

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/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Biometric digital key	4
6.1	Biometric cryptosystem.....	4
6.2	Model of biometric digital key	4
7	Biometric digital key framework.....	6
7.1	Framework overview.....	6
7.2	Prerequisites	6
7.3	Biometric digital key generation and protection framework.....	7
7.4	Biometric encryption and signature framework with biometric digital key...	10
8	Security requirements on biometric digital key framework	11
8.1	Basic security requirements.....	11
8.2	Security requirements on biometric digital key generation.....	12
8.3	Security requirements on biometric digital key protection	13
9	Biometric digital key with biometric certificate	14
9.1	Biometric certificate based biometric digital key.....	14
9.2	Biometric certificate-based biometric digital signature	15
10	Security requirements on biometric certificate-based biometric digital key	16
10.1	Basic security requirements.....	16
10.2	Security requirements on biometric certificate-based biometric digital key..	16
10.3	Security requirements on biometric certificate-based biometric digital key protection.....	17
10.4	Security requirements on client-side	18
10.5	Security requirements between client-side and BCA.....	19
10.6	Security requirements between client-side and CA.....	19
Appendix I – Biometric digital key based on biometric certificate		20
I.1	Biometric digital key	20
I.2	Biometric certificate generation for biometric digital key	20
I.3	BC-based biometric digital key generation	21



Documents

Document Sharing Hub

Rec. ITU-T X.1088 (05/2008)

iii

	Page
Appendix II – Applications of biometric digital key	22
II.1 Introduction	22
II.2 Server-side asymmetric biometric key generation	22
II.3 Client-side asymmetric biometric key generation	22
Bibliography	24

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.