ISO 24745 - Biometric Template Protection

Christoph Busch

Hochschule Darmstadt / Gjøvik University College / Fraunhofer IGD

IBPC 2010 -Satellite Workshop II
NIST

March 5, 2010

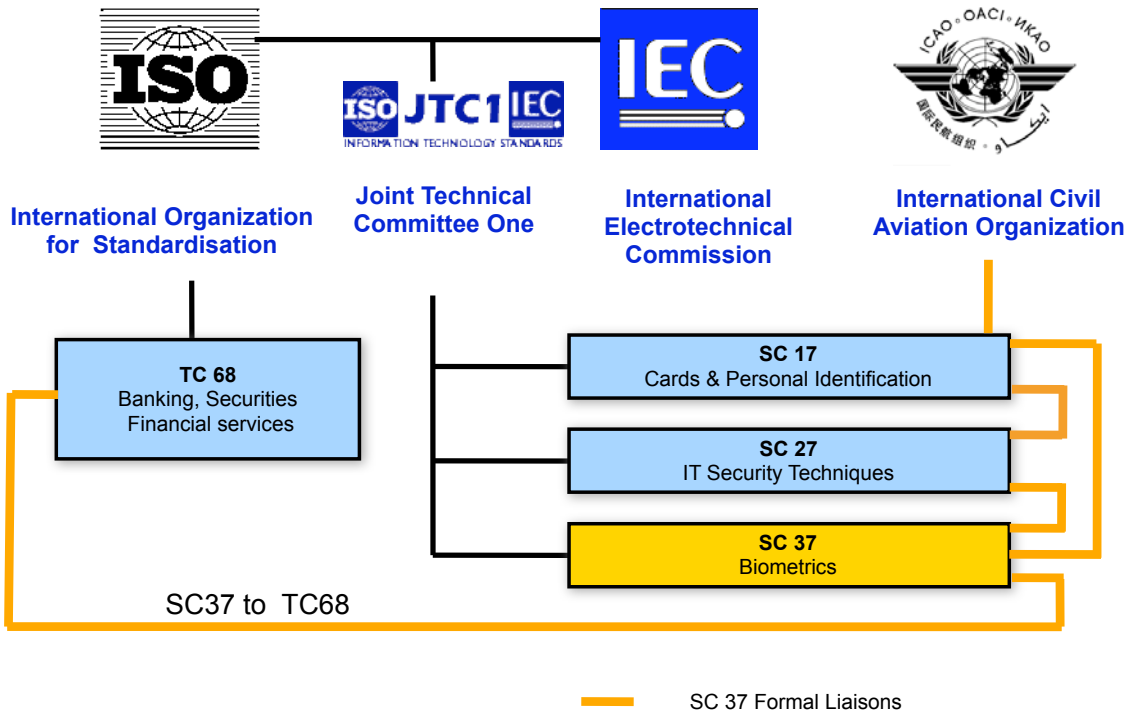
Its is time to standardize BTP

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 Brebaart et al. „A Reference Architecture for Biometric Template Protection based on Pseudo Identities“, GI-LNI: BIOSIG 2008
- Vendors:
  - IBM
  - Philips
  - priv-ID
  - GenKey
  - Mitsubishi
  - Hitachi
  - Sagem Securite
  - securis
  - secunet

Standardization on Template Protection

Biometric Standardisation



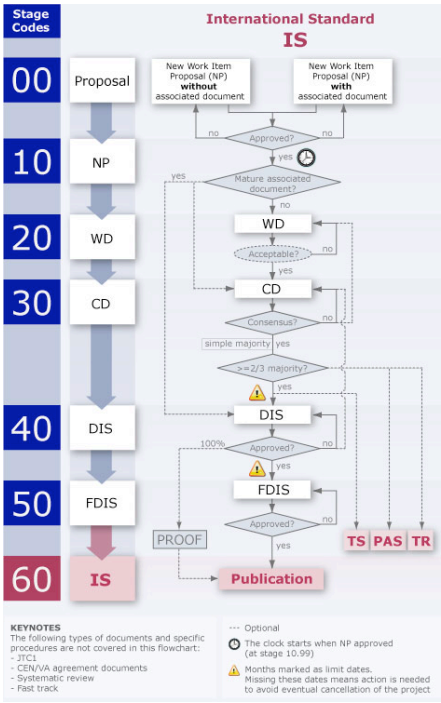
The Process

International Standard

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

Issues to consider:

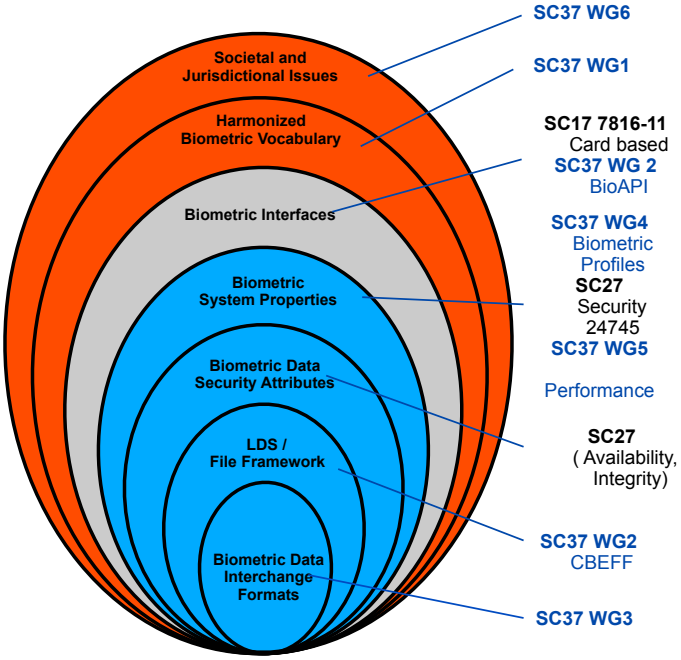
- Commenting periods
- Potentially multiple loops at one level
- Need for mature technology
  (has been argued for Template Protection...)
- Decisions are made on consensus
- Need to progress
- Five year revision cycle



Biometric Standardisation

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



ISO/IEC 24745

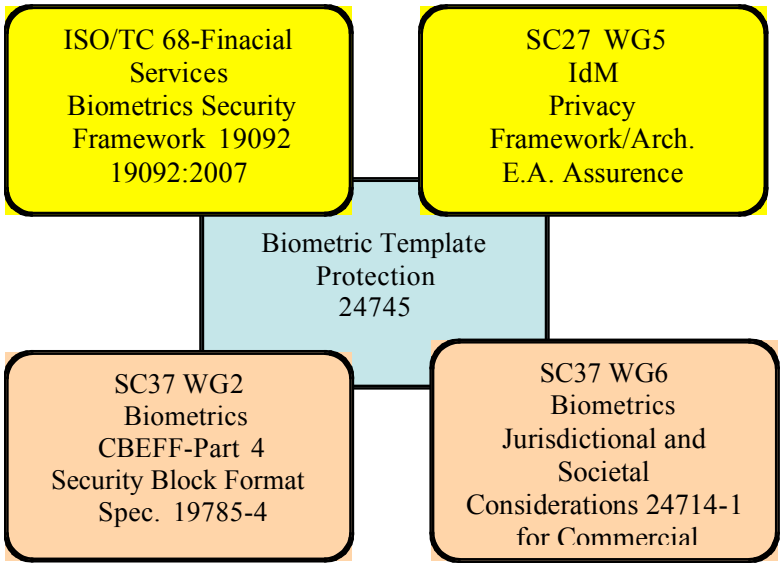
Biometric Template Protection

- October 2006
  - M.G. Chun and Mr. P.J. Lee were appointed as new Co-editors
  - 3rd WD had not been created
- October 2007: Lucerne meeting
  - Discussion on refocusing the standard
- April 2008: Kyoto meeting
  - NB commented on N6314 and accepted to continue with original scope (N3928rev1, 2004)
  - „.... project under its original scope“
- October 2008: Cyprus meeting
  - Inclusion of renewability and diversification
- November 2009: Redmond meeting
  - 2nd CD

ISO/IEC 24745

Biometric Template Protection

- Dependency to other projects



Content of 2nd CD ISO 24745

6.1 Security requirements for biometric sytems

- 6.1.1 Confidentiality
- 6.1.2 Integrity
- 6.1.3 Availability
- 6.1.4 Renewability and revocability

...

8.2 Biometric information privacy requirements

- 8.2.1 Irreversibility
- 8.2.2 Unlinkability
- 8.2.3 Confidentiality
- 8.2.4 Data minimization

Threats and Countermeasures

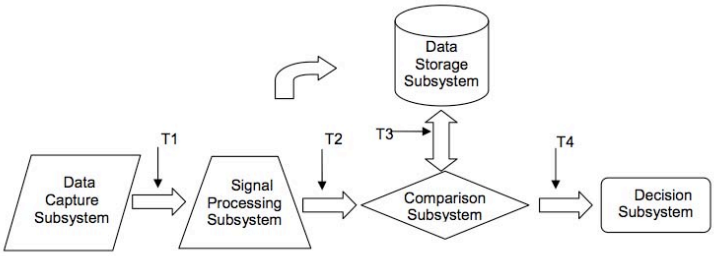
Against biometric system components

- Data capture: T sensor spoofing -
  - liveness detection / multimodal biometric, challenge response
- Signal processing: T insertion of imposter data
  - use approved algorithm
- Comparison: T manipulation of comparison scores
  - secure server and/or client, trusted COC
- Storage: T database compromise
  - diversification to allow renewability of biometric references
  - data separation
  - database access control
- Decision: T hill climbing, T threshold manipulation
  - secure channel , access control

Threats and Countermeasures

During transmission

- Data Capture -Signal Processing:
  - T Eavesdropping
  - T Replay
- Signal Processing-Comparison
  - T Brute Force
- Storage-Comparison
  - T Eavesdropping
  - T Replay
  - T Man in the middel
  - T Hill climbing
- Comparison-Decision
  - T: Comparison score manipulation



Security in Application Models

Classification of system regarding storage of biometric references and comparison

- Clause 7.2
  - 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

Consensus at Oct 2008 meeting

Biometric Template Protection should include Pseudonymous Identifieres

- Now a mature technology with various products
  - Significant progress over 1st ad 2nd WD
- Allows renewability/revocability
  - Create new Pseudonymous Identifiers from same biometric sample
- Prevents collisions and associated security / privacy risks
- Allows a data separation principle
  - PI and AD stored in different places to
    - Enhance security
    - Puts both data subject and service provider in control of comparison process and revocation

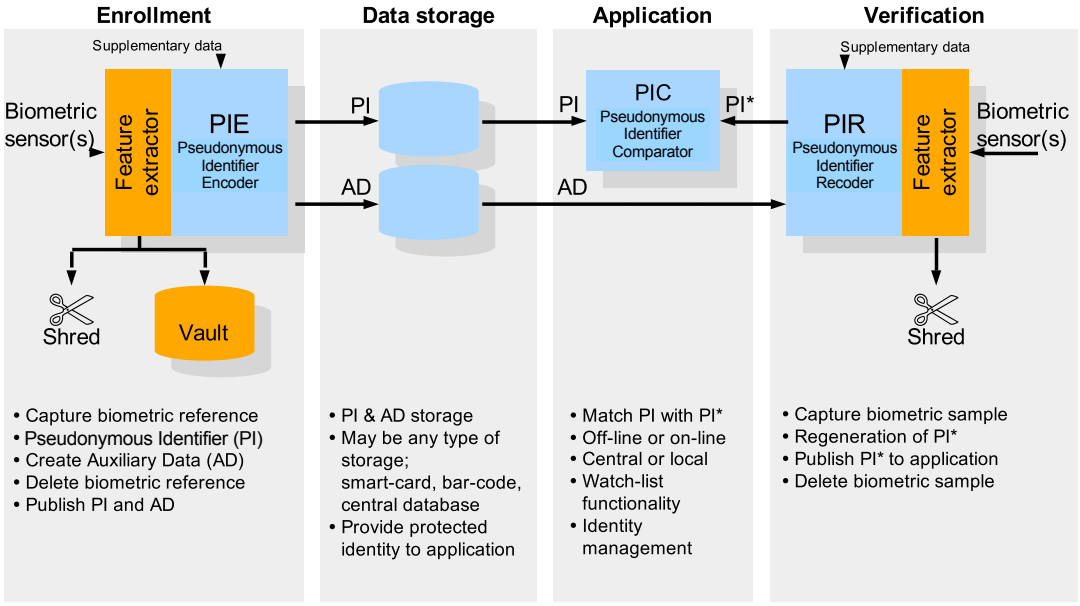
Renewable Biometric References

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

PI Framework

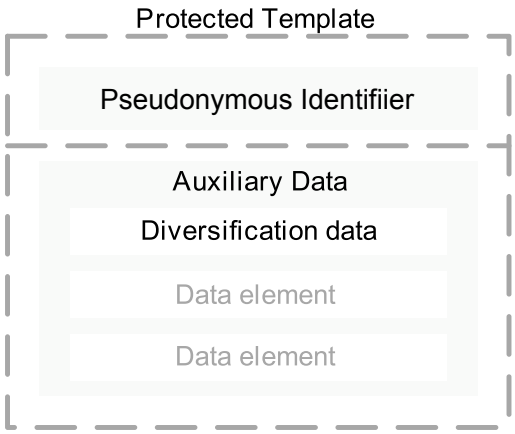
- Architecture for renewable biometric references



Protected Template Structure

Protected Template

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



Example Methods Generating PIs

Table C.1 maps existing methods to ISO 24745

Method	Reference	pseudonymous identifier (PI)	Auxiliary data (AD)
Helper data systems	[23]	Hash of secret string	Helper data
Fuzzy commitment	[24]	Hash of secret string	Offset
Biometric encryption	[25]	Cryptographic key	Filter and key link
Fuzzy vault	[26]	Hash of secret string	Point set P
Shielding functions	[27]	Hash of secret string	Authentication challenge W
Fuzzy extractors	[28]	Hash of secret string	Public string P
Extended PIR	[29]	Encrypted template	n/a
2D hexagonal quantization index modulation	[30]	Hash of a secret string	Quantization errors
Cancellable biometrics	[32]	Transformed template	Transform parameters

Example Methods Generating PIs

[23] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijen, G. J., Bazen, A. M., Veldhuis, R. N. J. "Practical biometric authentication with template protection" in *Audio and Video-based biometric person authentication*, pages 436-449, Springer, Berlin, Germany (2005)

[24] Juels, A., Wattenberg, M. "A fuzzy commitment scheme" in *ACM Conference on Computer and Communications Security*, pages 28–36 (1999)

[25] Soutar, C., Roberge, D., Stoianov, A., Gilroy,R., Vijaya Kumar, B. V. K. "Biometric Encryption using image processing" in *Proc. SPIE 3314*, pages 178–188 (1998)

[26] Juels, A., Wattenberg, M. "A fuzzy vault scheme" in *Proc. IEEE Int. Symposium on Information Theory* (2002)

[27] Linnartz, J-P. M. G., Tuyls, P. "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates" in *AVBPA*, pages 393–402 (2003)

[28] Dodis., Y., Reyzin, L., Smith, A. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data" in *Eurocrypt* (2004)

[29] Bringer, J., Chabanne, H., Pointcheval, D., Tang, Q. "Extended private information retrieval and its application in biometrics authentications" in *CANS* (2007)

[30] Buhan, I., Doumen, J., Hartel, P., Veldhuis, R. N. J. "Embedding renewable cryptographic keys into continuous noisy data" in *Information and communications security, 10th international conference ICICS*, Birmingham, UK, 294-310 (2008)

[31] ISO/IEC 7816-4: 2005, Identification circuit cards - Part 4: Organization, security and commands for interchange

[32] Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M. "Generating cancellable fingerprint templates" in *IEEE trans. pattern analysis and machine intelligence*, 29(4), pages 561-572 (2007)

Example Methods Generating PIs

Table C.1 Suggested add-ons to examples

Method	Reference	PI	AD
Biometric Robust Hashing	[1]	Hash of a robust binary string	One-way transformation
BioHashing	[2]	A robust binary string	Random projection matrix
Short-lived cryptokey	[3]	Crypto-keys	System parameters
Bio-tokens	[4]	Encrypted minutiae	Cryptographic keys
Secure sketch	[5]	Quantization residue	Quantizer
Robust Minutiae Hash	[6]	Robust binary string for each minutia	Random diversification table

References

[1] Sutcu, Y, Sencar, H.T., and Memon, N. "A secure biometric authentication scheme based on robust hashing," Proc. of ACM Multimedia and Security Workshop. New York, USA, 111-116 (2005).

[2] Teoh, A. B. J., Goh, A., and Ngo, D. C. L. "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," IEEE Trans. on Pattern Analysis and Machine Intelligence, 28(12), 1892–1901 (2006).

[3] GenKey. "System, portable device and method for digital authenticating, crypting and signing by generating short-lived cryptokeys," *US Patent 2006/0198514A1.*

[4] T. E. Boult, W. J. Scheirer, R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in *Proc. IEEE Inter. Conf. on Comput. Vis. & Patt. Recog*, USA, 2007.

[5] Q. Li, Y. Sutcu, N. Memon, "Secure Sketch for Biometric Templates," Advances in Cryptology – ASIACRYPT 2006.

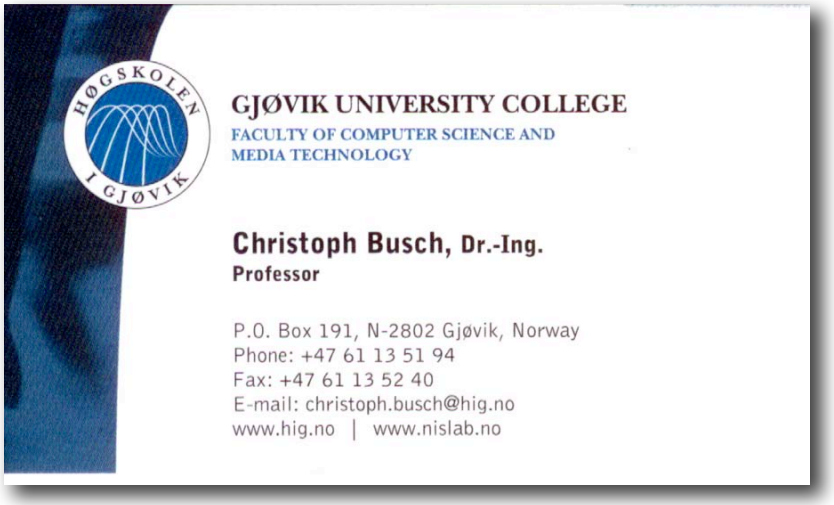
[6] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Robust Minutiae Hash for Fingerprint Template Protection," *SPIE Media Forensics and Security, Electronic Imaging*, Jan.17-21, San Jose, USA, 2010.

Current Status

- SC27 WG5 Redmond meeting addressed numerous comments - also from SC37
- Latest 2nd CD 24745
- Comments are due: April 8, 2010

Committee Draft **ISO/IEC 2nd CD 24745**	Reference number: ISO/IEC JTC 1/SC 27 **N8158**
Date: **2010-01-08**	Supersedes document SC 27 N7740
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.	
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-04-08** Please submit your votes and comments via the online balloting application by the due date indicated.
ISO/IEC 2nd CD 24745 Title: Information technology -- Security techniques – Biometric template protection Project: 1.27.45 (24745)	

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