International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1088

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection

Recommendation ITU-T X.1088

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	**X.1080–X.1099**
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1088

Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection

Summary

Recommendation ITU-T X.1088 describes a framework for biometric digital key generation, protection from a biometric template with public key certificate and biometric certificate in order to provide cryptographic secure authentication and secure communication on open network environments. This Recommendation also describes the security requirements in biometric digital key generation and protection. The framework described in this Recommendation can be applied to the biometric encryption and digital signature.

Source

Recommendation ITU-T X.1088 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

Biometric authentication, biometric certificate, biometric digital key framework, public key certificate, telebiometrics.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Page

Recommendation ITU-T X.1088

Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection

1 Scope

A general framework of biometric digital key is required in order to provide enhanced cryptographic secure authentication and security on telebiometric system. This Recommendation specifies a framework for biometric digital key generation and protection using biometric template with public key certificate and biometric certificate in order to provide secure authentication process on open network environments. This Recommendation also describes the security requirements in biometric digital key generation and protection for providing biometric authentication and secure communication.

However, this Recommendation does not cover the methodology of biometric digital key generation in detail because many different kinds of mechanisms can be used for generating and deriving biometric digital key from biometric template. And it also does not specify the detailed telebiometric system mechanism on biometric digital key generation and protection, as many models or system architecture can be used on biometric digital key on open network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure*.

[ISO/IEC 9797-2] ISO/IEC 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31136>

[ISO/IEC 11770-4] ISO/IEC 11770-4:2006, *Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39723>

[ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44226>

[ISO/IEC 14888-3] ISO/IEC 14888-3:2006, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based*

mechanisms.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43656>

[ISO/IEC 17799] ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612>

[ISO/IEC 18031] ISO/IEC 18031:2005, *Information technology – Security techniques – Random bit generation*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30816>

[ISO/IEC 18032] ISO/IEC 18032:2005, *Information technology – Security techniques – Prime number generation*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30817>

[ISO/IEC 18033-1] ISO/IEC 18033-1:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: General*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37970>

[ISO/IEC 19784-1] ISO/IEC 19784-1:2006, *Information technology – Biometric application programming interface – Part 1: BioAPI specification*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33922>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric [b-ISO/IEC 19785-1]: Pertaining to the field of biometrics.

NOTE – "biometric" should never be used as a noun.

3.1.2 biometrics [b-ISO/IEC 19785-1]: Automated recognition of individuals based on their behavioural and biological characteristics.

3.1.3 biometrics data [b-ISO/IEC 19785-1]: A biometric sample at any stage of processing, biometric reference, biometric feature or biometric property.

3.1.4 biometric authentication [b-ISO 19092]: Process of confirming an individual's identity, either by verification or by identification.

3.1.5 biometric identification [b-ISO 19092]: One-to-many process of comparing a submitted biometric sample against some or all enrolled reference templates to determine an individual's identity.

3.1.6 biometric sample [b-ISO/IEC 19785-1]: Information obtained from a biometric device, either directly or after further processing.

3.1.7 biometric template [ISO/IEC 19784-1]: A biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison.

3.1.8 biometric verification [b-ISO 19092]: Process of comparing a match template against reference based on a claimed identity (e.g., user ID, account number).

3.1.9 capture [b-ISO 19092]: Acquisition of a biometric sample.

3.1.10 enrolment [b-ISO 19092]: Process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person.

3.1.11 extraction [b-ISO 19092]: Process of converting raw biometric data into processed biometric for use in template comparison or reference template creation.

3.1.12 registration [b-ISO 19092]: Process in which a person shall prove their identity by presenting credentials to the biometric service provider before being allowed to enroll, and assigns an electronic identifier.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 biometric capture device: Device that collects a signal from a biometric characteristic and converts it to a biometric sample.

3.2.2 biometric capture process: Process of collecting or attempting to collect a signal from a biometric characteristic and converting it to a biometric sample.

3.2.3 biometric certificate: A data structure binding the user's identity and biometric feature and digital signed by the certificate authority which issued it.

3.2.4 biometric certificate authority: An entity, responsible for the issuance of biometric certificate.

3.2.5 biometric database: Collection of data organized according to a conceptual structure describing the characteristics of those data and the relationship among their corresponding entities, supporting one or more applications.

3.2.6 biometric digital signature: Digital signature function that performs a signature generation using private key on biometric message.

3.2.7 biometric encryption: Cryptographic encoding function that performs a cryptographic secure encoding and decoding using public key on biometric message.

3.2.8 client: Client terminal provides a biometric function for telecommunication service applications.

3.2.9 user: The receiver of the telecommunication service using the client.

3.2.10 verifier: Service provider based on a biometric authentication on telecommunication environments.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
BC	Biometric Certificate
BCA	Biometric Certificate Authority
BioAPI	Biometric Application Programming Interface
BSP	Biometric Service Provider
CA	Certificate Authority
CBEFF	Common Biometric Exchange Formats Framework
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
MD5	Message Digest 5
PKC	Public Key Cryptography

PKI	Public Key Infrastructure
SHA-1	Secure Hash Algorithm 1
TTP	Trusted Third Party
USB	Universal Serial Bus

5 Conventions

None.

6 Biometric digital key

6.1 Biometric cryptosystem

Biometrics is about measuring unique personal features, such as a subject's voice, fingerprint, or iris. It has the potential to identify individuals with a high degree of assurance, thus providing a foundation for trust. Cryptography, on the other hand, concerns itself with the projection of trust: with taking trust from where it exists to where it is needed.

The biometric-cryptosystem, which is a combination of biometrics and cryptography, is a very promising technique. In a cryptosystem, its security is determined by the security of the key. A user's identity must be authenticated whenever he wants to use the key. Because cryptographic keys are long and random, they are difficult to memorize. As a result, the cryptographic keys also can be stored somewhere (for example, on a computer or a smart card) and released by using some alternative authentication (e.g., password) mechanism, that is, upon assuring that they are being released to the authorized users only.

In order to guarantee the security of information and services, entity authentication and secure communication systems also should be considered as an important component in telebiometrics environments. In the real world, PKC-based authentication framework is the most widely used telecommunication security model and mechanism.

However, the existing PKC-based framework requires the users to remember or preserve their secret information securely, such as cryptographic private key. So, there must be a more secure and convenient method to generate digital key from each user's biometric data.

Therefore, biometrics-based authentication and encryption methods can be more powerful alternative methods than the existing ones, depending on the uniqueness and non-repudiation properties of biometric characteristic. So, this Recommendation describes a biometric digital key framework to providing secure authentication and encryption service in the telebiometric system. The following questions must be taken into account:

a) how to generate the biometric-based cryptographic key (symmetric and asymmetric) with biometric template; and

b) how to protect the key and stably extract the key accurately.

6.2 Model of biometric digital key

The methods of combination of key and biometrics determine the applicable models. Generally, there are two models in the biometric-cryptosystem.

6.2.1 Biometric key binding/generation

In this model, biometrics and the key are merged in a deep level and there is no 'naked' template. So this model has a secure level than the first model. Though it has a lower performance than the first one at present, the concept is rather promising.

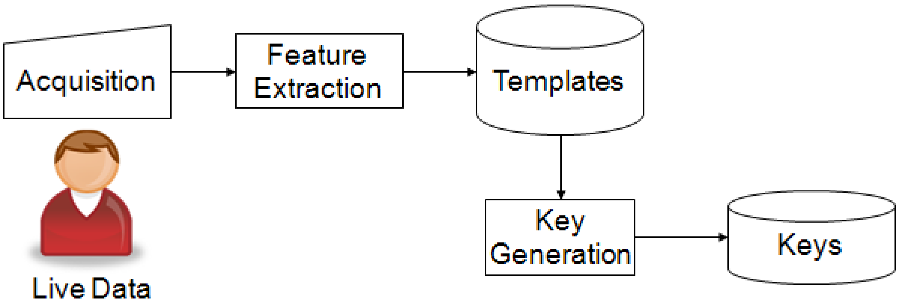

Figure 1 – Biometric key binding/generation model

There are also two ways to bind/generate the cryptographic key.

a) Biometric-key generation: Biometric data are directly mapped into a unique and repeatable binary string, and then are transformed into a cryptographic key. The most attractive point is that no biometric template would be needed to store. But these methods are not flexible, for biometric characteristics are unique and permanent and expected to generate a unique key, but in different application scenarios, a user possibly wants to use a different key. The hardest problem of this model is that the biometric data of a person vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition biometric capture device, and (in some cases) variations in the traits due to various pathophysiological phenomena. It cannot be guaranteed to generate the same, unique key every time from different biometric samples.

b) Biometric-key binding/restoring: A given cryptographic key is bound with the biometric template, and the template should be stored in some safe way. The system will restore/regenerate the same key with the safe template and genuine query sample. The "safe" template implies that the template does not leak any information about the "origin" biometric template and the given key. These schemes have some advantages compared with the first methods because the key is conveniently allocated by the system, and there is a "hidden" matching process in the key restoring/regeneration process.

6.2.2 Biometric key release

In this model, biometrics and cryptographic system are separate. A user can be authenticated in a traditional biometric system. And when he/she is verified, the system fetches the key from a secure position, such as a server or a smart card. This model is simple. But it also has some weaknesses on security, since the smart card could be lost, and the server could possibly be broken, which would compromise the security of the key.

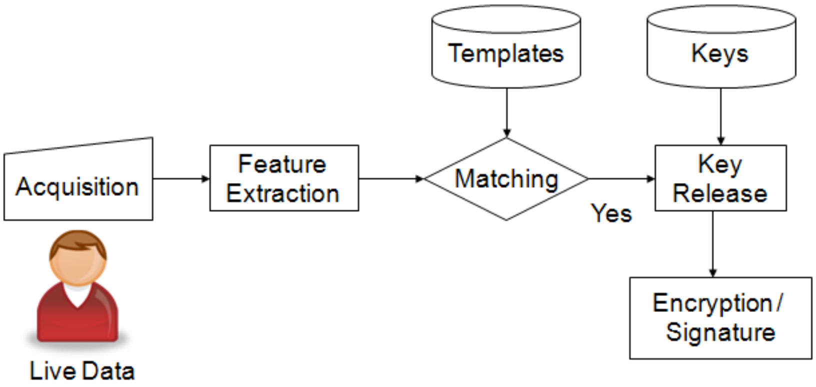

Figure 2 – Biometric key release model

7 Biometric digital key framework

7.1 Framework overview

A user's biometric template stored by the BCA can be used for identification, and it also can be used to generate private secret data, such as biometric digital key. Therefore, a common digital key generation and protection framework is required, using a biometric template that is incorporated with the existing cryptographic cipher mechanism, such as [ISO/IEC 18033-1] and [b-ISO/IEC 18033-2] for enhancing security and authentication. Additionally, security requirements must be considered in biometric digital key generation and digital signature framework, with both the public key certificate and the biometric certificate.

This Recommendation describes a 'Telebiometrics Digital Key Framework' for biometric digital key generation and protection to implement biometric identity authentication, and to provide a secure communication combined with biometric data. The framework includes:

– Biometric digital key generation/protection model and framework

– Biometric digital key extraction model and framework

– Security requirements in biometric digital key generation and protection

– Application such as biometric encryption and simplified biometric digital signature based on biometric digital key.

7.2 Prerequisites

This Recommendation has the following prerequisites:

– A trusted third party (TTP), such as certificate authority (CA), is required to authenticate a user's public key and to issue a certificate to each user.

– An additional TTP such as biometric certificate authority (BCA), is required to authenticate a user-registered biometric reference information, and to digitally sign that information using the biometric certificate in [ITU-T X.1089], and then it can be issued by a biometric certificate to each user.

– BCA (biometric certificate authority) manages the users' biometric templates securely (as defined in [ITU-T X.1089]), and the BCA must protect and prevent the subject's biometric data from leaking out. The CA manages the user's public key.

– Live data is a user's biometric data (biometric sample) that represents the user's identity input from the biometric capture device.

– A user's secret data (personal secret) is input by the user. By using it, it is possible to generate a cryptographic secure biometric digital key.

– Biometric image is captured through biometric capture devices, such as fingerprint sensor. The captured image is transformed into digital image format, such as jpeg, gif, etc. The digital image (biometric reference) is then stored in the user's local storage, such as a hard disk.

– The matching function verifies the user's identity by comparing the user's captured image with the biometric template in the BCA.

7.3 Biometric digital key generation and protection framework

To generate biometrics digital key from biometric template requires solving operational tasks, as follows:

1) Model of biometric digital key,

2) Biometric digital key generation,

3) Biometric digital key protection and extraction,

4) Biometric digital signature for secure communication and user authentication, and

5) Security requirements on biometric digital key.

This Recommendation describes a framework for a biometric digital key generation and protection with CA for PKC.

Figure 3 describes a framework for biometric digital key generation and protection. Biometric templates are processed-measurement feature vectors. Biometrics of different individuals are independent realizations of a random process that is equal for all individuals. Biometric cryptography can be classified into 'key derivation (generation)' and 'signature generation and verification' framework. The key derivation schemes imply that the signature key is derived directly from biometrics, while the key authentication schemes mean that the signature key is accessed by biometric authentication.

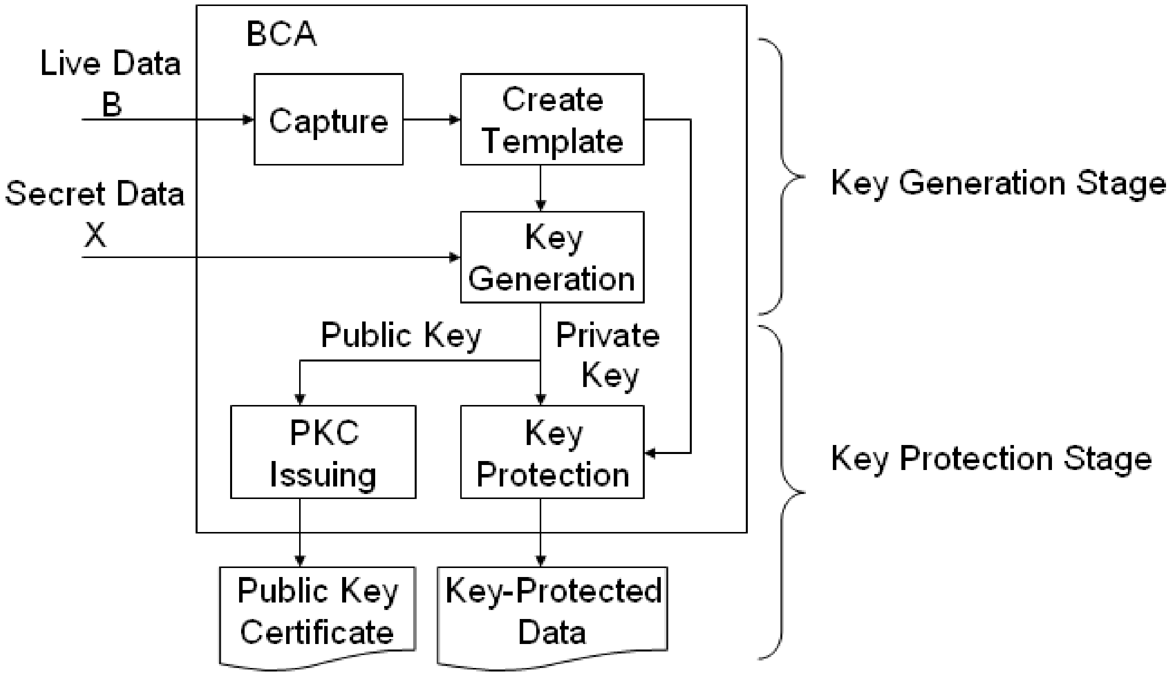

Figure 3 – Biometric digital key generation and protection framework

7.3.1 Input live data

Live data mean a user's biometric data and sample. A biometric data is a measurement of a person's behaviour or physiology. Based on this live data, a biometric key generation module can extract the biometric secret as algorithmically interpretable representations (e.g., a set of signals). The biometric key generation module typically applies statistical functions, or a set of features to the representations and uses the output to either derive or lock a cryptographic key.

7.3.2 Input secret data

It encompasses any secure information intended to be used for key derivation purposes. This information is specified with respect to one user and includes any biometric, template, or key, other than those associated with the user in question. It could also include any other information about the environment that might leak information about the biometric or results of using the key.

Commonly, secret data may be the n-bit secret identity, which is the practice of hiding a person's identity so the actual identity of the person is not known or suspected. Secret data must have random primitive. Random number generator specified in [ISO/IEC 18031] can be used in this secret data, and it is a computational or physical biometric capture device designed to generate a sequence of numbers or symbols that lack any pattern, i.e., appear random.

7.3.3 Capture biometric data

This biometric capturing process captures the biometric information from the claimant, and converts the information to the acquired biometric sample. The acquired biometric sample is transmitted to the signal subprocess. As BCA (biometric certificate authority) manages the users' biometric certificates, the biometric certificate contains the user's certified biometric template. In the model, the biometric certificate in the BCA is downloaded, and the user's biometric template in it is stored in the local storage. User authentication is performed by comparing the user's captured image in the previous capturing module with the biometric template in the BC (biometric certificate). If user authentication is successful, the following key generation step will be done; otherwise, the key generation mechanism is terminated.

Therefore, this is a sensing and input module with feature enhancement function. In fingerprint, ridge regions in the image are identified and normalized. In detail ridge orientations are determined, local ridge frequencies are calculated, and then contextual filters with the appropriate orientation and frequency are applied.

After the biometric capturing process, signal processing will be done. This process receives the acquired biometric sample from the data capture process, transforms the acquired biometric sample into the processed biometric sample of the form required by the comparison subprocess. The processed biometric sample is transmitted to the comparison subprocess.

7.3.4 Create biometric template

A template is any piece of information that is stored in the system for the purpose of regenerating the cryptographic key. Templates are generally created during an enrollment process and stored so that a user can easily recreate his or her key. For all practical purposes, templates must be considered publicly available. Note that this assumption implies that more standard biometric templates, which are typically employed for authentication purposes and are simply the encoding of a biometric, cannot be used securely in this setting. After capturing, biometric template is created from the biometric raw data on BioAPI modules specified in [ISO/IEC 19784-1] by using biometric capturing device. The noise on the captured image is reduced through image processing. Then the set of minutiae is extracted from the enhanced image. Finally, the biometric template is made from location and angle values of minutiae set.

7.3.5 Biometric digital key generation

It is a cryptographic key that is derived from one or more biometric samples during an enrollment phase. The key may later be regenerated using another biometric sample that is "close" to the original samples, and the template that was also the output during enrollment.

The private key is generated by either using MAC function specified in [ISO/IEC 9797-2], or a hash function such as MD5 or SHA-1 in the biometric template with the personal secret. Based on this secret private key information generated from live data and secret value, the existing public key cryptosystem for digital signature specified in [ISO/IEC 14888-1], or user-specific public key generation algorithm, can be used to generate the public key. Then this public key information can be issued as a public key certificate specified in [ITU-T X.509] by trusted third party, and the private key information can be stored as a protected data form.

If this private key generation module uses only the biometric template for private key generation, it always has to generate the same key since the biometric data is unique. Moreover, if the private key is disclosed, the user's biometric data cannot be used any more. Therefore, in order to cancel and regenerate the private key, the user's personal secret is also required for the generation of the private key. One reason for using the personal secret value is to make digital keys by adjusting the personal secret value. The biometric template from the BCA cannot be changed, since the template is unique information. Another reason for using the personal secret value is to make keys available, even if the biometric template is compromised. By using the personal secret value, various keys can be made from the same biometric template.

7.3.6 Biometric digital key protection

The private key is stored in the local storage. Disclosure of the private key is very dangerous. Therefore, the private key should not be stored in plain format. The private key would be concealed after shuffling with the user's biometric template on the personal secret data value.

Biometric template stores the subject's biometric feature data, which is vital to the overall system security and individual security. Once the biometric data is leaked out, the individual authentication is confronted with threat, and individual biometric authentication in other applications may be confronted with security vulnerability, too. So, it is most important to protect the biometric template. Private secret data should be stored in protected storage as a protected form, using cryptographic methods specified in [ISO/IEC 18033-1] and protected by using key management method and framework on weak secret such, as biometric specified in [ISO/IEC 11770-4].

The confidentiality of biometric private keys can be assured by using a key protection mechanism. Biometric private keys as well as biometric templates, are a type of individual private data. The certificate users have both the right and responsibility to delete their biometric private keys from the certificate database when the biometric certificate is revoked.

Because cryptographic keys are long and random, they are difficult to memorize. As a result, the cryptographic keys are stored somewhere (for example, on a computer or a smart card) and released based on some alternative authentication (e.g., password) mechanism, that is, upon assuring that they are being released to the authorized users only. Most passwords are so simple that they can be easily guessed (especially based on social engineering methods) or cracked, which brings threat to the whole network.

So there must be a more secure and convenient method to generate and store biometric digital key from each user's biometric data in the environment, where high security or special applications are needed. Key-protected data can then be used for storing the generated biometric digital key securely.

7.3.7 Public key certificate issuing

For interworking with X.500 service, the generated biometric public key should be certified by CA defined in [ITU-T X.1084] and [ITU-T X.509]. The [ITU-T X.509] certificate should contain a user's public key, identification and biometric information.

7.4 Biometric encryption and signature framework with biometric digital key

7.4.1 Biometric encryption framework with biometric digital key

Biometric encryption is a technology which accomplishes biometric authentication without storing any biometric data. It uses general encryption mechanism specified in [ISO/IEC 18033-1] to generate unique encryption keys dynamically from the biometric data of each user. As with other encryption-based authentication techniques specified in [ISO/IEC 18033-1], biometric encryption can either store a hash value of the key data on the server and use that for comparison (as with password authentication), or it can use a PKI authentication scheme, with the generated key data as the private key and the public key stored on the server. In either case, actual key data is not available on the server (biometric data is concealed), so these methods are able to maintain a strong protection of privacy while authenticating users.

The main objective of the biometric encryption is to provide privacy and confidentiality using a biometric digital key (a private and a public key pairs). In the biometric encryption systems, each client receives a public key from CA. Any entity wishing to securely send a message to the receiver obtains an authentic copy of the public key, and then uses the encryption function specified in [ISO/IEC 18033-1]. To decrypt, the receiver applies decryption transformation to obtain the original message after the biometric authentication process. Common biometric encryption mechanism with digital key is also possible. The biometric encryption framework with the biometric digital key is as shown in Figure 4.

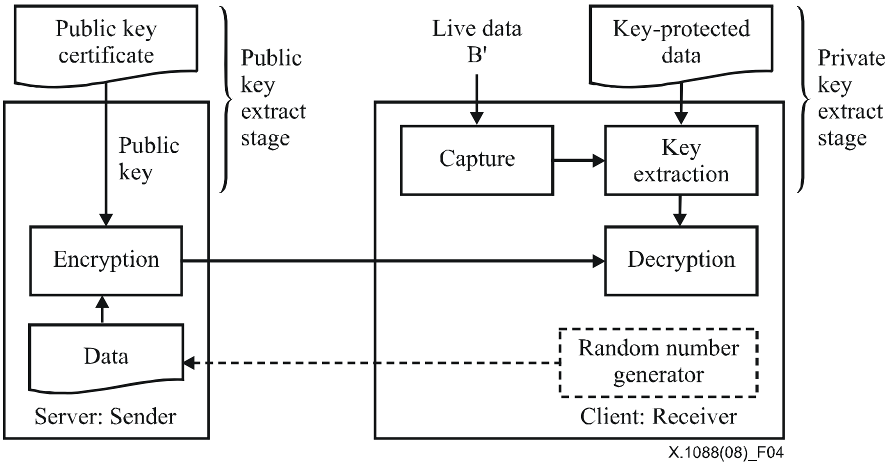

Figure 4 – Biometric encryption framework with biometric digital key

User authentication is performed at first the same as in the key generation mechanism. The user cannot disguise himself or herself as another for extracting the private key stored by a protected data. This basic requirement should be considered in the key extraction mechanism based on biometric data. The private key is extracted from the key-protected data by using, the 'key extracting' function with the biometric template.

7.4.2 Biometric digital signature framework with biometric digital key

Digital signature specified in [ISO/IEC 14888-1] is fast emerging technique as a viable information security solution, satisfying the objectives of data integrity, entity authentication, privacy, non-repudiation and certification. In this clause, a biometric digital signature generation framework is described using the proposed key generation/protection mechanisms in telebiometrics environment.

The signer gets the private key which is extracted from the key extraction mechanism. Then, the signer generates his (her) own digital signature on the message with the private key and sends it to the verifier.

The verifier gets the signer's public key from CA (certificate authority) and verifies the signature on the message with the public key. The signature verification mechanism is the same as that of the ordinary digital signature verification scheme specified in [ISO/IEC 14888-1] and [ISO/IEC 14888-3]. Entity at the receiver (server) can verify the digital signature by using the signer's public key and biometric certificate. The private key extracted from the previous module is used to sign the message. The message and the signature on it are sent to the verifier. The biometric digital signature framework with the biometric digital key is as shown in Figure 5.

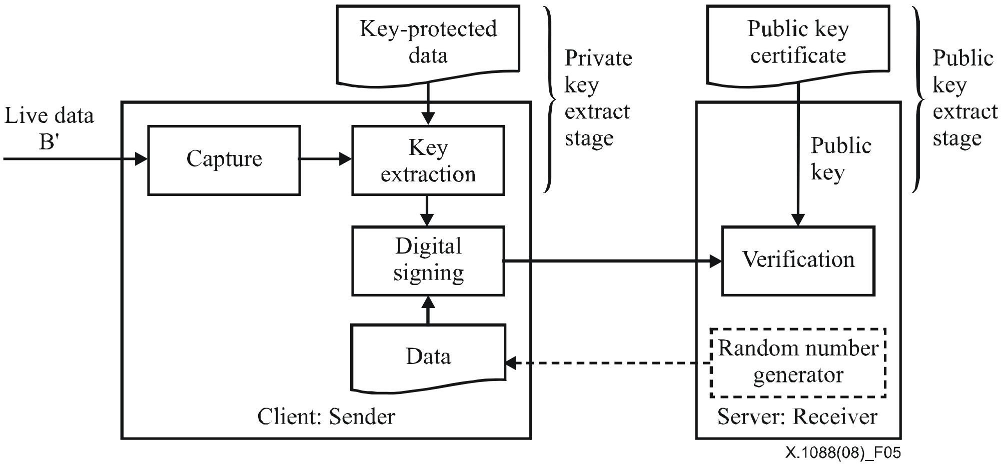

Figure 5 – Biometric digital signature framework with biometric digital key

8 Security requirements on biometric digital key framework

8.1 Basic security requirements

This clause describes the basic security requirements for biometric digital key framework in managing and securing biometric information for each application. The following basic requirements apply to all applications and environments, wherever biometric digital key is used:

a) Biometric digital key generation and protection mechanisms shall be in place to maintain the integrity of biometric data and authentication results between any two components, using the cryptographic mechanisms, such as a digital signature and verification specified in [ISO/IEC 14888-1] and [ISO/IEC 14888-3].

b) If desired, biometric digital key generation and protection mechanisms may be in place to ensure the confidentiality of the biometric data between any two components and within any component on the biometric system, using the cryptographic encryption/decryption.

The biometric functions necessary to construct the components described in [ITU-T X.1084] may be contained in a biometric service provider (BSP). The cryptographic functions necessary to protect biometric information may be contained in a separate cryptographic service provider (CSP), or within the BSP, an application layer, or an intermediate architectural layer.

In one possible implementation, the application submits a biometric function call to the architectural layer. The architectural layer insulates the BSP from the application and submits the biometric function call to the BSP. The BSP processes the biometric function call and manages all cryptography by communicating directly with the CSP. The call response is returned from the BSP to the architectural layer and then to the application. In an alternative approach, the application submits a biometric function call to the architectural layer. The architecture manages the cryptographic functions with the CSP and the biometric functions with the BSP. The call responses from the CSP and the BSP are returned to the application by the architectural layer. In a third approach, the application submits cryptographic function calls directly to the CSP and the biometric function calls directly to the BSP. No intermediate architecture is used. The call responses from the CSP and the BSP are returned directly to the application.

8.2 Security requirements on biometric digital key generation

8.2.1 Basic requirements on biometric digital key generation

This clause describes the basic security requirements for biometric key generation based on the biometric digital key framework.

a) The biometric digital key (public/private key) can be created by using a cryptographically secure hash function with both a user's biometric template and a personal secret value.

b) Therefore, the controlling organization should select a hash algorithm properly to standardize for the proposed key generation mechanism, such as MD5 and SHA-1, and should also consider how to concatenate a personal secret value and a biometric template.

c) Cryptographically secure hash functions should have the property that they are computationally infeasible to find another personal secret value that produces the same key.

d) The controlling organization should consider how to find secure big prime numbers against man-in-the-middle attack when the organization uses this biometric key as a key exchange mechanism in the biometric system.

8.2.2 Functional requirements on biometric digital key generation

This clause describes the functional security requirements for biometric key generation based on the biometric digital key framework. Based on the biometric key generation framework, public key and private key pairs can be generated.

a) The controlling organization maintains controls with the objective of providing reasonable assurance that the biometric digital key pairs are generated in accordance with industry standards.

b) Biometric digital key generation can use a random bit generator or pseudo-random bit generator, as specified in [ISO/IEC 18031].

c) When prime numbers are needed, key generation uses a prime number generator, as specified in [ISO/IEC 18032].

d) Biometric key generation takes place in a physically controlled environment.

e) Biometric key generation uses a key generation algorithm, as specified in an ISO (or equivalent national) standard.

Moreover, the following fundamentals should be considered in a biometric key generation framework:

a) The keys output by a biometric key generation appear random to any adversary who has access to auxiliary information and the template used to derive the key.

b) A user's biometric data used to make biometric key generation should satisfy the uniqueness property.

c) An adversary learns no useful information about a biometric given auxiliary information and the template used to derive the key.

d) An adversary learns no useful information about a biometric given auxiliary information, the template used to derive the key, and the key itself.

The controlling organization maintains controls with the objective of providing reasonable assurance that keys are used only for their intended functions in their intended locations. Cryptographic keys are generated and used solely for their intended purpose, which is specified and described during key generation, including:

a) Asymmetric key pairs for biometric data integrity and authentication of origin.

b) Asymmetric key pairs for biometric authentication of origin.

c) Asymmetric key pairs for biometric data confidentiality.

8.2.3 Requirements on biometric key length and backup

This clause describes the requirements for biometric key length and its backup requirements on the generated biometric digital key:

a) In case of a symmetric key, the key length should be as follows:
   - As cipher text under a key encryption key with at least the equivalent cryptographic strength of a double length DES key using triple DES, or the strength of AES;
   - As encrypted key fragments using dual control and split ownership, with the encryption used solely for that purpose, with at least the equivalent cryptographic strength of a double length DES key using triple DES, or the strength of AES;
   - As clear text that is directly injected into another secure cryptographic module, such as a key transportation biometric capture device using dual control; or
   - As symmetric key components under dual control and split knowledge.

b) In case of an asymmetric key, the key length should be as follows:
   - As a key public/private key length with at least the equivalent cryptographic strength of a RSA on biometric encryption and signature;

c) For key backup on biometric digital key, the requirements should be as follows:
   - If an asymmetric private key or symmetric key is backed up, it is stored and recovered by authorized personnel using dual control in a physically secured environment.
   - If an asymmetric private key or symmetric key is backed up, recovery of the key is conducted in the same secure schema used in the backup process, using dual control.
   - Procedures are in place to ensure that the integrity of the asymmetric private key or symmetric key is maintained throughout its life cycle.

8.3 Security requirements on biometric digital key protection

This clause describes the basic security requirements for biometric digital key framework in managing and securing biometric information for each application. The following basic requirements apply to all applications and environments, wherever biometric digital key is used.

In the biometric digital key protection framework, the following security requirement items should be considered:

a) Privacy protection of registered biometric key-protected data is essential.

b) Confidentiality of key-protected data is essential.

Additionally, a method should be provided to establish that safe data items, such as key-protected data, should be transferred through an integrity test module between biometric client/server. To do so, a specific key for message authentication code on key-protected data should be assigned. This may encode the acquired protected data with an assigned MAC key specified in [ISO/IEC 9797-2], and then be stored in the secure storage, such as smart card, protected device, etc. Detailed requirements will be as follows:

a) The biometric digital key must be stored as an encoded form using the personal secret data.

b) Non-encoded biometric digital key may enhance the risk of having their internal data exposed to an outside attacker, to be manipulated and/or analysed. Therefore, the biometric digital key protection mechanism can be provided to securely extract encoded biometric digital key by real-owner.

c) Access to a key-protected key must be limited to specific individuals with specific requirements, and the use and disclosure of biometric key-protected data should be clearly managed and supervised.

d) A multiple authentication method can be used for access to the key-protected data.

Unlike other general information, biometric key-protected data requires more sophisticated care and, therefore, they may need to be stored separately from other information, where possible. A biometric database for biometric key-protected data only must be established and managed through an independent system. Detailed requirements will be as follows:

a) Rather than saving biometric key-protected data from multiple users in a single database, a separate storage device, such as a smart card or a USB memory device for each individual, may be recommended to store individual biometric data as specified in [b-ITU-T X.1086].

b) If biometric key-protected data are transmitted from a smart card or USB memory, the system structure should be as directly physically connected to a matching system as possible in order to make any outside attack difficult.

c) And the challenge-response protocol based on [ISO/IEC 11770-4] must be established to prepare for any reply attack by providing secure management method on biometric key.

If an asymmetric private key or symmetric key is exported from a secure cryptographic module and moved to secure storage for purposes of backup and recovery based on [ISO/IEC 11770-4] for secure management on weak secret biometric data, then the cryptographic key is exported using a secure key management scheme based on [ISO/IEC 17799].

9 Biometric digital key with biometric certificate

9.1 Biometric certificate-based biometric digital key

Additionally, the identity of the user is verified by comparing the captured biometric data with biometric certificate (BC) that is stored in BCA specified in [ITU-T X.1089]. Therefore, no one can act for the original user in the key generation mechanism. Only the user who has registered his/her own biometric template on the BCA can make public and private key pairs.

Based on the biometric data, biometric certificate can be generated (updated) in the enrolment step. A user firstly registers to the system and asks the system to issue a BC. Then, the system generates the biometric feature template (origin template) and alignment help data. And the user randomly generates a key denoted 'secret data' to produce a binding data on the biometric digital key with the created input template (detailed description in Appendix II).

The binding key-protected data then is delivered to a protection module, which contains the information of the template and additional value such as a 'secret data', and is stored as a protected form. Generally, the biometric digital key and biometric feature belong to an identical feature space so the matching between the biometric key and sample will be taken in the key generation phase.

The protecting methods can be different according to different biometric traits. The biometric key and help data can be stored in the BC. Additionally, the system encrypts the feature template with 'secret data' to produce an encrypted template. The encrypted template, biometric digital key and some additional adjustment information will be stored in the BC. Because there is no feature template in the BC, no matter where the BC is stored, the security of the feature template can be assured. The framework for the biometric certificate generation with biometric digital key is as shown in Figure 6.

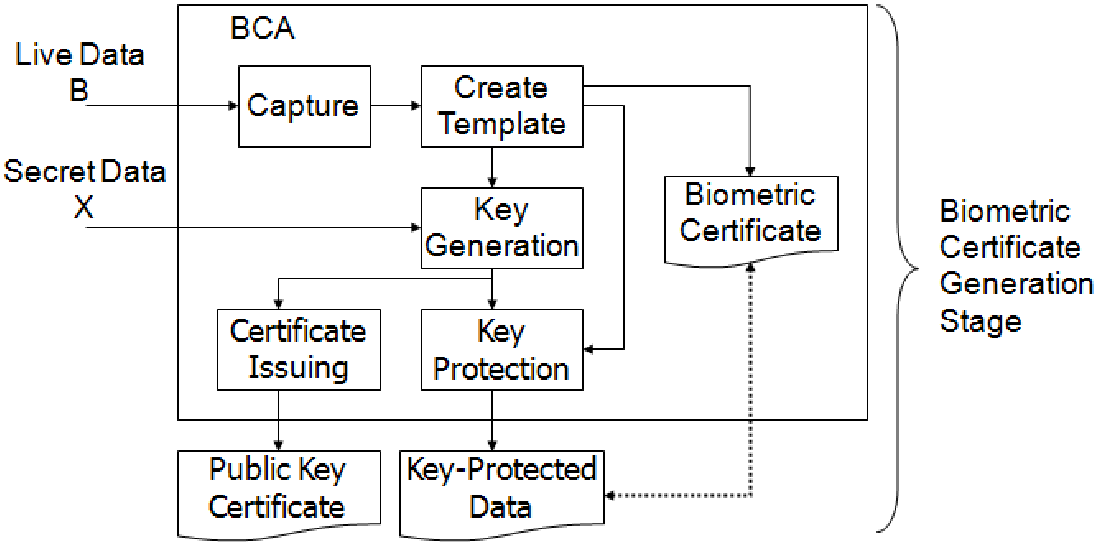

Figure 6 – Framework for biometric certificate generation with biometric digital key

9.2 Biometric certificate-based biometric digital signature

Biometric certificate also can be used for biometric digital signature. After accounting the input 'live data' using adjustment information stored in the BC, a matching is taken to filter/regenerate part of the genuine binding data. These data then are sent to the key extracting module to restore/regenerate with the 'secret data'. Key extraction module releases private key from the key-protected data. If they are matched, the template and a secret of the user will be fed in the key generation module to generate the biometric digital key. Since the template in the BC is unique, an identical biometric digital key can be guaranteed from different samples. The released private key then can be used in the biometric digital signature module (detailed description in Appendix II). The biometric certificate-based biometric digital signature framework is as shown in Figure 7.

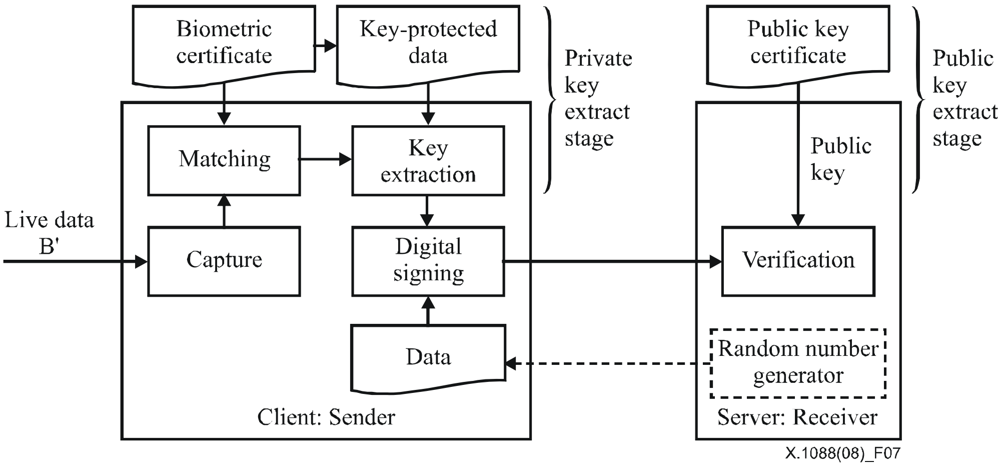

Figure 7 – Biometric certificate-based biometric digital signature framework

10 Security requirements on biometric certificate-based biometric digital key

10.1 Basic security requirements

This clause describes the basic security requirements for biometric digital key framework in managing and securing biometric information for each application. The basic security requirement in the biometric certificate-based biometric digital key also has similar requirements with clause 8.1. Additionally, the following basic requirements apply to all applications and environments, wherever the biometric digital key with biometric certificate is used.

a) Biometric certificate should be in place to maintain the integrity of the biometric template and additional certification data.

b) In the biometric digital key protection framework, the biometric certificate can be used to authenticate the user's identity. Therefore, the biometric certificate is a biometric data registered by the BCA. So the privacy protection mechanism should be considered.

c) Biometric digital key generation and protection mechanisms should be in place to maintain the integrity of biometric data and authentication results between any two components, using the cryptographic mechanisms, such as a digital signature and verification based on the BC.

d) If desired, the biometric digital key generation and protection mechanisms may be in place to ensure the confidentiality of the biometric data between any two components and within any component in the biometric system, using the cryptographic encryption/decryption based on the BC.

10.2 Security requirements on biometric certificate-based biometric digital key

10.2.1 Basic requirements on biometric certificate-based biometric digital key generation

This clause describes the basic security requirements for biometric key generation based on the biometric digital key framework.

a) The biometric digital key (public/private key) can be created by using a cryptographically secure hash function with both a user's biometric template and a personal secret value based on the BC.

b) Therefore the controlling organization should select a hash algorithm properly to standardize for the proposed key generation mechanism, such as MD5 and SHA-1, and should also consider how to concatenate a personal secret value and a biometric template from the BC.

c) Cryptographically secure hash functions should have the property that they are computationally infeasible to find another personal secret value that produces the same key.

d) The controlling organization should consider how to find secure big prime numbers against man-in-the-middle attack when the organization uses this biometric key as a key exchange mechanism in the biometric system with the BCA.

10.2.2 Functional requirements on biometric certificate-based biometric digital key generation

This clause describes the functional security requirements for biometric key generation based on the biometric digital key framework. Based on the biometric key generation framework, public key and private key pairs can be generated:

a) The controlling organization maintains controls with the objective of providing reasonable assurance that biometric digital key pairs are generated in accordance with industry standards.

b) Biometric digital key generation from the biometric template on the BC can use a random bit generator (RBG) or pseudo-random bit generator (PRBG), as specified in [ISO/IEC 18031].

c) When prime numbers are needed, key generation from the biometric template on the BC uses a prime number generator, as specified in [ISO/IEC 18032].

d) Biometric key generation from the biometric template on the BC takes place in a physically controlled environment.

e) Biometric key generation from the biometric template on the BC can use a key generation algorithm, as specified in an ISO (or equivalent national) standard.

Moreover, the following fundamentals should be considered in a biometric key generation framework:

a) The keys output by a biometric key generation with BC appear random to any adversary who has access to auxiliary information and the template used to derive the key.

b) A user's biometric data used to make biometric key generation from the BC should satisfy the uniqueness property.

c) An adversary learns no useful information about a biometric given auxiliary information and the template used to derive the key.

d) An adversary learns no useful information about a biometric given auxiliary information, the template used to derive the key, and the key itself.

The controlling organization maintains controls with the objective of providing reasonable assurance that keys are used only for their intended functions in their intended locations. Cryptographic keys are generated and used solely for their intended purpose, which is specified and described during key generation, including:

a) Asymmetric key pairs with BC for biometric data integrity.

b) Asymmetric key pairs with BC for authentication of origin.

c) Asymmetric key pairs with BC for enhancing the confidentiality of biometric data.

10.3 Security requirements on biometric certificate-based biometric digital key protection

This clause describes the basic security requirements for biometric digital key framework in managing and securing biometric information for each application. The following basic requirements apply to all applications and environments, wherever biometric digital key is used.

In the biometric digital key protection framework based on BC, the following security requirement items should be considered.

a) Privacy protection of registered biometric key-protected data on BC is essential.

b) Confidentiality of key-protected data on BC is essential.

Additionally, a method should be provided to establish that safe data items, such as key-protected data, should be transferred through an integrity test module between biometric client/server. To do so, a specific key for message authentication code on key-protected data should be assigned. This may encode the acquired protected data with an assigned MAC key specified in [ISO/IEC 9797-2], and then be stored in the secure storage, such as smart card, protected device, etc. Detailed requirements will be as follows:

a) The biometric digital key must be stored securely in the BC as an encoded form using the personal secret data.

b) Non-encoded biometric digital key may enhance the risk of having their internal data exposed to an outside attacker, to be manipulated and/or analysed.

c) Access to a key-protected key in the BC must be limited to specific individuals with specific requirements, and the use and disclosure of biometric key-protected data should be clearly managed and supervised.

Additionally, a biometric template matching should be securely done by client-terminal to extract stored key-protected data from the BC. In this case, detailed requirements will be as follows:

a) For generating biometric digital key with BC, the matching procedure should be done with both the input live data and the stored biometric template in the BC.

b) The biometric template matching segment generally accepts two biometric templates, compares their similarities based on probability, and informs the respective results.

c) Even though a biometric template is valid for matching, different results can be produced if the matching segment improperly processes it. Therefore, this segment is a core component that must be protected from any unauthorized external access, and requires a method to determine the validity of the matching results.

d) After passing the matching procedure, the key-protected data stored in the BC should be accessed securely for extracting biometric digital key (private key).

e) Based on this private key, the biometric digital signature mechanism can be useful for authentication and secure communication on open network based on [ISO/IEC 14888-1].

10.4 Security requirements on the client-side

The client-side for which the key generation/extraction modules are installed needs security analysis among sensor, capturing and matching modules.

a) Biometric data entered from biometric capture devices at client-side must be safely transmitted to the biometric key generation module.

b) A protection measure may be prepared for transmission if the data are transferred via a telecommunications network.

c) A method should be provided to establish that safe data items only are transferred through an integrity test conducted on any data transferred from a client-side.

Unlike other personal information, biometric data requires more sophisticated care and, therefore, they may need to be stored separately from other information, where possible. A database for biometric data only must be established and managed through an independent system.

10.5 Security requirements between client-side and BCA

The client-side receives the user's biometric template from the BCA and saves it in the local storage for user authentication. In the user authentication step, two cases should be considered as follows:

a) Firstly, the biometric template in BCA is disclosed and someone appropriates the template.

b) Secondly, security on the biometric template itself should be considered.

The client-side and BCA are interconnected via a public network. In this case, the information sent from BCA to client-side can be monitored, intercepted and modified by a hacker. To cope with these threats, the following considerations will be required:

a) Encrypt/decrypt method on biometric certificate is required securely with message authentication code on optionally.

b) Secure biometric data transmission protocol between client-side and BCA should be provided to authenticate the delivery of the certificate to the intended user.

10.6 Security requirements between client-side and CA

The public key created in the client-side is sent to the CA for registration. Therefore, security considerations will be required as follows:

a) The telebiometric system model specified in [ITU-T X.1084] can be used for the client, and CA can provide PKI-based security services to the client-side.

b) The client-side and the CA are also connected via a public open network. Several attacks, such as intercept, masquerade, and corruption threats on public key, should be protected in the open network.

c) Secure authentication procedures between the client-side and the CA should be provided between the client and the CA.

Appendix I

Biometric digital key based on biometric certificate

(This appendix does not form an integral part of this Recommendation)

I.1 Biometric digital key

This appendix shows one example model of the biometric digital key generation/protection mechanism with biometric certificate.

I.2 Biometric certificate generation for biometric digital key

The first step is to generate a biometric certificate from the biometric template. A user firstly registers to the system and asks the system to make a BC (biometric certificate – [ITU-T X.1089]) for him. Then, the system generates the biometric feature template (origin template) and alignment help data. And the system randomly generates a key denoted 'Secret' to produce a binding data with the input template (Figure I.1).

The binding data then is delivered to a protection module, which contains the information of the template and 'Secret', and is stored as a protected form. Generally, the biometric-key and biometric feature belong to an identical feature space, so the matching between the biometric-key and sample will be taken in the key generation phase.

The protecting methods can be different according to different biometric traits. The biometric-key and help data can be stored in the BC. Additionally, the system encrypts the feature template with 'Secret' to produce an encrypted-template. The encrypted-template, biometric-key and help data will be stored in the BC. Because there is no feature template in the BC, no matter where the BC is stored, the security of the feature template can be assured.

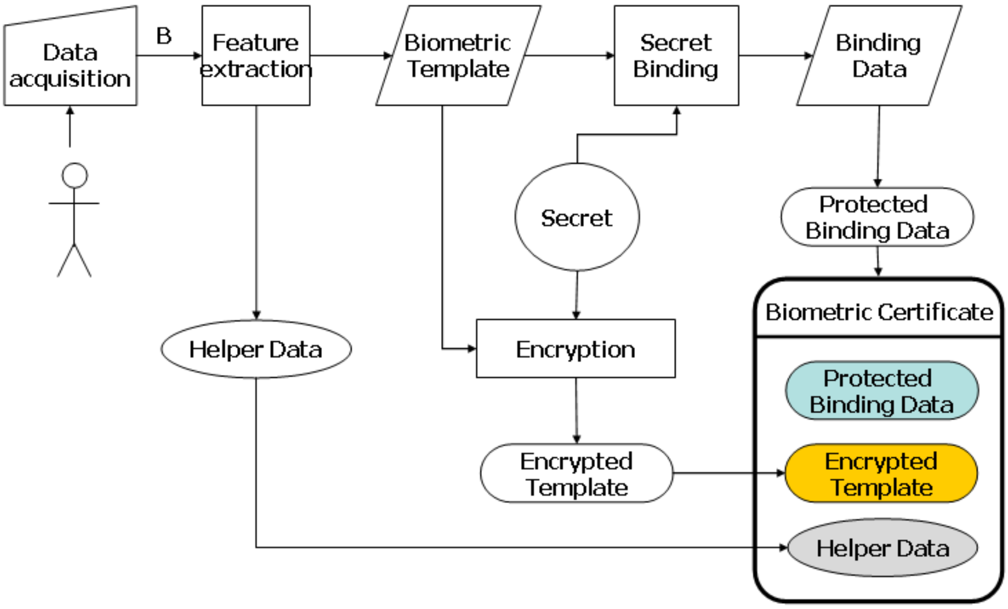

Figure I.1 – Biometric certificate generation on enrolment process

I.3 BC-based biometric digital key generation

After comparing the biometric-key with helper data in the BC, the system can make up the offset between the sample and the template. Then the biometric-key and sample are fed in the binding-data regeneration module, in which a matching is taken to filter/regenerate part of the genuine binding data. These data then are sent to the key extracting module to restore/regenerate the 'Secret'. The 'Secret' can be directly applied in encryption, decryption or signature.

Additionally, the matching in the binding-data regeneration module is viewed as primary matching. Instead of directly used in cryptographic application, the 'Secret' will be used to decrypt the cipher-template in the BC to get the original template. Then, the sample and template can be compared refinely. If they are matched, the template and a secret of the user will be fed in the key generation module to generate the biometric digital key. Since the template in the BC is unique, an identical biometric digital key can be guaranteed from different samples. The biometric digital key then can be applied in various cryptographic scenarios (Figure I.2).

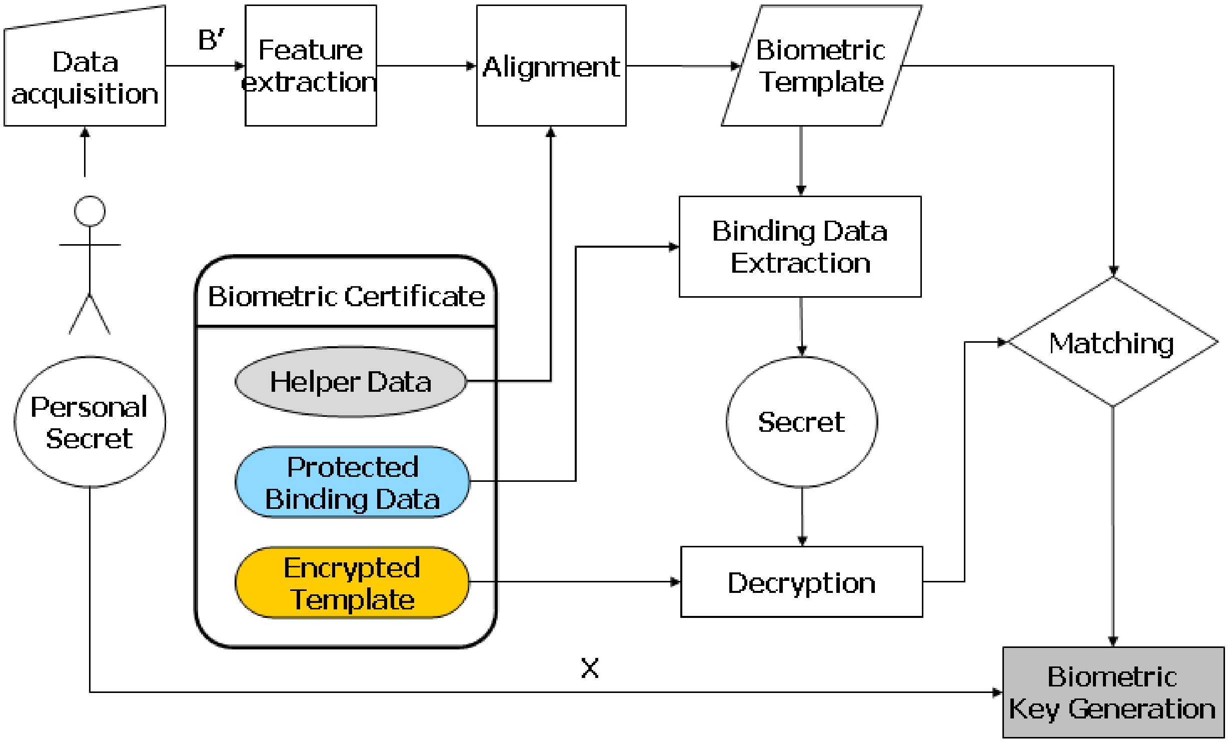

Figure I.2 – BC-based biometric digital key generation

Appendix II

Applications of biometric digital key

(This appendix does not form an integral part of this Recommendation)

II.1 Introduction

This appendix considers two kinds of possible applications of biometric digital key: biometric encryption with digital key based on server-side asymmetric key generation, and biometric digital signature for authentication based on client-side asymmetric key generation. A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable. Digital signatures have many applications in biometric security on telecommunication, including authentication, integrity and non-repudiation. Based on the previous biometric digital key framework, both models, such as client-side and server-side asymmetric key generation models, are possible.

II.2 Server-side asymmetric biometric key generation

In this model, a server-terminal (verifier) inputs his own biometric data, and it is compared with the BC for authentication of legal/illegal user after the matching process. Then biometric digital key pairs (private and public key) are generated by using the input secret from the server. The public key is stored in the public DB. Then the client-terminal (user) can get the public key from the DB for generating a biometric encryption message using this public key in the client-side. This mechanism can also be combined with secure communication with confidentiality and integrity in the encrypted message. In both cases, the BC is required to generate the biometric digital key pair.

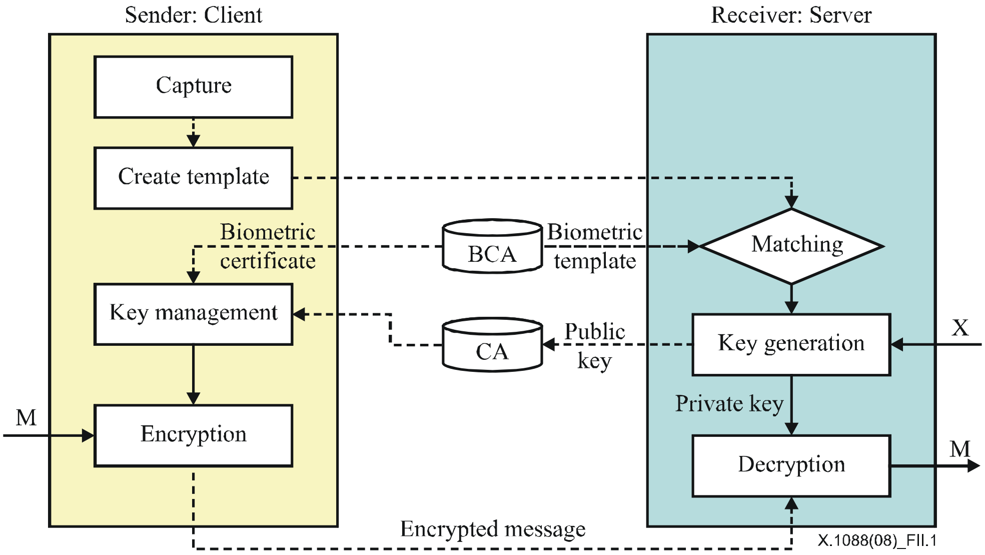

Figure II.1 – Asymmetric digital key generation and biometric encryption

II.3 Client-side asymmetric biometric key generation

In this model, a client-terminal (user) inputs his (her) biometric data and it is compared with the BC for authentication of legal/illegal user after the matching process. Then biometric digital key pairs (private and public key) are generated by the secret input from the user. The public key is issued as a PKC by the CA.

The user can generate a digital signature using this private key in the client-side. This mechanism can be combined with the user authentication process for verification of legal/illegal user on open communication environments.

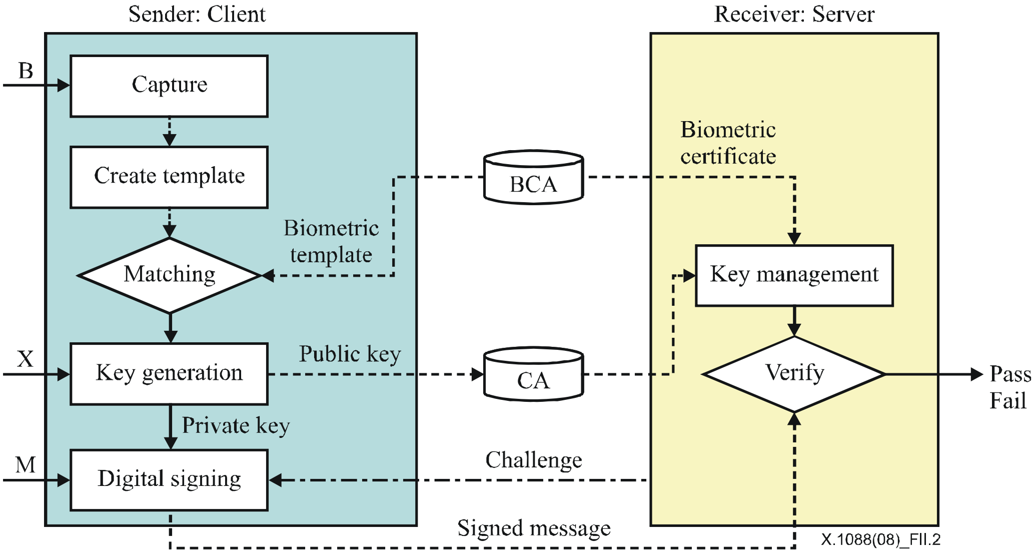

Figure II.2 – Asymmetric digital key generation and digital signature

Bibliography

[b-ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security*.

[b-ISO/IEC 18033-2] ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37971>

[b-ISO/IEC 19785-1] ISO/IEC 19785-1:2006, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41047>

[b-ISO 19092] ISO 19092:2008, *Financial services – Biometrics – Security framework*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50145>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009