Biometric cryptography:
a solution to protect privacy?

Global Forum

21 October 2008

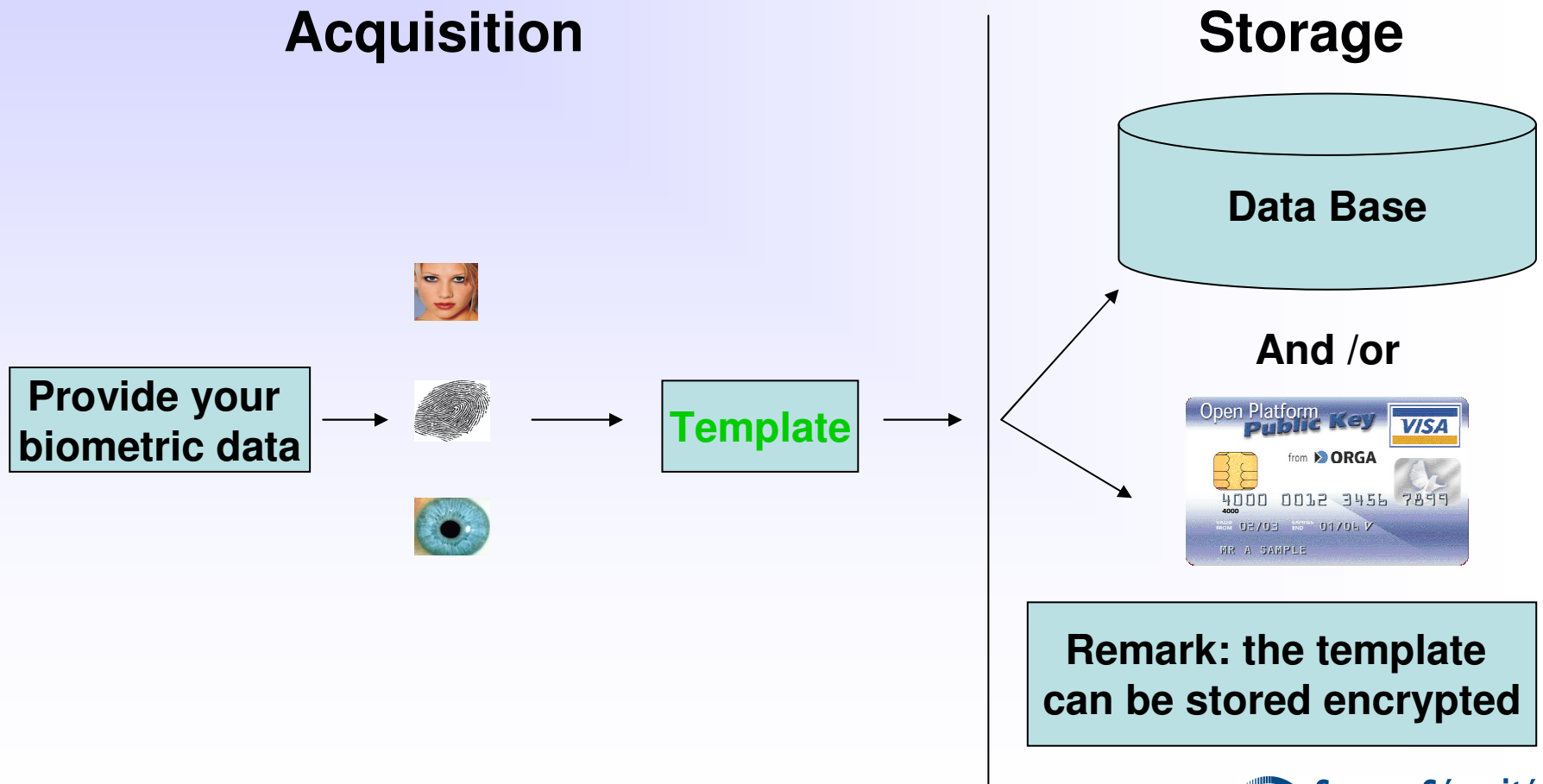Athens

Jean-Marc Suchier

Sagem Sécurité
Groupe SAFRAN

Biometrics: what for?

- Main goal of biometrics: Protect your Identity
  - Check that you are:
    - The true owner of this passport
    - The true owner of this credit card
    - The person authorised to enter this building /door
    - ....
  - Detect that nobody is trying to steal your identity

Sagem Sécurité
Groupe SAFRAN

How does it work?

- Enrolment (only once per application)

Acquisition

Storage

Data Base

And /or

Provide your biometric data → → **Template** →

Open Platform **Public Key** VISA
from ORGA
4000 0012 3456 7899
4000
VALID 02/03 THRU 01/06 V
MR A SAMPLE

Remark: the template can be stored encrypted

Sagem Sécurité
Groupe SAFRAN

How does it work?

- Authentication (each time you want to use it)

Acquisition

Storage

Provide your biometric data

Template

Same template?

Yes

No

Template

Or

Open Platform
Public Key   VISA
from ▶ ORGA
4000 0012 3456 7899
4000
VALID FROM 02/03   EXPIRES END 01/04 V
MR A SAMPLE

Template unencrypted

Sagem Sécurité
Groupe SAFRAN
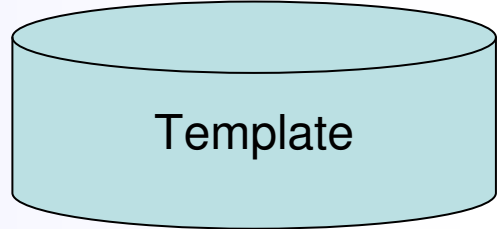
Can we improve privacy protection?

- Fake biometrics
  - The issue
    - If I have got your picture, a trace of your fingerprint, can I fake the system?

  - The answer:
    - Better technology to detect that it is faked data
      - Real person in front of a camera, not a picture
      - The fingerprint comes from a live finger (not a faked one)
      - The iris is live, and does not come from a lens
      - Combination of several modalities
   - ......
    - Human supervision

Can we improve privacy protection?

- Unforeseen use (Function creep)
  - If somebody gets access to the template from my stolen biometric passport , can he/she use it to access my bank account or my medical file, or…..?

- Is this possible?
  - Not so easy!
    - In sensitive applications, templates are encrypted.
      - They must be cracked
    - A direct access inside the targeted system is then needed
  - But an improved protection would be useful in the future, for very large deployment

Sagem Sécurité
Groupe SAFRAN

The approach to improve privacy protection

- Europe is a pioneer in data protection regulation
  - Regulation in place in member states

- **The "privacy by design" approach**

  - Enabling multiple identities for one unique individual
    - ID card
    - e-government
    - e–commerce
    - Social networks

  - Allowing an identity to be repudiated (revocable)

Sagem Sécurité
Groupe SAFRAN

Biometric cryptography: a solution?
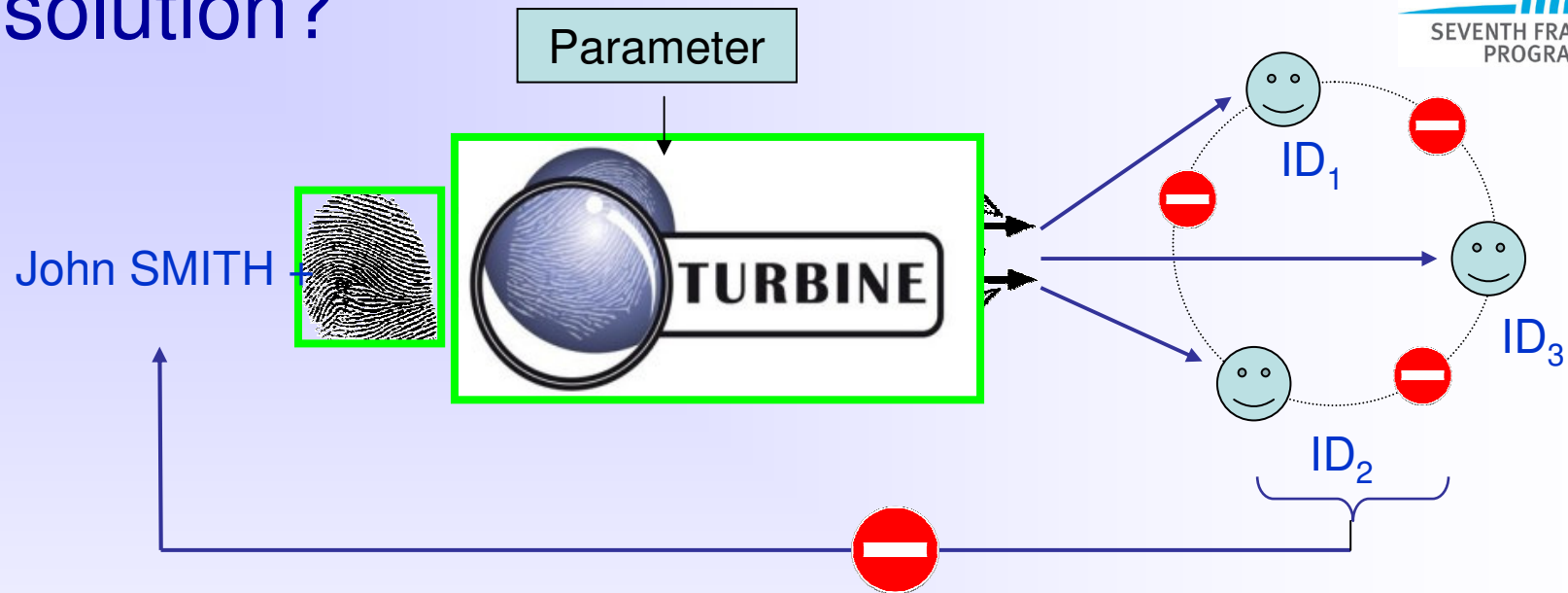
To transform fingerprint

1. into "pseudo-identity"
   - Parameters create independent identities: ID_1, ID_2, … ID_n
   - No possibility to link different "pseudo-identities"
2. without reverse-engineering capability

   ➔ **Revocation** of pseudo-identity is possible!

Europe leading research in privacy protection

- Several collaborative research projects funded by the European Commission. The key ones:
  - 3D Face, for facial data
  - TURBINE, for fingerprint data

- Results
  - They are promising
  - Still a couple of years to market large scale solutions

Sagem Sécurité
Groupe SAFRAN

Thank you for your attention

Jean-marc.suchier@sagem.com

Sagem Sécurité
Groupe SAFRAN