3D Face
Biometric Research

End-Users' Group Meeting Darmstadt

22th of March 2007

3D Face Technical Specifications

3D Face
Biometric Research

3D Technical Specifications: Presentation Overview

- General context of the system prototype
- Using the system in 4 stages
- Technical description of the system
- Legal issues
- Next steps for technical specifications

3D Technical Specifications: General Context

- The 3D Face prototype is an access control system
- Goals of the prototype:
  - To validate the concept of facial 3D recognition access control
    - Quick and easy
    - Non-intrusive
    - Accurate (better than the current state of the art)
    - Secure
  - To evaluate several solutions for the system and choose the best one
    - Biometric strategy
    - Data management

3D Face
Biometric Research

3D Technical Specifications: General Context

- The system will be deployed in several places:
  - Berlin Schönefeld Airport
  - BKA
  - Salzburg Airport
- Test objectives are (for each location):
  - 100 staff members or
  - 900 passengers
- Operational tests begin in December 2008

3D Face
Biometric Research

3D Technical Specifications: General Context: 4 Stages

- **4 Stages for the 3D Face Access Control System:**
  - **Enrolment**
  - **Authentication**
  - **De-enrolment**
  - **Re-enrolment**

- **For the person out of test population the former system will work in parallel**

3D Face
Biometric Research

3D Technical Specifications: Enrolment

- **Enrolment**

During the enrolment all data necessary for the authentication are recorded

- The person goes to the enrolment desk
- 3D and 2D biometrics are acquired by an operator
- The biometric data and/or templates are stored
  - On secure RFID card given to the person
  - In a protected database
- Some other data are stored as
  - Person ID
  - Height (useful for height adjustment)
  - Access rights
  - Validity period
  - ..

3D Face
Biometric Research

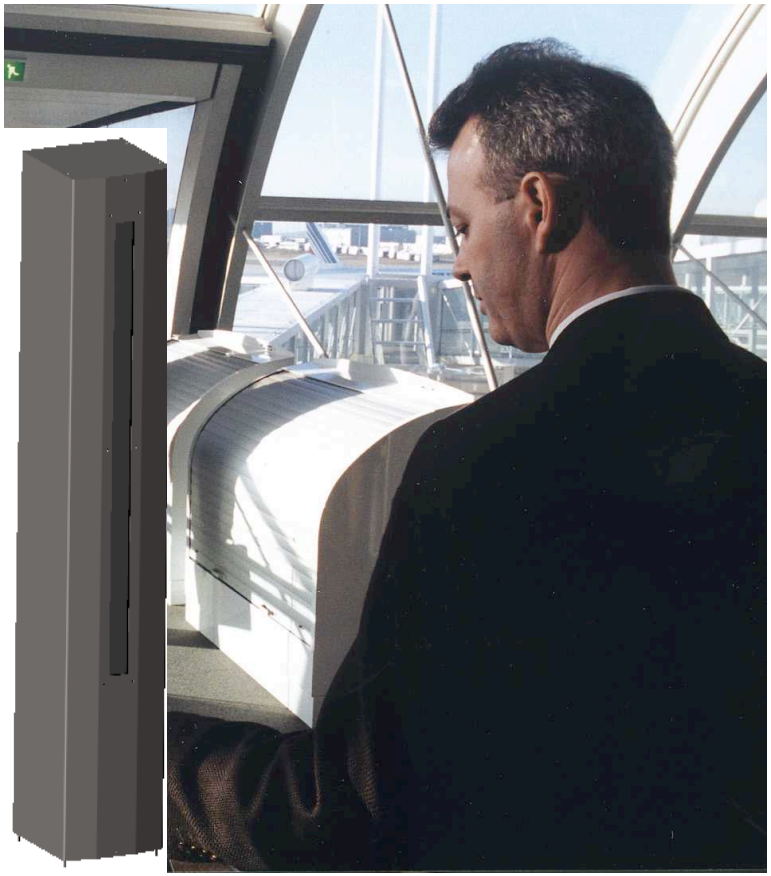
3D Technical Specifications: Authentication

- **Authentication**

The person has to access to a secured area, he must be authenticated

Five scenarios are possible:

- **First Scenario: the normal one (98 % of cases)**
  - **a) The user presents his/her card**
  - **b) He faces the 3D sensor**
  - **c) He is recognised as the proper user of the card**
  - **d) The access is granted**
  - **e) He goes through the access control device**



3D Technical Specifications: Authentication

- **Second scenario: failure to recognise**

  a) The user presents his card
  b) He faces the 3D sensor
  c) He is not recognised as the legitimate user of the card
  d) The door remains closed
  e) He cannot go through the access control device
  f) He has to start the authentication process again

If the problem persists : back up solution

3D Face
Biometric Research

3D Technical Specifications: Authentication

- **Third Scenario: failure to acquire**

  a) The user presents his card

  b) He faces the 3D sensor but not properly (e.g.: bad pose, occlusion, strong movement)

  c) The system fails to acquire correctly the user data

  d) The door remains closed

  e) He cannot go through the access control device

  f) He has to start the authentication process again

If the problem persists : back up solution

3D Face
Biometric Research

3D Technical Specifications: Authentication

- **Fourth Scenario: failure to read data**

  a) The user presents his card

  b) The system reads unauthorised data (bad area, bad validity period..) or cannot read the card properly

  c) He is rejected

  d) The door remains closed

  e) He cannot go through the access control device

  f) He has to present his card again or go to another checkpoint

If the problem persists : back up solution

Unauthorized access attempts are logged

3D Technical Specifications: Authentication

- **Fifth Scenario: Fake detection**

a) The user presents his card

b) He faces the 3D sensor

c) He is detected as an impostor (fake detection) and then rejected

d) The door remains closed

e) He cannot go through the access control device

d) A signal is sent to the security office

Faking attack detection is addressed by the project but the prototype should integrate only simple countermeasures.

3D Technical Specifications: De-enrolment

- The person does not need to access to secured areas anymore
- He must be de-enrolled
  - The person gives back the encrypted card
  - The card is invalidated
  - The biometric data are suppressed from the database

3D Technical Specifications: Re-enrolment

- Re-enrolment is a particular case of enrolment
- It is performed if the person is rejected permanently (face changes over time, or bad enrolment)
- If the person looses his card.
  - The person goes to the enrolment desk
  - 3D and 2D biometric are acquired by an operator
  - The biometric and/or templates are updated
    - In the secured database
    - On a secured RFID card given to the person
  - If the card has been lost, it is invalidated in the system

3D Technical Specifications: Technical Description

- **The prototype must be flexible:**
  - **Different assumptions are made (e.g.. database or not)**
  - **This strategy insures a great freedom to research tasks**
  - **It is planned to be able upgrade the components**

3D Technical Specifications: Technical Description

- The main entities of the 3D Face authentication system are:
  - The enrolment station
    - Acquires the biometric data of the person to enroll
    - Acquires metadata: name, access rights, validity period etc..
    - Stores this information on
      - A secured database
      - A secured RFID card
    - Checks if the person is already in the database
    - Supports template protection

3D Technical Specifications: Technical Description

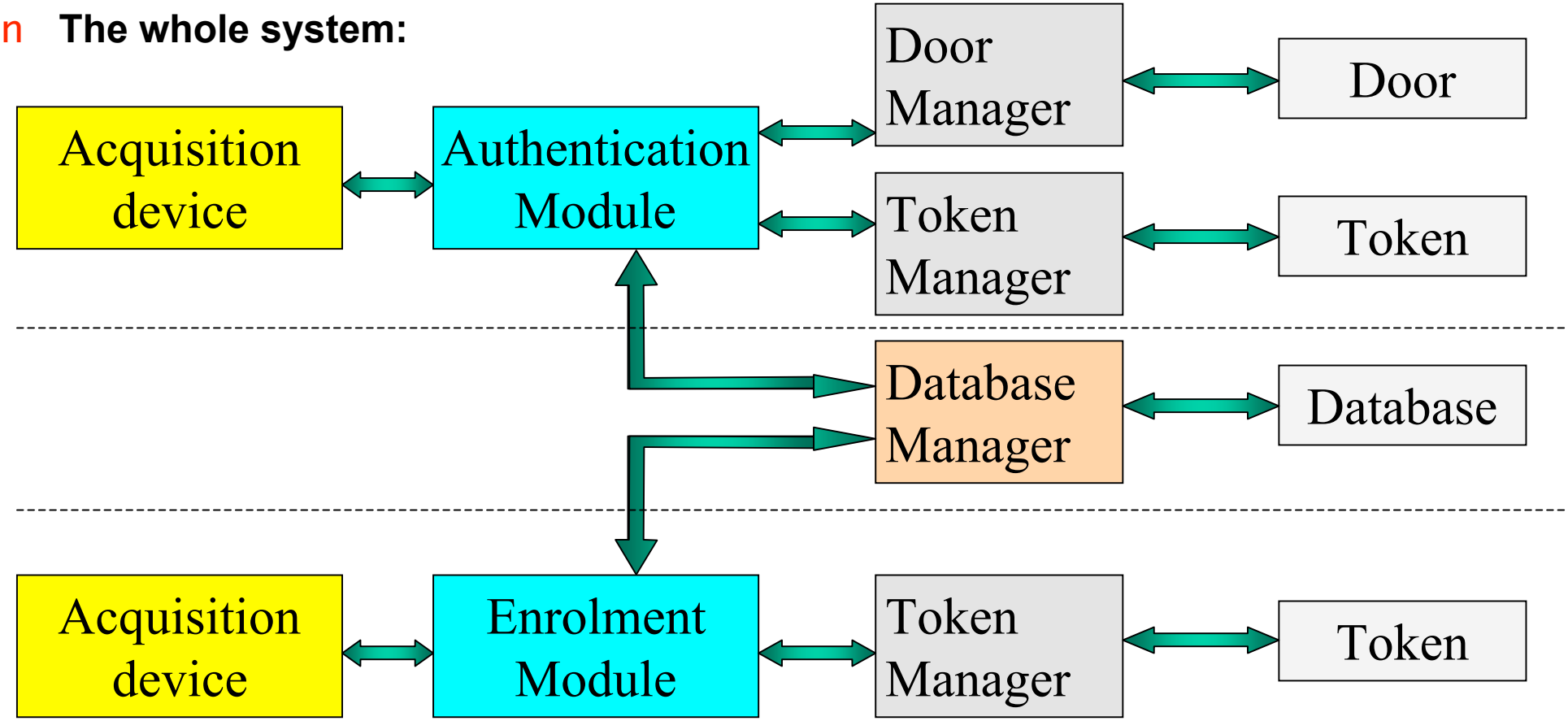
- The authentication station
  - Acquires the biometric information of the access applicant person
  - Performs the authentication process using the data stored
    - In the database or
    - On the encrypted card
  - Accepts / rejects the person
  - Actions associated to recognition result:
    - Opening a door or
    - Giving the authentication result to an operator
    - Logging the authentication result
  - Ensures system performance monitoring (Rejection rate, Acquisition Failure ..)
  - Supports template protection

3D Technical Specifications: Technical Description

- **The database module**
  - **Stores biometric data and metadata data**
  - **Answers to request on the biometric data**
  - **Stores authentication sessions information for off line replay**
  - **Allows access right management**
  - **Allows system monitoring (mainly by logging management)**

3D Technical Specifications: Technical Description

- **The whole system:**



3D Technical Specifications: Legal Issues

- **The prototype must be compliant with legislation concerning:**
  - **Database management (privacy legislation)**
  - **Labor legislation**
  - **Security procedures**
  - **Safety (illumination, electrical…)**

3D Face
Biometric Research

3D Technical Specifications: Next steps

- **Validate the technical specifications with new airport partners**
- **Refine the architecture of the whole system**
- **Validate the compliance of the system with legal obligations**

  - **End of October 2007: The whole integration process is <u>defined</u>**

Thank you