OUTLINE

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

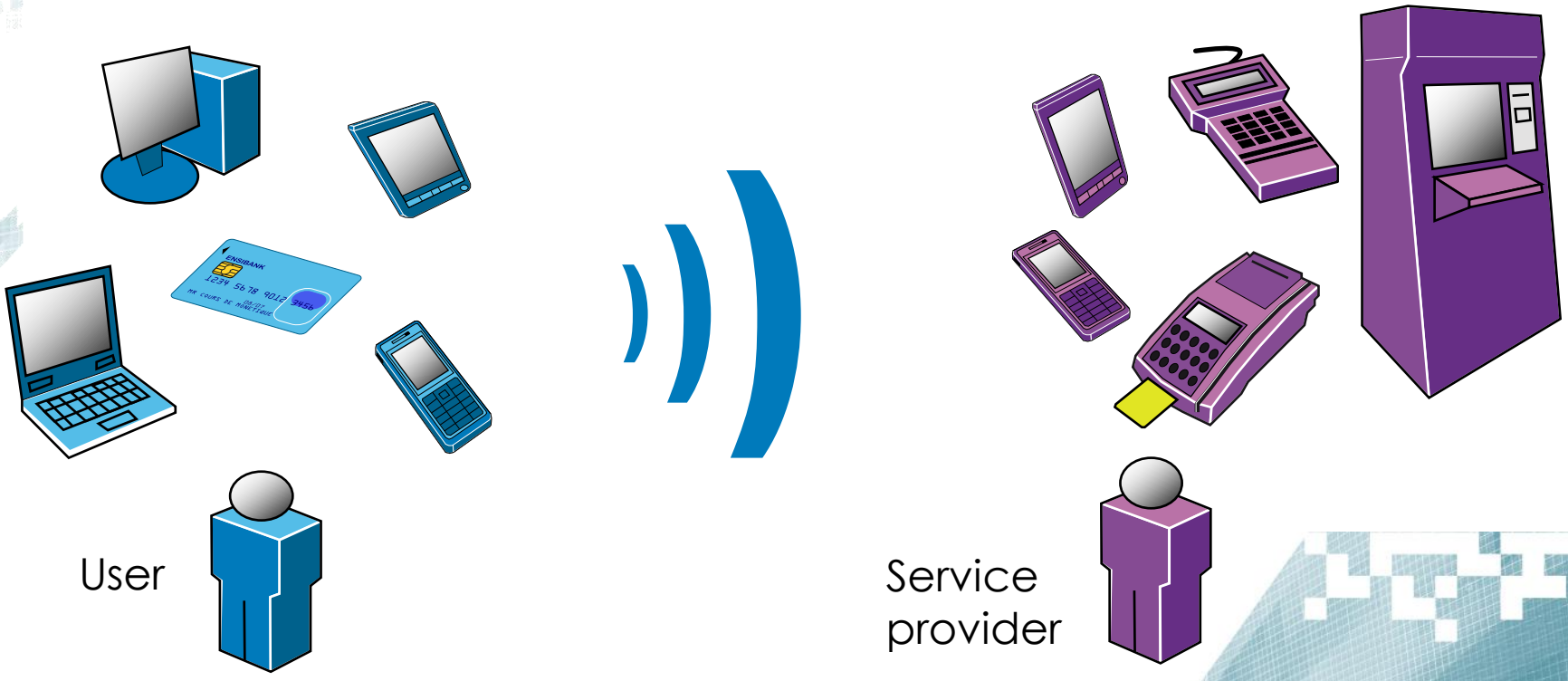
Mobile biometric authentication

GREYC

Two types of device:

- Specific ones with a biometric sensor
- Classic ones

Two locations for the biometric authentication:



Specific solutions: user

Match and capture on device

Fingerprint sensor

http://www.authentec.com/

Specific solutions: user

Match and capture on contactless card solution

Comparison between the template and the capture

Storage of the template fingerprint

Fingerprint sensor

http://www.e-smart.com/

Specific solutions: terminal

Match and capture on device solution

NFC reader

Fingerprint sensor

http://www.taztag.com/

Specific solutions: terminal

Capture on device solution

http://ekemp.en.alibaba.com

http://www.acs.com.hk/

http://www.naturalsecurity.com/

http://www.supremainc.com/

Specific solutions

Discussion:

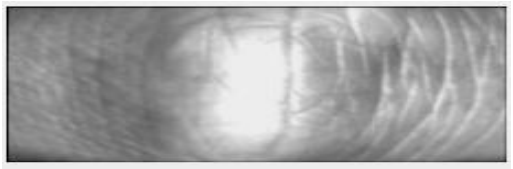
- There are many solutions especially for terminals
- Nearly all of them use fingerprint as biometric modality
  - ✓ well known and cheap technology
  - ✓ fast capture and verification
  - ✓ very good performance

Other solutions

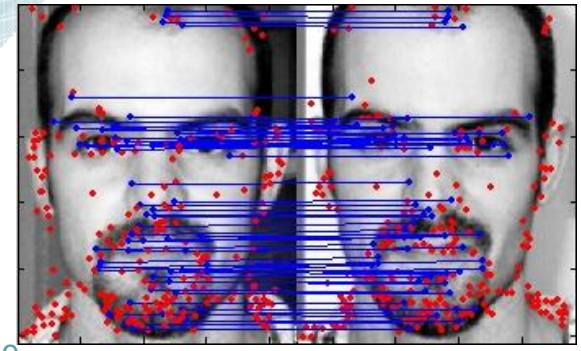
Solutions without any specific sensor:

- Smartcard:
  - ✓ storage of the biometric template
  - ✓ match on card

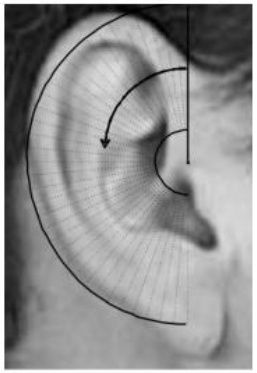
- Smart object (mobile phone, tablet, laptop...)
  - ✓ webcam :
    - Face recognition
    - Hand shape
    - Finger knuckle print
    - Ear...



Finger Knuckle Print



Face

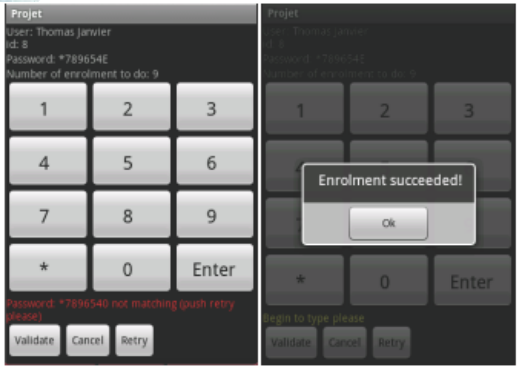


Ear

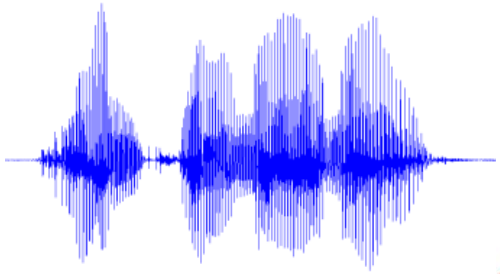
Hand shape

Other solutions

- Smart object (mobile phone, tablet, laptop...)
  - ✓ microphone :
    - speaker recognition: text-dependent or free-text
  - ✓ keyboard :
    - keystroke dynamics: passphrase, password or challenge
  - ✓ touch screen :
    - interaction: passphrase, password, challenge, task
    - signature dynamics



Touch screen interaction



Voice

Signature dynamics

Keystroke dynamics

Other solutions

Discussion:

- There are many possible solutions
- The most interesting candidates are:
  - ✓ voice
  - ✓ touch screen interaction
  - ✓ signature dynamics
  - ✓ face
  - ✓ hand shape

OUTLINE

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

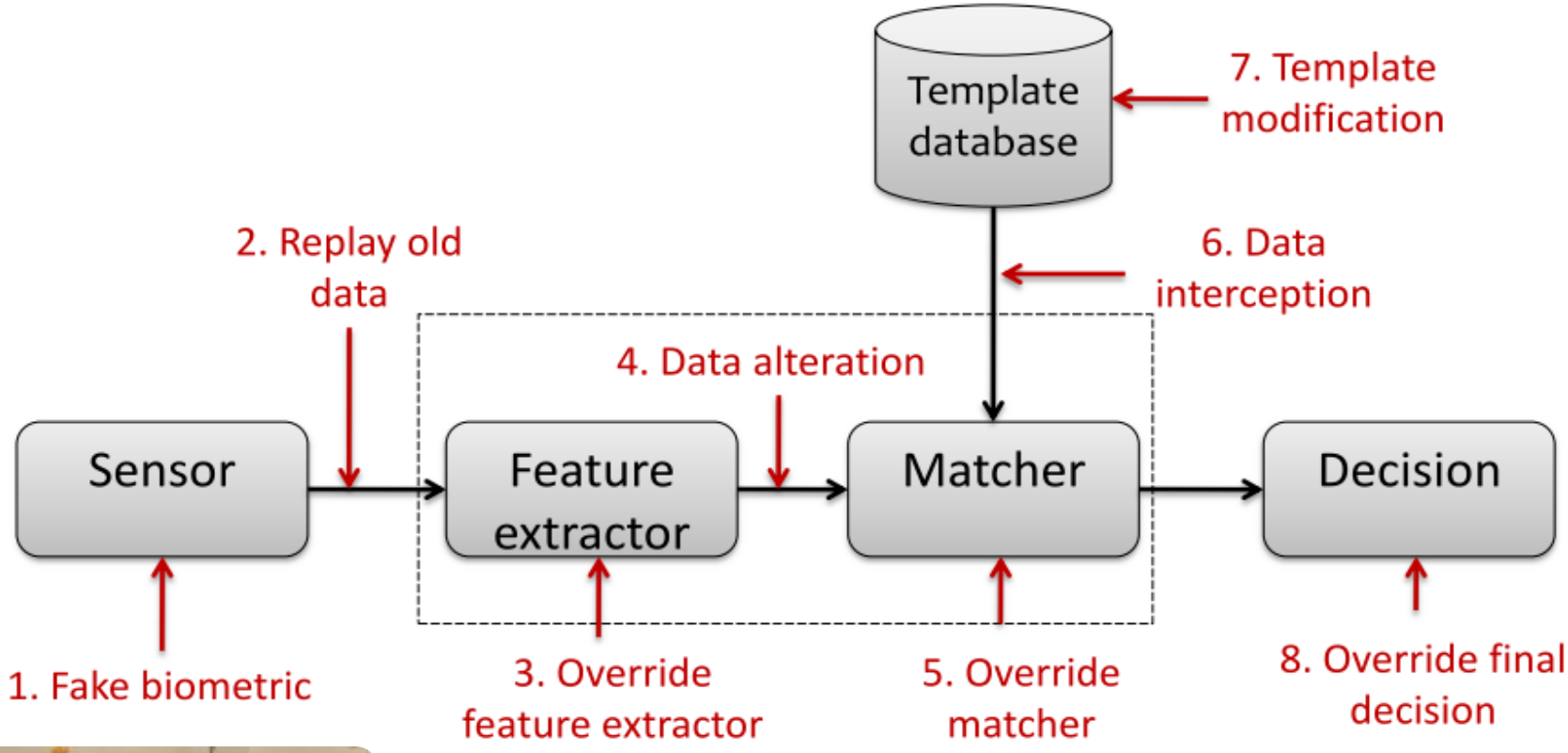
Protection of biometric data

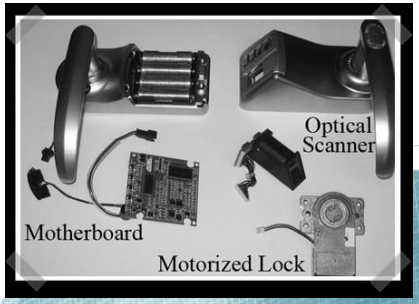
Why is it necessary ?

- Personal data
- Difficult to revoke a biometric data
- Can be captured without any consent
- Its encryption is not sufficient

Protection of biometric data

Attacks on a biometric system:



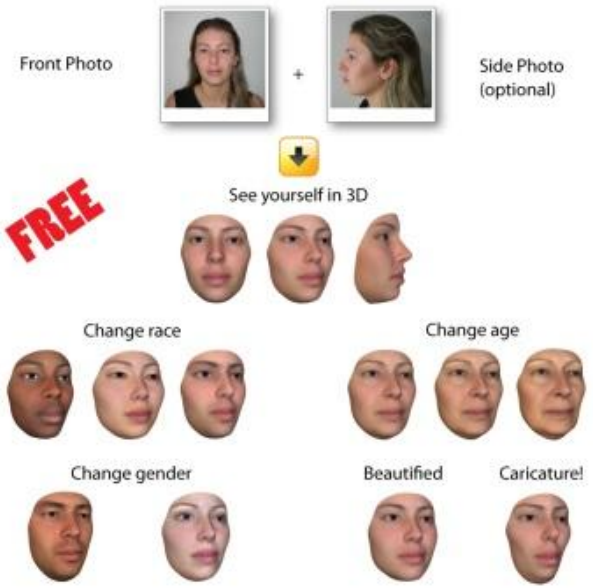


Protection of biometric data

Attacks on a biometric system:

Protection of biometric data

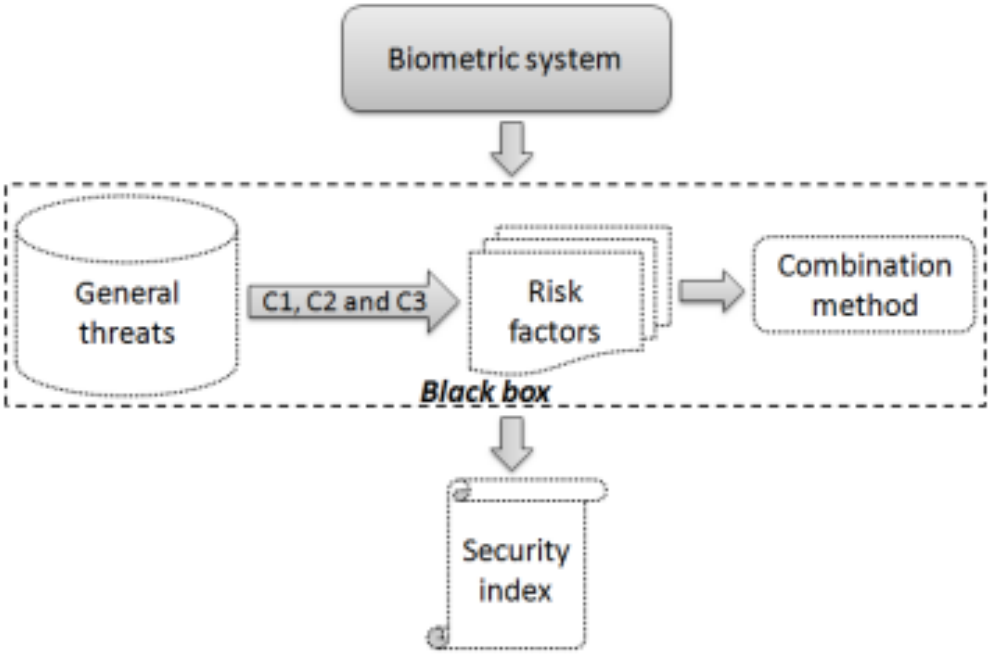
Attacks on a biometric system:

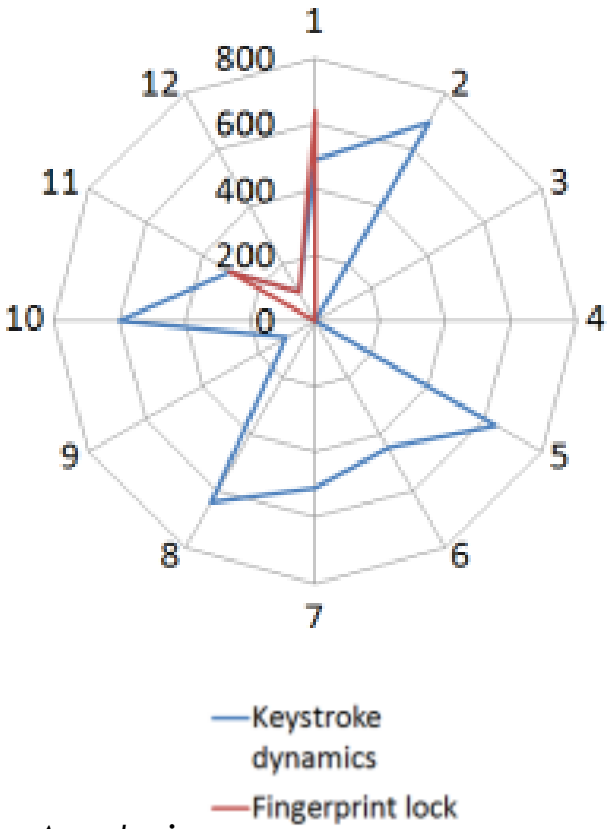


http://www.thatsmyface.com/

Protection of biometric data

Security index of a biometric systems



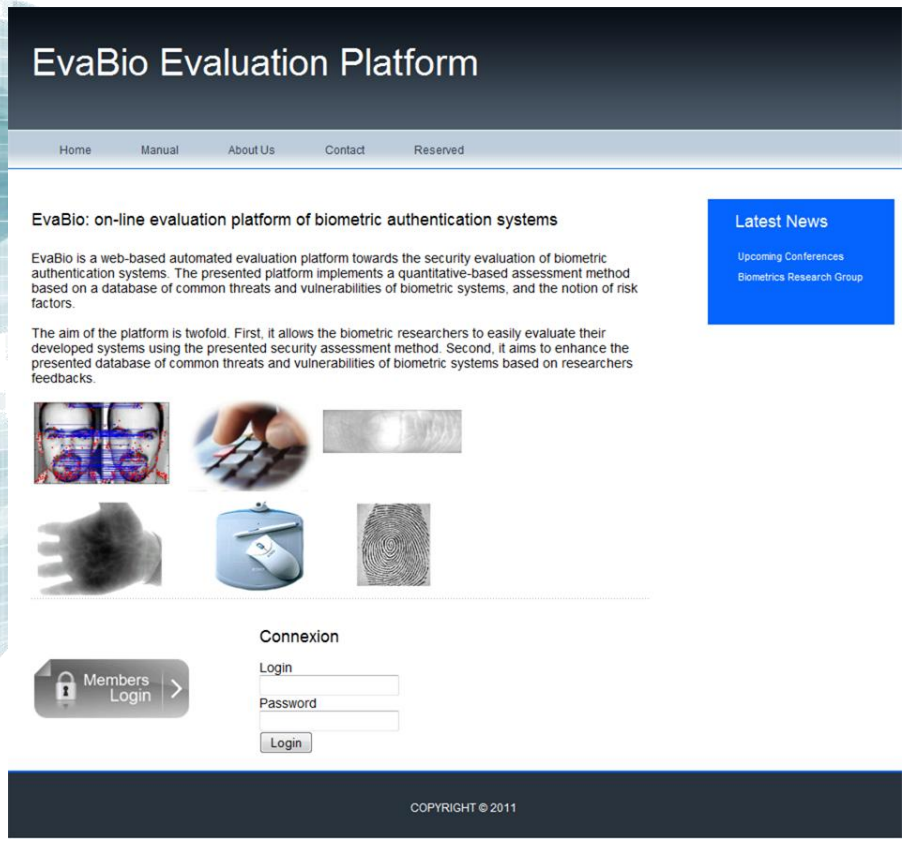


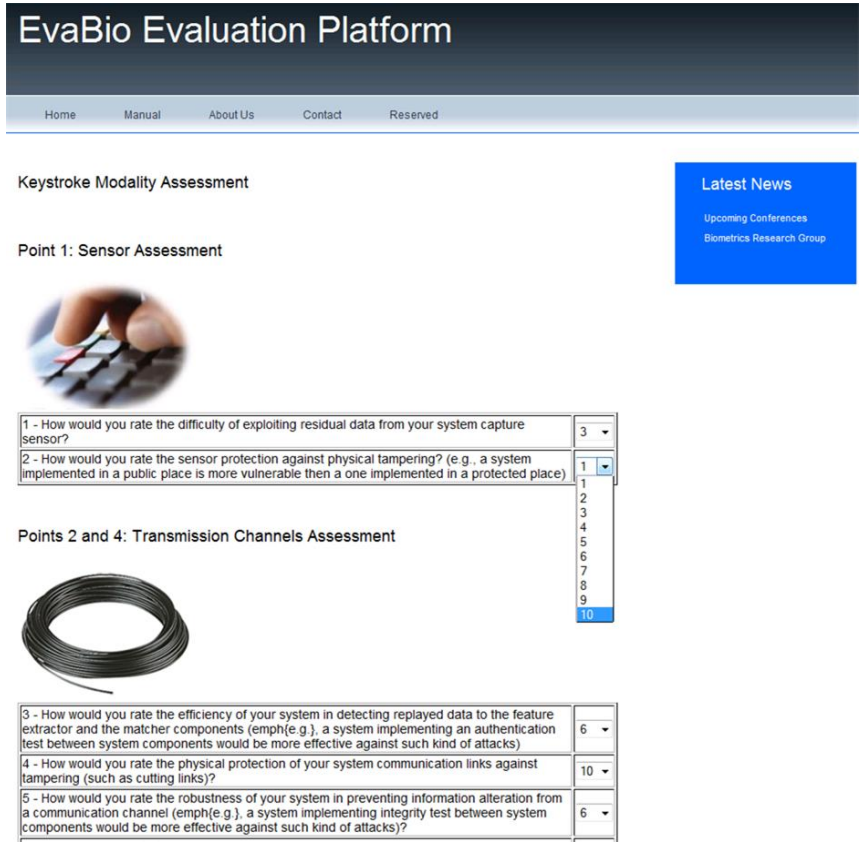
M. El Abed, P. Lacharme, C. Rosenberger, "EvaBio: An Analysis Tool for the Security Evaluation of Biometric Authentication Systems", IEEE/IAPR International Conference on Biometrics (ICB), p.7, 2012

Protection of biometric data

Security index of a biometric systems

http://www.epaymentbiometrics.ensicaen.fr/securityEvaBio/





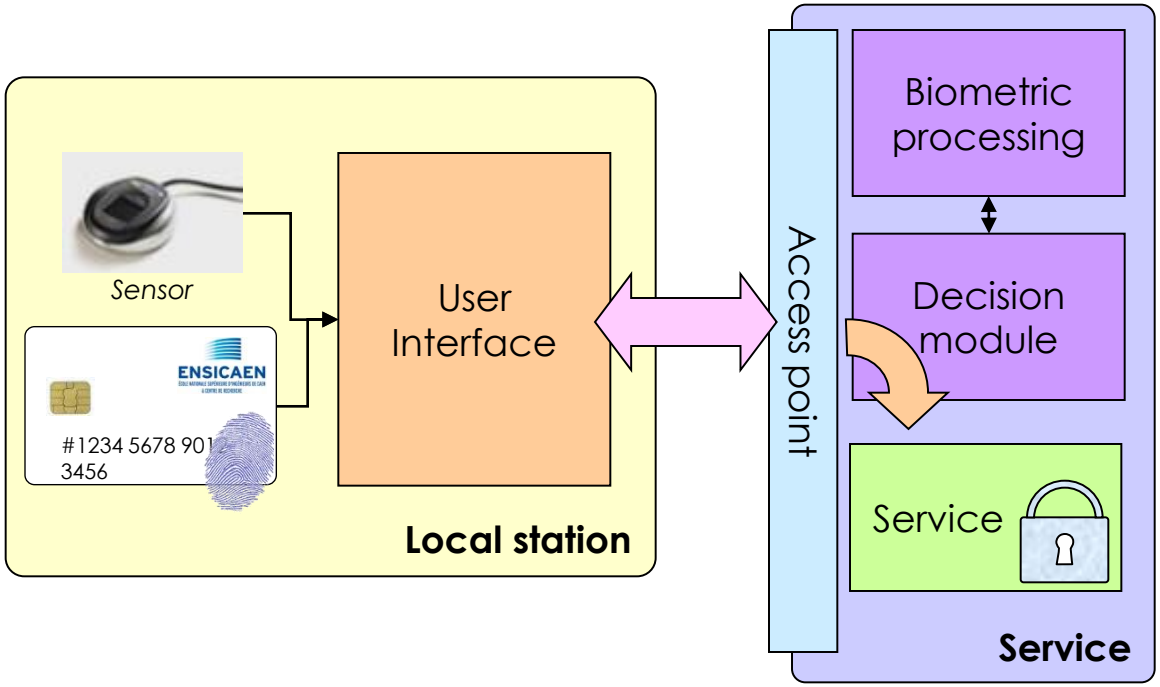
Protection of biometric data

Solutions:

- Secure architectures: store the biometric data in a secure element, avoid its transmission, match on card...
- Algorithmic solutions: transform the biometric data (cancelable biometrics), crypto-biometrics (fuzzy vault)..
- Combinations of the two previous solutions

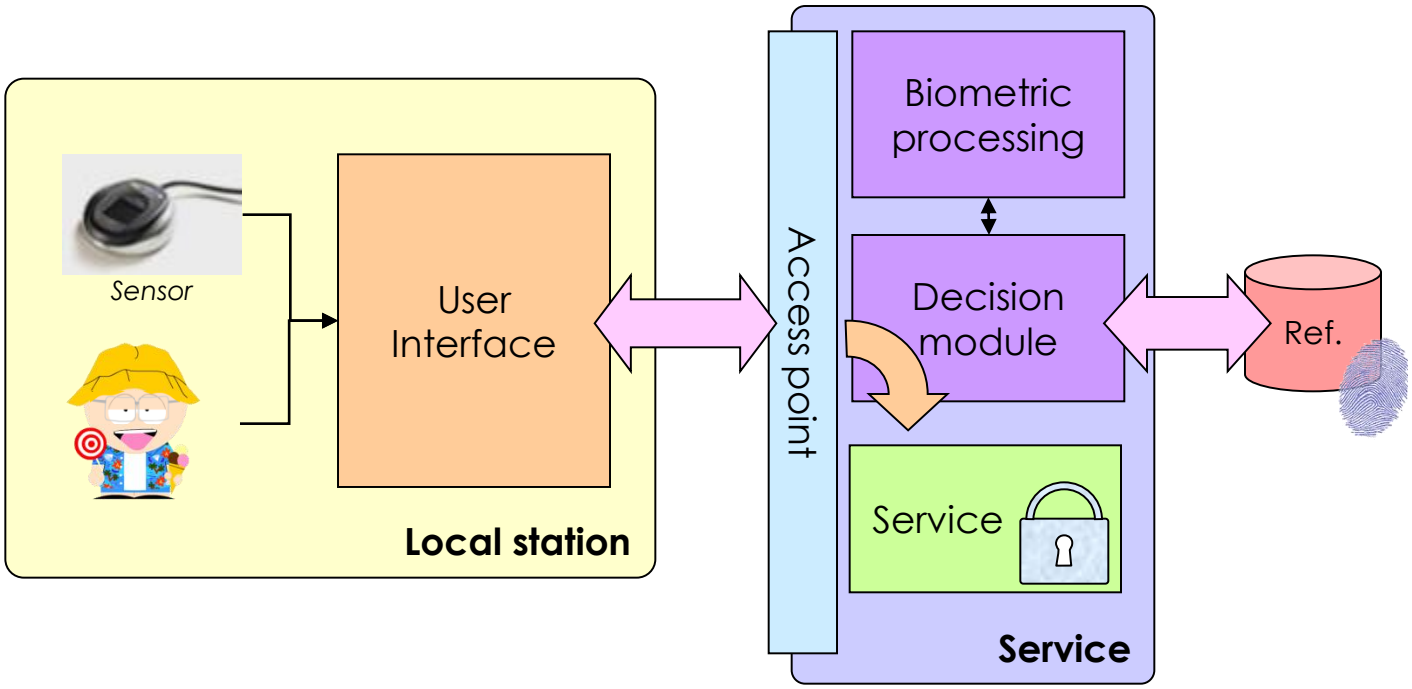
Protection of biometric data

Authentication / Reference stored in a secure element:



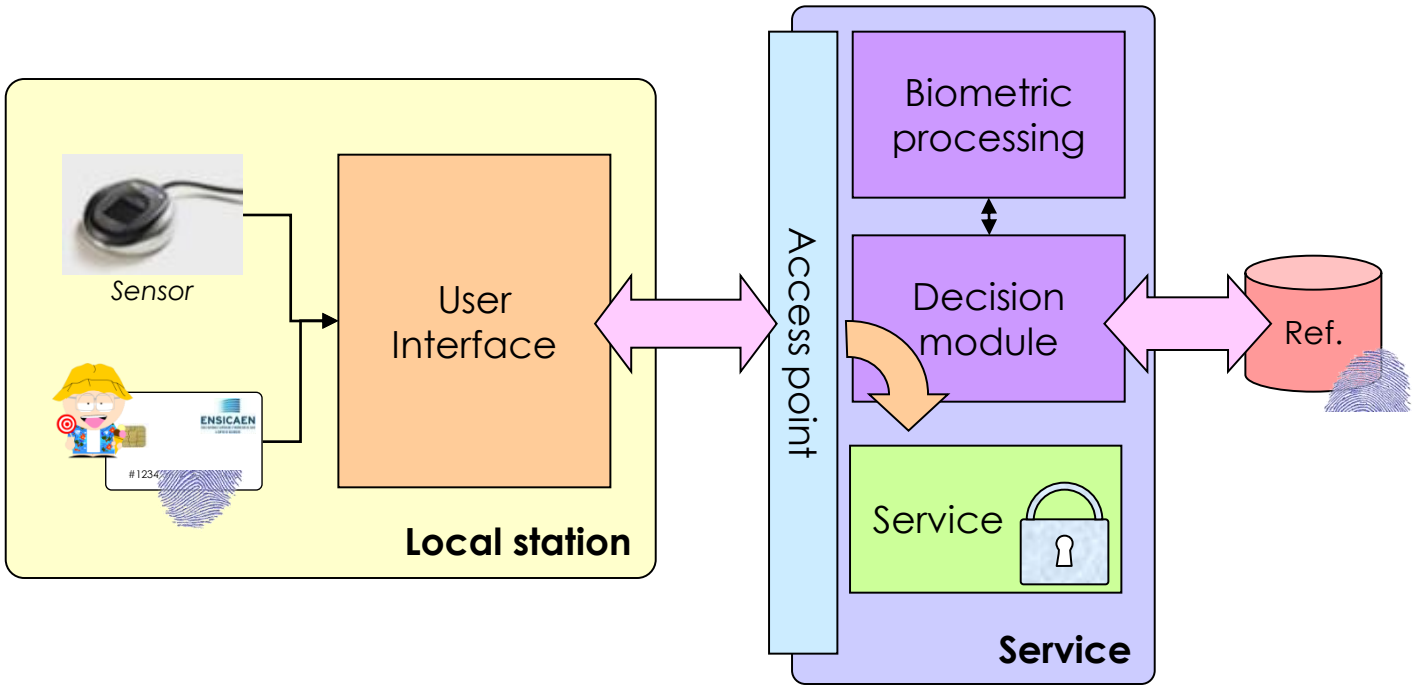
Protection of biometric data

Authentication / Reference stored in a database:



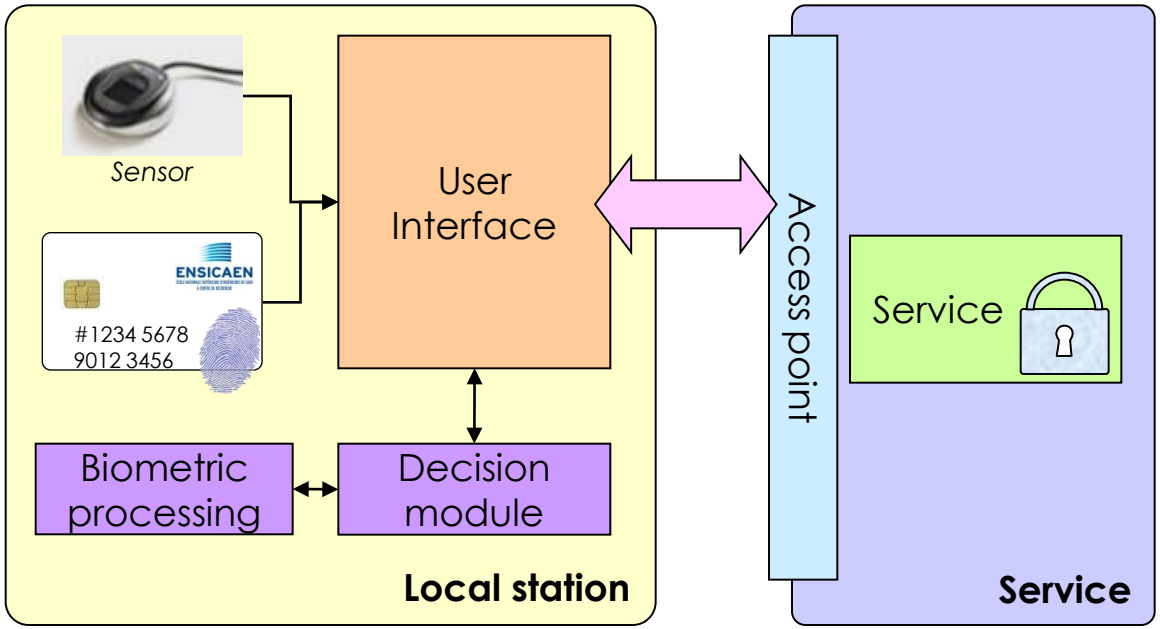
Protection of biometric data

Authentication / Shared reference:



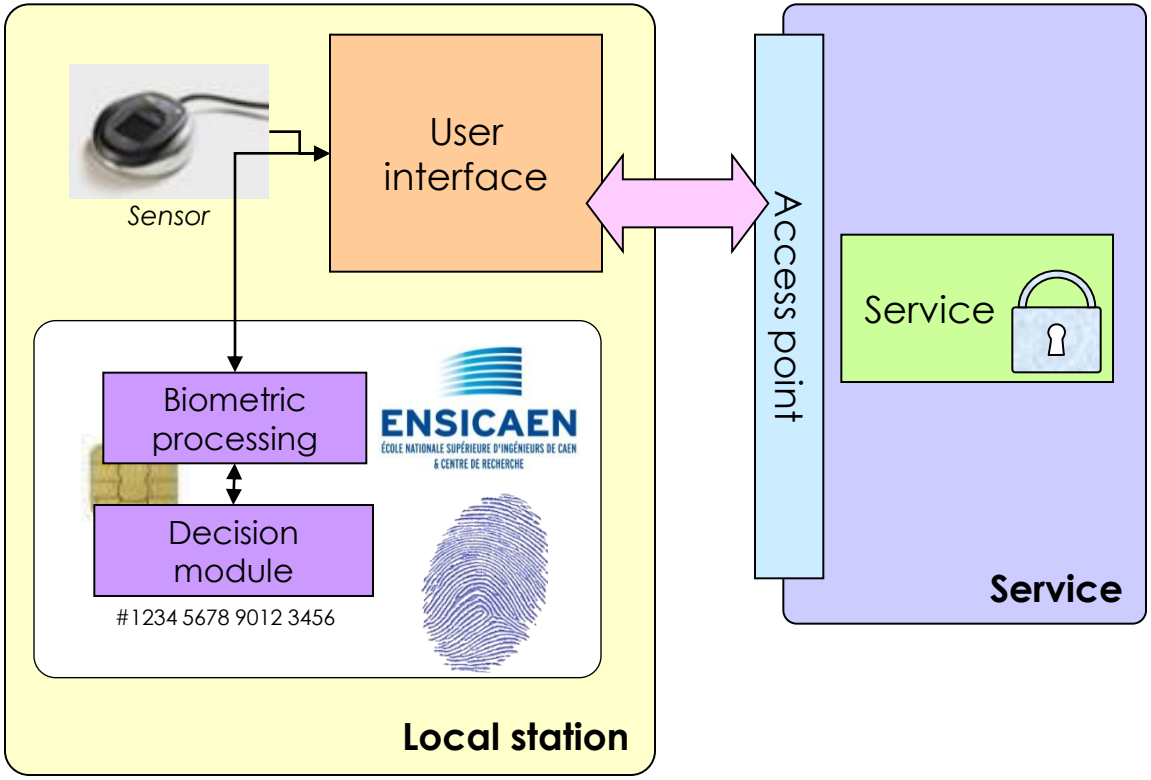
Protection of biometric data

Authentication / Local processing/ Reference stored in a SE:



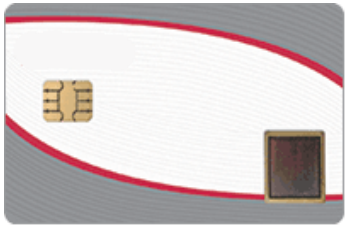
Protection of biometric data

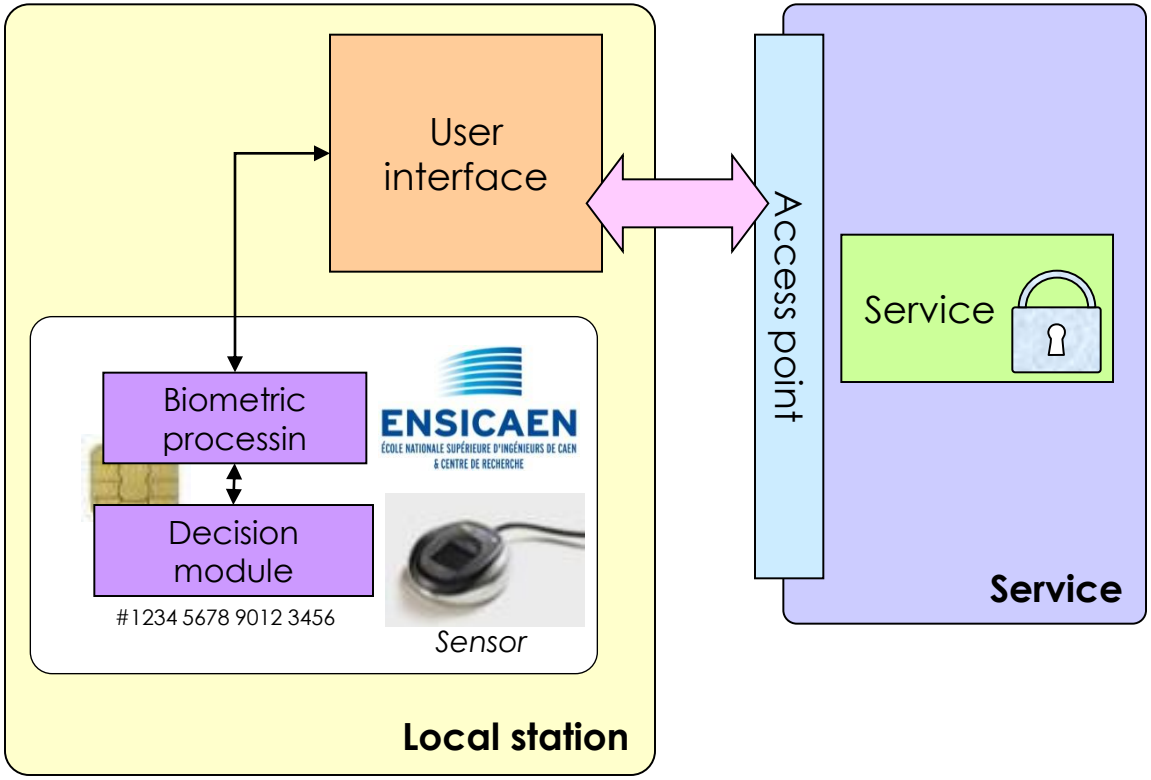
Authentication / Match on card:



Protection of biometric data

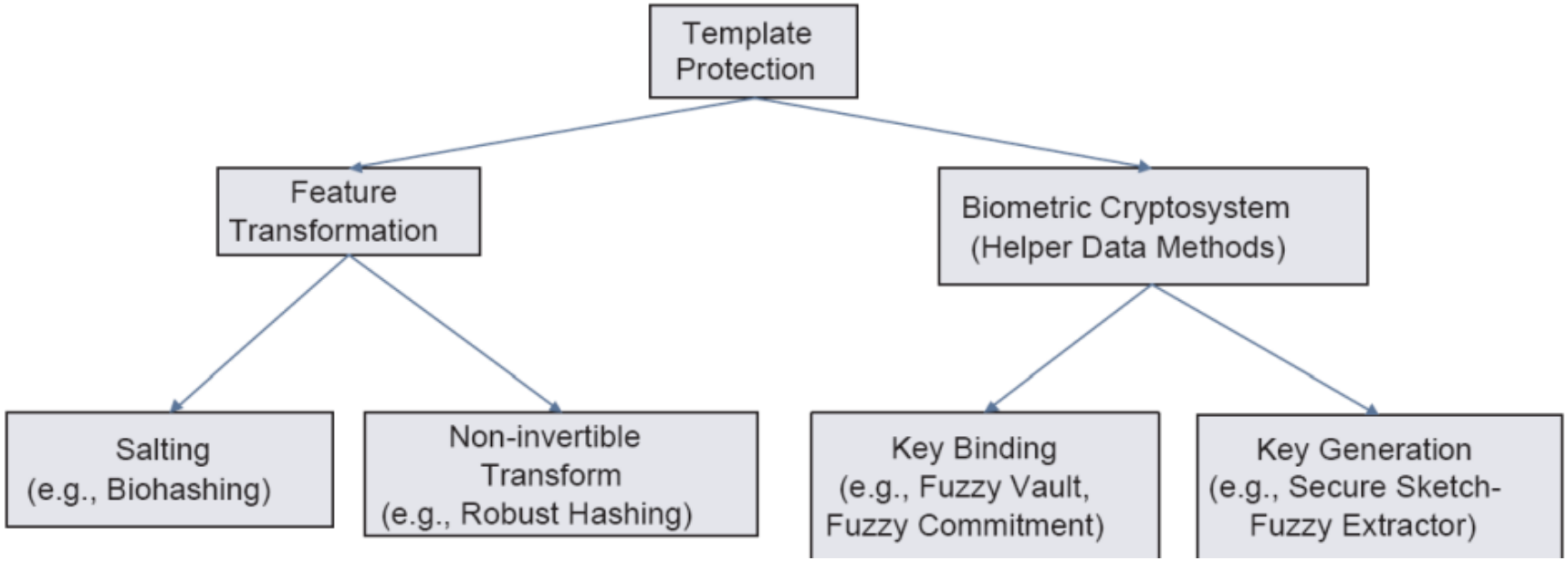
Authentication / Sensor and match on Card:





Protection of biometric data

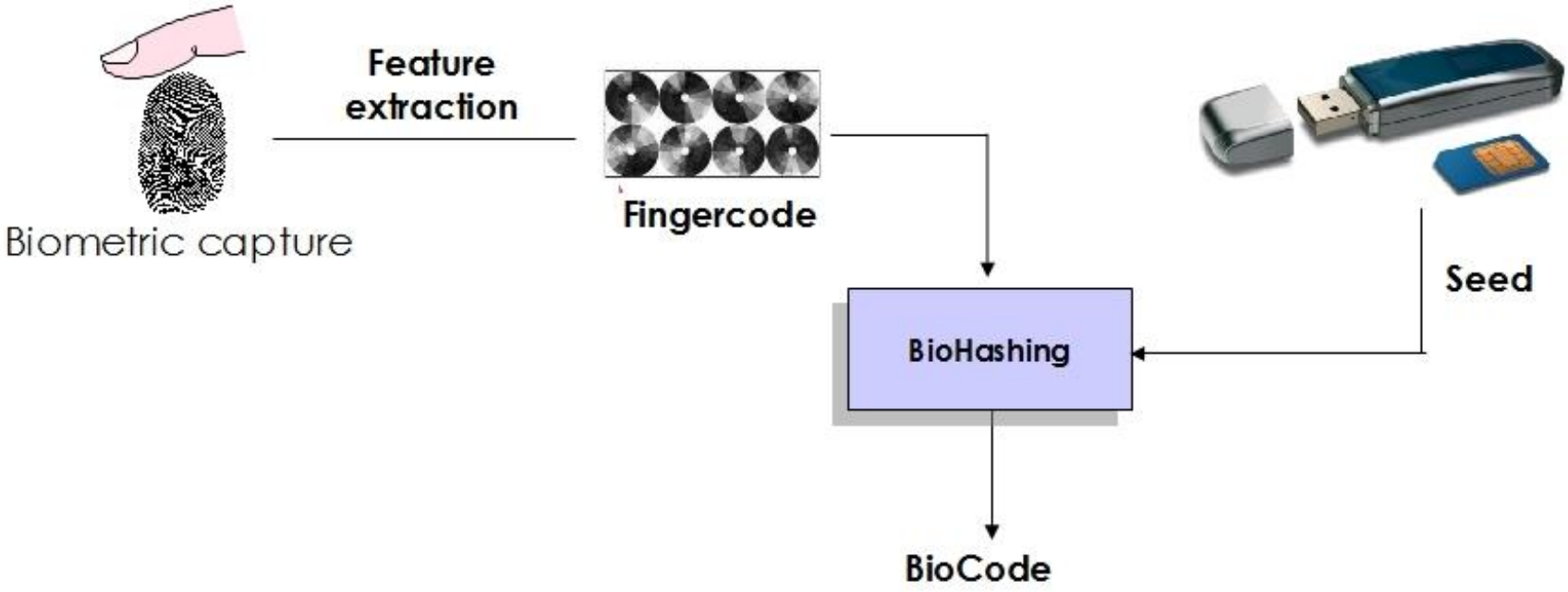
Algorithmic solutions:



Source: Jain, Nandakumar and Nagar, "Biometric Template security", EURASIP J. on Advances in Signal Processing, 2008

Protection of biometric data

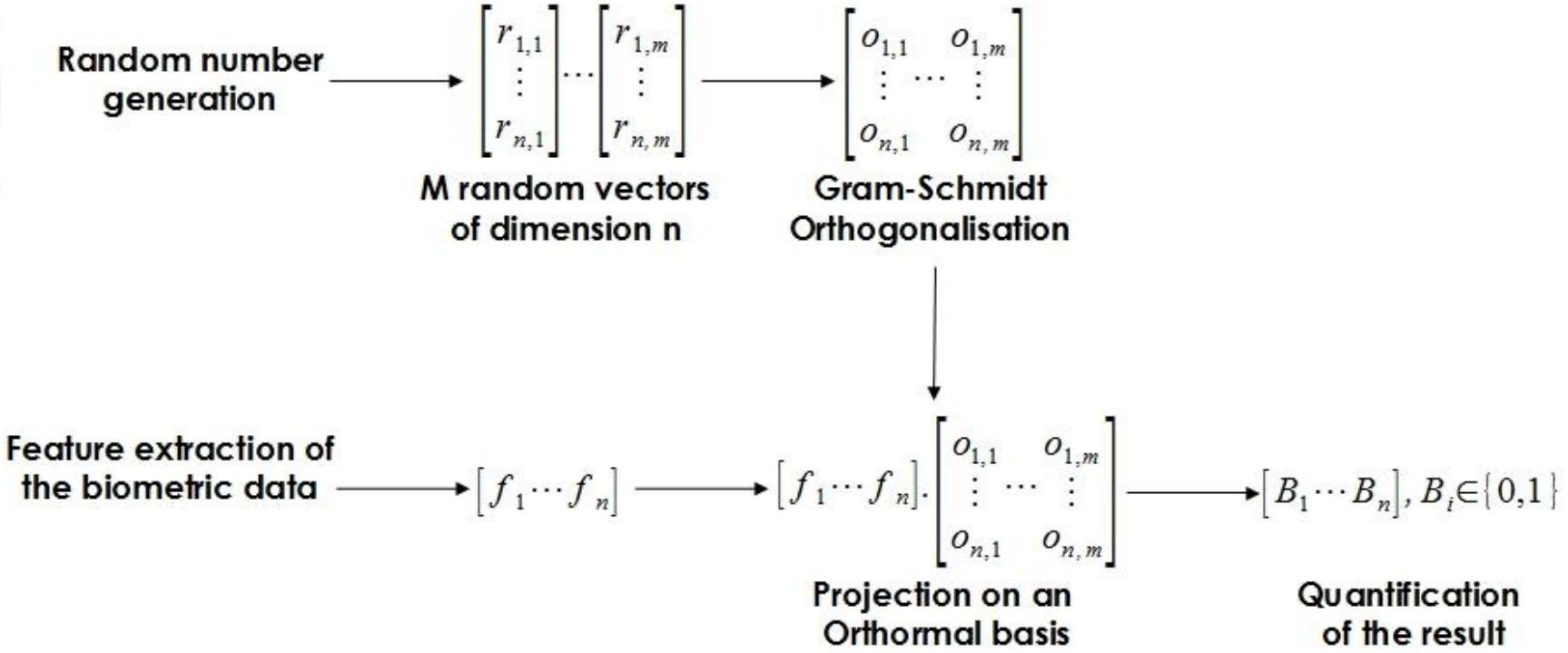
Cancelable biometrics: make the biometric template revocable



N. Ratha, J. Connelle, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication system," IBM Systems J., vol. 37, no. 11, pp. 2245–2255, 2001.

Protection of biometric data

Biohashing process:



Protection of biometric data

GREYC

Verification process

$$R_z = 1_{\{D_T(f(b_z,K_z),f(b_z',K_z))\leq\epsilon_T\}} \quad (1)$$

Where :

- R_z : decision result for the verification of user z using the cancelable system,
- D_T : distance function in the transformed domain,
- f : the feature transformation function,
- b_z, b_z' represent the template and query biometric features of user z,
- K_z : set of transformation parameters,
- ϵ_T : decision threshold.

Protection of biometric data

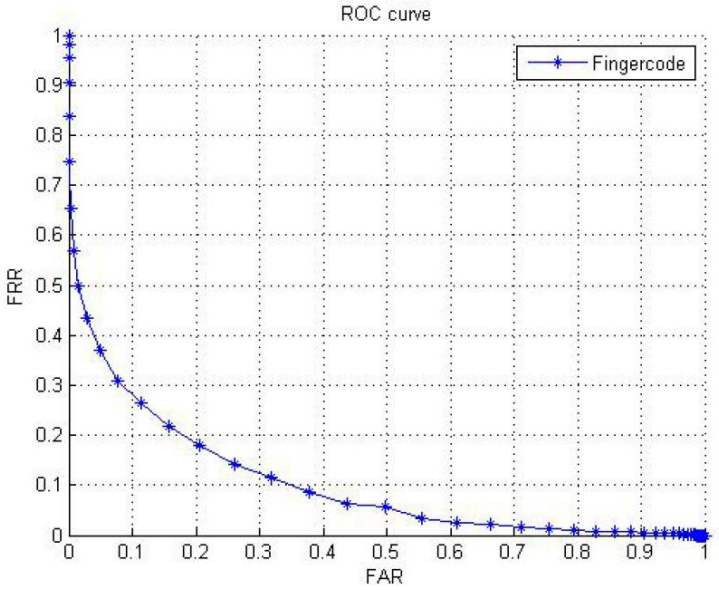
GREYC

Properties:

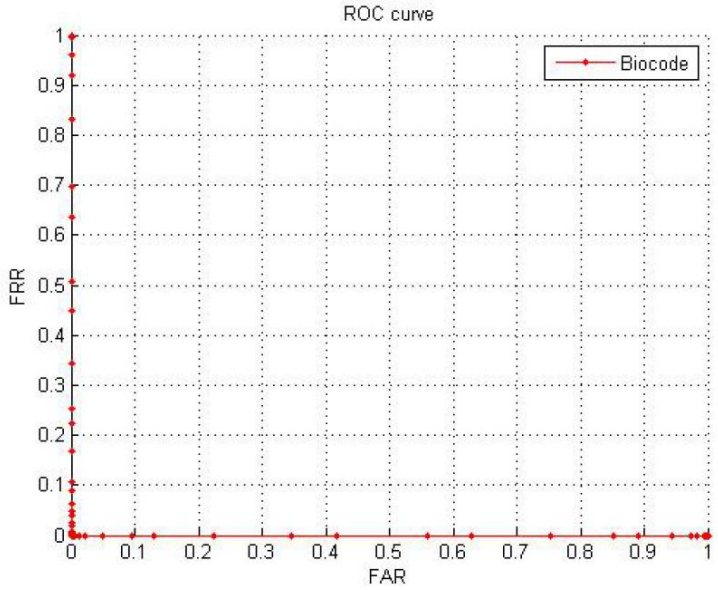
- Given the BioCode, the biometric raw data cannot be retrieved,
- Only the BioCode is stored,
- If the BioCode is intercepted, a new one can be generated,
- An individual can have many BioCodes for different applications,
- The BioHashing process improves performances,
- The comparison of two BioCodes is very fast (simple Hamming distance)

Protection of biometric data

Performance evaluation:



(a) FingerCode, EER=19%



(b) BioCode, EER=0%

	128 bits	256 bits	512 bits
FingerCode	19%	18%	17%
BioCode	0%	0%	0%

EER values for different sizes of the FingerCode and BioCode

Protection of biometric data

DEMO

Protection of biometric data

Study of the robustness of the solution

Security properties

- **Performance** : the template protection shall not deteriorate the performance of the original biometric system,
- **Revocability or renewability** : it shoud be possible to revoke a biometric template.
- **Non-invertibility or irreversibility** : from the transformed data, it should not be possible to obtain enough information on the original biometric data to forge a fake biometric template,
- **Diversity or unlinkability** : it should be possible to generate different biocodes for multiple applications, and no information should be deduced from their different realizations.

R. Belguechi, E. Cherrier, C. Rosenberger, "How to Evaluate Transformation Based Cancelable Biometric Systems?", NIST International Biometric Performance Testing Conference 2012.

Protection of biometric data

Study of the robustness of the solution

Probability of a sucessful attack by an impostor

$$FAR_A(\epsilon_T) = P(D_T(f(b_z, K_z), A_z) \leq \epsilon_T) \quad (3)$$

Where :

- $FAR_A(\epsilon_T)$: probability of a successful attack by the impostor for the threshold ϵ_T.
- A_z : generated biocode by the impostor with different methods,
- We can consider $\epsilon_T = \epsilon_{EER_T}$ (ϵ_{EER_T} : threshold to have the EER functionning point of the cancelable biometric system).

Protection of biometric data

GREYC

Study of the robustness of the solution

A priori information used by the impostor

- *Zero effort attack* (A_2) :
  An impostor provides one of its biometric sample to be authenticated as the user z : $A_z = f(\acute{b_x}, K_x)$,
- *Brute force attack* :
  An impostor tries to be authenticated by trying different random values of A : $A_z = A$,
- *Stolen token attack* :
  An impostor has obtained the token K_z of the genuine user z and tries different random values of b to generate : $A_z = f(b, K_z)$,
- *Stolen biometric data attack* :
  An impostor knows $\acute{b_z}$ and tries different random numbers K to generate : $A_z = f(\acute{b_z}, K)$.

Protection of biometric data

GREYC

Study of the robustness of the solution

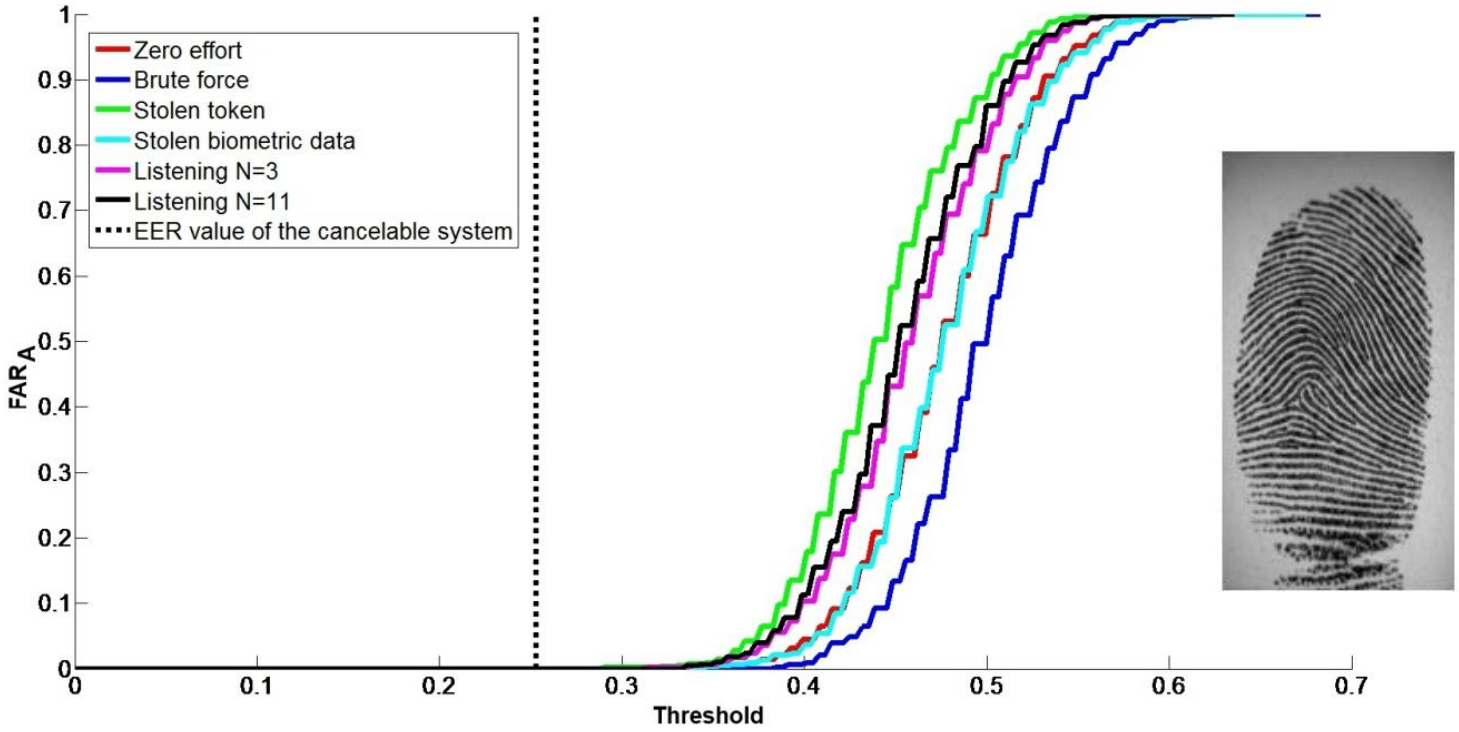
Listening attacks

For each template of the genuine user :

- Generation of Q biocodes $B_z = \{f(b_z, {K_z}^1), .., f(b_z, {K_z}^Q)\}$ for user z,
- Prediction of a possible biocode value by setting the most probable value of each bit given B_z,
- Computation of equation (2).
  $\Rightarrow A_7$ value for $Q = 3$ and A_8 for $Q = 11$

Protection of biometric data

Attacking on fingerprints

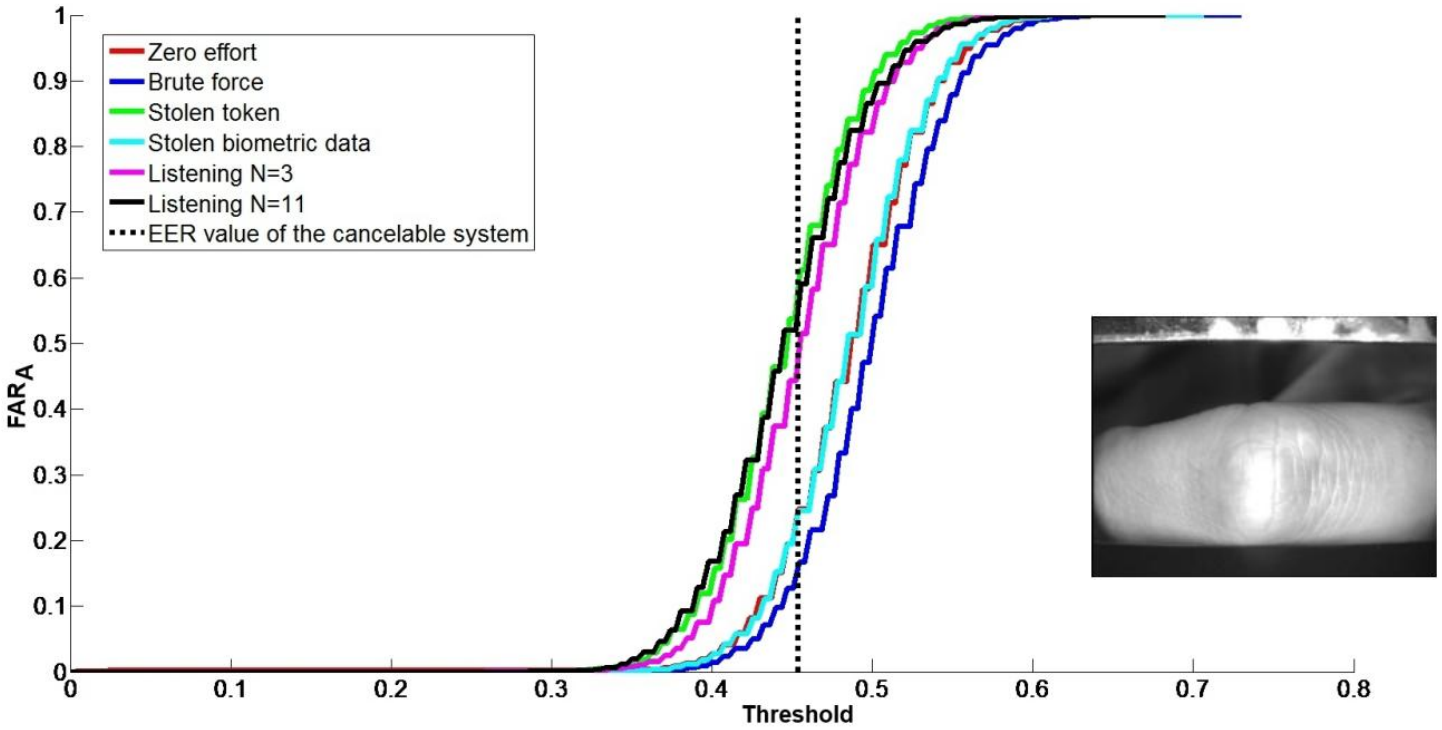


Analysis on fingerprints (FVC 2002)

R. Belguechi, E. Cherrier, C. Rosenberger, "Texture based Fingerprint BioHashing : Attacks and Robustness", IEEE/IAPR International Conference on Biometrics (ICB), p.7, 2012

Protection of biometric data

Attacking on finger knuckle prints



Analysis on finger knuckle prints (POLY FKP)

R. Belguechi, E. Cherrier, M. El Abed and C. Rosenberger, "Evaluation of Cancelable Biometric Systems : Application to Finger-Knuckle-Prints", IEEE International Conference on Hand-based Biometrics, 2011

Protection of biometric data

GREYC

New attack

Is it possible to determine the biometric feature knowing the secret key and the BioCode ?

What to do ?

To generate other BioCodes (after revokation)

It is a useful attack if the BioCode and the secret key are stored on an unsecure location (centralized database as for example)

Protection of biometric data

New attack

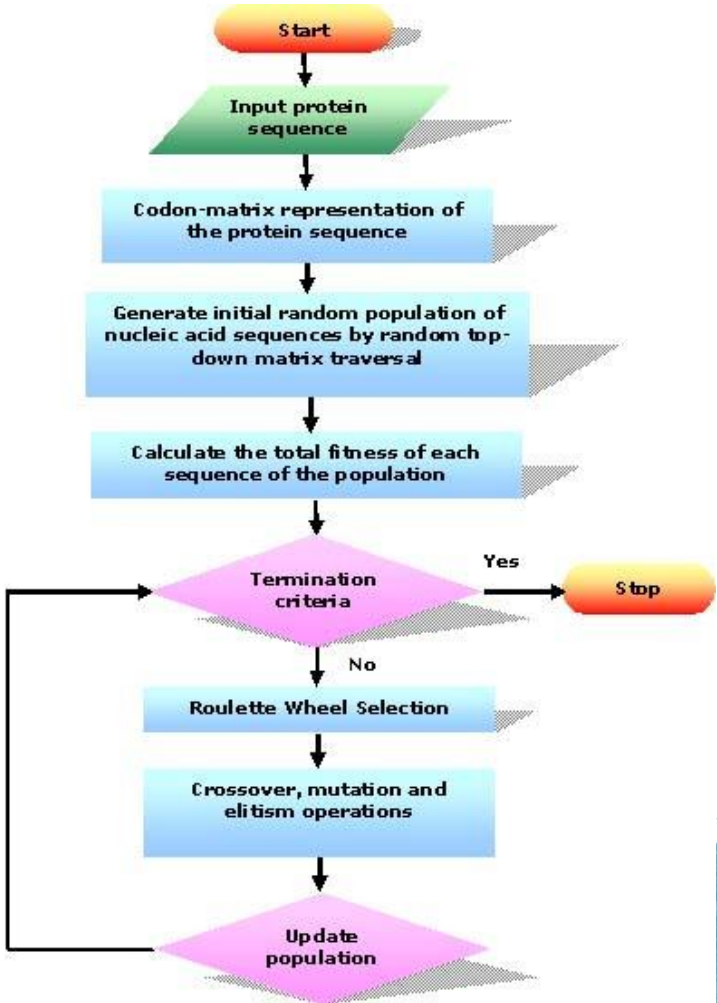
Task: determine bz knowing f(bz,Kz) and Kz

Use a genetic algorithm

Solution: random value bz'

Minimize DT(f(bz,Kz),f(bz',Kz))

It works !



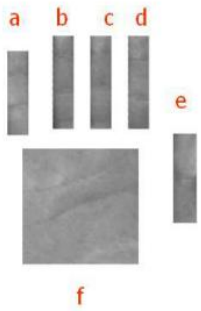
OUTLINE

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

Perspectives

Biometric authentication is necessary

- To make a real user authentication
- In order to guarantee the security of a mobile (contactless) transaction
- Many candidates biometric modalities
- Using secure elements to store and processing the data
- Many robust algorithmic solutions to enhance the privacy of users exist



Perspectives

Many trends have to be considered

- Centralized or decentralized storage of biometric data (example of UID in India)
- Is one biometric data enough ?
- Will it be possible to use biometric data enrolled by governments ?
- How to avoid the replay attack ?
- Is there any other biometric modalities that could be used (tongue...)
- Are services ready to use an authentication that "could" be good ?

Perspectives

New biometric modalities

Can we be recognized based on what we think ?

Very soon...

http://www.epaymentbiometrics.ensicaen.fr/