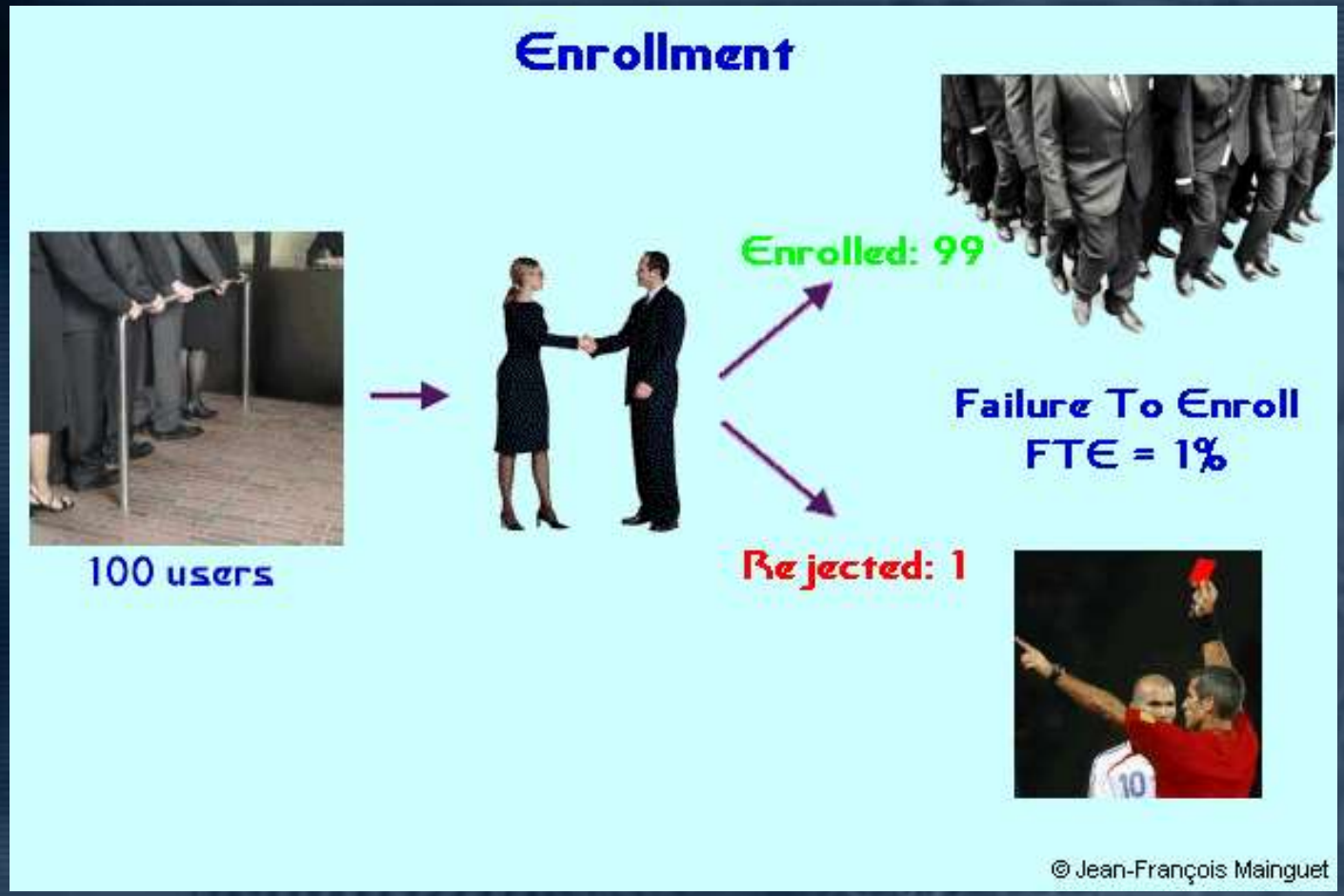
THE BAD: IT DOESN'T ALWAYS WORK… ACCURACY

BIOMETRIC RECOGNITION IS PERFECT

- **No! Biometrics cannot be 100%.**
- **It is not possible to acquire each time exactly the photo of your face, with exactly all the same pixels.**
- **So a threshold exists, with associated metrics:**
  - FAR: False Acceptance Rate (security)
  - FRR: False Rejection Rate (convenience)
- **FAR & FRR are linked:**
  the harder the system (=low FAR), the higher the FRR

THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

FAILURE TO ENROLL



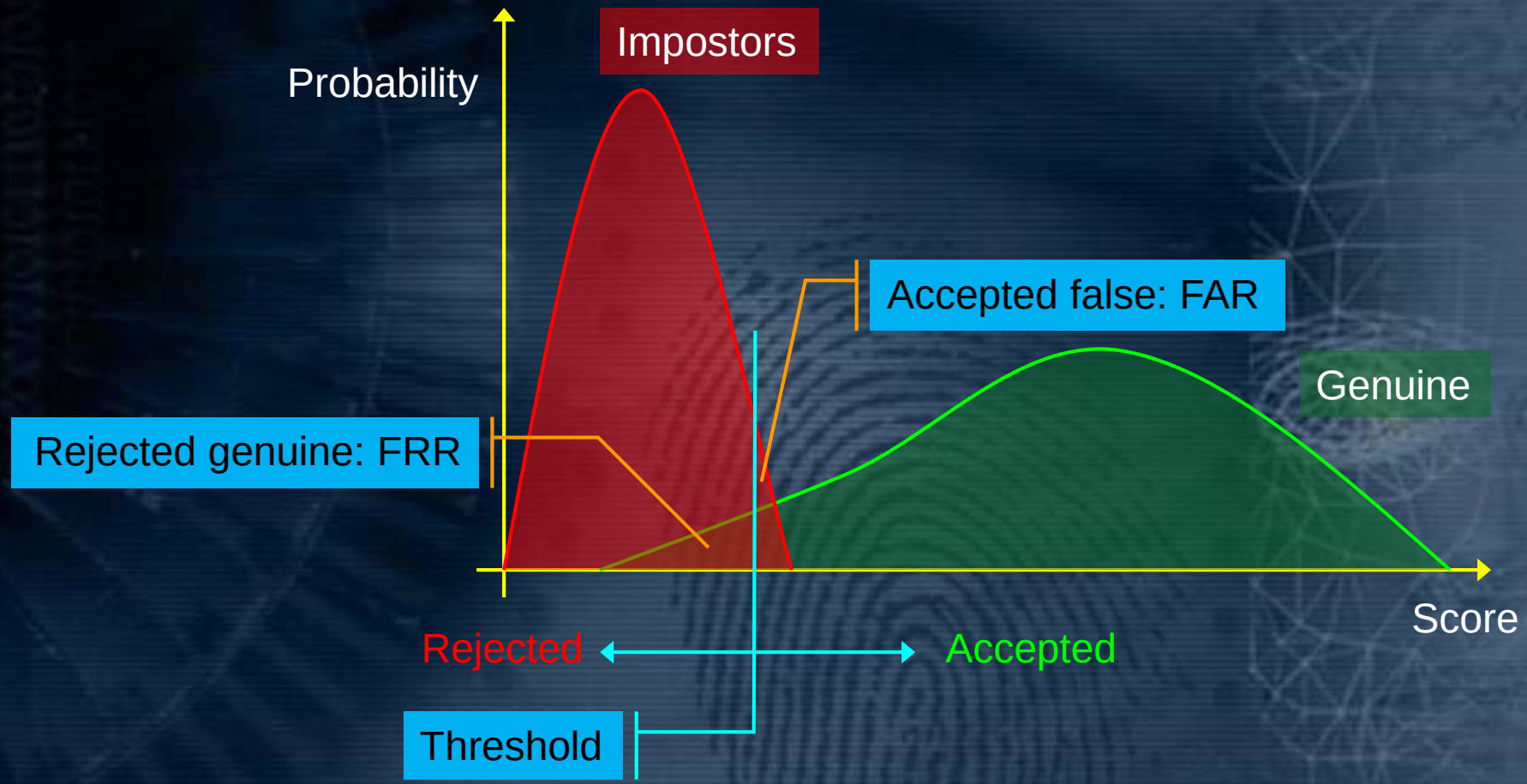
THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

SCORING & THRESHOLD

- **Is this the same person? Give a note!**

THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

FAR / FRR



THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

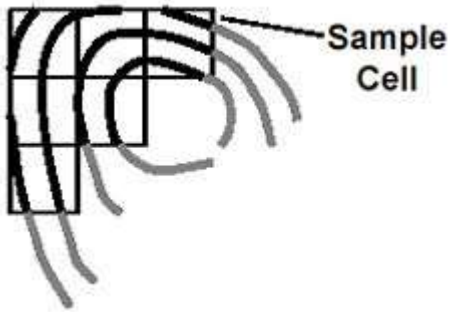
TESTING

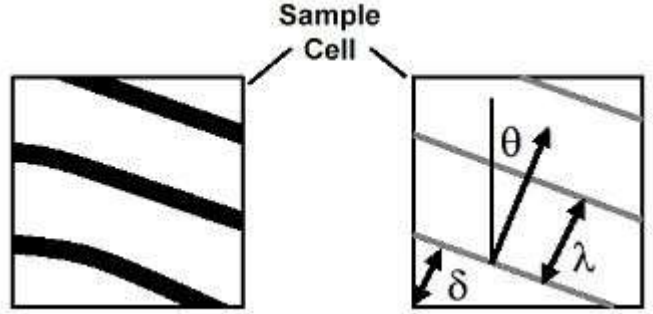
Type of Test	Technology (in vitro)	Scenario (in situ)	Operational (in vivo)
Database	Typically pre-collected, usually for testing multiple components	Gathered with system under test	Gathered with system under test
Data Comparisons	Offline	Online and/or Offline	Online (may have offline component)
Object of Testing	Biometric **component** (e.g., algorithm or sensor)	Biometric **system**	Biometric **system**
Physical Environment	Controlled or uncontrolled when biometric data recorded, Not applicable during testing	Controlled and/or recorded	Not controlled, preferably recorded
User Interaction	Maybe recorded when biometric data recorded, Not applicable during testing	Recorded	Recorded during enrollment, Maybe recorded during verification/identification
User Behavior	Controlled and/or Uncontrolled when biometric data recorded, Not applicable during testing	Controlled	Uncontrolled
Repeatability of Results	Repeatable (database fixed)	Quasi-repeatable (if test scenario and population controlled)	Non-repeatable
Typical Results Reported	Comparison of biometric components or versions of components (e.g., algorithms) Determine critical performance factors	Compare biometric systems Determine critical performance factors Predict simulated performance	Measure performance in an operational environment
Requirements	Appropriate test database, e.g., data gathered with a universal sensor	Operational, instrumented system with scores available	Operational, instrumented system (typically only decisions available, scores preferable)
Human Test Population	Recorded	Live	Live

FINGERPRINT ACCURACY

- **Many different algorithms exist to compare fingerprints**

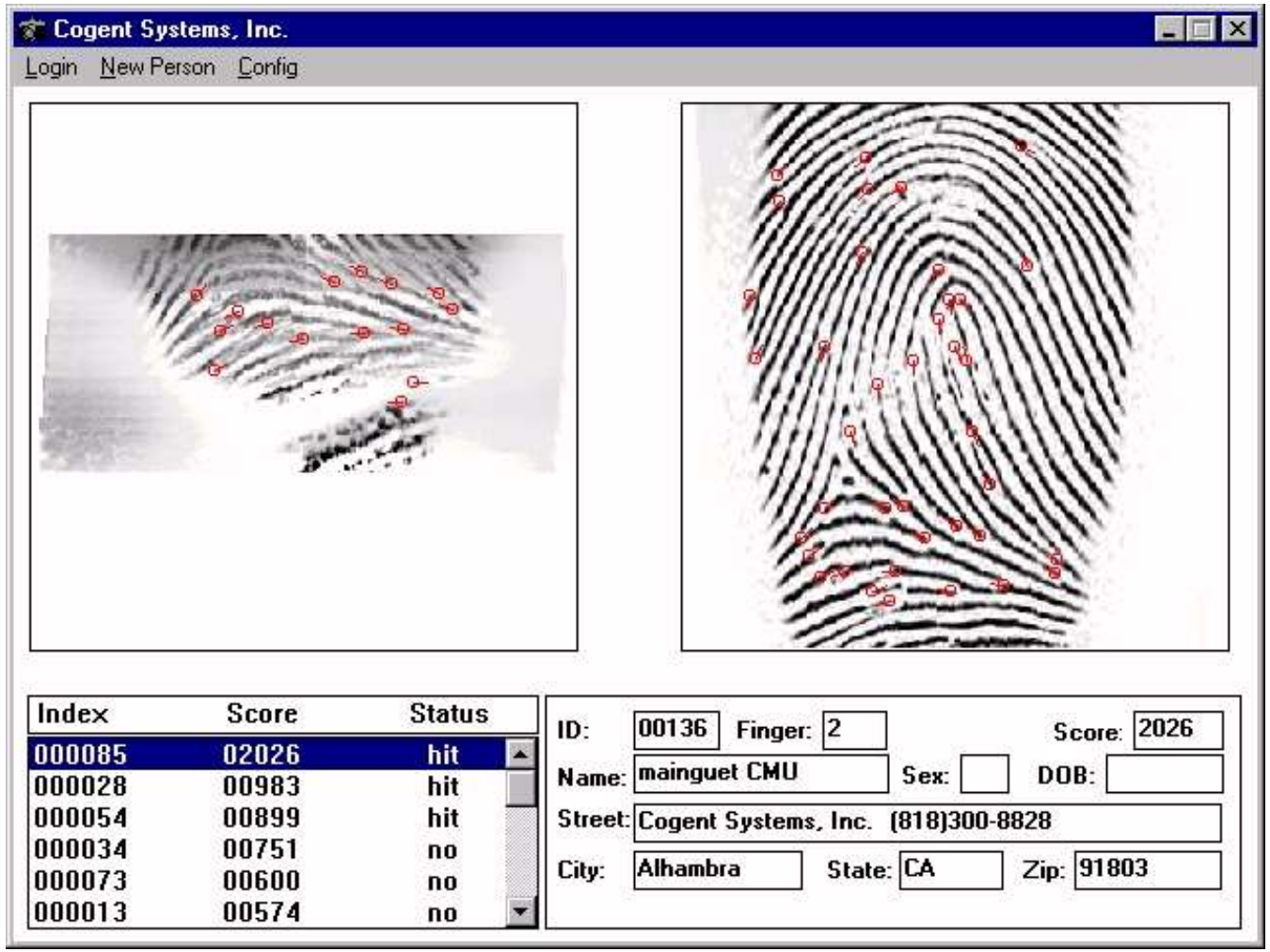
- **Two common types:**
  - Minutiae-Based
    - Minutiae locations and directions compared
    - Minutiae are generally mandatory for governmental applications (linked to standards)
  - Pattern-Based
    - General shape of the ridges compared





THE BAD: IT DOESN'T ALWAYS WORK… ACCURACY

SCORING: FINGERPRINT



THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY : DIFFICULT FINGERS

THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY : 3 MONTHS LATER

(a) (b)

SENSOR SIZE

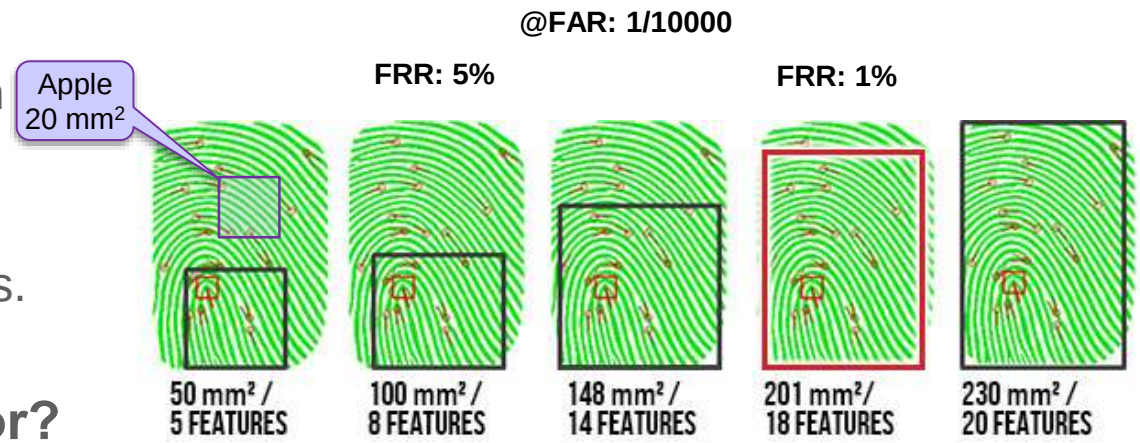
Same accuracy?

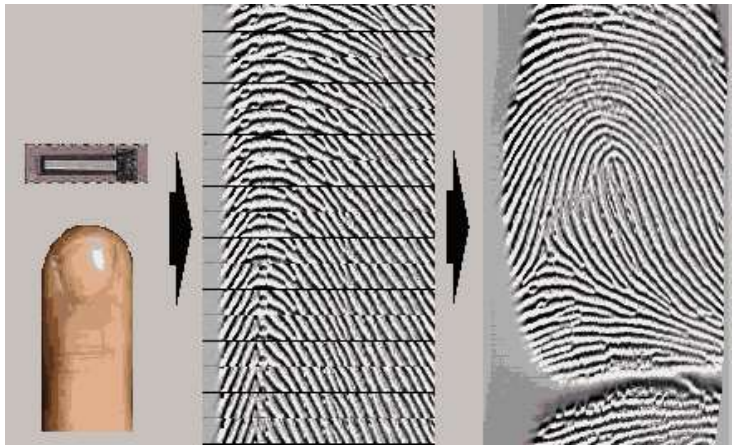
FINGERPRINT SENSOR
ACCURACY / SIZE OF THE SENSOR

- **The more data, the better**
  - Next Biometrics has ordered the “Madrid report” which shows that size does matter.
    3 market leading sensors, 600 people, 180.000 prints and more than 100 million comparisons
  - Apple is the opposite, and do not show any test results.

- **What is a “reasonable” minimum size for a sensor?**
  - Swipe sensors give larger images with a minimum size
    → at the cost of ergonomics + some distortion
  - Area sensors are the only ones “governmental certified”
    → compatible with minutia-based algorithms

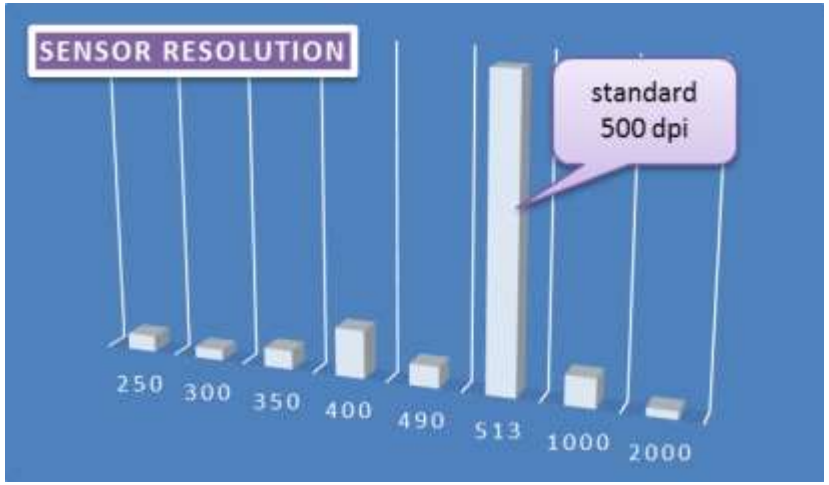
- **What about the bioengine?**

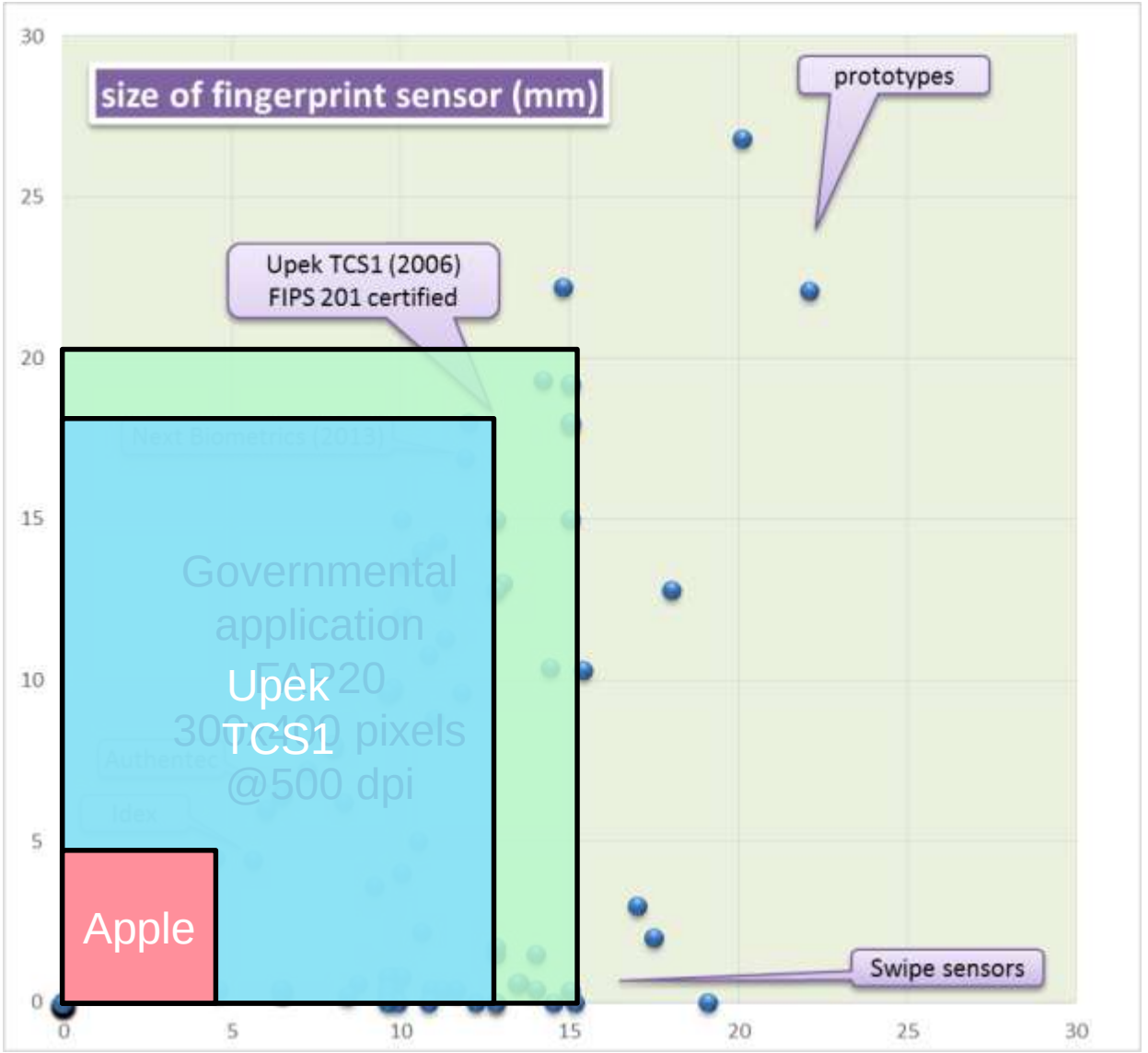




FINGERPRINT SENSOR MANUFACTURERS
SIZE OF SENSORS

- Products & prototypes from 58 organizations
- Hard to believe that everybody is wrong…





SPOOFING

THE BAD: IT DOESN'T ALWAYS WORK…
SECURITY

"The 6th day"

THE SIXTH DAY

THE SIXTH DAY

THE SIXTH DAY

THE BAD: IT DOESN'T ALWAYS WORK…
SECURITY

BOND . . . JAMES BOND . . .

THE BAD: IT DOESN'T ALWAYS WORK…
SECURITY

Diamonds are Forever (circa 1971)

THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

"I AGREE TO THE TRANSACTION"

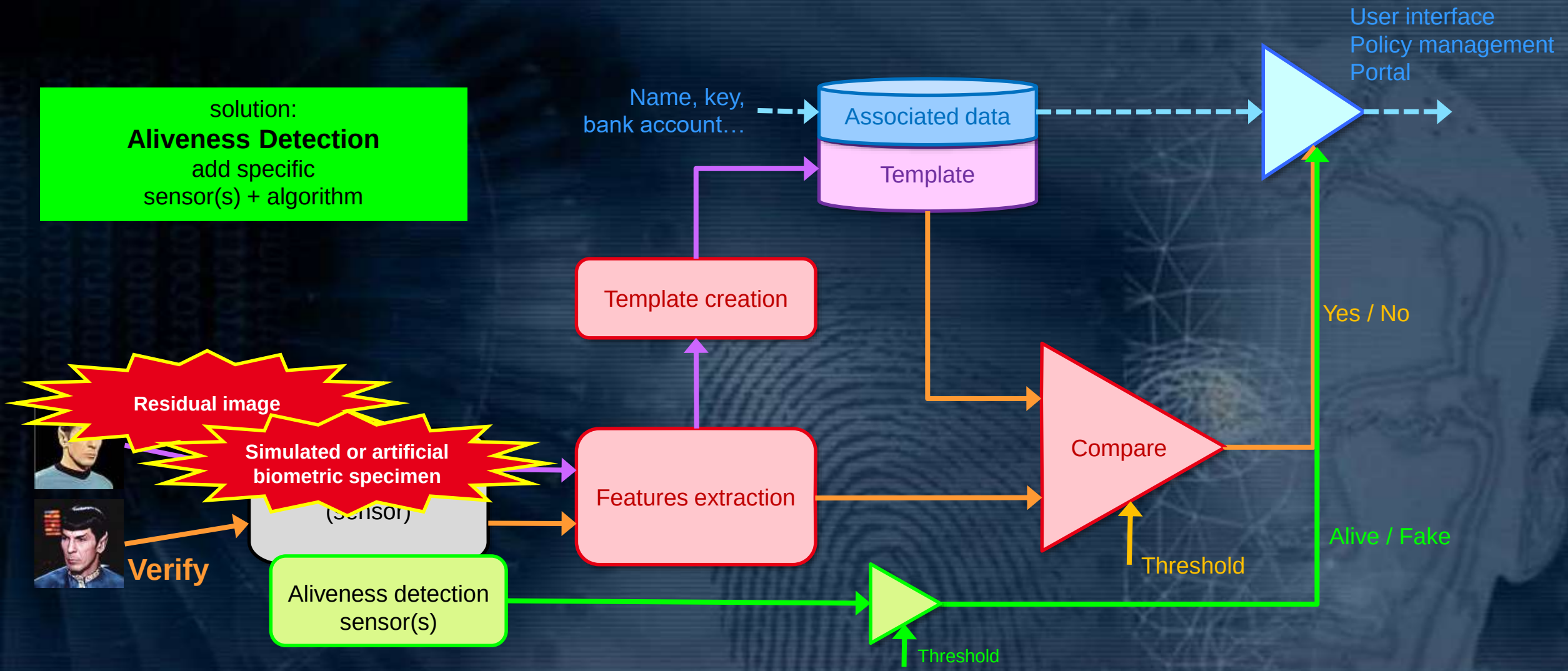
- **Proving that you are living is not enough.**
- **What is desired is to prove that:**
  - I'm a living person not under threat,
    and I agree to make such and such action
- **This is impossible: you can't read a person's mind.**
- **Once again, 100% security does not exist.**

ELECTRONIC & ALIVENESS SECURITY

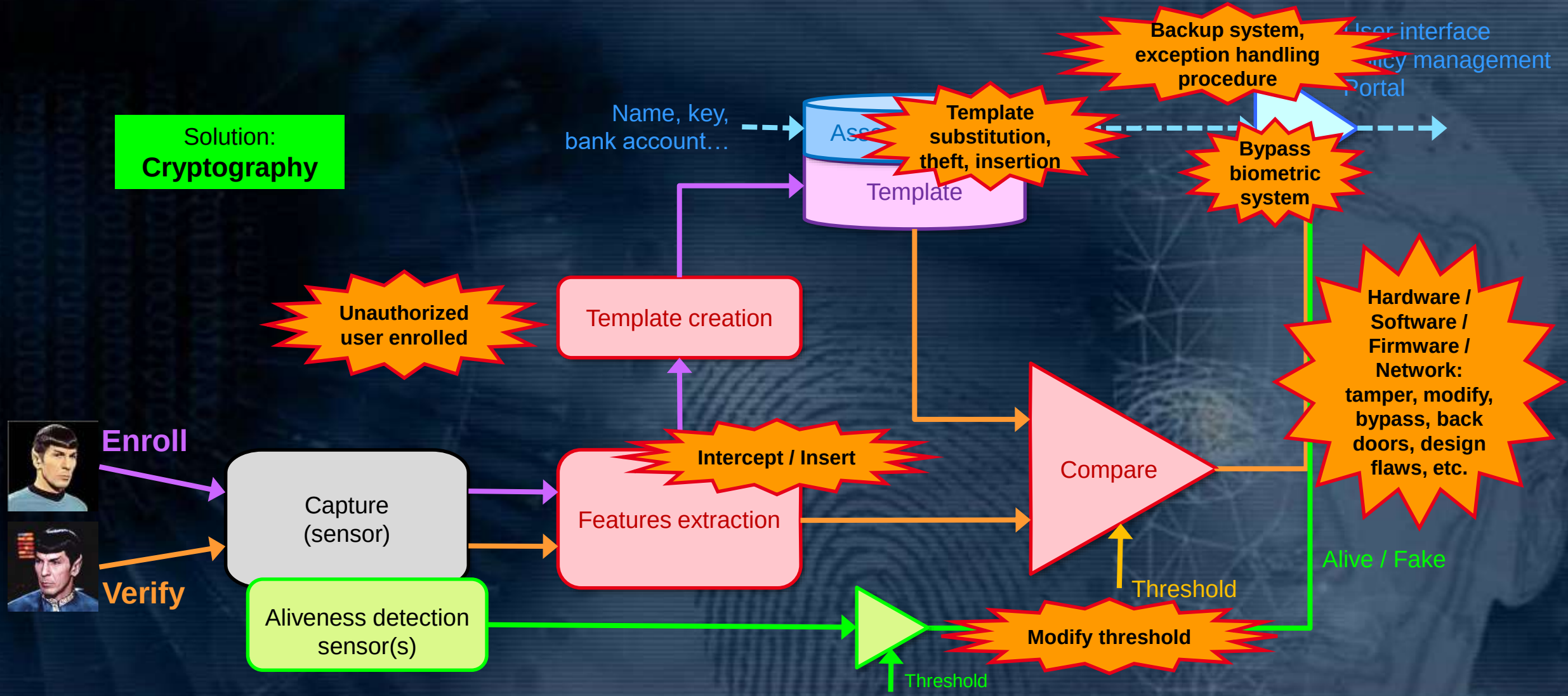
- **Security of an (electronic) biometric system may be divided into two main areas:**
  - Electronic security
    - Is it an authorized biometric system at the other end of the wires?
  - "Living" security
    - Is this finger alive, fake or dead?

BIOMETRICS
SECURITY THREATS : SPOOFING

solution:
Aliveness Detection
add specific
sensor(s) + algorithm

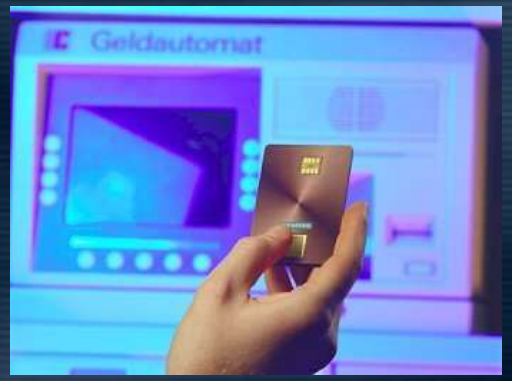


BIOMETRICS
SECURITY THREATS



THE BAD: IT DOESN'T ALWAYS WORK…
SMART CARD WITH INTEGRATED FINGERPRINT SENSOR

- **Where is the fingerprint reference?**
- **How is it cyphered?**
- **Where is the comparison algorithm?**
- **…**



Siemens 1999

MasterCard (South Africa) 2017

Kona 2016

THE BAD: IT DOESN'T ALWAYS WORK…
SECURITY

SECURITY BREACHES

- **Attended / unattended system?**
  - Attended:
    - Aliveness detection is likely not useful.
    - Do you better trust a person or a machine?
    - You can show your finger to say: "This is a true finger, not a fake!"
  - Unattended:
    - Aliveness detection is desirable.

COMPROMISED BIOMETRIC TRAITS

- **Common belief: If your fingerprint (face, iris…) has been copied once and used to spoof a system, then you cannot reuse it.**

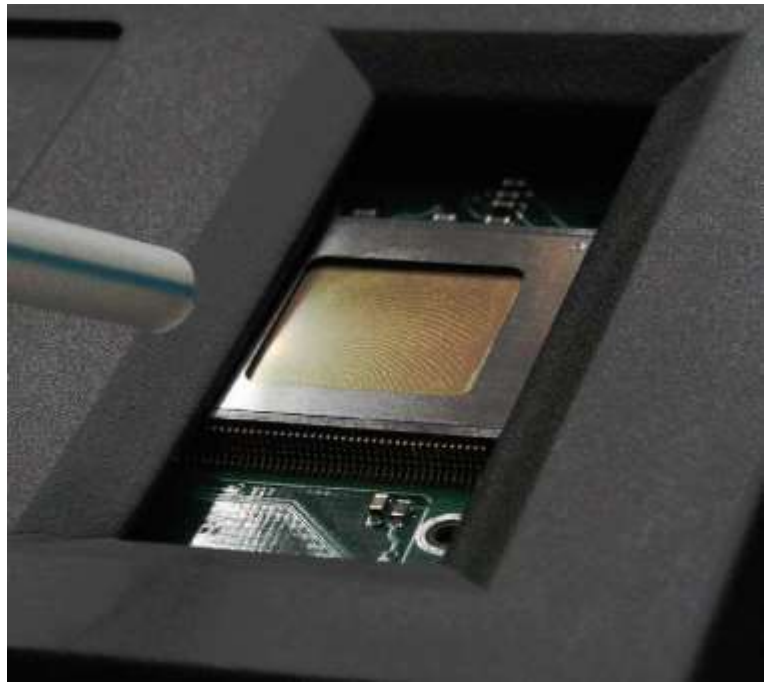
  It is *compromised*.

- **Solutions:**
  - Aliveness detection
  - Encryption: Cypher / sign the recorded biometric trait, so you can revoke this record.
    - If someone steals your credit card with your fingerprint inside, then it is possible to reject this card; the fake is of no use with this card.

ALIVENESS DETECTION LEVELS

- **Aliveness: hard to detect**
  - What is a dead finger?
    A surgeon is able to mend a cut finger (if kept in ice)!
  - Whole hands have already be transplanted from a deceased donor: also the fingerprints!

- **Definition of levels:**
  - Zero effort: a latent print left on the sensor
  - Fake/copies:
    - Fingerprint image
    - Fake made of gelatin, latex…
    - Thin layer of material glued to a real finger
  - Original finger:
    - Cut out
    - Belonging to a dead person



SPOOFING

- **CUT FINGER?**

Demolition Man 1994

THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

COPYING BIOMETRIC TRAITS

- **Biometric information is often public.**
  - Think about face recognition!
  - You cannot rely on the biometric data secrecy!
- **Donor cooperation helps but is not mandatory.**
  - DNA: just pick up organic residues
  - Face: a simple photo
  - Iris: a good high resolution photo
  - Fingerprint: latent prints
  - Voice: a recorder
  - Hand: a mold
  - Vein: no visible trace
- **Having the original sensor device helps.**
  - You get a genuine electronic copy!
  - And so, you can create a fake to spoof this sensor…

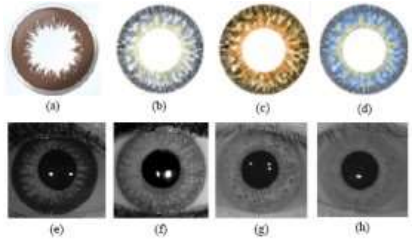


Figure 5. Samples of contact lenses((a)-(d)), fake iris((e),(f)) and live iris((g),(h)).

COPYING BIOMETRIC TRAITS

- **How difficult is it to make a fake finger?**
  - With cooperation
    - Making a mold is quite easy, and you can find information over the Internet.
    - Most articles dealing with this suppose cooperation.
  - From a latent print
    - Having the right latent print is not so obvious. (It is difficult to know which finger it is!)
    - Identifying the latent print is very often difficult, even for a forensic professional.
    - From a good picture, making a mold is not too hard; like a rubber stamp or a printed board.

THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

FAKE FINGEPRINTS

- **Many different materials have been tried**
  - Gelatin
  - Silicone
  - Rubber
  - Wood glue
  - Hot glue
  - Soft plastic
  - Latex
  - Alginate
  - Clay
  - Glycerin
  - …
- **We consider that making a latex copy is difficult, but far from being impossible.**

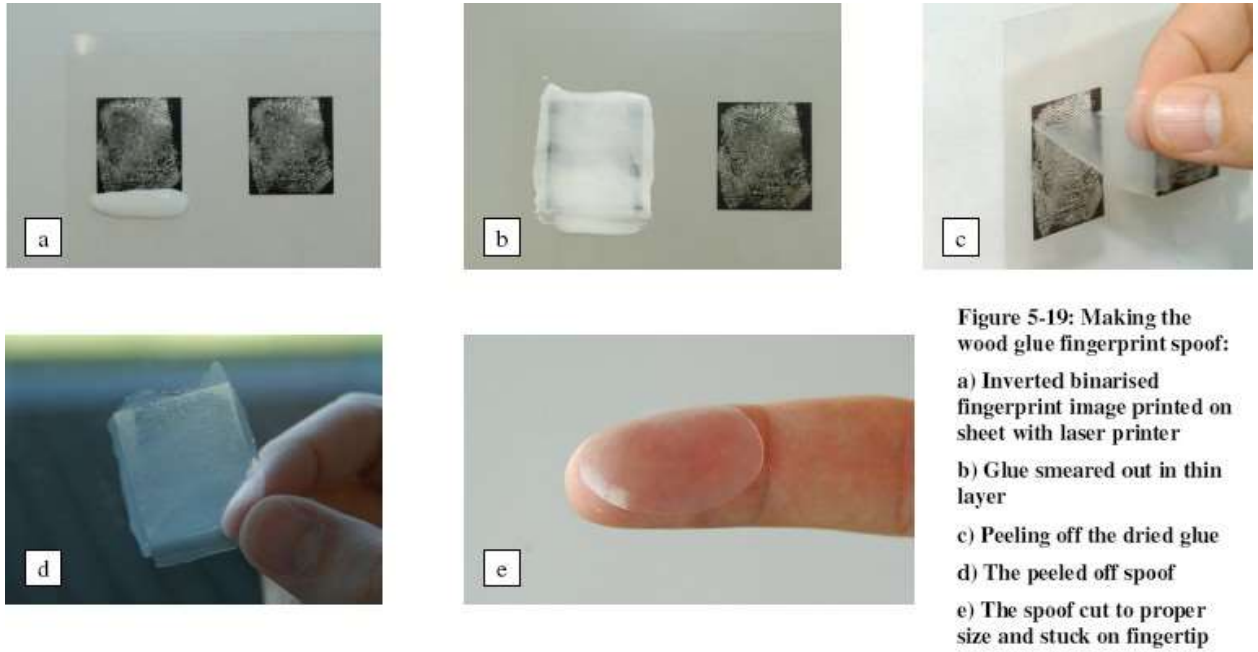


Figure 5-19: Making the wood glue fingerprint spoof:

a) Inverted binarised fingerprint image printed on sheet with laser printer

b) Glue smeared out in thin layer

c) Peeling off the dried glue

d) The peeled off spoof

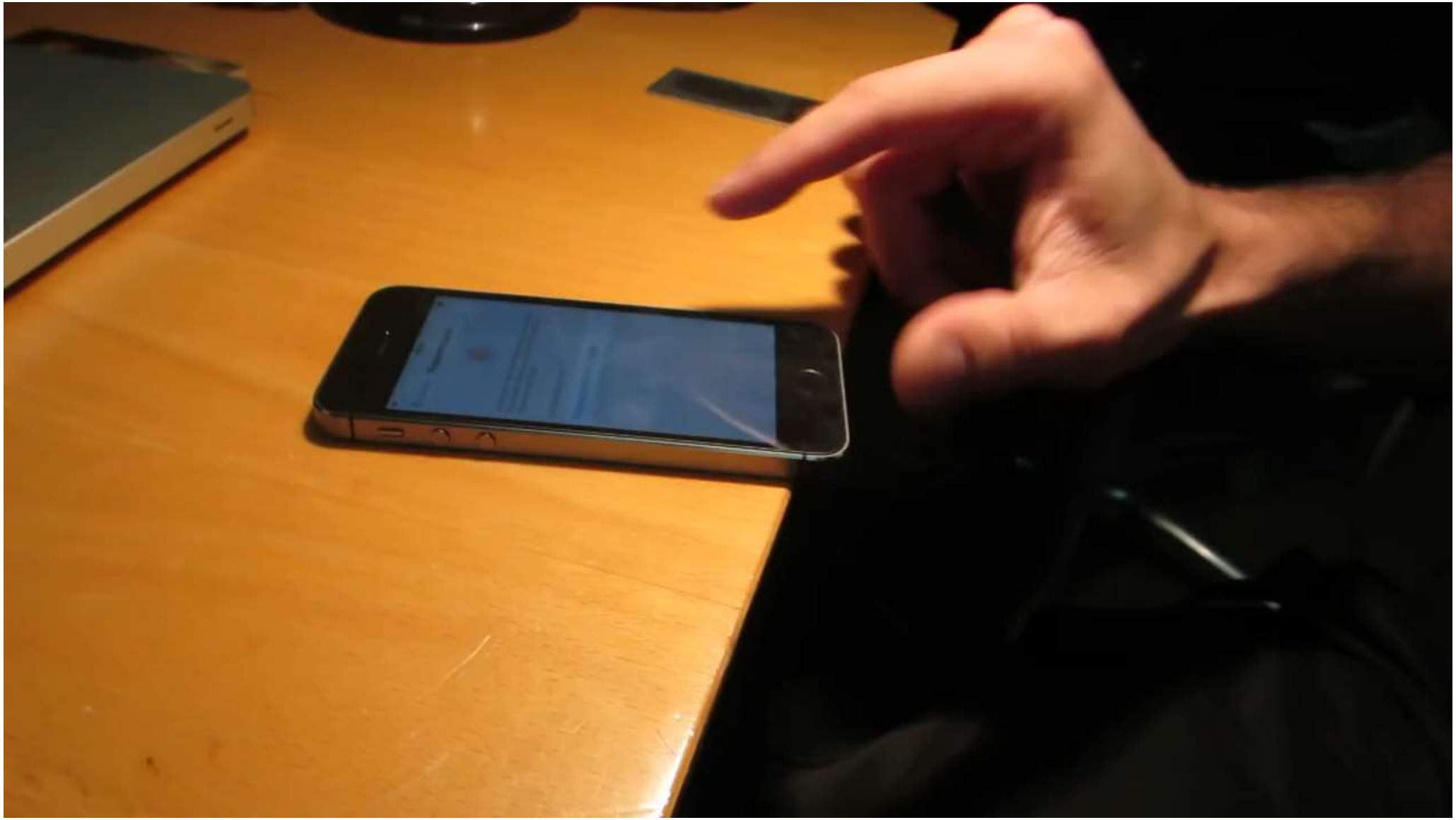
e) The spoof cut to proper size and stuck on fingertip

Fig. 5. Glycerin - left: thin layer - center: thick layer - right: 3D models

THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

IPHONE 5 & 6

- **Touch ID : no aliveness detection**
- Authentec said their sensor is working with a live finger…. But never said that fakes are also working!

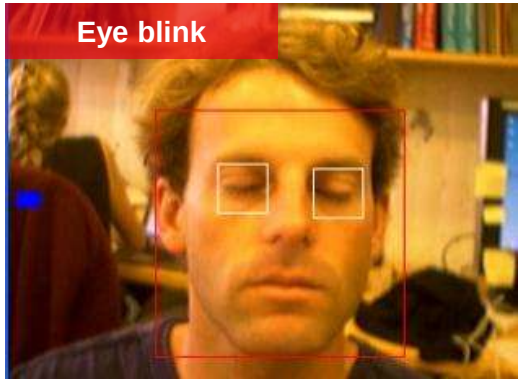


THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

SOME ALIVENESS DETECTION SYSTEMS

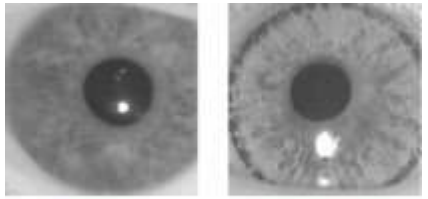
Red eye


pupillary light reflex / hippus




Skin distorsion (Maltoni)

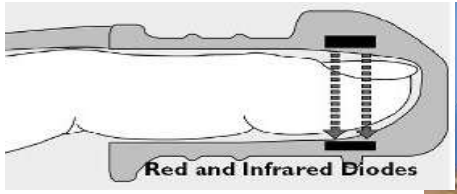

Skin impedance (Guardware)



Fourier analysis


Skin spectrum (Lumidigm)


3M Biosentry ultimate (1996)
pulse detection + EKG




Pulse oximetry

Perspiration (Schuckers)

- **First real known case**
  - Malaysia end of March 2005, where a team of carjackers on the prowl in Subang Jaya chopped off part of the left index finger when they realized that the S-Class Mercedes Benz had a security feature which would immobilize the car without his fingerprint.

- **Graft**
  - George attempted to enter the U.S. illegally on September 24, 2005 through the Nogales, Ariz. Port of Entry during which time U.S. Customs and Border Protection officers noted that his fingerprints had been surgically replaced with skin from his feet.
  - George stated that this procedure had been done to “clean” his identity by a doctor in Phoenix.

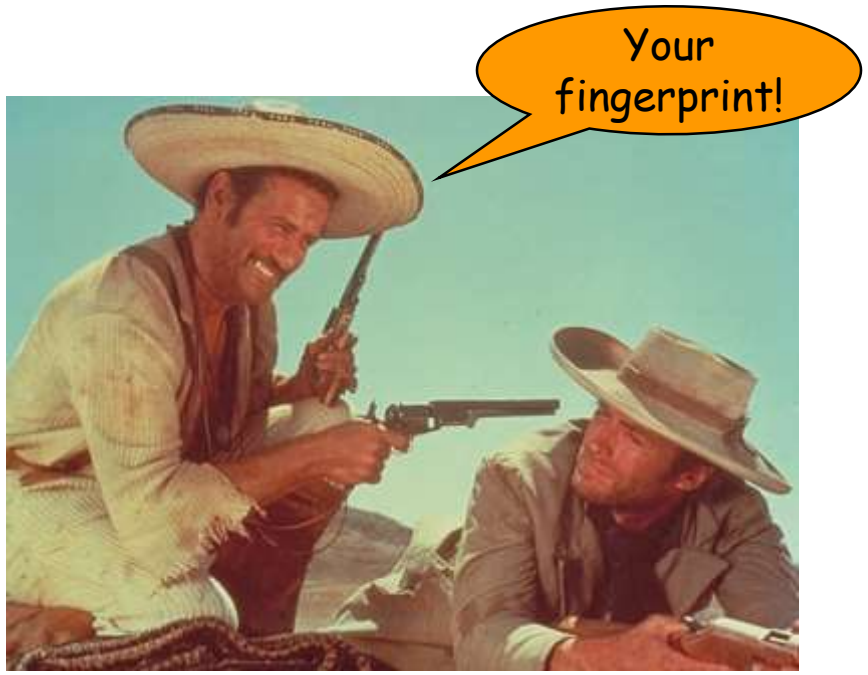
- **Angry wife gets Doha-Bali flight diverted to Chennai (2017 Nov, 5th)**
  - The Iranian woman, who was with her husband and their young child on a Qatar Airways flight from Doha to Bali on Sunday, unlocked her sleeping hubby's phone by putting his finger on the home button and found evidence he was cheating on her.

ALIVENESS DETECTION

- **What Liveness Testing IS:**
  - A means to minimize the effectiveness of artificial or simulated biometric specimens and thus improve the security posture of the biometric system.

- **What Liveness Testing IS NOT:**
  - A guarantee that the biometric specimen belongs to the authentic live human being.

- **"If man can make it, man can break it!"**



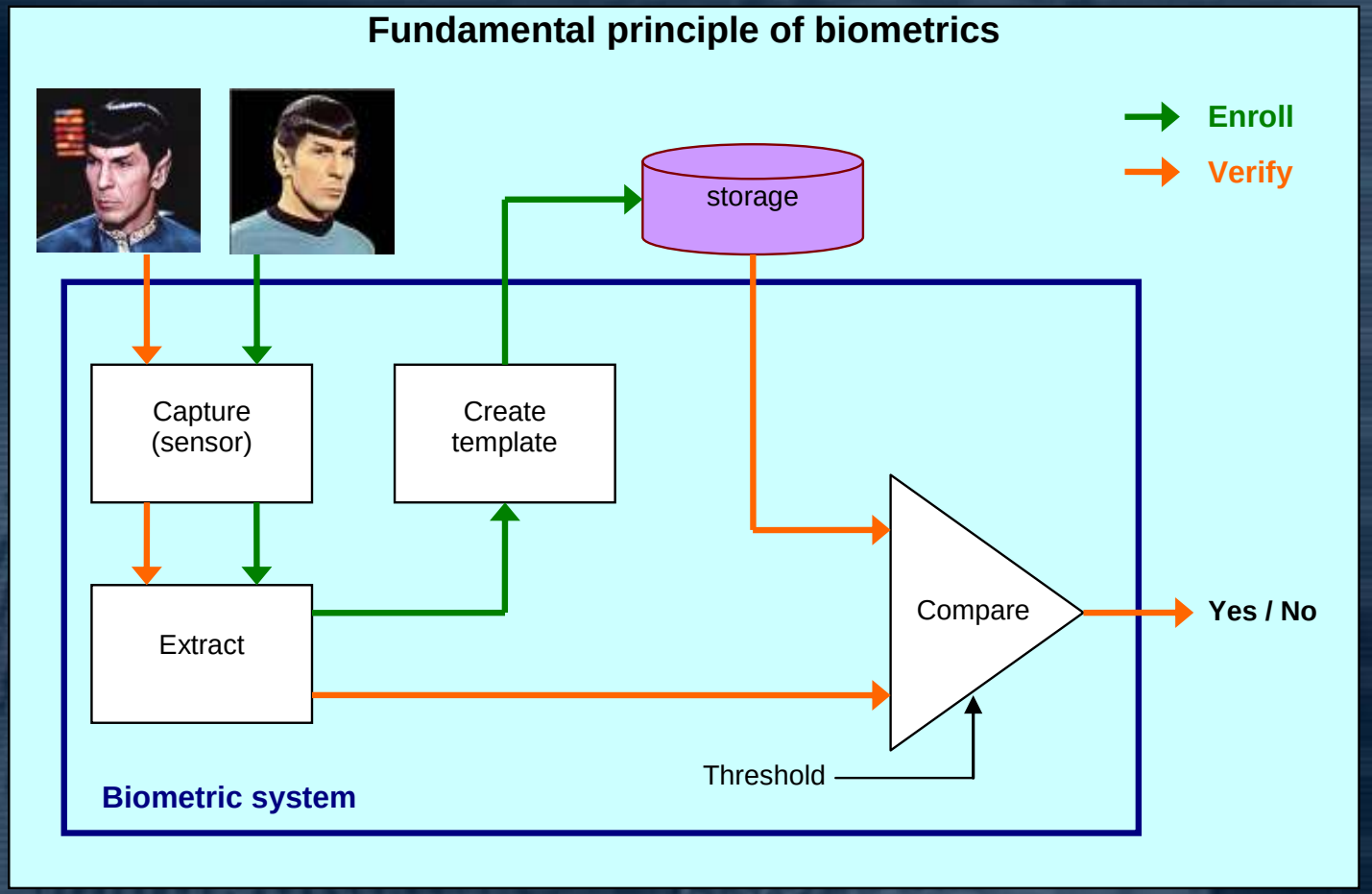
THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

CRYPTOGRAPHY & BIOMETRICS

- **How combining cryptography & biometrics?**
  - Biometrics basics
  - Cryptographics basics
  - Combining:
    - simple combination
    - hashed
    - intricated

THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

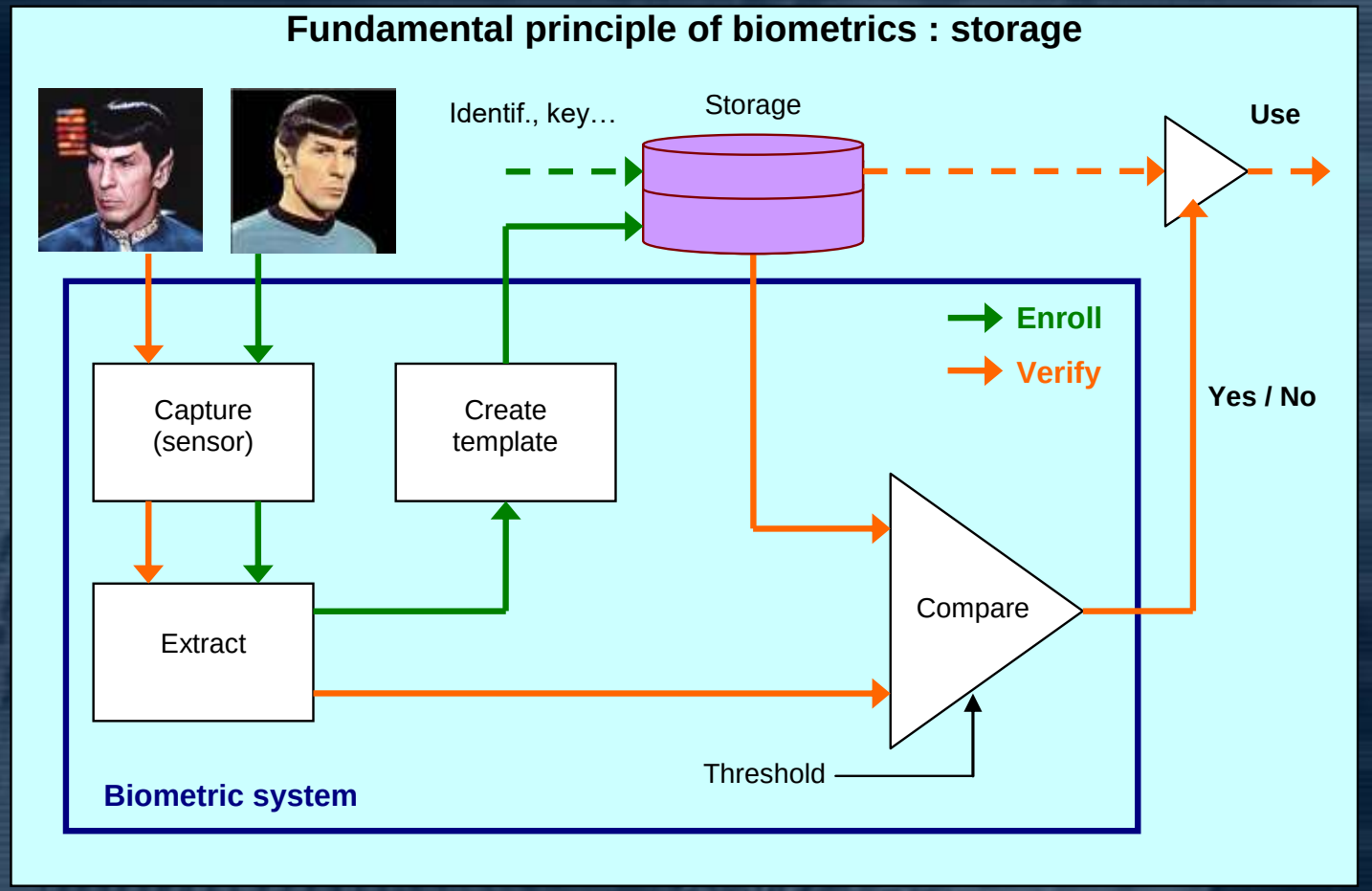
BIOMETRICS



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

BIOMETRICS + APPLICATION

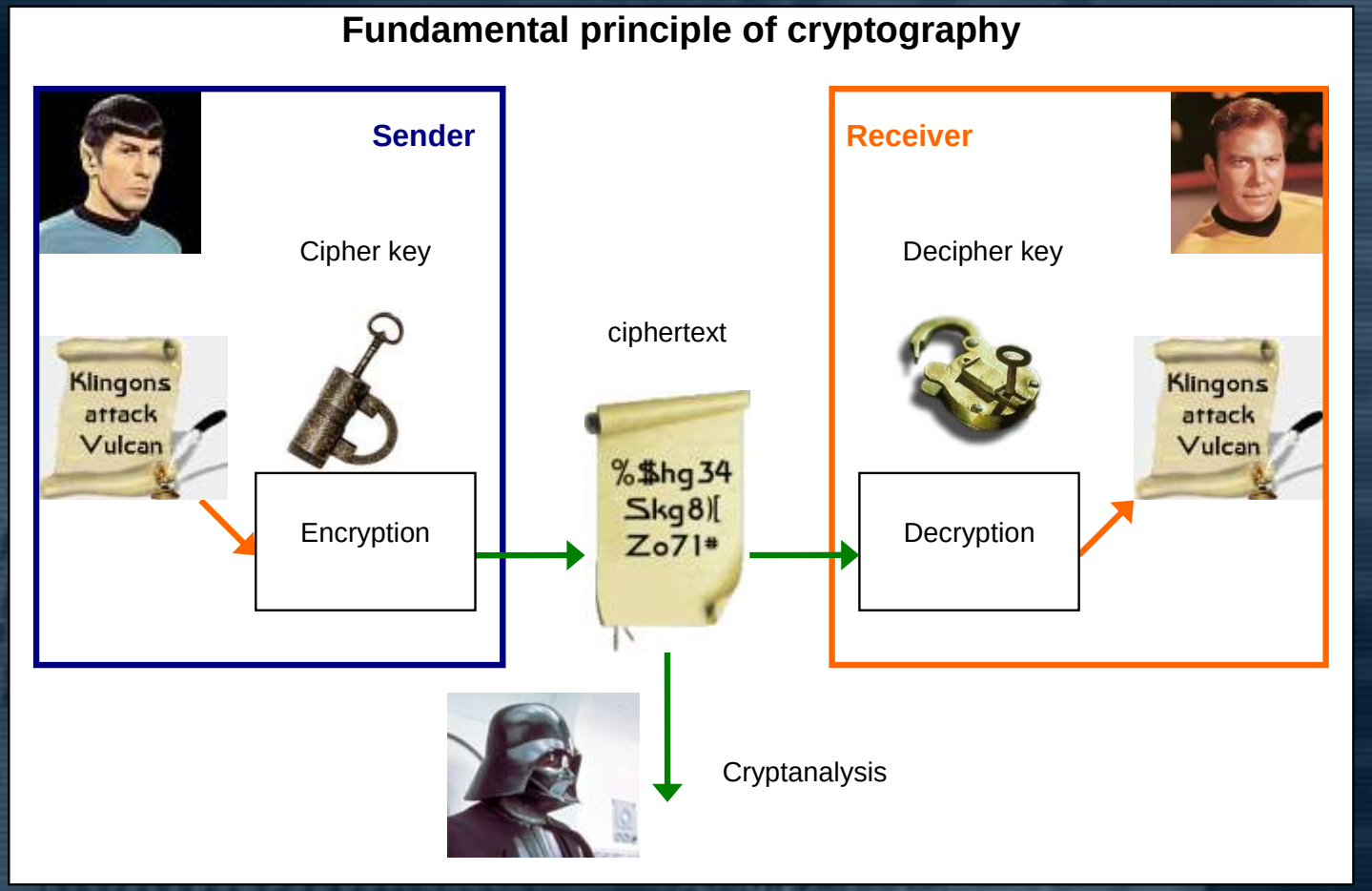
- More data are stored to allow a service



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

CRYPTOGRAPHY

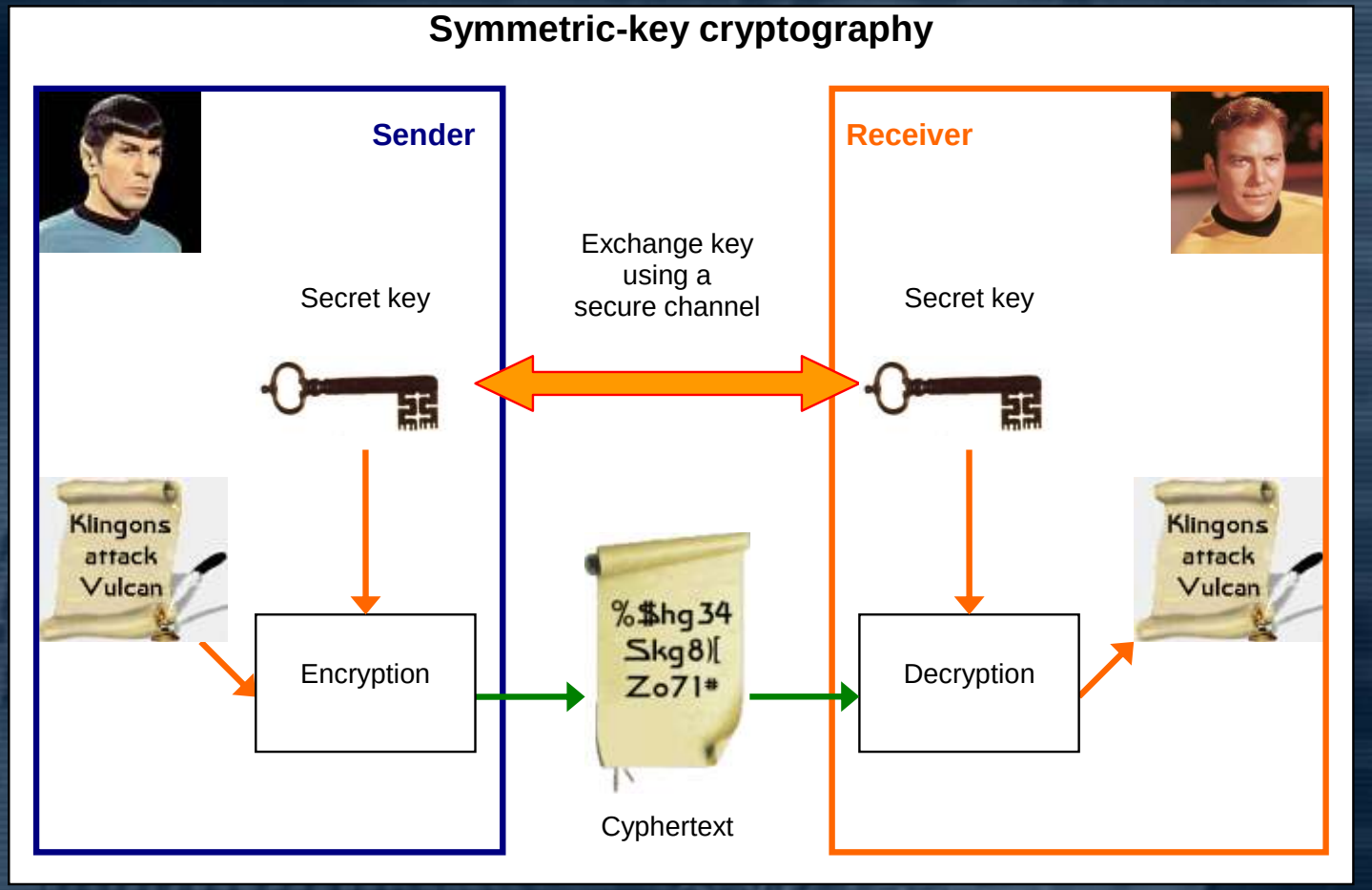
- **Some (secret) keys are needed to cypher the data**



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

SYMMETRICAL KEY

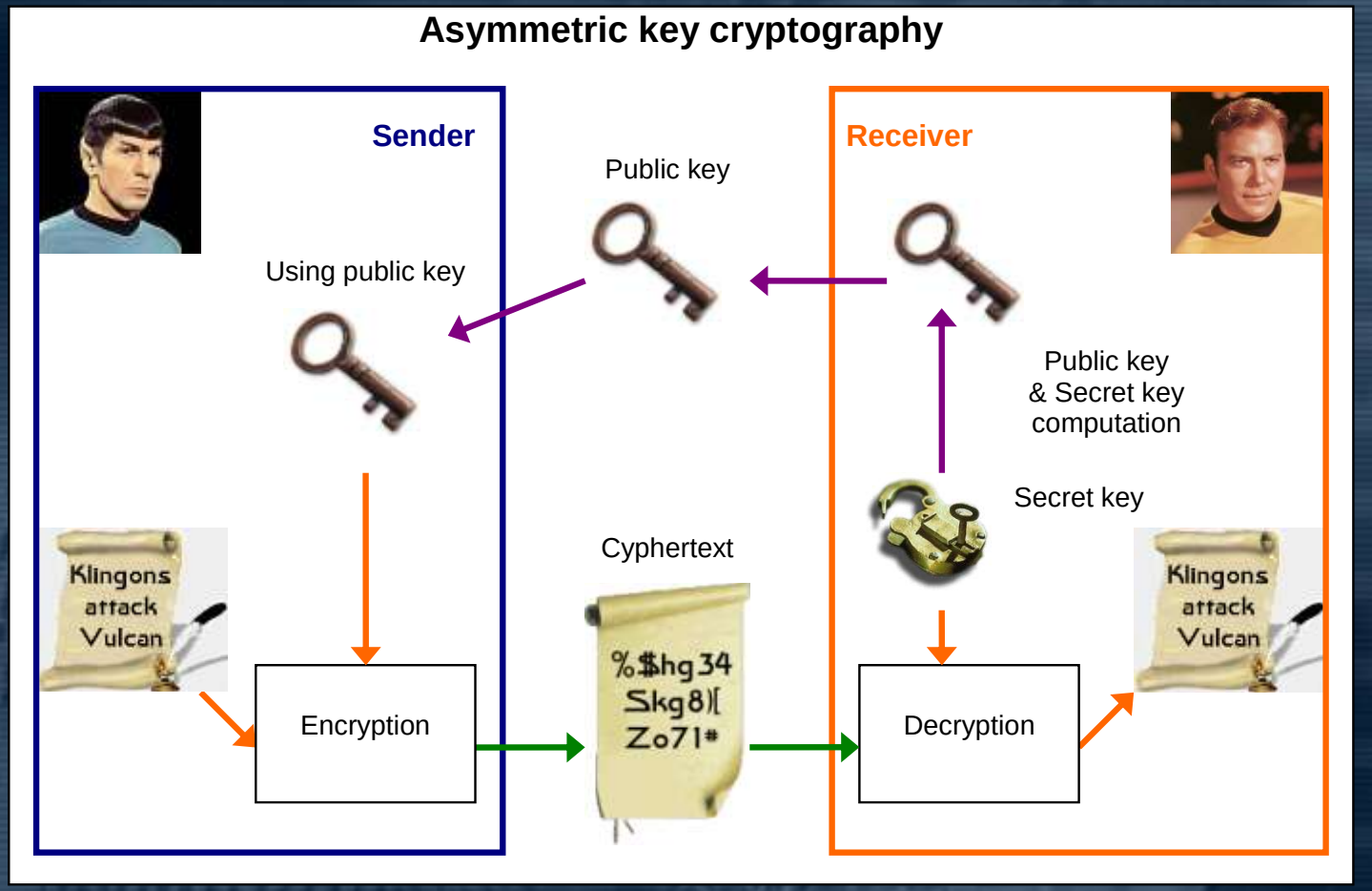
- **A secret is shared: it must be exchanged first**



THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

ASYMMETRICAL KEY

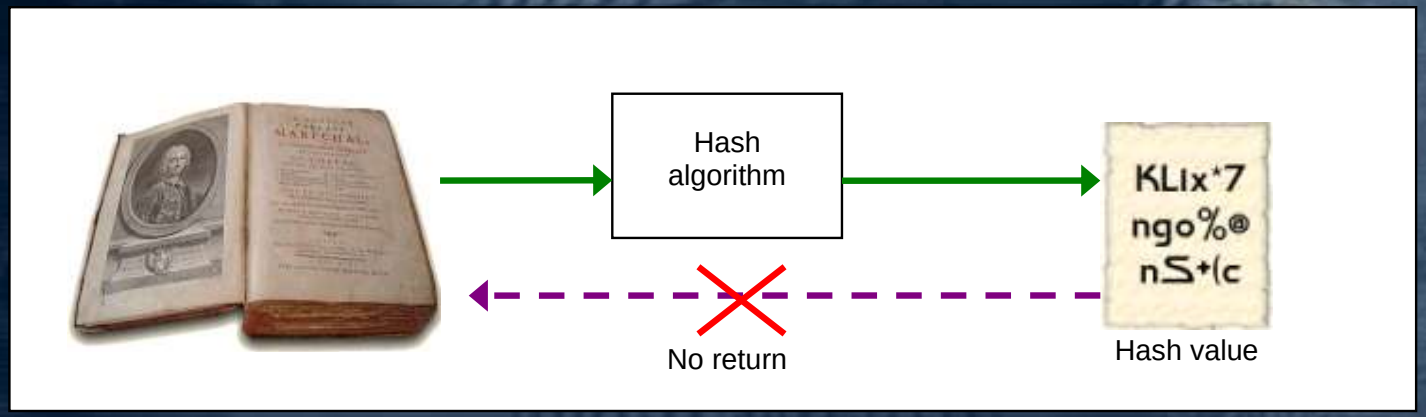
- **Public & secret keys**
- **Are you using the good key ?**
  → trusted third party



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

HASHING

- A unique number generated from data
- One bit of data changed
  → the unique number is changed « a lot »
- You cannot get back to the data from the number



THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

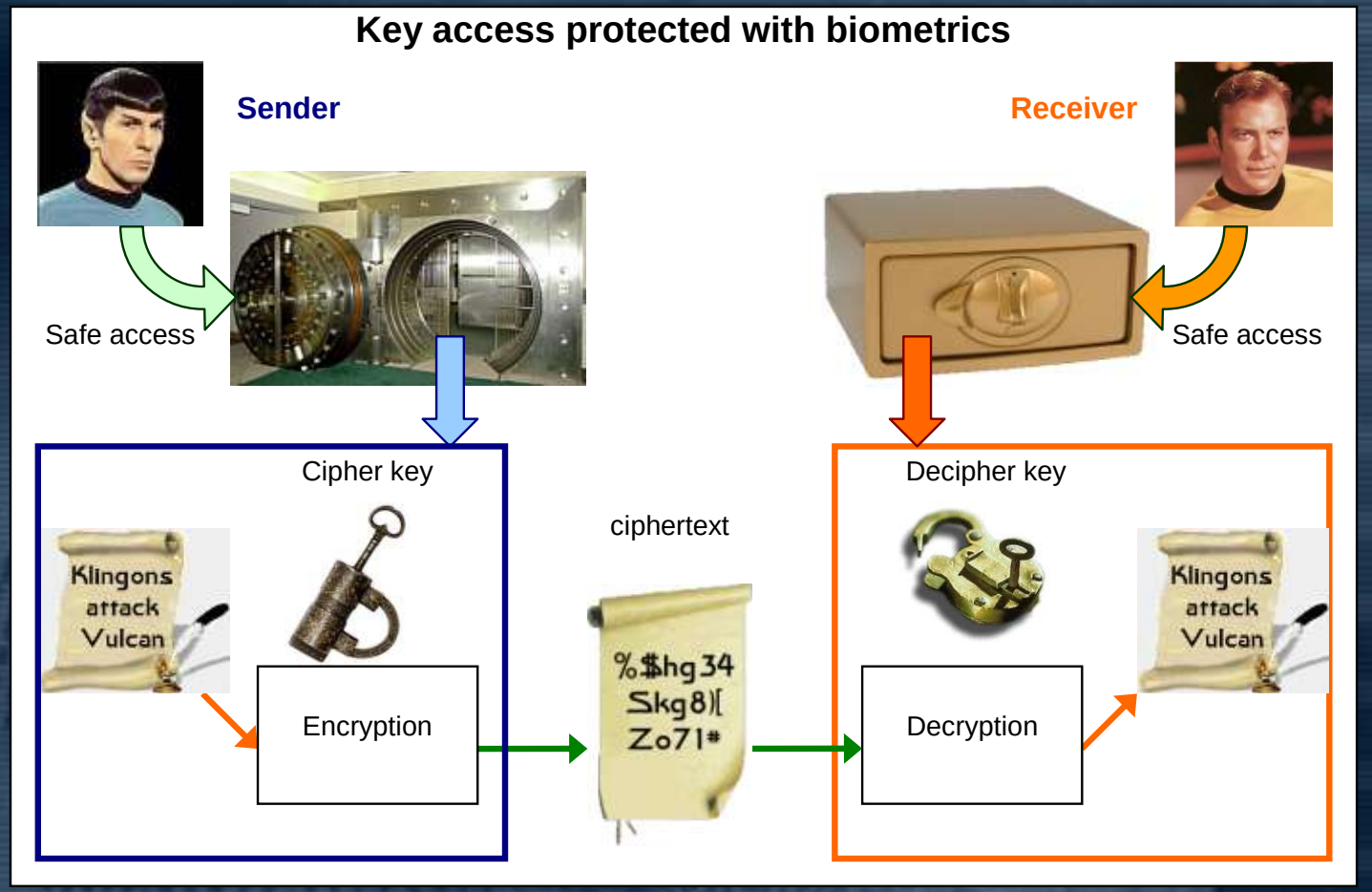
COMBINING

- Replacing the passwords to access keys
- Cyphering templates
- Hashing templates
- Intricated biometrics

THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

HOUSTON, WE'VE HAD A PROBLEM

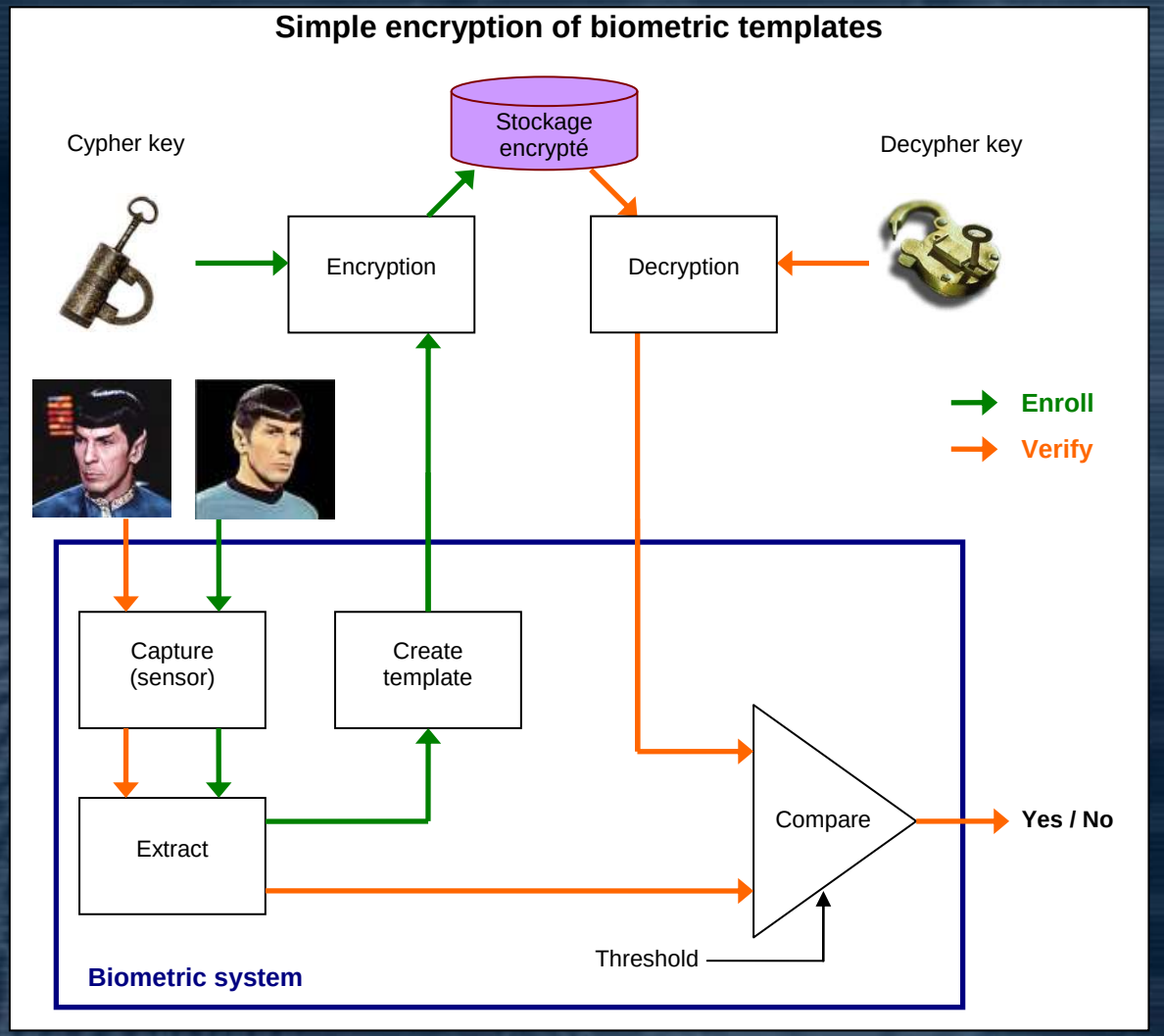
- **I need to protect my secret key**
  - Stored in a safe
  - Safe is biometrically protected
  - → protect my biometric template?
- **I need to protect my biometric template that opens the safe**
  - Cyphered with a secret key
  - I need the secret key to decipher the template so I can access the safe
  - So I cannot put the key inside the safe
  - → protect my secret key?



THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

CYPHERING TEMPLATES

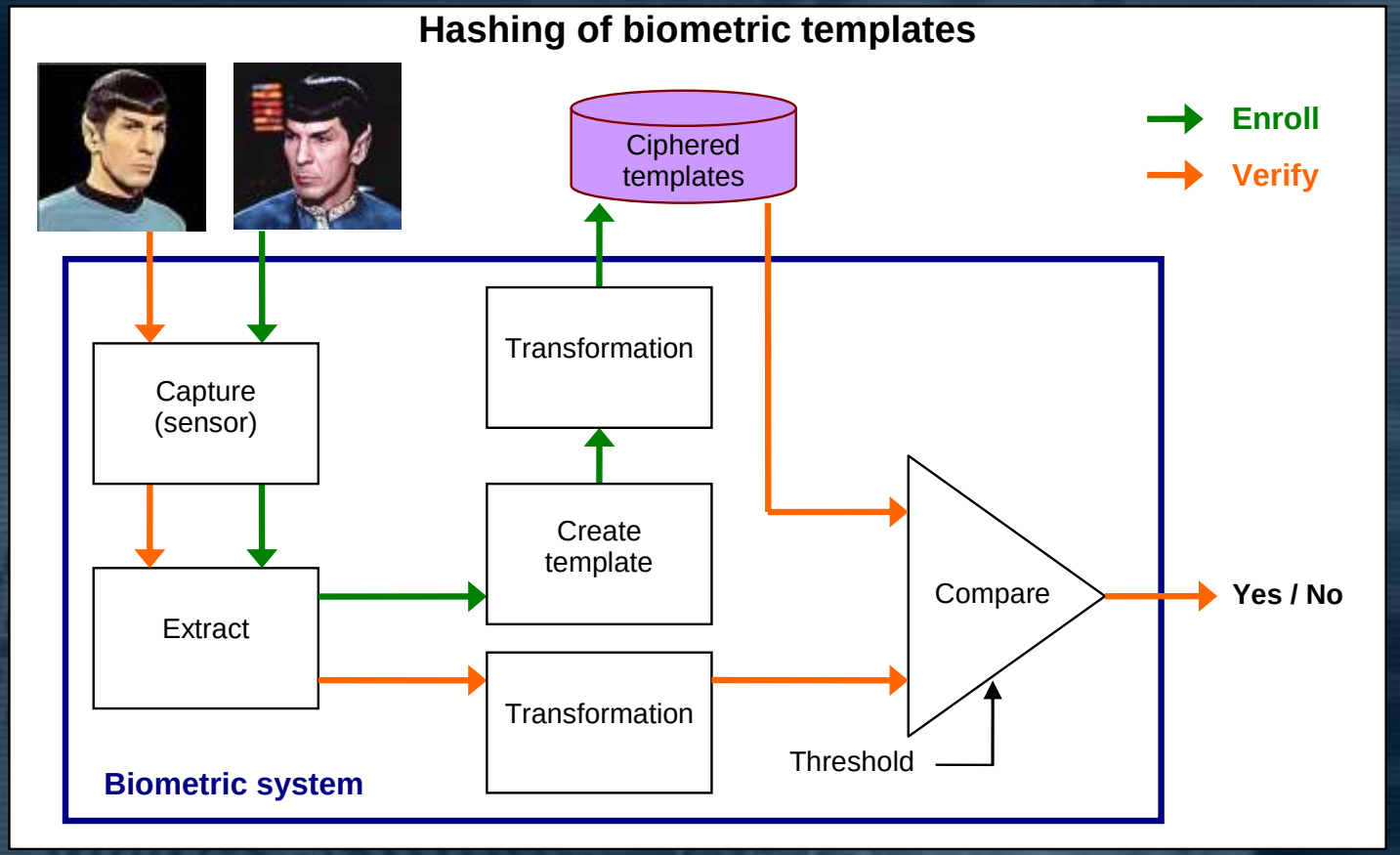
- Trying to cypher the template, to protect it, so nobody is able to modify/replace it.
- I don't know where to put my keys!



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

CANCELLABLE BIOMETRICS

- A transform is applied to the template
- Matching the cyphered template requires a specific comparison process
- If you know the transform, you can hack the system (replace Spock's template with Vador's template for instance)
- Cancellable = change the transform



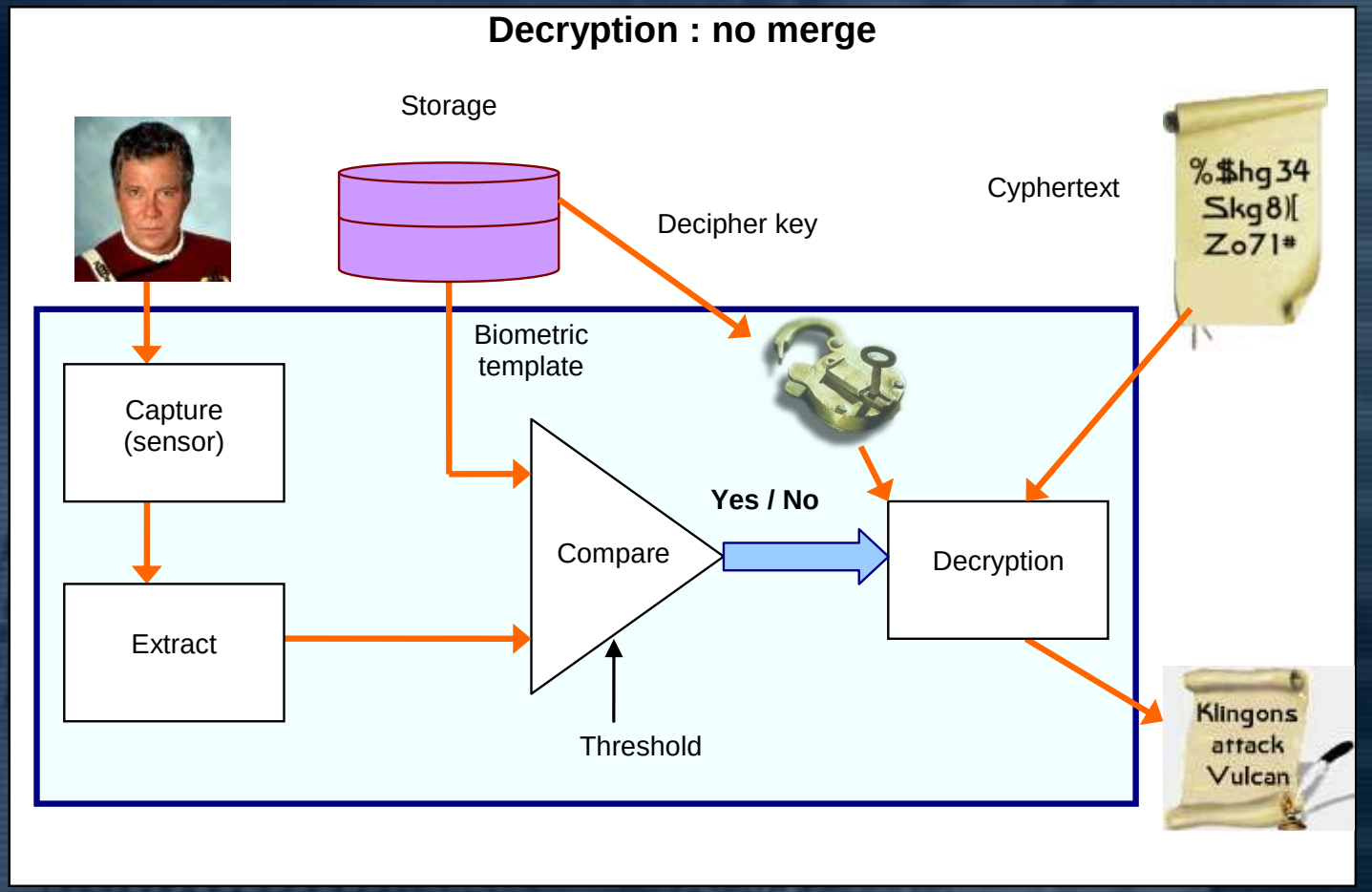
THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

TRYING TO MERGE

- No protection of the storage
- Biometric template in clear form
- Decipher key in clear form

- Weakness of comparison: entropy is 1 bit!

- Really bad! ☹ ☹ ☹



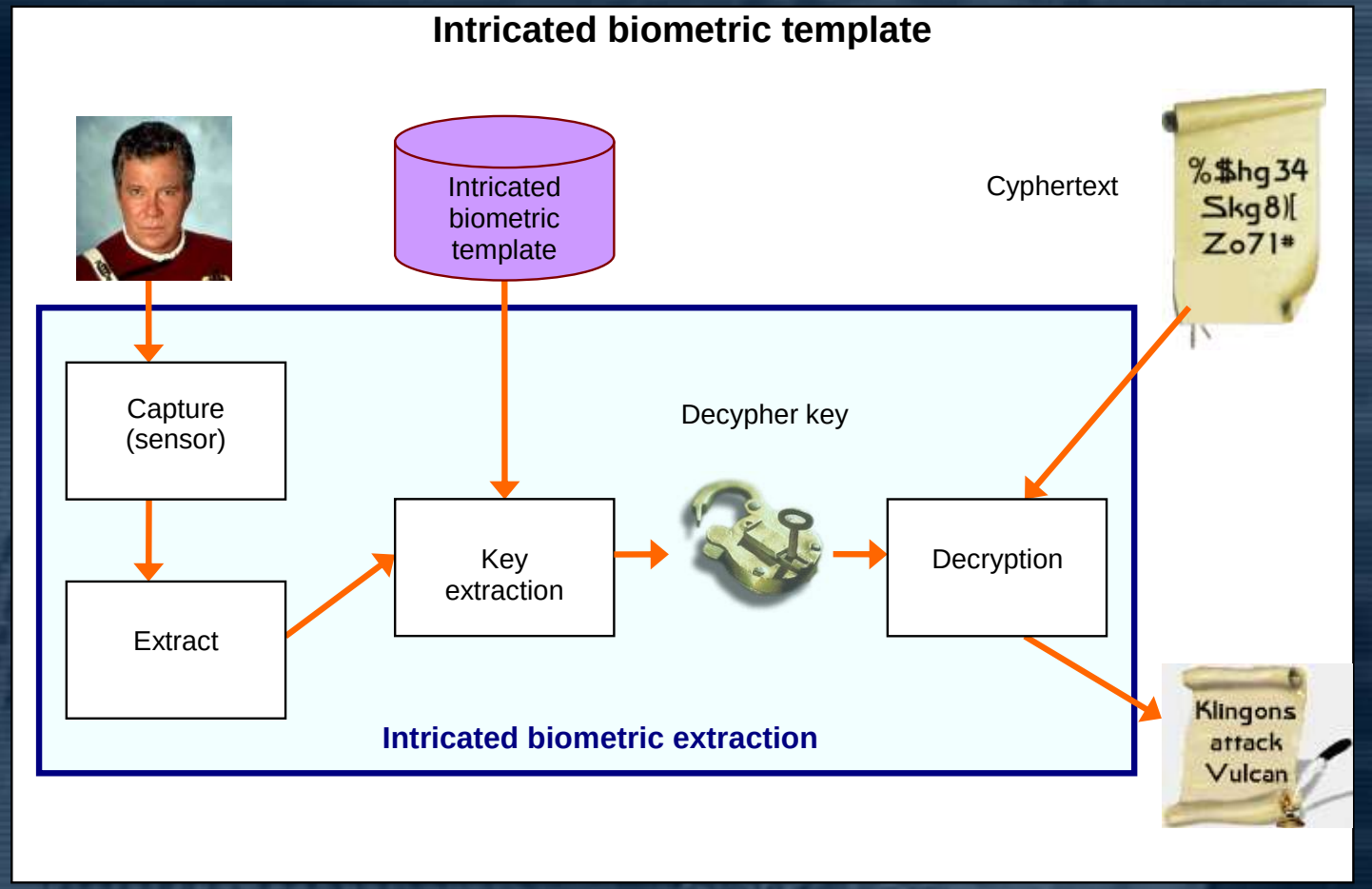
THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

WHAT WE WOULD LIKE

- Unreadable template
- Unreadable key

- No comparison
  → direct key extraction

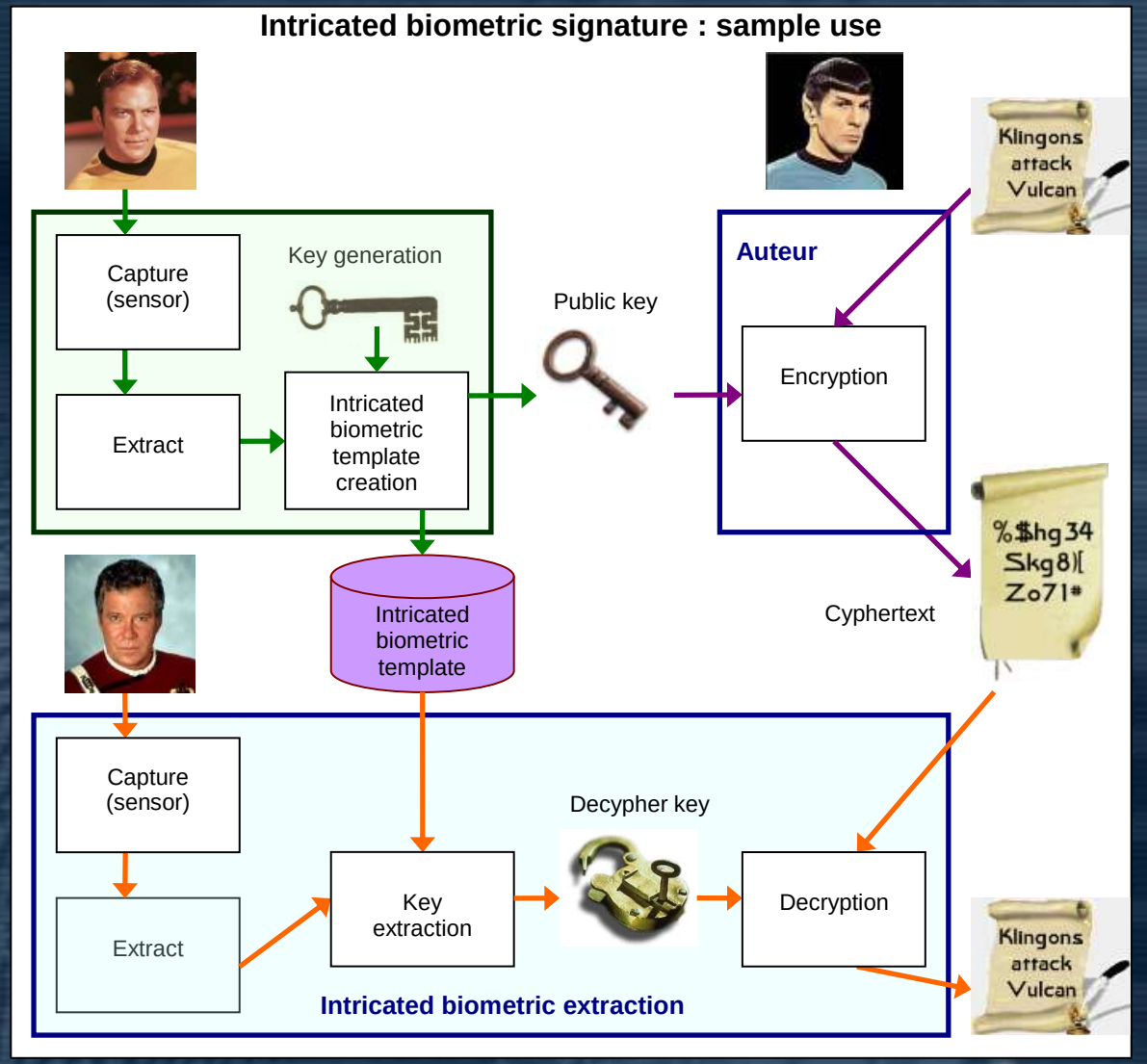
- Key appears only a short while in a safe place



THE BAD: IT DOESN'T ALWAYS WORK… CRYPTOGRAPHY

INTRICATION / ENTANGLEMENT

- Generation process:
- The decipher key is created a short while, intricated with the biometric template, and … destroyed ☺
- The public key is generated and published at the same time



THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

INTRICATION / ENTANGLEMENT

- One template per application
- If lost/compromised → revoked
- Impossible to merge databases
- Public signature → no database problems
- Not the right owner → wrong key is extracted, no usable data

- Is it possible ?

INTRICATION / ENTANGLEMENT : A SIMPLE EXAMPLE

Minutiae coordinates extraction

$(X_1,Y_1)\ (X_2,Y_2)\ \ldots\ \ldots\ (X_n,Y_n)$ — List of coordinates

Private / public key generation

A B C D E F … … N — Private key

Associate key & minutiae

$(X_1,Y_1,A)\ (X_2,Y_2,B)\ \ldots\ \ldots\ (X_n,Y_n,N)$ — Too easy to guess

Adding shaff points (voluntary bad points)
Mixing up

$(X_2,Y_2,B)\ (X_a,Y_a,Z)\ (X_b,Y_b,W)\ \ldots\ (X_n,Y_n,N)\ (X_c,Y_c,Z)\ (X_d,Y_d,U)\ \ldots\ (X_1,Y_1,A)\ (X_f,Y_f,V)$ — Intricated template

No order
Don't know which minutiae are good
Brute force unuseful if enough shaff points

THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY

(X_2,Y_2,B) (X_a,Y_a,Z) (X_b,Y_b,W) … (X_n,Y_n,N) (X_c,Y_c,Z) (X_d,Y_d,U) … (X_1,Y_1,A) (X_f,Y_f,V) Intricated template

Matching:
some minutiae matches, but not all.
Some may be wrong.

Live acquisition

Live minutiae coordinates extraction

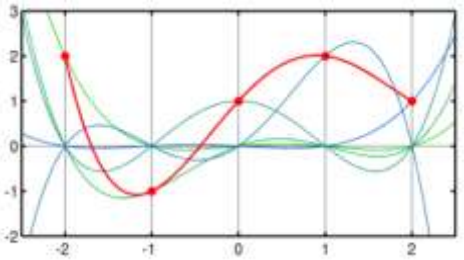
(X'_1,Y'_1) (X'_2,Y'_2) … … (X'_m,Y'_m)

Live list of coordinates

(X_2,Y_2,B) (X_1,Y_1,A) (X_c,Y_c,V)

Only a part of the secret key is found.

Lagrange polynomial
→ Only one solution will fit the points
→ Recovery of missing part, error elimination



A B C D E F … … N

If too much wrong minutiae, a wrong key is extracted, but no information will tell if it is correct or not!

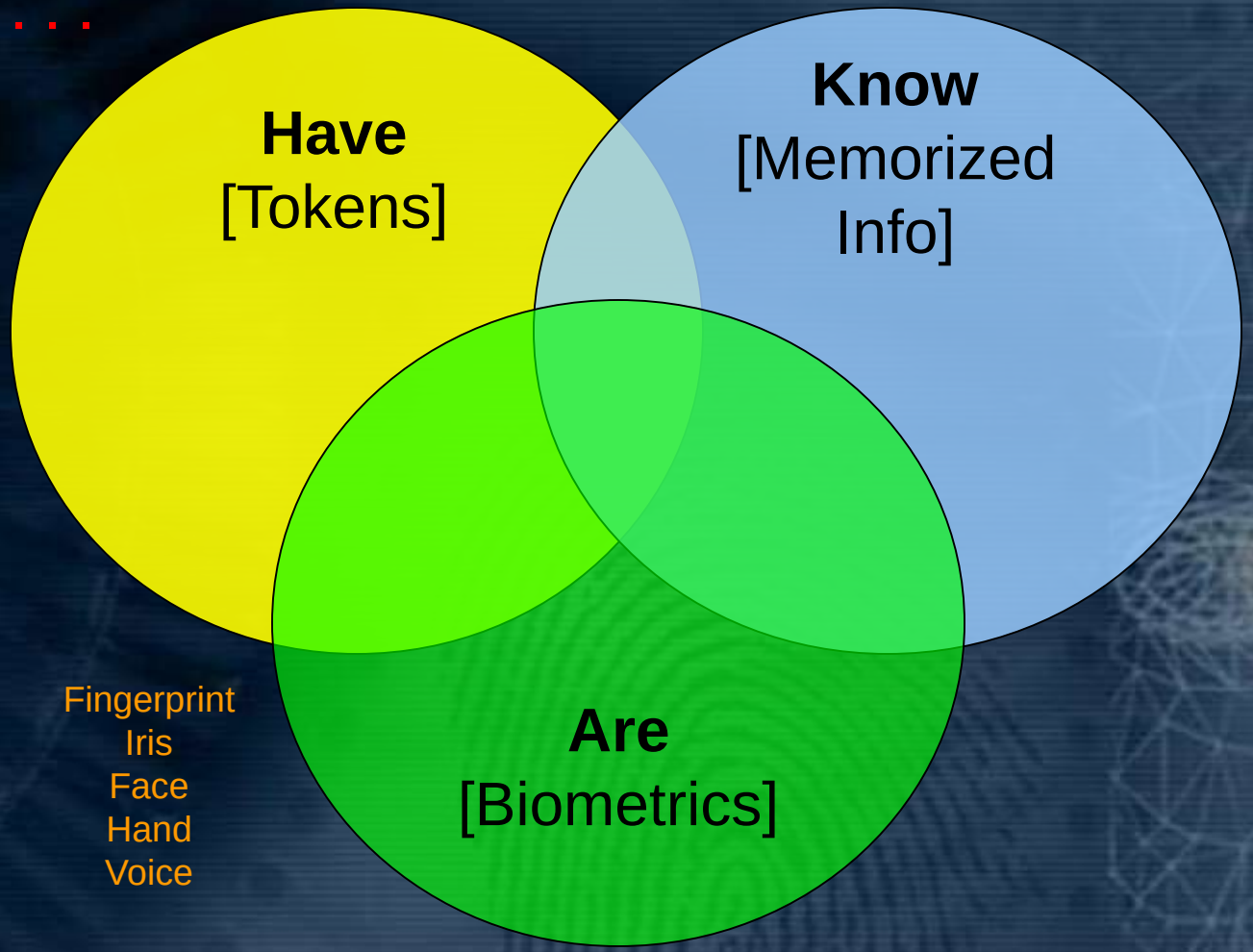
Not a demonstration!
Just a clue to say it should be feasible.

THE BAD: IT DOESN'T ALWAYS WORK…
CRYPTOGRAPHY : CONCLUSIONS

- **It is possible to create protected templates and keys**
  - But today, no proof exists
  - This is a full mathematical field to explore…
- **In the best case, a biometric system is using a (secret) key to protect the biometric template. The protection of the secret key is very often a real problem "put under the carpet"…**
- **Having intricated/entangled templates will be a deep change of the process**
  - Biometrics returns a service rather than a simple yes/no result
  - All data is public, all (temporary) secret data is destroyed just after the use
  - No problem with databases: everything is public, it is not possible to merge databases

THREE TIERS OF HUMAN AUTHENTICATION

Something you . . .



Passport
Documents
Driver's License
Photo ID
Physical keys
Encryption keys
Smart Cards
Badges

SSN
DOB
POB
Password
Passphrase
PIN
Secret

Fingerprint
Iris
Face
Hand
Voice

Used in various combinations, depending on the requirements of the particular application

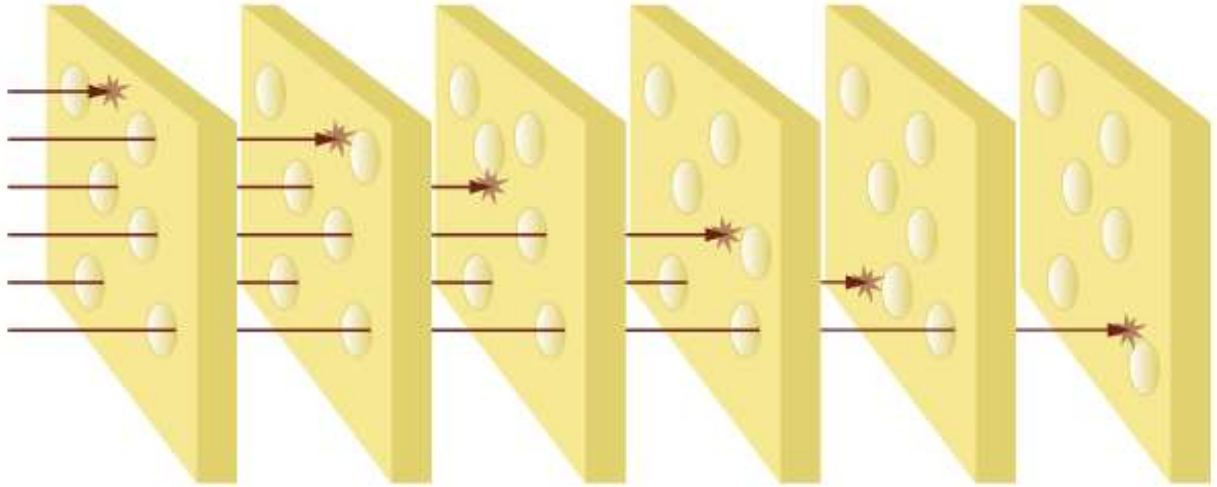
THE BAD: IT DOESN'T ALWAYS WORK… SECURITY

INCREASING SECURITY

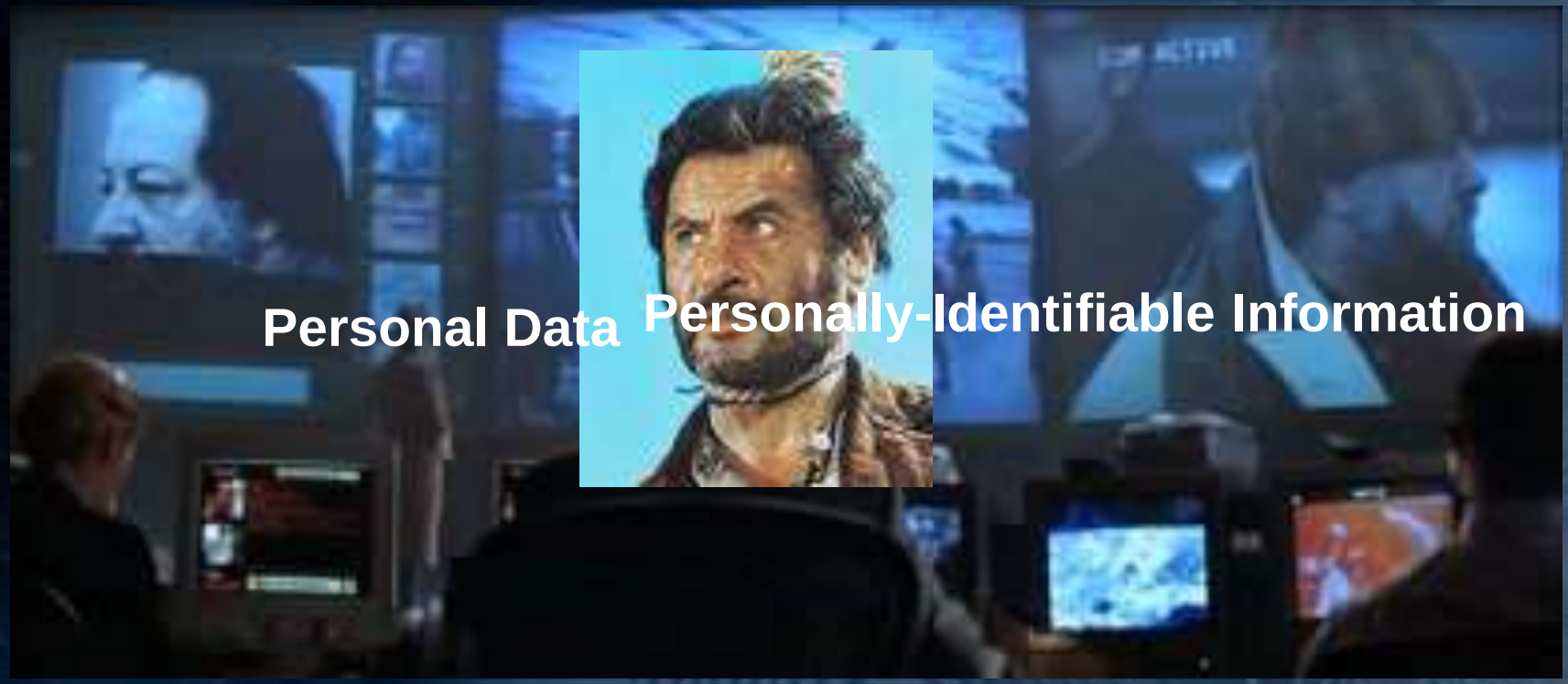
- **Combine Authentication Technologies to Enhance Security :**
  - You may require three fingerprints: it is more difficult to get three fake fingers than one
  - Layered biometrics: using face AND fingerprint AND iris
  - Add a token: a phone, a smart card (something you have)
  - Share a secret: a specific finger may be used as a silent alarm
  - Add a password (something you know)

CONCLUSION ABOUT SECURITY

- **100% secure is a myth.**
- **But — combining technologies will be very hard to deceive.**
  - The "Swiss cheese" model: each slice is not 100%; some holes exist.
  - More slices will stop most of threats.
  - But at the cost of each slice!



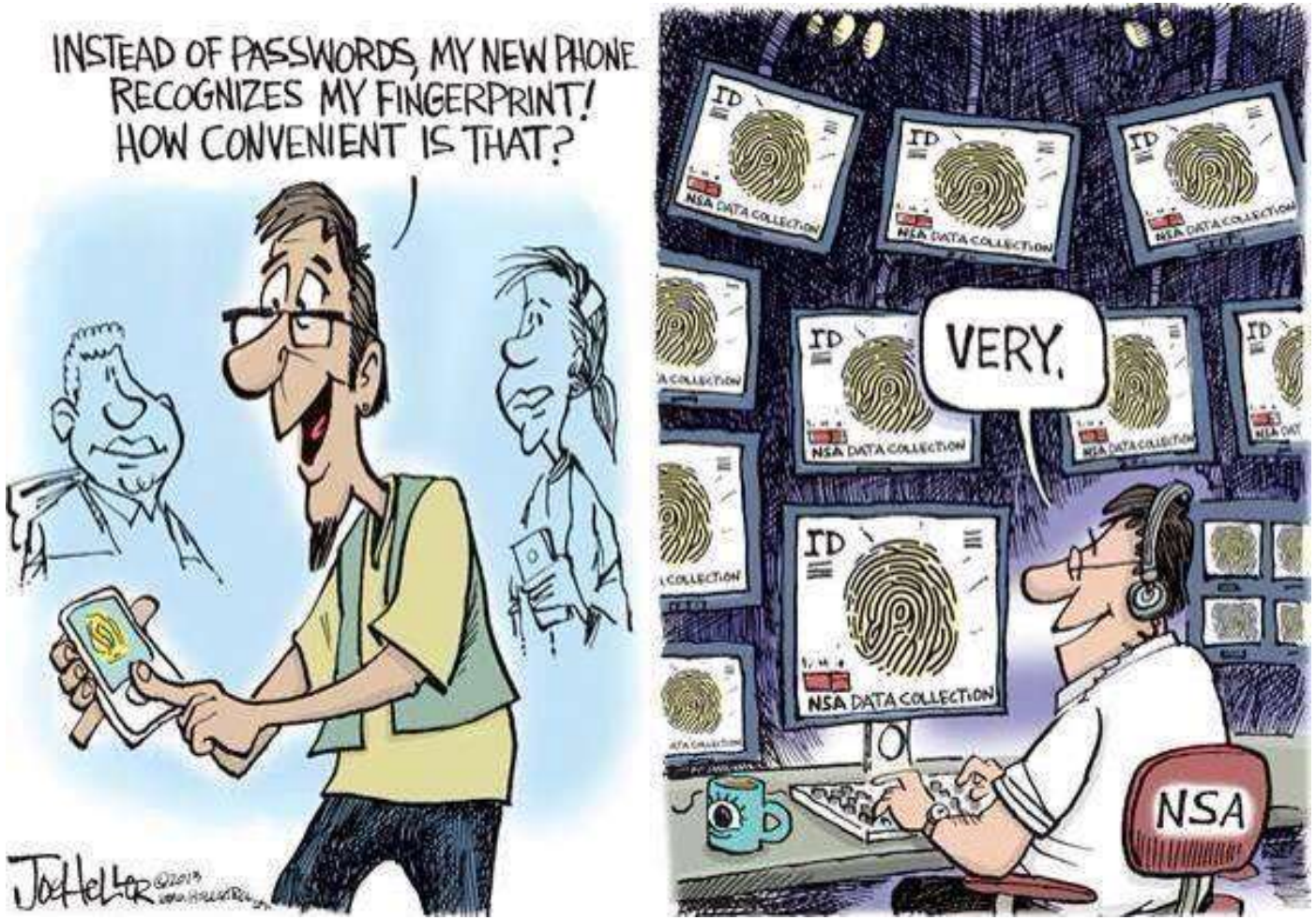
THE UGLY: PRIVACY



THE UGLY: PRIVACY

"This new Apple iPhone is great. It takes high quality pictures and recognizes my fingerprint. It's just like when I get arrested."

THE UGLY: PRIVACY



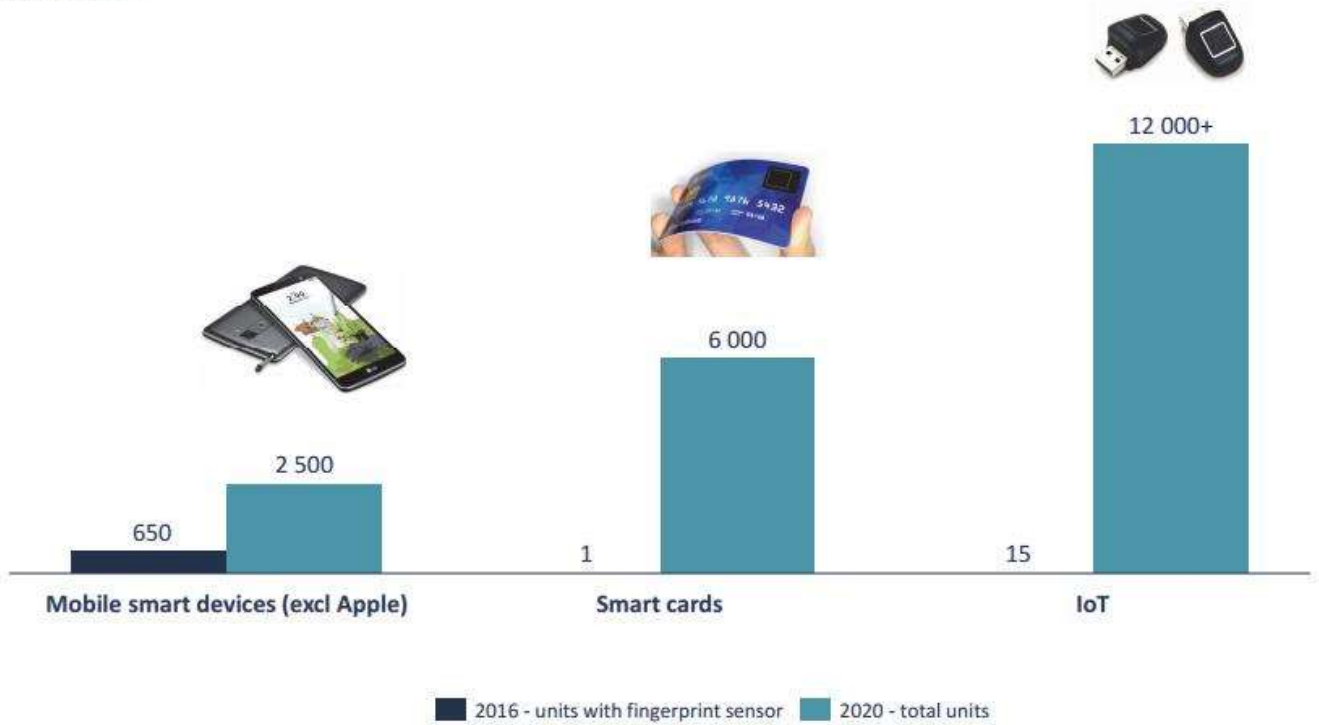
PRIVACY PROTECTION

- **Personal information**
  - Any information that could be used in any way to identify an individual
- **Biometric information is personal information**
- **A “privacy assessment” should be conducted any time biometric information/data will be used**
- **Privacy Assessments . . .**
  - Analyze the impact that the use of biometric data may have on an individual’s privacy
  - Ensure that biometric data will be used “appropriately”

Source: Privacy & Biometrics: Building a Conceptual Foundation
www.biometrics.gov/docs/privacy.pdf

DIFFICILE A PRÉDIRE LE FUTUR EST

Three massive markets – each with multi-billion unit potential in 2020
Million units



Source: Acuity Market Intelligence; Nilson Report; IHS; IDEX research

QUESTIONS ?

DE LA RECHERCHE À L'INDUSTRIE