



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1090

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Authentication framework with one-time telebiometric template

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/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 2011

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

Draft ITU-T Recommendation X.1090 (X.ott)

Authentication framework with one-time telebiometric template

Summary

This Recommendation describes a user authentication framework with a one-time telebiometric template. The framework provides secure user authentication and protection mechanisms for a biometric template transmitted over open networks. It prevents a replay attack and protects an original biometric template by generating a new template upon each completion of authentication. This Recommendation also addresses the security requirements associated with the framework for a one-time telebiometric template.

Keywords

One-time Telebiometric Template, Telebiometrics, Biometric Authentication, Replay Attack

Contents

1	Scope	4
2	References.....	4
3	Definitions	4
3.1	Terms defined elsewhere	4
3.2	Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	5
5	Conventions	5
6	One-time telebiometric template for authentication	6
6.1	Threats in telebiometric authentication	6
6.2	Authentication using one-time telebiometric template.....	6
7	Overview of authentication framework with one-time telebiometric template.....	6
7.1	Enrollment procedure	6
7.2	Verification procedure.....	7
8	Authentication framework with one-time telebiometric template.....	7
8.1	OTT generation model	7
8.1.1	Overview	7
8.1.2	Input template	8
8.1.3	Transformation information	8
8.1.4	OTT generation	8
8.1.5	OTT	8
8.2	User enrollment model with OTT	8
8.2.1	Overview	8
8.2.2	Template creation	9
8.2.3	Synchronization information	9
8.2.4	OTT DB.....	9
8.2.5	OTT token	9
8.3	Biometric verification model with OTT	9
8.3.1	Overview	9
8.3.2	Comparison.....	10
8.4	OTT DB update model	10
8.4.1	Overview	10
8.4.2	Transformation information generation	11

8.4.3	Random number generation	11
8.4.4	Synchronization information generation	11
8.5	Synchronization model	11
8.5.1	Overview	11
8.5.2	Checksum generation	12
8.5.3	Checksum verification	12
8.6	OTT token update model	12
8.6.1	Overview	12
8.6.2	Transformation information update	13
9	Requirements in authentication with OTT	13
9.1	General requirements	13
9.2	Requirements in OTT generation	13
9.3	Requirements in user enrollment	13
9.4	Requirements in biometric verification	14
9.5	Security requirements in authentication system	14
Annex A	OTT authentication with robust synchronization	15
A.1	Introduction	15
A.2	User enrollment model with OTT	15
A.3	Biometric verification model with OTT	16
A.4	OTT DB update model	16
A.5	Synchronization model	18
A.5.1	Overview	18
A.5.2	Random number R_S	18
A.5.3	C_C checksum generation	18
A.5.4	C_C verification	18
A.5.5	Random number R_C	19
A.5.6	C_S checksum generation	19
A.5.7	C_S verification	19
A.6	OTT token update model	19
Appendix I	Example of implementing OTT generation	20
I.1	Introduction	20
I.2	Template transformation and comparison	20
I.3	Update of template and transformation	21
I.4	Proof of consistency in comparison	21
Bibliography		24

1 Scope

This Recommendation describes a user authentication framework with a one-time telebiometric template to implement a secure biometric authentication system. It specifies the framework in terms of function models and security requirements. Note, however, that this Recommendation does not cover the transformation functions used to generate a one-time telebiometric template because many different kinds of transformation can be adopted to generate a one-time telebiometric template.

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.

- | | |
|-------------------|--|
| [ISO/IEC 18031] | ISO/IEC 18031:2005, <i>Information Technology – Security Techniques – Random Bit Generation</i> |
| [ISO/IEC 19784-1] | ISO/IEC 19784-1:2006, <i>Information Technology – Biometric Application Program Interface (BioAPI) – Part 1: BioAPI Specification</i> |
| [ISO/IEC 19785-1] | ISO/IEC 19785-1:2006, <i>Information Technology – Common Biometric Exchange Formats Framework (CBEFF) – Part 1: Data Element Specification</i> |
| [ISO 19092] | ISO 19092:2008, <i>Financial Services - Biometrics: Security Framework</i> |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 biometric** [ISO/IEC 19785-1]: Pertaining to the field of biometrics
- 3.1.2 biometrics** [ISO/IEC 19785-1]: Automated recognition of individuals based on their behavioral and biological characteristics
- 3.1.3 biometric authentication** [ISO 19092]: Process of confirming an individual's identity, either by verification or by identification
- 3.1.4 biometrics data** [ISO/IEC 19785-1]: A biometric sample at any stage of processing, biometric reference, biometric feature, or biometric property
- 3.1.5 biometric sample** [ISO/IEC 19785-1]: Information obtained from a biometric device, either directly or after further processing
- 3.1.6 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
- 3.1.7 biometric verification** [ISO 19092]: Process of comparing a match template against reference based on a claimed identity (e.g. user ID, account number)

3.1.8 enrollment [ISO 19092]: Process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 client: Entity that provides a biometric authentication service using a one-time telebiometric template on a user side in telecommunication environments

3.2.2 one-time biometric template: Biometric template that is once used, then revoked.

3.2.3 OTT database: Physical or logical storage device that stores data and information for user authentication and belongs to a server

3.2.4 one-time telebiometric template: One-time biometric template used in open network environments

3.2.5 original template: Biometric template that is created directly from a user's biometric sample and is neither transformed nor encoded

3.2.6 OTT token: Physical storage device that stores data and information for user authentication and belongs to a user

3.2.7 replay attack: Breach of security in open networks wherein a biometric template from a client is stored without authorization and retransmitted to a server to gain illegal access

3.2.8 server: Entity that provides a biometric authentication service using a one-time telebiometric template at the request of a user or a client in telecommunication environments

3.2.9 synchronization information: Non-biometric data that is used to keep transformation consistent between a client (or user) and a server

3.2.10 transformation: Process of distorting or converting a biometric template into another domain to protect and conceal its original value

3.2.11 transformation information: Non-biometric data that is used for transformation of a biometric template.

3.2.12 transformed template: Biometric template that is created through transformation

3.2.13 user: Receiver of a biometric authentication service through a client and a server

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

OTT	One-time Telebiometric Template
OTT DB	OTT Database
SI	Synchronization Information
TI	Transformation Information

5 Conventions

<None>

6 One-time telebiometric template for authentication

6.1 Threats in telebiometric authentication

As information technology advances, biometric authentication systems are increasingly employed in many areas to provide efficient and secure access control. Note, however, that this gives rise to privacy concerns as well since personal information needs to be stored in centralized systems and transmitted over open networks. These threats are not new, but they are more critical in biometric authentication due to the nature of biometric data [b-Ratha01]. Biometric data identifies a user as unique, but there are only a few substitutes. Therefore, once they lose their biometric data, they may permanently lose their identities. For example, a user has only one face and ten fingerprints, and it is impossible to change the biometric traits with new ones as if creating new passwords. Moreover, because biometric data is unique, it is much like the same password for multiple systems. Thus, an attacker stealing a user's biometric template from one system can log in to other systems using the stolen template. Unfortunately, conventional encryption will have no effect when coping with such threats. In addition, for template comparison, an encrypted template should be decrypted, and thus an original template are exposed for every comparison. Moreover, without attacking a server directly, an attacker can gain access control by eavesdropping on communication and simply replaying the encrypted message as if it were generated by any valid client or user.

6.2 Authentication using one-time telebiometric template

The authentication framework provides secure user authentication and protection for a biometric template transmitted over open networks. It converts a biometric template using transformation functions and uses a transformed template for user authentication and network transmission instead of an original template. If a template is lost or compromised, a new transformed template is created using a new instance of transforms. Similarly, by generating a new transformed template for each authentication, it effectively prevents a replay attack. Through template transformation, transformation information and biometric data are mixed together, and template comparison is performed in transformed state. Therefore, they are not separated even during template comparison and provide strong protection for each other.

7 Overview of authentication framework with one-time telebiometric template

7.1 Enrollment procedure

Figure 1 shows the outline of the enrollment procedure with a user's biometric data.

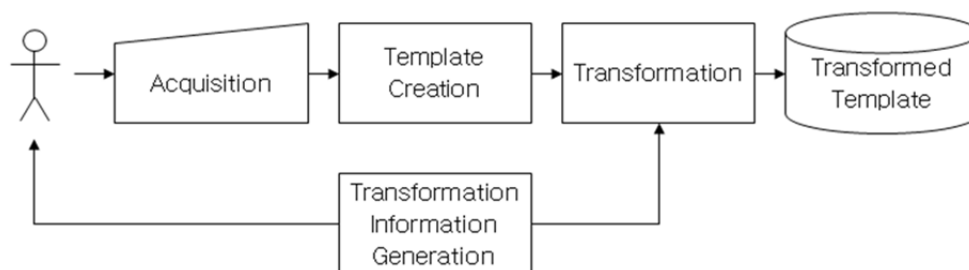


Figure 1 – Enrollment procedure with OTT

- The user provides his or her biometric data, for example face or fingerprint.
- The system extracts the user's biometric features and creates a biometric template.