GREYC

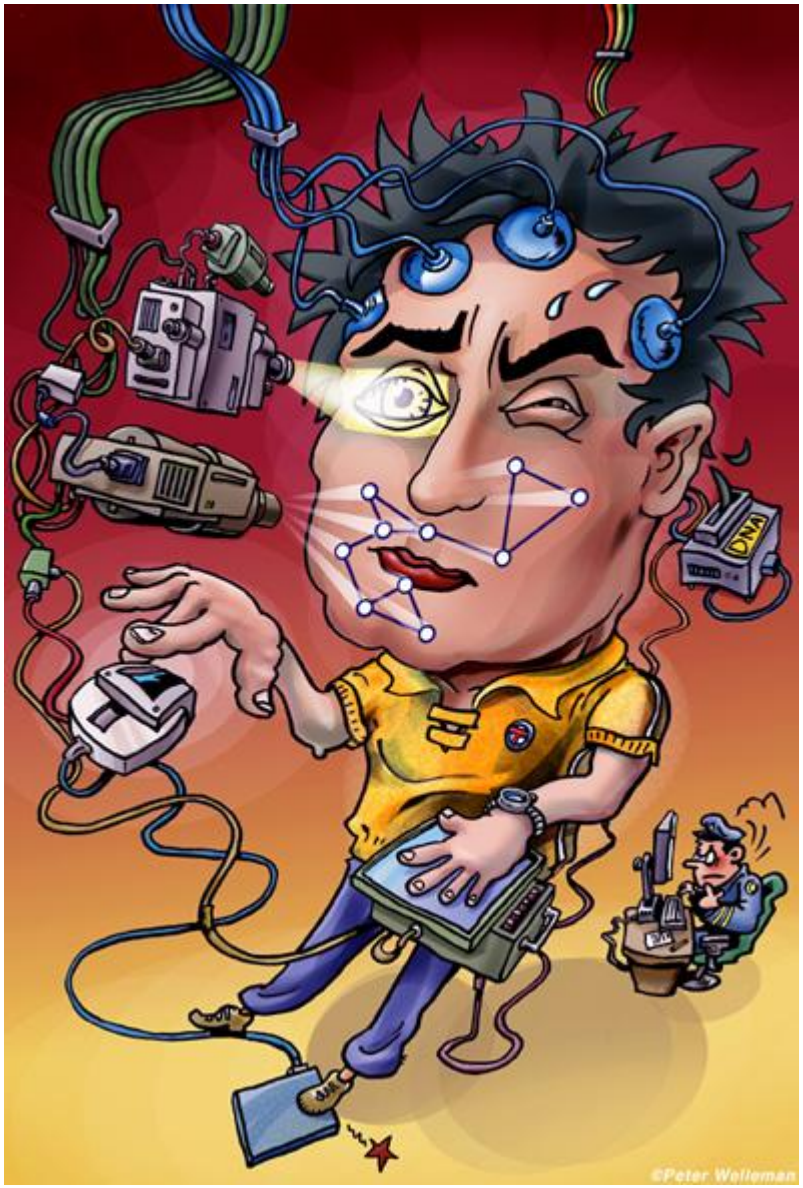
E-payment & Biometrics

Privacy compliant mobile biometric authentication

Christophe Rosenberger
GREYC Research Lab - France

cnrs UNICAEN université de Caen Basse-Normandie ENSICAEN

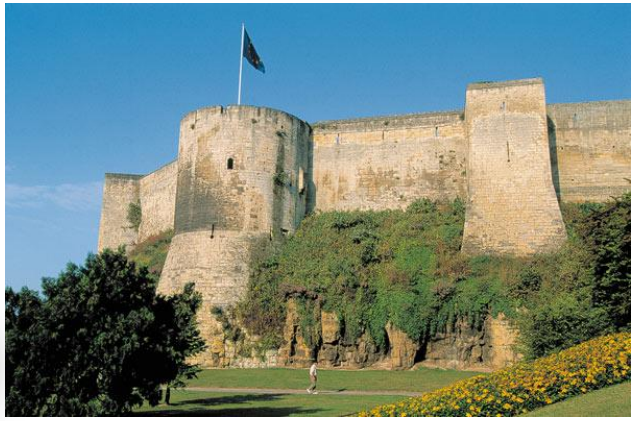
BIOMETRIC DESIGNER

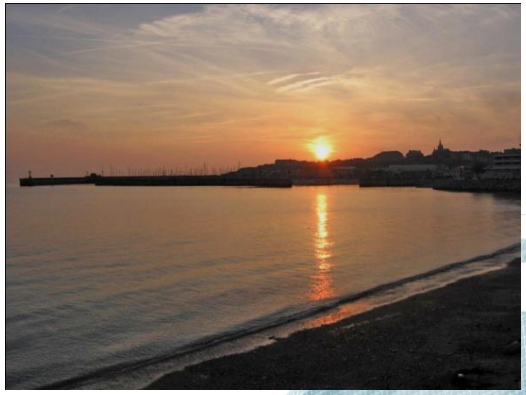


OUTLINE

- GREYC - E-payment & Biometrics
- Electronic transactions
- General definitions on biometrics
- Mobile biometric authentication
- Protection of biometric data
- Perspectives

GREYC Research Lab





GREYC Research Lab

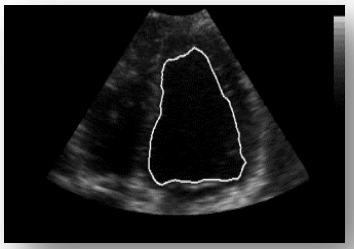
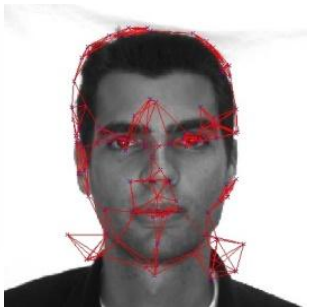
Research Group in Computer science, Automatics, Image processing and Electronics of Caen

Laboratory staff:

- 7 CNRS researchers
- 25 Full professors
- 18 Associate professors
- 48 Assistant professors
- 79 PhD students
- 17 permanent staff
- 30 Engineers and post-doc

Research topics:

- Electronics
- Image processing
- Algorithmic
- Document analysis
- Multi-agents
- Robotics navigation
- Automatics
- Computer security
- Natural language processing
- Biometrics
- Cryptography

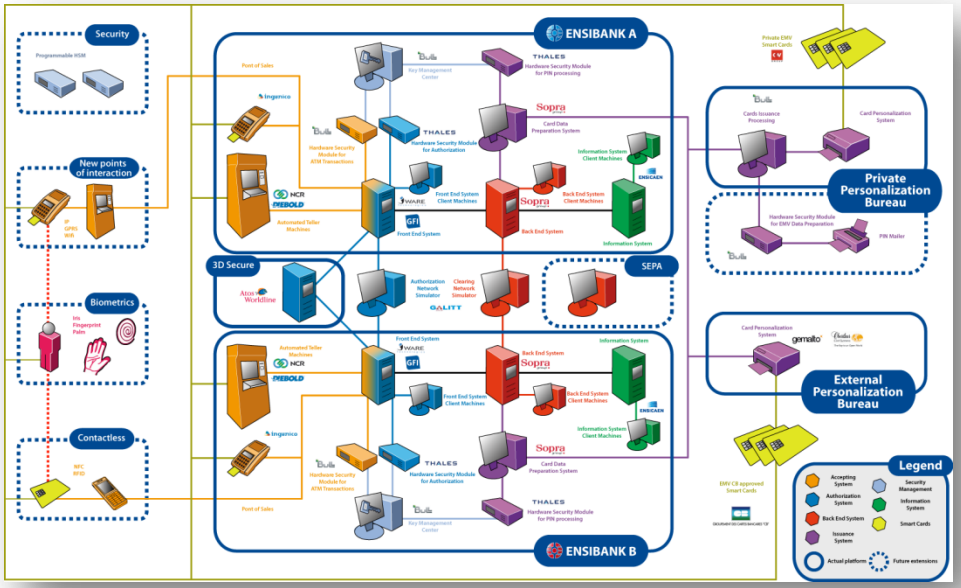
E-payment & Biometrics

Members (29):
3 full professors, 2 associate professors, 4 assistant professors, 4 permanent engineers, 8 PhD students, 2 Post-docs, 6 engineers.

Research topics (2): Biometrics and Trust

Application: E-payment

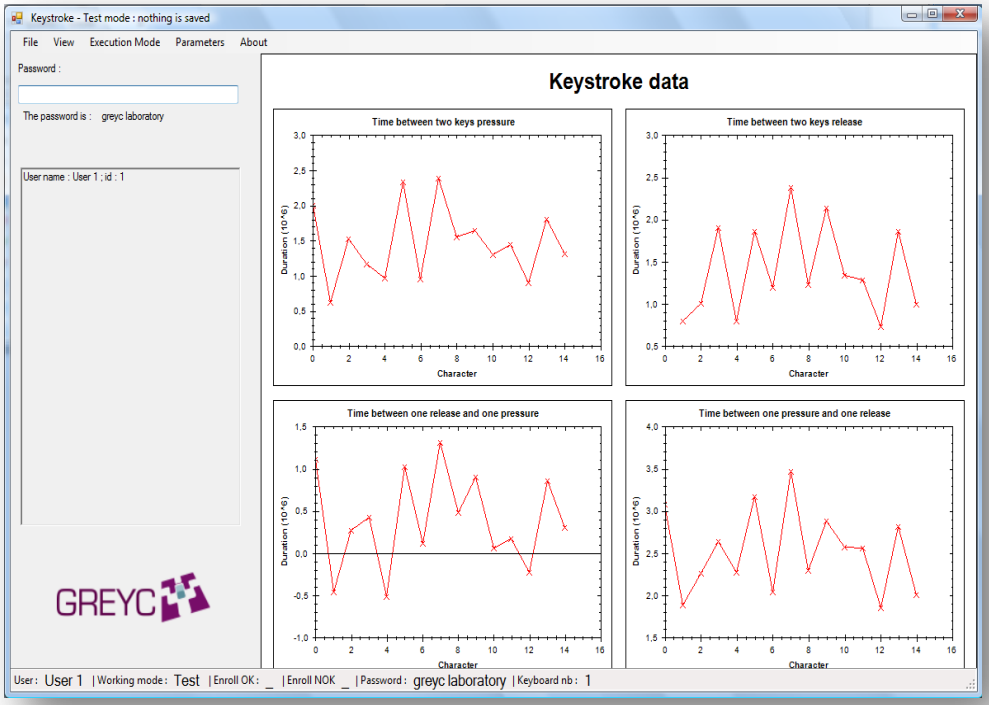
Research projects: ASAP(ANR), LYRICS(ANR), PAY2YOU(FUI), CAPI(FUI), ADS+(FUI), INOSSEM(GE), LUCIDMAN(EUREKA)



E-payment & Biometrics

Biometrics: Operational authentication that respects the privacy of users

- ❑ Biometric authentication (palm veins, keystroke dynamics…)
- ❑ Evaluation of biometric systems (usability, security…)
- ❑ Protection of biometrics (cancelable biometrics, smartcards…)



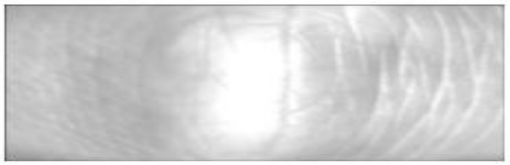
GREYC Keystroke
Keystroke dynamics authentication

pôle TES
e-secure transactions

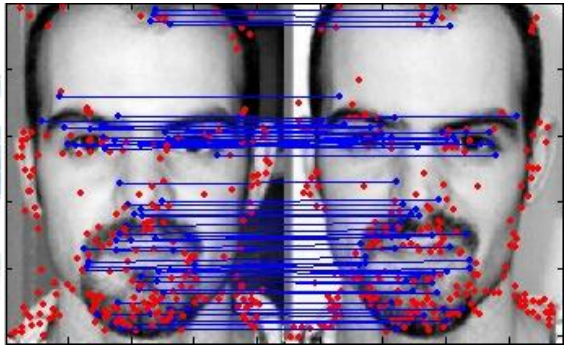
E-payment & Biometrics

Biometric systems:

Iris



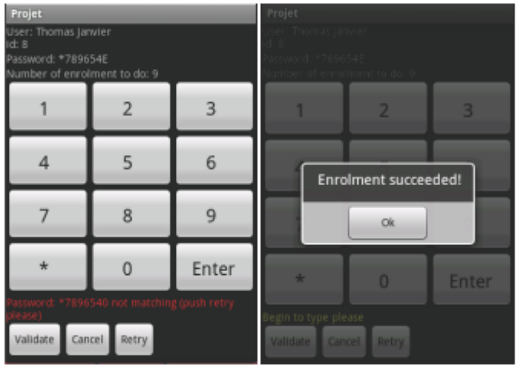
Finger Knuckle Print



Face

Keystroke dynamics

Signature dynamics

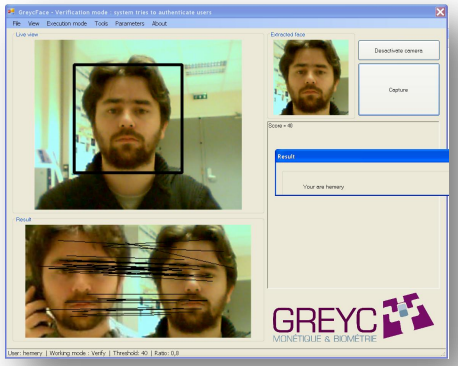


Touch screen interaction

Hand shape, palm vein

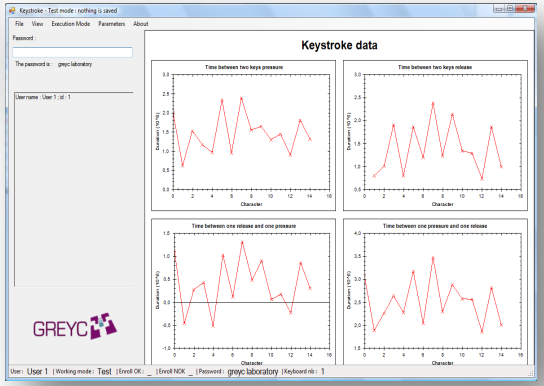
Fingerprint

Softwares

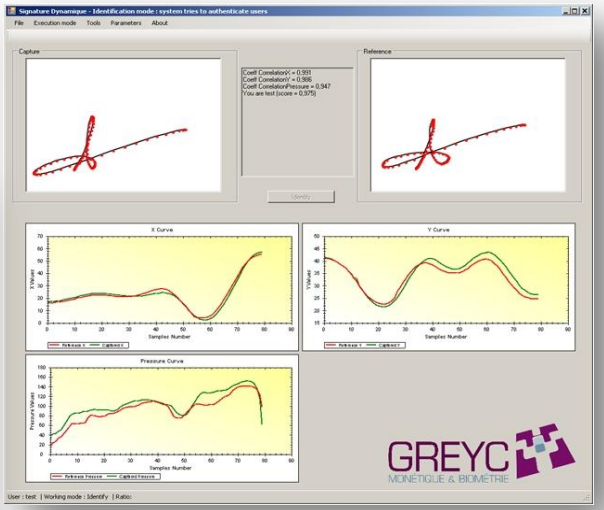


GREYC Face

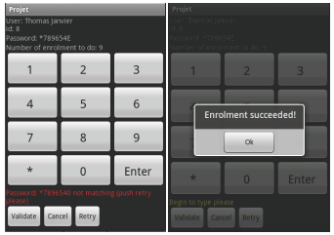
GREYC Iris



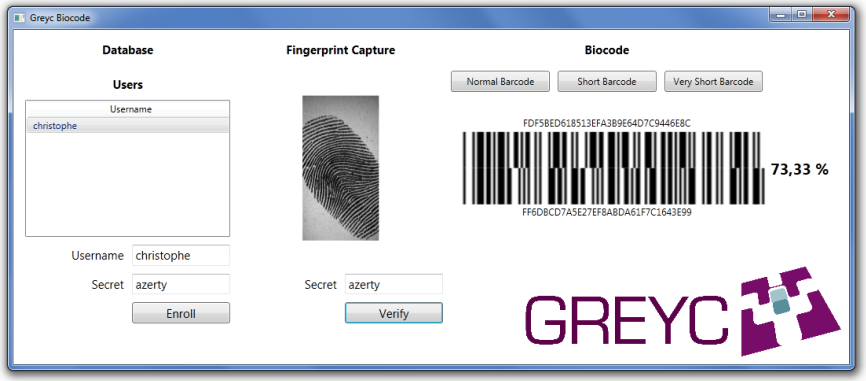
GREYC keytroke



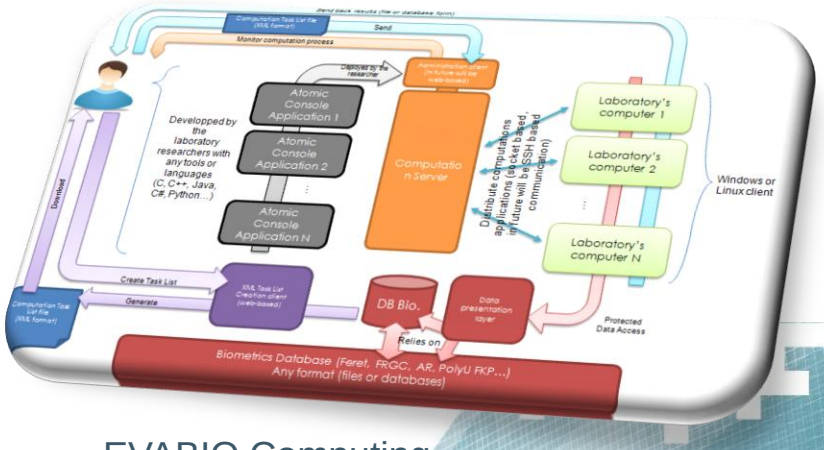
GREYC Signature



Android GREYC Interaction



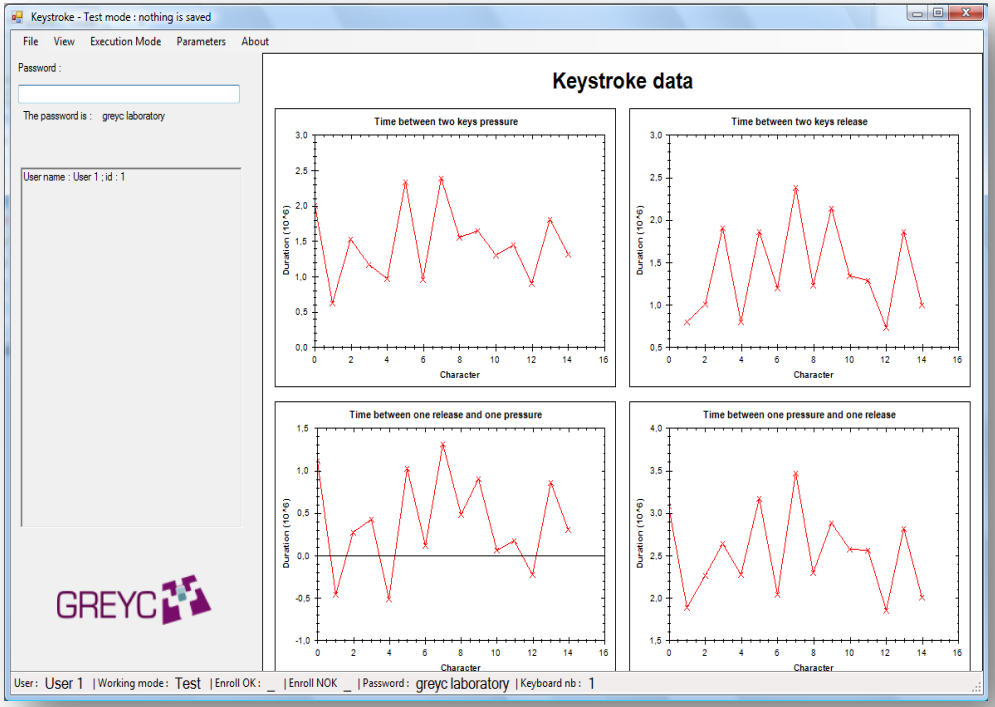
GREYC BioCode



EVABIO Computing

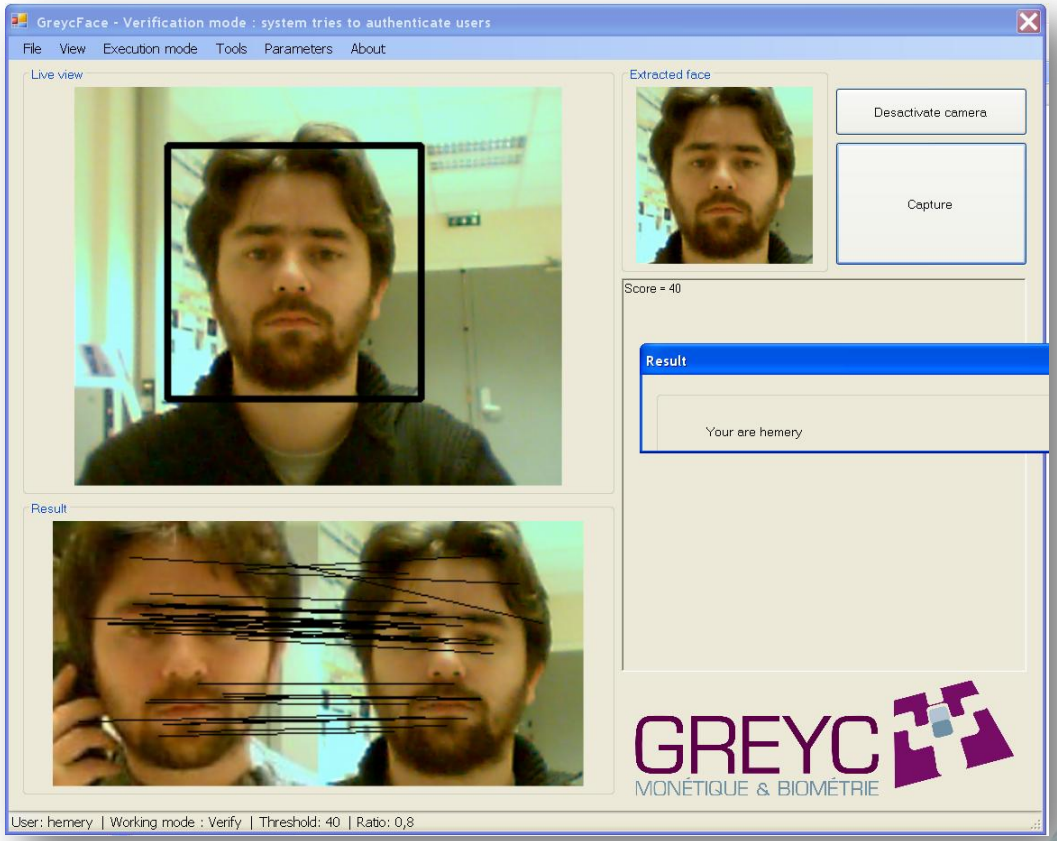
Softwares

DEMO



Softwares

DEMO



One funny thing

Gender recognition with keystroke dynamics:

Experiments on a dataset composed of 133 users

Use of a passphrase « Greyc laboratory »
Gender recognition: **~90%** (based on SVM learning)

Classical keystroke recognition: EER = 10.6%
Keystroke recognition (gender recognition): EER = 7.6%

Recent work on free text
Gender recognition: **~80%** (if using many sentences)

R. Giot, C. Rosenberger, "A New Soft Biometric Approach For Keystroke Dynamics Based On Gender Recognition" International Journal of Information Technology and Management (IJITM) Special Issue on : "Advances and Trends in Biometrics". Dr Lidong Wang, pages 1-16, 2011.

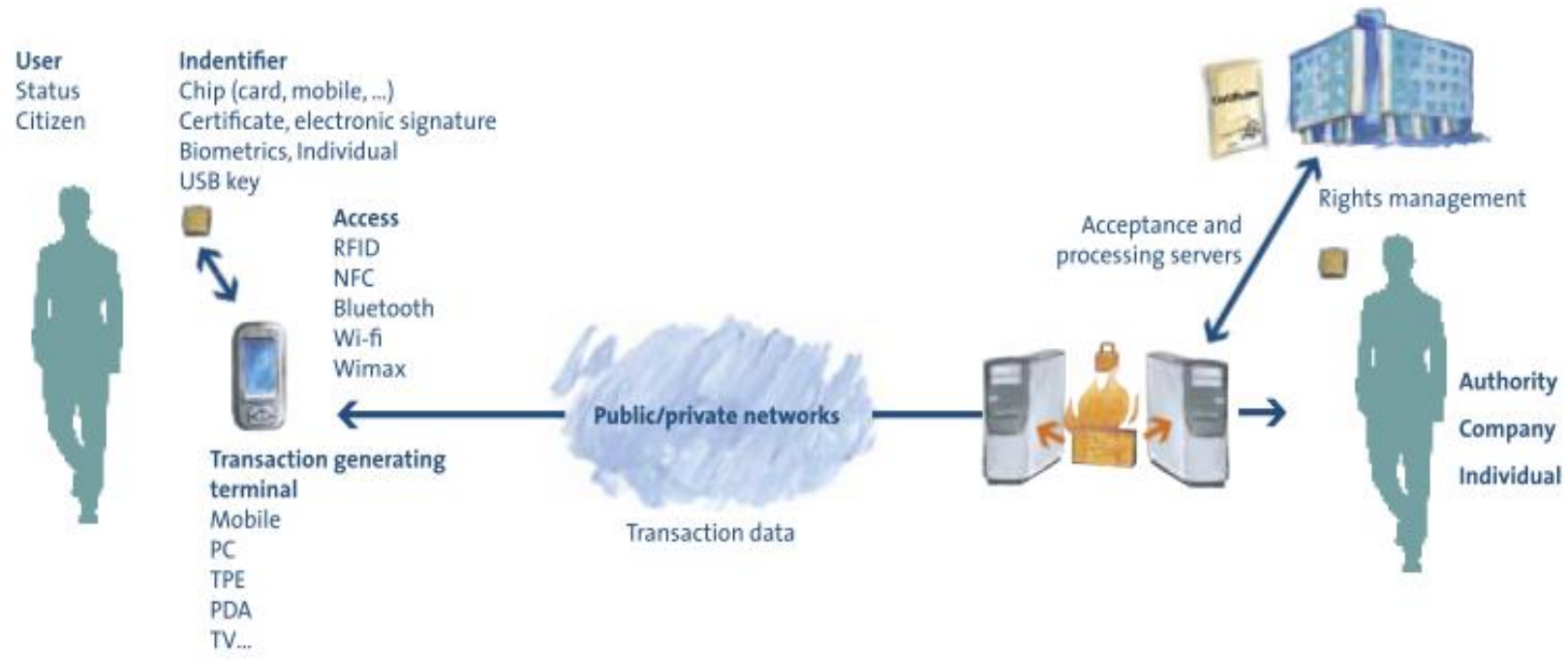
OUTLINE

- GREYC - E-payment & Biometrics
- Electronic transactions
- General definitions on biometrics
- Mobile biometric authentication
- Protection of biometric data
- Perspectives

Electronic transactions

E-Secure transactions

Different technologies are combined



E-transactions (© E-secure Transactions Cluster)

Electronic transactions

Terminal for the transaction

More and more mobile terminals

Electronic transactions

Infrastructure of an E-Secure transaction

Trust in an e-transaction depends on many factors.

E-transactions (© E-secure Transactions Cluster)

Electronic transactions

User authentication:

Security and privacy properties:

- Confidentiality
- Integrity
- Non repudiation
- Authentication

- Unlinkability
- Revocability

Electronic transactions

GREYC

User authentication:

Authentication methods are based on:

- We know [Secret]
- We own [Token, smartcard, RFID tag]
- We Are [Biometrics]
- The way we do things [Behavioral biometrics]
- The use of a reliable third party [Relationship]

They are called authentication factors.

Electronic transactions

Authentication process:

To authenticate himself, a user provides in general two elements:

- its login;
- one or multiple authentication elements.

Electronic transactions

GREYC

Static passwords:

Username and password authentication is the most used method.

Simple, robust, even rustic, his biggest flaw is that the level of security depends directly on the complexity of the password.

Simple passwords are weak, and too complex passwords bring users to implement strategies to remember them: Post-it list, in an Excel file or in the smart phone ...

A password is called static (vs. dynamic) when it does not change from one transaction to another.

Electronic transactions

Password complexity index: passwordmeter.com

Test Your Password		Minimum Requirements
Password:	•••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	34%	
Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 2
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

- **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
- **Sufficient:** Meets minimum standards. Additional bonuses are applied.
- **Warning:** Advisory against employing bad practices. Overall score is reduced.
- **Failure:** Does not meet the minimum standards. Overall score is reduced.

Quick Footnotes

- **Flat:** Rates that add/remove in non-changing increments.
- **Incr:** Rates that add/remove in adjusting increments.
- **Cond:** Rates that add/remove depending on additional factors.
- **Comp:** Rates that are too complex to summarize. See source code for details.
- **n:** Refers to the total number of occurrences.
- **len:** Refers to the total password length.
- Additional bonus scores are given for increased character variety.
- Final score is a cumulative result of all bonuses minus deductions.
- Final score is capped with a minimum of 0 and a maximum of 100.
- Score and Complexity ratings are not conditional on meeting minimum requirements.

DISCLAIMER

This application is designed to assess the strength of password strings. The instantaneous visual feedback provides the user a means to improve the strength of their passwords, with a hard focus on breaking the typical bad habits of faulty password formulation. Since no official weighting system exists, we created our own formulas to assess the overall strength of a given password. Please note, that this application does not utilize the typical "days-to-crack" approach for strength determination. We have found that particular system to be severely lacking and unreliable for real-world scenarios. This application is neither perfect nor foolproof, and should only be utilized as a loose guide in determining methods for improving the password creation process.

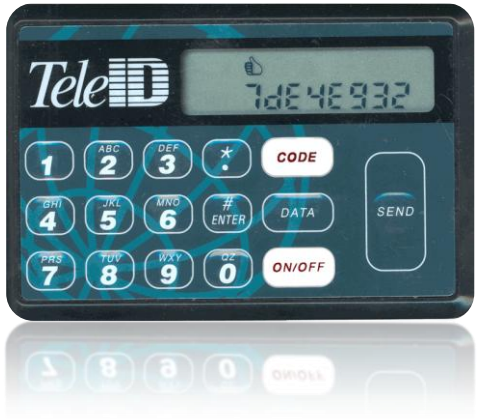
Download Password Meter Package

Electronic transactions

One time passwords:

Calculators using a challenge

This type of calculator is based on the principle of question-answer (challenge-response). The authentication server sends to the user a question (challenge). The user types the number on the keyboard integrated into the calculator. The calculator then calculates an answer to this question, i.e. an OTP (response).



Electronic transactions

Certificates:

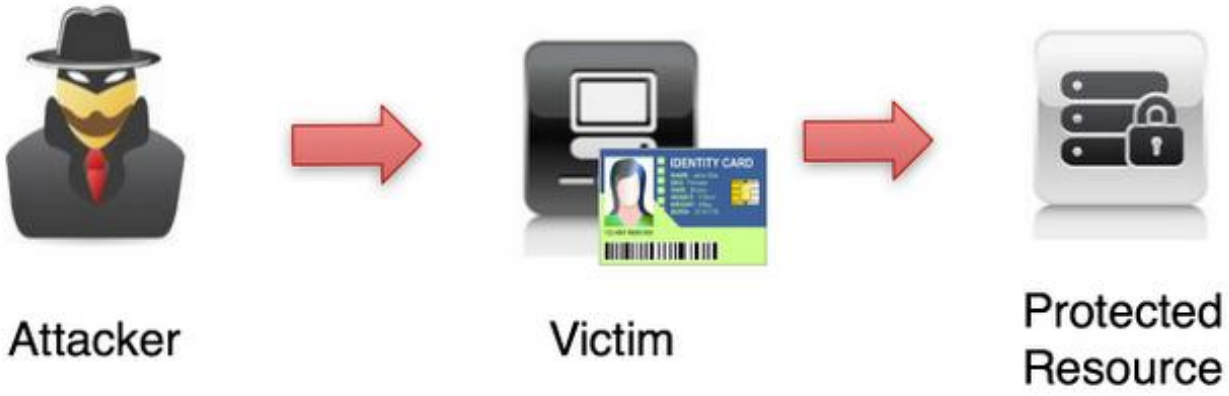
X.509 certificates are implementing an advanced encryption technology that can encrypt or sign messages without having to share a secret.

The identifier is a public certificate that is signed and thus guaranteed by a recognized certification authority. The user must provide a secret to use different cryptographic elements.

Electronic transactions

Limitations:

- More related to machine authentication
- Not so difficult to attack
- No real relationship between the user and its authenticator



Electronic transactions

Biometrics :

- The only **one** authentication method using an authenticator related to the user

OUTLINE

- GREYC - E-payment & Biometrics
- Electronic transactions
- General definitions on biometrics
- Mobile biometric authentication
- Protection of biometric data
- Perspectives

Biometrics

GREYC

Properties

A biometric information must comply with the following properties:

- **Universality**: All individuals can be characterized by this information;
- **Uniqueness**: This information must be as different as possible for two different individuals;
- **Permanence**: It should not change during the life of the individual;
- **Collectability**: It must be measured easily;
- **Acceptability**: Users must be willing to give this information.

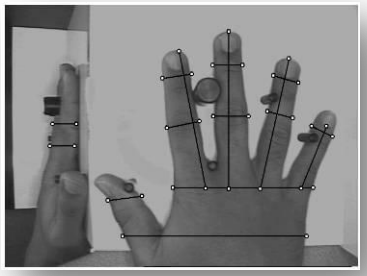
Biometrics

GREYC

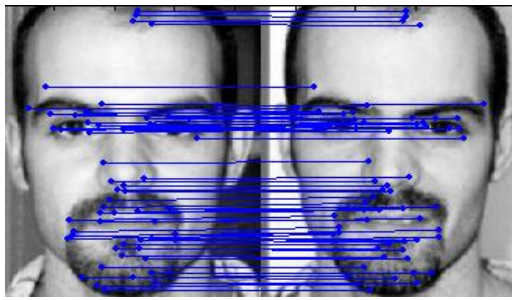
Biometric modalities:

- **Biological analysis**:
  EEG signal, DNA…

- **Behavioural analysis**:
  Keystroke dynamics, voice, gait, signature dynamics...

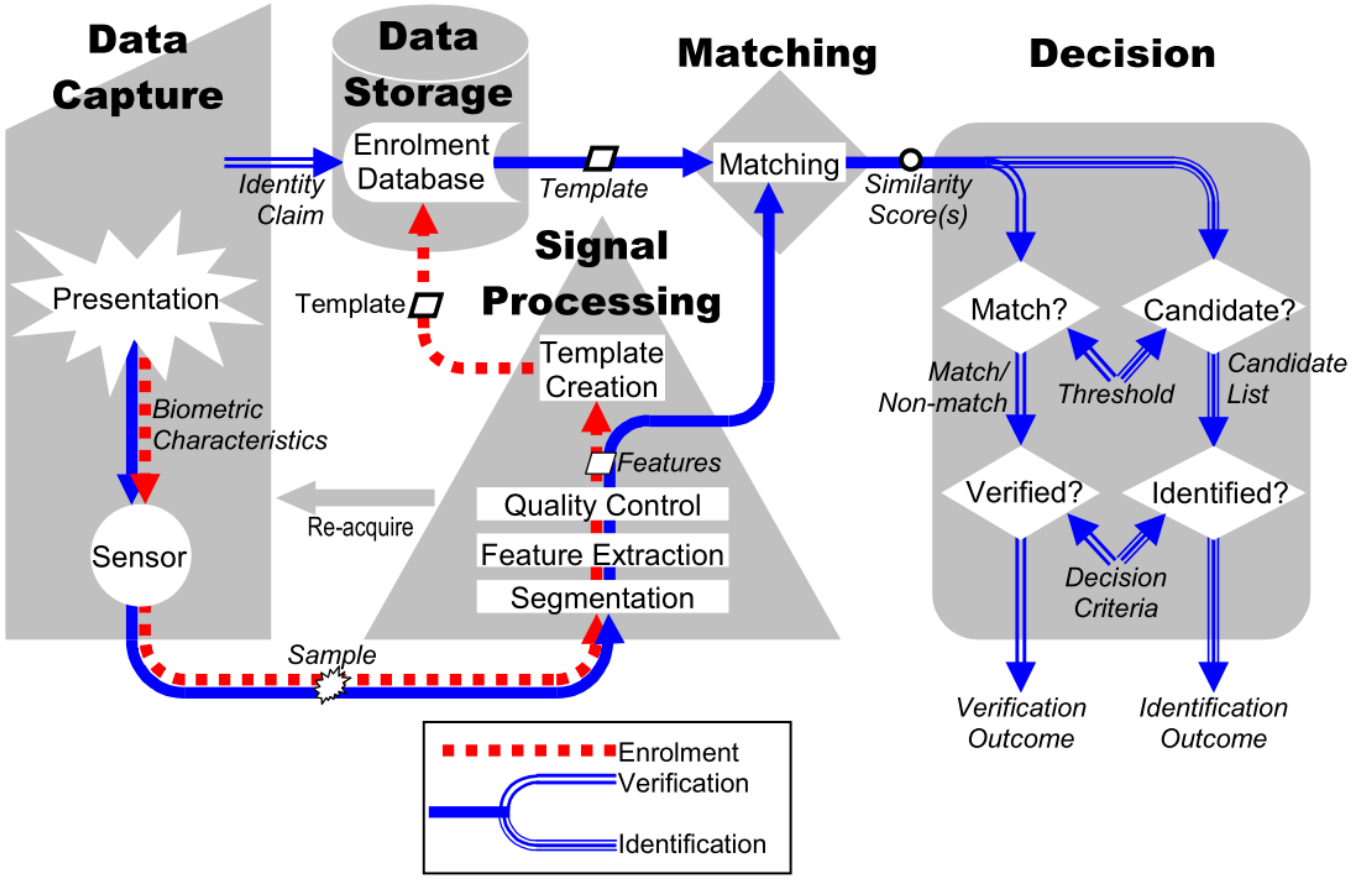


- **Morphological analysis**:
  Fingerprint, iris, palmprint, finger veins, face, ear…



Biometrics

Biometric system: general architecture



Source ISO/IEC19794-1 Information technology — Biometric data interchange formats — Part 1: Framework

Biometrics

GREYC

Verification process

$$R_z = 1_{\{D(b_z, \acute{b_z}) \leq \epsilon\}} \quad (1)$$

Where :

- R_z : decision result for the verification of user z using the biometric system,
- D : distance function in the biometric feature domain,
- b_z, $\acute{b_z}$ represent the template and query biometric features of user z,
- ϵ : decision threshold.

Biometrics

Performance evaluation:

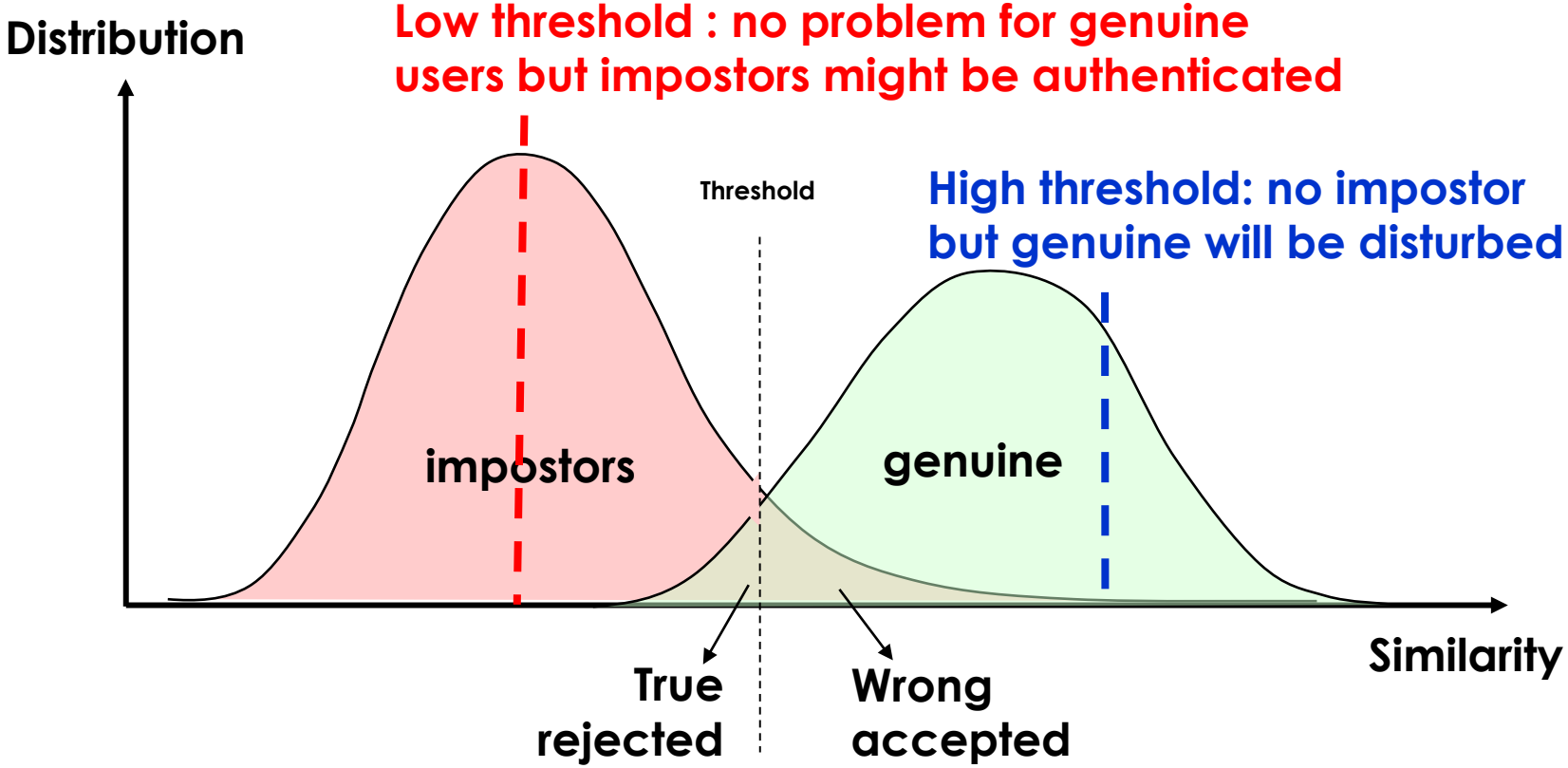
In order to quantify the efficiency of a biometric system, we generally use two databases:

1-Learning database: used for the enrolment of individuals (can use different capture for the model definition);

2-Testing database: used for verification or identification with captures of known individuals (impostors and genuine users).

Biometrics

Scores distribution:



Biometrics

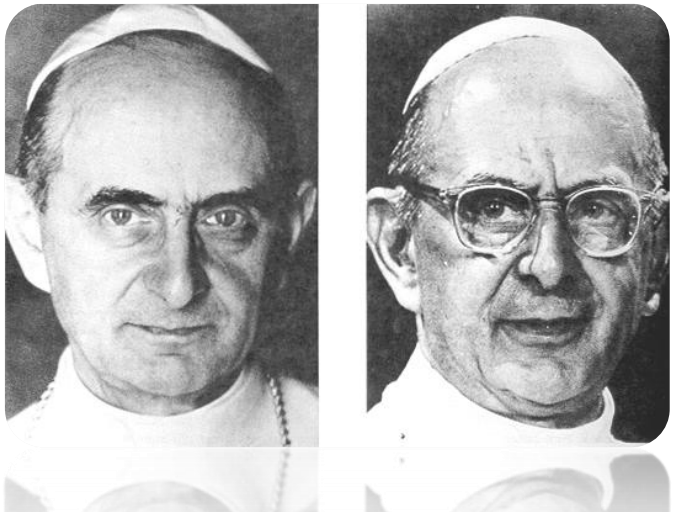
Acquisition metrics

- **Failure to acquire rate**
  - FTAR
  - Problem during capture
  - Physical incapacity
  - Sensor does not work
- **Failure to enroll rate**
  - FTER
  - Insufficient biometric quality
  - User does not want to enroll himself

Biometrics

Error metrics (1):

- **False match rate**
  - FMR
  - Ratio of impostors accepted
- **False non match rate**
  - FNMR
  - Ratio of genuine users refused



Biometrics

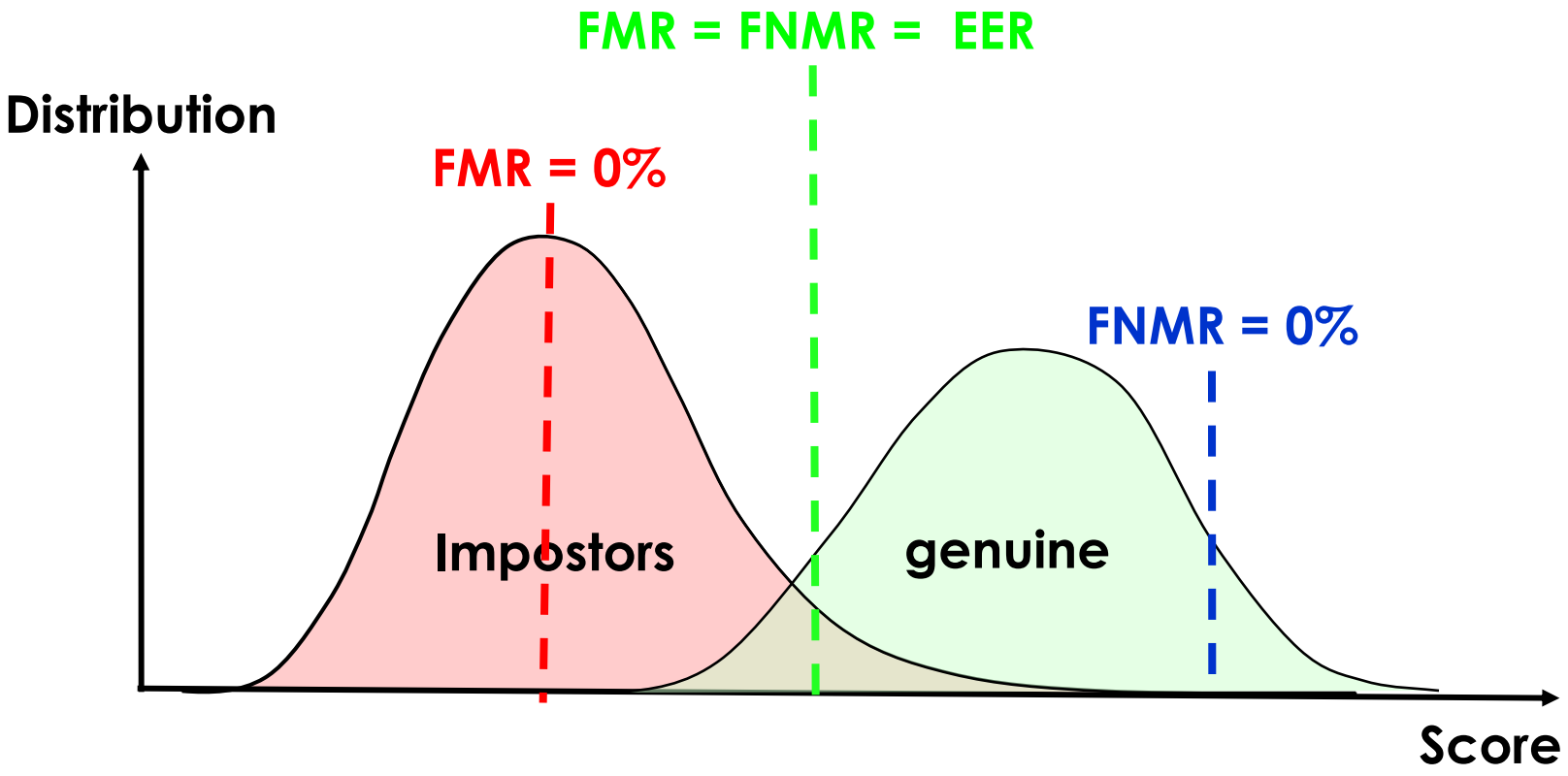
GREYC

Error metrics (2):

- **False Acceptation Rate**
  - FAR
  - $FAR(\varepsilon) = (1 - FTAR).FMR(\varepsilon)$
- **False Rejection Rate**
  - FRR
  - $FRR(\varepsilon) = (1 - FTAR).FNMR(\varepsilon) + FTAR$
- **Egality**
  - EER – Equal Error Rate

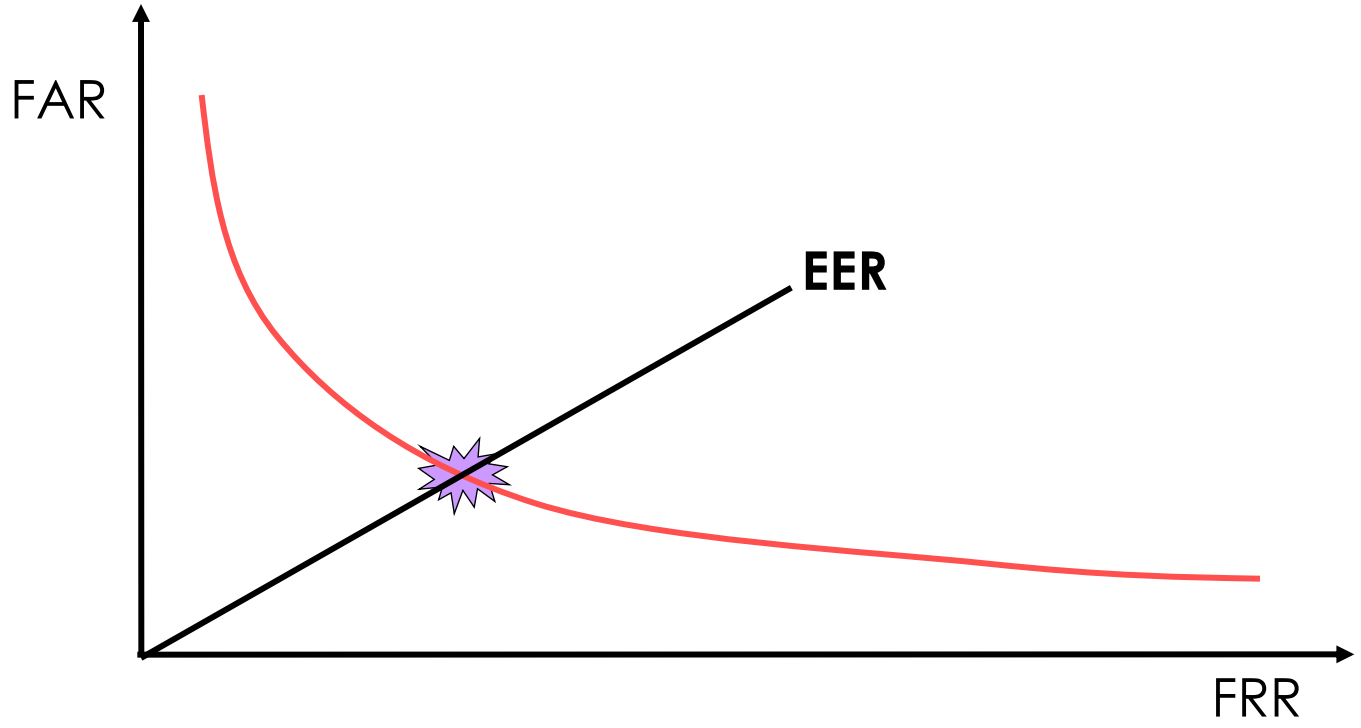
Biometrics

Scores distribution:



Biometrics

Performance curves:



One functionning point is often used : FRR value @FAR 10^-4

Biometrics

UID example:

UID Status

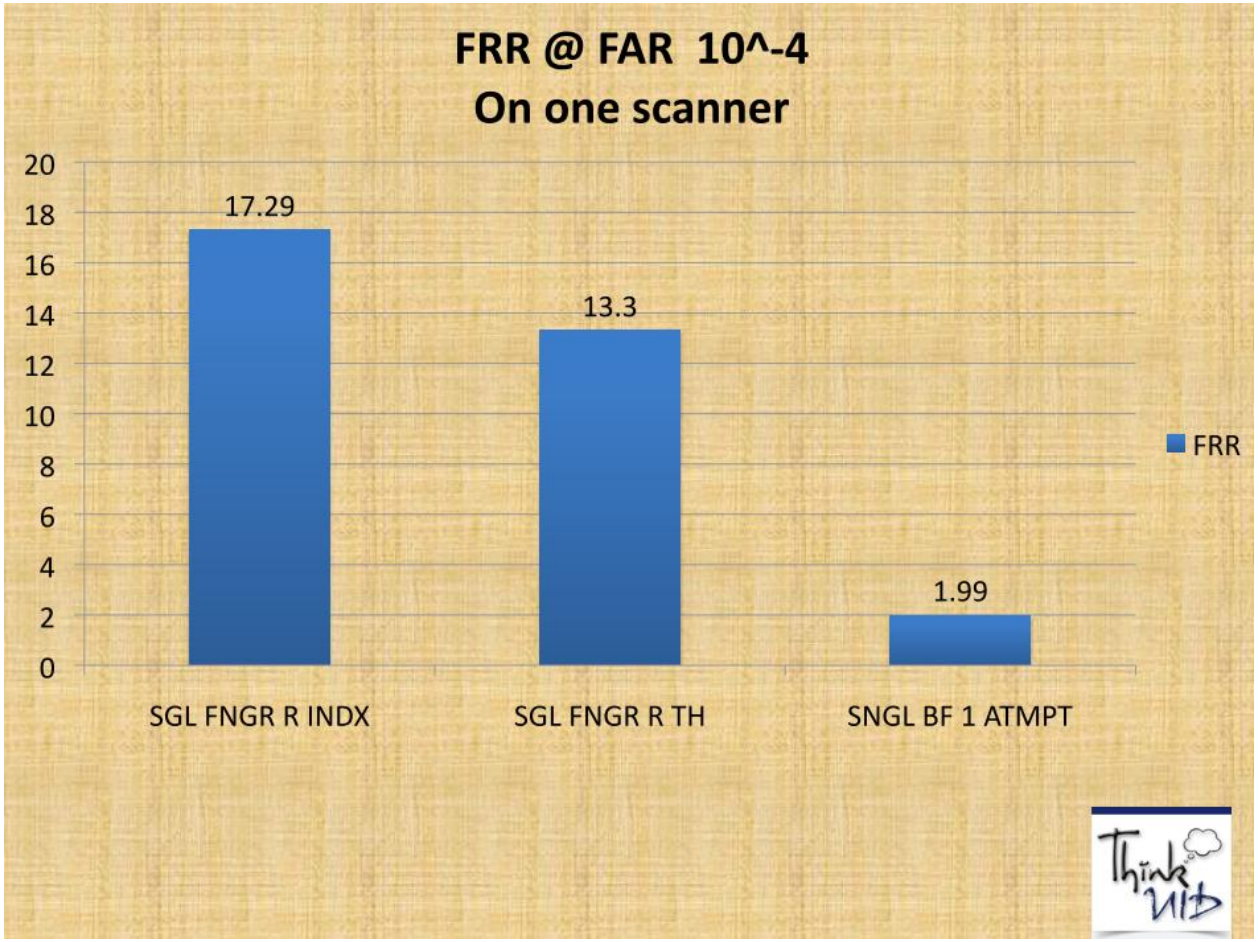
- Enrollment (multi-modal biometric)
  - 36,000 enrollment stations, 87K certified operators
  - 11 models of certified devices
  - 200 Million enrolled
  - 400 Million planned for FY '13
  - 1M/day enrollment rate
  - *100 trillion person matches/day*
- Biometric Verification
  - 8 PoC
  - Two pilot programs underway

The Dalai Lama enrols for Aadhaar in Dharmshala in April 2011

Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

Biometrics

Performance evaluation:



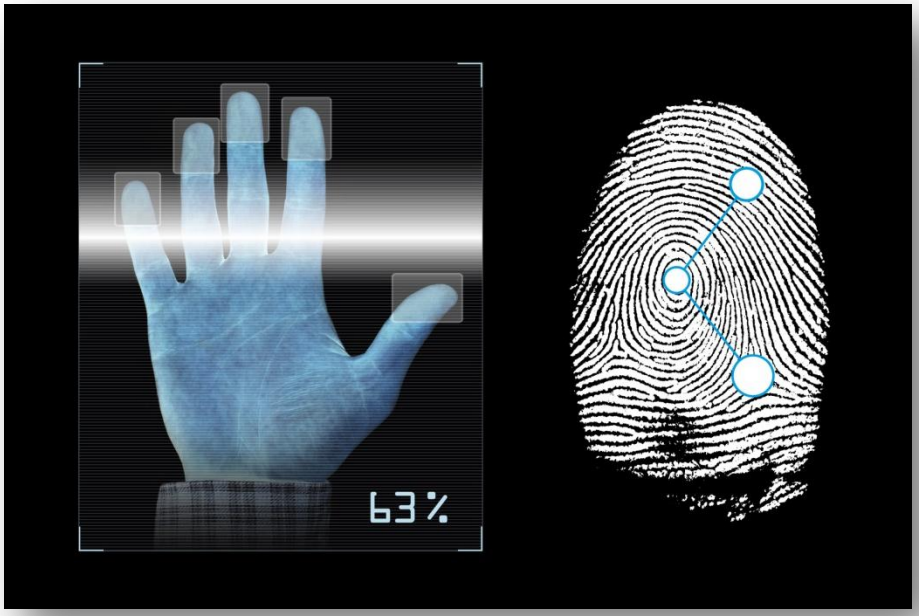
Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

Biometrics

GREYC

Advantages:

- The only one **user** authentication method
- It is more easy to use
- It is much more difficult to attack or falsify



Biometrics

GREYC

Drawbacks:

- False rejection and acceptance are possible
- In general, it is not possible to revoke a biometric data
- It is sensitive to the replay attack
- There are many privacy concerns