

From Liveness Detection to Presentation Attack Detection

Christoph Busch

Gjøvik University College
<http://www.christoph-busch.de>

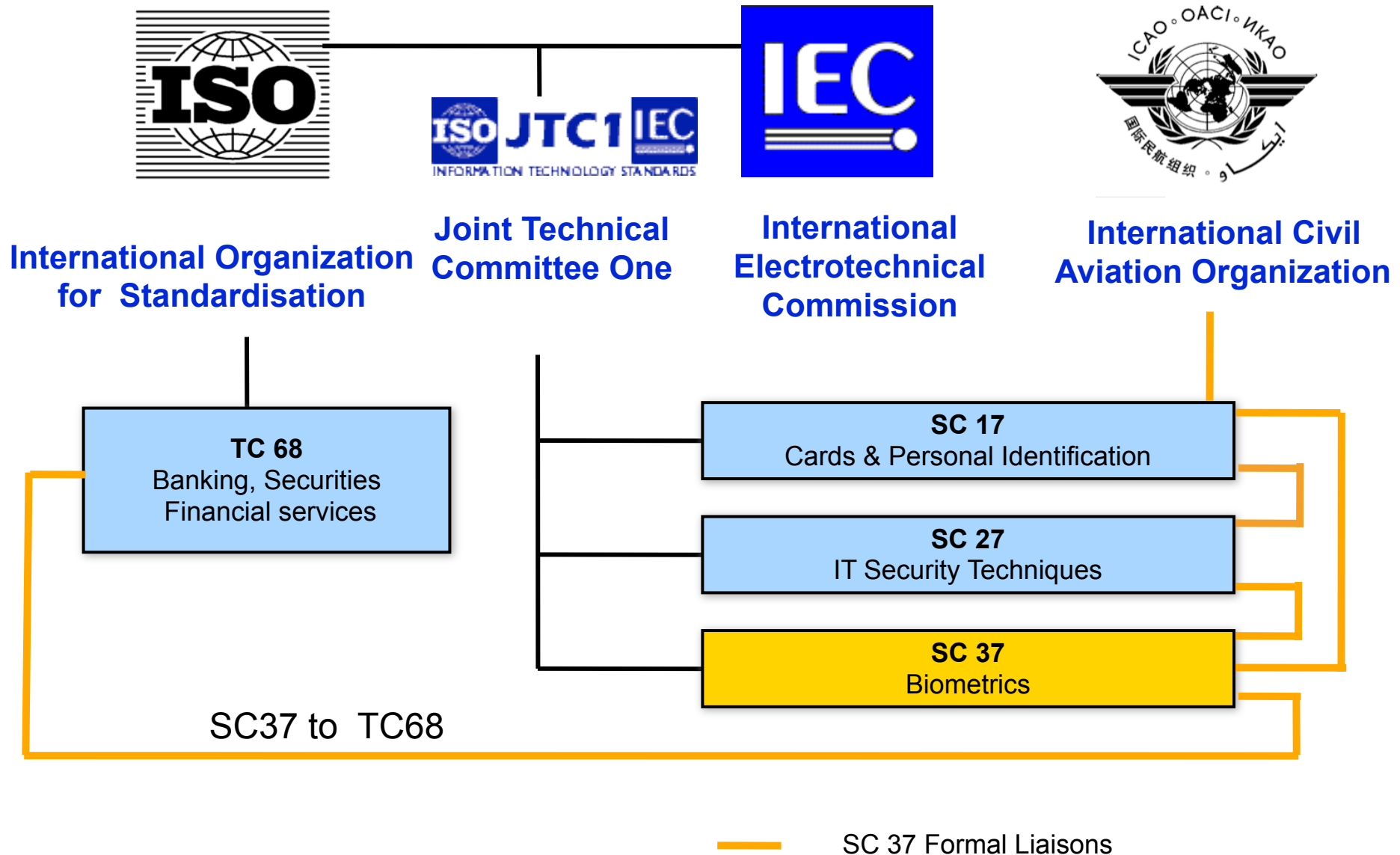
Norsk Biometri Forum
Oslo November 27, 2014

Agenda

- Certification is important and requested
 - should one develop new standards to test against?
 - should one test against existing standards?
- Existing International Standardisation
- Performance Testing
- Vulnerability of Biometric Capture Devices
 - Development of the Presentation Attack Detection Standard

International Standardisation

Biometric Standardisation



ISO/IEC 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

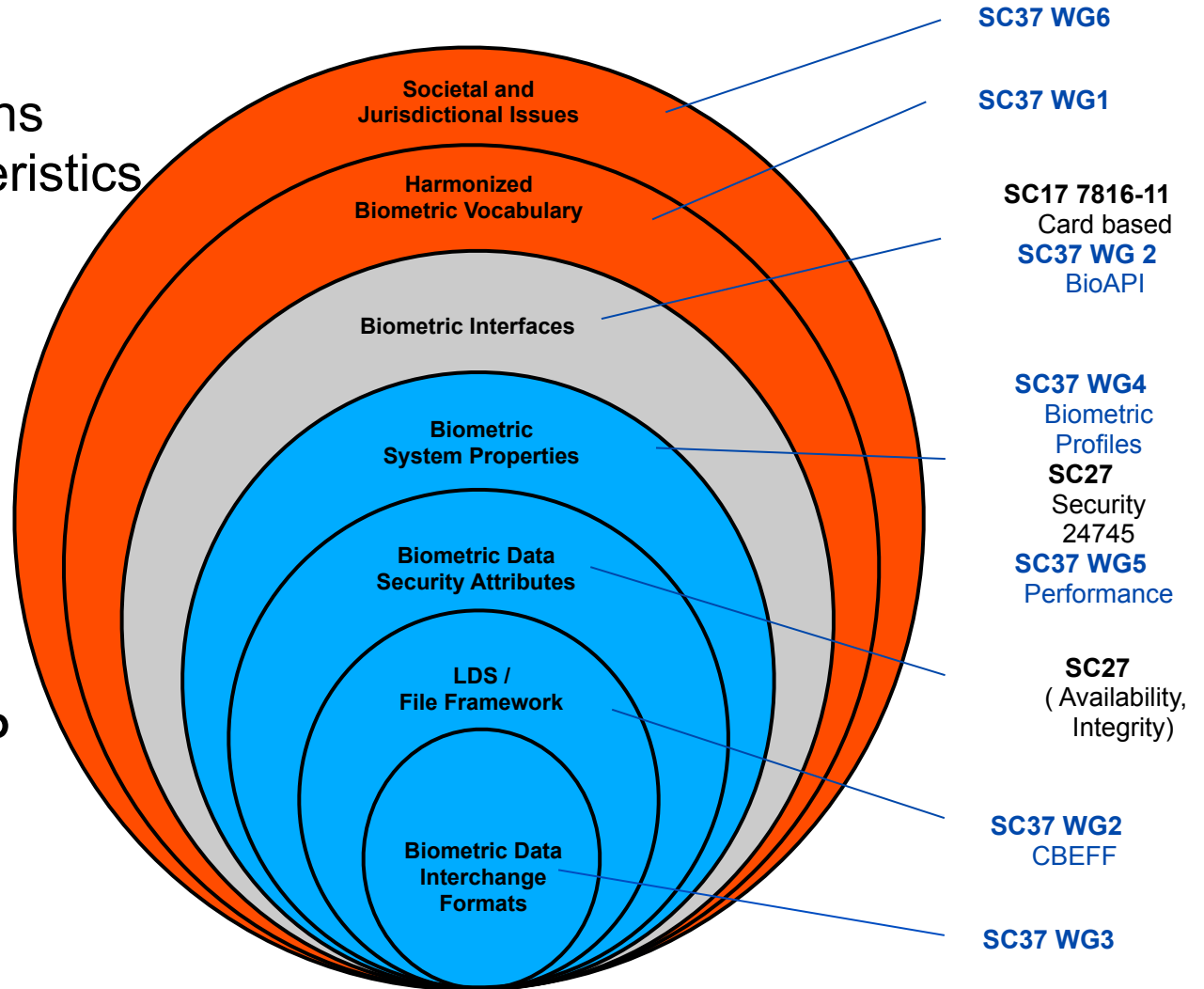
- “Standardization of *generic biometric* technologies pertaining to *human* beings to support *interoperability* and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming *interfaces*; biometric data interchange *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 two meetings: January 2015 in Spain
June 2015 in Gjøvik

Biometric Standardisation

Onion Layers

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



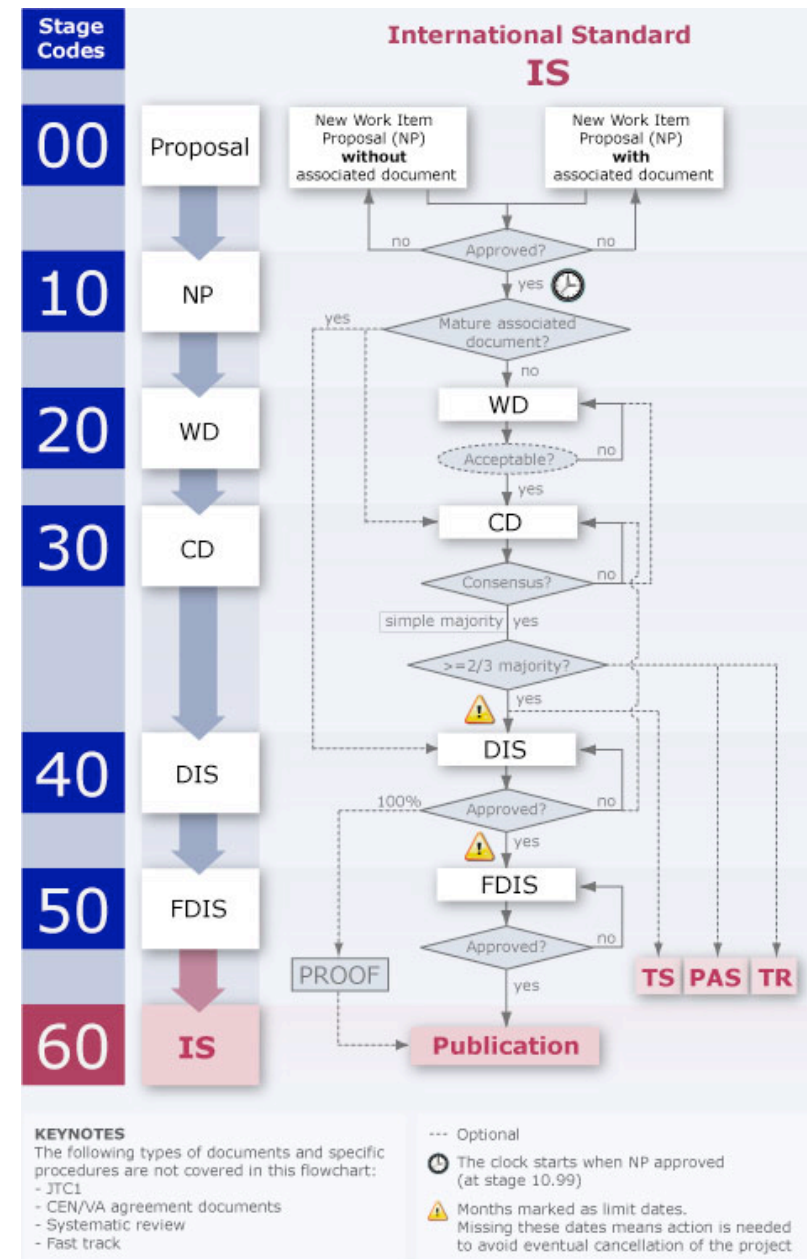
Levels of Development?

Progression levels

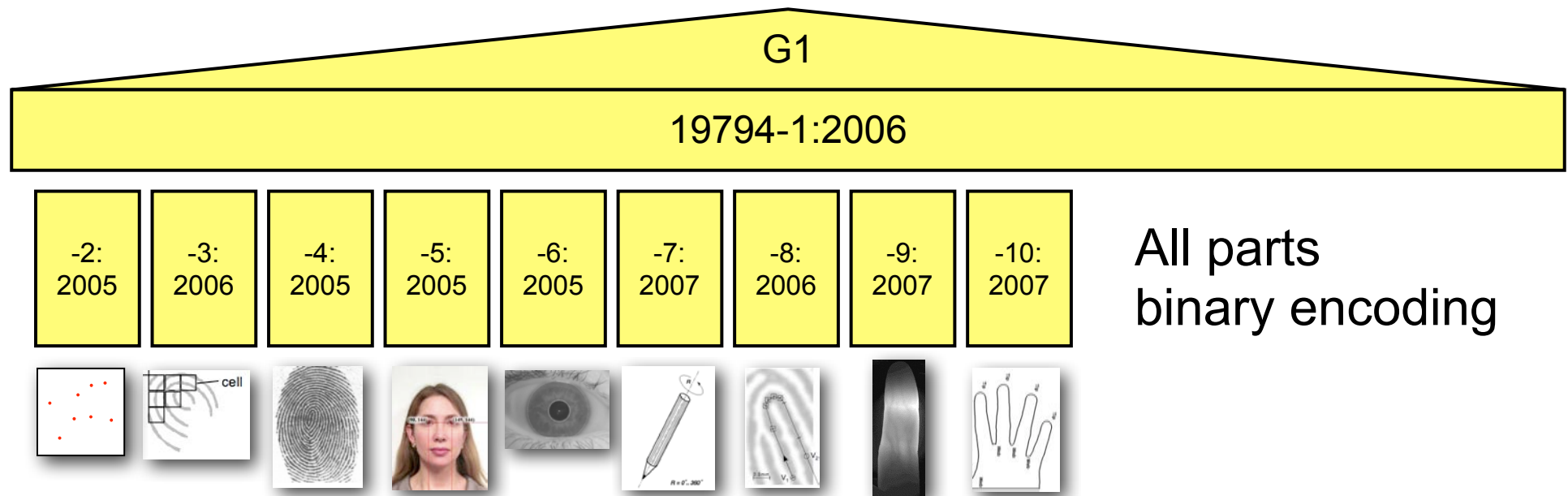
- Working Draft (WD)
- Committee Draft (CD)
- Draft International Standard (DIS)
- Final Draft International Standard (FDIS)
- International Standard (IS)

Issues to consider:

- Need for mature technology
- Decisions are made on consensus
- Commenting periods
- Potentially multiple loops at one level
- Need to progress
- Five year revision cycle

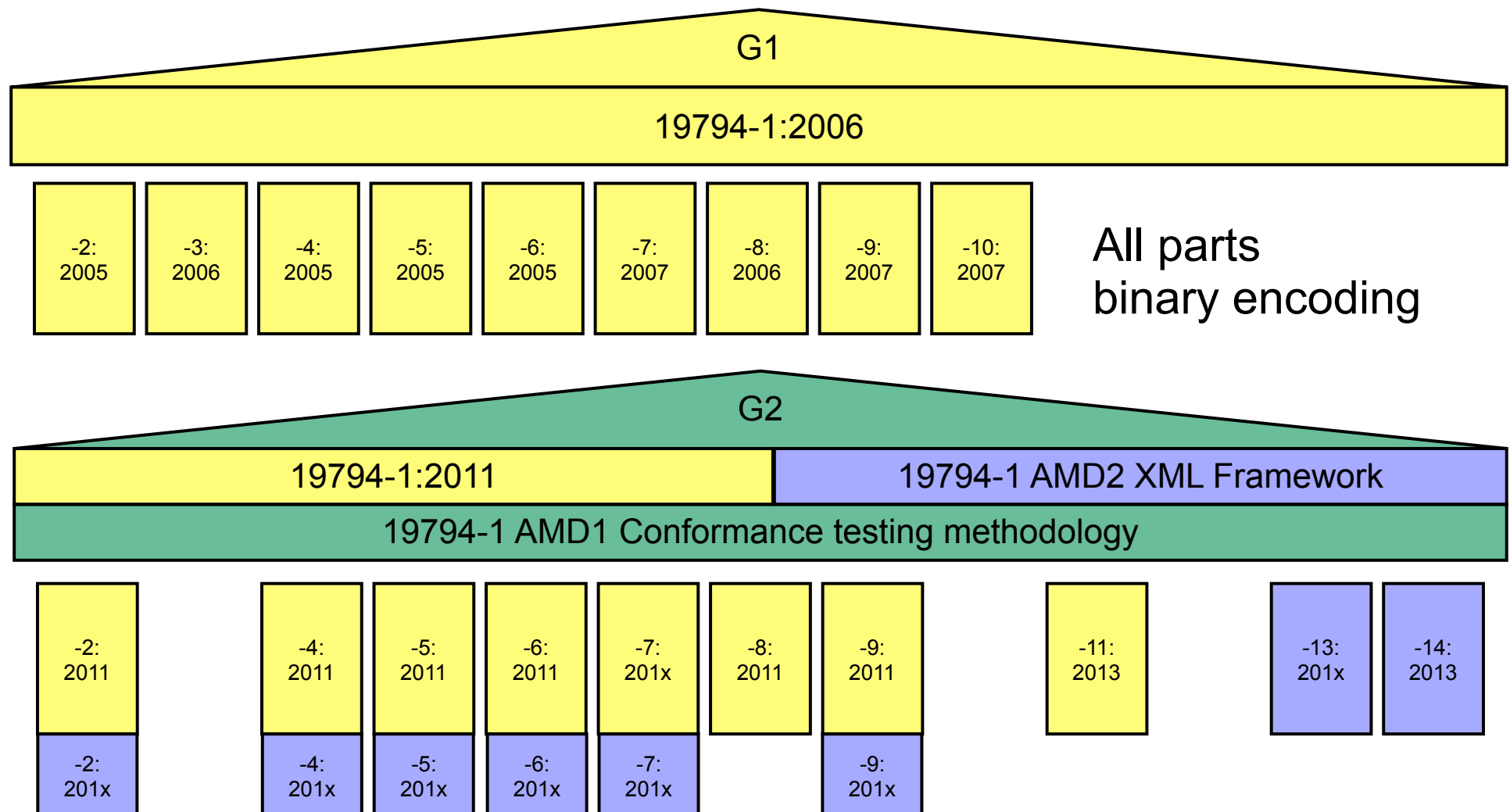


ISO/IEC Interchange Format Standards



The 19794-Family: Biometric data interchange formats

Generation 2 of ISO/IEC 19794



the semantic is equivalent for binary encoded and XML encoded records

Biometric Performance Testing

ISO/IEC 19795-1:2006

Biometric Performance Testing

Operators **may** think:

„what are the error rates?“



Biometric Performance Testing Standard

ISO/IEC 19795-x, Information technology - Biometric performance testing and reporting

- Part 1: Principles & Framework
 - Guidance applicable to the broad range of tests
- Part 2: Testing Methodologies for Technology and Scenario Evaluation
 - Multiple visits, habituation, enrolment
- Part 3: Modality-Specific Testing
 - Modality (& application) specific methodologies
- Part 4: Interoperability Performance Testing
 - Performance on other vendors data
- Part 5: Framework for biometric device performance evaluation for access control
- Part 6: Testing Methodologies for Operational Evaluation
- Part 7: Testing of ISO/IEC 7816-based Verification Algorithms
- Part 8: Performance Testing of Template Protection Schemes

Performance Metrics

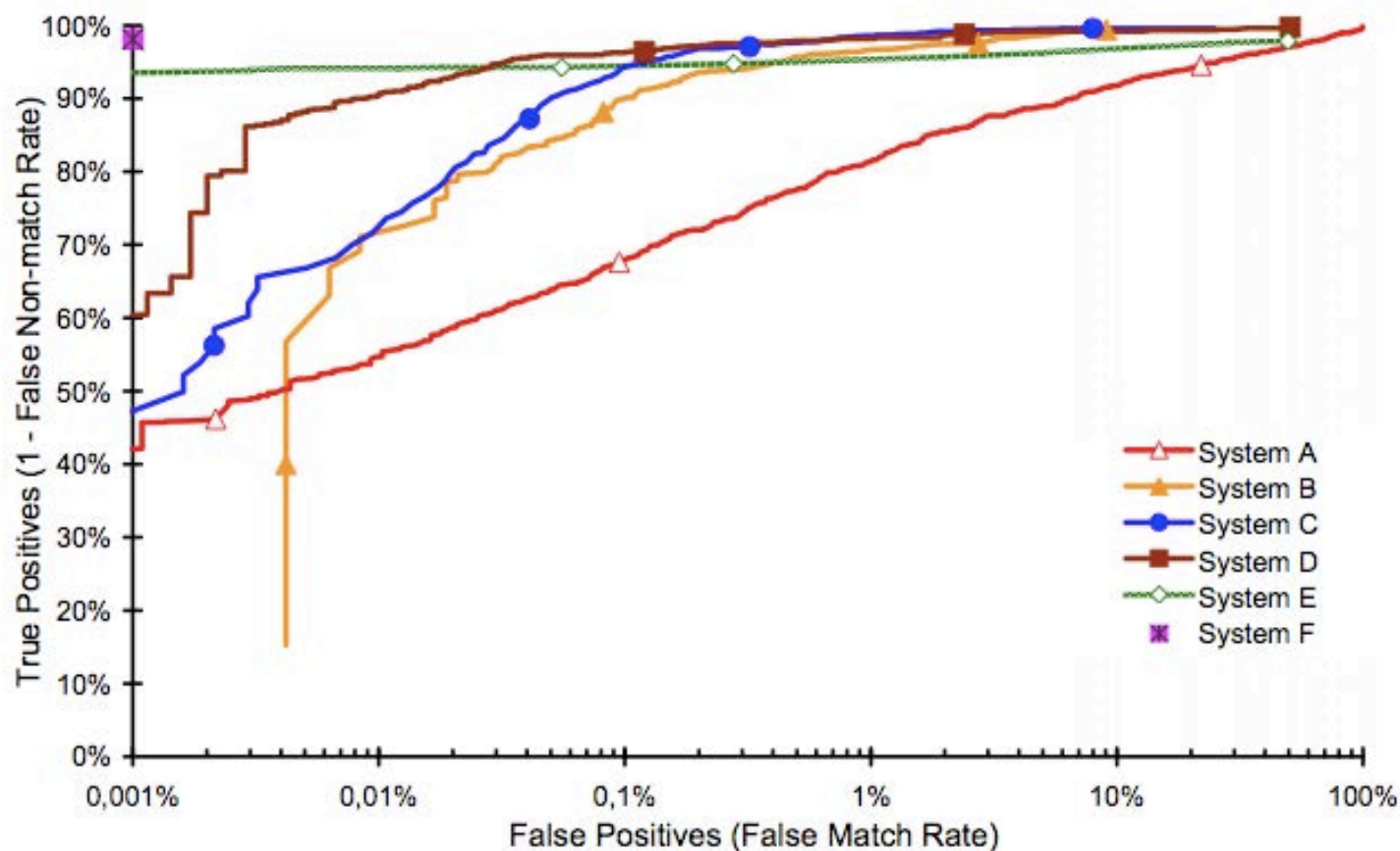
Categorization

- Technology testing
 - **Algorithmic level** verification error
 - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ imposter
 - False-Non-Match-Rate (FNMR) - algorithm rejects true identity
- Scenario testing and operational testing
 - **System level** verification error
 - False-Accept-Rate (FAR)
 - False-Reject-Rate (FRR)
 - System level error requires observation of:
 - Sample generation: Failure-to-Capture (FTC)
 - Enrolment: Failure-to-Enrol (FTE) - no reference for this subject
 - Verification: Failure-to-Acquire (FTA) - no probe feature vector

Graphical Presentation

ROC curve (Receiver operating characteristic curve)

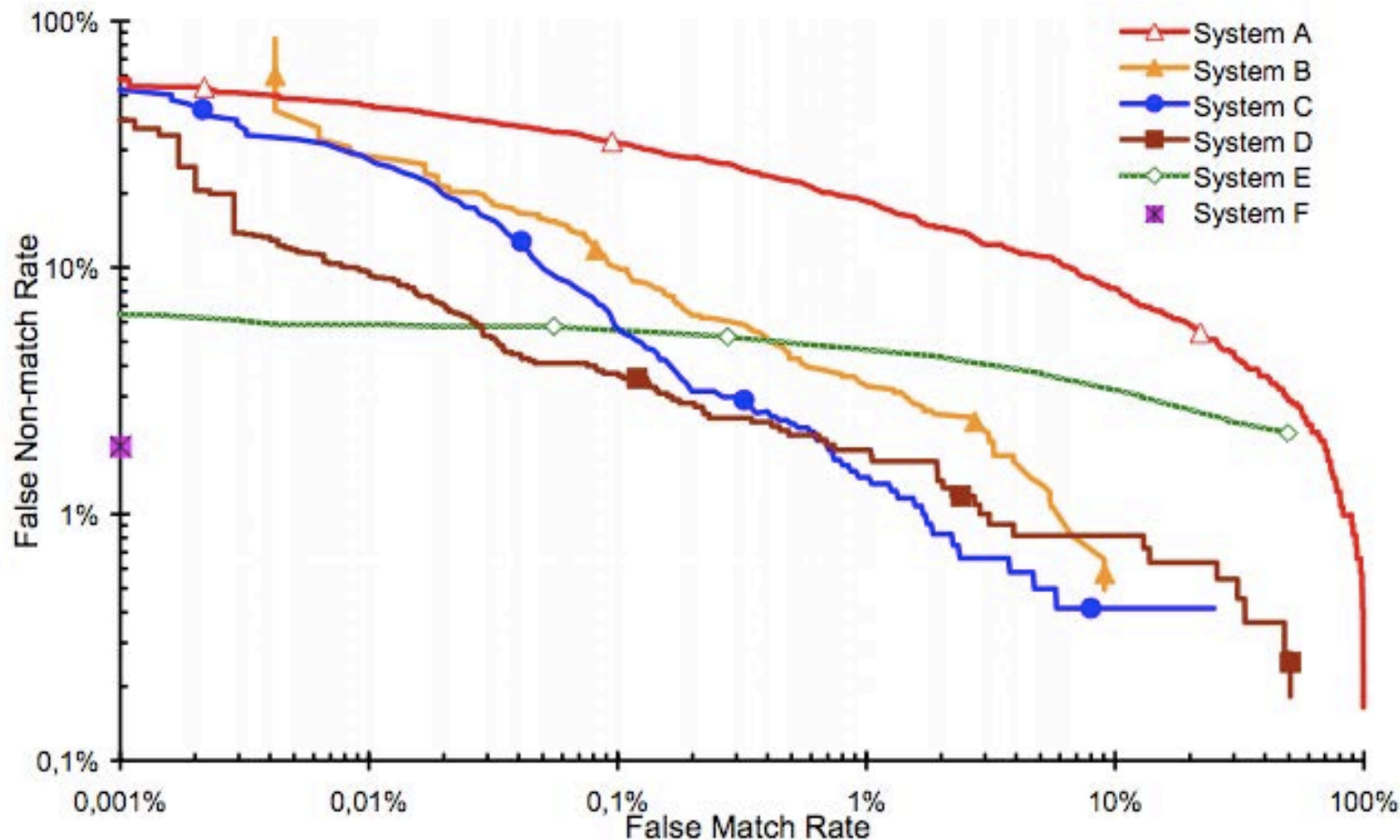
- Plot of the rate of **false positives** (i.e. impostor attempts accepted) on the x-axis against the corresponding rate of **true positives** (i.e genuine attempts accepted) on the y-axis plotted parametrically as a function of the decision threshold



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)



Vulnerability Testing

Vulnerability Testing

Operators **may** think:

„Biometric sensors can not detect gummy and cut-off fingers“



Smart Phone Access Contol

- Presentation Attacks



Gummy Finger Production in 2000 !

Attack **without** support of an enrolled individual

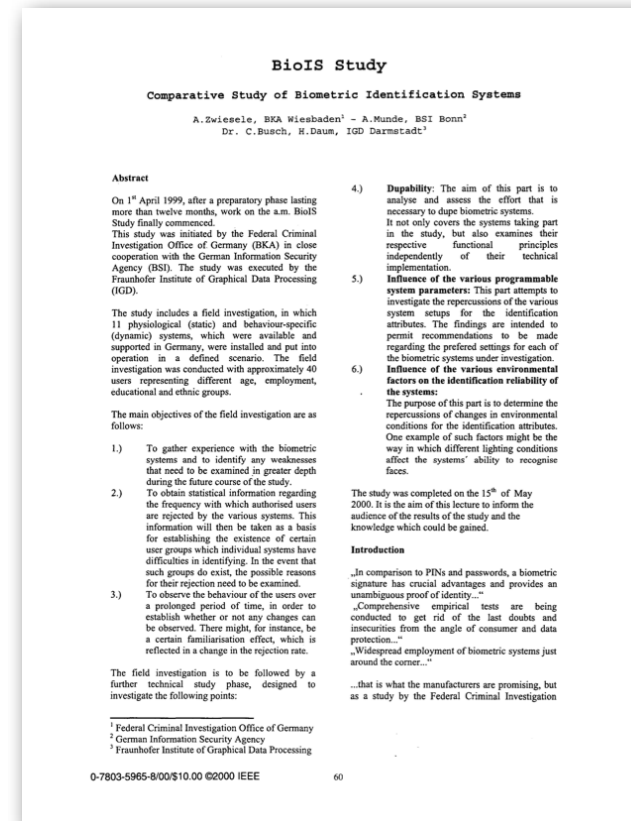
- Recording of an analog fingerprint from flat surface material
 - z.B. glass, CD-cover, etc.
with iron powder and tape
- Scanning and post processing:
 - Correction of scanning errors
 - Closing of ridge lines (as needed)
 - Image inversion
- Print on transparent slide
- Photochemical production of a platine



Gummy Finger Production in 2000 !

Reported in a publication by BKA

- A. Zwieselee et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)



Face Mask Production in 2013

Attack again **without** support of an enrolled individual

- Frontal and profile photos are uploaded
- 3D face dataset rendered and produced



Smartphone Access Contol

Capture process

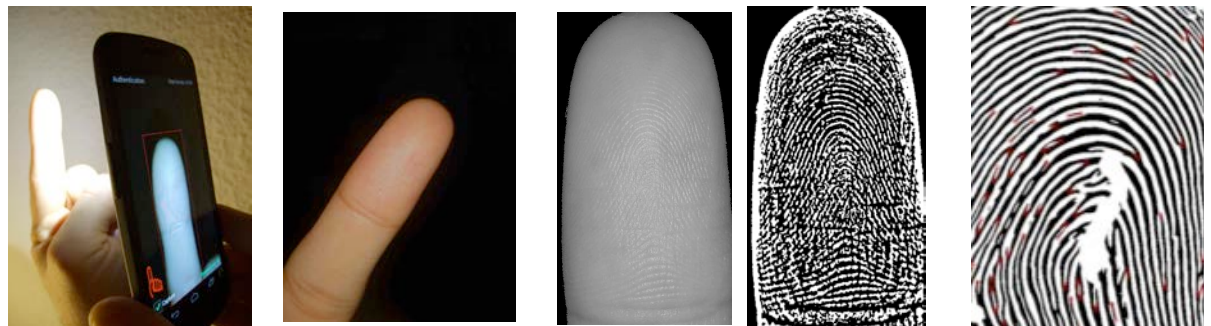
- Camera operating in **macro** modus



Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on

Finger illuminated

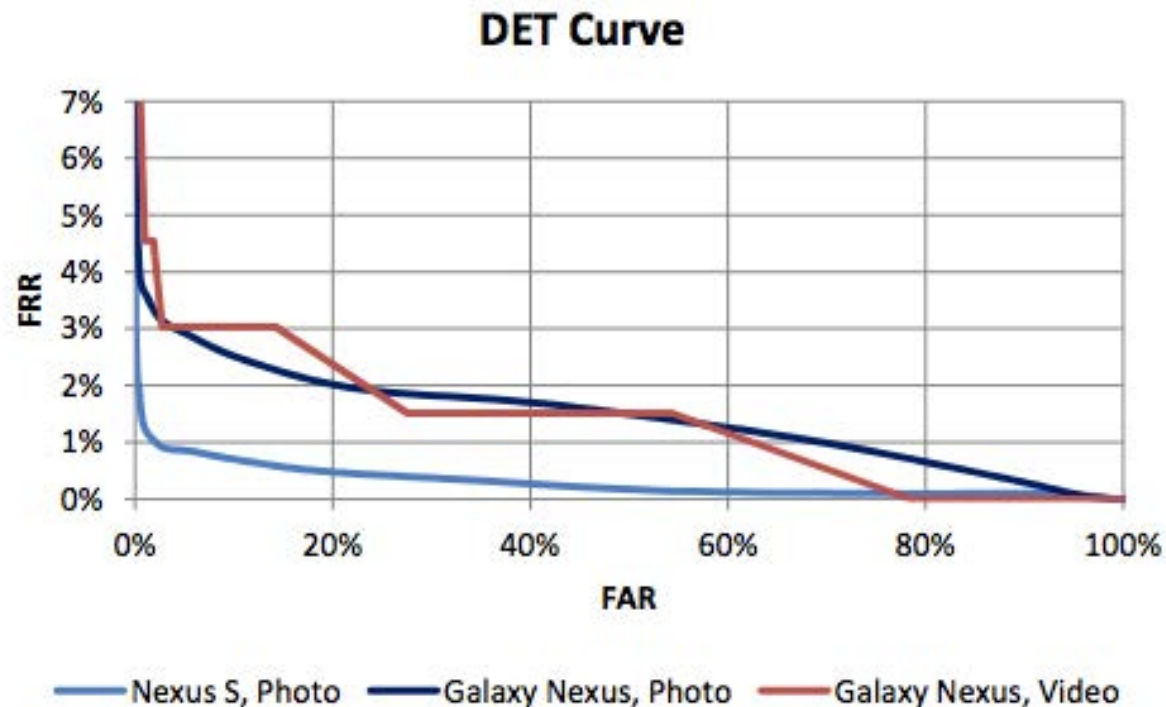


[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Smartphone Access Contol

Finger recognition study - 2012/2013

- Results: **biometric performance** at 1.2% EER



Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR=0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smartphone Access Contol

Finger recognition study - 2012/2013

- Presentation Attacks
 - 1: replay from Smartphone display (simple)
 - 2: self generated print-outs (not critical to detect)
 - 3: Ralph Breithaupt's / BSI best artefacts (very challenging)



Replay attack



Simple artefacts



Challenging artefacts

Smartphone Access Contol

Finger recognition study - 2012/2013

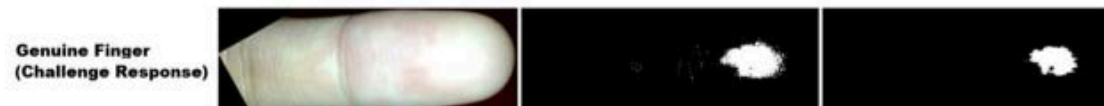
- Observation
 - significant strong **light reflection** near the fingertip
 - from the cameras LED
- Reflection depends on
 - **Shape** of the finger
 - **Consistency** of the finger
 - **Angle** of the finger to the camera
- Attack detection, as light reflection differs from artefacts to genuine fingers
- [SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)



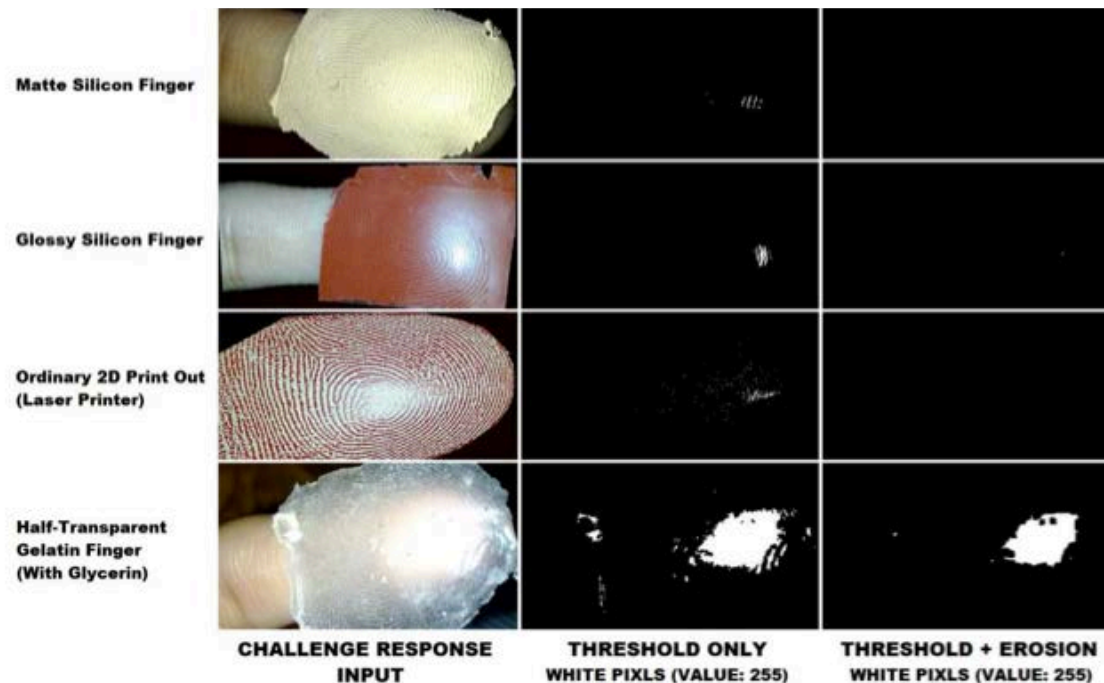
Smartphone Access Contol

Finger recognition study - 2012/2013

- Normal presentation with genuine finger



- Results: Presentation Attack Detection (PAD)

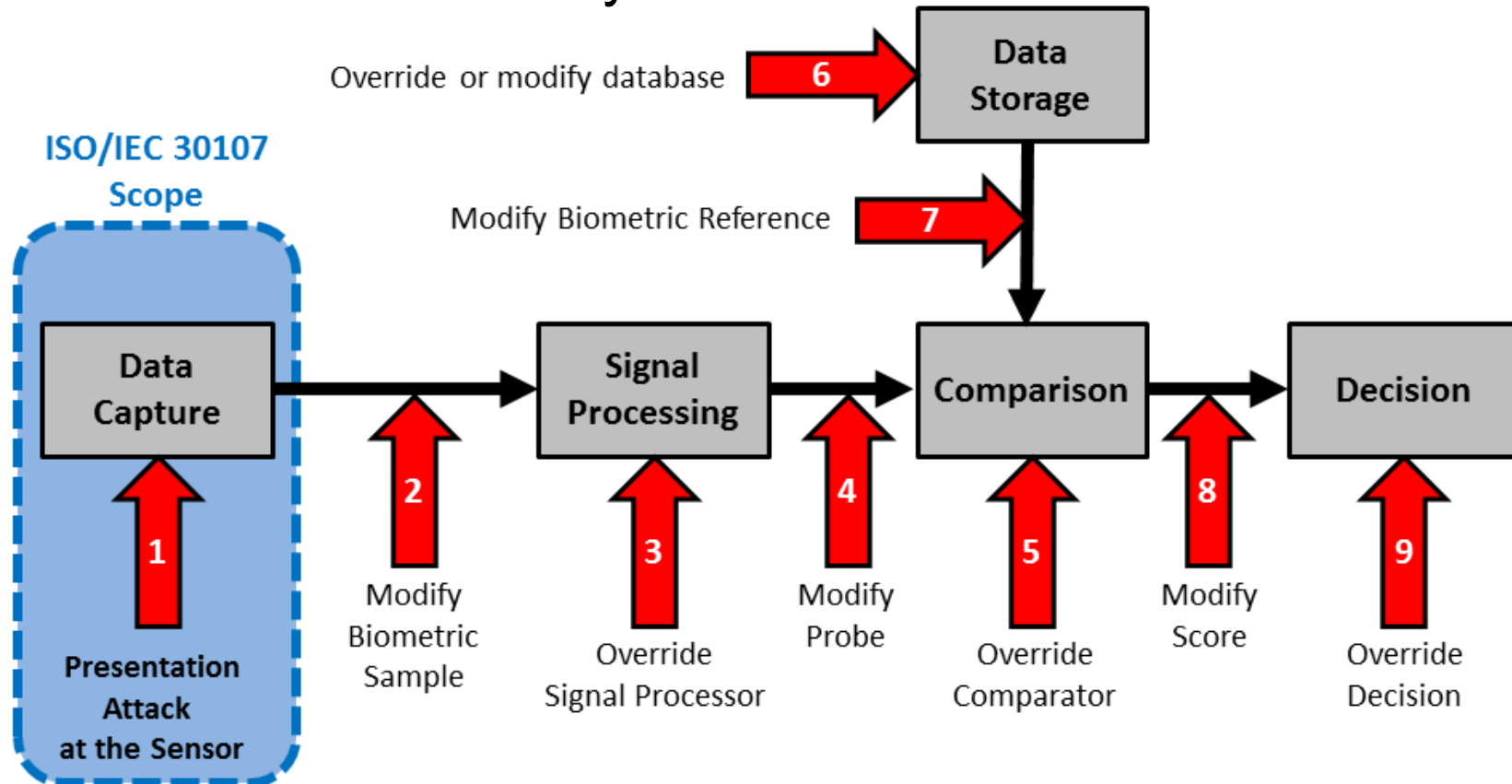


- Conclusion:
better **Presentation Attack Detection** than capacitive sensors

Liveness Detection

ISO/IEC CD 30107 - Presentation Attack Detection

- Attacks on Biometric Systems



Source: ISO/IEC 30107-1 inspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

Presentation Attack Detection

ISO/IEC 30107 - Scope

- terms and **definitions** that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common **data format** for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and **methods** for performance **assessment** of presentation attack detection algorithms or mechanisms; and

Outside the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

Presentation Attack Detection

30107 parts

- Part 1 (IS) - Framework
 - Elaine Newton
 - status: 2nd CD
- Part 2 (IS) - Data formats
 - Olaf Henniger
 - status: WD
- Part 3 (IS) Testing and Reporting
 - Michael Thieme
 - status: WD

Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**

*presentation to the biometric capture subsystem with the goal of **interfering** with the operation of the biometric system*

- **presentation attack detection (PAD)**

*automated **determination of** a presentation **attack***

Definitions in ISO/IEC 2382-37: Vocabulary

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

- **impostor**

*subversive biometric capture subject who attempts to being matched to **someone else's** biometric reference*

- **identity concealer**

*subversive biometric capture subject who attempts to **avoid being matched** to their own biometric reference*

Presentation Attack Detection

ISO/IEC 30107 - Examples of Artificial and Human Attack Presentation

Artificial	<i>Complete</i>	gummy finger, video of face
	<i>Partial</i>	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up
Human	<i>Lifeless</i>	cadaver part, severed finger/hand
	<i>Altered</i>	mutilation, surgical switching of fingerprints between hands and/or toes
	<i>Non-Conformant</i>	facial expression/extreme, tip or side of finger
	<i>Coerced¹</i>	unconscious, under duress
	<i>Conformant</i>	zero effort impostor attempt

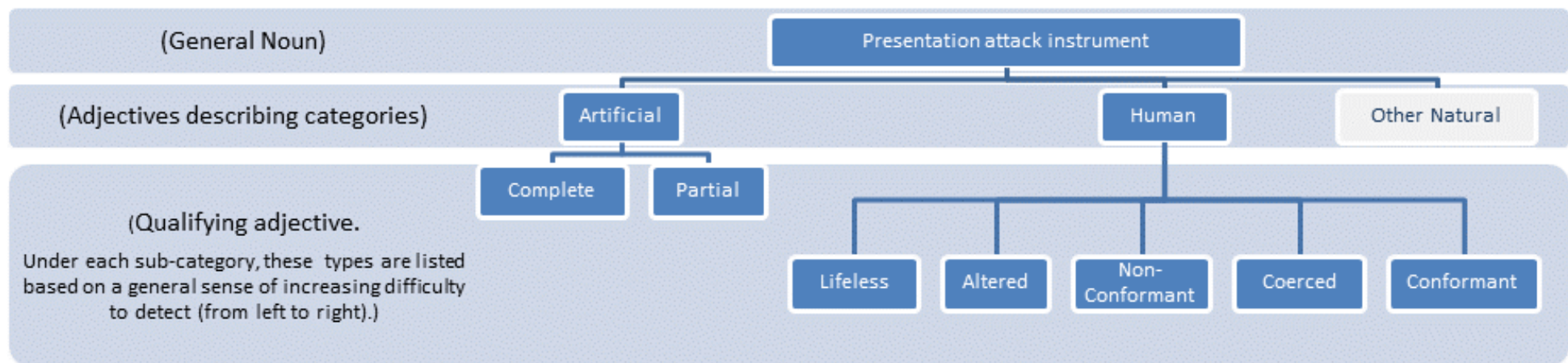
Source: ISO/IEC 30107

Presentation Attack Detection

ISO/IEC 30107 - Definitions

- **presentation attack instrument (PAI)**
*biometric characteristic or **object used** in a presentation attack*
- **artefact**
*artificial object or representation presenting a **copy** of biometric characteristics or synthetic biometric patterns*

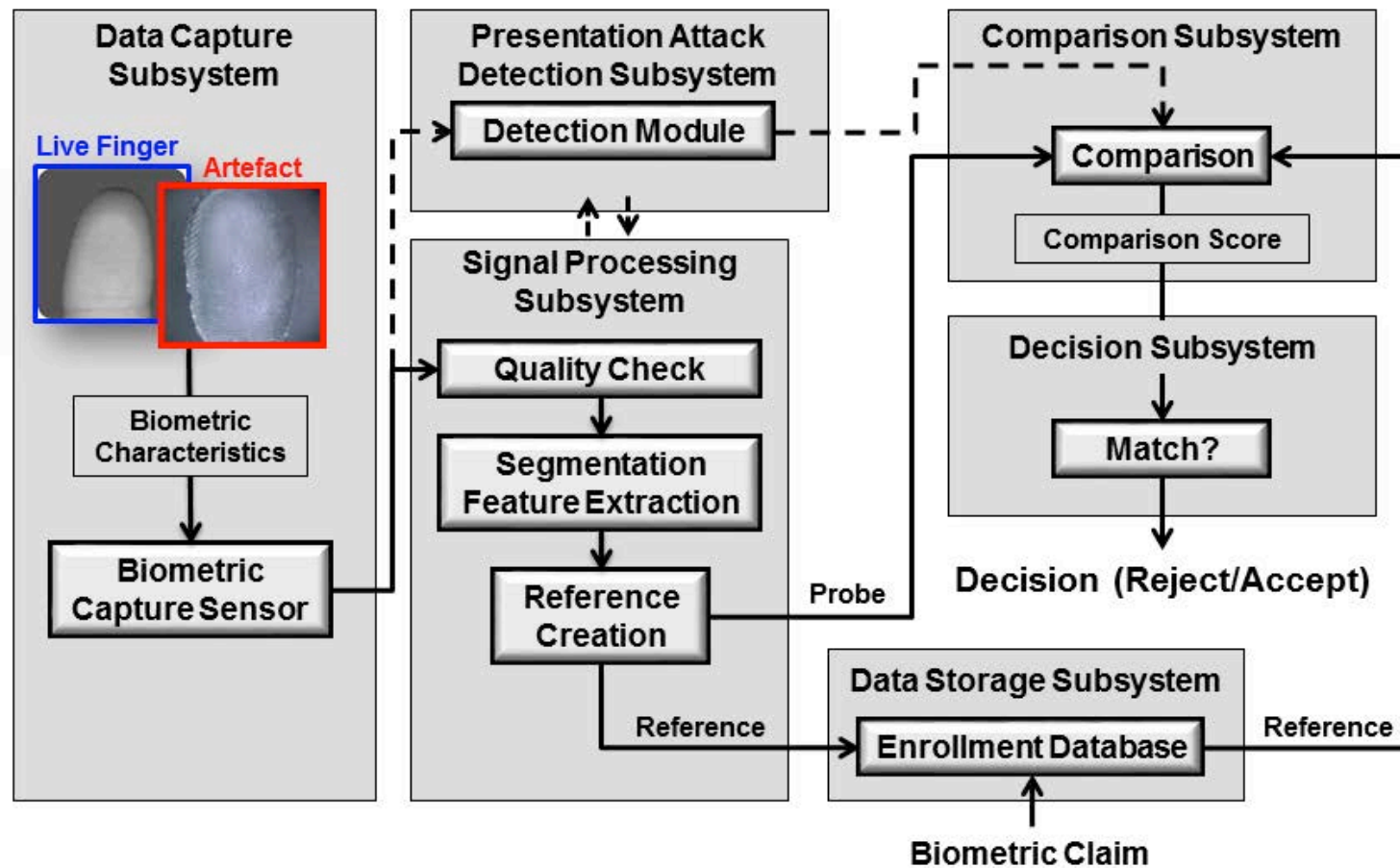
Types of presentation attacks



Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD



Source: ISO/IEC 30107

Reporting about the PAD using ISO/IEC 30107-3

Methodology in ISO/IEC 30107 Presentation Attack Detection - Part 3: Testing and reporting

- Security Evaluation
 - for evaluations using the **Common Criteria** Framework
 - Protection Profile (PP) (e.g. from German BSI)
 - Security Target (ST)
 - Evaluation Assurance Level (EAL)
 - Assessment of the attack potential
 - „if there is at least **one** artefact that can **reproducibly successful** attack the PAD-component - then the PAD failed the test“
- Other approaches
 - for evaluations in academic and technology development
 - tolerating the **limited statistical significance** of small test set
 - the statistical distribution is unknown and for sure not **normal**
 - „a **score based metric** can tell us, if the method improved“

Metrics in ISO/IEC 30107 Presentation Attack Detection - Part 3: Testing and reporting

- **Attack presentation classification error rate (APCER)**
proportion of attack presentations incorrectly classified as normal presentations at the component level in a specific scenario
- **Normal presentation classification error rate (NPCER)**
proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario

Applying ISO/IEC 30107-3 Metrics

Do the metrics currently in ISO/IEC 30107 PAD - Part 3: serve to provide a meaningful report?

- [SBB13] - Publication:
The reported number of attack presentations incorrectly classified as normal presentations was **one** out of **four** artefacts
- Thus the APCER to be reported is

$$APCER = \frac{1}{4} = 0.25$$

- but there were in fact **27 artefact species**, that were used in the background but **not reported** as they are not challenging

$$APCER = \frac{1}{27} = 0.04$$

Thoughts for improving ISO/IEC WD 30107

Refining ISO/IEC 30107-3 Metrics

Trust in a biometric sensor relates to risk

Apply classical risk assessment ?

- $Risk = \textit{Impact of Risk event} \times \textit{Probability of Occurrence}$
- we do not know the impact!

Modified assessment

- $Vulnerability = \textit{Attack Potential} \times \textit{Probability of Occurrence}$

Refining ISO/IEC 30107-3 Metrics

Needed Change

- The **size** of the corpus with the artefact species is essential
- The CC-related **attack potential** should be included in the metric definition for non-cc evaluations
 - 30107-1: **attack potential** - *attribute of a biometric presentation attack expressing the effort expended in the preparation and execution of the attack in terms of elapsed time, expertise, knowledge about the capture device being attacked, window of opportunity and equipment, graded as “no rating”, “minimal”, “basic”, “enhanced-basic,” “moderate” or “high.*
- The known **success rate** of a presentation artefact instrument is relevant and might be an approximation for the **probability of occurrence**

Refining ISO/IEC 30107-3 Metrics

Suggested **augmented** metric for ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
*proportion of attack presentations incorrectly classified as normal presentations at the component level a specific scenario - taking the **attack potential** and the known **attack instrument success rate** into account.*
- **Attack potential (AP)** = {0.2 for “minimal”, 0.4 for “basic”, 0.6 for “enhanced-basic,” 0.8 for “moderate”, 1.0 for “high.”}
- **Presentation attack instrument success rate (PAISR)**
Proportion of evaluated capture devices that could be spoofed by the specific PAI (i.e. artefact).
 - would start with a value of 1 for a new discovered artefact species and could be reduced over time (as more sensors become robust)

Refining ISO/IEC 30107-3 Metrics

Suggested refined metrics for ISO/IEC 30107-3

- The APCER could thus be expressed as

$$APCER = \frac{\sum_{i=1}^{N_{AS}} (RES_i * AP_i * PAISR_i)}{N_{AS}}$$

N_{AS} number of presentation attack instruments (PAI)
(i.e. artefact species) in the corpus

RES_i result of attack with i^{th} PAI
{0 for detected attack, 1 for successful attack}

AP_i attack potential of the i^{th} PAI
(close to zero, if artefact is easy to produce)

$PAISR_i$ presentation attack instrument success rate
(close to zero, if all sensor can detect this artefact)

Refining ISO/IEC 30107-3 Metrics

Suggested refined metrics for ISO/IEC 30107-3

- **Normal presentation classification error rate (NPCER):**
proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario
- The NPCER could thus be expressed as

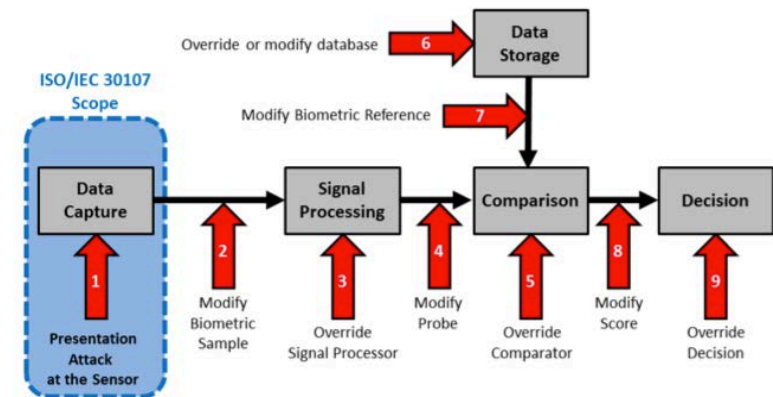
$$NPCER = \frac{\sum_{i=1}^{N_{GPA}} RES_i}{N_{GPA}}$$

- N_{GPA} number of normal presentations from a genuine subject
- RES_i result of presentation detection component for the i^{th} attempt
{0 for no detected attack, 1 for false alarm}

Conclusion

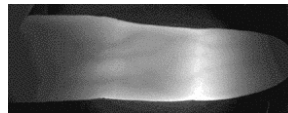
The standardisation process is **open** process

- Register and contribute to ISO/IEC 30107 Presentation Attack Detection
- Open question:
 - should PAD metrics and performance metrics be merged ?



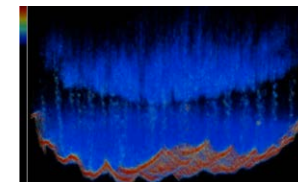
Recent research provides effective **countermeasures** to **detect** artefacts

- Vein recognition



Fingervein image

- Fingerprint Recognition with Optical Coherence Tomography (OCT)



3D Finger OCT scan

References

Web

- WG3 convenors website with latest news
<http://www.christoph-busch.de/standards-sc37wg3.html>
- ISO/IEC JTC SC37
<http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&objAction=browse&sort=name>
- Wikipedia
http://en.wikipedia.org/wiki/ISO/IEC_JTC_1/SC_37
- Published ISO Standards
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- ISO/IEC 19795-1:2006, Biometric performance testing and reporting - Part 1: Principles and framework
- ISO/IEC 24745:2011, Biometric information protection
- ISO/IEC CD 30107-1, Biometric presentation attack detection - Part 1: Framework
- ISO/IEC WD 30107-3, Biometric presentation attack detection - Part 3: Testing and reporting

Visit Norway in 2015

Norwegian Biometrics Laboratory Workshop 2015

- Presentation Attack Detection in Biometrics: Solved and Unsolved Challenges
- Chair: Dr. Raghavendra Ramachandra
- Monday, March 2, 2015
- please follow us at:
http://nislabs.no/biometrics_lab

ISO/IEC JTC1 SC37 Conference

- Working Group Meetings
- June 22 to 26, 2015 in GUC
- Standards Norge
- We are seeking **Sponsors** for the ISO - conference

Contact

