Introduction
Biometric Systems (DTU 02238)

Christoph Busch

Session 1 and 2

Overview

Structure of this session

- Organizational issues and term papers
- Definition of Biometric Recognition
- Reference Architecture and process stages
- Harmonized Biometric Vocabulary
- Advantages and disadvantages of biometrics
- Examples of biometric characteristics and applications

Biometric Characteristic

Biometric activities

- Lecturer in Darmstadt, Gjøvik and Copenhagen
- Convener of the Working Group 3 on Biometric Data Interchange Formats in ISO/IEC JTC1 SC37
- Board-member European Association for Biometrics
- Chair of the TeleTrusT working group on Biometrics
- Co-Chair of the Norsk Biometri Forum

Recent projects related to Biometrics

- Hochschule Darmstadt:
  - HWMK/BMBF ATHENE https://www.athene-center.de/en/
  - BSI DIRECT-PAD
  - EU H2020 iMARS, TReSPAsS
- NorwegianBiometricsLab@NTNU:
  - EU H2020 iMARS https://imars-project.eu/
  - eu-LISA https://christoph-busch.de/projects-euLISA
  - IKTPLUSS SWAN https://www.ntnu.edu/iik/swan

Organizational Matters

Lecturer contact information:

Prof. Dr. Christoph Busch
Hochschule Darmstadt
ATHENE
Schöfferstr. 10
64295 Darmstadt, Germany

- email: `christoph.busch@h-da.de`
- Skype: chr.busch

Teaching assistants:

- Mathias Ibsen
- email: `mathias.ibsen@h-da.de`
- Pia Bauspiess
- email: `pia.bauspiess@ntnu.no`

Organizational Matters

Scope and form:

- Lectures and individual project

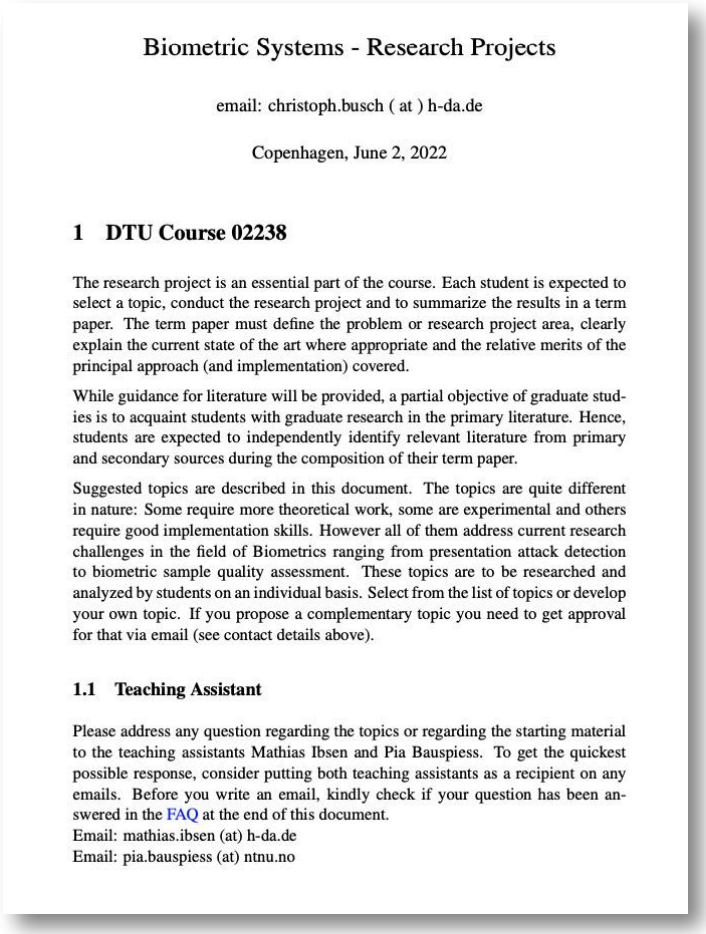
Duration:

- June 02 - June 23 (3 weeks)
- Lectures: June 07 - June 10

Organizational Matters

Type of assessment:

- Evaluation of term papers (research reports)
- Final submission deadline on June 27th at 23.59h
- 12 page research paper
- See course syllabus for further details: Syllabus-dtu-02238.pdf
- Register for a project topic by June 9th at: https://framadate.org/F6FFMwASiiebT2wF
  - Password: Bio22DTU
  - first come - first served



Biometric Systems - Research Projects

email: christoph.busch (at) h-da.de

Copenhagen, June 2, 2022

1 DTU Course 02238

The research project is an essential part of the course. Each student is expected to select a topic, conduct the research project and to summarize the results in a term paper. The term paper must define the problem or research project area, clearly explain the current state of the art where appropriate and the relative merits of the principal approach (and implementation) covered.

While guidance for literature will be provided, a partial objective of graduate studies is to acquaint students with graduate research in the primary literature. Hence, students are expected to independently identify relevant literature from primary and secondary sources during the composition of their term paper.

Suggested topics are described in this document. The topics are quite different in nature: Some require more theoretical work, some are experimental and others require good implementation skills. However all of them address current research challenges in the field of Biometrics ranging from presentation attack detection to biometric sample quality assessment. These topics are to be researched and analyzed by students on an individual basis. Select from the list of topics or develop your own topic. If you propose a complementary topic you need to get approval for that via email (see contact details above).

1.1 Teaching Assistant

Please address any question regarding the topics or regarding the starting material to the teaching assistants Mathias Ibsen and Pia Bauspiess. To get the quickest possible response, consider putting both teaching assistants as a recipient on any emails. Before you write an email, kindly check if your question has been answered in the FAQ at the end of this document.
Email: mathias.ibsen (at) h-da.de
Email: pia.bauspiess (at) ntnu.no

Organizational Matters

Research Topics

Machine Learning for Fingerprint Recognition: An Overview (MFR)(0.4)
Contactless Fingerprint Feature Extraction and Comparison (FPE)(0.9)
Modeling realistic 2D contactless Finger Images (MTL)(0.7)
Color-based Comparison of contactless Fingerprint Images (CCF)(0.7)
Survey on Hand Recognition (SHR)(0.4)
Face Morphing Attack Detection (MAD)(0.8)
Survey on Child Face Recognition (SCR)(0.4)
Face Mask Analysis (FMA)(0.7)
Tattoo Detection Survey (DTS) (0.4)
Face Morphing Capacity (FMC)(0.8)
Face Beauty Score (FBS)(0.4)
Blurred Face Image Quality (FIQ)(0.8)
Face Anonymisation Experiments (FAE)(0.8)
Face Stretching Analysis (FSA)(0.7)

Organizational Matters

Research Topics (cont.)

Survey about Face Age Modification (SAM)(0.4)
Survey about Face Age Estimation (SAE)(0.4)
Survey about Head Pose Estimation (SPE)(0.4)
Face Recognition Evaluation using Face Compensation Illumination (DCE)(0.8)
Data Projection on Morphing Images (DPM)(0.7)
Face recognition evaluation using Super-Resolution (SSR)(0.7)
Analysing Explainable Visualisation for Morphing Attack Detection (AEV)(1.0)
Survey on Detection of Digital Face Manipulations (DFM)(0.4)
Free 2D Face Recognition Software (FRS)(0.4)
Benchmarking Facial Soft-Biometric Extractors (BFE)(0.7)
Post-Quantum Secure Biometric Systems (PQB)(0.4)
Survey on Inclusive Fairness in Biometrics (IFB)(0.4)
Early-Decision for Biometric Identification (EDI)(0.7)

Organizational Matters

If you are satisfied with your paper:

- Consider submission to the European biometrics conference
- BIOSIG 2022
  - submission deadline July 3rd
- If the paper is accepted there, you will get sponsorship for travel and registration fee
- For further details: http://www.biosig.de

Call for Papers

BIOSIG 2022

21st International Conference of the Biometrics Special Interest Group

14.-16.09.2022, Darmstadt, Germany

http://www.biosig.de

Biometrics Special Interest Group in cooperation with IEEE

Fraunhofer ATHENE

Biometrics provides efficient and reliable solutions to recognize individuals. With increasing number of identity theft and miss-use incidents we do observe a significant fraud in e-commerce and thus growing interests on trustworthiness of person authentication. Nowadays we find biometric applications in areas like border control, national ID cards, e-banking, e-commerce, e-health etc. Large-scale applications such as the upcoming European Union Entry Exit System (EES), the Visa Information System (VIS) and Unique Identification (UID) in India require high accuracy and also reliability, interoperability, scalability and usability. Many of these are joint requirements also for forensic applications.
Multimodal biometrics combined with fusion techniques can improve recognition performance. Efficient searching or indexing methods can accelerate identification efficiency. Additionally, quality of captured biometric samples can strongly influence the performance. Moreover, mobile biometrics is an emerging area and biometrics-based smartphones can support deployment and acceptance of biometric systems.
However, concerns about security and privacy cannot be neglected. The relevant techniques in the area of presentation attack detection (liveness detection) and template protection are about to supplement biometric systems, in order to improve fake resistance, prevent potential attacks such as cross matching, identity theft etc.
The BIOSIG 2022 conference addresses these issues and will present innovations and best practices that can be transferred into future applications. The conference is jointly organized by the Competence Center for Applied Security Technology (CAST), the German Federal Office for Information Security (BSI), the European Association for Biometrics (EAB), the Norwegian Biometrics Laboratory (NBL), National Research Center for Applied Cybersecurity (ATHENE), the Hochschule Ansbach, the Fraunhofer Institute for Computer Graphics Research IGD, IET Biometrics Journal and the special interest group BIOSIG of the Gesellschaft für Informatik e.V. (GI). Accepted papers will be submitted for inclusion into IEEE *Xplore* subject to meeting IEEE *Xplore*'s scope and quality requirements (approval pending).

We invite stakeholders and technical experts to submit original research papers. Industrial contributions presenting lessons learnt from practical usage, case study, recent results of prototypes, are also welcomed.

Important Dates

15.06.2022	Deadline for submissions
25.07.2022	Notification of authors via e-mail
19.08.2022	Deadline for final papers (ready for press)
12.09.2022	Satellite Workshop TTT Working Group
12.-14.09.2022	EAB-Research Project Conference
14.09.2022	EAB European Research and Industry Award
15./16.09.2022	Main Conference: Talks and Presentations

Invited Talks

TBD

Special Interest Group BIOSIG

The BIOSIG Group is dedicated to the foundations of biometrics. Its objective is to to link practical experience with academic innovations. Thus, the Special Interest Group BIOSIG together with its co-organizers is providing with its annual conference a suitable platform to work on these issues.

Topics of Interest

Topics of the conference include but are not limited to: Biometric standards and interoperability, multimodal and multi-biometrics, security analysis of biometric components or systems, on-card comparison, fake resistance, liveness detection, aging of reference data, template protection, de-identification, user interface design for biometric systems, biometric performance measurement, sample quality, best practices, usability, continuous authentication, forensics and other emerging applications, ethical, legal and socio-technological aspects, biometrics for public administrations.

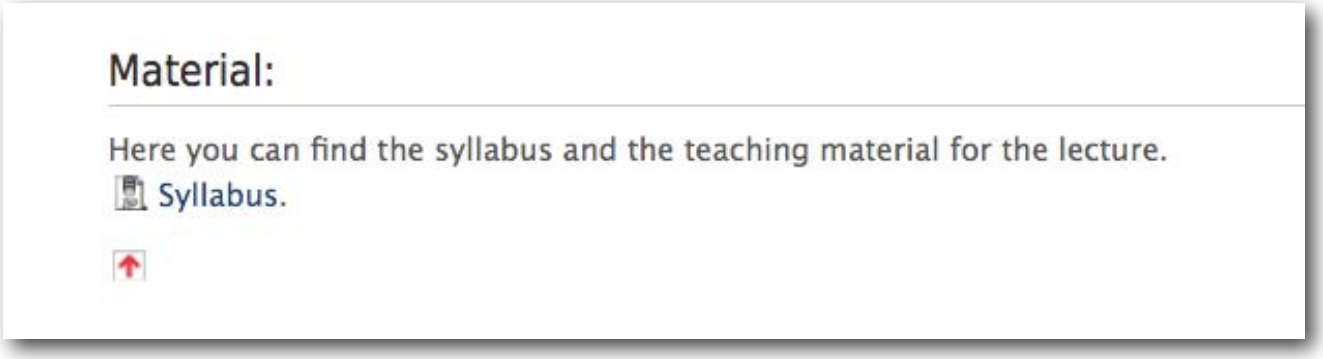
Organizing Committee

General Chair: Marta Gomez-Barrero
Program Chairs: Naser Damer, Antitza Dantcheva, Kiran Raja, Christian Rathgeb, Andreas Uhl
Publication Chair: Arslan Brömme
Publicity Chair: Victor Philipp Busch, Ana Filipa Sequeira
Local Chairs: Alexander Nouak, Claudia Prediger

- check older BIOSIG proceedings: https://dl.gi.de/bitstream/handle/20.500.12116/4660/lni-p-270-komplett.pdf

Organizational Matters

- Slides of the lecture will be available:
  - http://www.christoph-busch.de/teaching-biometric-systems.html



  - password: „lyngby-2022“

- Complementary reading material

NOTE: Partly copyrighted material !

Organizational Matters

Recommended reading

- A. Jain, P. Flynn, A. Russ
  Handbook of Biometrics, Springer, 2008
- S. Li and A. Jain
  Handbook of Face Recognition, Springer, 2011
- D. Maltoni , D. Maio, A. Jain, S Prabhakar
  Handbook of Fingerprint Recognition, Springer, 2009
- S. Marcel, M. Nixon, J. Fierrez, N. Evans
  Handbook of Biometric Anti-Spoofing: Presentation Attack Detection
  Springer, 2019.
- P. Tuyls, B. Skroic, T. Kevenaar
  Security with Noisy Data, Springer, 2007
- A. Uhl, C. Busch, S. Marcel, R. Veldhuis
  Handbook of Vascular Biometrics, Springer, 2020
- C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, C. Busch
  Handbook of Digital Face Manipulation and Detection, Springer, 2021

These books are **recommended only** - not mandatory

Introduction

The lecture covers:

- An overview on biometric systems

Introduction

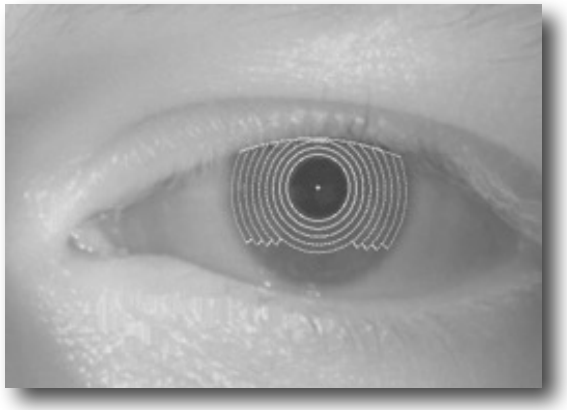
The lecture covers:

- An overview on biometric systems
  - Introduction to Biometrics
  - Evaluation of Biometric Systems
  - Fingerprint Recognition
  - Vein Recognition
  - Face Recognition
  - Iris Recognition
  - Sample Quality
  - Privacy and Data Protection
  - Security Risks of Biometric Systems
    - Presentation Attack Detection
    - Template Protection
  - Machine Learning
  - Multibiometrics
  - Case Studies (ePassport, Identification Systems)

Introduction

What is Biometrics?

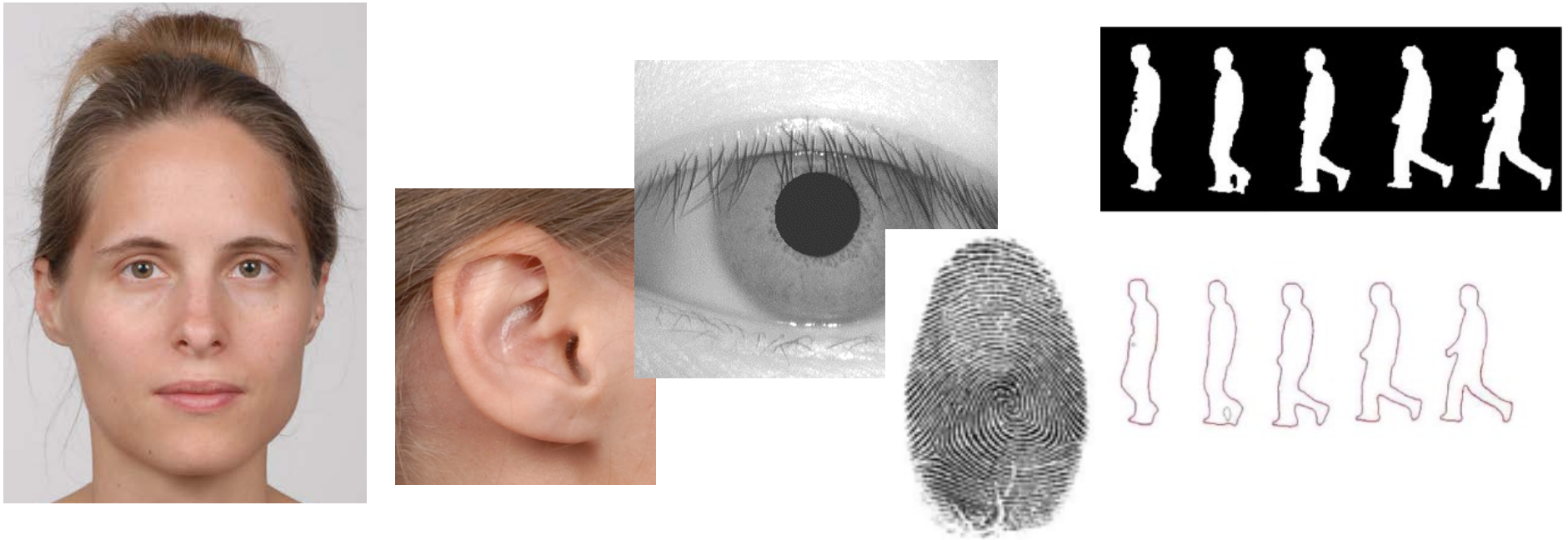
- The observation (greek: „μετρειν“) of characteristics of the human body for the purpose of identification (recognition)



staff identity = „busch“

Definition

- International Organization for Standardization defines:
  - **Biometrics**:
    "*automated recognition of individuals based on their behavioural and biological characteristics* "
  - Remark: behavioural has to do with the function of the body
    biological / anatomical has to do with the structure of the body



Access Control

Authentication can be achieved by:

- Something you know:
  Password, PIN, other secret

Passwords and PIN

PINs are a tragic choice

- PINs are exploiting our (brains) resources
  - the concept works well, when we have to manage only a few passwords but in reality we are expected to remember more than 100 passwords and we fail to do so

Some Statistics to Passwords

Password Statistics based on 32 million passwords

- 20% were names and trivial passwords
- Top 5 passwords:

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622

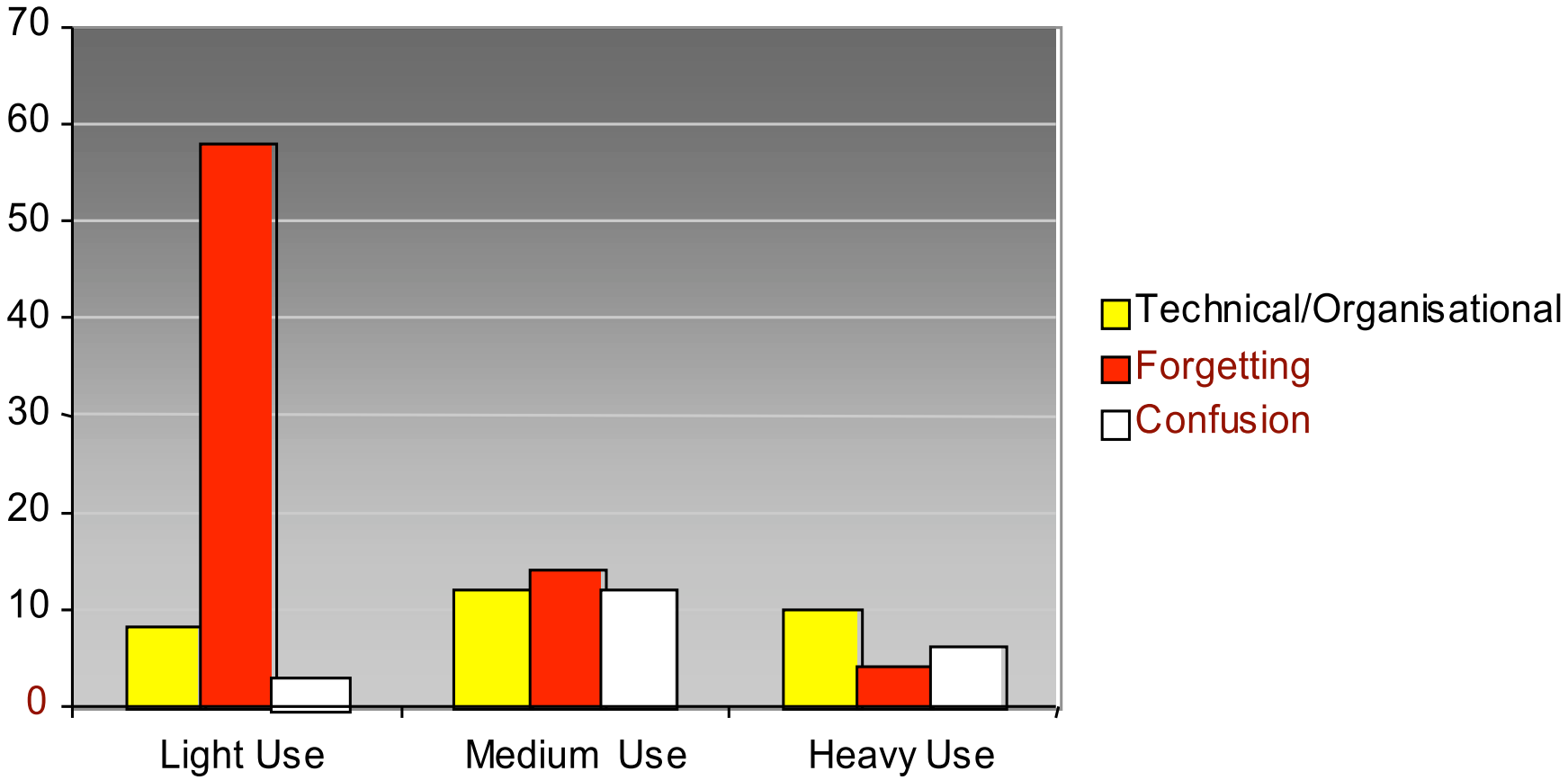
Source: Imperva 2009

- Check your password strength: http://www.passwordmeter.com

Some Statistics to Passwords

Password Survey by A. Sasse (2002)

- Forgetting biggest problem - 56%
  especially for lightly used (1 per month) passwords



Access Control

Authentication can be achieved bv:

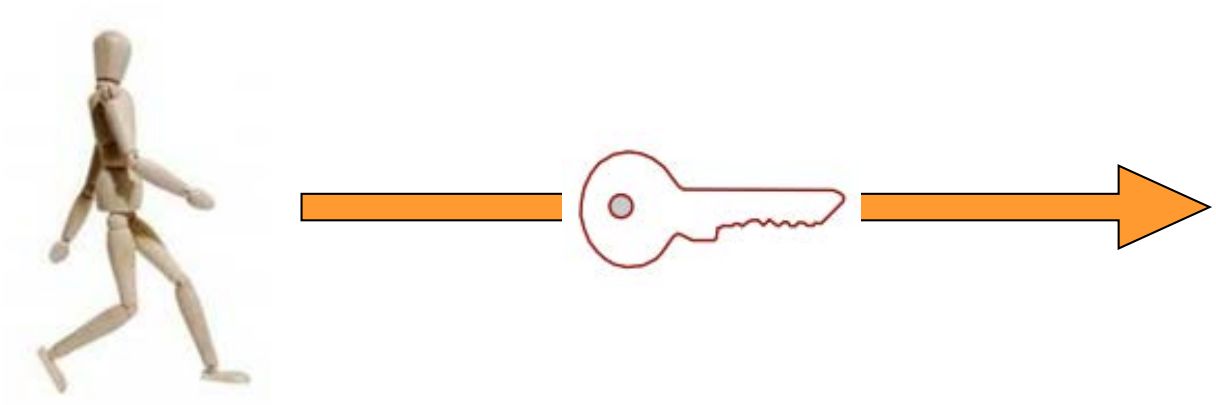
- Something you know:
  Password, PIN, other secret

- Something you own:
  SmartCard, USB-token, key

Access Control

Traditionally we place between

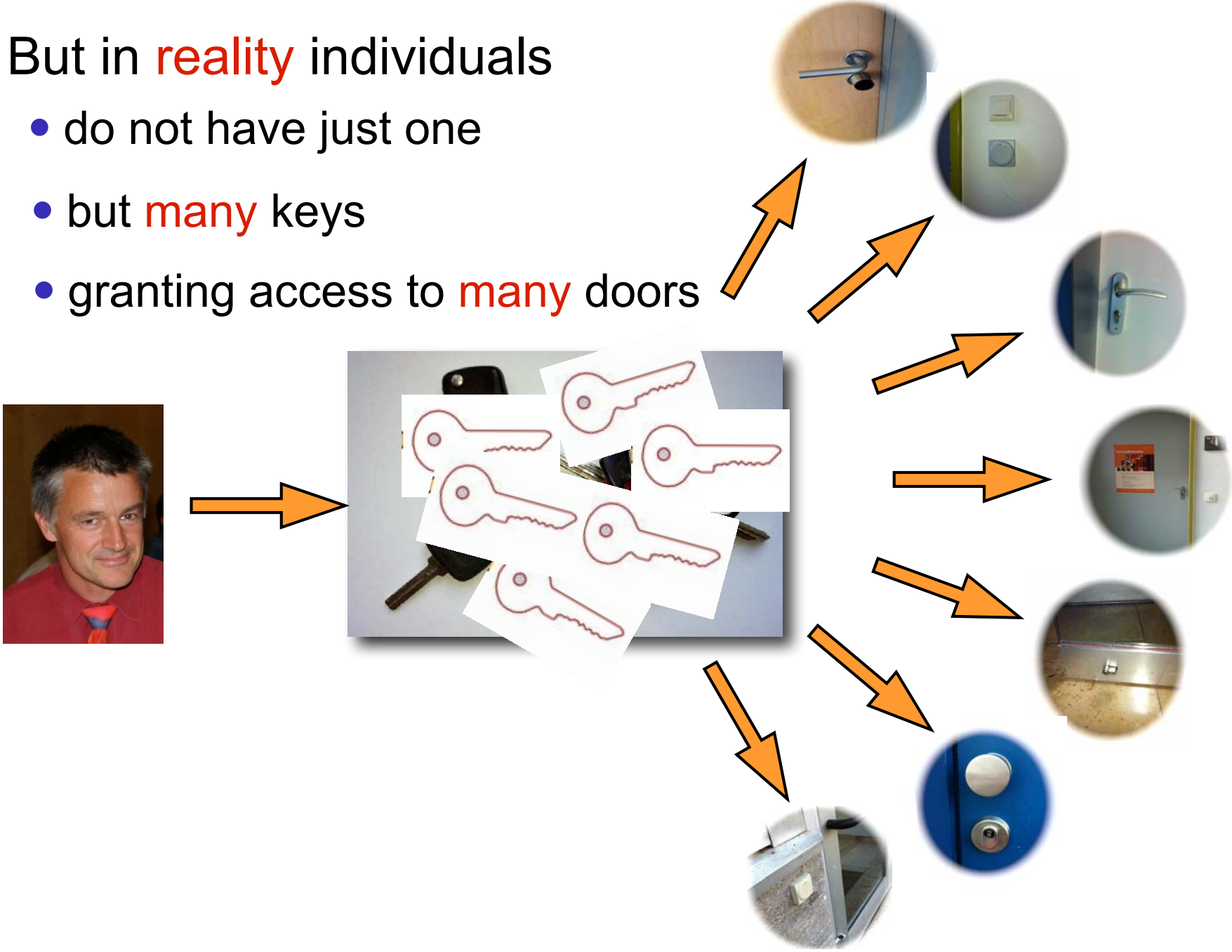
- individuals
- and objects
- a token (i.e. key)



Access Control

But in reality individuals

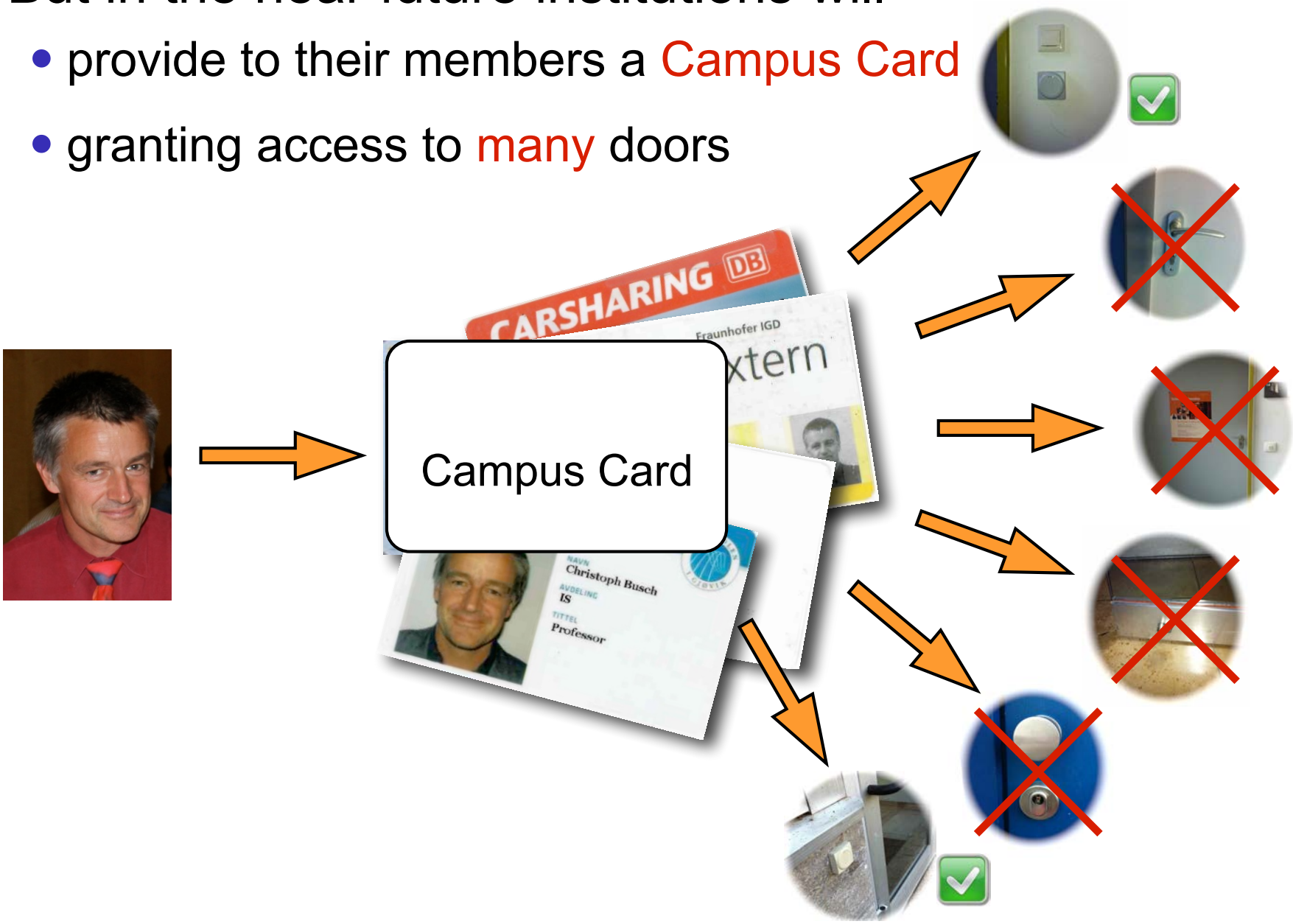
- do not have just one
- but many keys
- granting access to many doors



Access Control

But in the near future institutions will

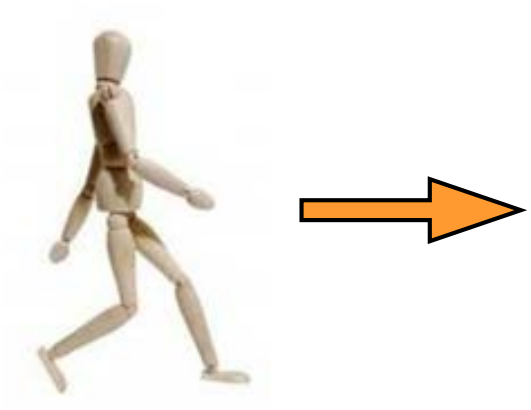
- provide to their members a Campus Card
- granting access to many doors



Access Control

For some individuals

- the collection of cards is quite impressive and inconvenient



Access Control

Authentication can be achieved bv:

- Something you know:
  Password, PIN, other secret

- Something you own:
  SmartCard, USB-token, key

- Something you are:
  Body characteristics

Something you know or own
you may loose, forget or forward to someone else,
with biometrics this is more difficult.

Benchmark of Biometrics and PIN

There are two striking arguments why biometric authentication is better than the PIN

- 1.) The entropy of a 4 or 6-digit PIN is very limited
  - Even for a 6 digit numeric PIN (e.g. with the German eID card) the entropy $H = L * log_2 N$ is limited to less than 20bit (with $L=6, N=10$)
  - The reported entropy for different biometric characteristics is
    - Fingerprints 84bit [Ratha2001], Iris 249bit [Daugman2006] Face 56bit [Adler2006], Voice 127bit [Nautsch2015]

[Ratha2001] N. Ratha, J. Connell, R. Bolle: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, vol. 2091, pp. 223–228. Springer, (2001)

[Daugman2006] J. Daugman: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)

[Adler2006] A. Adler, R. Youmaran, S.Loyka: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering, (CCECE'06). pp. 210–213 (2006)

[Nautsch2015] A. Nautsch, C. Rathgeb, R. Saeidi, C. Busch: Entropy Analysis of I-Vector Feature Spaces in Duration-Sensitive Speaker Recognition, in 40th IEEE ICASSP Conference, 19-24 April 2015, Brisbane, Australia, (2015)

Benchmark of Biometrics and PIN

There are two striking arguments why biometric authentication is better than the PIN

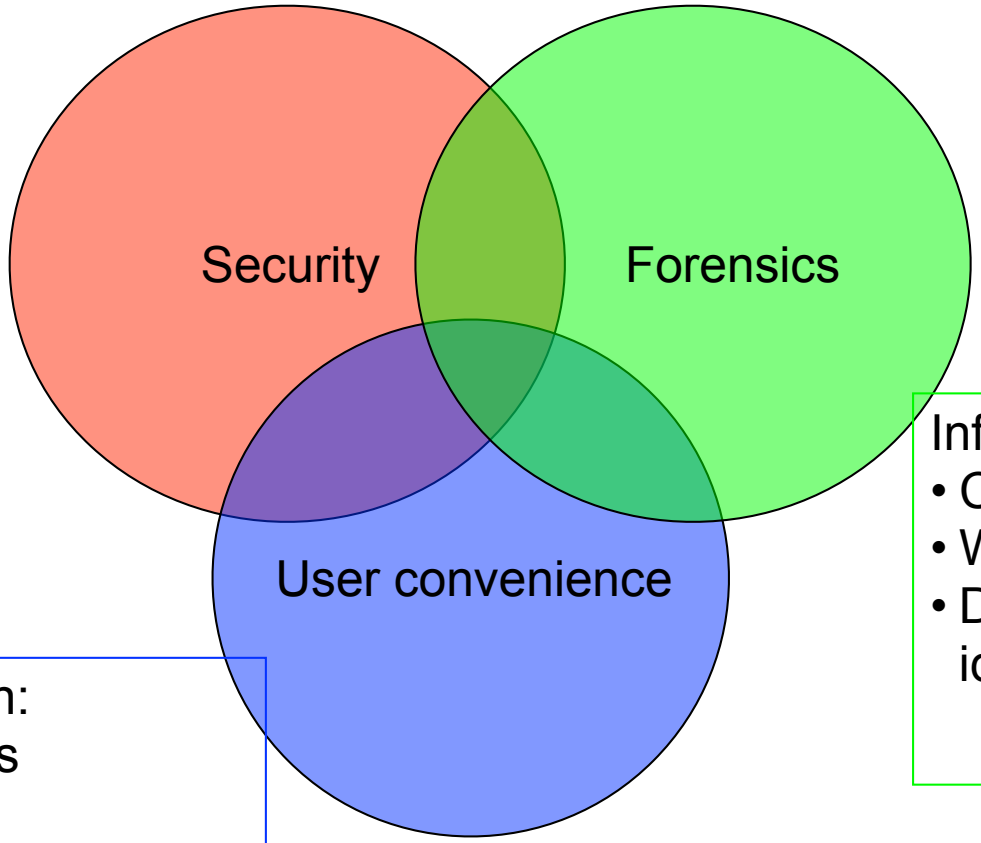
- 2.) PINs can be delegated in violation of the security policy
  - „*This transaction was done by Mr. Popov, who was mis-using my card*“
  - biometric authentication enables non-repudiation of transactions

Biometrics are better than PINs !

Biometric Application Domains

Access control:
- information
- devices / token ownership
- locations

Immigration / Border Control



Information retrieval
- Camera surveillance
- Watch lists
- Disaster victim identification

Personalization:
- home systems
- computers
- social inclusion

Ease of use:
- no PINS/tokens
- ongoing authentication

Biometrics and Blacklist Comparison

Scenario: Banned shopping mall customers

- Shopping mall Amsterdam
- Approx. 1000 individuals in the blacklist

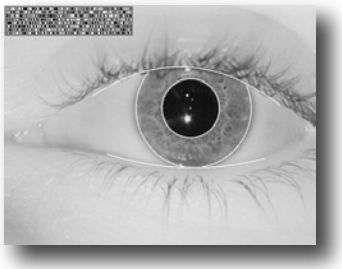
Scenario: Banned travellers

- Visitors with a criminal record are rejected
- US VISIT

Biometrics and Access Control

Scenario:

- Logical Access Control
- Physical Access Control
  - staff member authentication via iris and face
    - improved security with speed gates



  - Reduce fraudulent use of season tickets
    - convenience: season ticket holders do not need to queue up
    - minimized waiting period

Biometrics and Access Control

The Entry-Exit-System (EES)

- will be applied to all external Schengen borders
  - sea, land and air
- will introduce a central register to record all entries/exists and denials to/from the Schengen area
  - for Third Country Nationals (TCN)
- will replace the analog stamping in the passport
- for each traveller a record will be created in the EES
  - identity based on the passport data
  - link to the biometric data
    - facial image of all travelers
    - fingerprint images of visa exempt travelers
- the EES will be linked to the Visa Information System (VIS)

EES will record

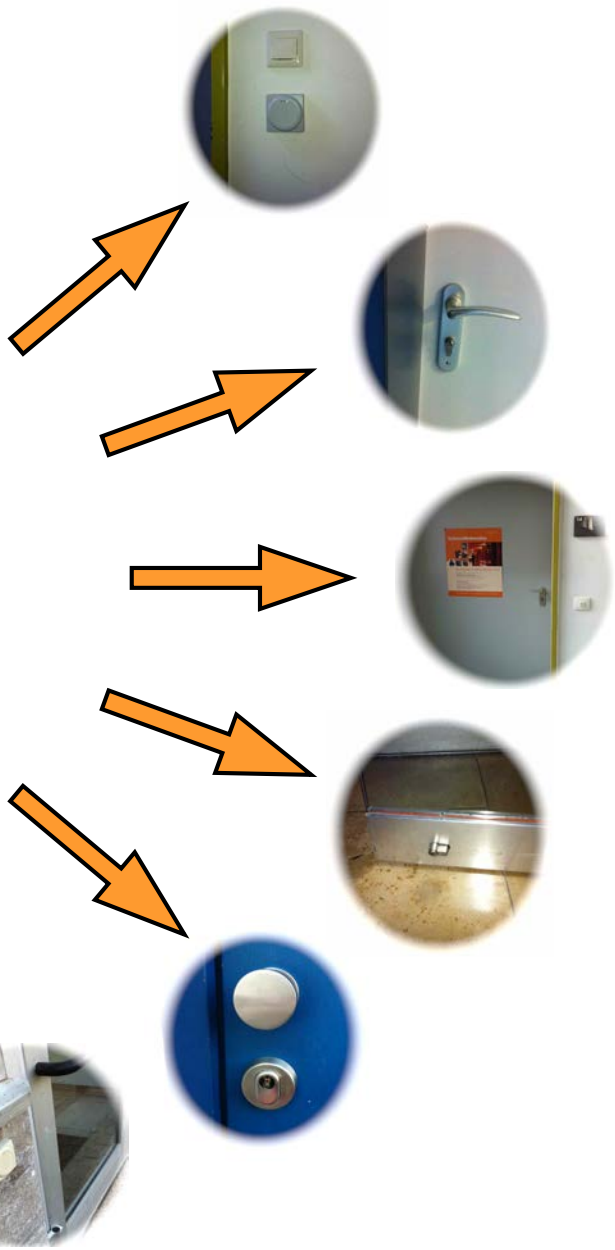
EES will replace

EES will collect

Biometric and Access Control

Should we have

- Biometric access control at every door?

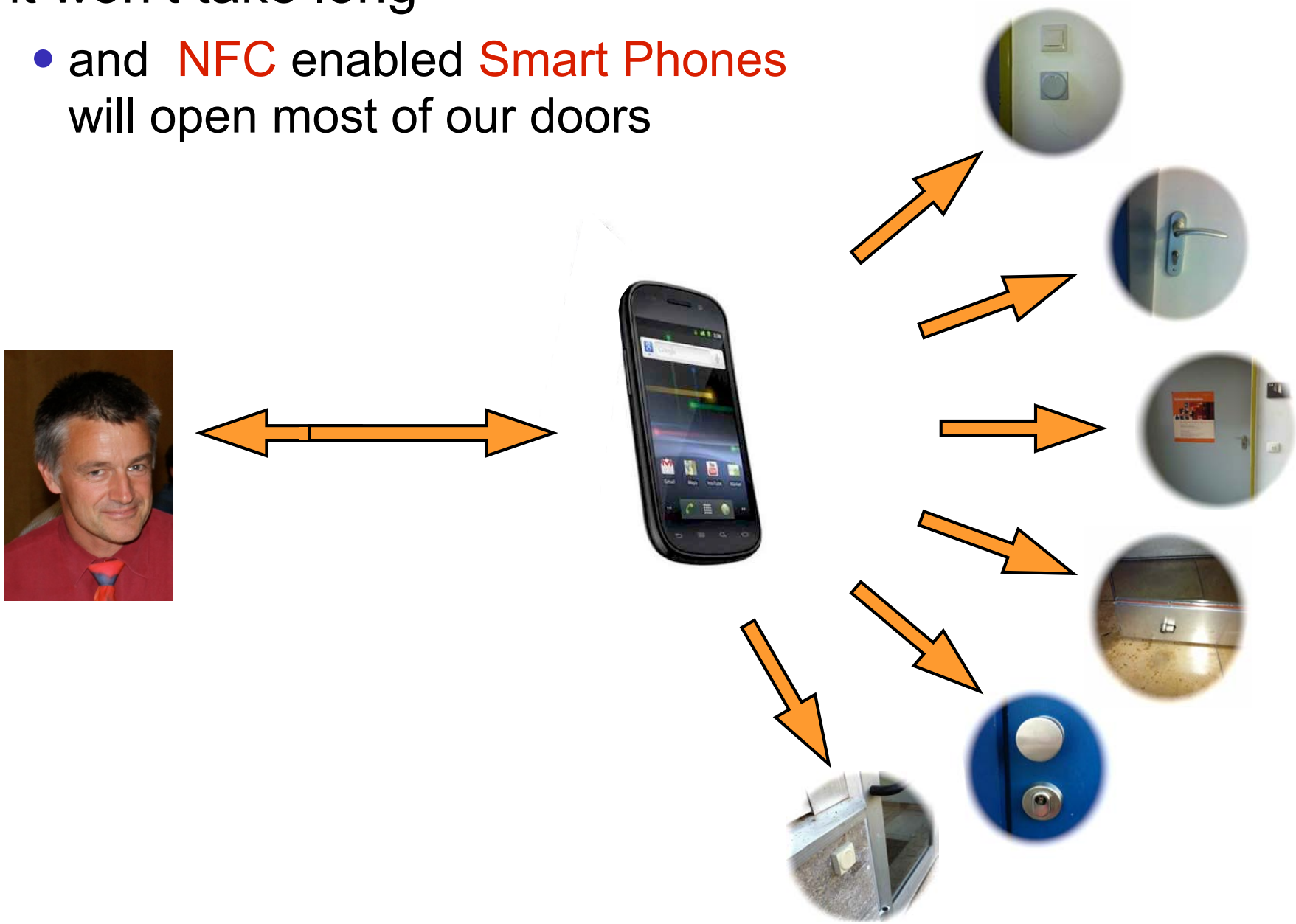


- Cost-factor of sensors?
- Where do we store references?

Smart Phone Based Access Control

it won‘t take long

- and NFC enabled Smart Phones will open most of our doors



Biometric Processing

Workflow in a Biometric System

- Enrolment

Generic Perspective on the Biometric Workflow

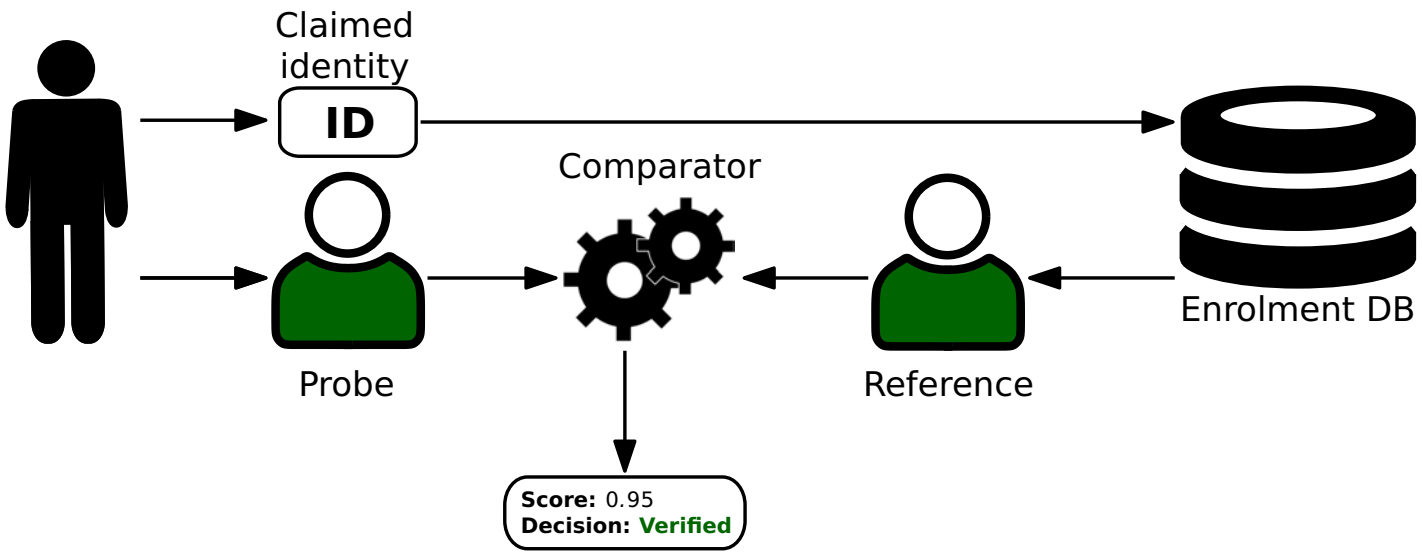
Biometric Workflow

- An analog or digital representation (biometric sample) of a biometric characteristic of the data subject is recorded and stored for reference (enrolment)
  - The data subject („end-user“) is introduced to the system.
- For a recognition attempt the biometric characteristic is recorded again and compared with the stored reference
  - If the comparison score exceeds a defined threshold, the capture subject is authenticated.
- Along with the acquisition of the biometric sample, background processes check whether the presented biometric characteristic is alive
  - Presentation Attack Detection (PAD)

Verification - Identification

Verification

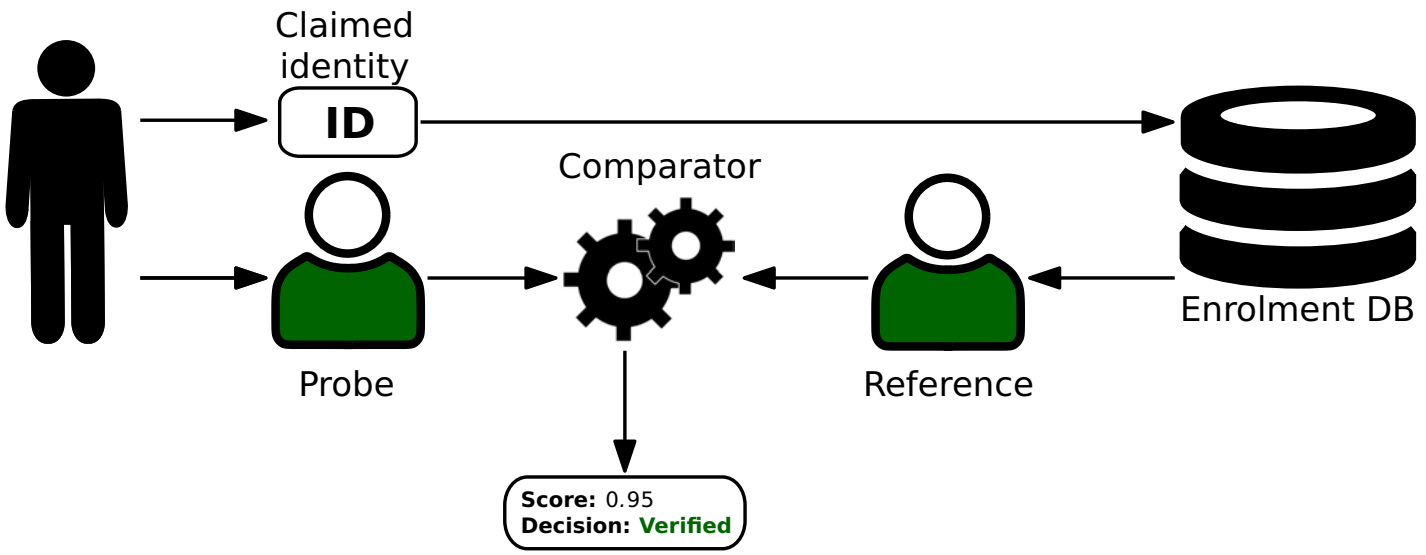
- 1:1
- validate a biometric claim



Verification - Identification

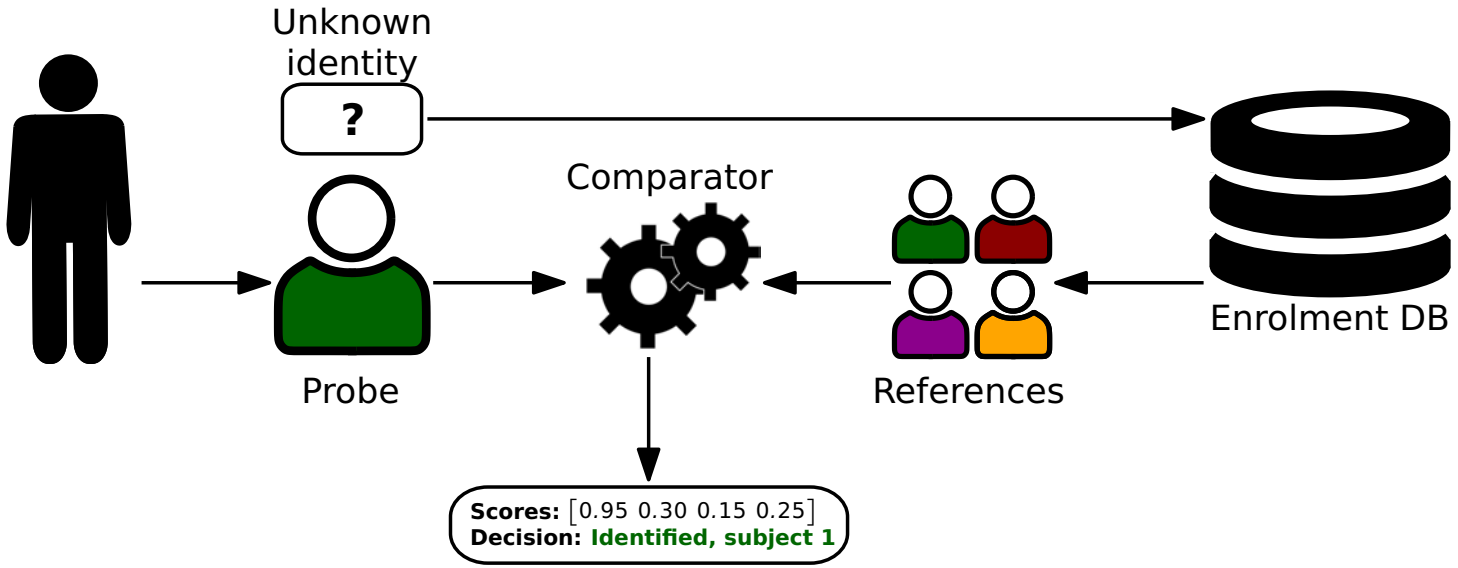
Verification

- 1:1
- validate a biometric claim



Identification

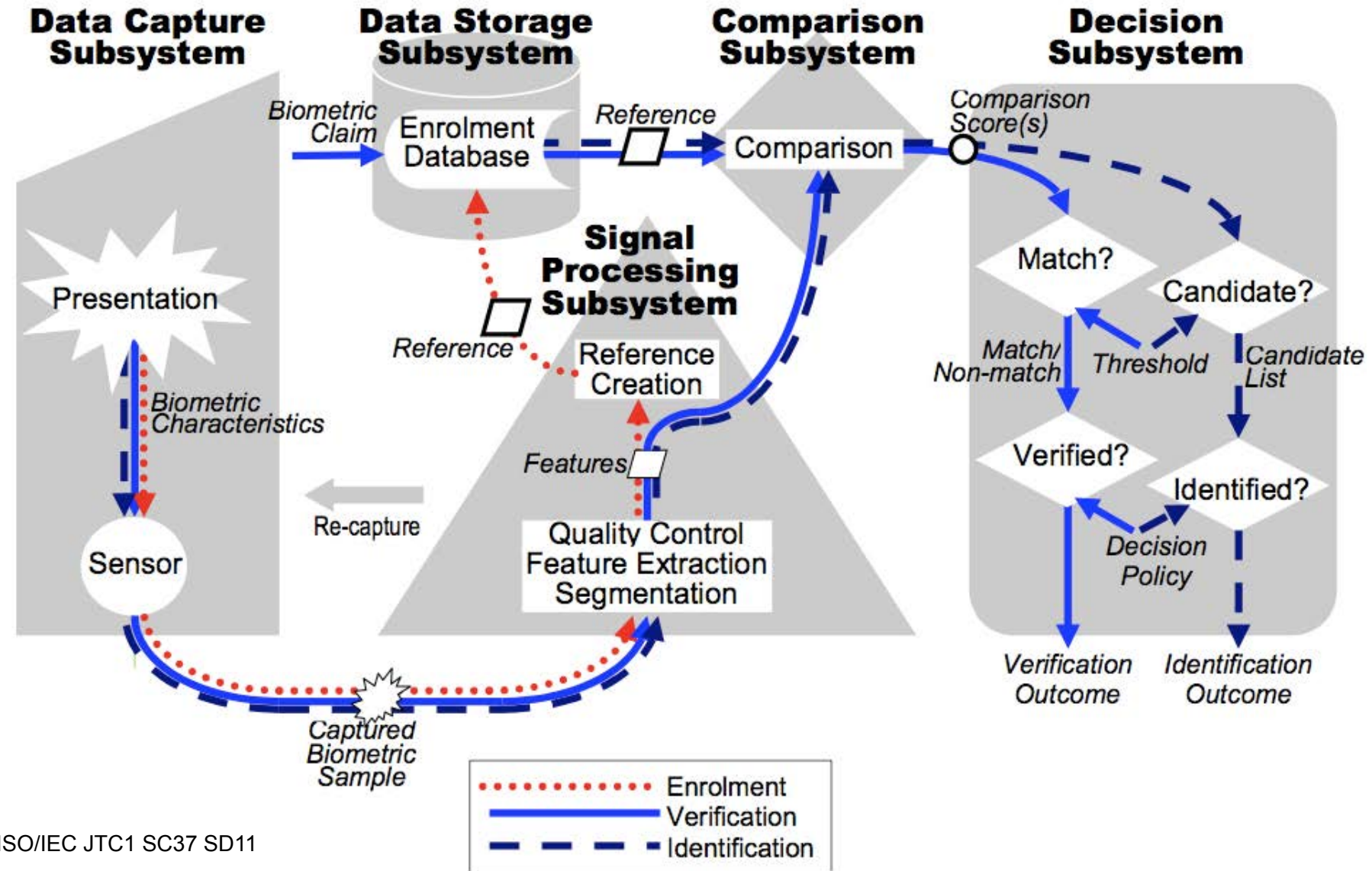
- 1:n search



Architecture of a Biometric System

ISO/IEC SC37 Standing Document 11

- Components of a General Biometric System



Source: ISO/IEC JTC1 SC37 SD11

Properties of Biometric Characteristics / Systems

Biom. Characteristic	Sensor / Acquisition	Properties

Biometric Characteristic

Relevant properties - derived from [JainBoPan99]

- Universality - every individual should have it.
- Uniqueness - is the characteristic distinctive such that any two individuals are sufficiently different.
- Performance - primarily associated with accuracy (low errors) and not with throughput time
- Permanence - the characteristic should be invariant over time. (persistent / immutable / limited ageing effects)
- Collectability - the characteristic is measurable and the quantitive result is reproducible.
- Acceptability - convenient measurement at low cost and unobtrusive for data subjects.
- Circumvention - hard to collect and replicate a fake biometric characteristic (Security)

Biometric Characteristics

Biological

- Fingerprint recognition
- Face recognition
  (also thermogram)
- Retina recognition
- Iris recognition
- Hand geometry recognition
  (also thermal)
- Vein recognition
- DNA recognition
- Ear / Inner ear acoustic recognition

Behavioral

- Keystroke recognition
- Signature recognition
- Voice recognition
- Body movement recognition
  - Gait
  - Lips movements
- Body odor recognition
- EKG recognition

Origins of a Biometric Characteristic

Epigenetic

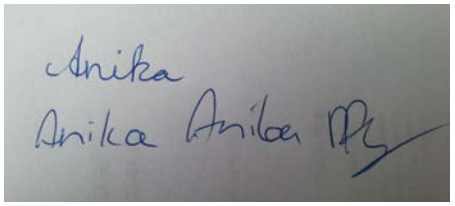
- Biometric characteristics are influenced by one‘s parents genes and can thus are - partly - inherited

Randotypical

- Biometric characteristics are created during pregnancy (early foetal life) and to a large extend result of a random process
  - The resulting characteristics remain constant for entire lifespan

Conditioned

- Biometric characteristics represent the pattern of one‘s behavior and thus can be - partly - trained and changed.



Each biometric characteristic is influenced by all **three** factors!

Example: Fingerprint Recognition

Analog/digital representation of the finger ridges

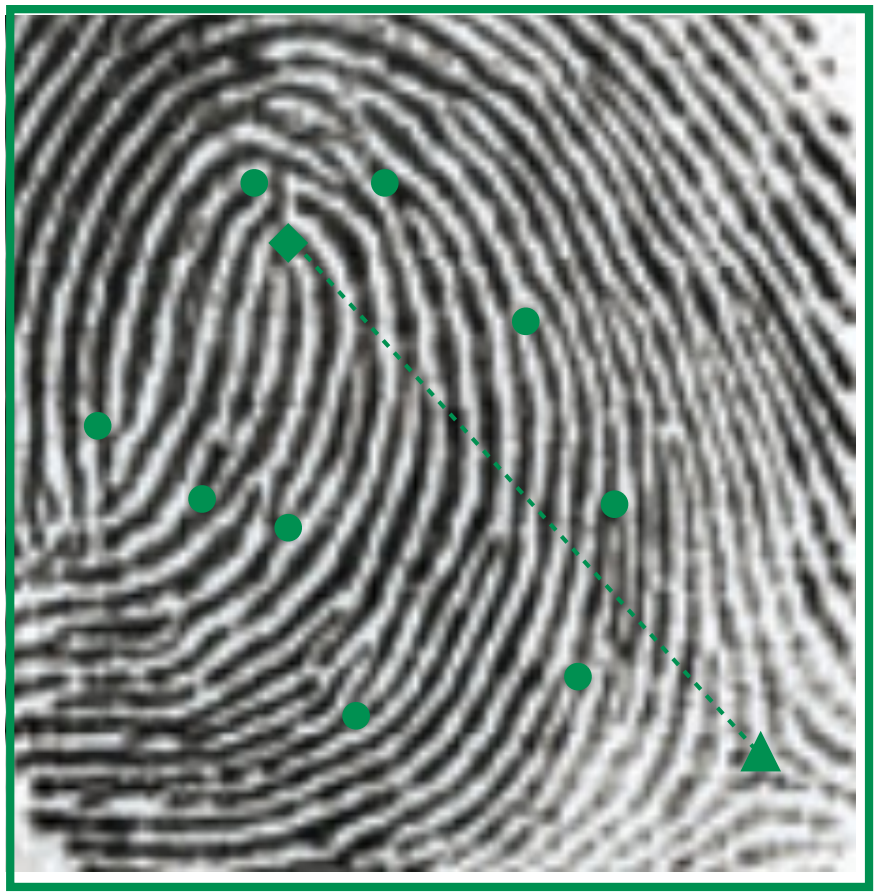
- Distinguished points of the fingerprint: Minutia

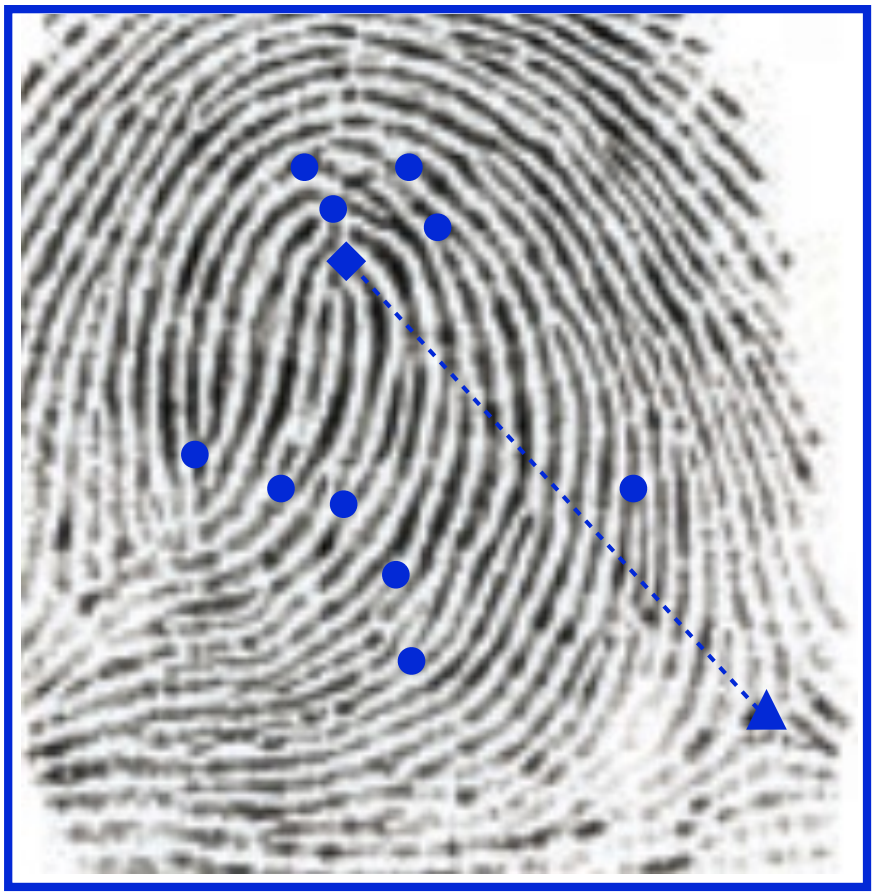
Example: Fingerprint Recognition

Comparison of reference image against a probe image

Example: Fingerprint Recognition

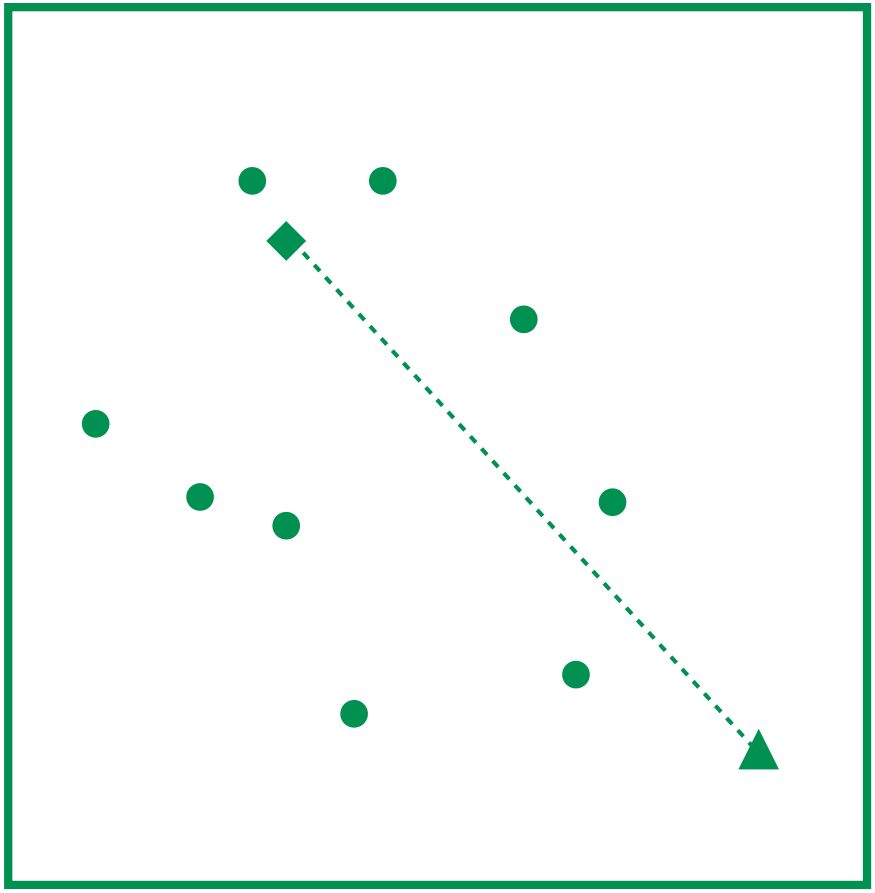
Comparison of reference image
against a probe image

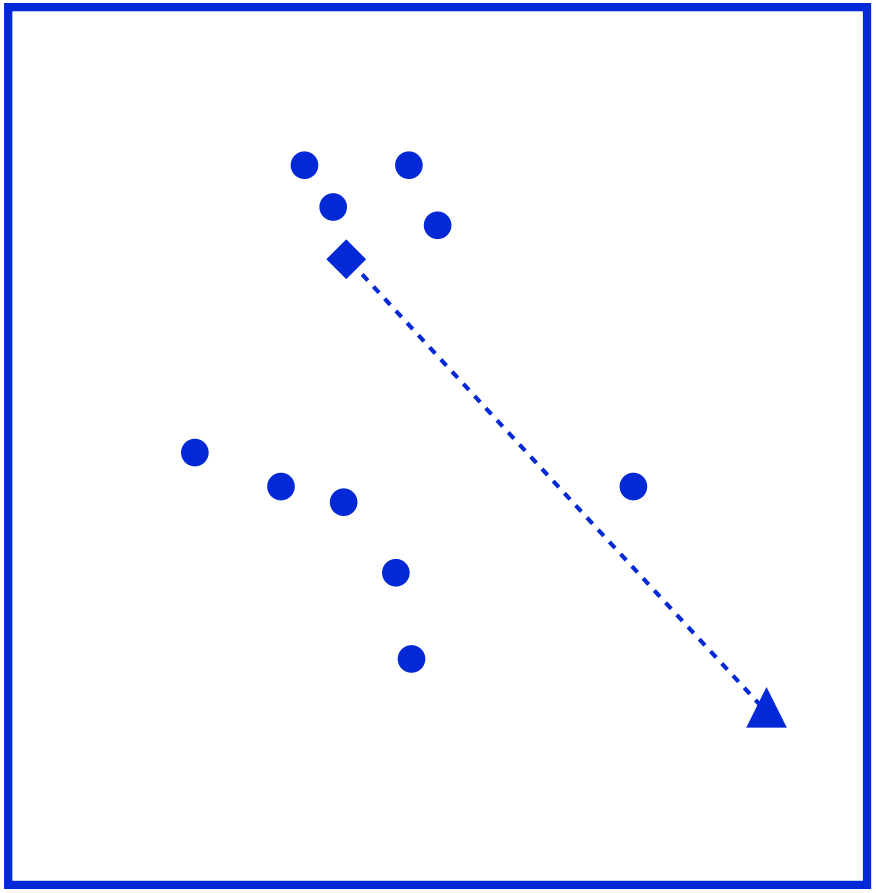




Example: Fingerprint Recognition

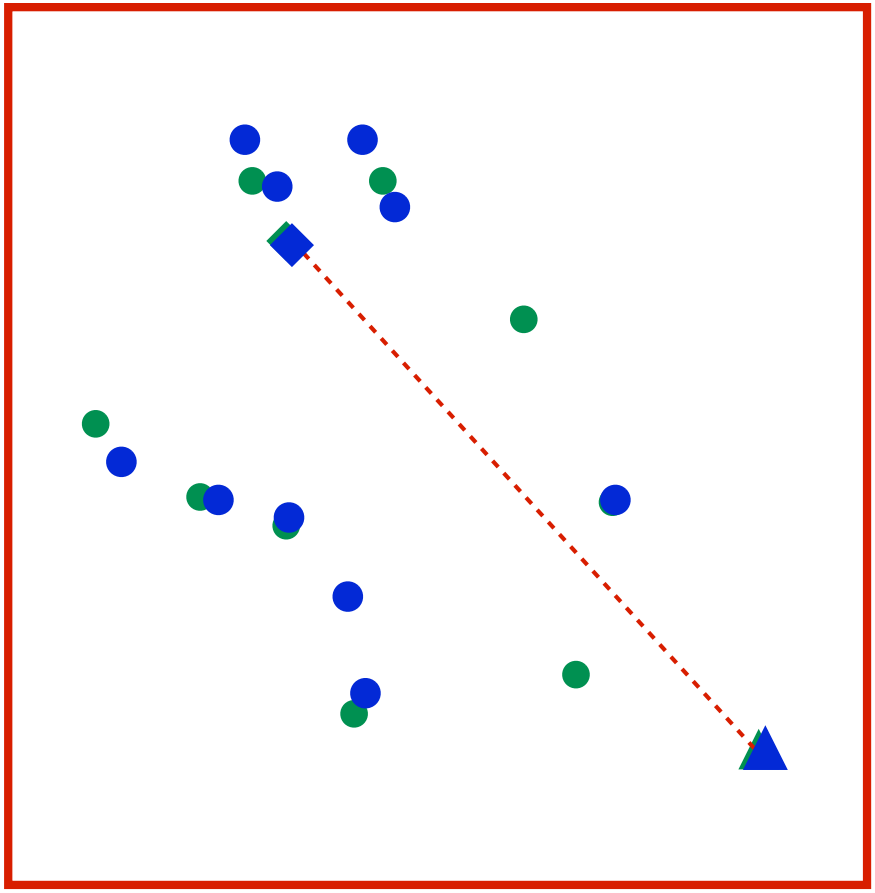
Comparison of reference feature vector against a probe feature vector





Example: Fingerprint Recognition

Comparison of reference feature vector against a probe feature vector



Standardized Terminology

Why Standardization?

Increase the level of interoperability

Why Standardization?

Reduce the level of misunderstanding

- Jim Wayman:
  - *„With our current biometric vocabulary, some of our analytic truths sound self-contradictory“*
  - Example:
    A false non-match occurs if two matched samples
    are matched and found not to match

Why Standardization?

Reduce the level of misunderstanding

- Jim Wayman:
  - *„With our current biometric vocabulary, some of our analytic truths sound self-contradictory“*
  - Example:
    A false non-match occurs if two matched samples
    are matched and found not to match

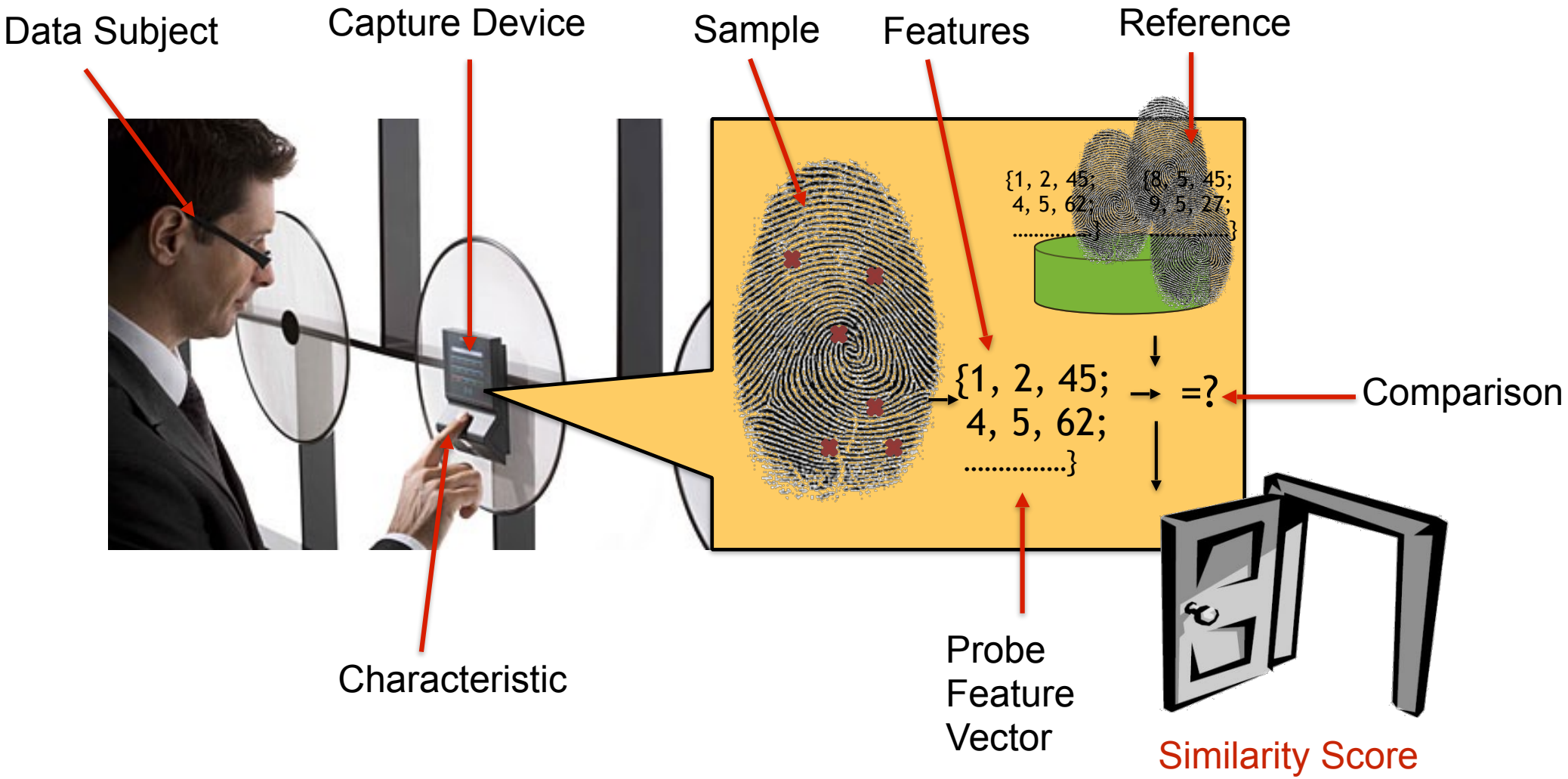
Why Standardization?

Reduce the level of misunderstanding

- Jim Wayman:
  - *„With our current biometric vocabulary, some of our analytic truths sound self-contradictory“*
  - Solution:
    A false non-match occurs if two mated samples (i.e. from the same source) are compared and found not to match
- ISO Definition of comparison:
  - *„estimation, calculation or measurement of similarity or dissimilarity between biometric probe (s) and biometric reference(s)“*

    NOTE: match / matching (n) is deprecated
    as a synonym for comparison!

Some Terms from the Standard



Harmonized Biometric Vocabulary

ISO-Vocabulary

- **biometric characteristic:**
  - *biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition*
- **biometric sample:**
  - *analog or digital representation of biometric characteristics prior to biometric feature extraction*
- **biometric feature:**
  - *numbers or labels extracted from biometric samples and used for comparison*
- **comparison score:**
  - *numerical value (or set of values) resulting from a comparison*

Harmonized Biometric Vocabulary

ISO-Vocabulary

- **biometric reference:**
  - *one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object for biometric comparison*
  - **biometric sample:** (see above)
  - **biometric template:**
    - *set of stored biometric features comparable directly to probe biometric features*
  - **biometric model:**
    - *stored function generated from biometric data*
  - **probe:**
    - *biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference(s)*

Harmonized Biometric Vocabulary

ISO-Vocabulary

- **comparison:**
  - *estimation, calculation or measurement of similarity or dissimilarity between biometric probe (s) and biometric reference(s)*

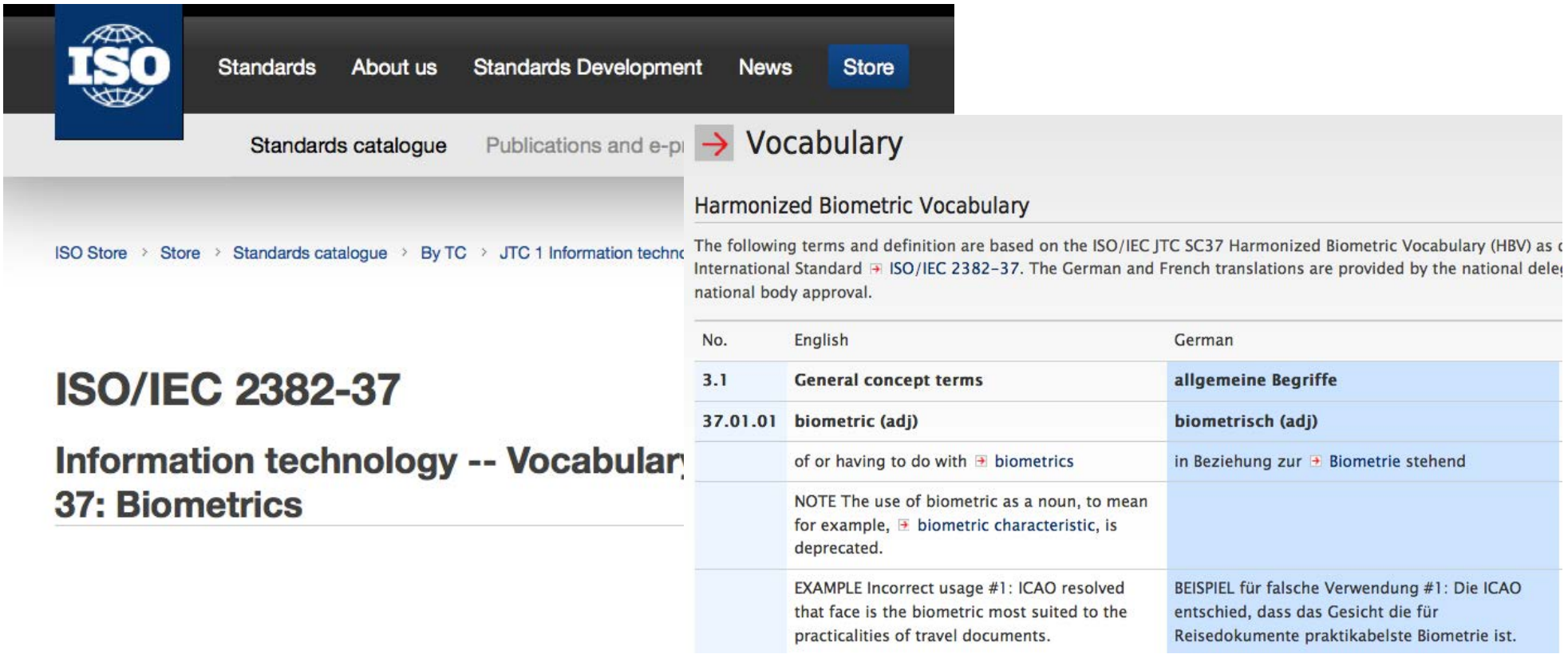
    NOTE: ~~match / matching~~ (n) is deprecated as a synonym for comparison!

Harmonized Biometric Vocabulary

ISO/IEC-Vocabulary: ISO/IEC 2382-37

- available at:

  http://www.christoph-busch.de/standards.html



Writing term papers compliant to vocabulary standard is **mandatory**

Categorization of Biometric Systems

- static vs. dynamic


- cooperative vs. non-cooperative


- habituated vs. non-habituated
- contact-less vs. body contact

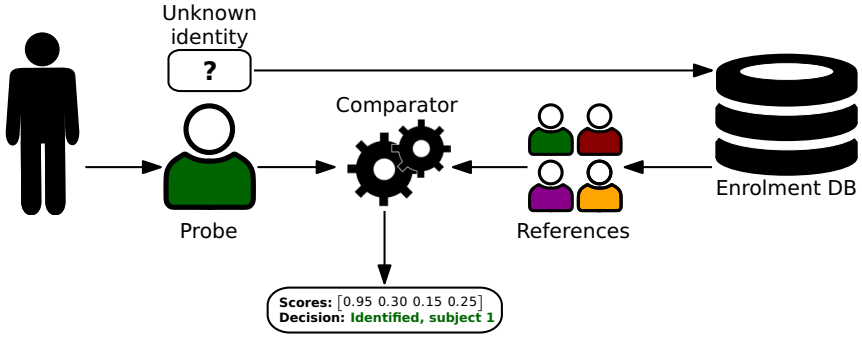
- private vs. public


- open vs. close

Categorization of Biometric Systems

- attended vs. non-attended

- positive identification vs. negative identification



- Costs
  - Installation- and maintenance costs
- Operating expense
  - Duration (transaction time) and complexity of operation
  - Adaptation time

Categorization of Biometric Systems

Further categories that we will discuss in more detail

- Biometric performance
  - How precise does the system recognize individuals?
  - What are the error rates?
- Presentation Attack Detection (PAD)
  - Does the system detect artefacts of biometric characteristics (a.k.a fakes)

The perfect Biometric Method ...

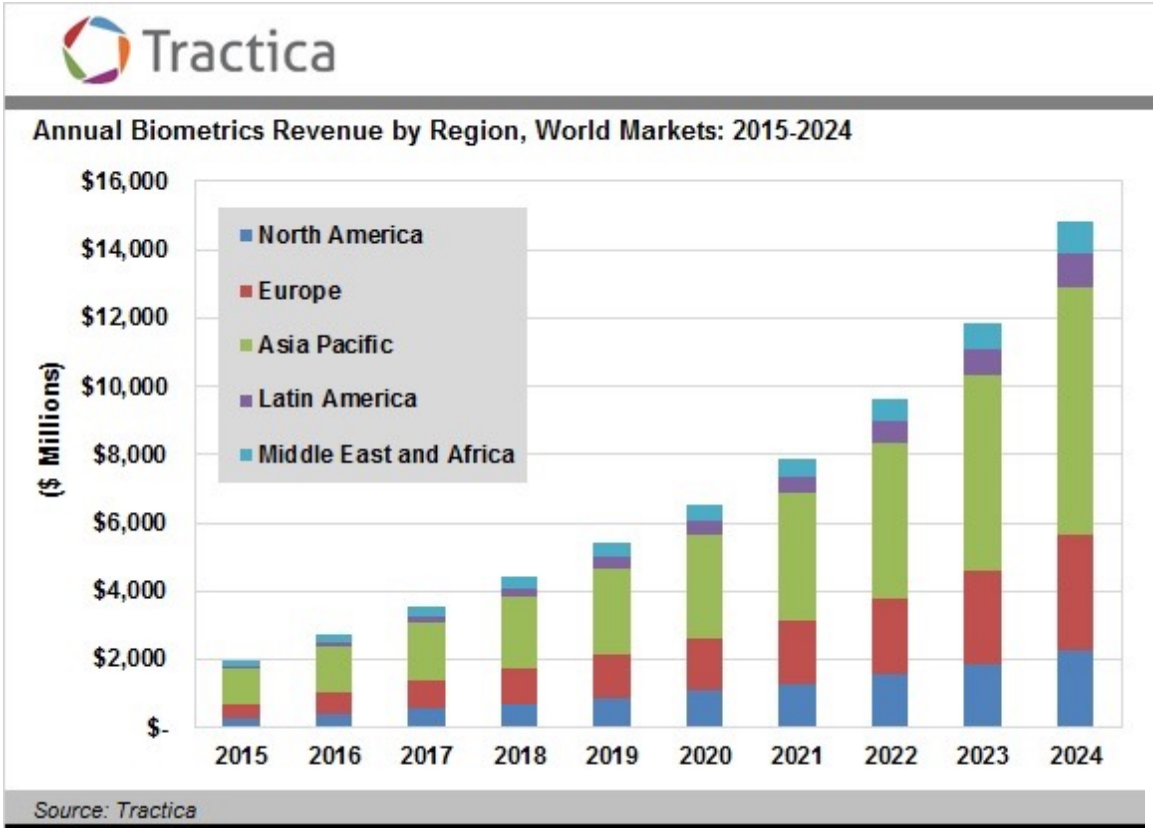
... for all applications does not exist.

- Application scenario „Nuclear Power Plant“:
  - Fake resistance important
  - Low false acceptance is relevant
  - Costs and operating expenses of limited interest
- Application scenario „Fitness Studio Membership Card“:
  - Low costs important
  - Complexity of operation impact convenience
  - Low false reject is relevant

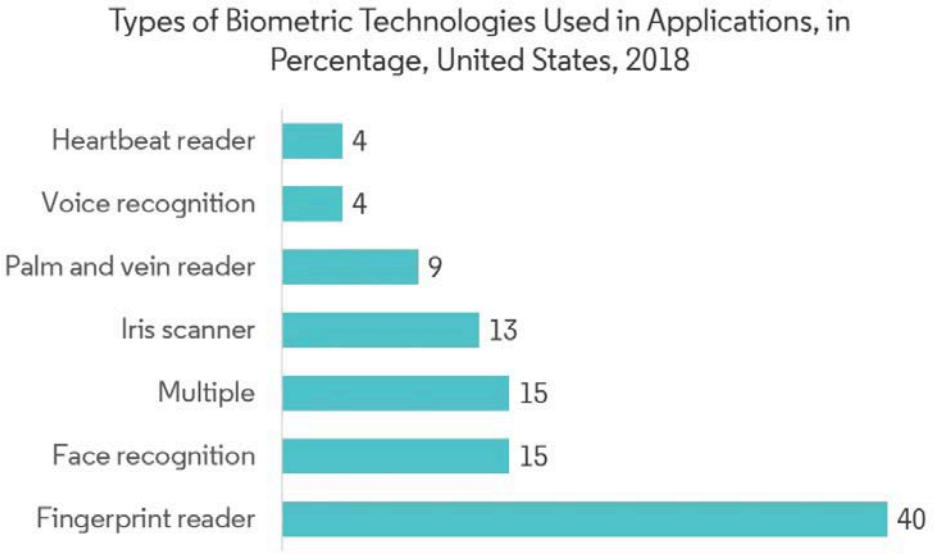
The Market Perspective Slides

Image you are an investor ....

- "*The market for global biometrics is forecast to reach $45.96 billion in 2024,*" Source: Frost & Sullivan 2020



Source: Tractica Markets 2015



Source: University of Texas, 2018

References

Web

- European Association for Biometrics http://www.eab.org
- da/sec biometric research group https://www.dasec.h-da.de/
- TeleTrusT working group on Biometrics
  http://www.christoph-busch.de/about-ag-biometrie.html
- Norwegian Biometrics Laboratory (NBL)
  https://www.ntnu.edu/nbl
- Norsk Biometri Forum (NBF)
  http://www.christoph-busch.de/about-nbf.html
- ISO/IEC JTC1 SC37 Working Group 3
  http://isotc.iso.org/livelink/livelink/open/jtc1sc37wg3
  http://www.christoph-busch.de/standards-sc37wg3.html

References

Complementary reading

- ISO/IEC TR 24741: “Biometrics Tutorial”, 2021
- ISO/IEC SC37 SD11, “General Biometric System Architecture”, 2010