Überblick
Biometrie-Standardisierung

Christoph Busch

Hochschule Darmstadt

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

Overview Standardisation

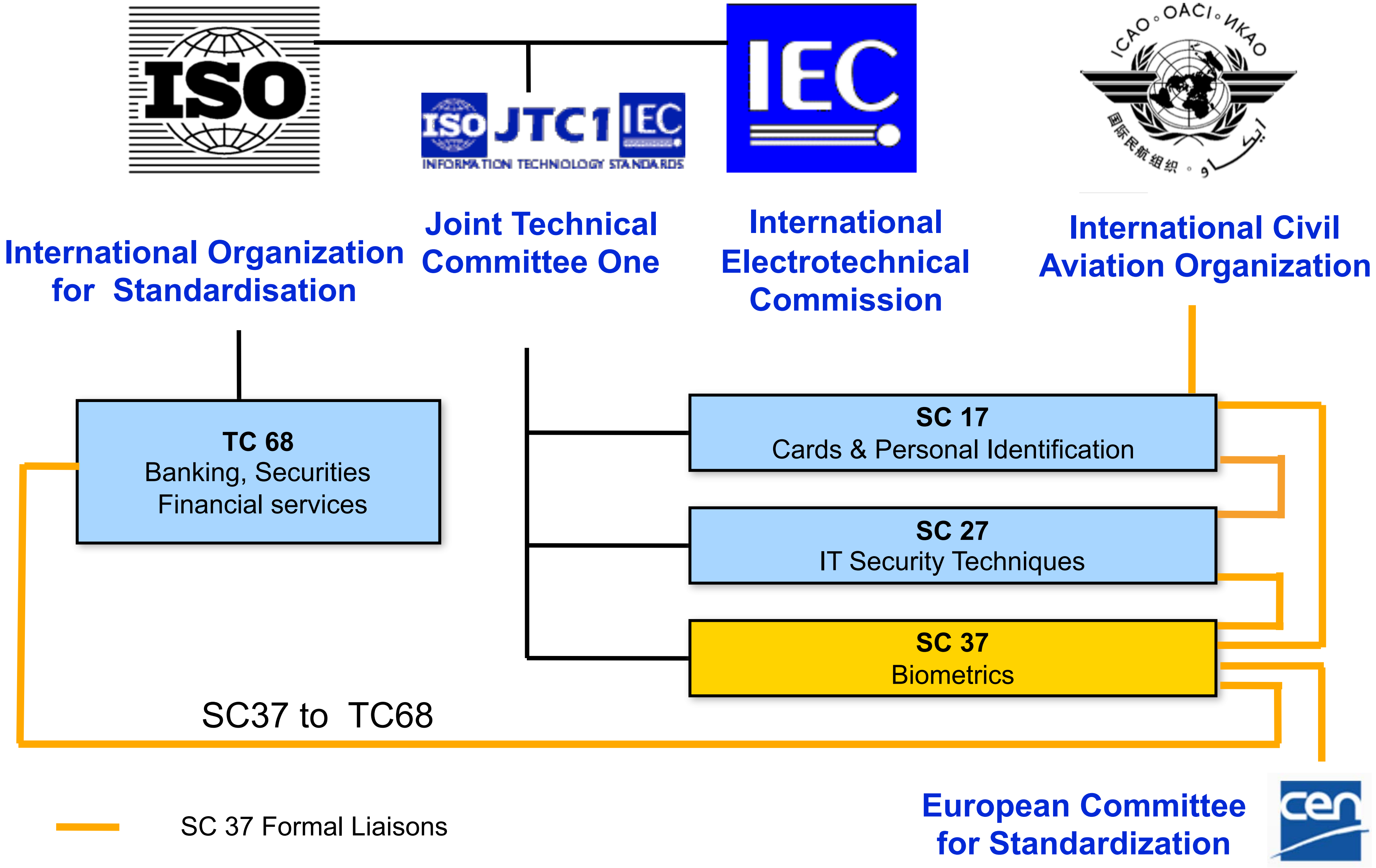
Structure of this session - relevant standards

- BioAPI
- Interchange formats
- Biometric performance
- Sample quality
- Presentation attack detection

Biometric Standardisation

How does standardisation work?

Biometric Standardisation



International Organization for Standardisation

Joint Technical Committee One

International Electrotechnical Commission

International Civil Aviation Organization

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

European Committee for Standardization

— SC 37 Formal Liaisons

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 meeting: July, 2018

ISO/IEC SC37 Biometrics

Members in SC37

- 29 Participating members (P-member):
  - Australia, Canada, China, Czech Republic, Denmark, Egypt, Finland, France, Germany, India, Israel, Italy, Japan, Republic of Korea, Malaysia, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Ukraine, United Kingdom, United States of America.

- 13 Observing members (O-member):
  - Austria, Belgium, Bosnia and Herzegovina, Ghana, Hungary, Indonesia, Islamic Republic of Iran, Ireland, Kenya, Romania, Serbia, Thailand, Turkey

Working Group 1

Title: Harmonized Biometric Vocabulary

- Convenor: Steve Clarke (Australia)

Terms of Reference:

- Create a document of terms and definitions to be used throughout SC37 International Standards.
- Define a process for accepting or developing terms and definitions based on appropriate ISO/IEC standards.
- Identify sources of terms and definitions for possible use in an SC37 vocabulary
- Minimize ambiguity in terms and definitions in SC37 Standards arising from differences in cultures.

“*Getting the language harmonized and correct*”

Working Group 2

Title: Biometric Technical Interfaces

- Convenor: Young Bin Kwon (Korea)

Terms of Reference:

- To consider the standardization of all necessary interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems. To consider the need for a reference model for the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their application.

"*Getting equipment to talk together*"

Working Group 3

Title: Biometric Data Interchange

- Convenor: Christoph Busch (Germany)

Terms of Reference:

- To consider the standardisation of the content, meaning, and representation of biometric data formats which are specific to a particular biometric technology. To ensure a common look and feel for Biometric Data Structure standards, with notation and transfer formats that provide platform independence and separation of transfer syntax from content definition

“Getting equipment to understand each other”

Working Group 4

Title: Technical Implementation of Biometric Systems

- Convenor: Michael Hogan (U.S.)

Terms of Reference:

- Develop technical best practices, guidance, implementation requirements and biometric profiles that support the successful use and interoperability of biometric applications

"*Making it fit the purpose*"

Working Group 5

Title: Biometric Testing and Reporting

- Convenor: Nigel Gordon (UK)

Terms of Reference:

- To create testing and reporting methodologies and metrics that cover biometric technologies, systems and components
- To develop Working Drafts for approved projects on biometric testing and reporting.

“*how to check it works*”

Working Group 6

Title: Cross-Jurisdictional and Societal Aspects

- Convenor: Mario Savastano (Italy)

Terms of Reference:

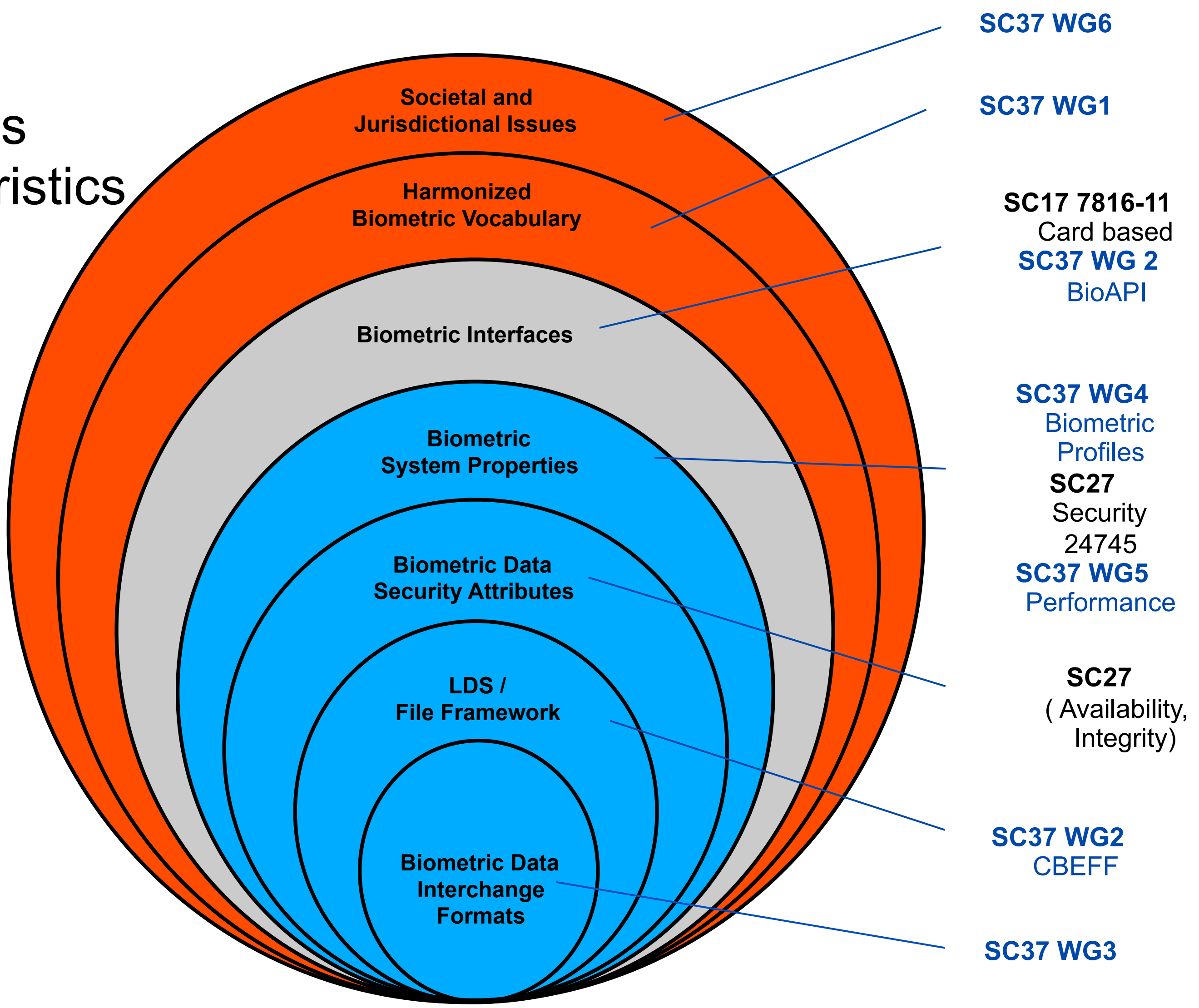
- Within this context, the terms of reference include the support of design and implementation of biometric technologies with respect to: accessibility, health and safety, support of legal requirements and acknowledgement of cross-jurisdictional and societal considerations pertaining to personal information.

"*making it acceptable*"

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


Societal and Jurisdictional Issues
Harmonized Biometric Vocabulary
Biometric Interfaces
Biometric System Properties
Biometric Data Security Attributes
LDS / File Framework
Biometric Data Interchange Formats
SC37 WG6
SC37 WG1
SC17 7816-11
Card based
SC37 WG 2
BioAPI
SC37 WG4
Biometric Profiles
SC27
Security
24745
SC37 WG5
Performance
SC27
(Availability, Integrity)
SC37 WG2
CBEFF
SC37 WG3

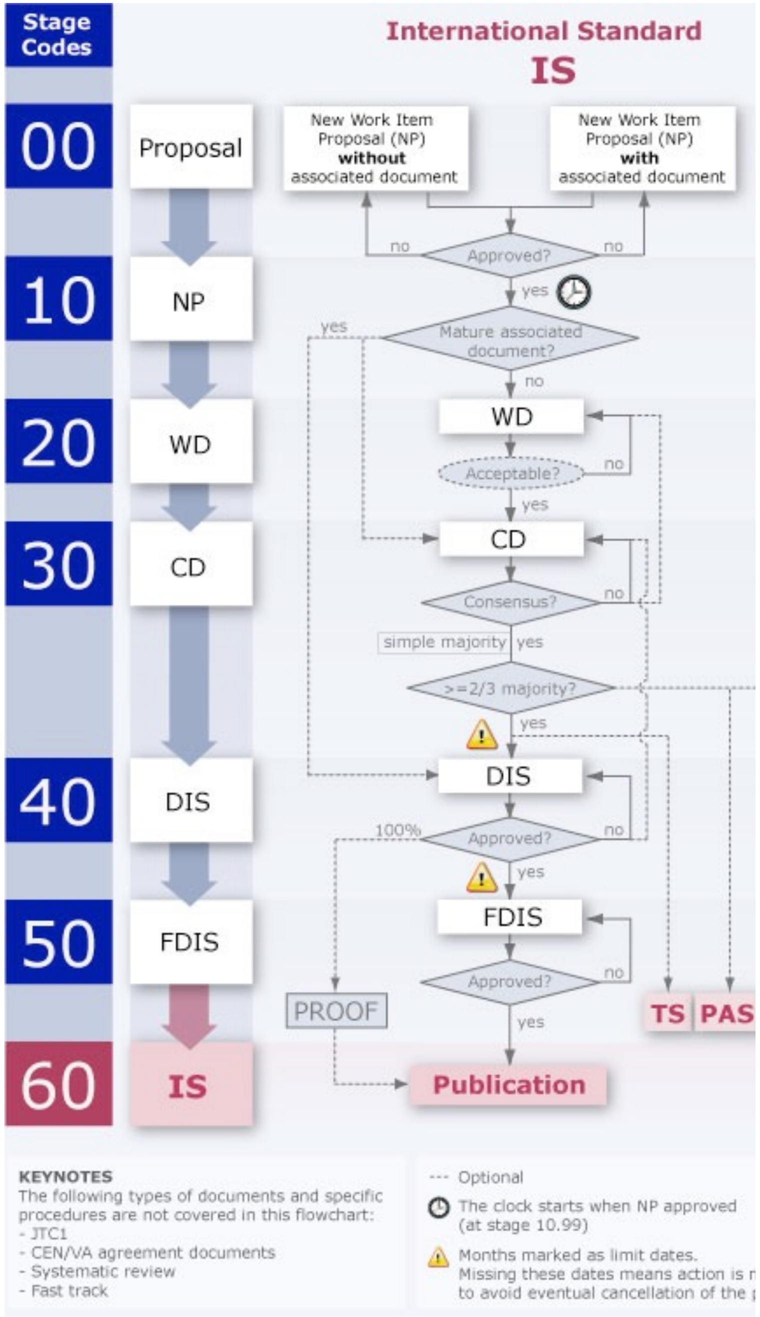
Levels of Development - Standards

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



KEYNOTES
The following types of documents and specific procedures are not covered in this flowchart:
- JTC1
- CEN/VA agreement documents
- Systematic review
- Fast track

--- Optional

The clock starts when NP approved (at stage 10.99)

Months marked as limit dates. Missing these dates means action is r
to avoid eventual cancellation of the p

Expressions in International Standards

In order to make clear what the user must do,

the following verbal forms are used in standards:

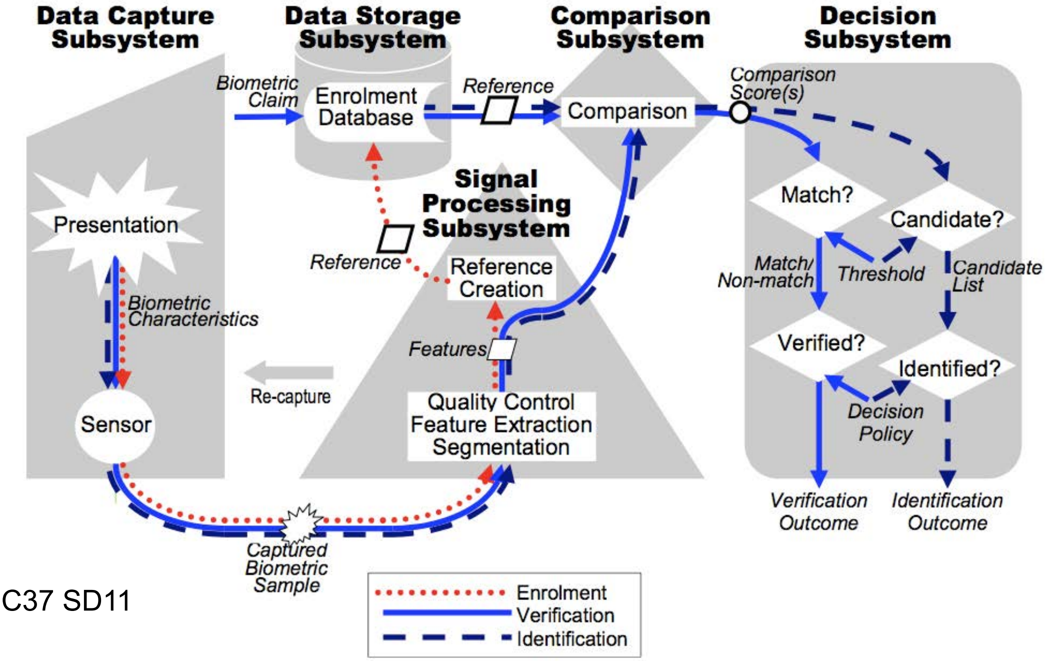
- Requirements – shall, shall not
- Recommendations – should, should not
- Permission – may, need not
- Possibility and capability – can, cannot

Biometric Application Programming Interface

Application Programming Interface - API

Biometric systems maintenance requires

- flexibility (plug-in of components)
- avoiding vendor lock-in,
  - rather allow transparency and exchangeability
- supports scalability and expandable platform
- upgrade partial components (sensors, algorithms) with little/no impact on the entire system



Source: ISO/IEC JTC1 SC37 SD11

Application Programming Interface - API

BioAPI (Biometric API)

- supports biometric enrolment and recognition
- defines interfaces between subsystems that enables software or sensors from multiple vendors to be integrated
- communication between (sub-) systems using the Biometric Interworking Protocol (BIP)
- support for applications, which observe multiple biometric characteristics (for example fingerprint, iris, and face)

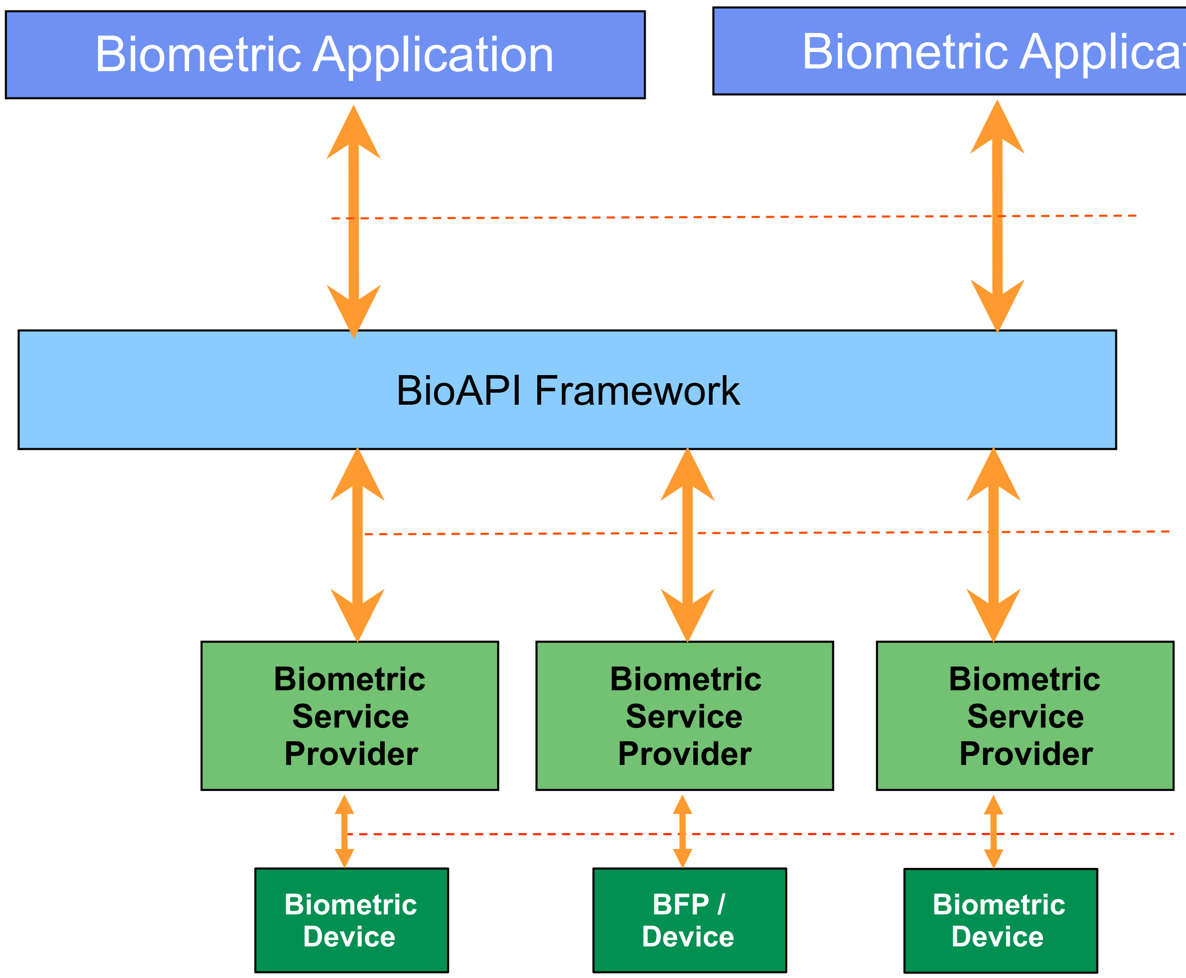
ISO/IEC 19784-1: BioAPI specification, 2006

  - Framework architecture and interfaces
  - High-level C programming language specifications
  - currently in revision process

- also standards for embedded BioAPI and object oriented BioAPI (Java, C#)

BioAPI Application

Elements of a BioAPI application



API

SPI - Service Provider Interface:
Standardized biometric
data is embedded in the
CBEFF structure

Biometric Data
Interchange Format
Standards

Biometric Performance Testing and Reporting

Performance Metrics

Probability density Distribution Function (PDF)

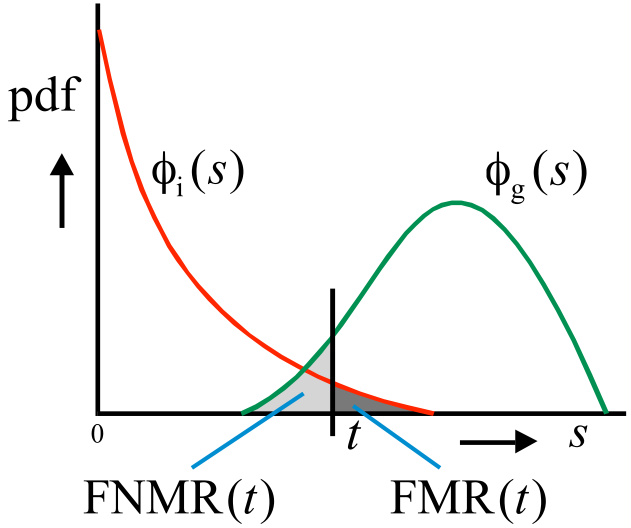
$\Phi_g(s)$: PDF of genuine similarity score $s(Q,R)$

$\Phi_i(s)$: PDF of impostor similarity score $s(Q,R)$

False-Match-Rate (FMR)

- **Def in ISO-HBV:** *proportion of the completed biometric non-mated comparison trials that result in a false match*
- Note: non-mated comparison trials are also referred to as impostor trials

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



Performance Metrics

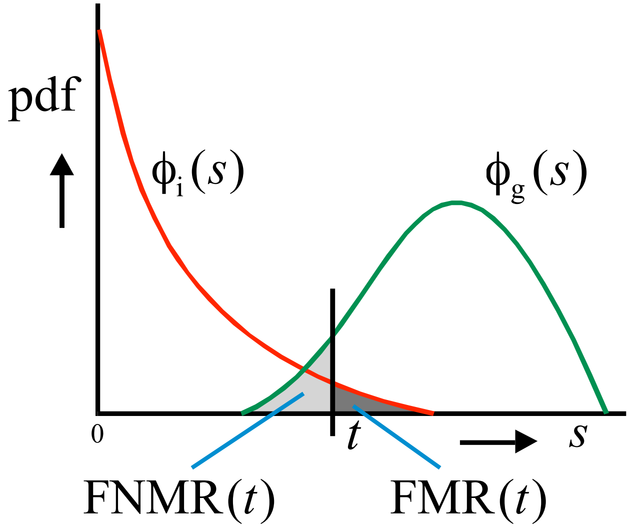
Probability density Distribution Function (PDF)

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

False-Non-Match-Rate (FNMR)

- **Def in ISO-HBV:** *proportion of the completed biometric mated comparison trials that result in a false non-match*
- Note: mated comparison trials are also referred to as genuine trials

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



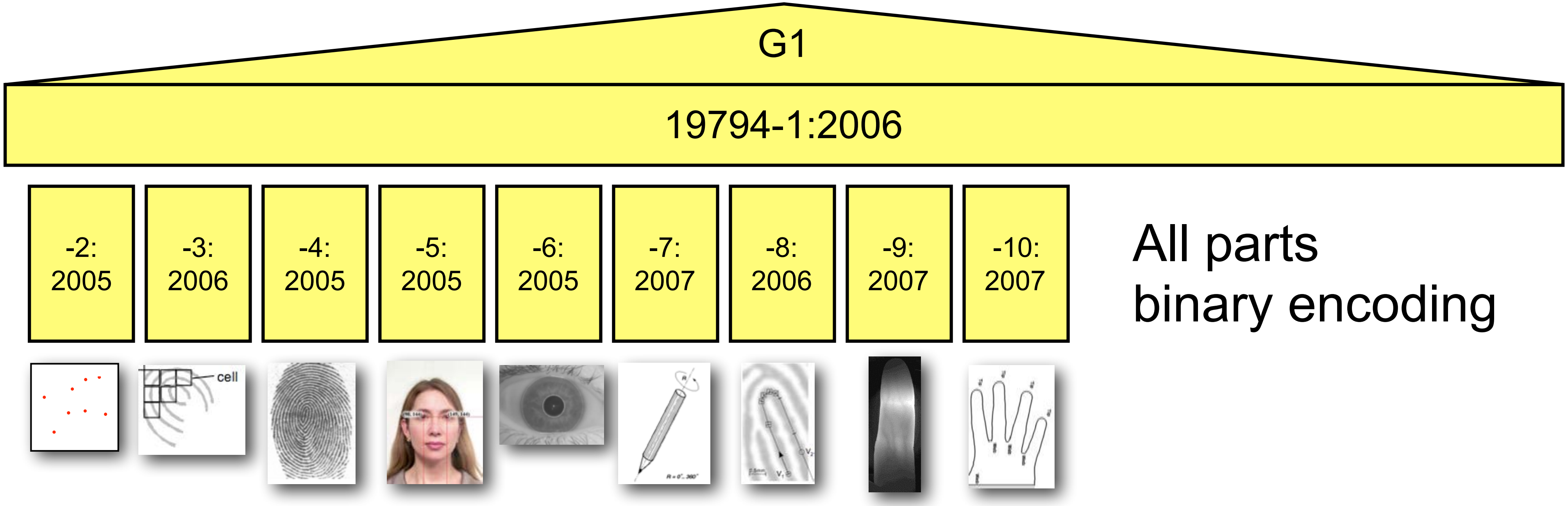
Overview Metrics

From algorithm testing to system level testing

- Technology testing
  - Algorithmic level verification error
    - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ impostor
    - 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

Biometric Data Interchange Formats

First Generation Format Standards



G1

19794-1:2006

-2: 2005

-3: 2006

-4: 2005

-5: 2005

-6: 2005

-7: 2007

-8: 2006

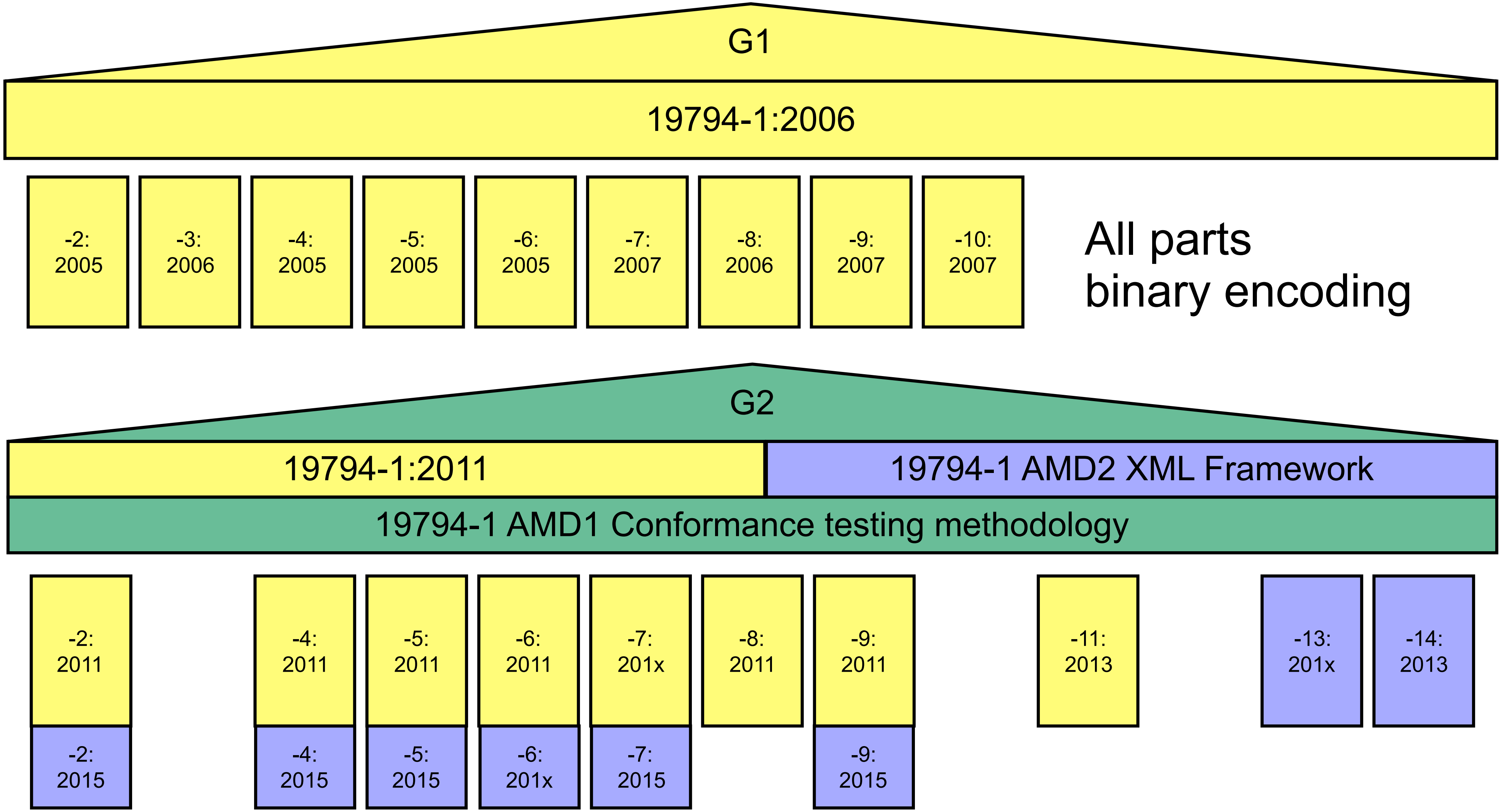
-9: 2007

-10: 2007

All parts
binary encoding

The 19794-Family: Biometric data interchange formats

Generation 2 of ISO/IEC 19794



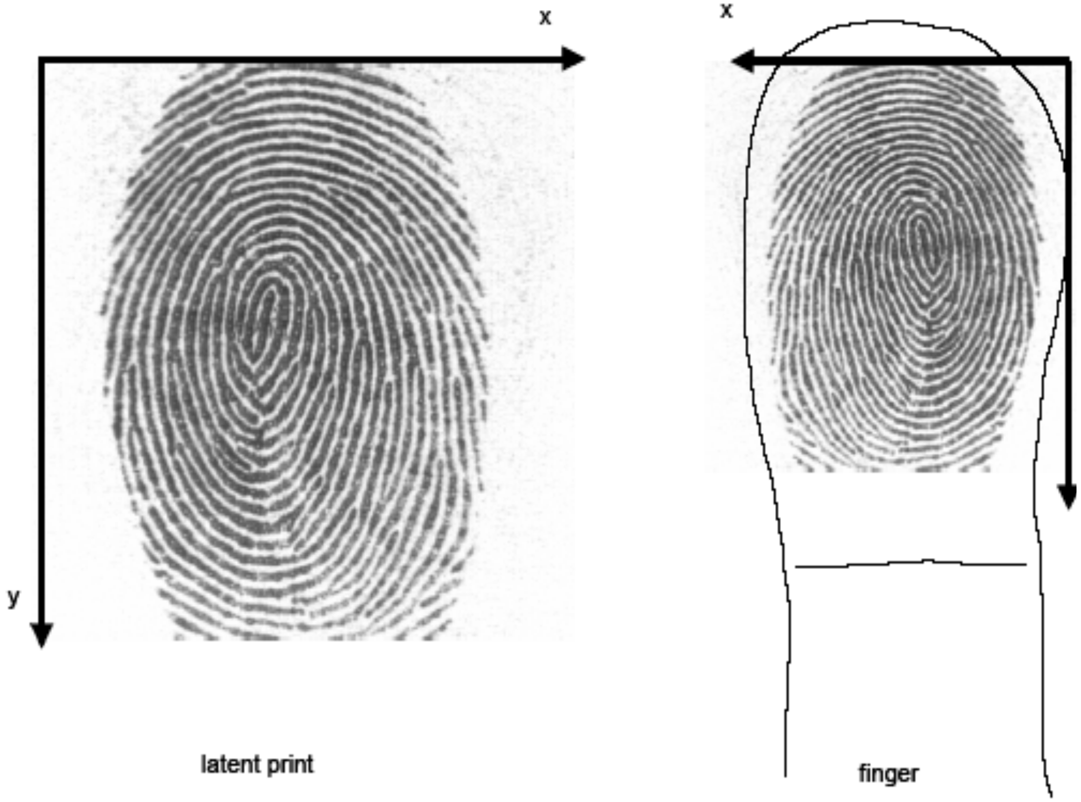
All parts
binary encoding

the semantic is equivalent for binary encoded and XML encoded records

Part 2: Finger minutiae data

ISO/IEC 19794-2:2011

- Ridges and valleys, core and delta
- Ridge bifurcation and ridge endings
  - finger minutiae
- Encoded information
  - Minutia point (coordinates x,y)
  - Minutia direction (angle θ)
- How many finger minutiae, and how many ridges between each pair of them?
- A very mature technology



Source: ISO/IEC 19794-4

Part 2: Finger minutiae data

Further information that is encoded

- Number of finger representations in one record
- Capture device (to identify the equipment and its certification)
- Size of the scanned image (in pixel)
- Horizontal and vertical spatial sampling rate (resolution)
- Finger header: Finger position, Impression type

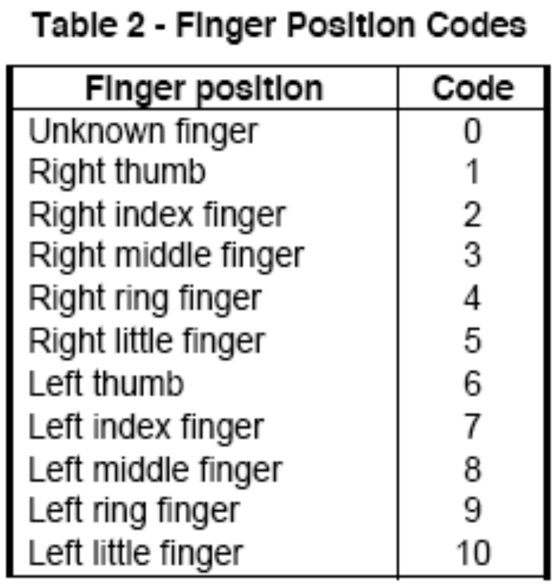


Table 2 - Finger Position Codes

Finger position	Code
Unknown finger	0
Right thumb	1
Right index finger	2
Right middle finger	3
Right ring finger	4
Right little finger	5
Left thumb	6
Left index finger	7
Left middle finger	8
Left ring finger	9
Left little finger	10

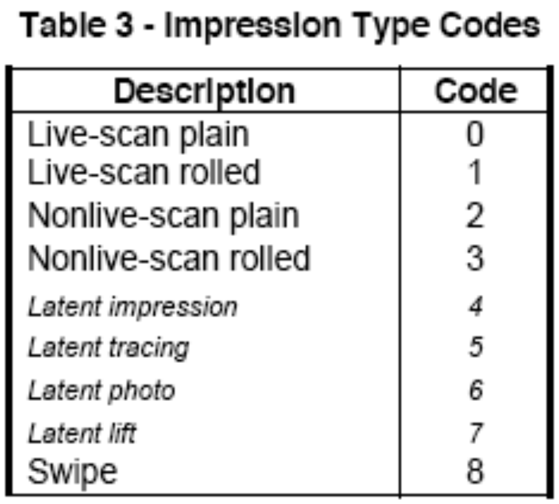


Table 3 - Impression Type Codes

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3
Latent impression	*4*
Latent tracing	*5*
Latent photo	*6*
Latent lift	*7*
Swipe	8

Source: ISO/IEC 19794-4

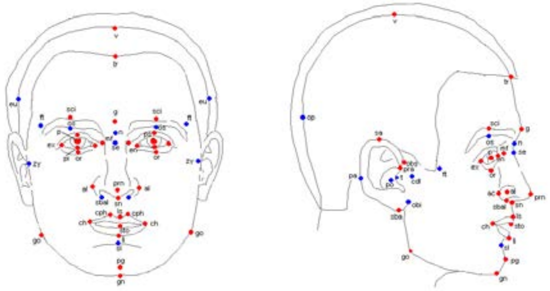
Part 4: Finger image data

ISO/IEC 19794-4:2011

- This part specifies image based encoding of one or more finger images or palm image areas
- Maximum retention of information from the biometric source
- Highest level of interoperability
  - No dependability on the comparison algorithm
- The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information
- Encoded information
  - Images (JPEG, JPEG2000, WSQ)
- This format is in use in EU-passports

Part 5: Face image data

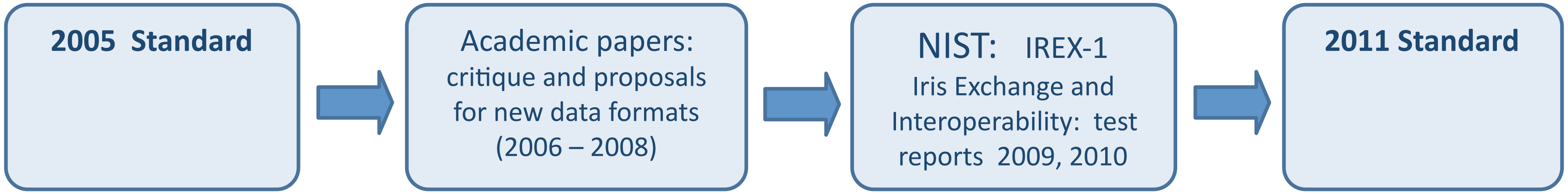
ISO/IEC 19794-5:2011



- Extended over 19794-5:2005 as integrated with
  - 3D Face Image Data Interchange Format
  - Conditions for taking photographs for face image data
- Specific in G2
  - for records from video sequences
  - for biometric records at higher spatial sampling rate levels
  - for specification of post acquisition steps
    - cropping, down-sampling, in-plan rotation, adjusting white balance not requiring new image types vs.
    - interpolation, pose correction, age processing etc. requiring a new “post-processed” image type
    - Support for lossless compression (PNG, JPEG 2000 lossless)

Part 6: Iris image data

ISO/IEC 19794-6:2011



2005 Standard

Academic papers: critique and proposals for new data formats (2006 – 2008)

NIST: IREX-1
Iris Exchange and Interoperability: test reports 2009, 2010

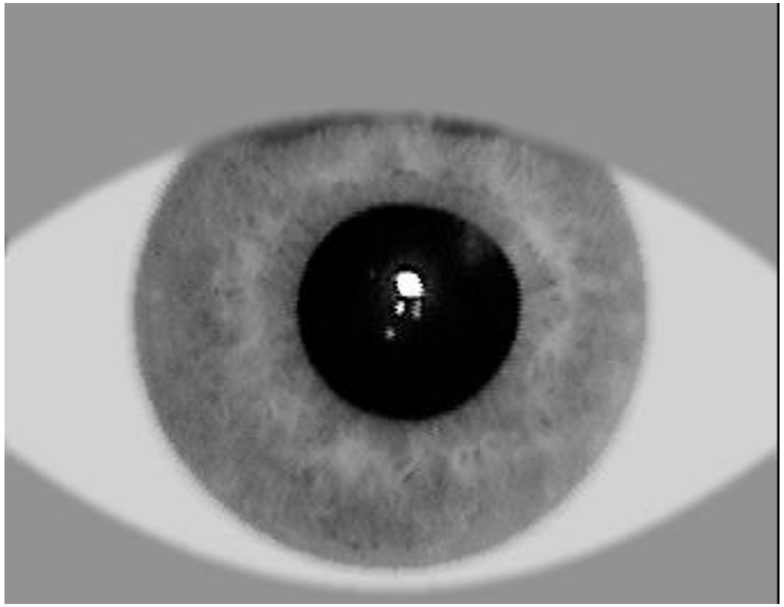
2011 Standard

- 4 new iris image formats, compressible to as little as 2,000 bytes
- Iris formats are now highly empirically based, thanks to NIST IREX testing results
- Recommended target record sizes for different applications
- Recommended compression for different applications
- Formats differ in their required amount of image pre-processing
- Original 19794-6:2005 raw image format retained as one case

Part 6: Iris image data

One new data format in 19794-6:2011

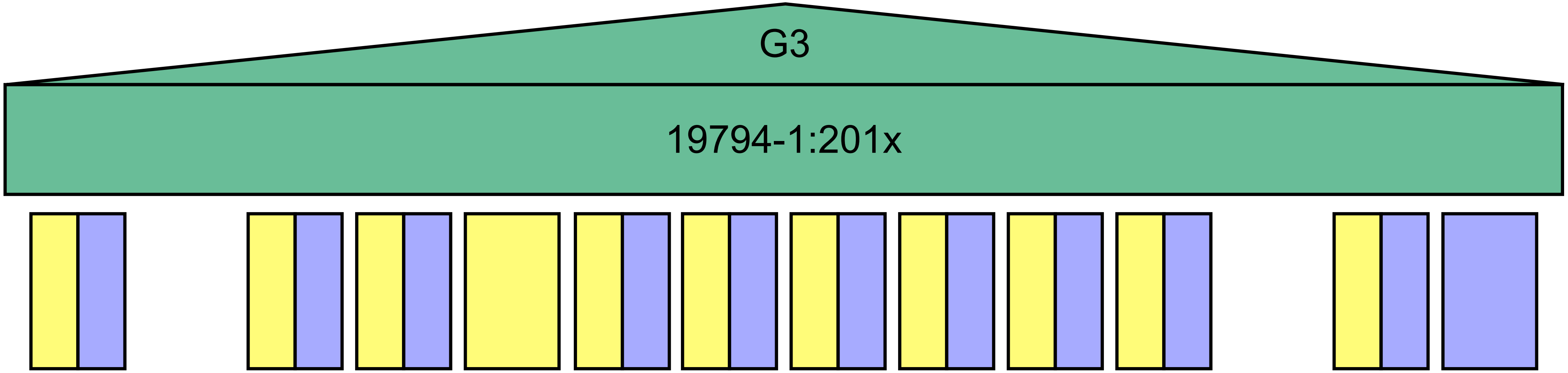
- highly compact iris image, compressed to 2,000 bytes



Source: ISO/IEC 19794-6

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

WG3 Roadmap



Generation 3:

- The common semantics amongst all parts will continue to form the Framework of Generation 3
- All parts will exist in a ASN.1 encoding - XML and/or binary version with a (revised) harmonized semantic can be derived by translation
- PAD data will be encoded
- Again Conformance testing will be included in Annex A of each part

G3 development

Data Interchange Format

- Reflecting need for distributed systems with XML encoding
- Reflecting need for actionable feedback with quality vectors
- Reflecting need for secure system with PAD encoding

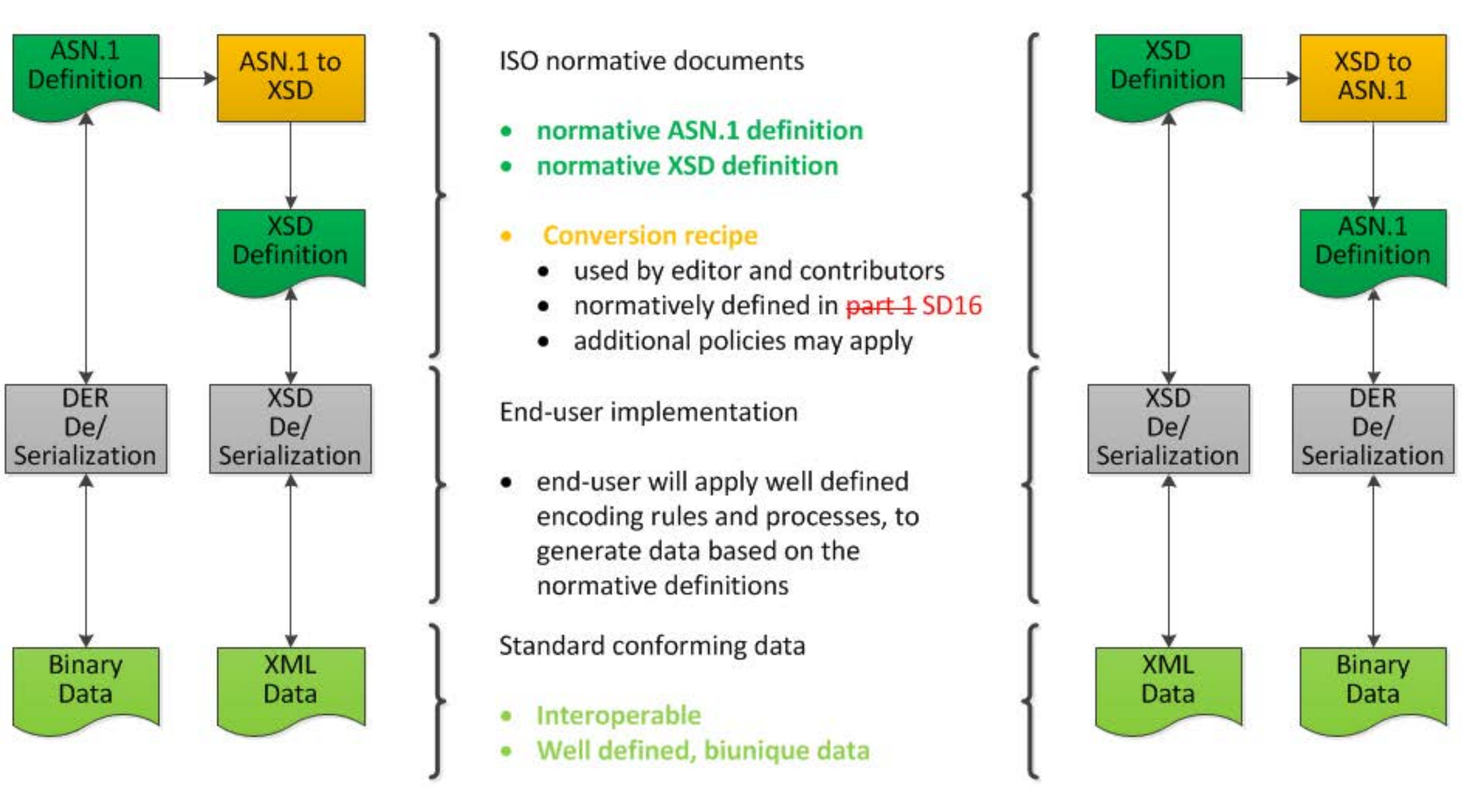
Roadmap

- Definition on transition period from G1 to G2 in ICAO 9393
- Suitable revision cycles for definition in ICAO 9303
- Forward and backwards compatibility
- Transcodability from XML to BIN and vice versa

G3 development

Encoding in Abstract Syntax Notation (ASN.1)

More restricted, but easier/faster approach (recommended)



ISO normative documents

- normative ASN.1 definition
- normative XSD definition

- Conversion recipe
  - used by editor and contributors
  - normatively defined in ~~part 1~~ SD16
  - additional policies may apply

End-user implementation

- end-user will apply well defined encoding rules and processes, to generate data based on the normative definitions

Standard conforming data

- Interoperable
- Well defined, biunique data

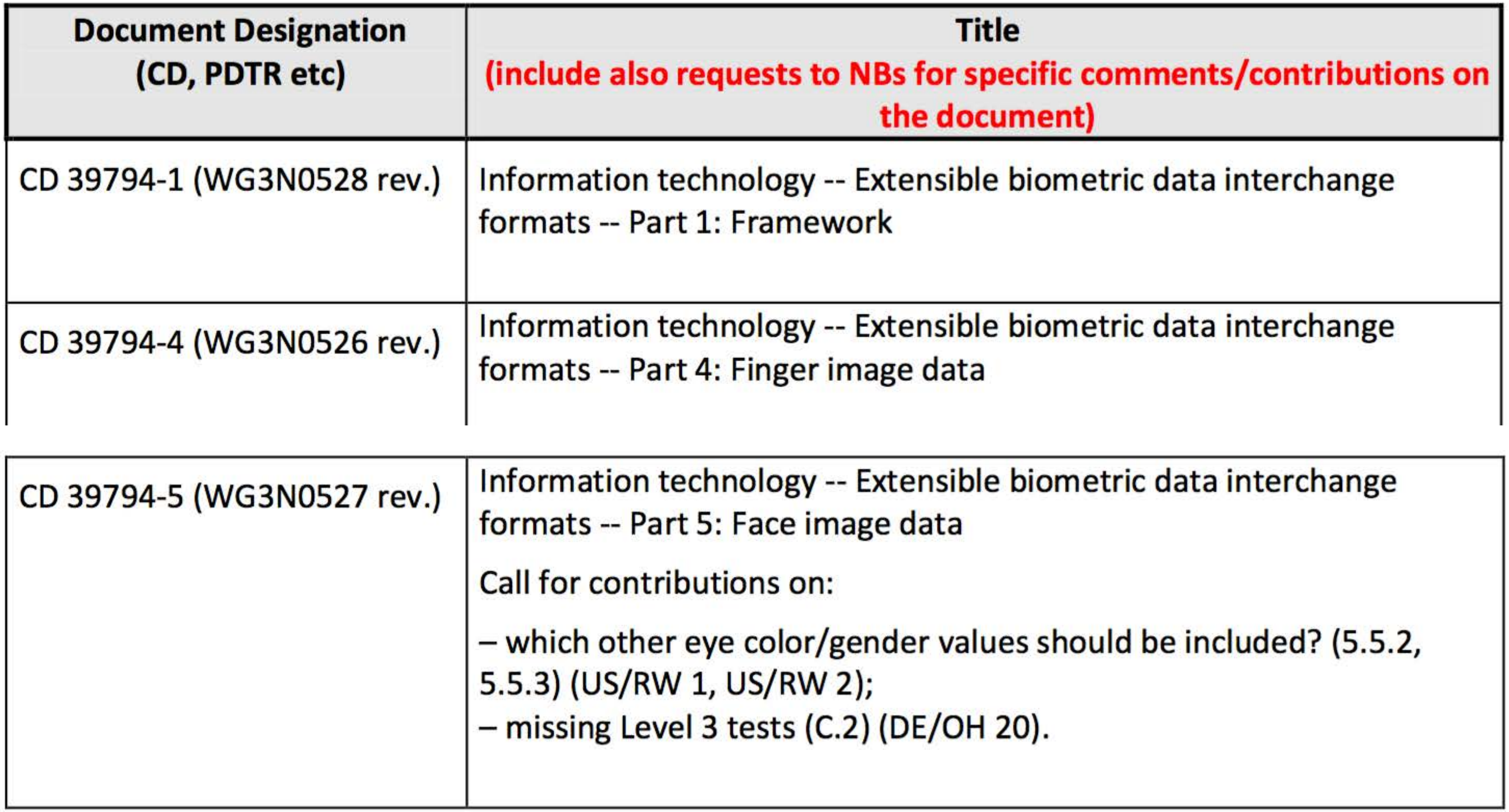
Restrictions and assumptions for simplification

- The following operations will be restricted by the standard
  - The standard does NOT PERMIT the generation of XML data from the ASN.1 definition.
  - The standard does NOT PERMIT the generation of binary data from the XSD definition.
- The binary data and the XML data must be equal in regard to the information content.
- No “round trip conformance test” applicable because of well defined unique encoding pipelines.

Resolutions

CD circulation

resolution 3.6



Document Designation (CD, PDTR etc)	Title **(include also requests to NBs for specific comments/contributions on the document)**
CD 39794-1 (WG3N0528 rev.)	Information technology -- Extensible biometric data interchange formats -- Part 1: Framework
CD 39794-4 (WG3N0526 rev.)	Information technology -- Extensible biometric data interchange formats -- Part 4: Finger image data
CD 39794-5 (WG3N0527 rev.)	Information technology -- Extensible biometric data interchange formats -- Part 5: Face image data Call for contributions on: – which other eye color/gender values should be included? (5.5.2, 5.5.3) (US/RW 1, US/RW 2); – missing Level 3 tests (C.2) (DE/OH 20).

ISO/IEC 30137

CCTV in Takamatsu

- Harmonization group operational:
  - multi-camera operation, mapping table
- Part 1, Design and specification (WG 4) - 3rd CD
- Part 2, Performance testing and reporting (WG 5) -2nd C
- Part 3, Data formats (WG 3)- cancelled
- Part 4, Ground truth and video annotation procedure - 2nd WD
  - agnostic on modality (face and gait)
  - not only humans
  - moving multi-camera, body worn camera, re-identification
  - drones

Biometric Sample Quality

Biometric Sample Quality

G2-version completed for

- ISO/IEC 29794 Part 1: framework
- ISO/IEC 29794 Part 6: iris image data
- ISO/IEC 29794 Part 4: finger image data
  - upgrade from TR to IS to incorporate NFIQ2.0 findings see: http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm

Biometric Sample Quality

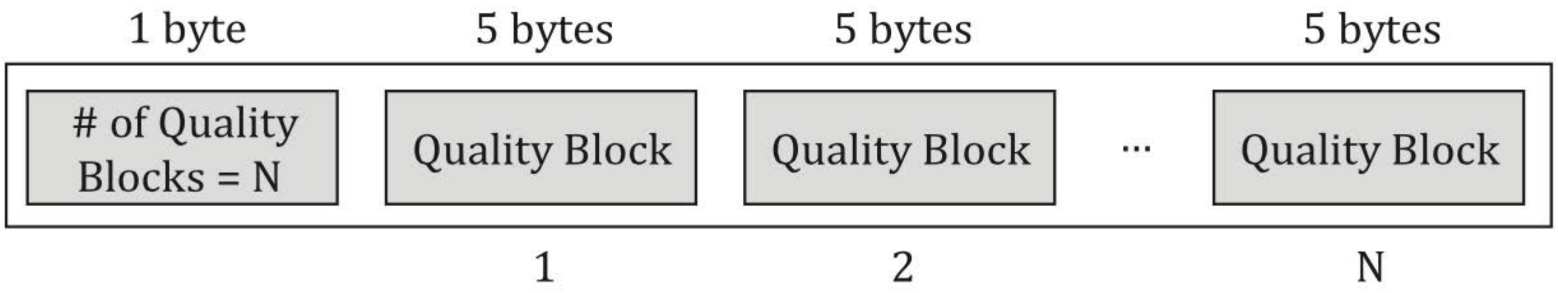
Revision ISO/IEC 29794-1:2016

Definitions

- allow for a vector of quality blocks

Goal:

- Actionable quality
- Each quality score is in the range 0 to 100.



Source: ISO/IEC 29794-1

Biometric Information Protection

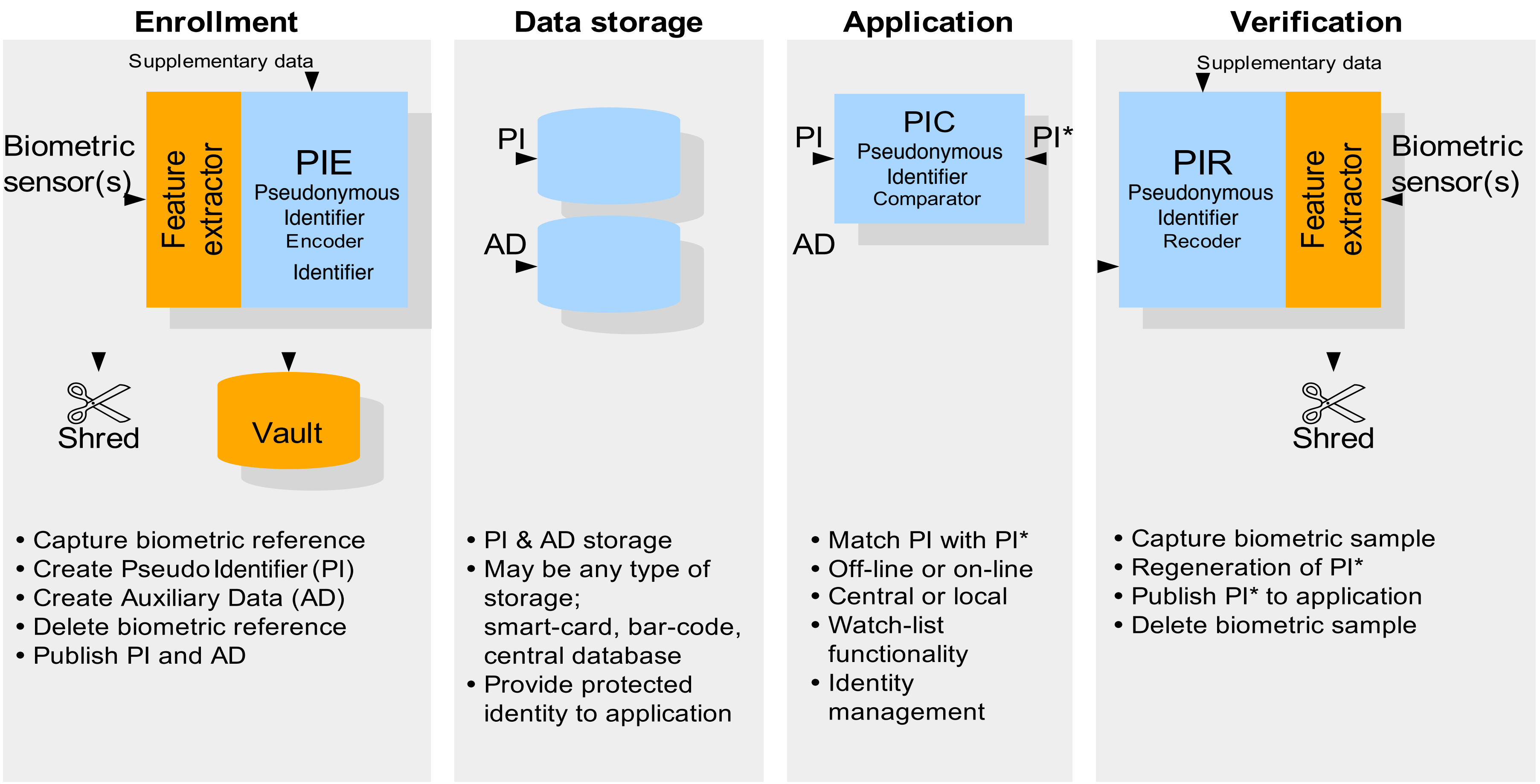
ISO/IEC 24745

Privacy Requirements

- Irreversibility
  “biometric data shall be processed by irreversible transforms before storage”
- Unlinkability
  “the stored biometric references shall not be linkable across applications or databases”.
- Confidentiality
  “data separation by storing (part of the) biometric references on a personal token or card instead of using centralized databases is a countermeasure to reduce privacy risks.”

ISO/IEC 24745

- Architecture for renewable biometric references



Enrollment

- Capture biometric reference
- Create Pseudo Identifier (PI)
- Create Auxiliary Data (AD)
- Delete biometric reference
- Publish PI and AD

Data storage

- PI & AD storage
- May be any type of storage; smart-card, bar-code, central database
- Provide protected identity to application

Application

- Match PI with PI*
- Off-line or on-line
- Central or local
- Watch-list functionality
- Identity management

Verification

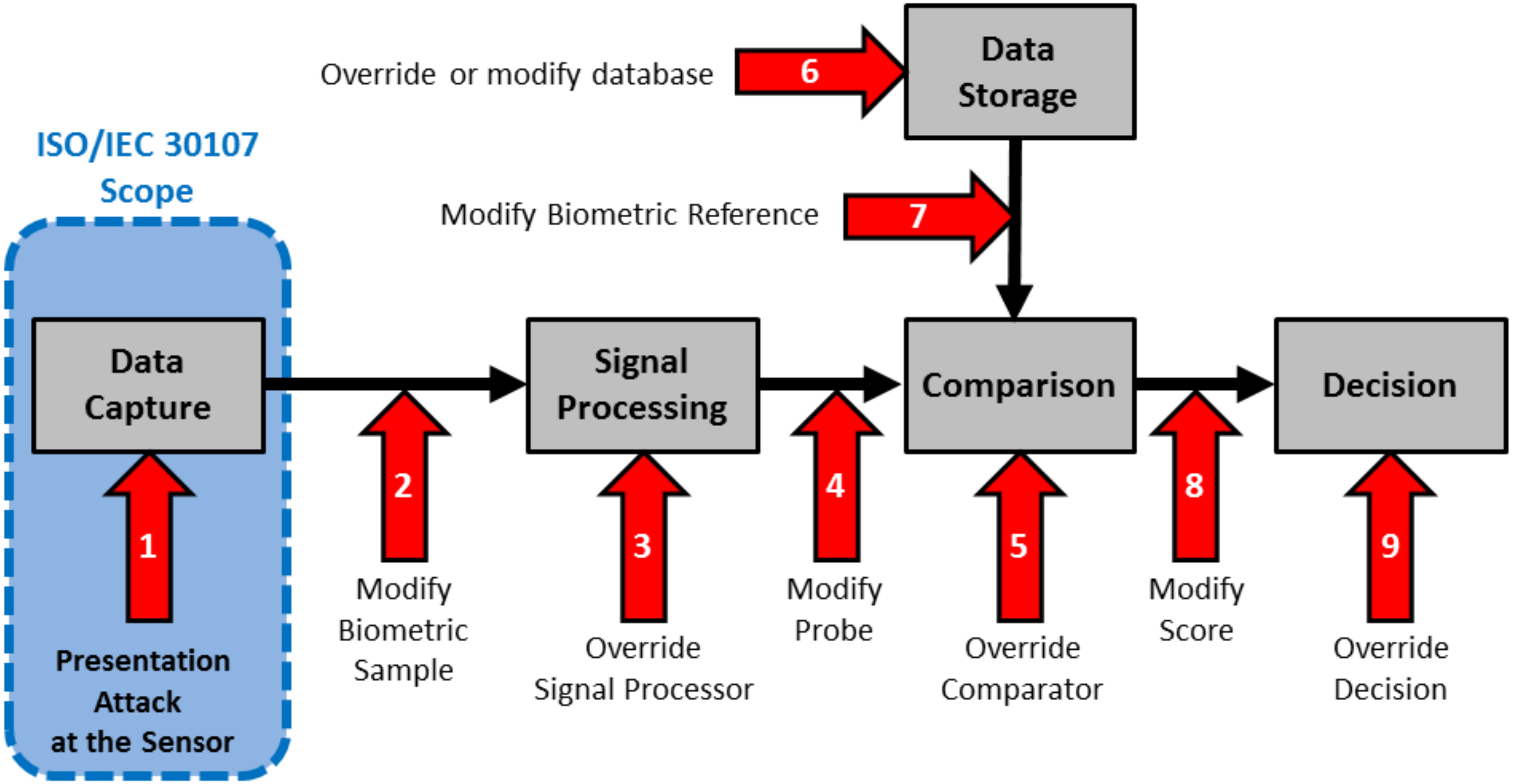
- Capture biometric sample
- Regeneration of PI*
- Publish PI* to application
- Delete biometric sample

Presentation Attack Detection

Liveness Detection

ISO/IEC 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
- a classification of known attacks types (in an informative annex).

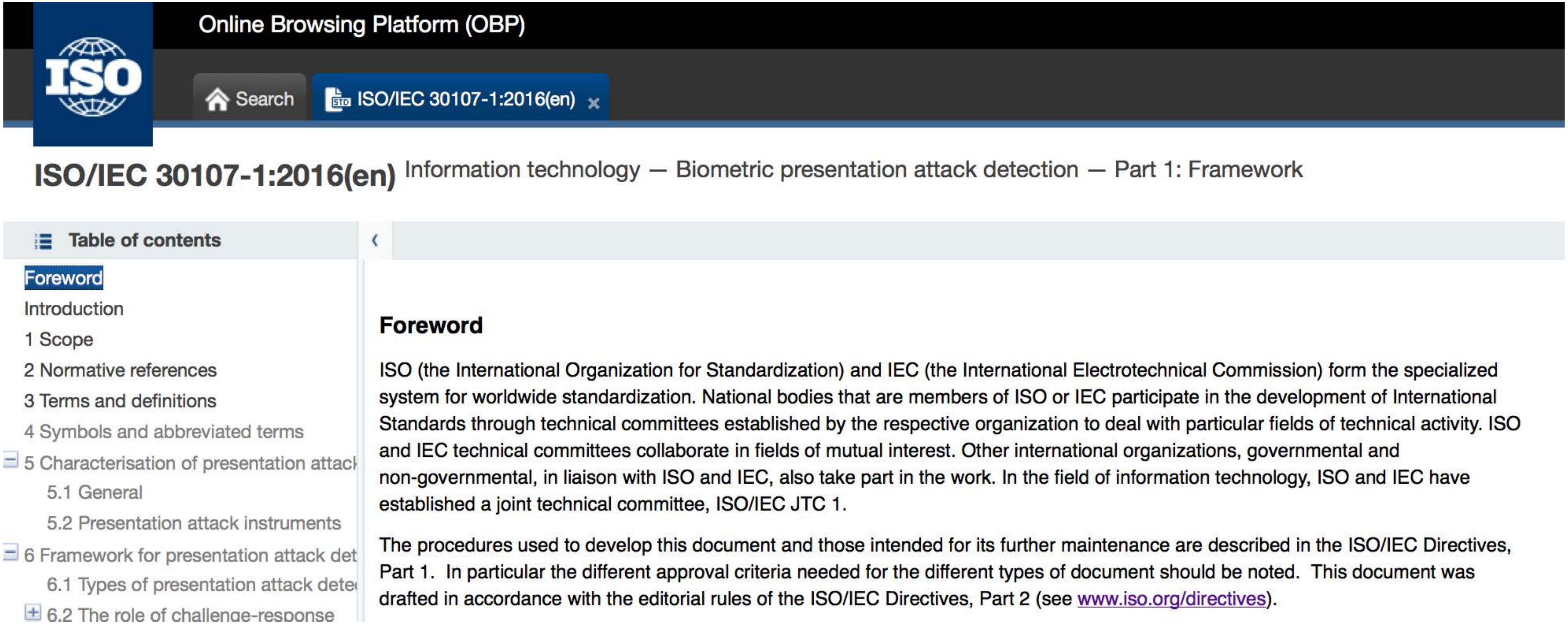
Outside the scope are

- 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 - Framework

ISO/IEC 30107-1

- now freely available in the ISO-Portal
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip



ISO/IEC 30107-1:2016(en) Information technology — Biometric presentation attack detection — Part 1: Framework

Table of contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

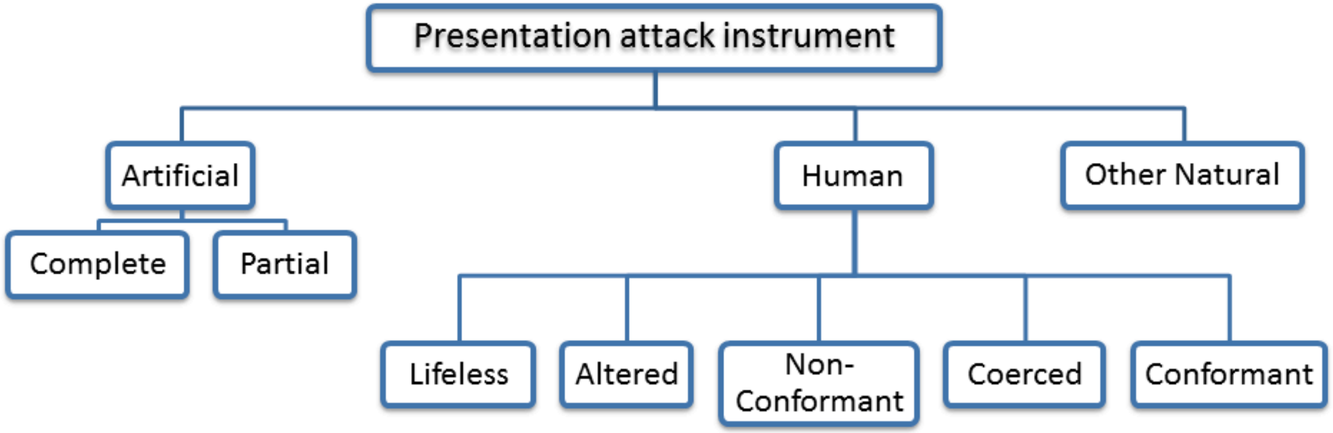
- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection

ISO/IEC 30107-1 - 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



(General Noun)

Presentation attack instrument

(Adjectives describing categories)

Artificial

Human

Other Natural

(Qualifying adjectives)

Complete

Partial

Lifeless

Altered

Non-Conformant

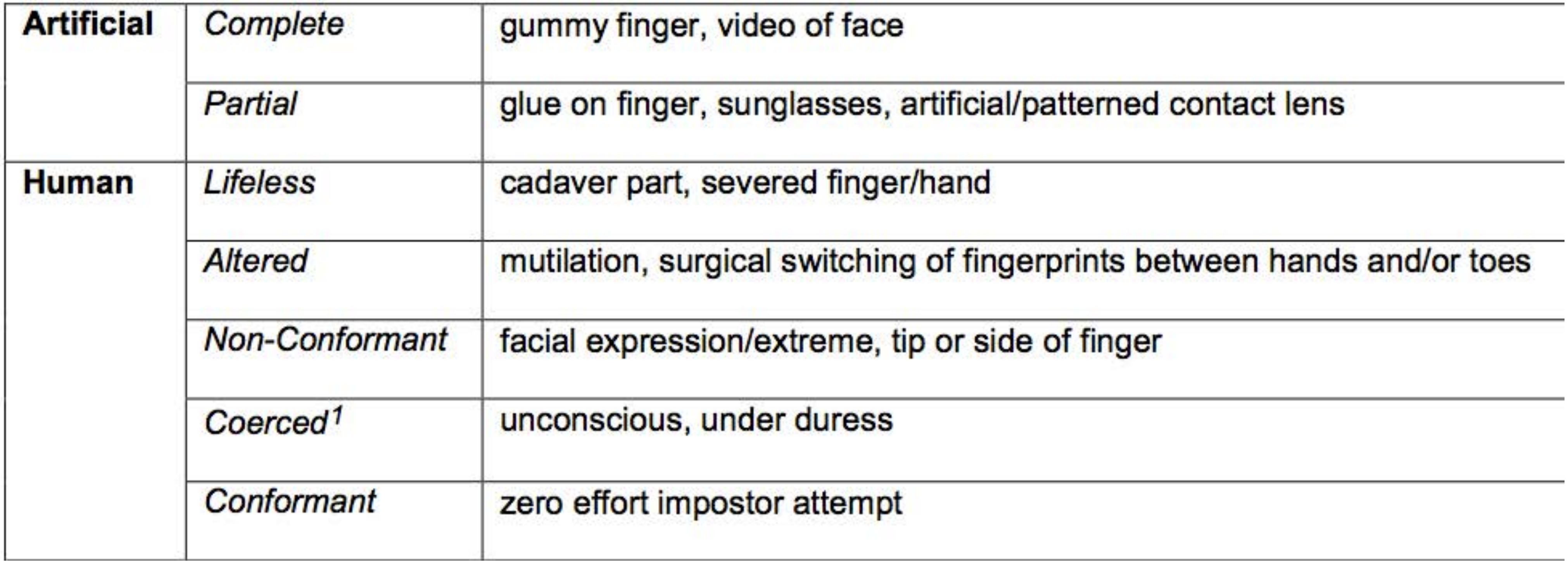
Coerced

Conformant

Source: ISO/IEC 30107-1

Presentation Attack Detection

ISO/IEC 30107-1: Examples of Artificial and Human Presentation Attack Instruments

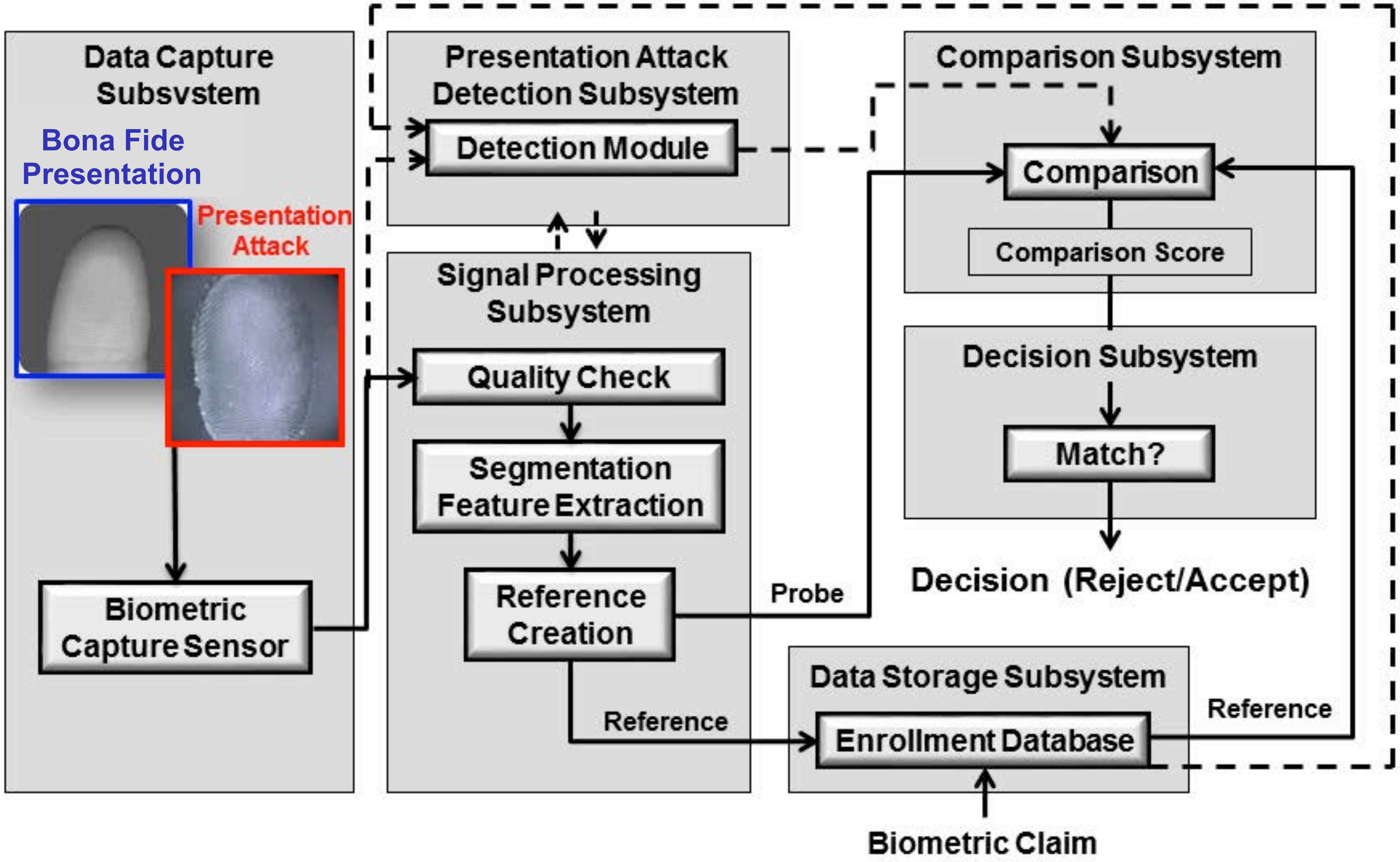


Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens
Human	*Lifeless*	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip or side of finger
	Coerced[1]	unconscious, under duress
	Conformant	zero effort impostor attempt

Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD

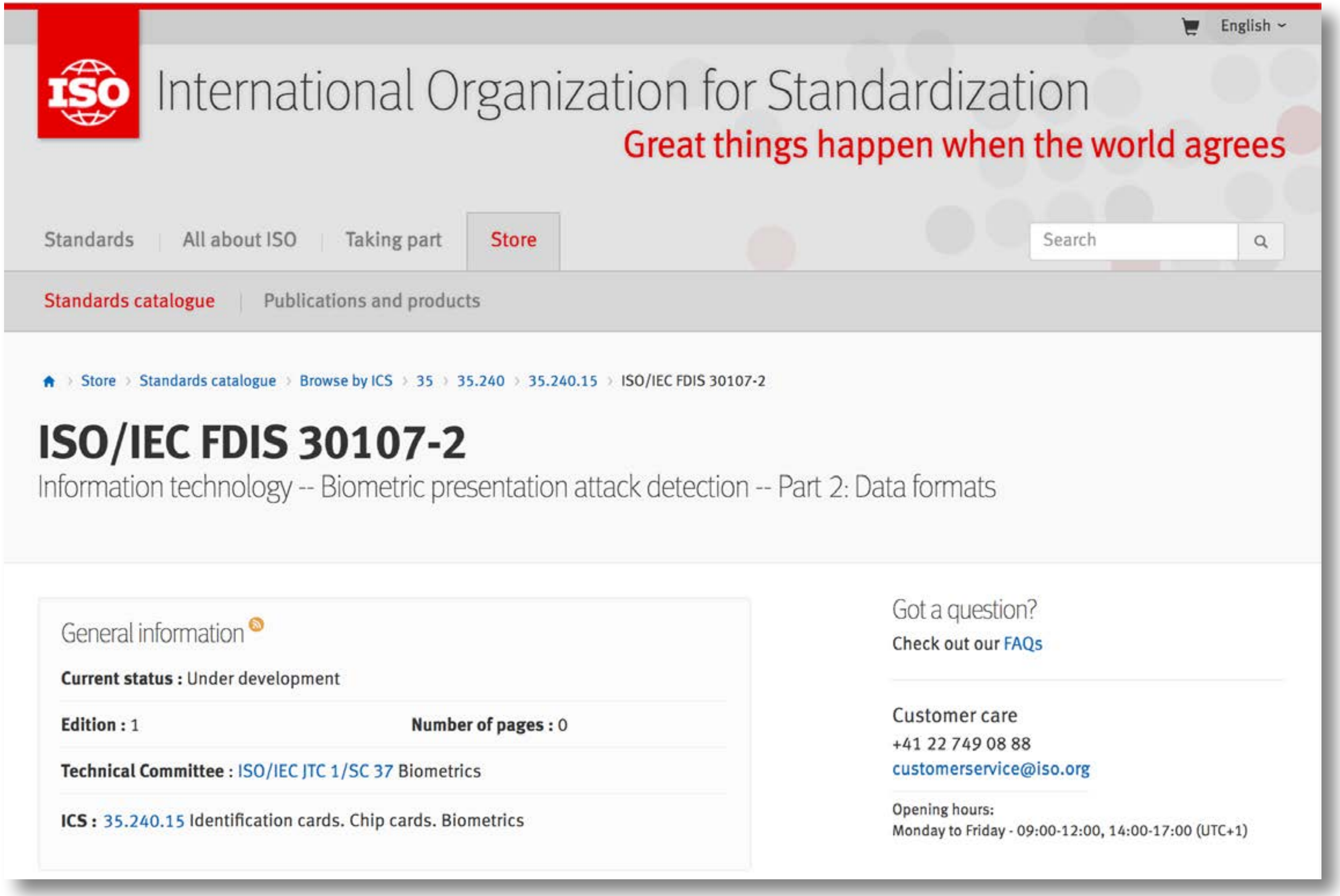


Source: ISO/IEC 30107-1

Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- will soon be available in the ISO/IEC Portal
  https://www.iso.org/standard/67380.html



English
ISO
International Organization for Standardization
Great things happen when the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products

Store › Standards catalogue › Browse by ICS › 35 › 35.240 › 35.240.15 › ISO/IEC FDIS 30107-2

ISO/IEC FDIS 30107-2

Information technology -- Biometric presentation attack detection -- Part 2: Data formats

General information

Current status : Under development

Edition : 1

Number of pages : 0

Technical Committee : ISO/IEC JTC 1/SC 37 Biometrics

ICS : 35.240.15 Identification cards. Chip cards. Biometrics

Got a question?

Check out our FAQs

Customer care

+41 22 749 08 88

customerservice@iso.org

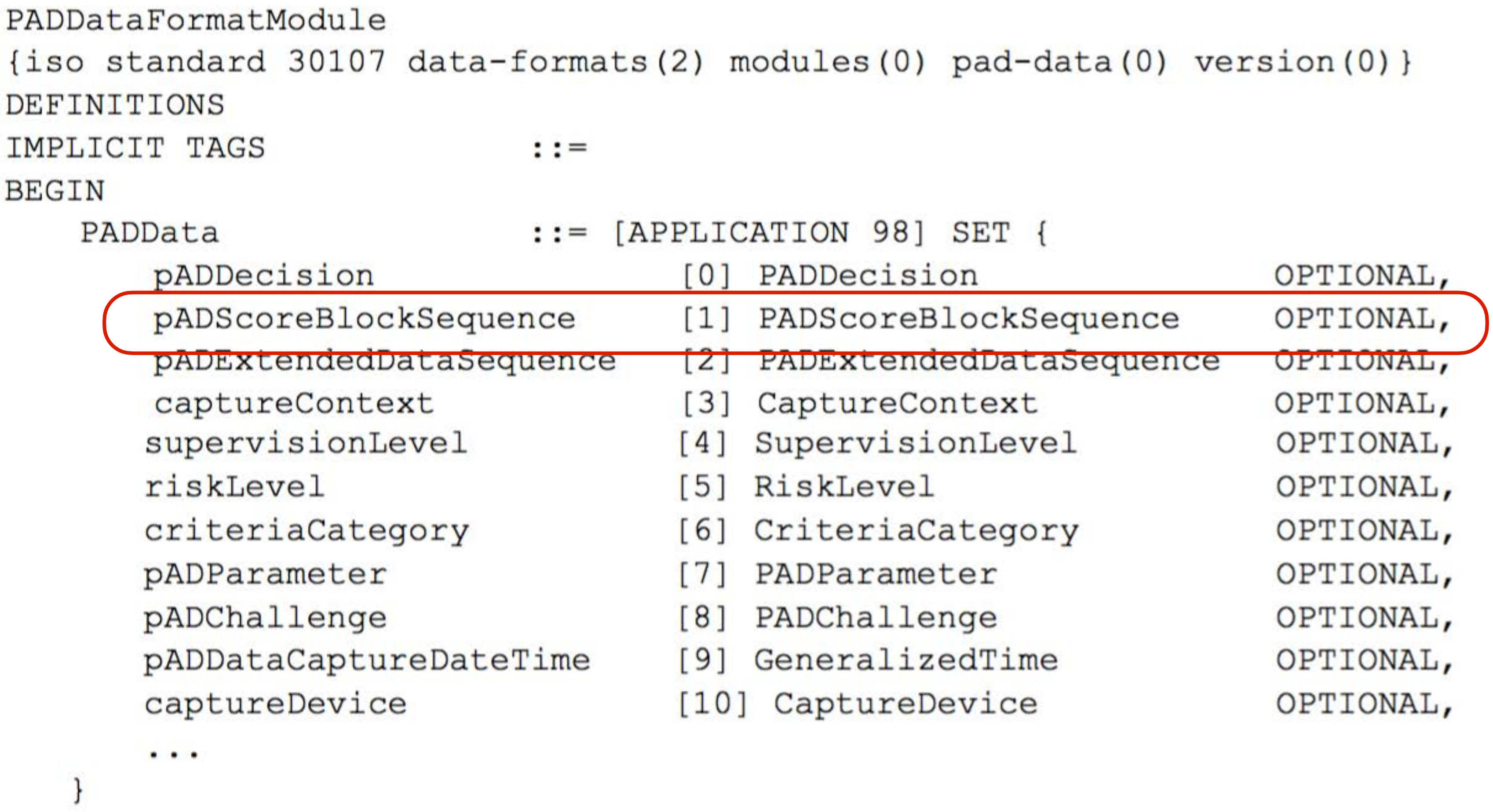
Opening hours:

Monday to Friday - 09:00-12:00, 14:00-17:00 (UTC+1)

Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- Abstract syntax of the PAD information in ASN.1



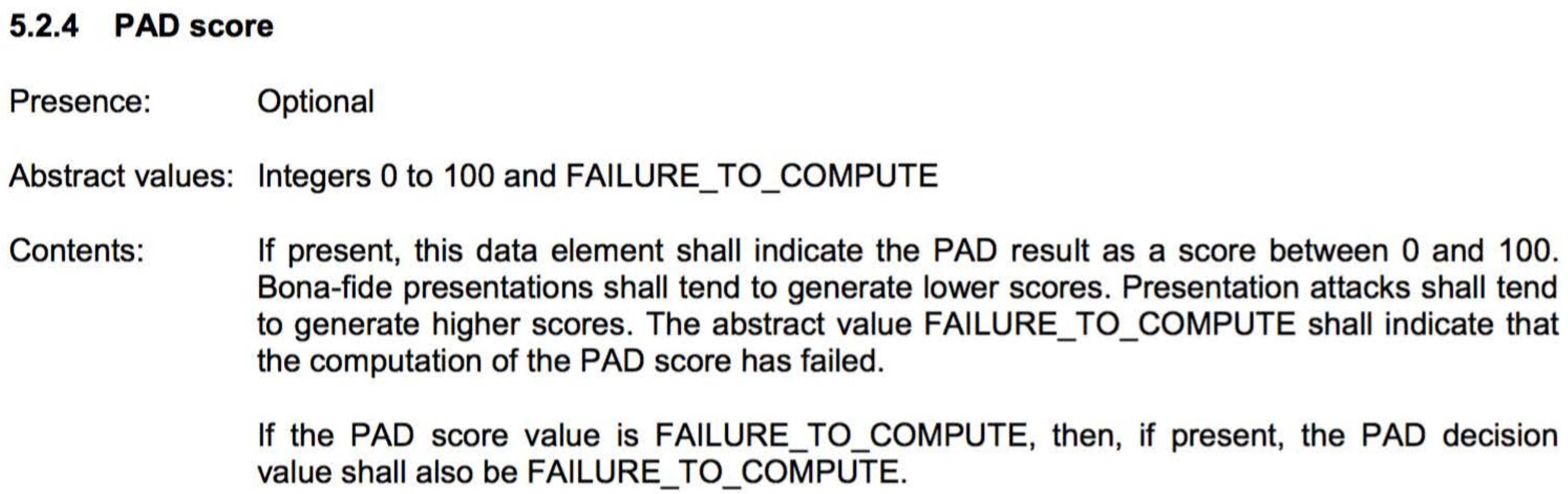
```
PADDataFormatModule
{iso standard 30107 data-formats(2) modules(0) pad-data(0) version(0)}
DEFINITIONS
IMPLICIT TAGS                ::=
BEGIN
    PADData                  ::= [APPLICATION 98] SET {
        pADDecision                    [0] PADDecision              OPTIONAL,
        pADScoreBlockSequence          [1] PADScoreBlockSequence    OPTIONAL,
        pADExtendedDataSequence        [2] PADExtendedDataSequence  OPTIONAL,
        captureContext                 [3] CaptureContext           OPTIONAL,
        supervisionLevel               [4] SupervisionLevel         OPTIONAL,
        riskLevel                      [5] RiskLevel                OPTIONAL,
        criteriaCategory               [6] CriteriaCategory         OPTIONAL,
        pADParameter                   [7] PADParameter             OPTIONAL,
        pADChallenge                   [8] PADChallenge             OPTIONAL,
        pADDataCaptureDateTime         [9] GeneralizedTime          OPTIONAL,
        captureDevice                  [10] CaptureDevice           OPTIONAL,
        ...
    }
```

Source: ISO/IEC 30107-2

Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- PAD score



5.2.4 PAD score

Presence: Optional

Abstract values: Integers 0 to 100 and FAILURE_TO_COMPUTE

Contents: If present, this data element shall indicate the PAD result as a score between 0 and 100. Bona-fide presentations shall tend to generate lower scores. Presentation attacks shall tend to generate higher scores. The abstract value FAILURE_TO_COMPUTE shall indicate that the computation of the PAD score has failed.

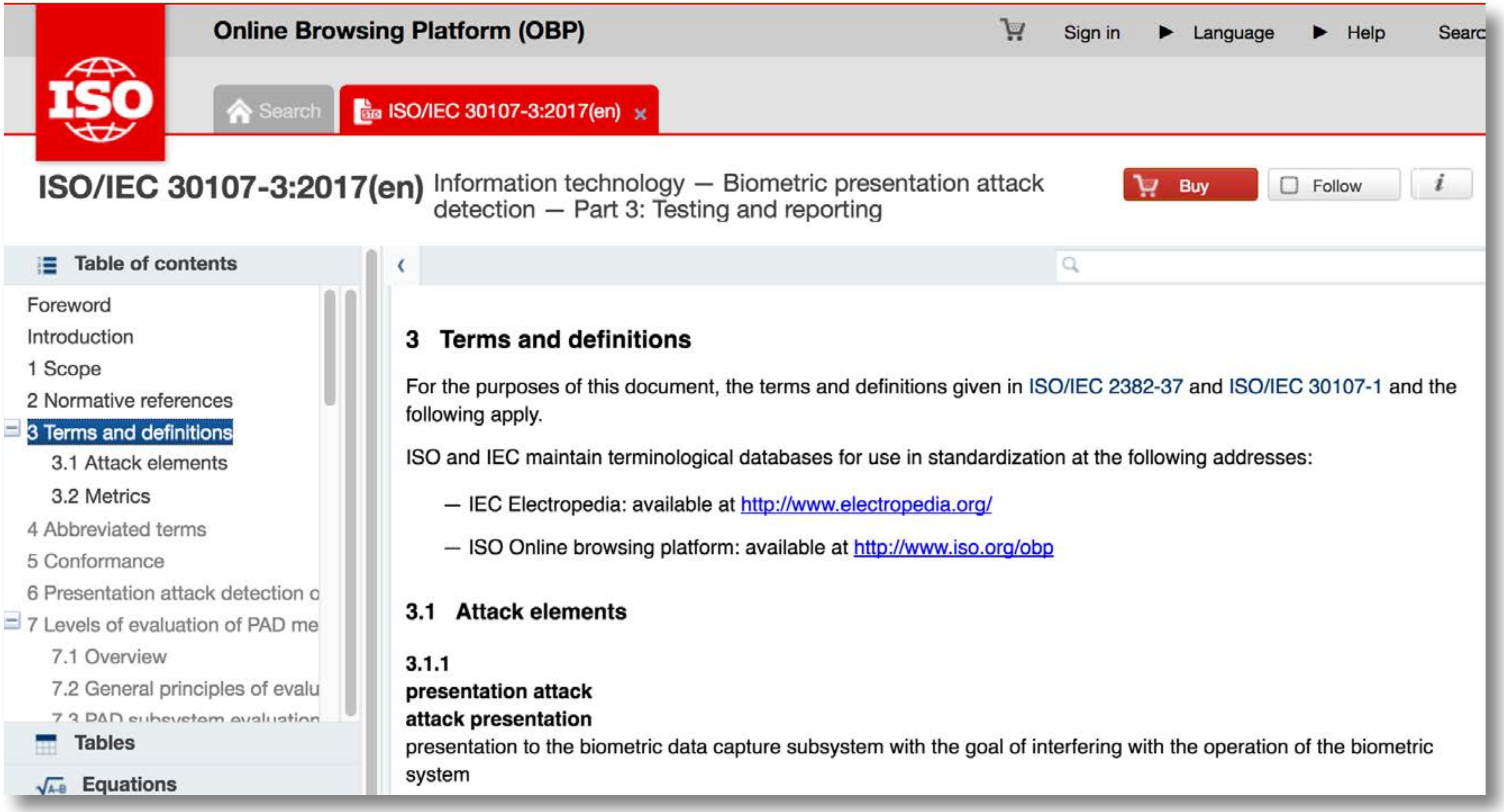
If the PAD score value is FAILURE_TO_COMPUTE, then, if present, the PAD decision value shall also be FAILURE_TO_COMPUTE.

Source: ISO/IEC 30107-2

Presentation Attack Detection - Testing

ISO/IEC 30107-3

- available in the ISO/IEC Portal
  https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en



ISO/IEC 30107-3:2017(en) Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 30107-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Attack elements

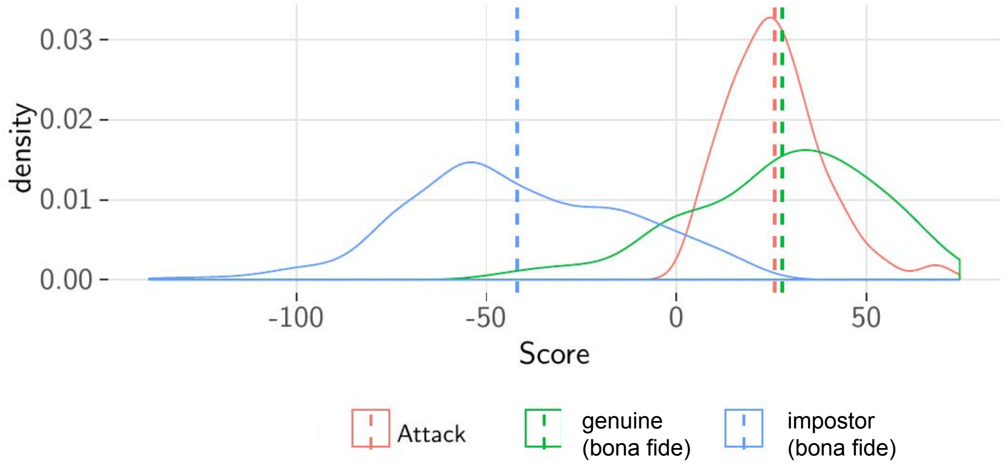
3.1.1
presentation attack
attack presentation
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Presentation Attack Detection - Testing

Definition of full system vulnerability metric w.r.t attacks

- **Impostor attack presentation match rate (IAPMR)**
  <in a full-system evaluation of a verification system> the proportion of impostor attack presentation using the same PAI species in which the target reference is matched

Source: ISO/IEC 30107-3



- **Concealer attack presentation non-match rate (CAPNMR)**
  in a full-system evaluation of a verification system, the proportion of concealer attack presentations using the same PAI species in which the target reference is not matched.

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative and false-positive errors:

- **Attack presentation classification error rate (APCER)** *proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario*

- **Bona fide presentation classification error rate (BPCER)** *proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario*

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics elements

- **PAI species**
  class of presentation attack instruments created using a common production method and based on different biometric characteristic
- **Attack potential**
  measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation
- **target of evaluation (TOE)**
  within Common Criteria, the IT product that is the subject of the evaluation

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative errors:

- **Attack presentation classification error rate (APCER)** *proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario*

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right)\sum_{i=1}^{N_{PAIS}} Res_{i}$$

Source: ISO/IEC 30107-3

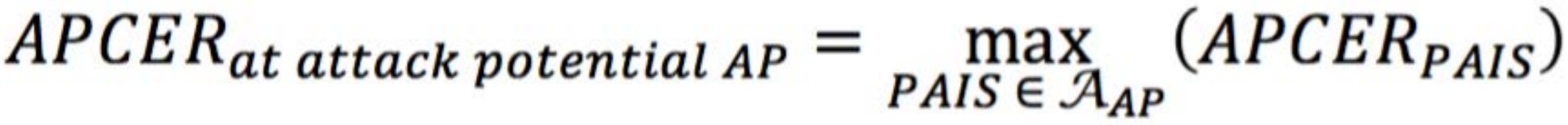
- *N_{PAIS} is the number of attack presentations for the given PAI species*
- *Res_i takes value 1 if the i^{th} presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

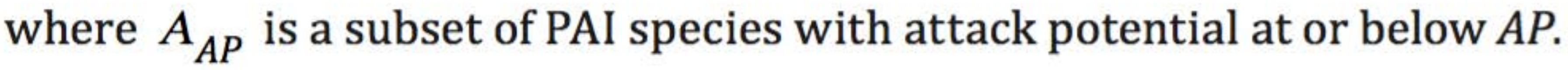
- Testing the PAD subsystem with false-negative errors:

- **Attack presentation classification error rate (APCER)**
  the highest APCER (i.e. that of the most successful PAI) should be used as follows:



$$APCER_{at\ attack\ potential\ AP} = \max_{PAIS \in \mathcal{A}_{AP}} (APCER_{PAIS})$$

Source: ISO/IEC 30107-3



where A_{AP} is a subset of PAI species with attack potential at or below AP.

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-positive errors:

- **Bona fide presentation classification error rate (BPCER)**
  BPCER shall be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} RES_i}{N_{BF}}$$

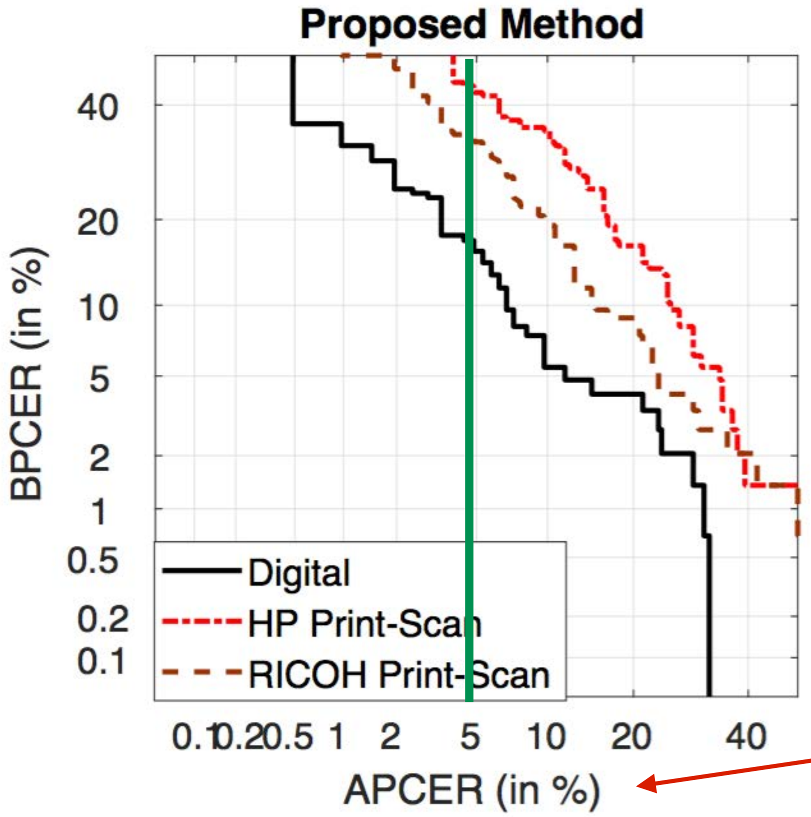
Source: ISO/IEC 30107-3

- *N_{BF} is the number of bona fide presentations*
- *Res_i takes value 1 if the ith presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- DET curve analyzing operating points for various security measures and convenience measures
- Example:



convenience measure

security measure (strength of function)

Source: R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing a specific security level:

  PAD mechanism may be reported in a single figure

- *BPCER at a fixed APCER:*

  One may report BPCER when $APCER_{AP}$ is 5% as BPCER20

Source: ISO/IEC 30107-3

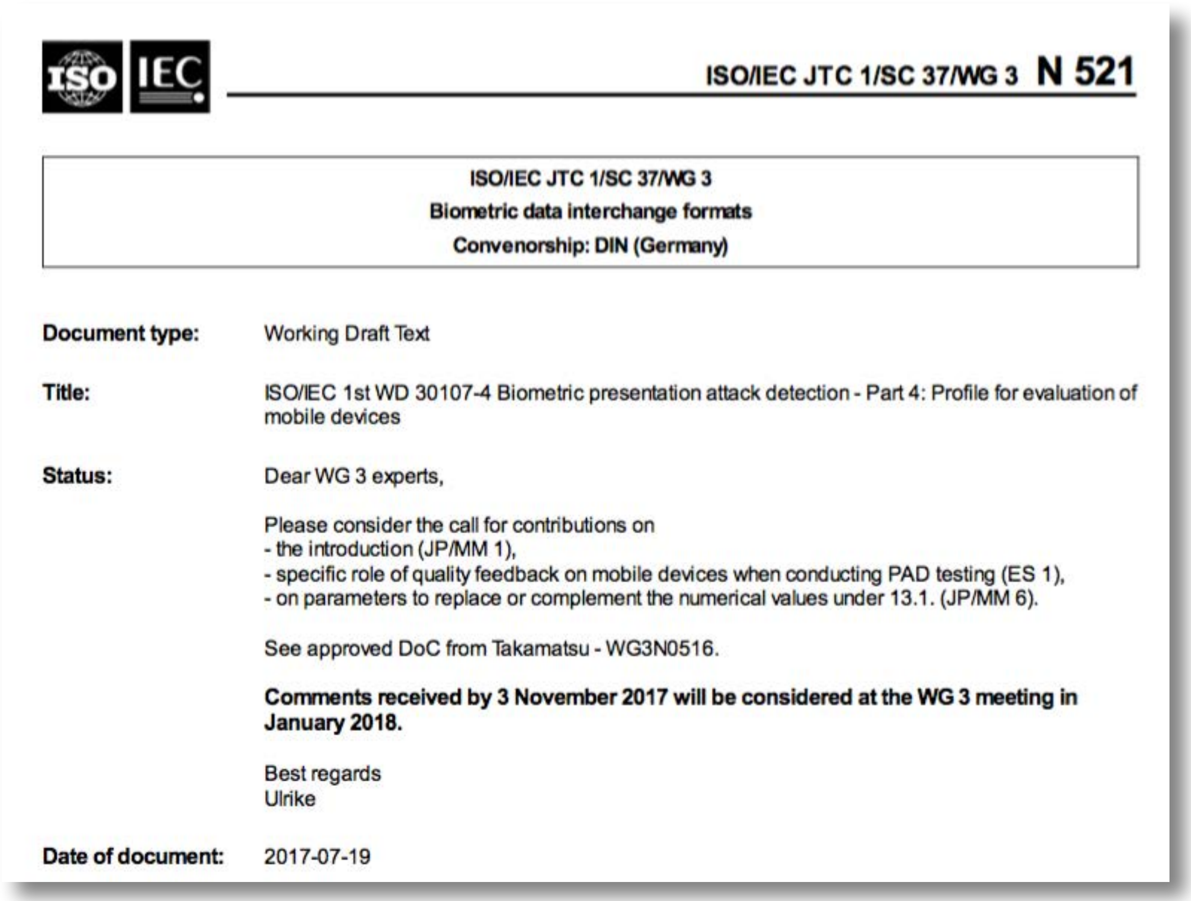
Presentation Attack Detection

ISO/IEC 30107 - Biometric presentation attack detection - Part 4: Testing and reporting

Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- Profile for testing and reporting on mobile devices
- Working Draft available in the ISO/IEC livelink
  http://isotc.iso.org/livelink/livelink?func=ll&objId=19121718&objAction=Open&viewType=1



ISO/IEC JTC 1/SC 37/WG 3 **N 521**

ISO/IEC JTC 1/SC 37/WG 3
Biometric data interchange formats
Convenorship: DIN (Germany)

Document type: Working Draft Text

Title: ISO/IEC 1st WD 30107-4 Biometric presentation attack detection - Part 4: Profile for evaluation of mobile devices

Status: Dear WG 3 experts,

Please consider the call for contributions on
- the introduction (JP/MM 1),
- specific role of quality feedback on mobile devices when conducting PAD testing (ES 1),
- on parameters to replace or complement the numerical values under 13.1. (JP/MM 6).

See approved DoC from Takamatsu - WG3N0516.

Comments received by 3 November 2017 will be considered at the WG 3 meeting in January 2018.

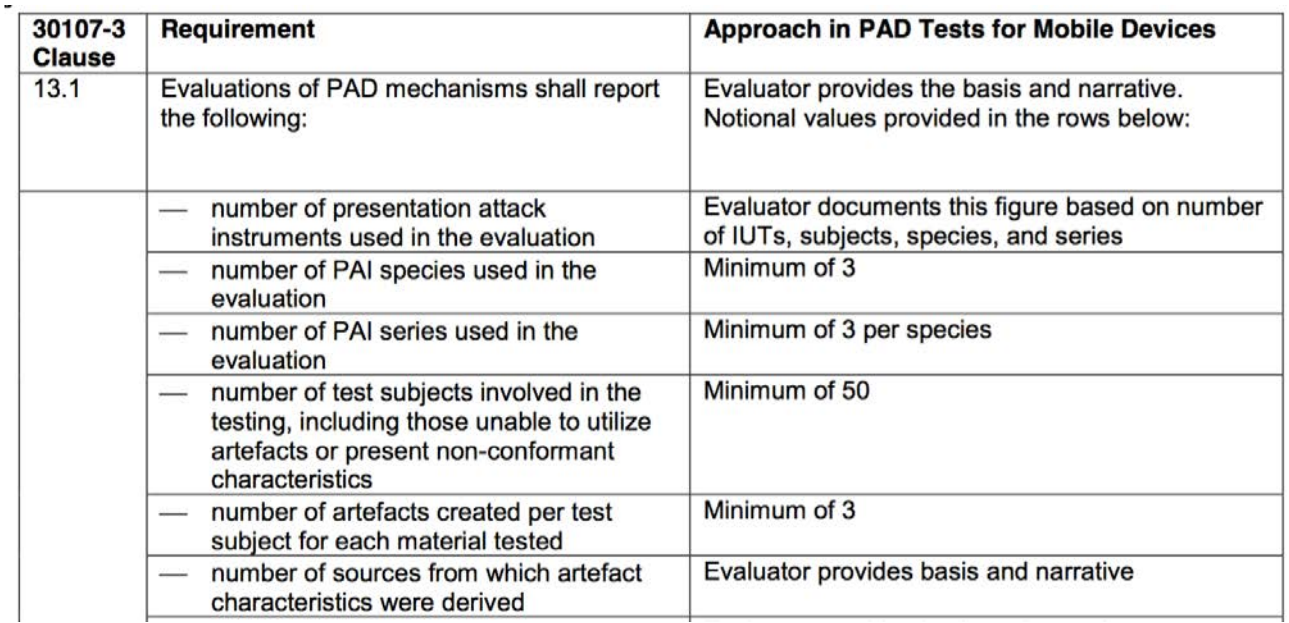
Best regards
Ulrike

Date of document: 2017-07-19

Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- Scope:
  - *This standard provides guidance for testing biometric presentation attack detection mechanisms on mobile devices with local biometric authentication.*
  - *The standard considers: specification of a minimum PAI species and specification of a minimum number of subjects*
- Example:



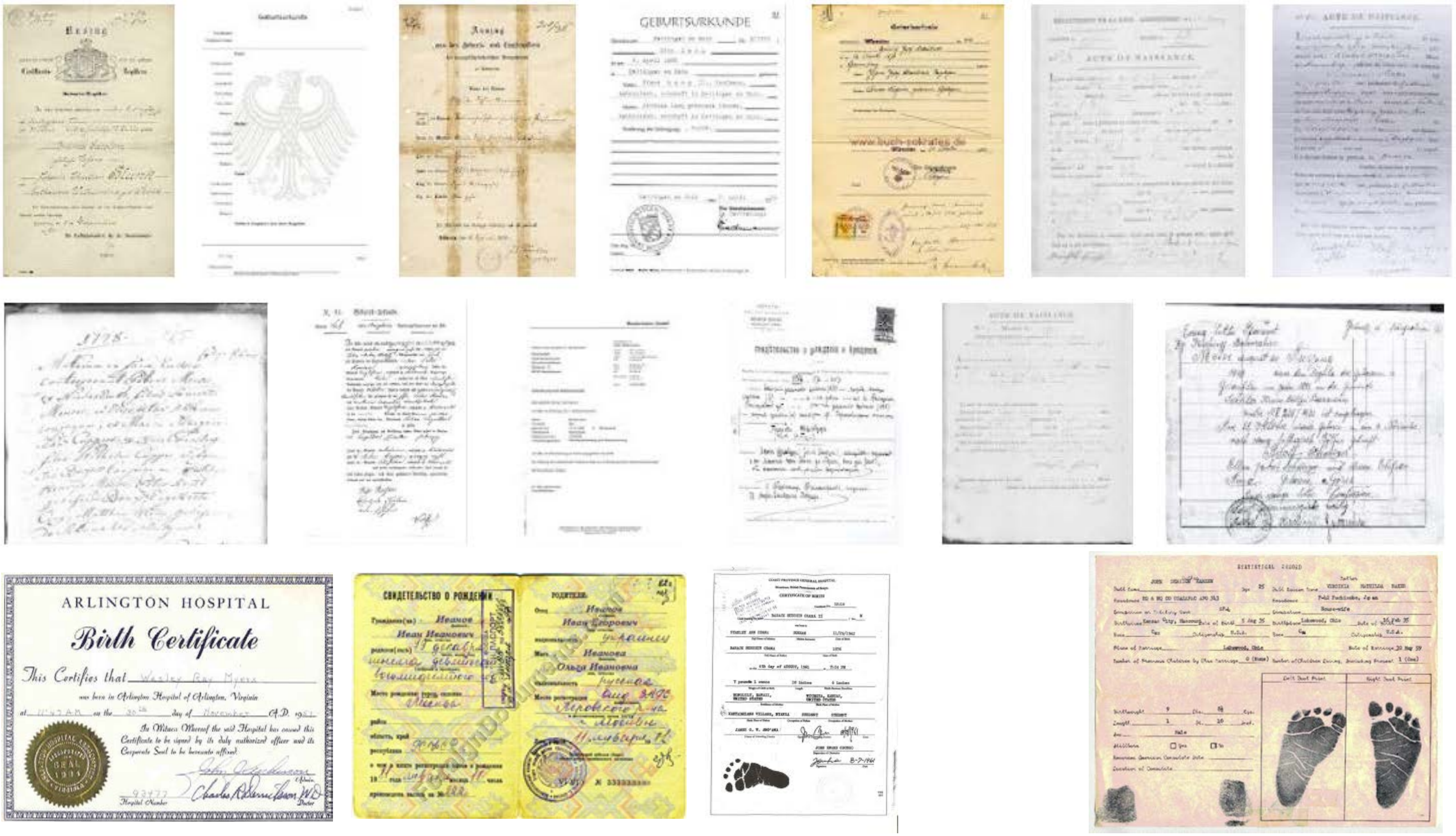
30107-3 Clause	**Requirement**	**Approach in PAD Tests for Mobile Devices**
13.1	Evaluations of PAD mechanisms shall report the following:	Evaluator provides the basis and narrative. Notional values provided in the rows below:
	— number of presentation attack instruments used in the evaluation	Evaluator documents this figure based on number of IUTs, subjects, species, and series
	— number of PAI species used in the evaluation	Minimum of 3
	— number of PAI series used in the evaluation	Minimum of 3 per species
	— number of test subjects involved in the testing, including those unable to utilize artefacts or present non-conformant characteristics	Minimum of 50
	— number of artefacts created per test subject for each material tested	Minimum of 3
	— number of sources from which artefact characteristics were derived	Evaluator provides basis and narrative

Birth Certificates

Birth Certificates

A missing standard for a secure Evidence of Identity

- birth certificates have no common format or content

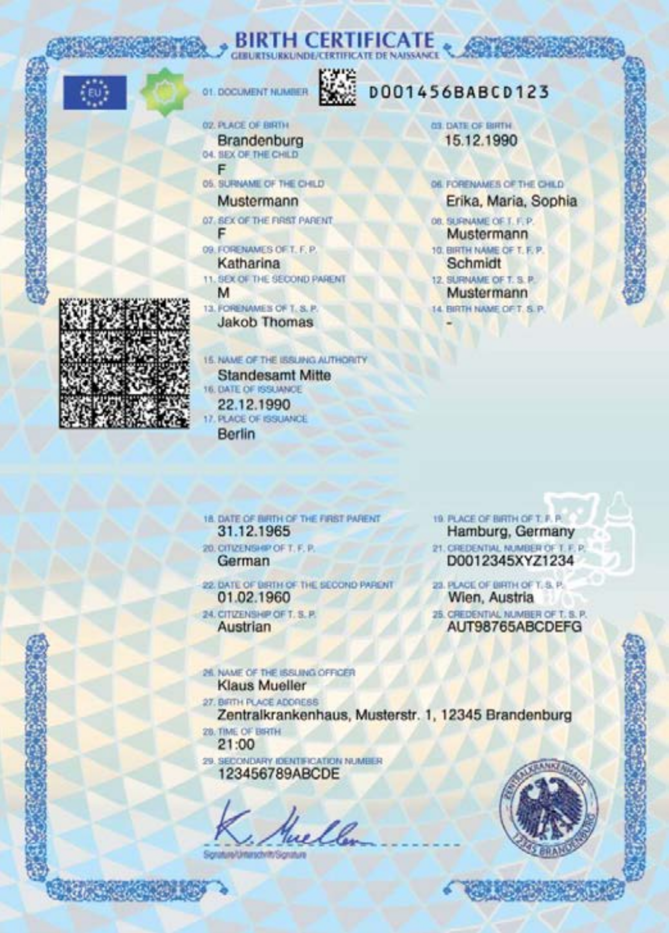


Birth Certificates

A missing standard for a secure Evidence of Identity

- Birth certificates
  - have no common format / content
  - have no common set of security features (electronic signature, special paper, special ink, …)
- Consequences:
  - Can be counterfeited quite easily
  - Issuance of highly secure ePassports based on unsecure breeder documents
  - Example: In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent breeder documents (article in “Le Parisien”, 19.12.2011)

Breeder Document - Harmonized Layout



BIRTH CERTIFICATE
GEBURTSURKUNDE/CERTIFICATE DE NAISSANCE

EU

01. DOCUMENT NUMBER D001456BABCD123

02. PLACE OF BIRTH
Brandenburg

03. DATE OF BIRTH
15.12.1990

04. SEX OF THE CHILD
F

05. SURNAME OF THE CHILD
Mustermann

06. FORENAMES OF THE CHILD
Erika, Maria, Sophia

07. SEX OF THE FIRST PARENT
F

08. SURNAME OF T. F. P.
Mustermann

09. FORENAMES OF T. F. P.
Katharina

10. BIRTH NAME OF T. F. P.
Schmidt

11. SEX OF THE SECOND PARENT
M

12. SURNAME OF T. S. P.
Mustermann

13. FORENAMES OF T. S. P.
Jakob Thomas

14. BIRTH NAME OF T. S. P.
-

15. NAME OF THE ISSUING AUTHORITY
Standesamt Mitte

16. DATE OF ISSUANCE
22.12.1990

17. PLACE OF ISSUANCE
Berlin

18. DATE OF BIRTH OF THE FIRST PARENT
31.12.1965

19. PLACE OF BIRTH OF T. F. P.
Hamburg, Germany

20. CITIZENSHIP OF T. F. P.
German

21. CREDENTIAL NUMBER OF T. F. P.
D0012345XYZ1234

22. DATE OF BIRTH OF THE SECOND PARENT
01.02.1960

23. PLACE OF BIRTH OF T. S. P.
Wien, Austria

24. CITIZENSHIP OF T. S. P.
Austrian

25. CREDENTIAL NUMBER OF T. S. P.
AUT98765ABCDEFG

26. NAME OF THE ISSUING OFFICER
Klaus Mueller

27. BIRTH PLACE ADDRESS
Zentralkrankenhaus, Musterstr. 1, 12345 Brandenburg

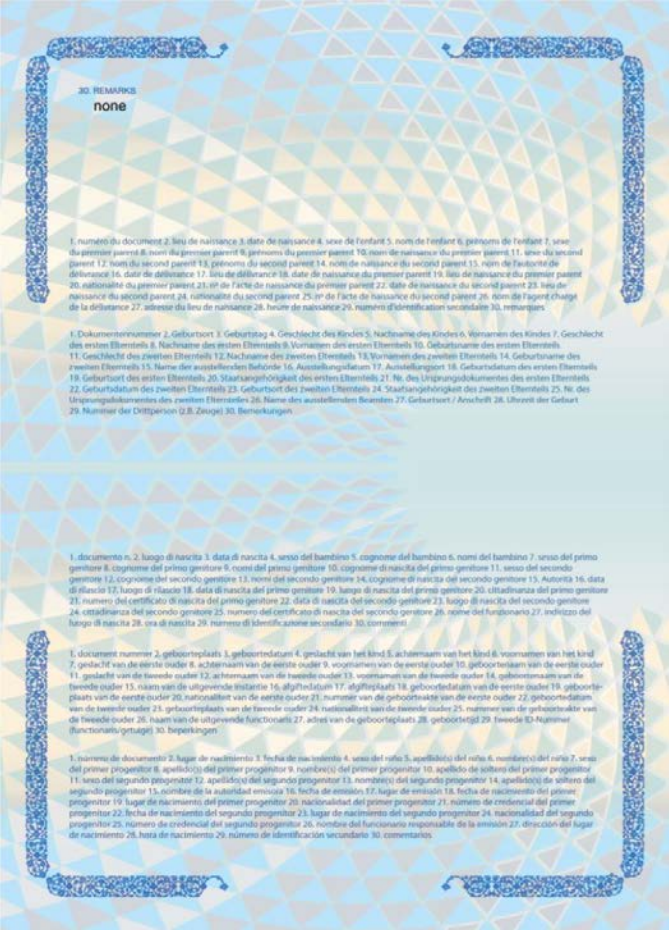
28. TIME OF BIRTH
21:00

29. SECONDARY IDENTIFICATION NUMBER
123456789ABCDE

K. Mueller

Signature/Unterschrift/Signature

ZENTRALKRANKENHAUS 12345 BRANDENBURG



30. REMARKS
none

1. numéro du document 2. lieu de naissance 3. date de naissance 4. sexe de l'enfant 5. nom de l'enfant 6. prénoms de l'enfant 7. sexe du premier parent 8. nom du premier parent 9. prénoms du premier parent 10. nom de naissance du premier parent 11. sexe du second parent 12. nom du second parent 13. prénoms du second parent 14. nom de naissance du second parent 15. nom de l'autorité de délivrance 16. date de délivrance 17. lieu de délivrance 18. date de naissance du premier parent 19. lieu de naissance du premier parent 20. nationalité du premier parent 21. nº de l'acte de naissance du premier parent 22. date de naissance du second parent 23. lieu de naissance du second parent 24. nationalité du second parent 25. nº de l'acte de naissance du second parent 26. nom de l'agent chargé de la délivrance 27. adresse du lieu de naissance 28. heure de naissance 29. numéro d'identification secondaire 30. remarques

1. Dokumentennummer 2. Geburtsort 3. Geburtstag 4. Geschlecht des Kindes 5. Nachname des Kindes 6. Vornamen des Kindes 7. Geschlecht des ersten Elternteils 8. Nachname des ersten Elternteils 9. Vornamen des ersten Elternteils 10. Geburtsname des ersten Elternteils 11. Geschlecht des zweiten Elternteils 12. Nachname des zweiten Elternteils 13. Vornamen des zweiten Elternteils 14. Geburtsname des zweiten Elternteils 15. Name der ausstellenden Behörde 16. Ausstellungsdatum 17. Ausstellungsort 18. Geburtsdatum des ersten Elternteils 19. Geburtsort des ersten Elternteils 20. Staatsangehörigkeit des ersten Elternteils 21. Nr. des Ursprungsdokumentes des ersten Elternteils 22. Geburtsdatum des zweiten Elternteils 23. Geburtsort des zweiten Elternteils 24. Staatsangehörigkeit des zweiten Elternteils 25. Nr. des Ursprungsdokumentes des zweiten Elternteiles 26. Name des ausstellenden Beamten 27. Geburtsort / Anschrift 28. Uhrzeit der Geburt 29. Nummer der Drittperson (z.B. Zeuge) 30. Bemerkungen

1. documento n. 2. luogo di nascita 3. data di nascita 4. sesso del bambino 5. cognome del bambino 6. nomi del bambino 7. sesso del primo genitore 8. cognome del primo genitore 9. nomi del primo genitore 10. cognome di nascita del primo genitore 11. sesso del secondo genitore 12. cognome del secondo genitore 13. nomi del secondo genitore 14. cognome di nascita del secondo genitore 15. Autorità 16. data di rilascio 17. luogo di rilascio 18. data di nascita del primo genitore 19. luogo di nascita del primo genitore 20. cittadinanza del primo genitore 21. numero del certificato di nascita del primo genitore 22. data di nascita del secondo genitore 23. luogo di nascita del secondo genitore 24. cittadinanza del secondo genitore 25. numero del certificato di nascita del secondo genitore 26. nome del funzionario 27. indirizzo del luogo di nascita 28. ora di nascita 29. numero di identificazione secondario 30. commenti

1. document nummer 2. geboorteplaats 3. geboortedatum 4. geslacht van het kind 5. achternaam van het kind 6. voornamen van het kind 7. geslacht van de eerste ouder 8. achternaam van de eerste ouder 9. voornamen van de eerste ouder 10. geboortenaam van de eerste ouder 11. geslacht van de tweede ouder 12. achternaam van de tweede ouder 13. voornamen van de tweede ouder 14. geboortenaam van de tweede ouder 15. naam van de uitgevende instantie 16. afgiftedatum 17. afgifteplaats 18. geboortedatum van de eerste ouder 19. geboorteplaats van de eerste ouder 20. nationaliteit van de eerste ouder 21. nummer van de geboorteakte van de eerste ouder 22. geboortedatum van de tweede ouder 23. geboorteplaats van de tweede ouder 24. nationaliteit van de tweede ouder 25. nummer van de geboorteakte van de tweede ouder 26. naam van de uitgevende functionaris 27. adres van de geboorteplaats 28. geboortetijd 29. tweede ID-Nummer (functionaris/getuige) 30. beperkingen

1. número de documento 2. lugar de nacimiento 3. fecha de nacimiento 4. sexo del niño 5. apellido(s) del niño 6. nombre(s) del niño 7. sexo del primer progenitor 8. apellido(s) del primer progenitor 9. nombre(s) del primer progenitor 10. apellido de soltero del primer progenitor 11. sexo del segundo progenitor 12. apellido(s) del segundo progenitor 13. nombre(s) del segundo progenitor 14. apellido(s) de soltero del segundo progenitor 15. nombre de la autoridad emisora 16. fecha de emisión 17. lugar de emisión 18. fecha de nacimiento del primer progenitor 19. lugar de nacimiento del primer progenitor 20. nacionalidad del primer progenitor 21. número de credencial del primer progenitor 22. fecha de nacimiento del segundo progenitor 23. lugar de nacimiento del segundo progenitor 24. nacionalidad del segundo progenitor 25. número de credencial del segundo progenitor 26. nombre del funcionario responsable de la emisión 27. dirección del lugar de nacimiento 28. hora de nacimiento 29. número de identificación secundario 30. comentarios

Breeder Document - Content

Data entries based on the 2013 draft ICCS Convention recommendations

Mandatory data records

1 Document number

2 Place of birth

3 Date of birth

4 Sex of the child

5 Surname of the child

6 Forenames of the child

7 Sex of the first parent

8 Surname of the first parent

9 Forenames of the first parent

10 Birth name of the first parent

11 Sex of the second parent

12 Surname of the second parent

13 Forenames of the second parent

14 Birth name of the second parent

15 Name of the issuing authority

16 Date of issuance

17 Place of issuance

Recommended data records

18 Date of birth of the first parent

19 Place of birth of the first parent

20 Citizenship of the first parent

21 Credential number of the first parent

18 Date of birth of the second parent

19 Place of birth of the second parent

20 Citizenship of the second parent

21 Credential number of the second parent

26 Name of the issuing officer

27 Birth place address

28 Time of birth

29 Secondary identification number

30 Remarks

Breeder Document - Number Space

Harmonised design and data entries in all EU Member States (with additional country-specific information).

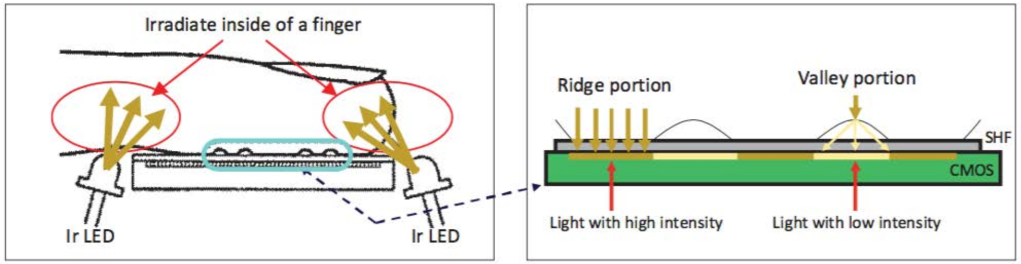
- Electronic national or regional or local databases.
- Europe-wide harmonised numbering system
  - Example: 15 digits

ABC	**1A3B5**	**XY67Z89**
country code	issuing authority	serial number

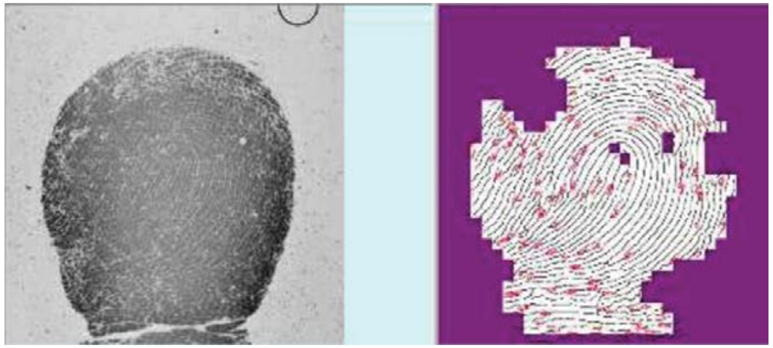
Breeder Document

Biometric References

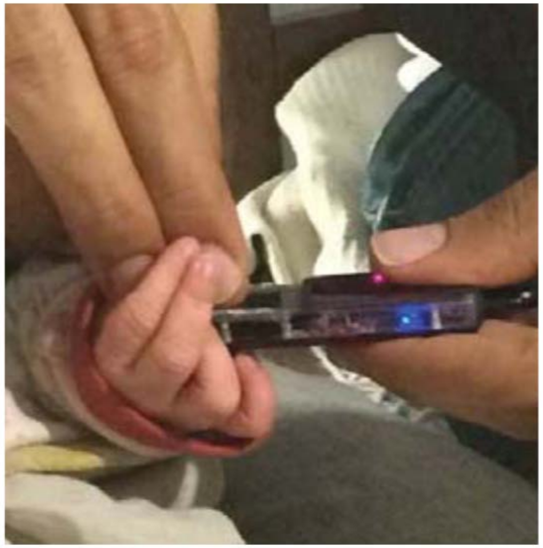
- Fingerprint capturing
  - Use modern fingerprint scanners that are designed for newborns



Scatter Light Direct Reading Method



Fingerprint image and extracted features from six-hour old newborn



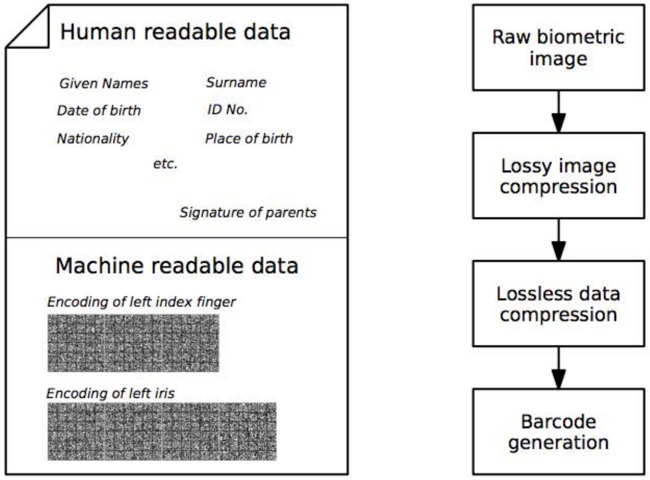
Capturing fingerprint of a six-hour old newborn

Source:
[Koda16] Y. Koda, T. Higuchi, A. Jain: „Advances in Capturing Child Fingerprints: A High Resolution CMOS Image Sensor with SLDR Method“, (BIOSIG 2016)

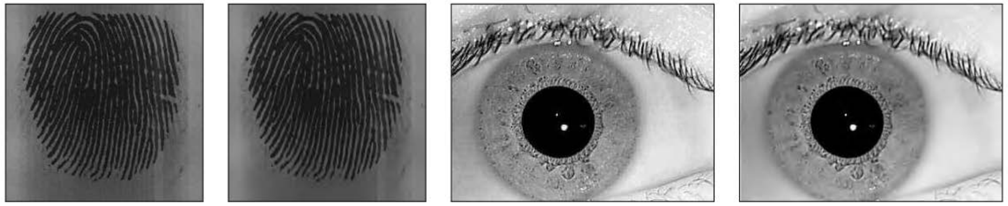
Breeder Document

Biometric References

- Encoding of interchange data - with good compression
  - Store compressed reference image in 2D-barcode



(a) document layout (b) processing chain



(a) *JPG-F* (b) *J2K-F* (c) *JPG-I* (d) *J2K-I*

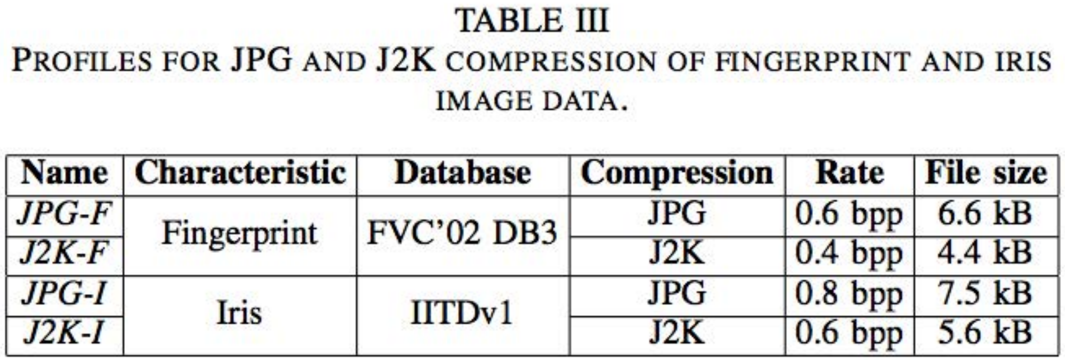


TABLE III
PROFILES FOR JPG AND J2K COMPRESSION OF FINGERPRINT AND IRIS IMAGE DATA.

Name	Characteristic	Database	Compression	Rate	File size
JPG-F	Fingerprint	FVC'02 DB3	JPG	0.6 bpp	6.6 kB
J2K-F			J2K	0.4 bpp	4.4 kB
JPG-I	Iris	IITDv1	JPG	0.8 bpp	7.5 kB
J2K-I			J2K	0.6 bpp	5.6 kB

Proposed birth certificate layout.
Sizes of barcodes correspond
to the approximated storage requirement

Source:
[Buchmann16] N. Buchmann, C. Rathgeb, et al: „A Preliminary Study on the Feasibility of Storing Fingerprint and Iris Image Data in 2D-Barcodes“, (BIOSIG 2016)

References

Web

- WG3 convenor’s website with latest new
  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
- ISO: How to write standards
  http://www.iso.org/iso/how-to-write-standards.pdf
- 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
- Common Criteria Portal:
  http://www.commoncriteriaportal.org/

References

Complementary reading

- ISO/IEC TR 24741, “Biometrics tutorial”, 2007
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-1:v1:en
- ISO/IEC SC37 SD11, “General biometric system architecture”, 2010
  http://isotc.iso.org/livelink/livelink?func=ll&objId=8755976&objAction=Open
- ISO/IEC 2382-37, “Harmonized biometric vocabulary, 2012
  http://www.christoph-busch.de/standards.html
- ISO/IEC 24722, “Multimodal biometrics”, 2015
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en
- ISO/IEC 19795-1, “Biometric performance testing and reporting”, 2006
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19795:-1:ed-1:v1:en

References

Complementary reading - interchange formats

- ISO/IEC 19794-1, “Biometric data interchange formats - Part 1: Framework”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-1:ed-2:v1:en
- ISO/IEC 19794-2, “Biometric data interchange formats - Part 2: Finger minutiae data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-2:ed-2:v1:en
- ISO/IEC 19794-4, “Biometric data interchange formats - Part 4: Finger image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-4:ed-2:v1:en
- ISO/IEC 19794-5, “Biometric data interchange formats - Part 5: Face image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-5:ed-2:v1:en
- ISO/IEC 19794-6, “Biometric data interchange formats - Part 6: Iris image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-6:ed-2:v1:en

References

Complementary reading - quality

- ISO/IEC 29794-1, “Biometric sample quality - Part 1: Framework”, 2011 https://www.iso.org/obp/ui/#iso:std:iso-iec:29794:-1:ed-2:v2:en
- ISO/IEC DIS 29794-4, “Biometric sample quality - Part 4: Finger image data” http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62791
- ISO/IEC TR 29794-5, “Biometric sample quality - Part 5: Face image data”, 2010 https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29794:-5:ed-1:v1:en
- ISO/IEC 29794-6, “Biometric sample quality - Part 6: Iris image data”, 2011 https://www.iso.org/obp/ui/#iso:std:iso-iec:29794:-6:ed-1:v1:en

References

Complementary reading - protection, PAD and mobile

- ISO/IEC 24745, “Biometric Information Protection”, 2011
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52946
- ISO/IEC 30107-1, “Biometric presentation attack detection -
  Part 1: Framework”, 2016
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip
- ISO/IEC 30107-3, “Biometric presentation attack detection -
  Part 3: Testing and reporting”, 2016
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381
- ISO/IEC TR 30125, “Biometrics used with mobile devices”, 2016
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:30125:ed-1:v1:en
- ISO/IEC 15408: “Security Techniques -
  Evaluation Criteria for IT Security / Common Criteria“