DRAFT International Standard

ISO/IEC DIS 30136

Information technology — Performance testing of biometric template protection schemes

ICS: 35.240.15

ISO/IEC JTC **1**/SC **37**

Secretariat: **ANSI**

Voting begins on:
2026-02-16

Voting terminates on:
2026-05-11

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 30136:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Conformance ... **4**
6 Methods for biometric template protection (informative) ... **4**
6.1 General ... 4
6.2 Generalized architecture for biometric template protection system ... 5
6.3 Data separation ... 7
6.4 Examples of typical architectures in template protection systems ... 7
7 Overview of performance evaluation for biometric template protection schemes ... **8**
7.1 Methods for attacking a biometric template protection system ... 8
7.2 Necessity of metrics beyond traditional recognition performance ... 8
7.3 Technology evaluation ... 8
7.4 Theoretical evaluation and empirical evaluation ... 8
7.5 Threat models ... 9
7.5.1 Naive model ... 9
7.5.2 Collision model ... 9
7.5.3 General models ... 9
8 Performance metrics for biometric template protection systems ... **10**
8.1 General ... 10
8.2 Case of multiple biometric recognition systems ... 11
8.3 Metrics for enrolment and recognition performance ... 11
8.3.1 General ... 11
8.3.2 Accuracy degradation ... 11
8.3.3 Template diversity ... 12
8.3.4 Storage requirement per registered individual ... 13
8.4 Metrics for security and privacy protection performance ... 13
8.4.1 Irreversibility ... 13
8.4.2 Unlinkability ... 15
8.4.3 Successful Attack Rate (SAR) (optional) ... 18
Annex A (informative) **Publication of algorithms or proofs used in performance evaluations** ... **20**
Annex B (Informative) **Example of Unlinkability Empirical Evaluation** ... **21**
Bibliography ... **23**

© ISO/IEC 2026 – All rights reserved

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 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC 30136:2018), which has been technically revised. The main changes compared to the previous edition are as follows:

— A new set of unlinkability metrics is introduced in Clause 8 and Annex B

— The document is aligned with the updated ISO/IEC 24745:2022 and the Harmonized Biometrics Vocabulary

— Redundancies have been removed

© ISO/IEC 2026 – All rights reserved

Introduction

In conventional biometric recognition systems, an adversary who compromises an enrolment database may gain access to the initial biometric data of the individuals enrolled therein. This is undesirable because, if the biometric system is vulnerable to presentation attacks or replay attacks, the adversary could impersonate an individual and gain access to the system after gaining access to the enrolment database. Furthermore, if the biometric enrolment databases contain unprotected templates and the same biometric modality is adopted in multiple applications, the adversary could link the accounts of the individual across those applications (cross-matching).

NOTE to avoid confusion with concepts such as generative AI, the wording “generative biometric data” has been replaced by “initial biometric data”. Other terms such as generated or input were considered, but the experts chose initial.

A biometric template stored in an enrolment database is a reference set of biometric features derived from the biological and behavioural characteristics of an individual. If the system implementation allows it, a biometric enrolment that is known to have been compromised may be revoked and renewed a limited number of times. However, the number of unique biometrics that can be extracted from an individual is limited and thus biometric enrolments cannot be revoked and then re-issued an unlimited number of times like new credit card numbers or passwords. The compromise of biometric enrolment records stored in an enrolment database is a serious issue. Therefore, methods and procedures to mitigate the risk of compromise are needed.

Secure biometric recognition

The biometrics research community has invested significant effort in enabling biometric recognition without directly needing to store an individual’s biometric features in the clear at the enrolment database. This has led to the development of new methods referred to as “biometric template protection”, “biometric information protection”, or simply “secure biometrics”. In this document, the term “biometric template protection” is used.

The rationale behind this strategy is that, instead of storing the biometric features directly, the biometric recognition system derives some data from the biometric features and stores this derived data on the device. During the biometric recognition phase, the system receives a probe biometric sample from the individual seeking access. Then, the system combines the probe biometric sample and the derived data and generates a biometric recognition decision. The main property of the derived data is that it reveals little or no information about the underlying biometric characteristic that was captured during the enrolment phase.

Thus, if the biometric recognition system is compromised by an adversary, only the derived data falls into the hands of the adversary, but this does not enable the adversary to recover the biometric characteristics of the individuals enrolled in the database. Clearly, this strategy protects the privacy of the individuals enrolled in the database.

Further, if an adversary attempts to gain access, i.e. to log in, to the system by providing a fake probe biometric sample, then in a well-designed secure biometric system, combining the fake probe biometric sample with the derived stored data results in biometric recognition failure. Thus, this strategy protects the secrecy of the individuals enrolled in the database.

Rationale for new metrics

There are several ways in which biometric template protection can be realized. Some of these methods are described in ISO/IEC 24745:2022. Regardless of the method employed to construct the derived data, the following questions can be asked when evaluating a biometric template protection system:

a) What is the probability that the system rejects a mated trial and accepts a non-mated trial? This is a natural question to ask of *any* biometric recognition system. The metrics, False Non-Match Rate (FNMR) and False Match Rate (FMR) measure this performance [ISO/IEC 19795-1] for the conventional biometric system in which enrolment biometric features are compared with probe biometric features. A biometric

© ISO/IEC 2026 – All rights reserved

template protection system will also inherit these metrics, though the method of measuring them may vary depending upon the particular realization of the template protection algorithm.

b) What is the probability that an adversary enhanced with some knowledge about the database of enrolled individuals can be successfully recognized as one of those enrolled?

c) How much information can an adversary obtain by compromising a biometric system and stealing the derived (stored) enrolment information? In conventional biometric systems, the adversary may obtain significant information, in the form of the stored biometric template, or the stored feature vector. The goal of biometric template protection systems is to ensure that the stored derived data does not leak information about the enrolled individuals.

d) What is the probability that an adversary, having successfully compromised one or more biometric systems and having stolen the data stored on them, uses the information gained to be successfully recognized at a biometric system?

These questions form the basis for evaluating the accuracy, secrecy, and privacy of a biometric template protection system, which introduces a new set of metrics not previously associated with evaluating traditional biometric systems.

Necessity for standardization

There are several architectures under the umbrella of biometric template protection, e.g., fuzzy vault-based systems, secure sketch-based systems, cancellable biometric systems, secure multiparty computation-based systems, etc. It is necessary to define key metrics that not only answer the questions posed above, but also apply to a wide variety of biometric template protection architectures, thereby providing a common basis for comparison of systems based on different architectures. The goal of this document is to specify new metrics to evaluate a certain class of systems, namely biometric template protection systems described in ISO/IEC 24745:2022. At the same time, it is desirable to specify metrics that are as general as possible, and that apply to a generalized biometric verification architecture described in Clause 6. Theoretical and empirical definitions are provided for each metric in Clause 8. Throughout this document, the usual distinction is made between biometric verification, which involves a one-to-one comparison operation, and biometric identification which involves a one-to-many comparison operation.

© ISO/IEC 2026 – All rights reserved

Information technology — Performance testing of biometric template protection schemes

1 Scope

This document supports evaluation of the accuracy, secrecy, and privacy of biometric template protection schemes. It establishes definitions, terminology, and metrics for stating the performance of such schemes. Particularly, this document establishes requirements for the measurement and reporting of:

— theoretical and empirical accuracy of biometric template protection schemes,

— theoretical and empirical probability of a successful attack on biometric template protection schemes (single or multiple), and

— the biometric information leaked when one or more biometric template protection schemes are compromised.

This document also gives guidance on measuring and reporting diversity and unlinkability of templates.

This document does not:

— establish template protection schemes;

— address testing of traditional encryption schemes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19795-1, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 24745, *Information security, cybersecurity and privacy protection — Biometric information protection*

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 24745 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
accuracy degradation
difference in false negative recognition rate at a fixed false positive recognition rate for a biometric system tested both with and without template protection scheme

© ISO/IEC 2026 – All rights reserved

3.2
adversary
one who compromises an enrolment database and may gain access to the generated biometric data of the individuals enrolled therein

3.3
biometric template protection
BTP
protection of biometric references under various requirements for secrecy, irreversibility, and renewability for the duration of the lifecycle

3.4
initial biometric data
biometric data (sample(s) or features) used as primary input to the biometric template protection scheme

3.5
irreversibility
property of a transform that creates a biometric reference from generated biometric data such that knowledge of the transformed biometric reference cannot be used to determine any information about the generated biometric data

Note 1 to entry: Metrics introduced by this document aim to measure irreversibility by the degree of difficulty faced by an adversary in recreating an original unprotected version of the biometric data.

3.6
privacy compromise
event in which an adversary discovers part of the fenerated biometric data of an individual enrolled in the database of a biometric recognition system

Note 1 to entry: Discovery of part of the generated biometric data does not mean that successful biometric recognition is achieved, i.e. biometric system secrecy is not compromised by the discovery itself.

3.7
privacy leakage
<template protection scheme> amount of information about an individual‘s generated biometric data which an adversary can learn from the stored reference data

3.8
pseudonymous identifier comparator
PIC
system, process or algorithm that compares the pseudonymous identifier generated during enrolment by the pseudonymous identifier encoder and the pseudonymous identifier reconstructed during recognition by the pseudonymous identifier recoder, and returns a similarity score representing the similarity between the two

3.9
pseudonymous identifier recoder
PIR
system, process or algorithm that reconstructs a pseudonymous identifier based on the provided auxiliary data and the extracted features

3.10
secrecy
degree of difficulty faced by an adversary in determining input data, from a protected biometric template, that achieves biometric recognition, when impersonating an individual enrolled in the biometric enrolment database of a template protection system

© ISO/IEC 2026 – All rights reserved

3.11
secrecy compromise
event in which an adversary achieves biometric recognition when impersonating an individual enrolled in the biometric enrolment database of a template protection system

Note 1 to entry: Secrecy compromise includes the case in which the adversary gains unlawful access without necessarily discovering the generated biometric data of the individual being impersonated, i.e. the case in which the adversary remains unable to cause a privacy compromise.

3.12
successful attack rate
SAR
probability that an informed adversary can obtain a false accept result in a biometric system

Note 1 to entry: An informed adversary is one that has compromised (gained access to) a subset of the biometric enrolment database and the secret parameters (if any) associated with one or more biometric recognition systems (potentially including the target system under consideration) in which common individuals are enrolled.

3.13
template diversity
number of independent protected templates that can be generated from a given initial biometric data by a biometric template protection scheme

3.14
biometric reference size
size of stored biometric reference data

3.15
unlinkability
property of two or more biometric references that they cannot be linked to each other or to the subject(s) from which they were derived

[SOURCE: ISO/IEC 24745:2022, 3.38]

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AD	Auxiliary Data
BTP	Biometric Template Protection
ECC	Error Correcting Code, or Error Correction Coding
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
H(X)	Information-theoretic Entropy of a random variable X
H(X | Y)	Conditional entropy of random variable X given random variable Y
I(X; Y)	Mutual information between random variables X and Y
PI	Pseudonymous Identifier
PIE	Pseudonymous Identifier Encoder

© ISO/IEC 2026 – All rights reserved