Biometric System Overview - and relevant Standards

Christoph Busch

Norwegian Biometrics Laboratory @ Gjøvik University College

http://www.christoph-busch.de

April 18, 2012

CASED

HØGSKOLEN I GJØVIK

Norwegian Biometrics Laboratory (NBL)

Introduction of the Biometrics Lab

- established in 02‘2011 at the Gjøvik University College (GUC)
- it represents an active focus point of GUC

Driving motivation

- the Biometrics Lab assembles faculty members and PhD students that all have innovative techniques for biometric authentication as their joint interest.
  - 5 full time professor / associate professor
  - 2 post-doc researcher
  - 7 Ph.D. students

- Projects
  - TURBINE (FP7, 2008-2011), BEST network (EU, 2009-2011), FIDELITY(FP7, 2012-2016)
  - NIST-BTP-metrics (NIST, 2010-2011), NIST-NFIQ2.0 (NIST-BSI, 2011-2014)
  - Hitachi vein recognition, IDEX fingerprint evalaution, Fujitsu vein recognition, secunet, dermalog

Agenda

- Introduction
- Biometric sytem overview
- Relevant standards and Biometric performance testing
- Physical and logical access control
- Gait recognition and convenience of authentication
- Relevant research topics

Introduction

This talk covers:

- „Biometric Systems“

What is Biometrics?

- International Organization for Standardization:

  - Biometrics (06/2004):
    “*Automated recognition of individuals based on their behavioral and biological characteristics.*”

Access Control

Access Control

Identity authentication can be achieved by:

- Something you know:
  Password, PIN, other secret

Some Statistics on Passwords

Password Statistics based on 32 million passwords

- 20% were names and trivial passwords
- Top 5 passwords (@ www.rockyou.com)

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

Access Control

Identity authentication can be achieved by:

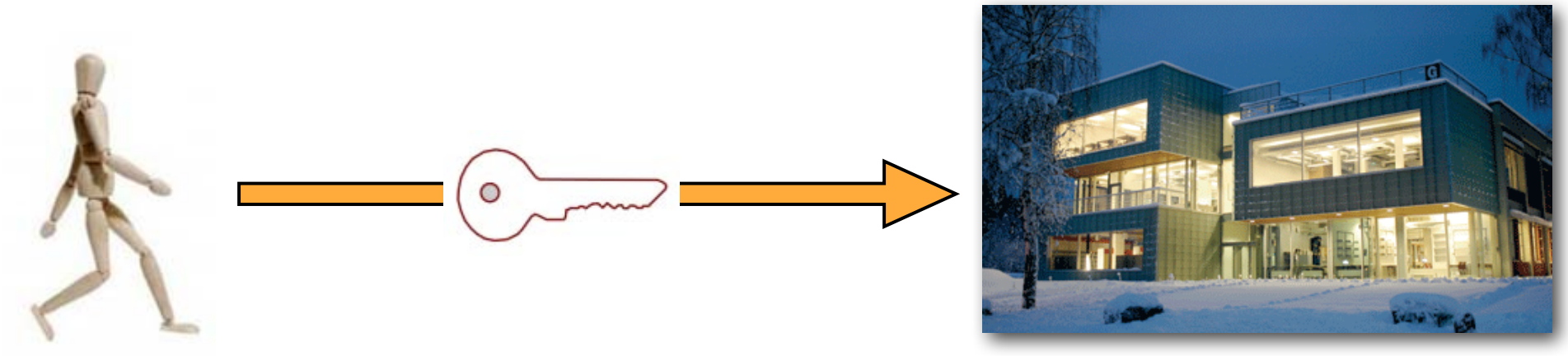
- Something you know:
  Password, PIN, other secret

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

Access Control

Traditionally we place between

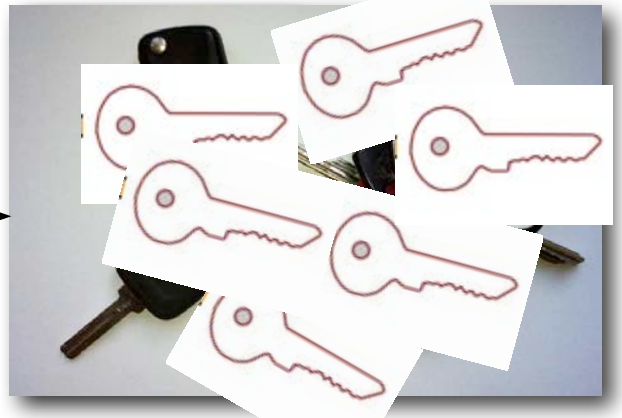
- individuals
- and objects
- a token (i.e. key)

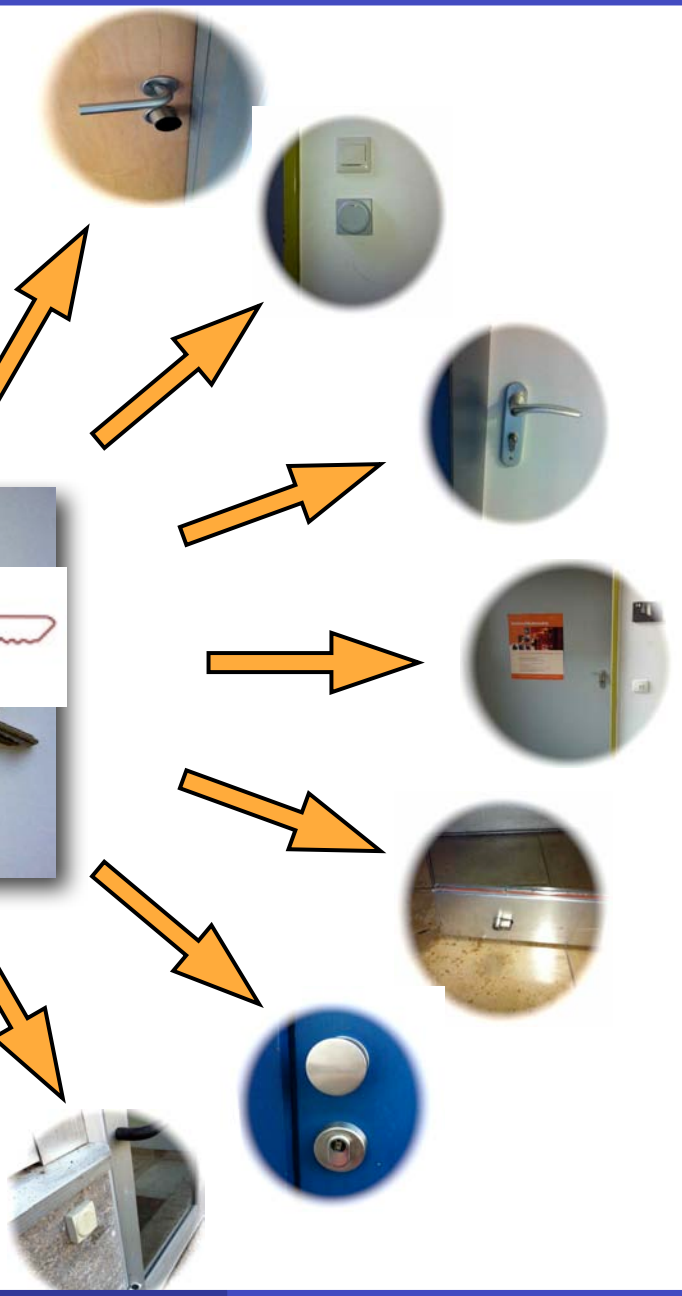


Access Control

But in reality individuals

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





Access Control

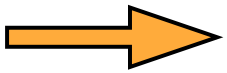
But in the near future many institutions

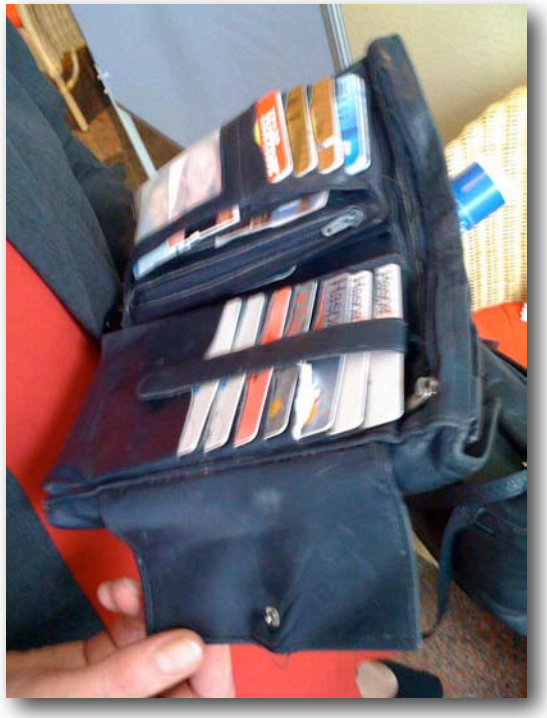
- will grant staff member cards
- granting access to many doors

Access Control

For some individuals

- the collection of cards is quite impressive and inconvenient





Access Control

Identity authentication can be achieved by:

- 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.

- security policy not violated by delegation
- non-repudiation of transactions
  „This was initiated by *Igor Popov* misusing my card“

Biometrics in a Nutshell

Example: Fingerprint Recognition

Analog/digital representation of the finger ridges

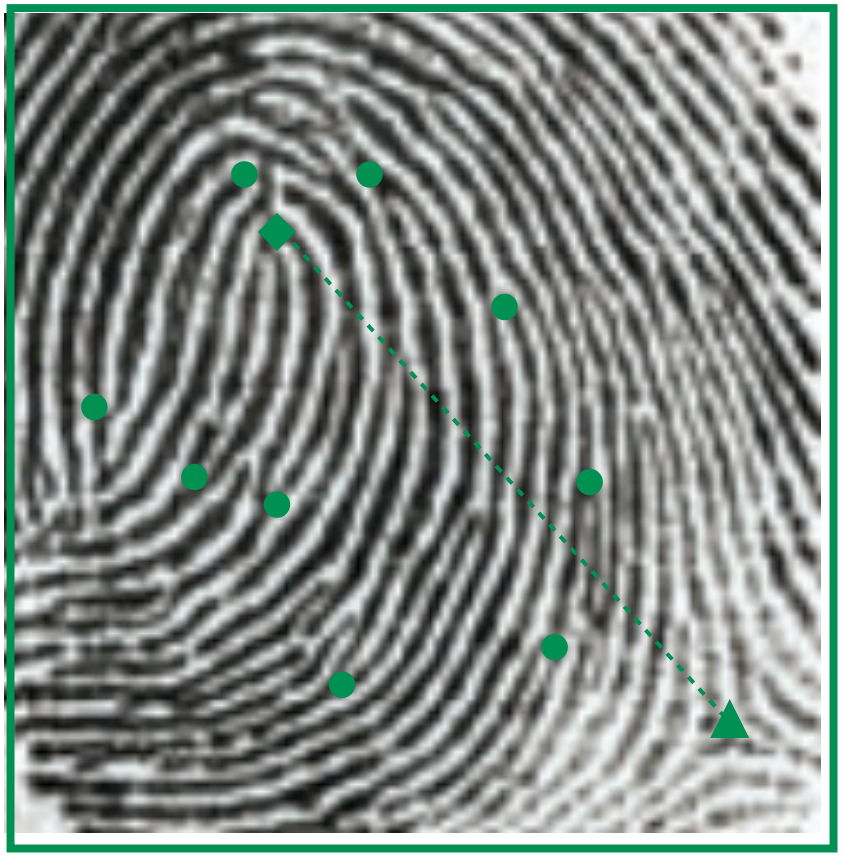
- Distinguished points of the fingerprint: Minutia

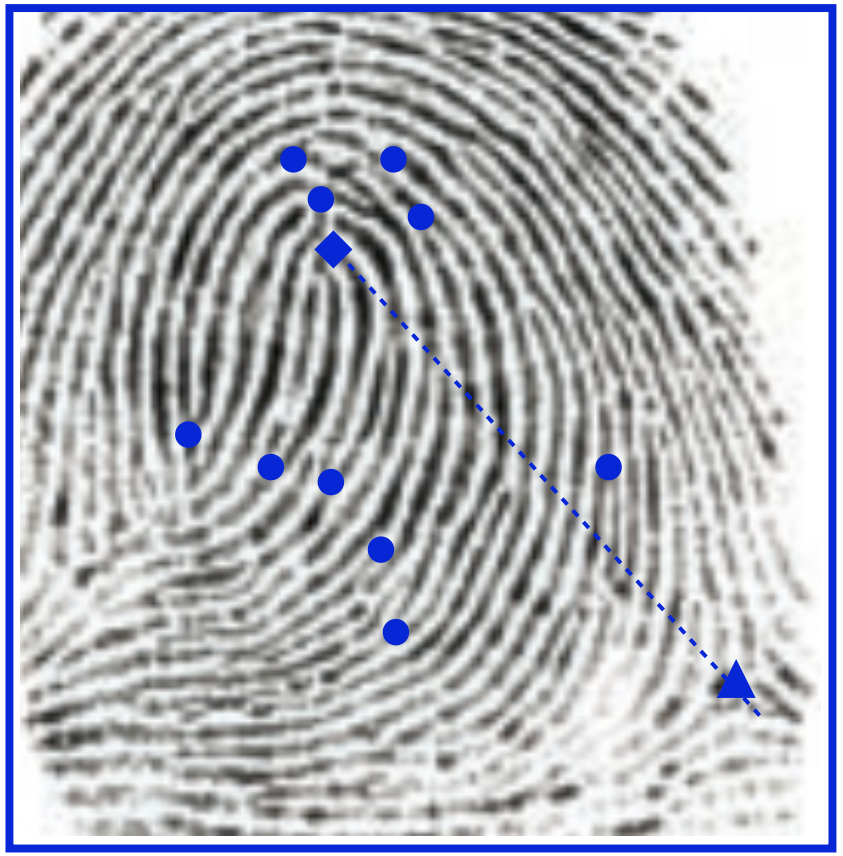
Example: Fingerprint Recognition

Comparison of reference image against a probe image

Example: Fingerprint Recognition

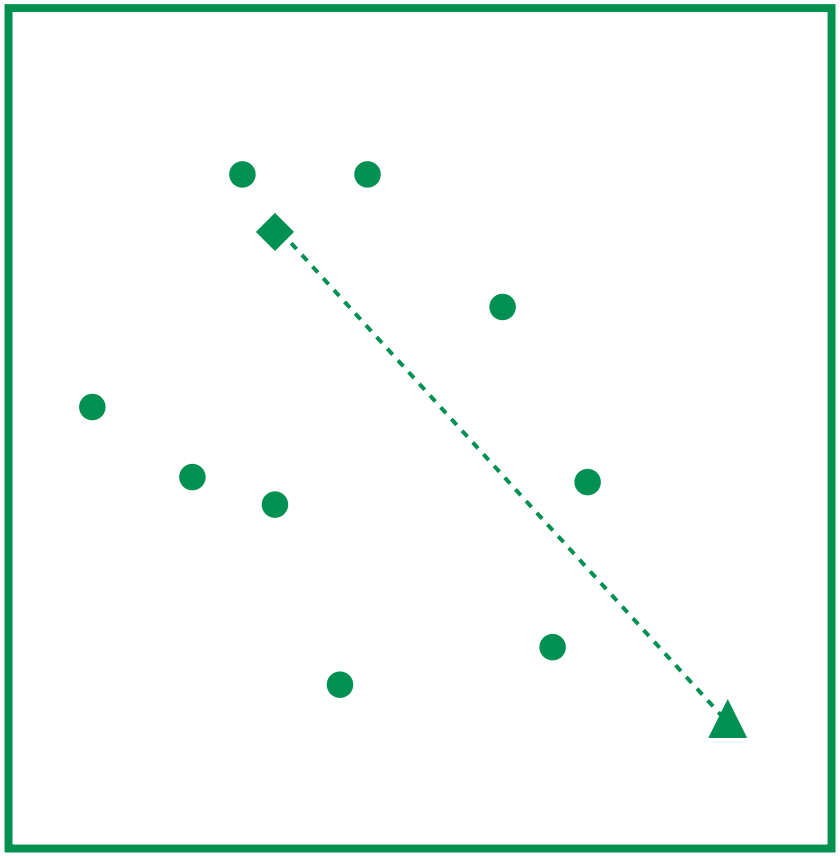
Comparison of reference image
against a probe image

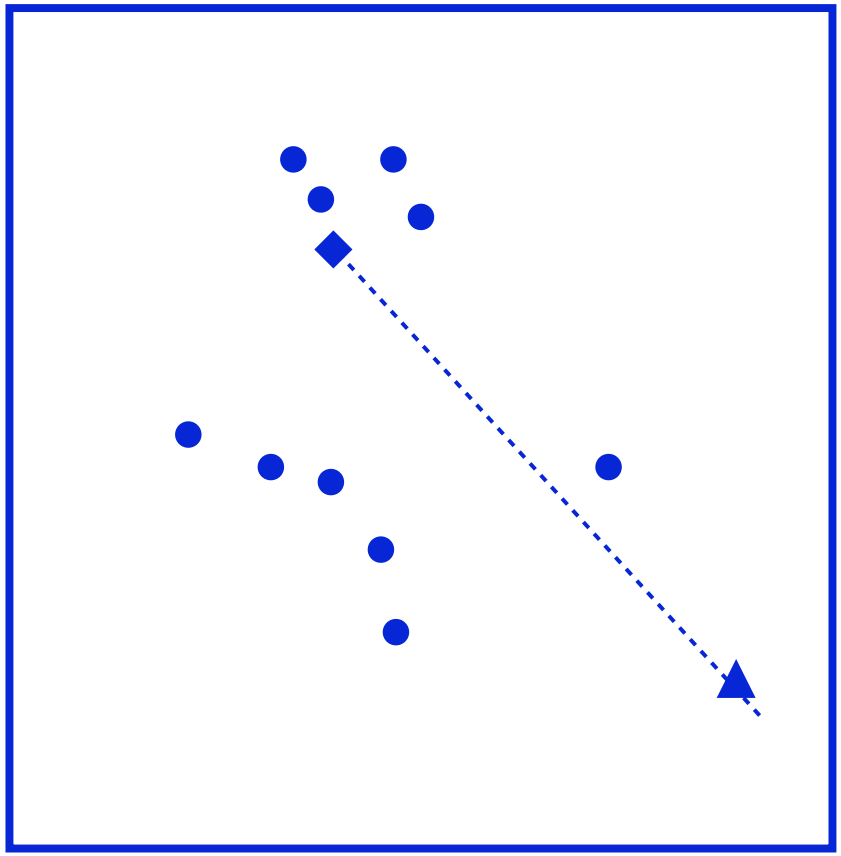




Example: Fingerprint Recognition

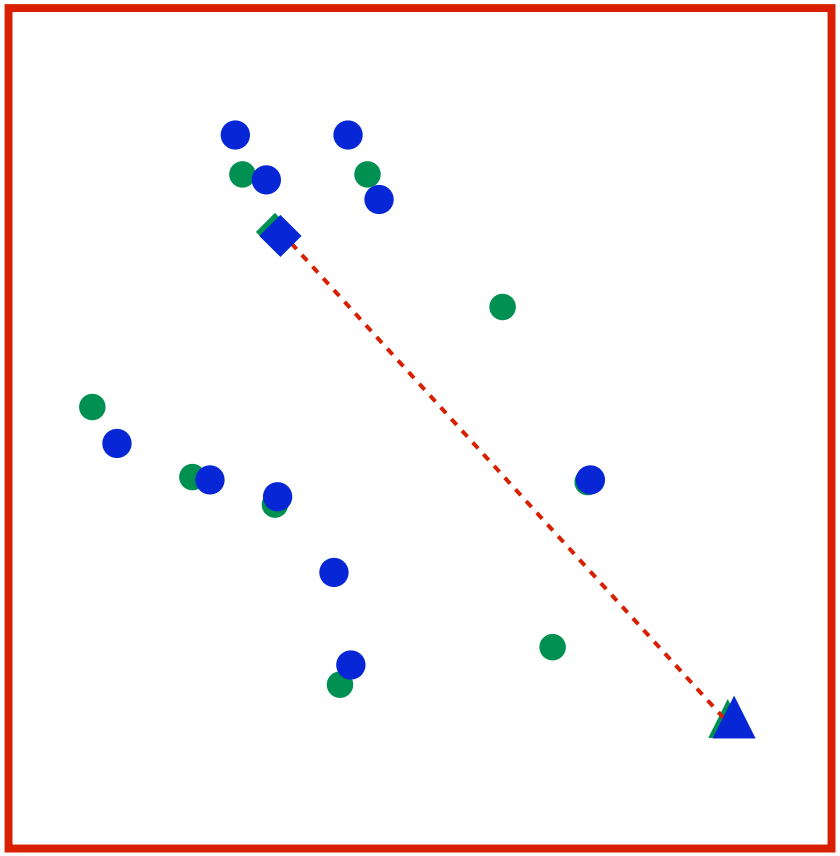
Comparison of reference feature vector against a probe feature vector





Example: Fingerprint Recognition

Comparison of reference feature vector against a probe feature vector



Identification - Verification

Identification:

- Recognize the identity of an individual (1:n - comparison)

staff identity = „busch“

Verification:

- Validation of an identity claim (1:1 - comparison)

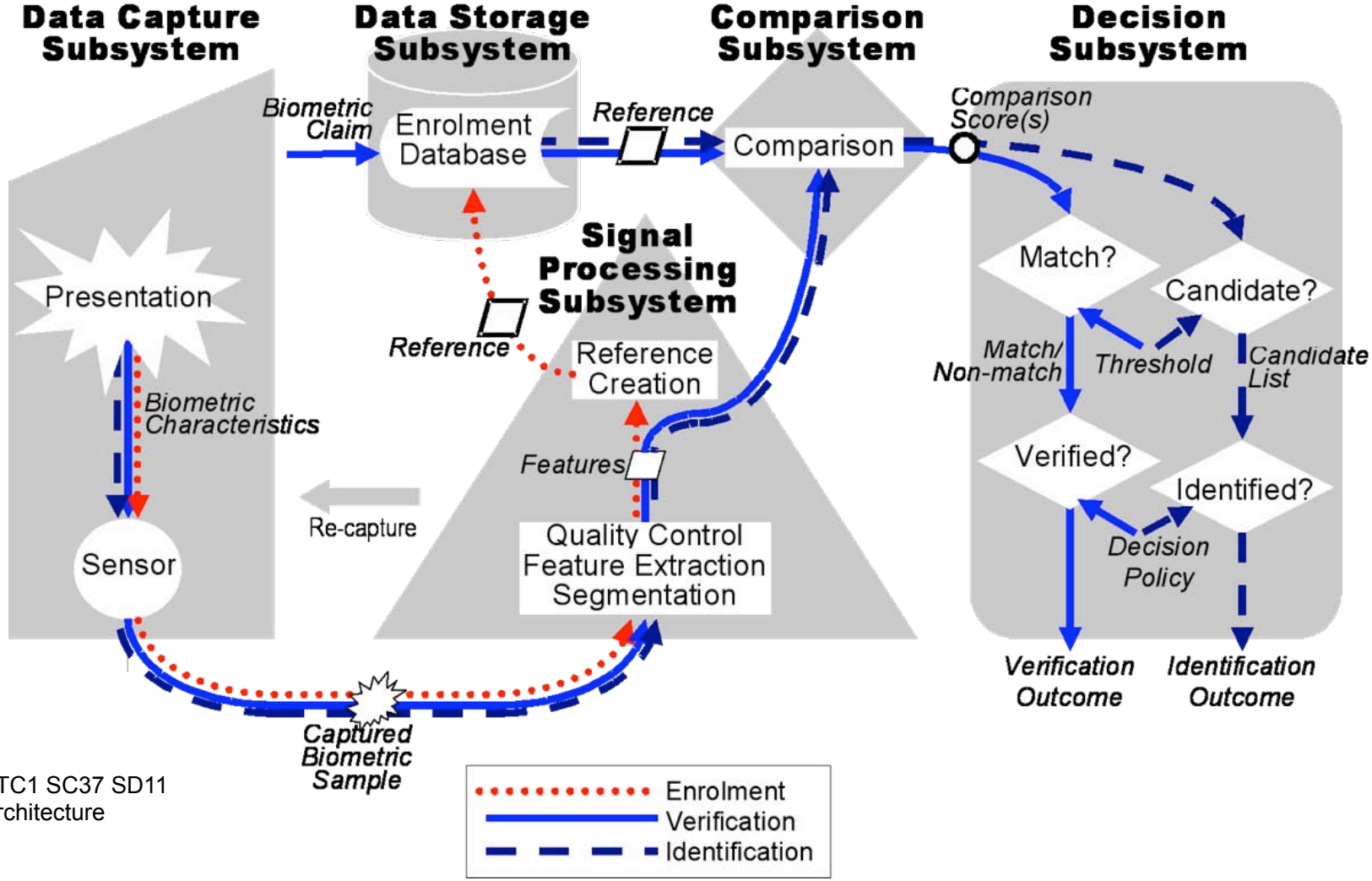
similarity: „71%“

(Comparison-Score)

Architecture of a Biometric System

ISO/IEC JTC1 SC37 Standing Document 11

http://isotc.iso.org/livelink/livelink?func=ll&objId=9626779&objAction=Open



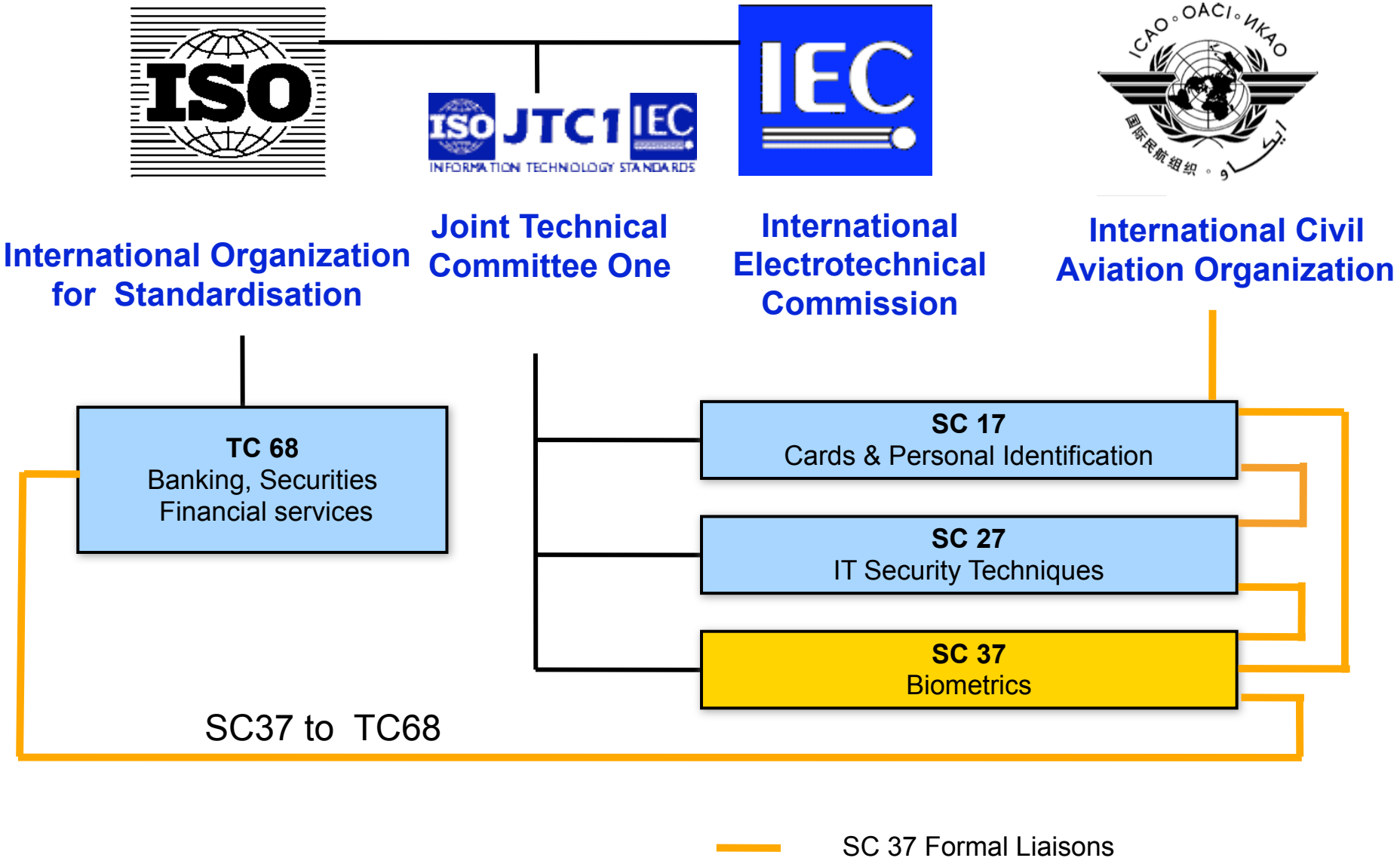
Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture

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 - capture throughput time but primarily associated with biometric performcance (low errors)
- Permanence - the characteristic should be invariant over time. (persistent / immutable / limited ageing effects)
- Collectability - the characteristic is measurable and the quantative result is reproducible.
- Acceptability - convenient measurement at low cost and unobstrusive for data subjects.
- Circumvention - hard to collect and replicate a fake biometric characteristic (Security)

Biometric Standardisation



ISO/IEC JTC1 SC37 Biometrics

Established by JTC 1 in June 2002 to ensure

- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

Scope of SC37

- *"Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects"*

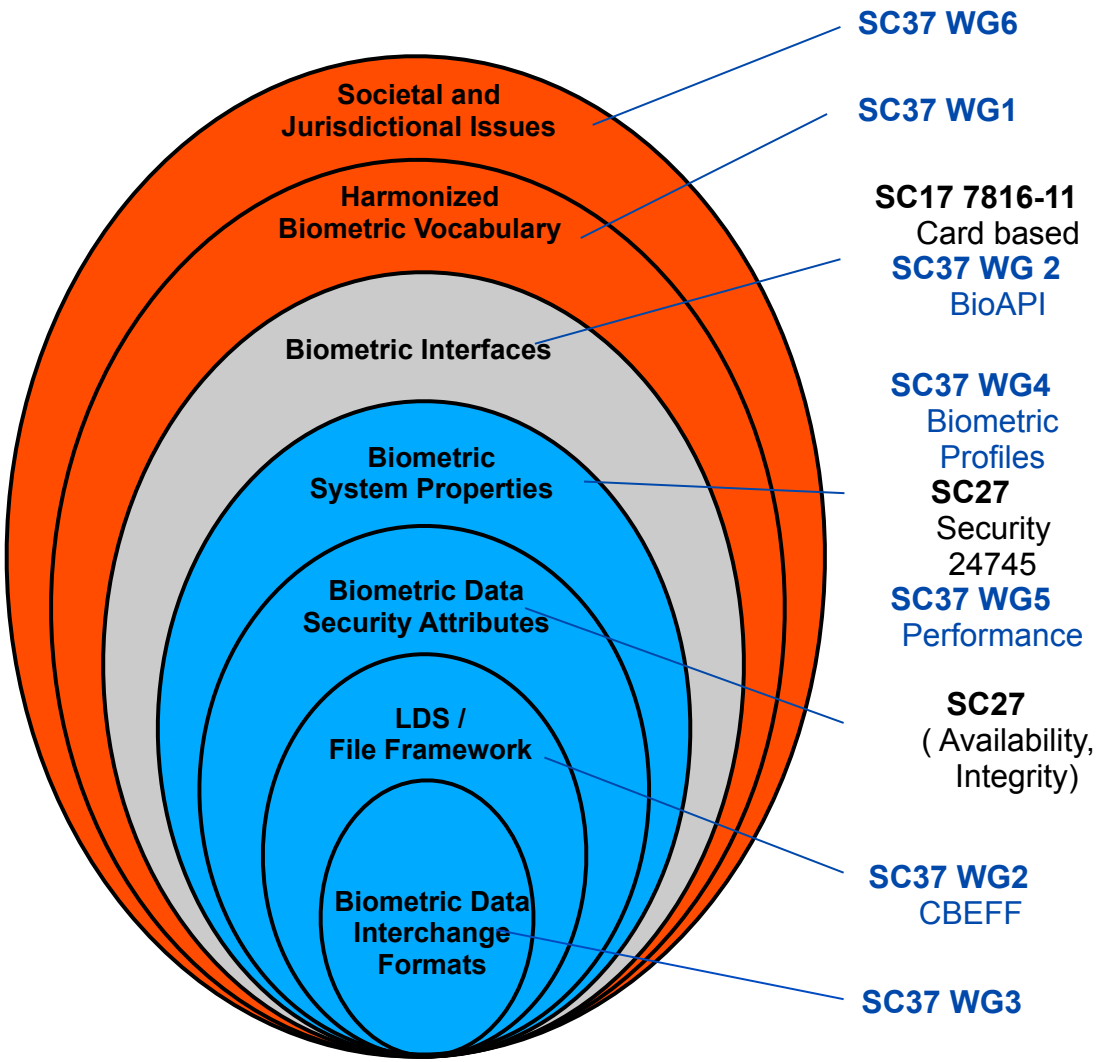
http://www.jtc1.org

Next meeting: July, 2012

Relevant Standards

Onion Layers

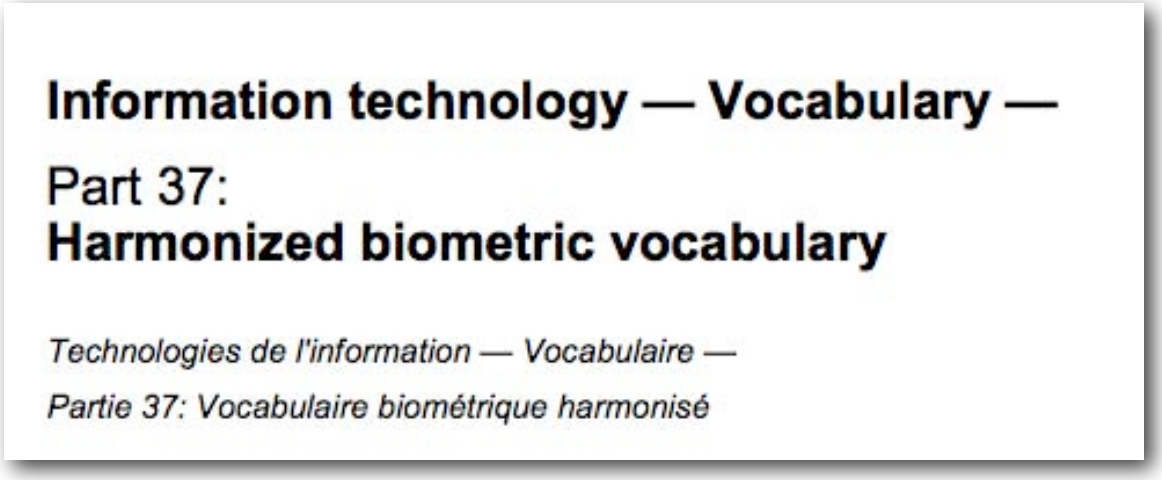
- Layer 1: BDB
  - Digital representations of biometric characteristics
- Layer 2: LDS
  - CBEFF Meta-data
- Layer 3+4: System properties
  - Security
  - Performance
- Layer 5: BioAPI, BIP
  - System Integration



Relevant Standards

ISO/IEC FDIS 2382-37

- Harmonized biometric vocabulary



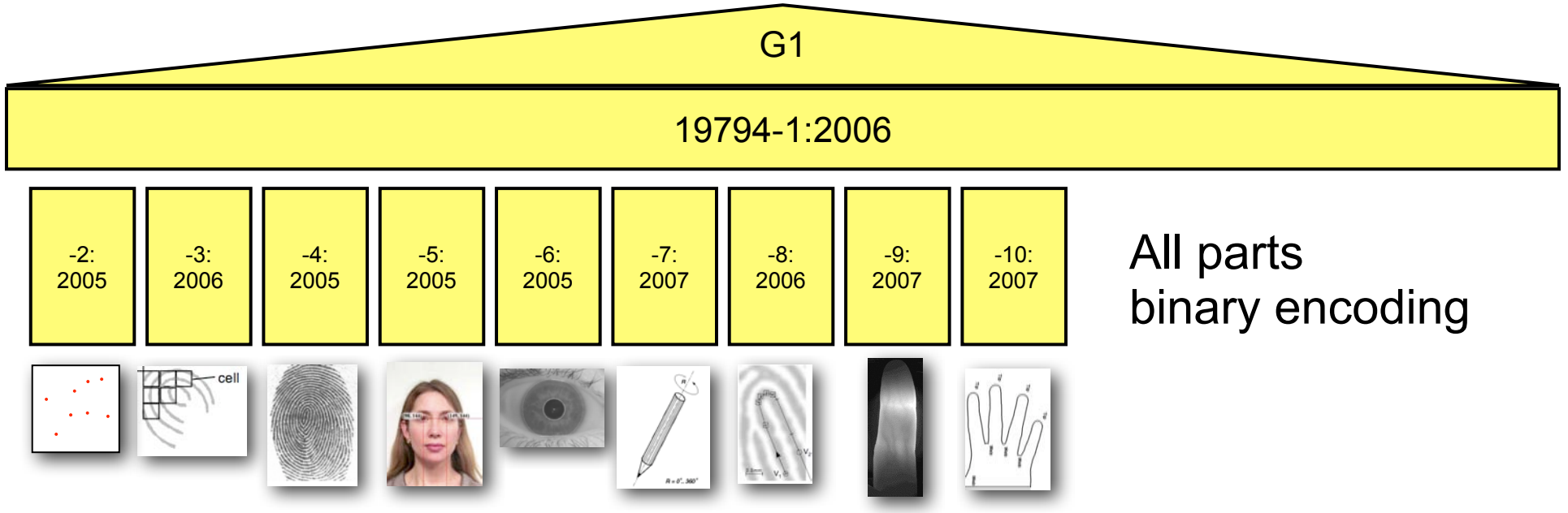
will soon be available online at:
http://www.christoph-busch.de/standards.html

Biometric Data Formats: 19794-Family

- Biometric data interchange formats
  - Part 1: Framework (IS) - rev (IS)
  - Part 2: Finger minutiae data (IS) - rev (IS)
  - Part 3: Finger pattern spectral data (IS) - no revision
  - Part 4: Finger image data (IS) - rev (IS)
  - Part 5: Face image data (IS) - rev (IS)
  - Part 6: Iris image data (IS) - rev (IS)
  - Part 7: Signature/Sign time series data (IS) - rev (CD)
  - Part 8: Finger pattern skeletal data (IS) - rev (IS)
  - Part 9: Vascular image data (IS) - rev (IS)
  - Part 10: Hand geometry silhouette data (IS) - no revision
  - Part 11: Signature/Sign processed dynamic data (DIS)
  - Part 13: Voice data (WD)
  - Part 14: DNA data (DIS)

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on

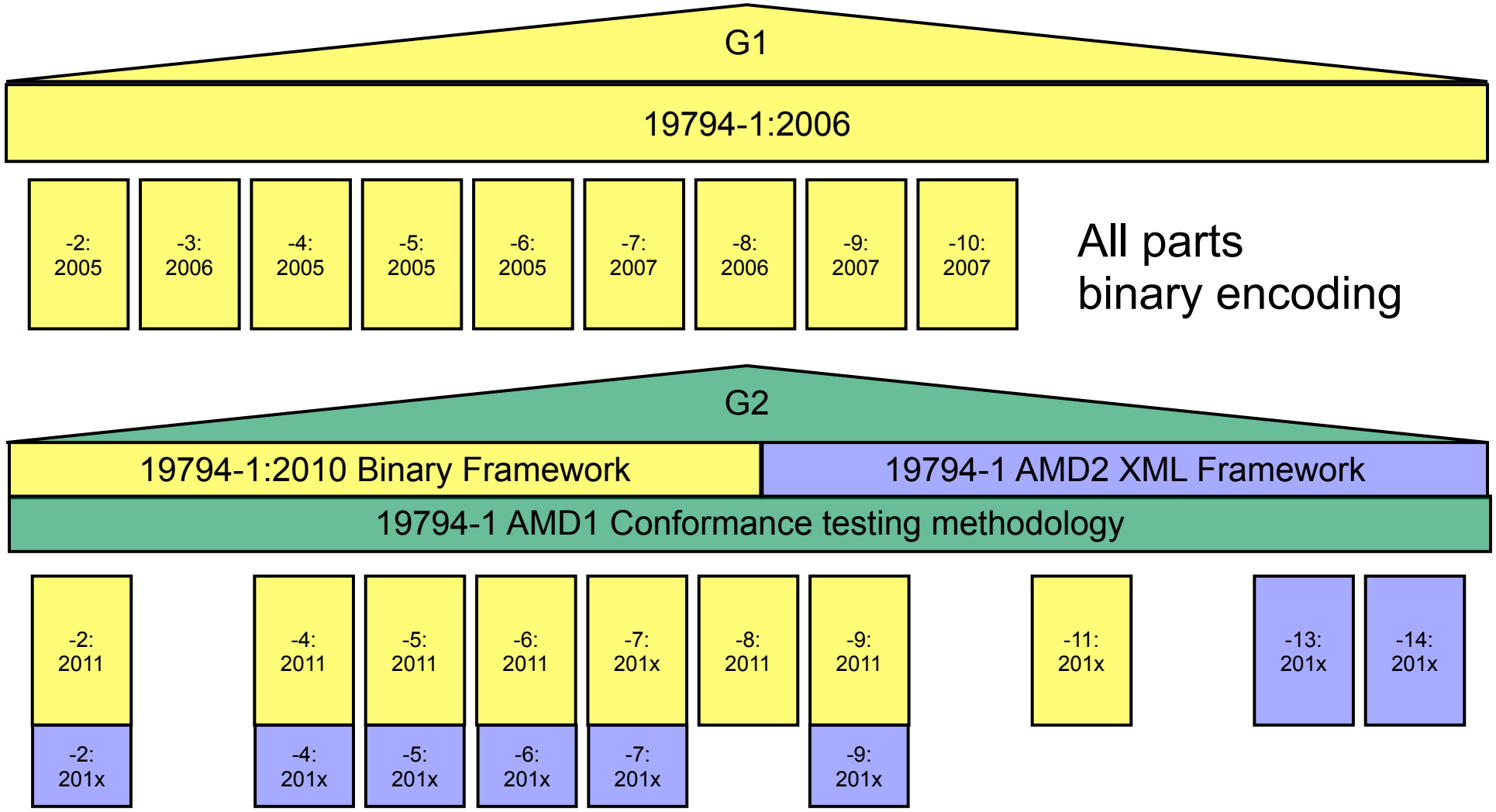
First Generation Format Standards



All parts
binary encoding

The 19794-Family

Generation 2 of ISO/IEC 19794

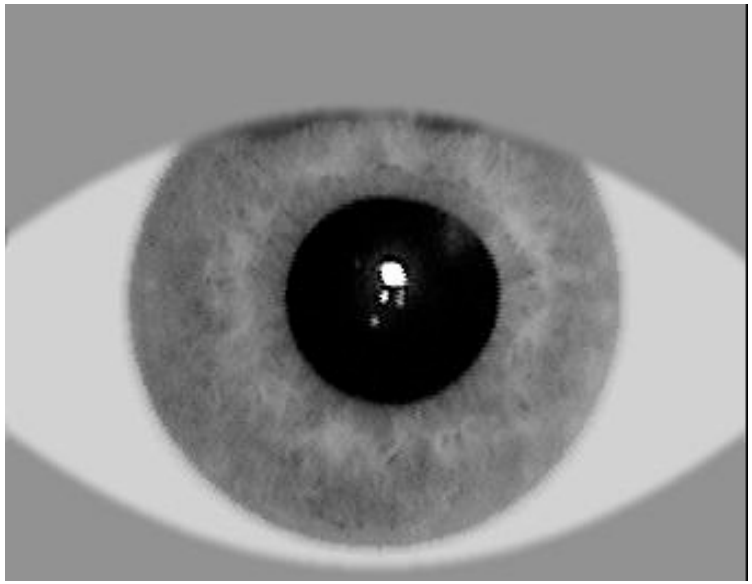


the semantic (i.e. general header / structure of representation header)
is identical for binary encoded and XML encoded parts in G2

Formats - Iris Image Data

ISO/IEC 19794-6:2011

- highly compact iris image, compressed to 2,000 bytes



- Cropping, and masking non-iris regions, preserves the coding budget
- Pixels outside the ROI fixed to constant values, for normal segmentation
- Interoperability of this vendor-neutral format confirmed by IREX results
- At only 2,000 bytes, iris images are now
  much more compact than fingerprints

ISO/IEC 19795-1

Biometric performance testing

- likelihood for a failure to occur
- specified in error probabilities (error rates)

System Errors vs. Algorithm Errors

- FAR, FRR vs. FMR, FNMR

ISO/IEC 19795-1 Metrics

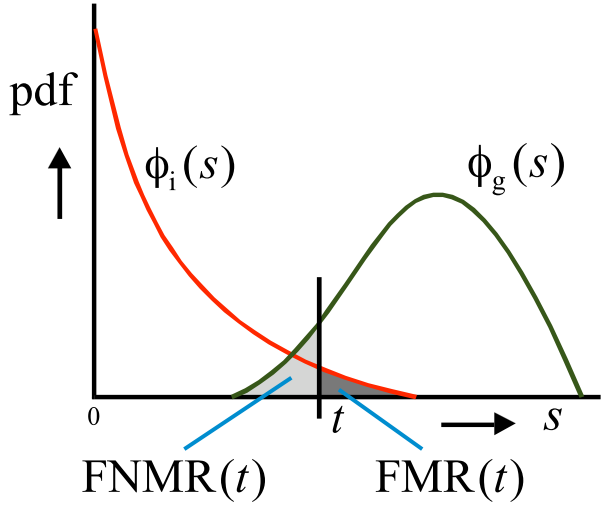
Probability densitiy Distribution Function (PDF)

$\Phi_g(s)$: PDF of genuine similarity score $s(Q,R)$
$\Phi_i(s)$: PDF of imposter similarity score $s(Q,R)$

False-Match-Rate (FMR)

- proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self reference

$$FMR(t) = \int_t^1 \Phi_i(s)ds$$



ISO/IEC 19795-1 Metrics

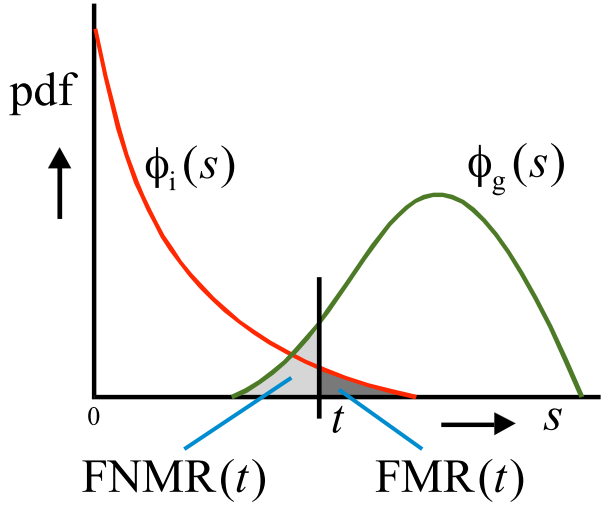
Probability densitiy Distribution Function (PDF)

$\Phi_g(s)$: PDF of genuine similarity score $s(Q,R)$
$\Phi_i(s)$: PDF of imposter similarity score $s(Q,R)$

False-Non-Match-Rate (FNMR)

- proportion of genuine attempt samples
  falsely declared not to match
  the reference of the same characteristic from same subject

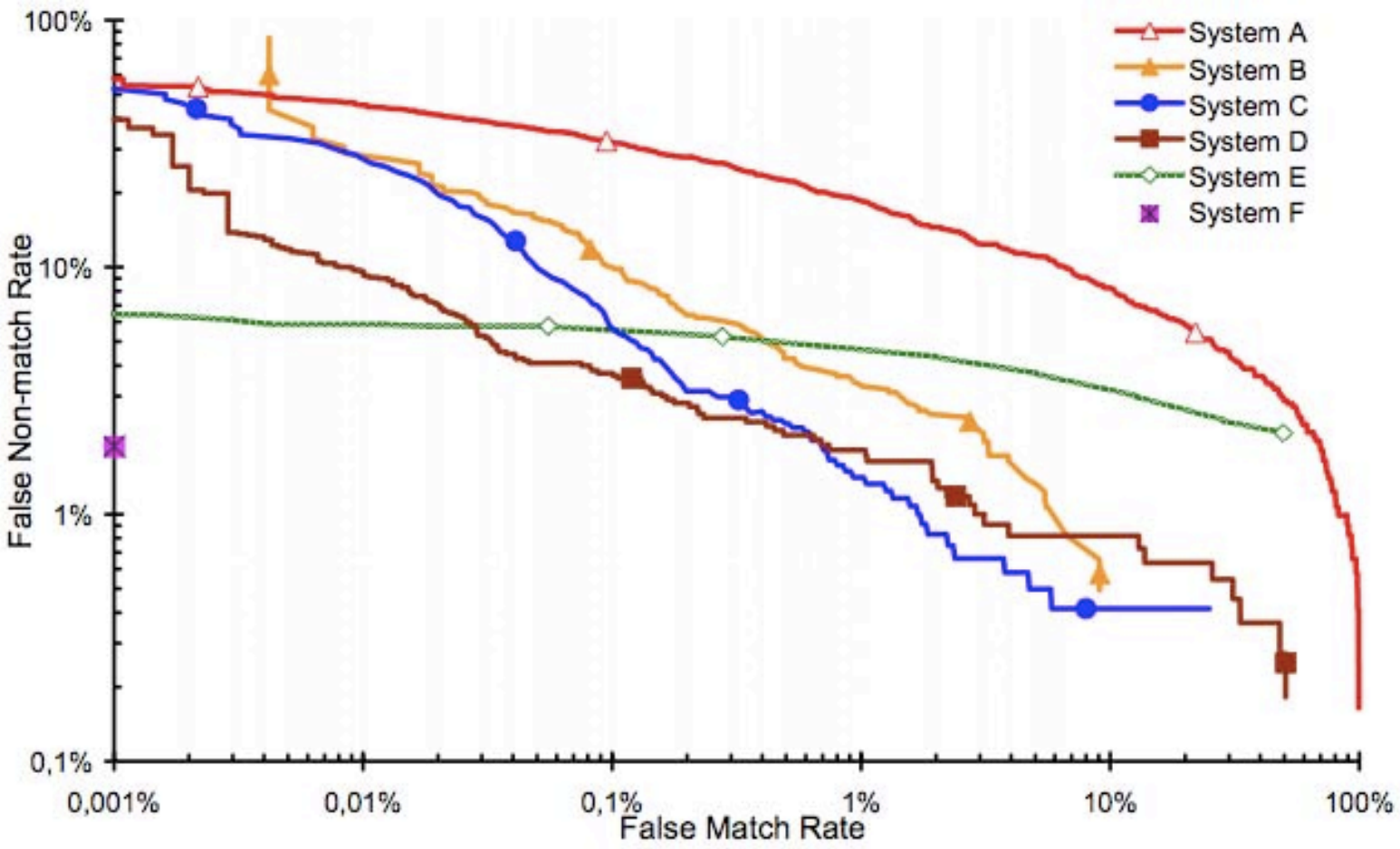
$$FNMR(t) = \int_0^t \Phi_g(s)ds$$



Graphical Presentation

DET curve (detection error trade-off curve)

- modified ROC curve which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)



Three Biometric Applications

The Indian UID System

Goal of the UID: Biometrics and Inclusion

- Provide a unique number to every resident of india
- Remove ghost identities in a 1.2 Billion database
- Improve service delivery
- Provide identity proof
- Avoid vendor lock-in
  - Multi-ABIS System
- System design based on ISO/IEC standards

Source: UID

Biometrics and Automated Board Control

EasyPASS @ Frankfurt Airport

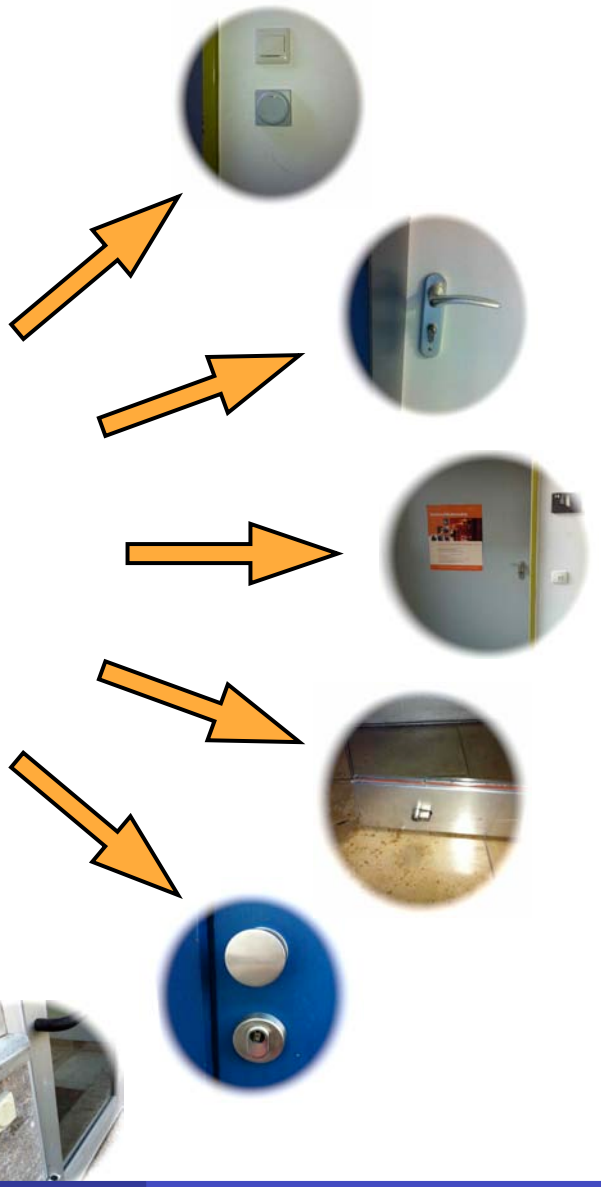
- Automated but supervised border control since 08‘2009
- Self-Service to increase throughput

Source: BSI

Access Control in Personal Environments

Should we in the long term future

- have biometric access control at every door?

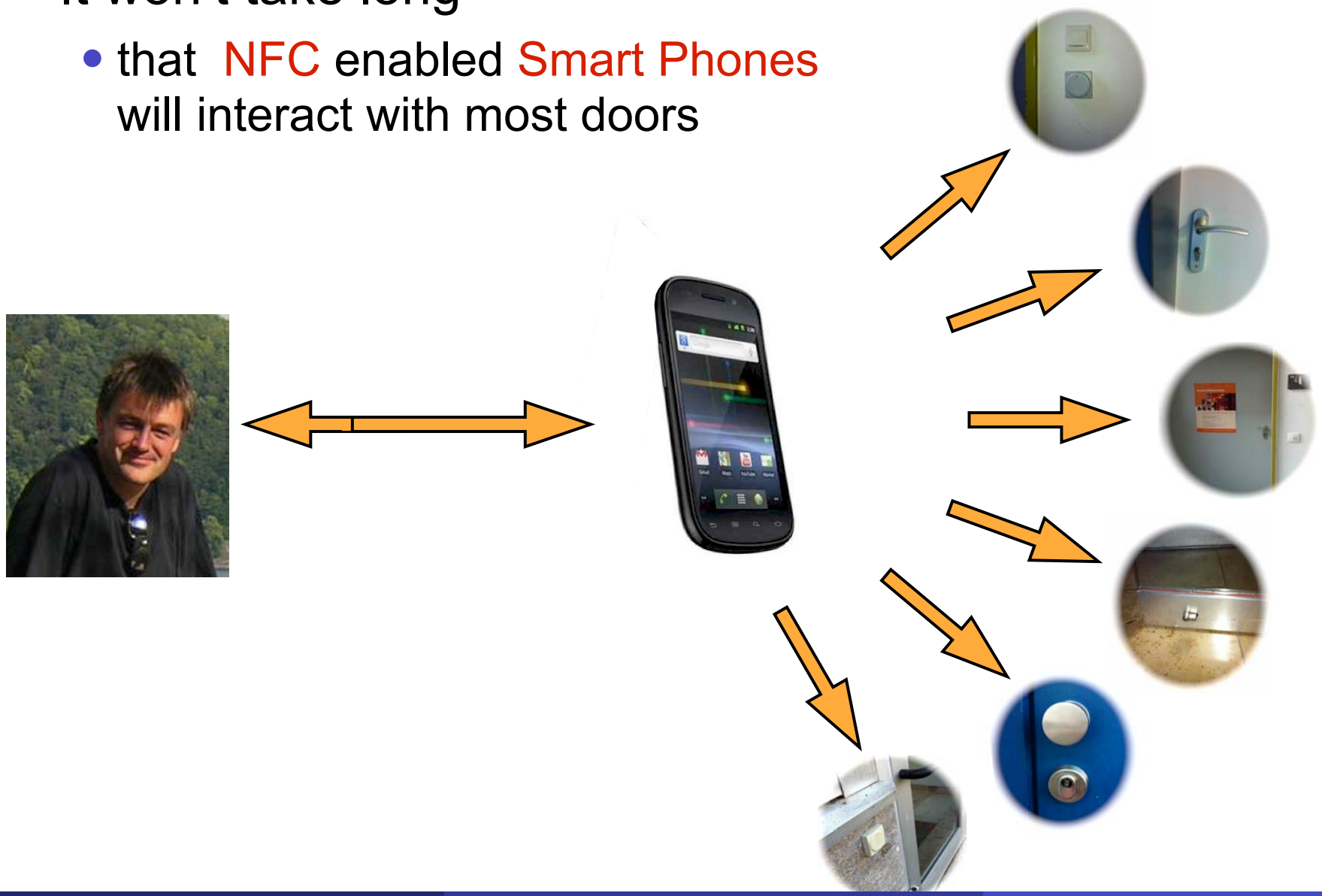


- cost factor for sensors?
- where do we store references?

Smart Phone Based Access Control

It won‘t take long

- that NFC enabled Smart Phones will interact with most doors



Do we use Access Control to Smart Phones?

Threat Analysis

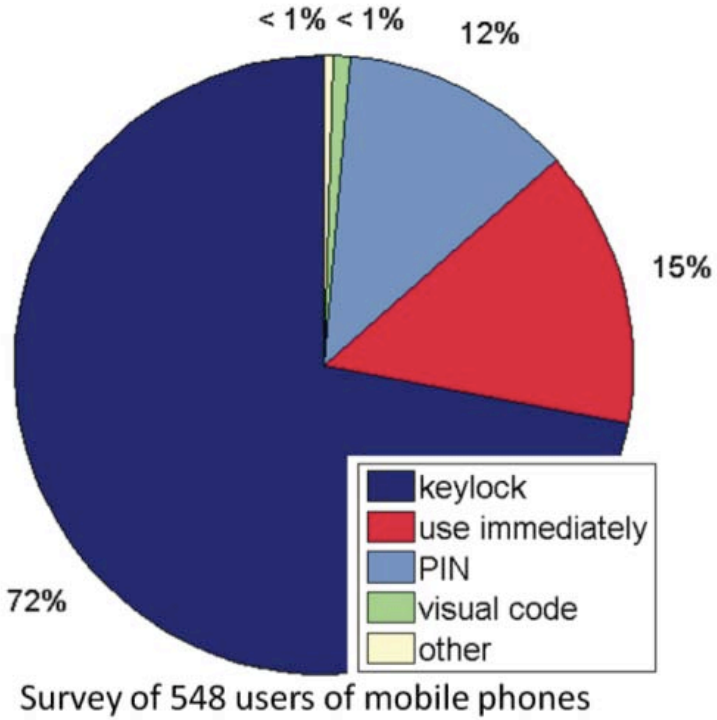
Data in mobile devices is often insufficiently protected

No PIN-authentication required after stand-by phase

- Survey-result:
  only 13% use PIN code

All data on the phone is freely available

- Emails, addresses,
- appointments, photos
- PINs etc.



Survey of 548 users of mobile phones

Reason for this:

- PIN-authentication is too much effort (30%)
- People are self-responsible for their phones

Smart Phone Access Contol

Foreground authentication (user interaction)

- Camera-Sensor
  - Fingerprint recognition
  - Face recognition
  - Iris recognition

Background authentication (observation of the user)

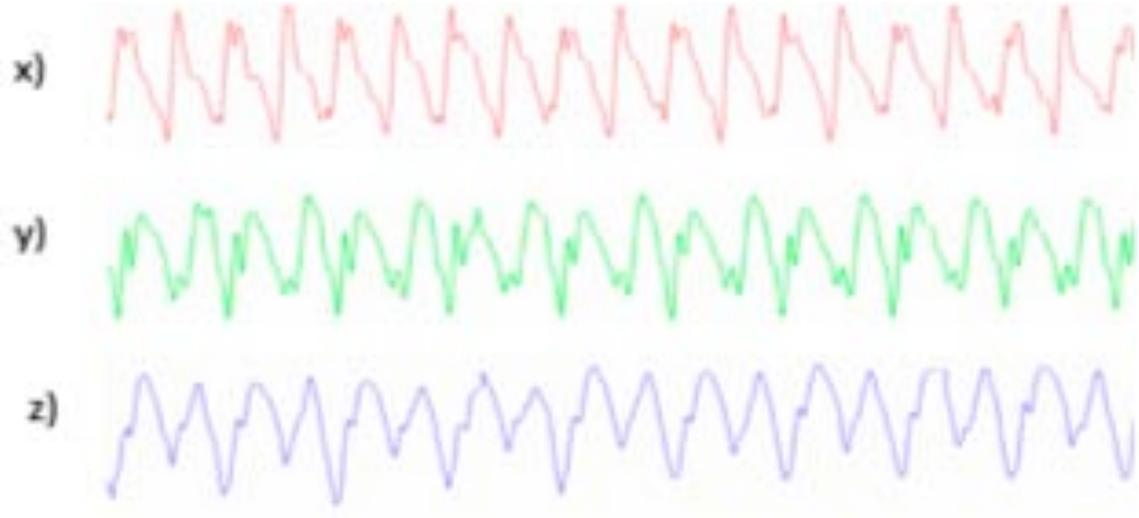
- Microphone
  - Speaker recogntion
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

Gait Recognition

Biometric Gait Recognition

Offer an unobtrusive authentication method based on gait

- Use accelerometers - already embedded in mobile devices to record the gait
  - Many phones contain accelerometers
  - No extra hardware is necessary
  - Acceleration measured in 3-directions



Biometric Gait Recognition

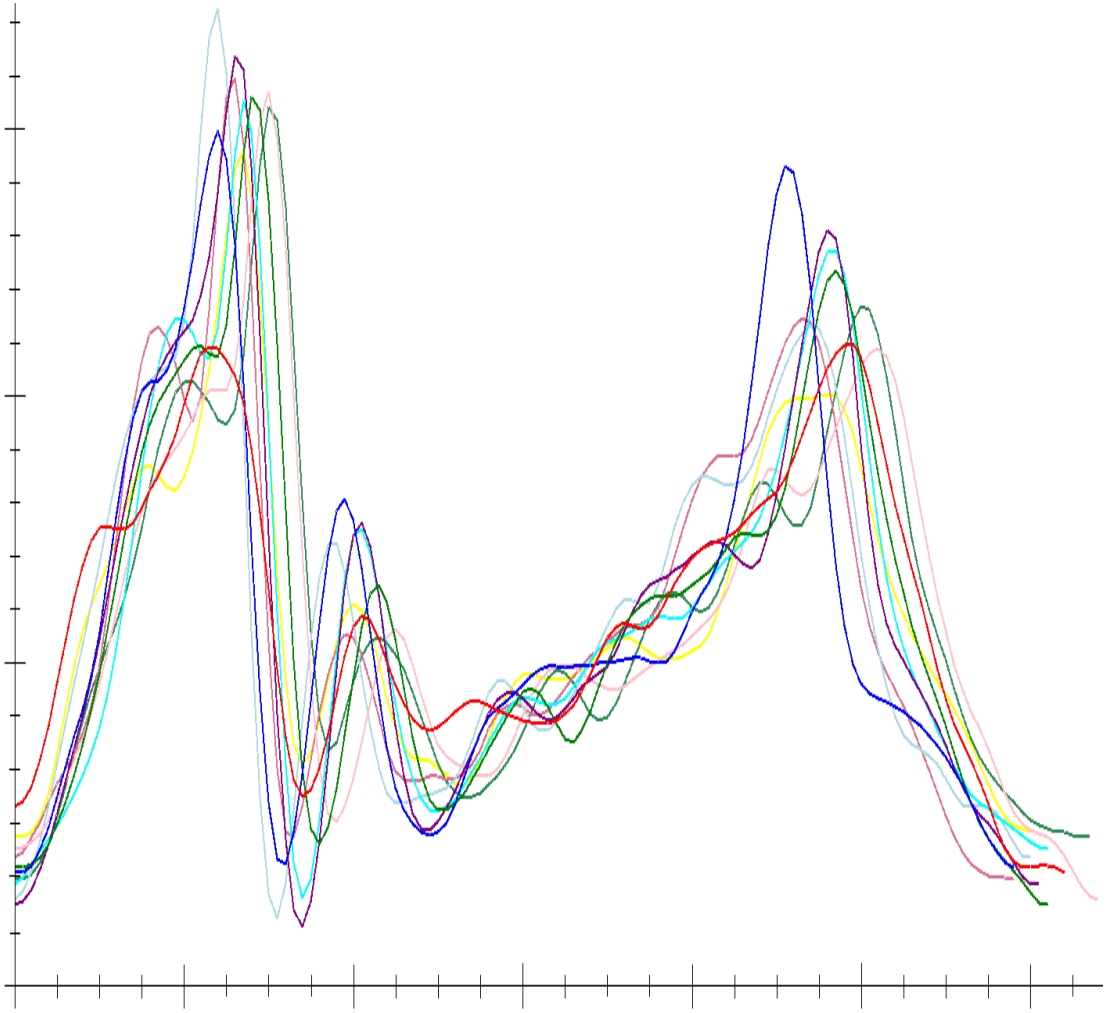
Offer an unobtrusive authentication

- While the owner is walking with the phone, he is recognized based on his gait
  - no PIN-authentication necessary

Gait Recognition - Authentication

Low Intra-Class variance

- high inter-class variance



Research Topics

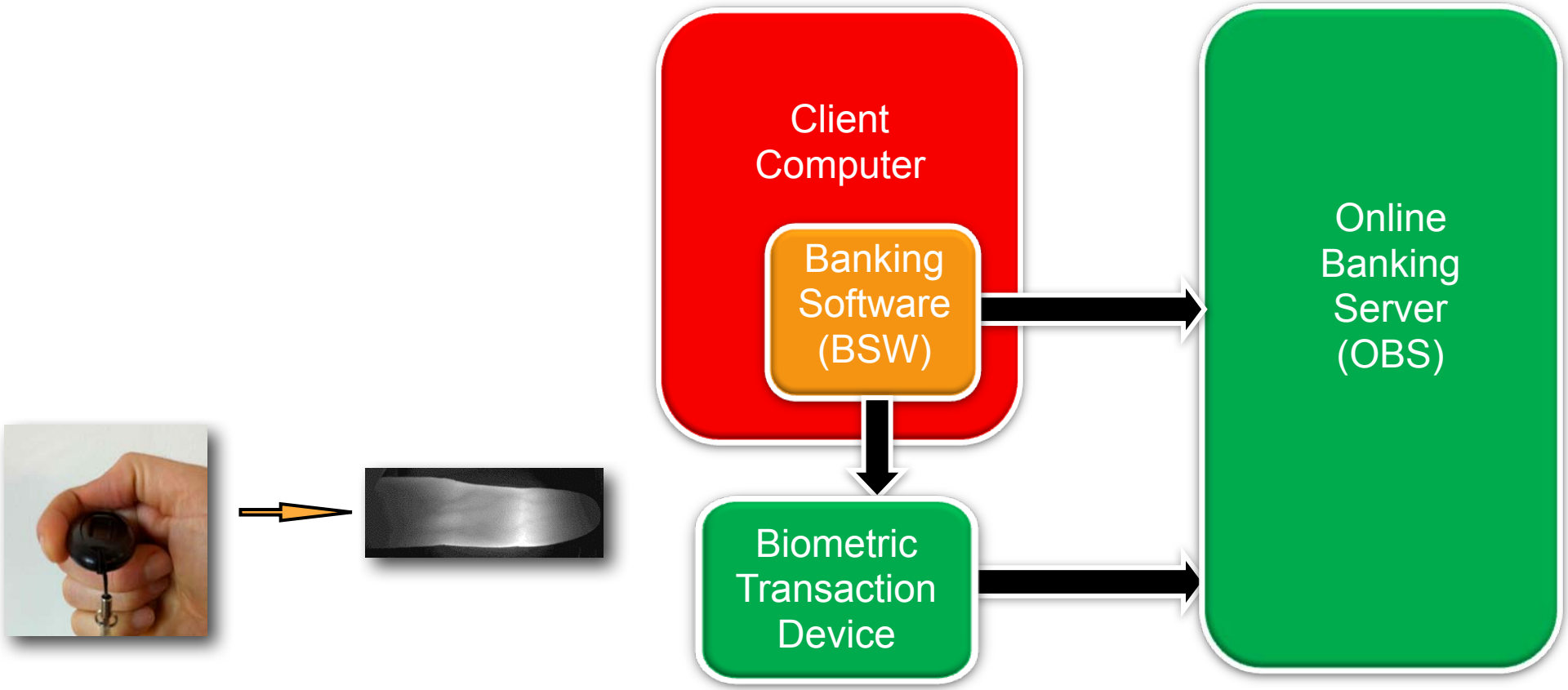
Liveness Detection

- Suspicious Presentation Detection (SPD)
  - alias artefact detection
  - alias spoof detection
- ISO/IEC WD 30107
  - [JTC1SC37] Information Technology - Biometrics - Antispoofing and liveness detection, 2012

Research Topics

Identity theft prevention with biometrics

- Biometric Online Banking
  - [Hart10] D. Hartung, C. Busch: "Biometric Transaction Authentication Protocol “, in Proceedings of the IEEE Securware conference, July, (2010) http://www.christoph-busch.de/projects-btap.html



Conclusion

- Large Scale Biometric Identification Systems
  - detect dubplcate enrolements
  - can be build based upon standards
- Automated Biometric Border control beomes widespread
- Biometric sensors are available in Smartphones at zero cost
  - even though they were built-in for other purposes
- Gait recognition shows reasonable biometric performance
- Implementing NFC door communication
  - will grant significant convenience

Further Information on Biometrics

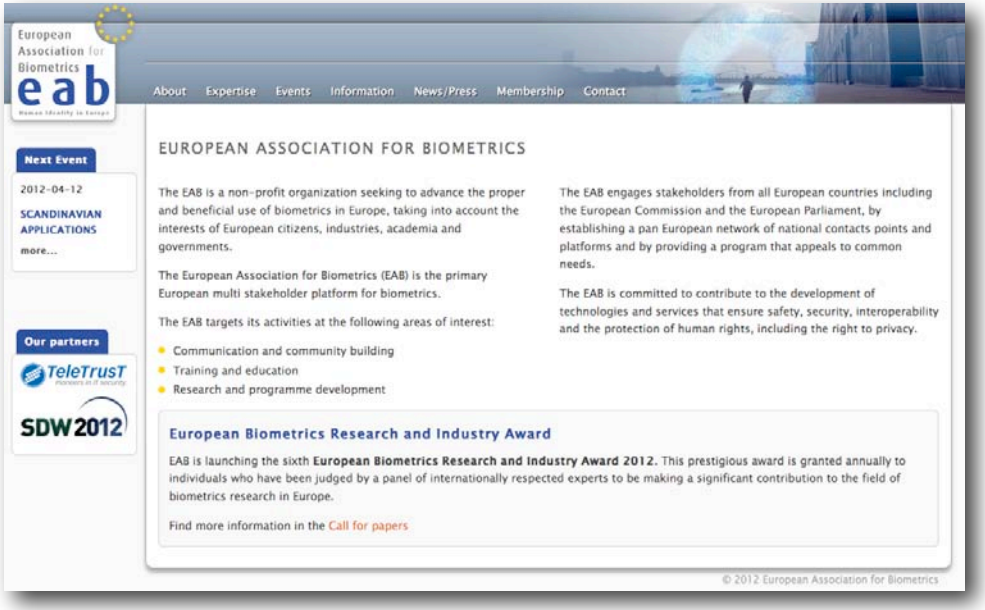
EAB

NEW: „European Association for Biometrics“

Vision:

- Services for the automated recognition of human identity is of increasing importance to the economic and social welfare
- The European context creates special requirements
- The EAB envisions and strives for a future where biometric and allied technologies are used in the service of Europe and for the benefit of all.

Website: www.eab.org



EAB

Mission

- To advance the proper and beneficial use of biometrics in Europe

Areas of interest

- Community building
- Training and education
- Research and programme development
- The EAB can set up Committees, Working Groups and Special Interest Groups
- Each area of interest shall have its own drivers and work program, supported and approved by the management board
- Target audiences:
  policy, industry, research & academia and citizens

The EAB is a non-profit organisation

BIOSIG 2012

10th BIOSIG conference - now in cooperation with IEEE

- September 6-7, 2012 / Darmstadt, Germany
  www.biosig.org/biosig2012

GI special interest group BIOSIG
in cooperation with

IEEE

Fraunhofer IGD

JRC EUROPEAN COMMISSION

Call for Papers

BIOSIG 2012

06.-07.09.2012, Darmstadt

Gesellschaft für Informatik e.V. (GI)

www.cast-forum.de · www.biosig.org

Nowadays, biometric applications are growing rapidly and have reached different areas such as health monitoring, national ID cards, e-banking, e-commerce, etc. The European Union Visa Information System (VIS) and the Indian UIDAI System are large-scale deployed systems that validate the capabilities of today's biometric products. However deployed systems are still facing challenges towards better biometric performance, interoperability, system reliability and usability. New modalities and innovative acquisition techniques such as efficient 3D-face reconstruction taken from a distance, multispectral fingerprint images, in vivo imaging are important to increase the versatility of biometrics and its area of use. Moreover biometric recognition is now used as access control schemes towards mobile phones with its embedded sensors such that many convenience applications can now be served. Both in security and convenience applications efficient fusion techniques for multimodality systems are necessary to improve performance and robustness. When biometrics is chosen to increase the security of an access control system then the security of the biometric system itself must be investigated. This includes fake resistance of sensors, biometric information protection and crypto-biometrics to enhance the privacy of data subjects and to protect biometric references. Moreover, security analysis and certification of security properties need to be developed. Beyond that critical issues such as the compliance to standards and the early assessment of sample quality with standardized metrics systems are important to guarantee successful use of biometrics in practice.

The BIOSIG 2012 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 Joint Research Centre of the European Commission (JRC), the TeleTrusT-Association, the Norwegian Biometrics Laboratory (NBL), the Center for Advanced Security Research Darmstadt (CASED) the Fraunhofer Institute for Computer Graphics Research IGD, and the special interest group BIOSIG of the Gesellschaft für Informatik e.V. (GI). The conference will be technically co-sponsored by IEEE and papers will be added to IEEE Xplore.

We invite stakeholders and technical experts to submit original research papers. Industrial contributions presenting lessons learned from practical usage, case study, recent results of prototypes, are also welcomed. Submissions should be full papers (max. 12 pages) in English. Authors should upload their submission to the EasyChair platform at:
https://www.easychair.org/account/signin.cgi?conf=biosig2012
and use the GI format for which templates are available at:
http://www.gi.de/fileadmin/redaktion/Autorenrichtlinien/LNI-LaTeX-Vorlage.zip (LaTeX-template)
and
http://www.gi.de/fileadmin/redaktion/Autorenrichtlinien/LNI-word-vorlage-en.doc (Word-template).

Important Dates

15.05.2012	Deadline for electronic submissions
30.06.2012	Notification of authors via e-mail
31.07.2012	Deadline for final papers (ready for press)
06./07.09.2012	Conference: Talks and Presentations

Special Interest Group BIOSIG

The BIOSIG Group is dedicated to the foundations of biometrics. In order to develop the topics in this context and to link practical experience with academic innovations 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

The topics of the conference include but are not limited to: Biometric standards and interoperability, multimodal and multi-biometrics (sensor, modality, sample, feature, score and decision fusion), security analysis of biometric components or systems, on-card comparison, fake resistance, liveness detection, aging of reference data, template protection, derivation of cryptographic keys from biometrics, biometric middleware, user interface design for biometric systems, biometric performance measurement, sample quality, best practices, usability, emerging applications, ethical, legal and socio-technological aspects, biometrics for public administrations.

Organizer

Organizer GI-BIOSIG and CAST e.V:
Christoph Busch: christoph.busch@cast-forum.de
Arslan Brömme: arslan.broemme@aviomatik.de
BIOSIG Webmaster: V.-P. Busch: **webmaster@biosig.de**

Program Committee

H. Baier (HDA-CASED, DE), O. Bausinger (BSI, DE), B. Brecht (BDR, DE), A. Brömme (GI/BIOSIG, DE), P. Bours (GUC, NO), J. Bringer (Morpho, FR), C. Busch (CAST-Forum, DE), V.-P. Busch (Uni HH, DE), P. Campisi (Uni Roma, IT), H. Daum (G&D, DE), N. Delvaux (Morpho, FR), F. Deravi (UKE, UK), B. Dorizzi (IT, FR), M. Drahansky (BUT, CZ), J. Fierrez (UAM, ES), S. Fischer-Hübner (KAU, SE), P. Flynn (ND, US), L. Fritsch (NR, NO), R. Grimm (Uni Koblenz, DE), P. Grother (NIST, US), D. Hartung (GUC, NO), O. Henniger (Fraunhofer IGD, DE), D. Hühnlein (ecsec, DE), H. Ihmor (BSI, DE), C. Kaplan (softpro, DE), S. Katzenbeisser (TUD-CASED, DE), U. Korte (BSI, DE), B. Kowalski (BSI, DE), A. Kumar (Poly, HK), H. Leitold (a-sit, AT), S. Li (CBSR, CN), L. Lo Iacono (EUFH, DE), M. Lockie (PB, UK), U. Mahlmeister (L1, US), D. Maltoni (UDB, IT), T. Mansfield (NPL, UK), J. Merkle (secunet, DE), E. Mordini (CSSC, IT), A. Munde (BSI, DE), C. Nickel (HDA-CASED, DE), A. Nouak (Fraunhofer IGD, DE), M. Nuppeney (BSI, DE), H. Ogata (Hitachi, JP), J. Ortega-Garcia (UAM, ES), M. Peirce (Daon, IR), I. Pitas (AUT, GR), F. Podio (NIST, US), R. Posch (TUG, AT), N. Ratha (IBM, US), C. Rathgeb (HDA-CASED, DE), K. Rannenberg (Uni FFM, DE), M. Rejman-Greene (HO, UK), A. Ross (WVU, US), H. Roßnagel (Fraunhofer IAO, DE), R. Sanchez-Reillo (UC3M, ES), S. Schuckers (CIU, US), G. Schumacher (JRC, IT), T. Shinzaki (Fujitsu, JP), M. Snijder (EBG, NL), E. Tabassi (NIST, US), T. Tan (NLPR, CN), M. Tistarelli (UNISS, IT), C. Tilton (Daon, US), D. Tzovoras (CfRaT, GR), M. Ullmann (BSI, DE), M. v.d. Veen (GenKey, NL), R. Veldhuis (UTW, NL), B. Yang (GUC, NO), J. Wayman (SJSU, US), F. Willems (UE, NL), A. Wolf (BDR, DE), H. Xu (UTW, NL), X. Zhou (HDA-CASED, DE)

Norsk Biometri Forum

National working group for Biometrics

- Topics are related to biometric research, technologies and applications

Scope

- The working group is an open platform dedicated to regular exchange of information related to the field of Biometrics.
- The target of the working group is the interdisciplinary discussion between research, technology developers, data privacy experts, governmental agencies and operators of Biometric Systems.
- The group identifies new applications and offers a platform to present latest research results and products.

Next meeting: November 15th, 2012 @ NID

Contact


HØGSKOLEN I GJØVIK
GJØVIK UNIVERSITY COLLEGE
FACULTY OF COMPUTER SCIENCE AND MEDIA TECHNOLOGY
Christoph Busch, Dr.-Ing.
Professor
P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no