INTERNATIONAL STANDARD

ISO/IEC 17922

First edition
2017-09

Information technology — Security techniques — Telebiometric authentication framework using biometric hardware security module

Technologies de l'information — Techniques de sécurité — Infrastructure d'authentification télébiométrique utilisant un module de sécurité matériel biométrique

Reference number
ISO/IEC 17922:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T X.1085 (10/2016).

© ISO/IEC 2017 – All rights reserved

INTERNATIONAL STANDARD ISO/IEC 17922
RECOMMENDATION ITU-T X.1085

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

Summary

Recommendation ITU-T X.1085 | ISO/IEC 17992 describes a telebiometric authentication scheme using biometric hardware security module (BHSM) for the telebiometric authentication of proving owner of ITU-T X.509 certificate registered individual at registration authority (RA). This Recommendation | International Standard provides the requirements for deploying the BHSM scheme to securely operate the telebiometric authentication under PKI environments. The scheme focuses on providing how to assure the telebiometric authentication with biometric techniques and hardware security module and it also suggests ASN.1 standard format for including the proposed scheme in ITU-T X.509 framework when telebiometric authentication and ITU-T X.509 certificate are combined to prove the owner of the certificate.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1085	2016-10-14	17	11.1002/1000/13060

Keywords

Biometric hardware security module, BHSM, ITU-T X.509 certificate, ISO/IEC 24761, pseudonymous identifier, PSID, public key infrastructure, PKI, telebiometric authentication.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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 2017

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

© ISO/IEC 2017 – All rights reserved

CONTENTS

Page

1 Scope 1
2 Normative references 1
2.1 Identical Recommendations | International Standards 1
2.2 Paired Recommendations | International Standards equivalent in technical content 2
2.3 Additional references 2
3 Definitions 2
3.1 Terms defined in this Recommendation | International Standard 2
3.2 Terms defined in other International Standards 2
4 Abbreviations 3
5 Symbols and terminology 3
6 Biometric hardware security module for telebiometric authentication 3
6.1 Additional feature of BHSM to the HSM 3
6.2 General scenario for use of the BHSM 4
6.3 Telebiometric authentication using the BHSM 4
7 Telebiometric authentication with biometric hardware security module 5
7.1 General 5
7.2 Enrolment procedures 5
7.3 Telebiometric authentication processes 7
8 BHSM based telebiometric authentication procedures 9
8.1 PSID generation and ITU-T X.509 certificate 9
8.2 BHSM based telebiometric authentication process 10
8.3 ASN.1 type for the encrypted PSID 10
Annex A – PSID and related information 11
A.1 General 11
A.2 Encrypted PSID requesting an ITU-T X.509 certificate 11
A.3 ASN.1 for PSID 11
Annex B – Procedures for inserting PSID using PKCS #10 with modification 13
Bibliography 14

Introduction

This Recommendation | International Standard describes a telebiometric authentication scheme using a biometric hardware security module (BHSM) for the telebiometric authentication of the person who presents the BHSM as the owner of an ITU-T X.509 certificate embedded in the BHSM as registered with the certification authority (CA). This Recommendation | International Standard provides the requirements for deploying a BHSM scheme to provide secure telebiometric authentication within public key infrastructure (PKI) environments. The scheme provides assurance for telebiometric authentication using biometric recognition integrated into a hardware security module. It also provides ASN.1 definitions that allow the biometric authentication to be incorporated into an ITU-T X.509 framework to authenticate the user as the owner of the ITU-T X.509 certificate.

© ISO/IEC 2017 – All rights reserved

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

1 Scope

To prove ownership of an ITU-T X.509 certificate registered individually with the registration authority (RA), a biometric hardware security module has been considered to provide a high-level biometric authentication. This Recommendation | International Standard provides a framework for telebiometric authentication using BHSM.

Within the scope of this Recommendation | International Standard, the following issues are addressed:

- telebiometric authentication mechanisms using BHSM in telecommunication network environments; and
- abstract syntax notation one (ASN.1) format and protocols for implementing the mechanisms in the ITU-T X.509 framework.

The related standard environment is depicted in Figure 1. The main role of this Recommendation | International Standard is to harmonize with existing telebiometric authentication and public key infrastructure (PKI) standards and to establish a standard mechanism using BHSM to verify the ownership of the ITU-T X.509 certificate in the telebiometric environment.

NOTE – In this Recommendation | International Standard, ITU-T X.509 certificate means ITU-T X.509 public-key certificate.

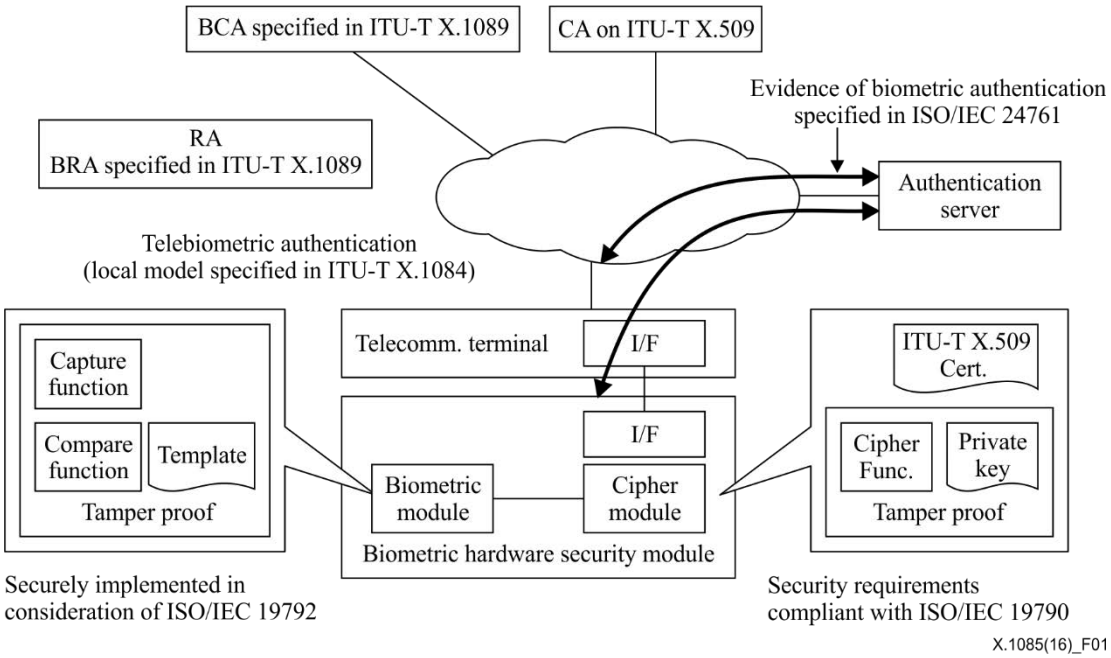


Figure 1 – Standard environment for BHSM

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2016, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

2.2 Paired Recommendations | International Standards equivalent in technical content

None.

2.3 Additional references

- ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*.
- ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.
- ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.

3 Definitions

3.1 Terms defined in this Recommendation | International Standard

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1.1 biometric hardware security module: Hardware security module incorporating biometric sensor(s) and biometric recognition to authenticate the user.

NOTE – In case of a comparison of biometric hardware security modules, they come traditionally in the form of a smart card but recently also in the form of a universal serial bus (USB) type security token which can be attached directly to general purpose computers.

3.1.2 hardware security module: Hardware implementation of a secure crypto-processor using an ITU-T X.509 certificate and a private key to provide secure authentication.

3.1.3 telebiometric authentication: Biometric authentication utilising data communication by telephony, radio or a related technology.

3.2 Terms defined in other International Standards

3.2.1 The following terms are defined in ISO/IEC 2382-37:

a) **biometric reference**: One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison.

b) **biometric sample**: Analogue or digital representation of biometric characteristics prior to biometric feature extraction.

3.2.2 The following term is defined in ISO/IEC 9798-1:

a) **entity authentication**: Corroboration that an entity is the one claimed.

3.2.3 The following terms are defined in ISO/IEC 24745:

a) **identity reference**: Non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain.

b) **pseudonymous identifier**: Part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any).

c) **renewability**: Property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference.

d) **renewable biometric reference**: Revocable or renewable identifier that represents an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from the captured biometric sample.

NOTE – A renewable biometric reference consists of a pseudonymous identifier and additional optional data elements required for biometric verification or identification such as auxiliary data.

e) **revocability**: Ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference.

© ISO/IEC 2017 – All rights reserved