ISO/IEC Standard 24745 - Biometric Information Protection

Christoph Busch

www.christoph-busch.de

BTP Workshop
2012-07-13, Paris

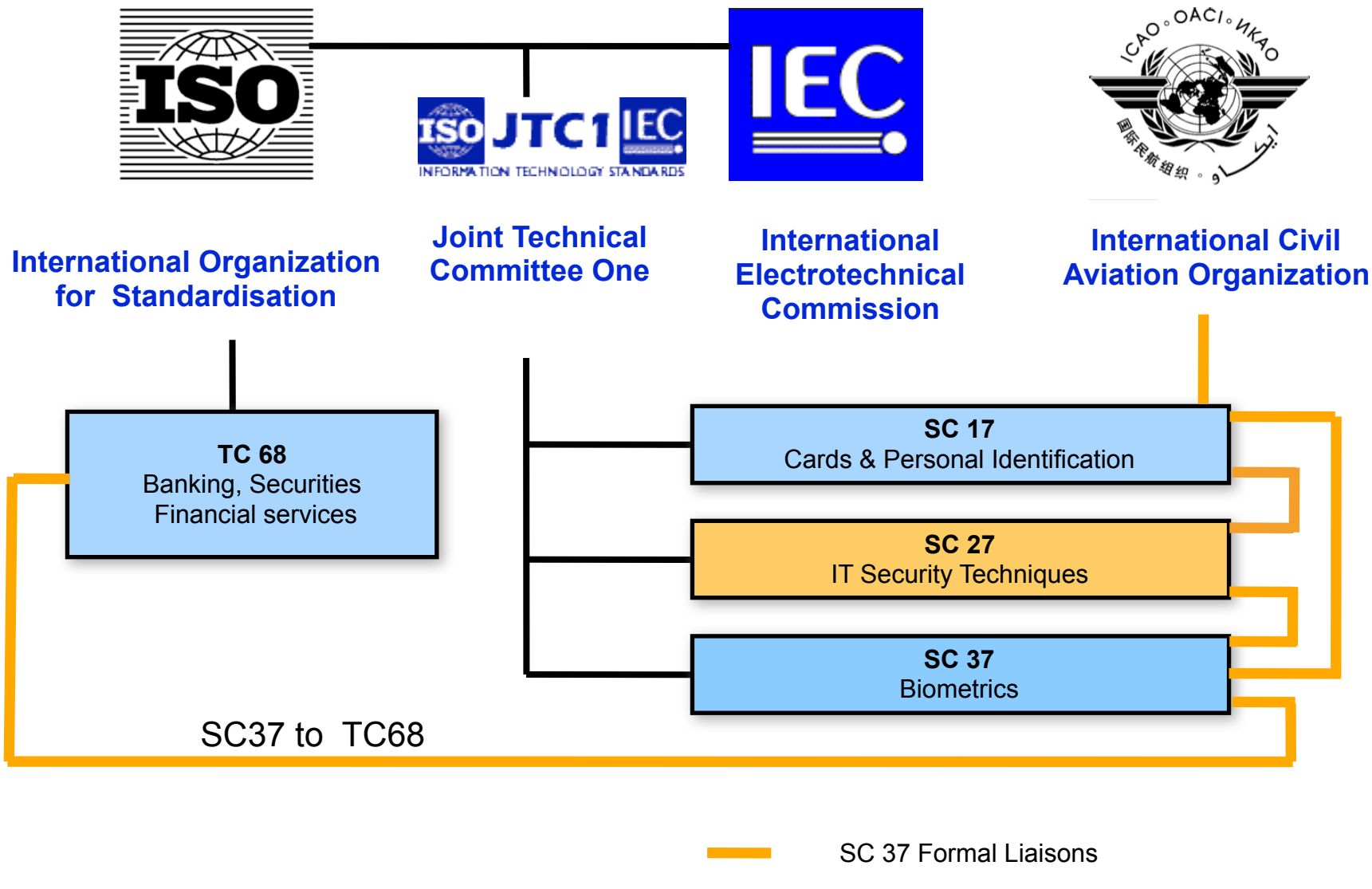
CASED

Fraunhofer IGD

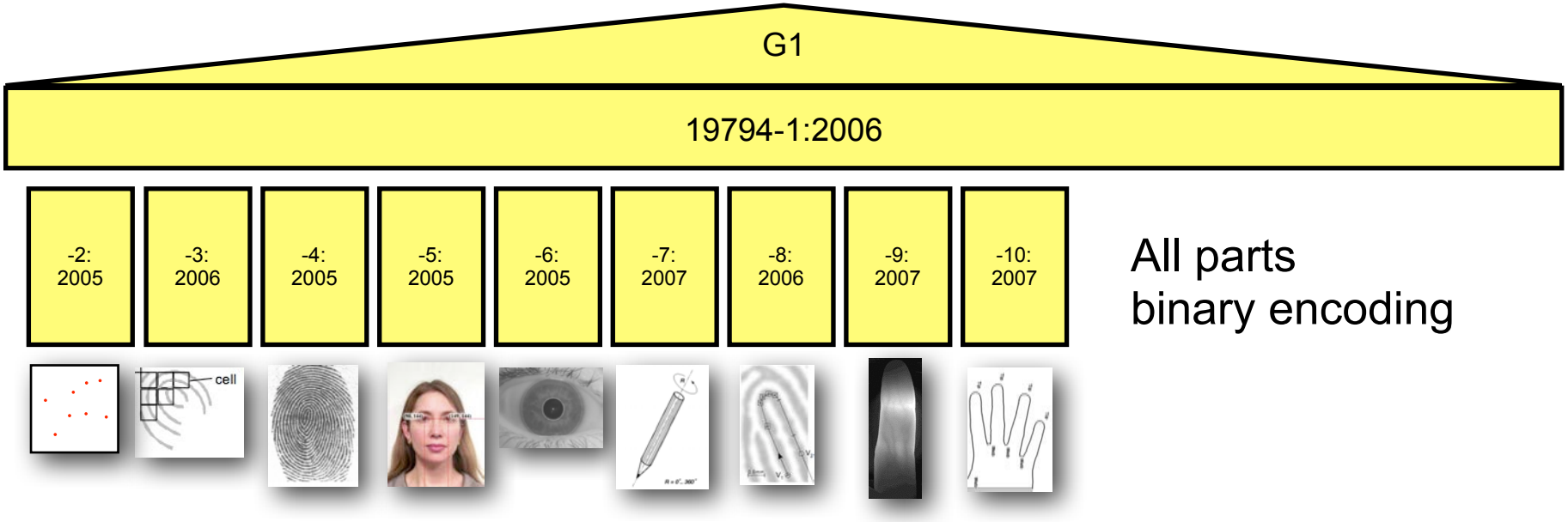
HØGSKOLEN I GJØVIK

What has been standardized in the past

Biometric Standardisation



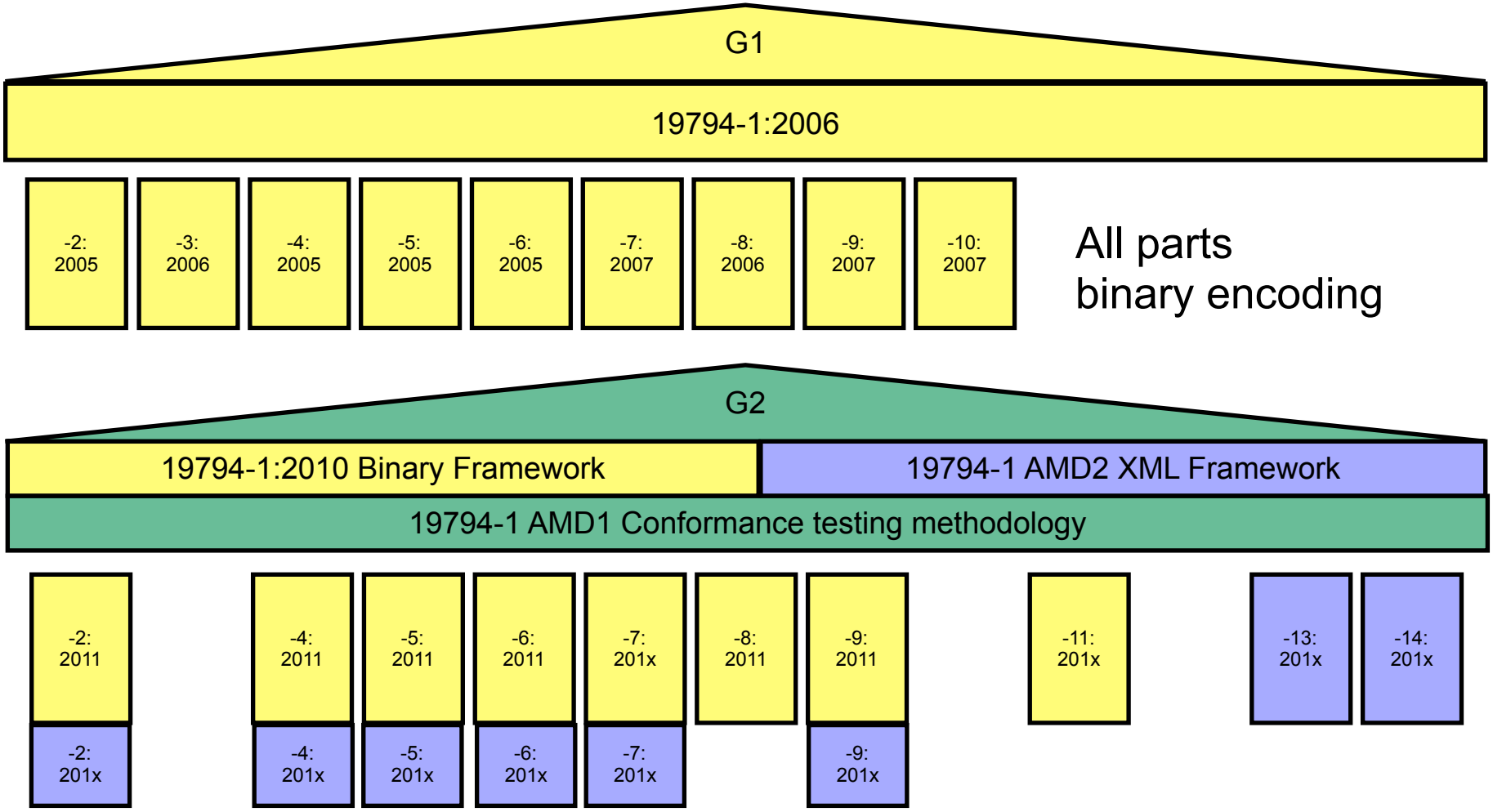
Biometric Data Interchange Format Standards



All parts
binary encoding

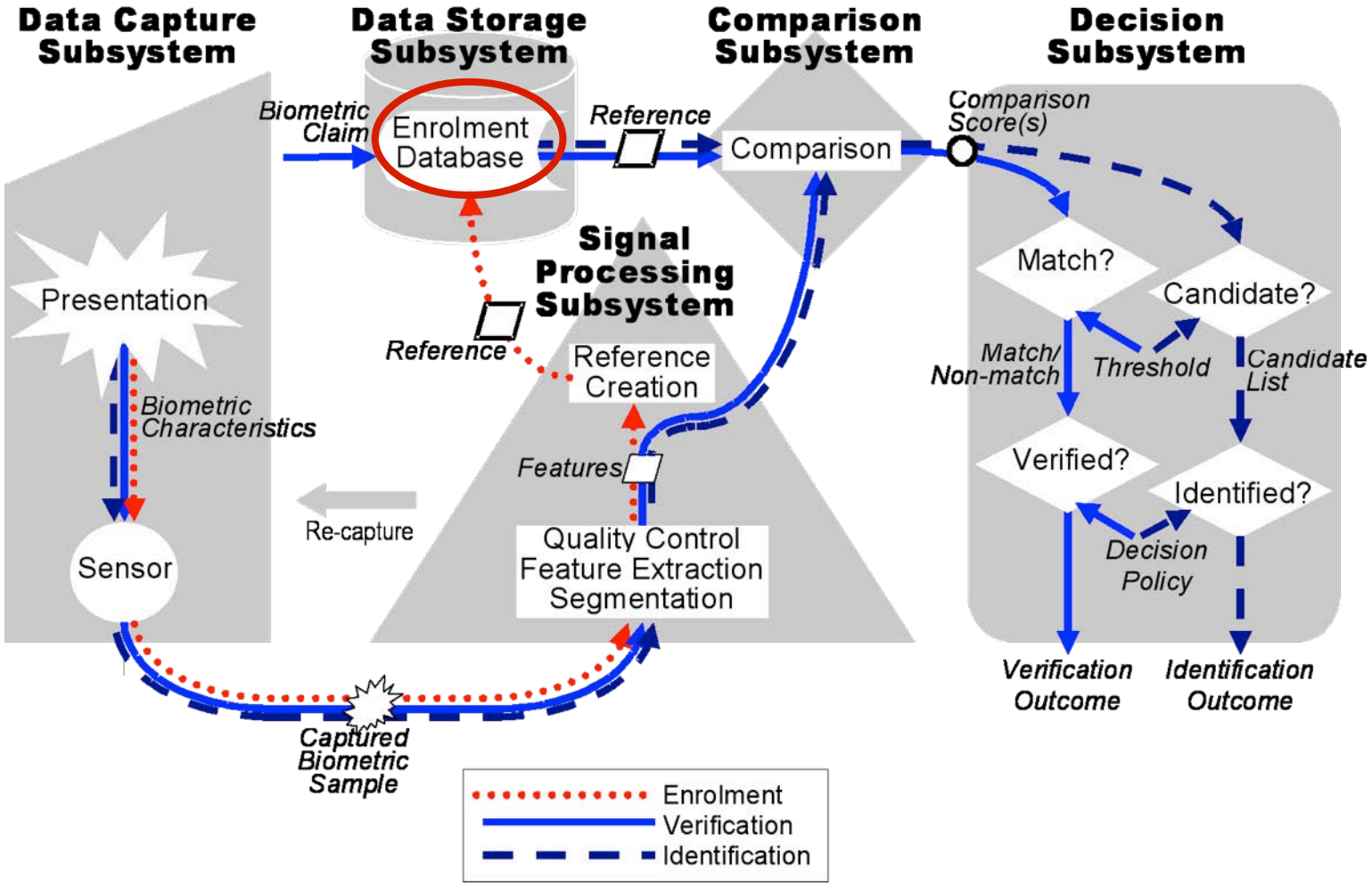
The 19794-Family

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

Risiks in Biometric Systems



Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture

BTP is a widely used Concept

Biometric Template Protection

- alias {Helper Data Scheme, biotoken, biotypes, Pseudo Identities, Pseudonymous Identifier, Fuzzy commitment, Cancelable Biometrics, Biometric encryption, Biohasing, Fuzzy Vault, Shielding functions, Fuzzy extractors, Extended PIR, BIOCRYPTICS,}
- All of them can be represented in a unified architecture
  - see Breebaart et al. „A Reference Architecture for Biometric Template Protection based on Pseudo Identities“, BIOSIG 2008, GI-LNI, (2008)
- Vendors:
  - IBM
  - Philips / priv-ID / GenKey
  - Mitsubishi
  - Hitachi
  - Morpho
  - securis
  - secunet

ISO/IEC 24745

- SC27 published ISO/IEC 24745 in 2011

ISO/IEC 24745

Topics addressed:

- Threats and countermeasures to biometric systems;
- Cryptographic requirements for the implementation of countermeasures;
- Requirements for the binding of a biometric reference with an identity reference;
- Several models of biometric system different scenarios for the storage and comparison of biometric references;
- Privacy requirements for the protection of the individuals data during the storage and processing of biometric information.

Security in Application Models

Classification of system regarding storage of biometric references and comparison

- Clause 8.2
  - Model A – Store on server and compare on server
  - Model B – Store on token and compare on server
  - Model C – Store on server and compare on client
  - Model D – Store on client and compare on client
  - Model E – Store on token and compare on client
  - Model F – Store on token and compare on token
  - Model G – Store distributed on token and server, compare on server
  - Model H – Store distributed on token and client, compare on client

Security in Application Model A

Store on server and compare on server

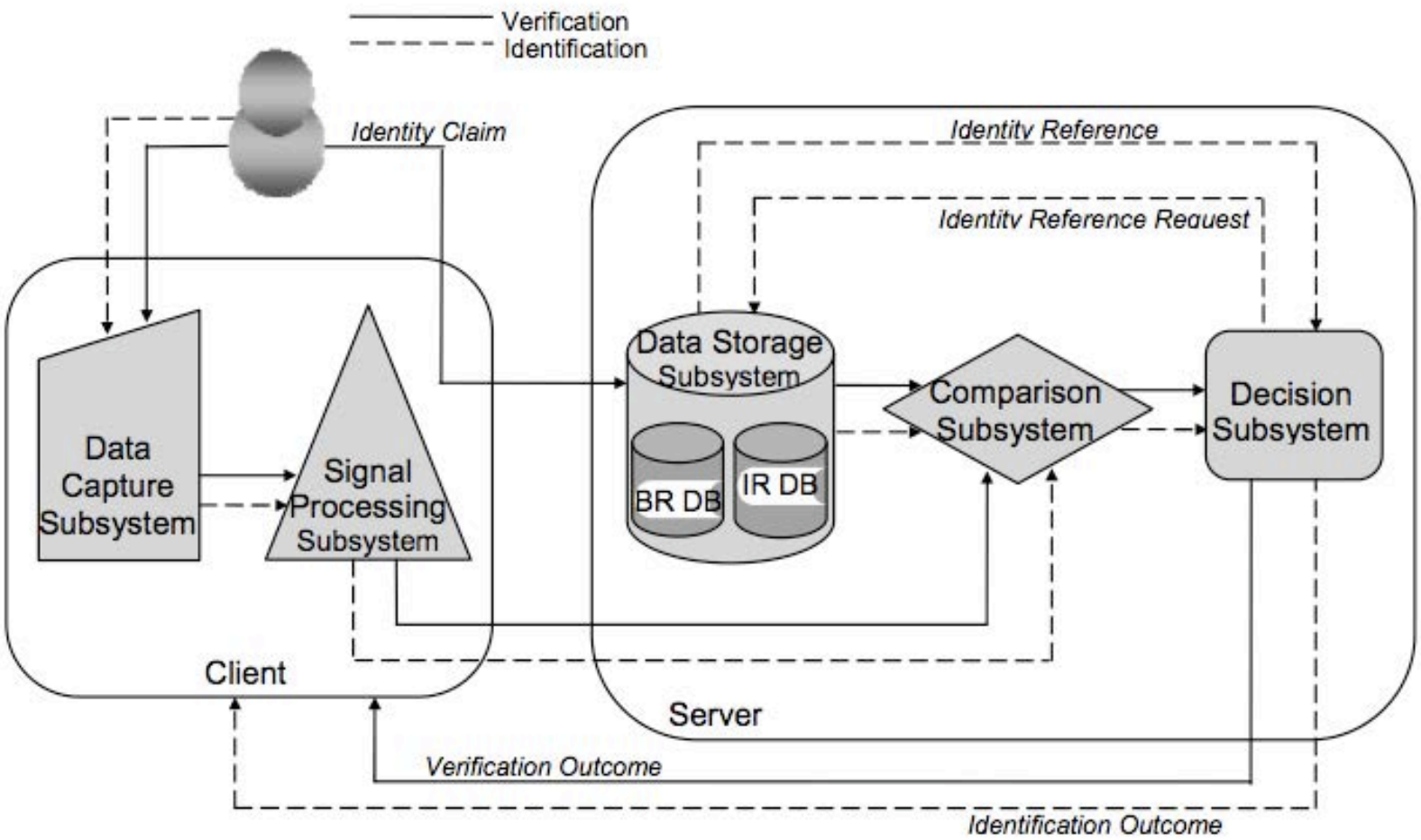


Figure 6 — Model A: store on server and compare on server using BRs

Security in Application Model E

Store on token and compare on token

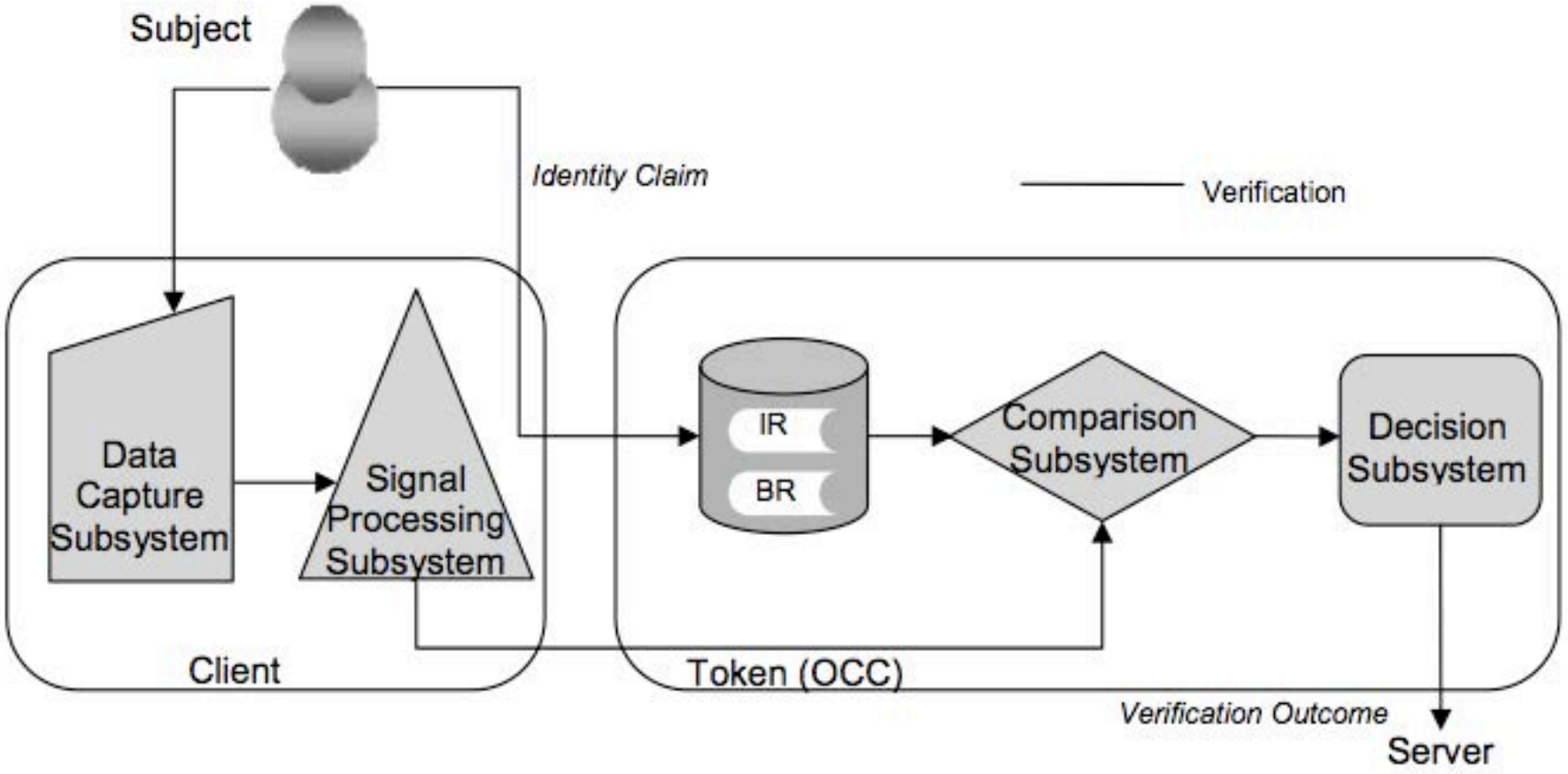


Figure 16 — Model F: Store on token and compare on token using BRs

ISO/IEC 24745

Security Requirements

- Confidentiality

  "...property that protects information against unauthorized access or disclosure..."

- Integrity

  "…property of safeguarding the accuracy and completeness of assets."

- Renewability and revocability

  "…revocation is required to prevent the attacker from future (or continued) unauthorized access."

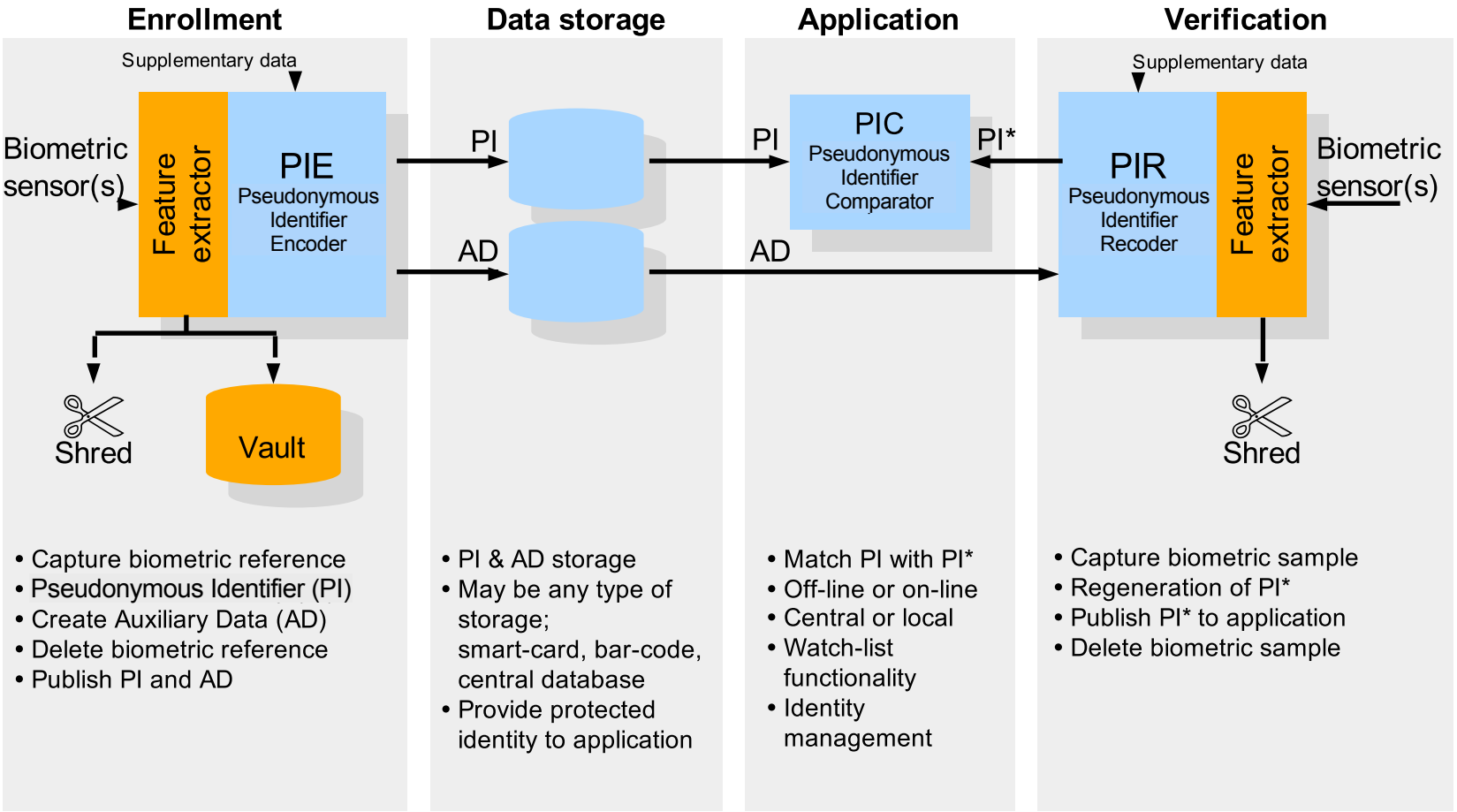
ISO/IEC 24745

Privacy Requirements

- Irreversibility
  "To prevent the use of biometric data for any purpose other than originally intended, biometric data shall be processed by irreversible transforms before storage."
- Unlinkability
  "The stored biometric references shall not be linkable across applications or databases".
- Confidentiality
  „To protect biometric references against access by an unauthorized outsider resulting in a privacy risk, biometric references shall be kept confidential."

PI Framework

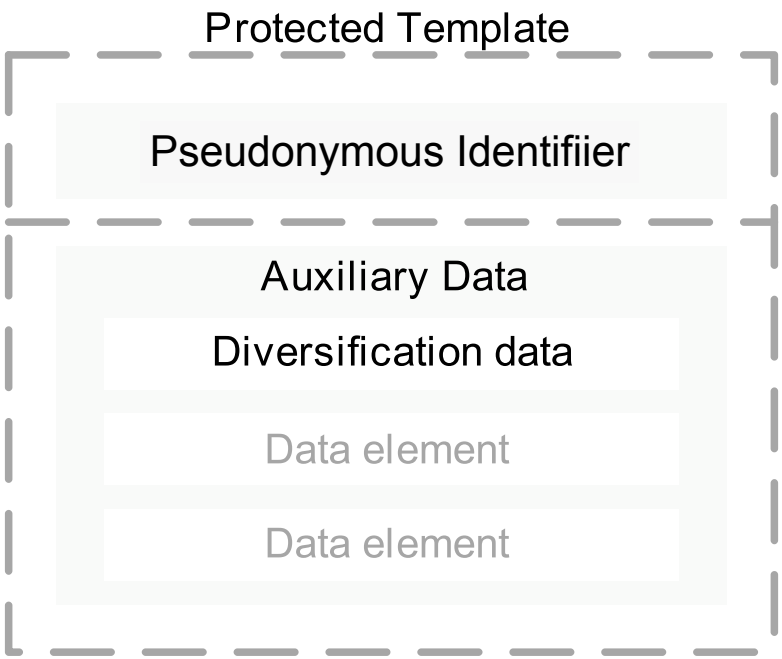
- Architecture for renewable biometric references



Protected Template Structure

Protected Template

- Pseudonymous Identifier
- Auxiliary Data
  - Diversification Data
  - Other data elements



Renewable Biometric References

Elements in the architecture

- auxiliary data AD
  - subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general
- pseudonymous identifier PI
  - part of a renewable biometric reference that represents an individual or data subject within a certain context by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any)
- supplementary data SD
  - data intended for security amplification of renewable biometric references by means of possession, knowledge or application-based secrets that are both required during enrolment and verification and are not stored with biometric references nor dependent on biometric characteristics, that are either provided by the data subject or the identity management system

How to maintain interoperability with protected templates - a suggestion as short term solution

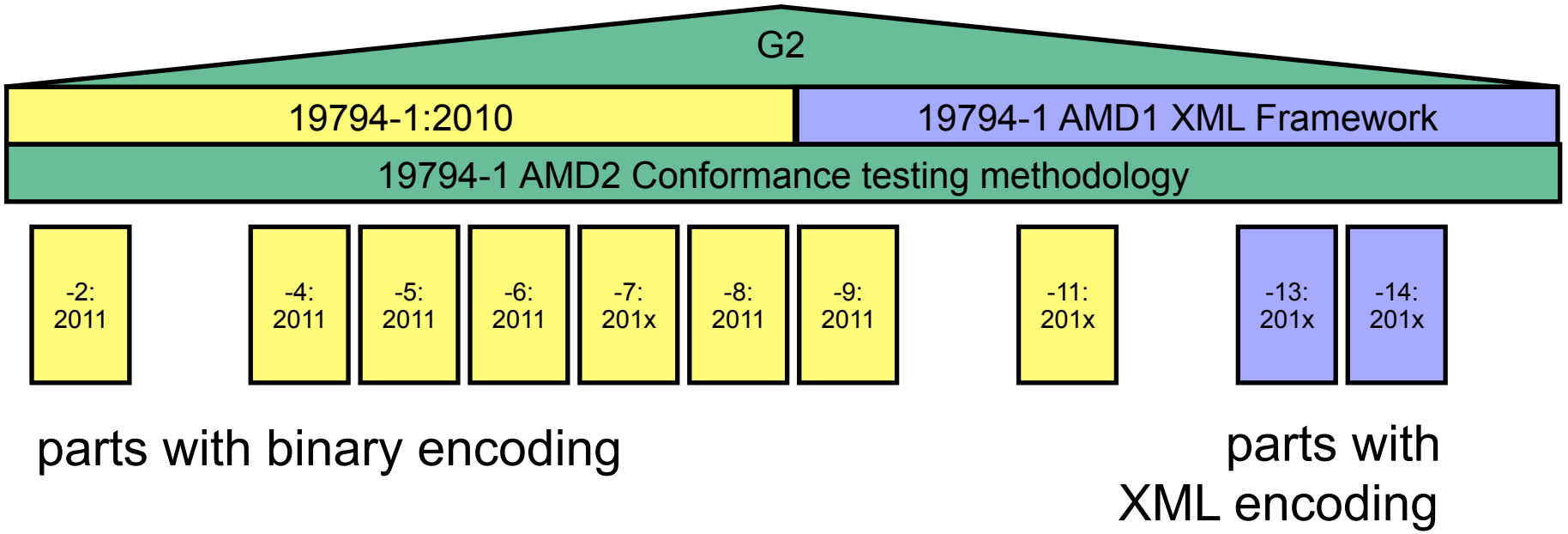
Interoperability of Protected Templates

Interoperability currently not existing!

- Standardization of reference records can be achieved even without consensus on the standardized algorithm

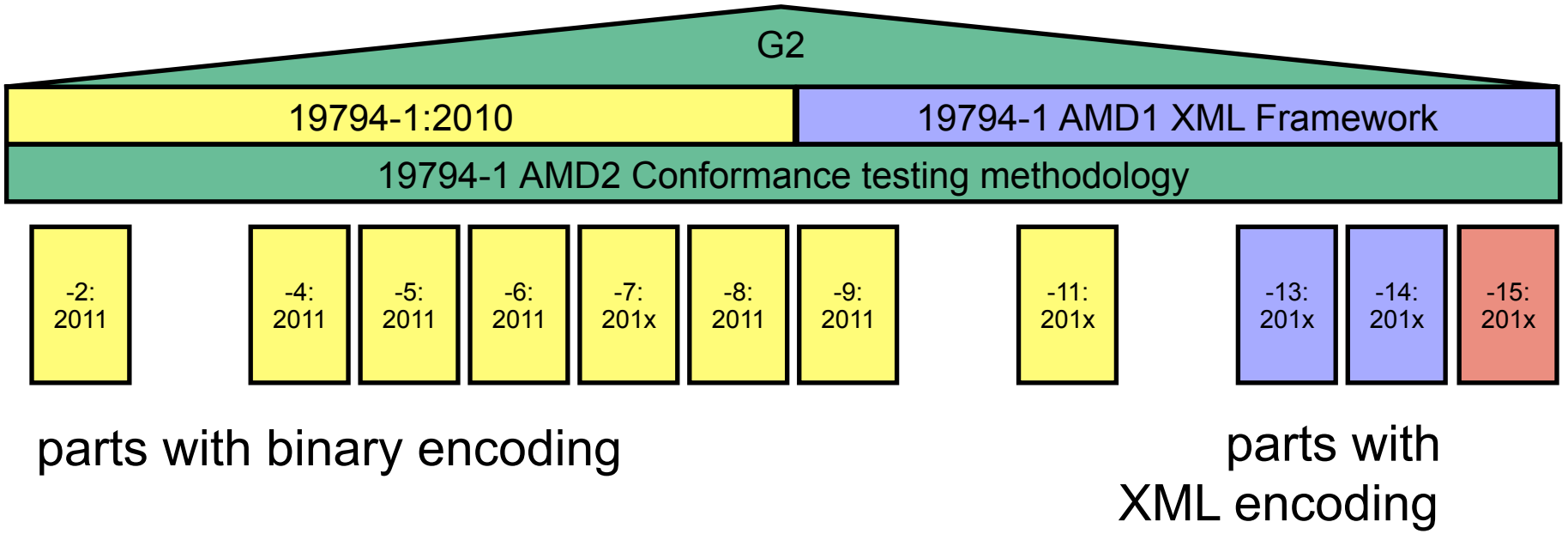
Interoperabilty of Protected Templates

- Standardization of reference records can be achieved even without consensus on the standardized algorithm



Interoperabilty of Protected Templates

- Standardization of reference records can be achieved even without consensus on the standardized algorithm



Interoperabilty of Protected Templates

- Standardization of reference records can be achieved even without consensus on the standardized algorithm
- Algorithm ID
  - This approach has been used for the quality ID case in ISO/IEC 29794-1

Quality Block	Quality Score	1 byte	[0,100] 255	0: lowest 100: highest 255: failed attempt to assign a quality score
	Quality Algorithm Vendor ID	2 bytes	[1,65535]	Quality Algorithm Vendor ID shall be registered with IBIA as a CBEFF biometric organization. Refer to CBEFF vendor ID registry procedures in ISO/IEC 19785-2.
	Quality Algorithm ID	2 bytes	[1,65535]	Quality Algorithm ID may be optionally registered with IBIA as a CBEFF Product Code. Refer to CBEFF product registry

Interoperabilty of Protected Templates

Standardization of reference records can be achieved even without consensus on the standardized algorithm

- Algorithm ID
- Apply the approach from ISO/IEC 29794-1
- PI-Encoder (PIE) generates interchange record with PI, AD and algorithm ID
- PI-Recoder (PIR) can read the AD,PI and can recode the PI*
- The business model is equivalent to the PDF-approach:
  - you pay for the PI-Encoder
  - but the PI-Recoder is free of charge
- Requires vendors (and their national bodies) to participate

The long-term perspective - a Biometric Encryption Standard (BES)competition

A Standard Template Protection Algorithm

Can we standardize a BES (Biometric Encryption Standard)?

First we need to rank BTP algorithm candidates?

- assess security properties and biometric performance in one framework
  - cirteria to assess biometric performance are given in ISO/IEC 19795
  - criteria to assess the security properties
    - an open research field
    - need also to provide numbers
  - see the TURBINE and NIST work published at ICB 2012 (Koen Simoens)

We may want to launch a template protection competition?

- as it was conducted for AES and recently for hash-functions
- as a result of the competition we standardize the winner
- but - we need a BTP testing standard

A Standard for BTP Testing

NWIP in SC37 WG5?

Ways forward:

- NIST-KUL-GUC Study (published at ICB 2012)
- JP NB: SC37 N4933
- US NB: SC37 N5057

Information Technology — ISO/IEC 19795 — Biometrics Performance Testing and Reporting — Part 8: Performance Testing of Template Protection Schemes

Conclusion

- Standardization will increase opportunities for industry and academics
- Revocability of Pseudonymous Identifiers grants a significant improvements in data privacy
- The long-term goal is a BES
- A PI-interchange standard would support deployment of Biometric Template Protection as short-term solution

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