

Telebiometric authentication: one time template and biometric HSM

Myung Geun Chun
Chungbuk National University
Korea

January. 18. 2011

This work was supported by the National Research Foundation of Korea Grant
Funded by the Korean Government(MEST)"(NRF-2010--0024037)



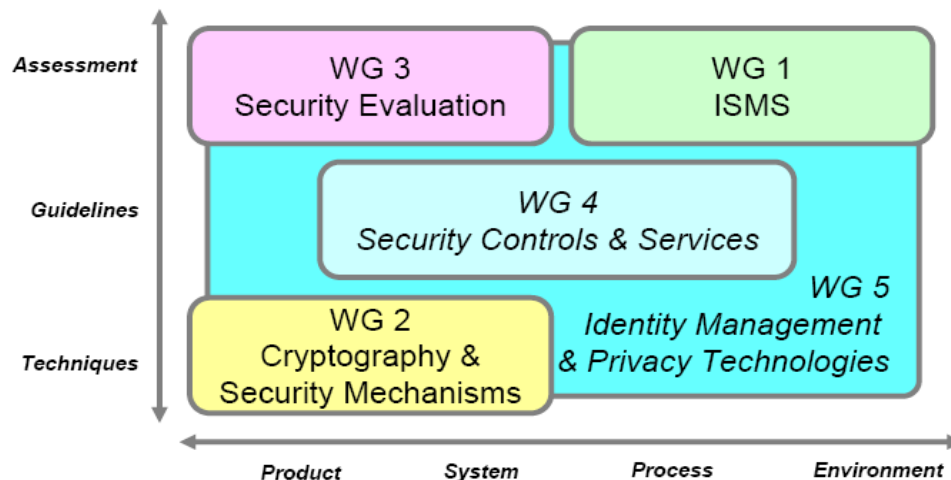
Contents

- Biometric Information Security Standards in ISO / IEC JTC 1 / SC27
- Biometric Information Security Standards in ITU-T SG17/ Q.9
- Telebiometric Authentication
 - One time template
 - Biometric HSM(Hardware Security Module)

Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

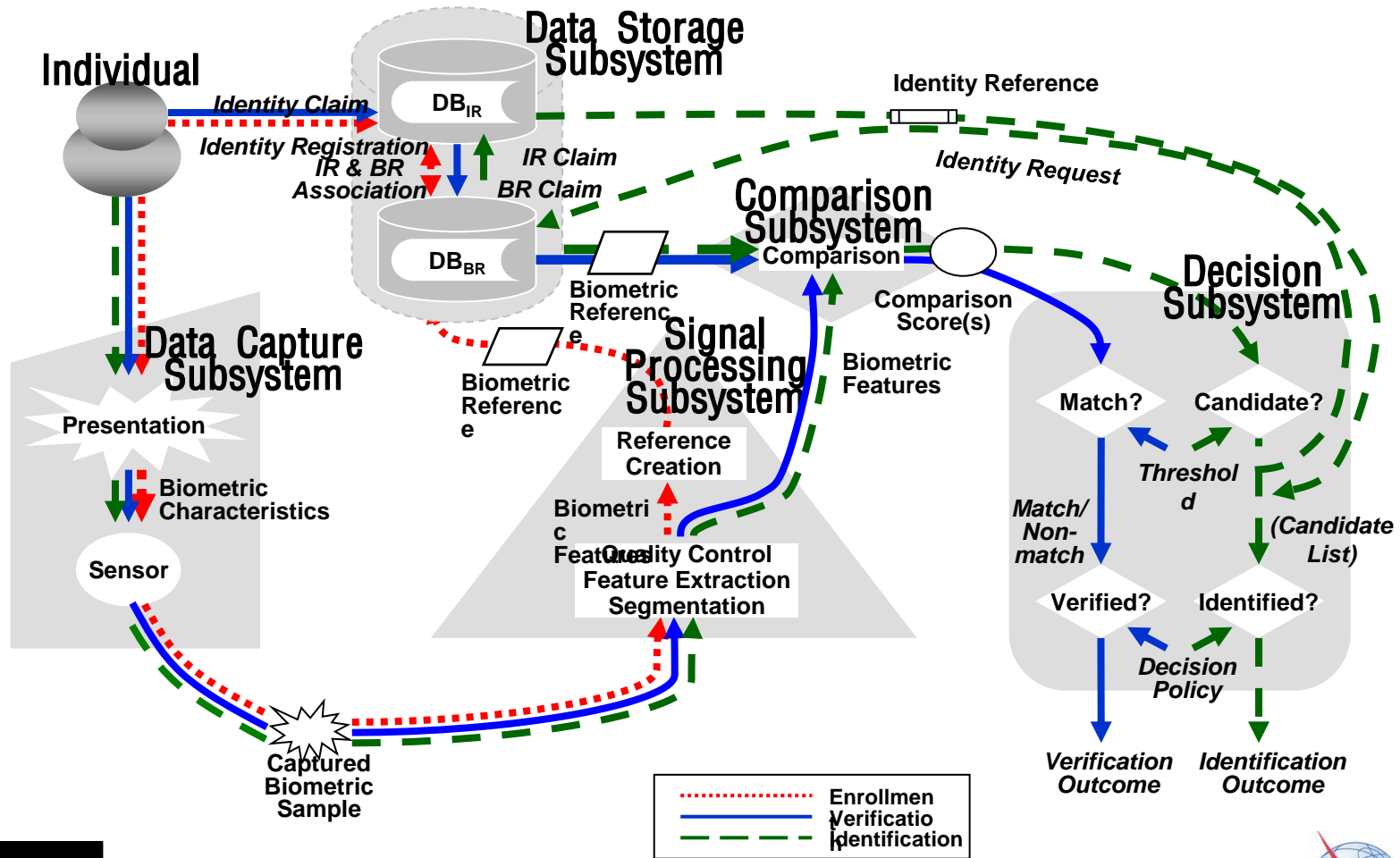
■ ISO/IEC JTC 1/SC 27 Biometrics Works

Project Number	Status	Title
19792/WG3	IS(2009)	Security evaluation of biometrics
24761/WG5	IS(2009)	Authentication context for biometrics
24745/WG5	FDIS	Biometric information protection



Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

■ ISO/IEC 24745 “Biometric Information Protection”

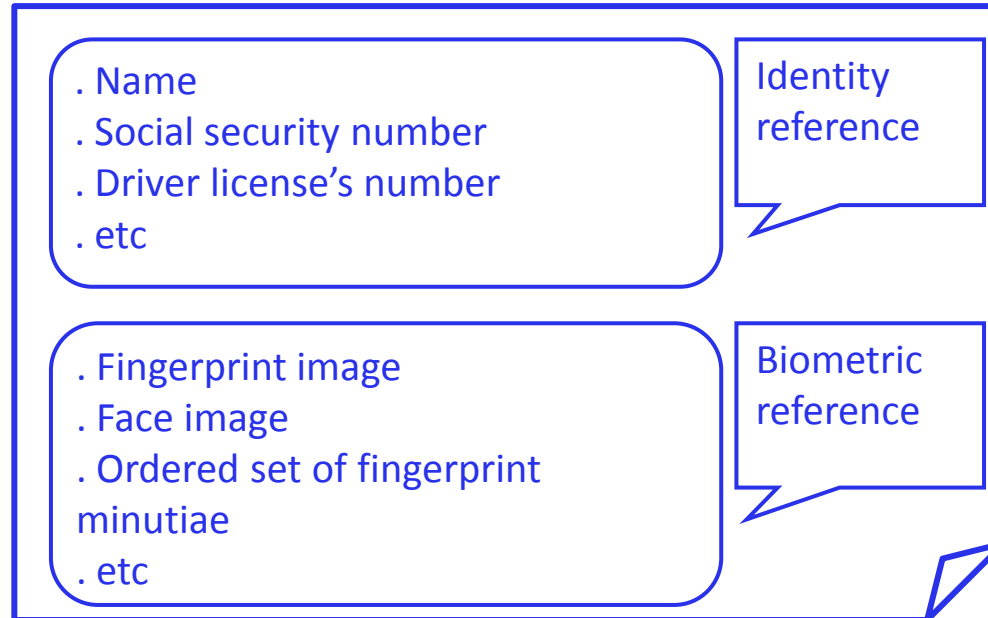


Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

- ISO/IEC 24745 “Biometric Information Protection”
 - analysis of the threats to and countermeasures inherent in biometric system application models;
 - security requirements for securely binding a biometric reference with an identity reference
 - biometric system application models with different scenarios for the storage of biometric references and comparison; and
 - guidance on the protection of an individual’s privacy

Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

- Biometric reference: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison
- Identity reference: an identifier with a value that remains the same for the duration of the existence of the entity in a domain

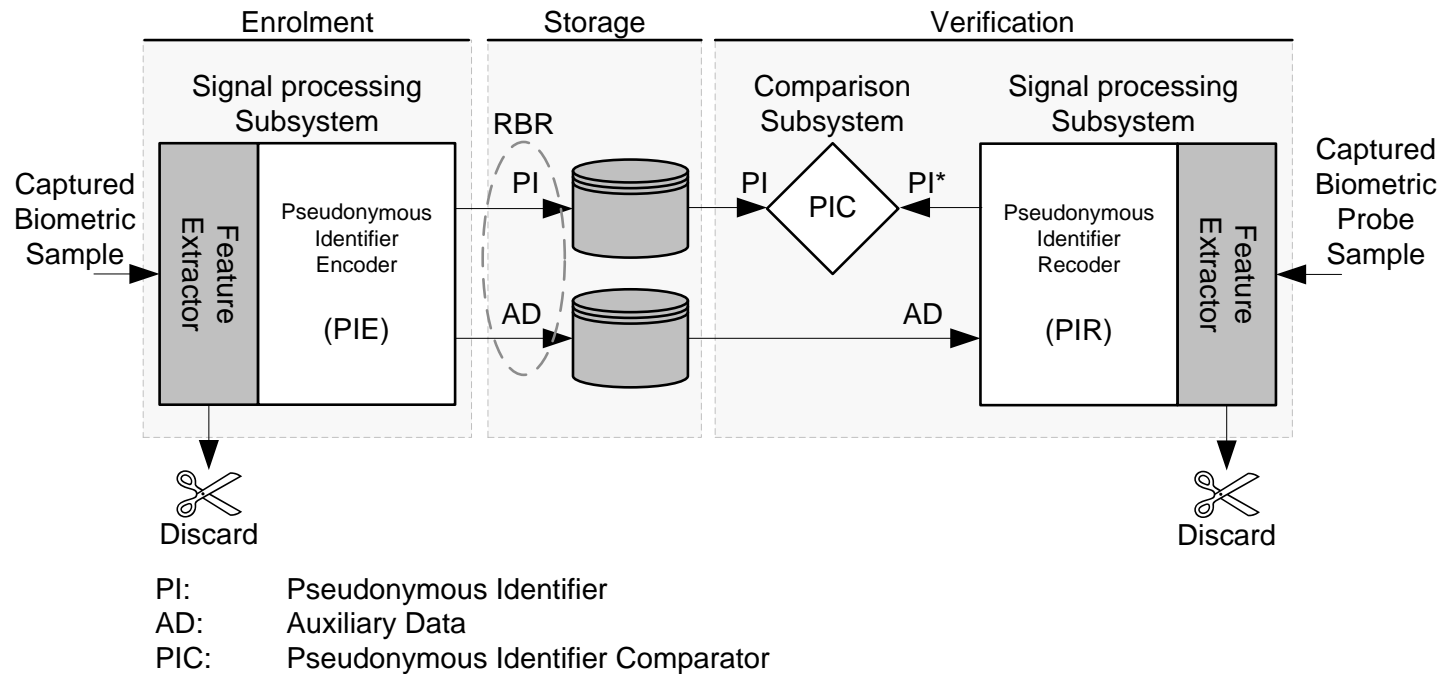


Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

- Security Requirements for biometric systems
 - **Confidentiality:** protect biometric information against unauthorized access or disclosure
 - **Integrity:** safeguard the accuracy and completeness of biometric information
 - **Renewability :** property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples while not revealing information about the original reference.
 - **revocability:** ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference

Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

■ Architecture for renewable biometric



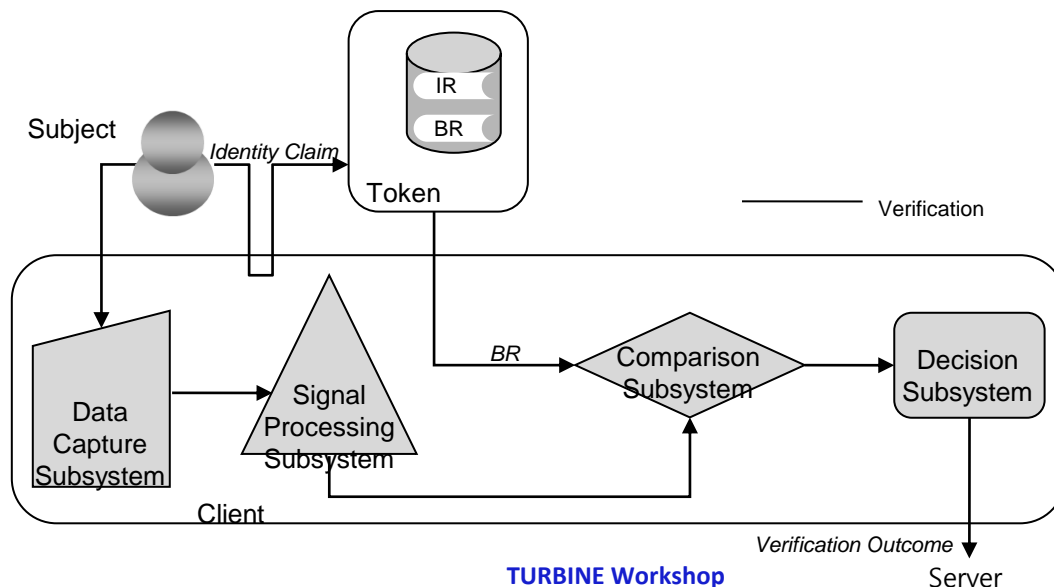
Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

- Biometric information privacy requirements and guidelines
 - **Irreversibility:** biometric data shall be processed by irreversible transforms before storage
 - > Encryption/pseudonymous identifier
 - **Unlinkability:** Stored biometric references should not be linkable across applications or databases.
 - >Encryption with different keys/diversification process
 - **Confidentiality:** To protect biometric references against access by an unauthorized outsider resulting in a privacy risk, biometric references shall be kept confidential.
 - > Data separation/encryption of biometric references

Biometric Information Security Standards in ISO/IEC JTC 1/SC 27

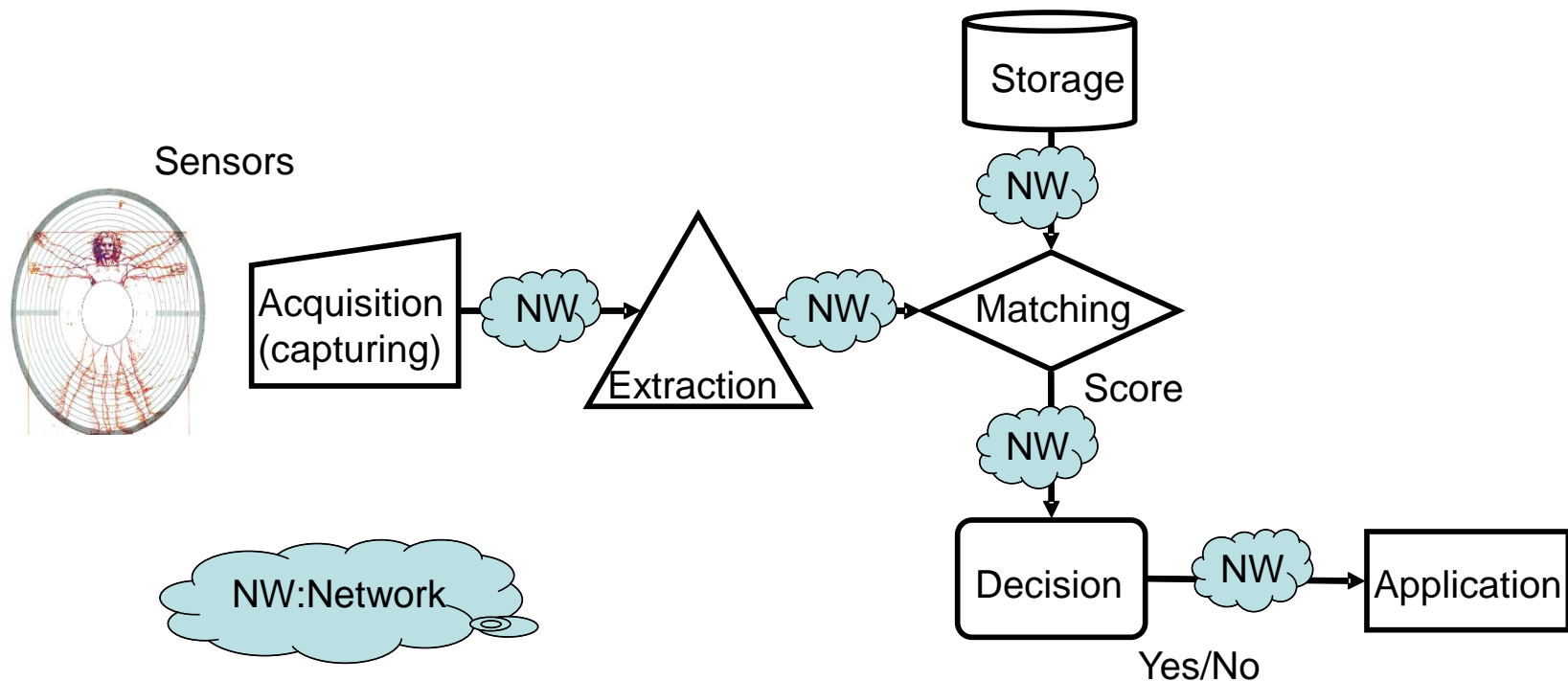
■ Application Models: Security and privacy issues

		Storage			
		Server	Client	Token	Distributed
Comparison	Server	A		B	G
	Client	C	D	E	H
	Token			F	



Biometric Information Security Standards in ITU-T SG17/Q.9

■ Functional blocks of SG17/Q.9



Biometric Information Security Standards in ITU-T SG17/Q.9

- Scope of SG17/Q.9 includes:
 - How should security countermeasures be assessed for particular applications of telebiometrics?
 - How can identification and authentication of users be improved by the use of interoperable models for safe and secure telebiometric methods?
 - What mechanisms need to be supported to ensure safe and secure manipulation of biometric data in any application of telebiometrics, e.g., telemedicine or telehealth?

Biometric Information Security Standards in ITU-T SG17/Q.9

■ Published standards include:

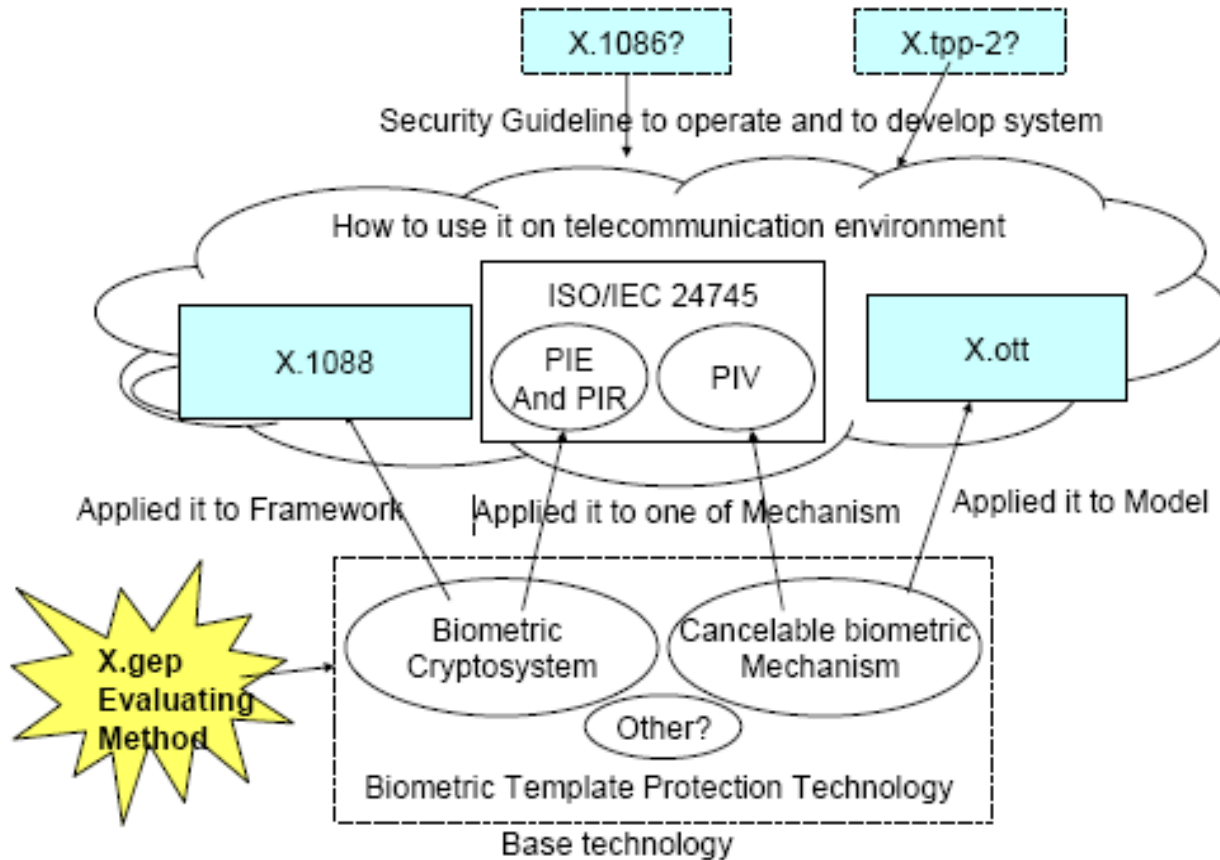
- X.1086 – Telebiometrics Protection Procedures-Part1: A guideline of technical and managerial countermeasures for biometric data security.
- X.1088 – Telebiometrics Digital Key: A framework for biometric digital key generation and protection.
- X.1089 – Telebiometrics Authentication Infrastructure.

■ Ongoing standards include:

- X.1098 – A guideline for evaluating telebiometric template protection techniques.
- X.1090 – Authentication framework with one-time telebiometric template.

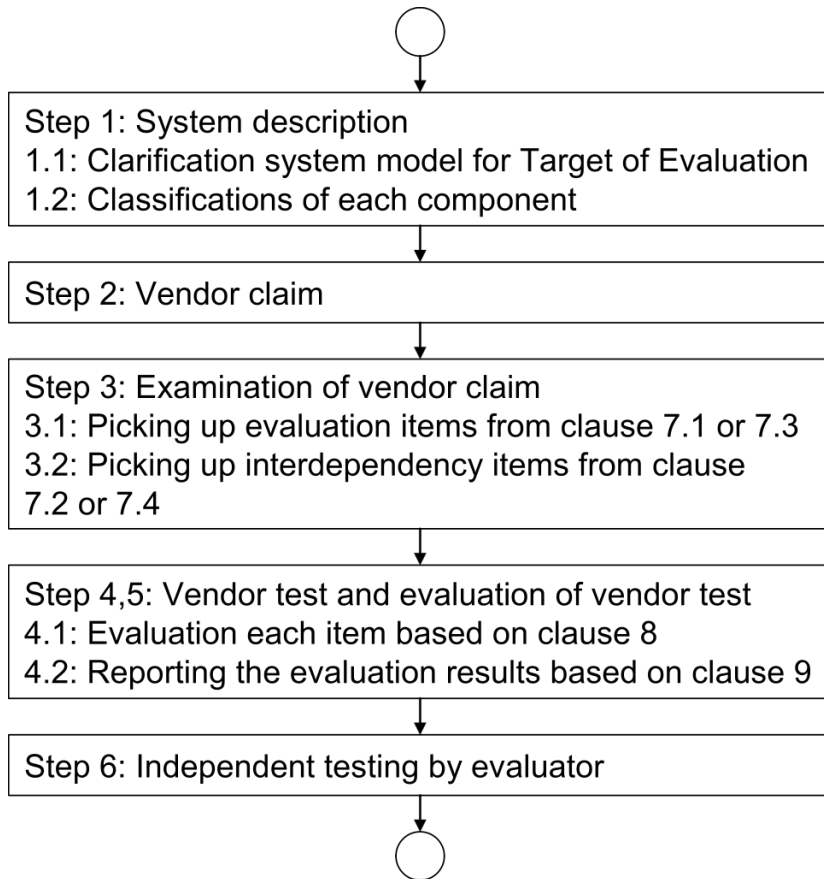
Biometric Information Security Standards in ITU-T SG17/Q.9

- X.1098 : A guideline for evaluating telebiometric template protection techniques



Biometric Information Security Standards in ITU-T SG17/Q.9

X.1098 : A guideline for evaluating telebiometric template protection techniques



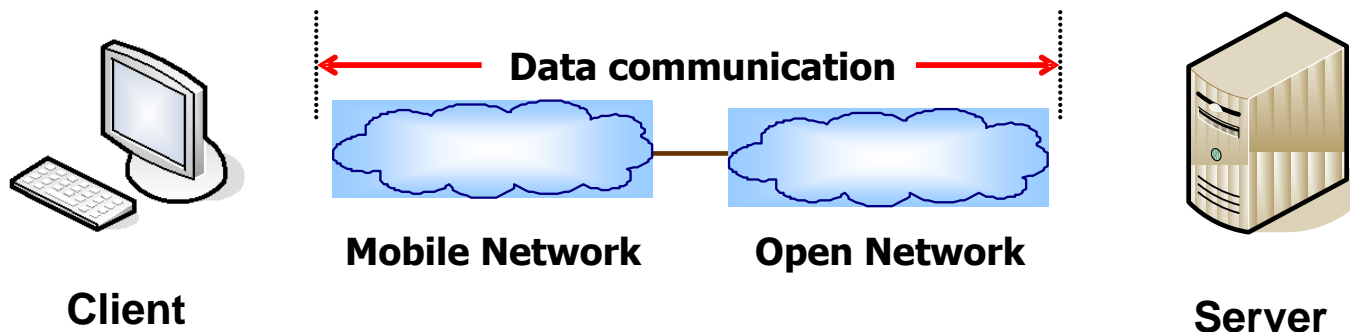
Flow diagram of evaluation steps for
biometric template protection techniques
Based on ISO/IEC 19792

The protection capabilities of biometric template protection techniques have dependencies of the accuracy of comparison

- ISO/IEC 19792 provides steps for “Testing security-relevant error rates”.
- The evaluation target of this draft Recommendation is a relationship of **protection capability** and **error rates** mainly
- This draft Recommendation provides extended detail evaluation step based on ISO/IEC 19792 for biometric template protection techniques

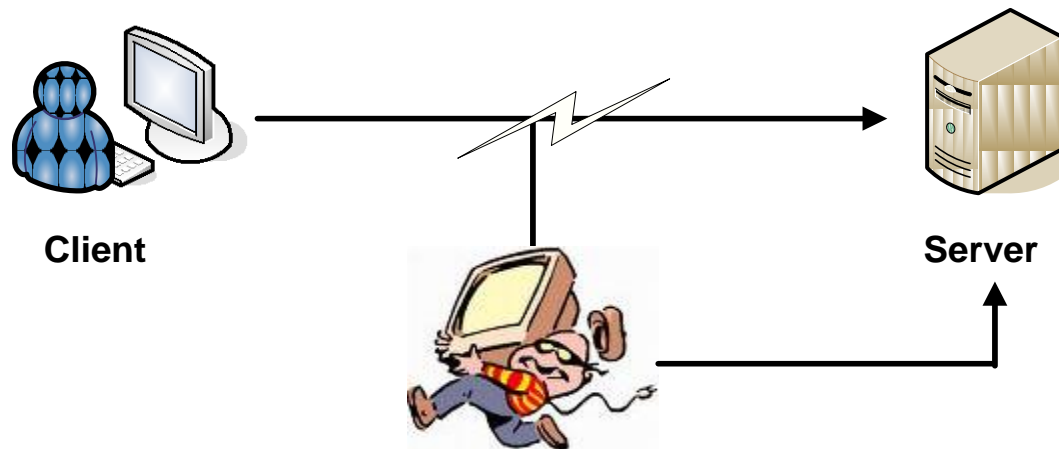
Telebiometric Authentication: One time template

- X.1090 : Authentication framework with one-time telebiometric template
 - Open Network Environment
 - Client/Server
 - On-line Authentication
 - Passwords/Templates are transmitted from a client to a server.



Telebiometric Authentication: One time template

- X.1090 : Authentication framework with one-time telebiometric template
 - User authentication in network: static passwords
 - The same passwords for every authentication.
 - Replay Attack: Copy and re-transmit to a server
 - Encrypted/Hashed passwords cannot prevent ‘Replay Attacks’.



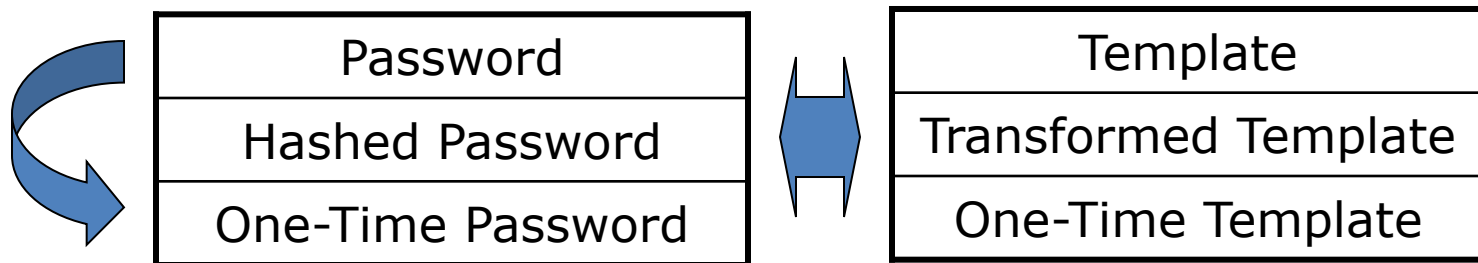
Telebiometric Authentication: One time template

- X.1090 : Authentication framework with one-time telebiometric template
 - Biometric Templates transmitted over Networks.
 - Biometric Templates \approx Static Passwords
 - Transformed templates (cancelable biometrics) cannot prevent 'Replay Attacks'



Telebiometric Authentication: One time template

- X.1090 : Authentication framework with one-time telebiometric template
 - A new password for each authentication.
 - An old one should be obsolete.
 - It is impossible to infer a new password from an old one.
 - Two-Factor Authentication
 - Password + Personal Token
 - A similar extension for biometrics like one-time passwords

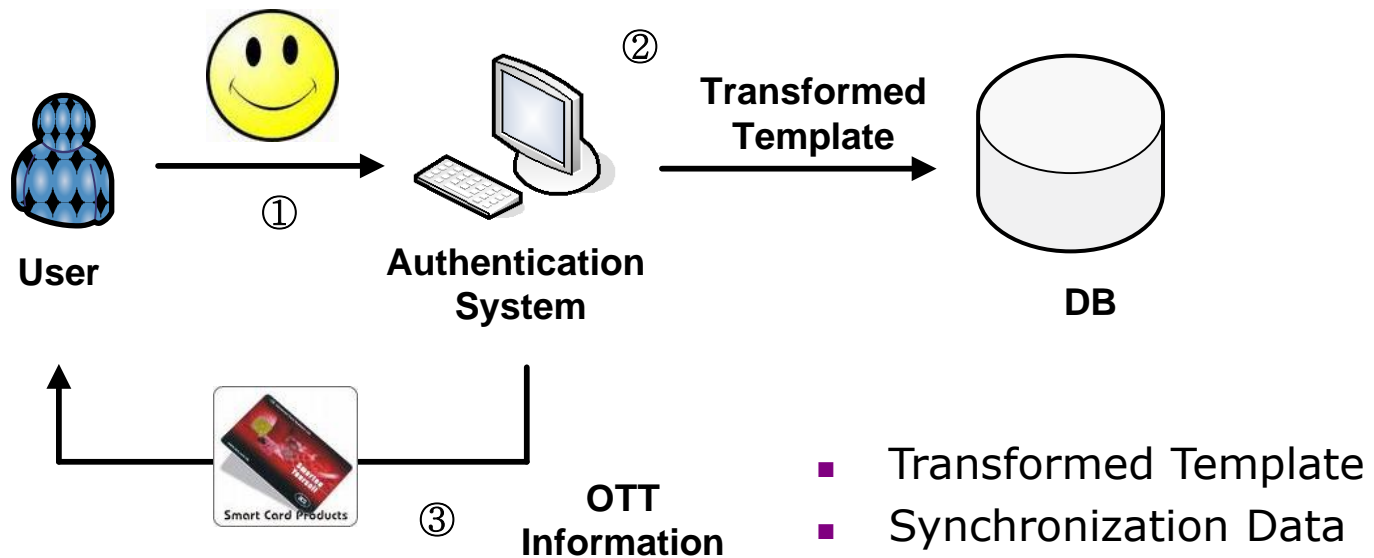


Telebiometric Authentication: One time template

- X.1090 : Authentication framework with one-time telebiometric template
 - Requirements of OTT in Open Networks.
 - Transformed Templates should be used for user-authentication and network transmission.
 - A new template should be used for each authentication.
 - Template matching should be performed in a transformed state.
 - It should be difficult to infer original templates from data transmitted over networks.
 - A user must provide both of his or her valid biometric information and personal token for positive authentication.
 - The loss of a user's personal token must not increase the possibility of false authentication.

Telebiometric Authentication: One time template

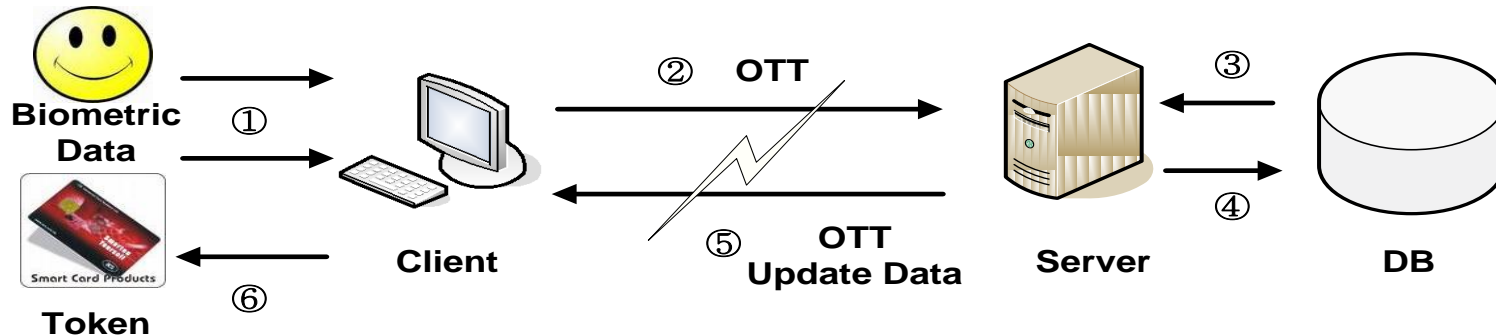
- X.1090 : Authentication framework with one-time telebiometric template



- Transform Information
- Synchronization Data

Telebiometric Authentication: One time template

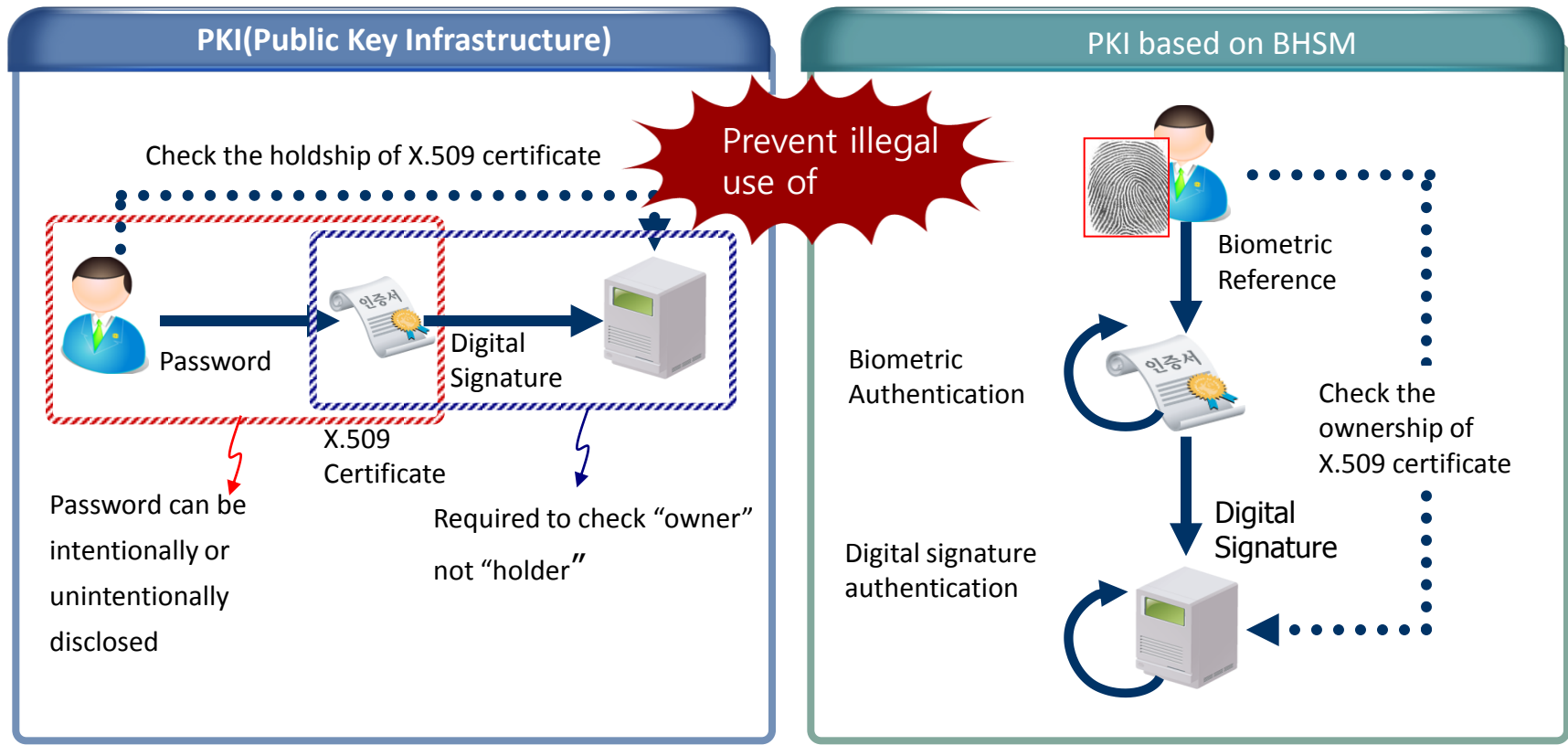
- X.1090 : Authentication framework with one-time telebiometric template



- A client sends a transformed template to a server
- A server performs matching using transformed templates.
- If a user is verified as a genuine,
 - A server generates a new transformed template.
 - A client updates OTT information.
- A new template is generated using new OTT information at next authentication.

Telebiometric Authentication: Biometric HSM(Hardware security Modue)

- X.bhsm: personal authentication framework for biometric HSM



Telebiometric Authentication: Biometric HSM(Hardware security Modue)

- X.bhsm: personal authentication framework for biometric HSM



www.unioncomm.co.kr



www.suprema.co.kr

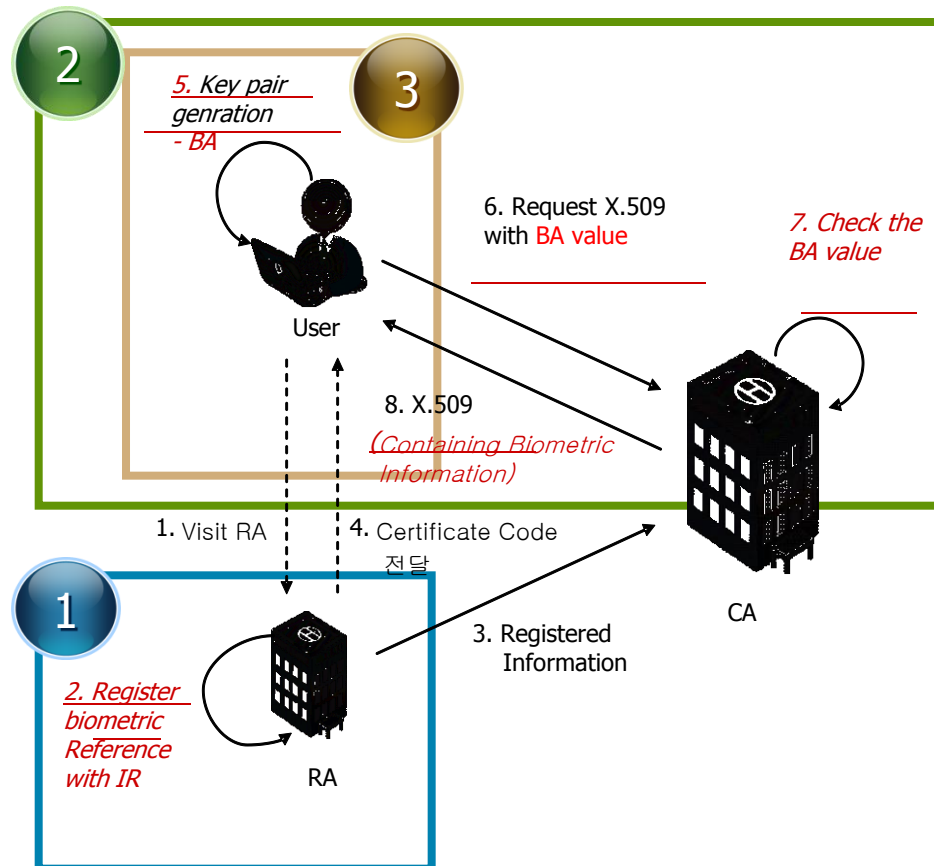


- A type of secure cryptoprocessor at managing digital keys in terms of digital signings and for providing strong authentication to access critical keys.
- Traditionally come in the form of smartcard or some other USB type security token that can be attached directly to general purpose computer.
- BHSM consists of HSM and biometric sensor

BHSMs for Korea on-line
e-procurement system

Telebiometric Authentication: Biometric HSM(Hardware security Modue)

- X.bhsm: personal authentication framework for biometric HSM



Telebiometric Authentication: Biometric HSM(Hardware security Modue)

- X.bhsm: personal authentication framework for biometric HSM

In the standard,

- What kinds of application models can be used for personal authentication?
- What are the countermeasures to protect biometric HSM from attacks?
- What are the cryptographic mechanisms for providing the integrity of biometric reference and secure binding it with private key belonging to X.509 certificate?

The scope of standard are:

- Definition of BHSM and their functions
- BHSM related security threats and countermeasures
- Application models for deployment of BHSM
- Security mechanisms for personal authentication operation of BHSM
- Privacy considerations in BHSM application

Concluding Remarks

- The requirements for supporting crypto-biometrics have been reflected in ISO/IEC JTC 1/SC27 24745 standard
- Several standards for telebiometric authentication have been established in ITU-T SG17/Q.9

High performing (in terms of recognition rate and protection capability) crypto-biometric techniques are requiring for daily life applications !!!

Thank for your attention!

Q & A