

---

---

**Information technology — Biometrics  
— The use of biometric technology  
in commercial Identity Management  
applications and processes**

*Technologies de l'information — Biométrie — Utilisation de la  
technologie biométrique dans les processus et les applications de  
gestion de l'identité dans le commerce*

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO/IEC TR 29144:2014

<https://standards.iteh.ai/catalog/standards/sist/64f17a01-f6c2-456e-b809-096c9fb06089/iso-iec-tr-29144-2014>



**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC TR 29144:2014](https://standards.iteh.ai/catalog/standards/sist/64f17a01-f6c2-456e-b809-096c9fb06089/iso-iec-tr-29144-2014)

<https://standards.iteh.ai/catalog/standards/sist/64f17a01-f6c2-456e-b809-096c9fb06089/iso-iec-tr-29144-2014>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2014

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  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
1.1 In scope.....	1
1.2 Exclusions.....	1
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>2</b>
<b>5 Biometrics and Identity Management Systems</b> .....	<b>2</b>
5.1 General.....	2
5.2 Biometrics and identity.....	2
5.3 Identity and biometric identification.....	2
5.4 Biometric identifiers.....	3
5.5 Human role in biometrics.....	4
5.6 Assuring the integrity of the database.....	4
<b>6 Biometric considerations in Identity Management Systems</b> .....	<b>4</b>
6.1 General.....	4
6.2 Capturing and recording biometric characteristics.....	4
6.3 Adhesion of biometric characteristics.....	5
6.4 Changes to name, alias and identification data.....	7
6.5 Changes of condition.....	7
6.6 Biometric spoofing.....	7
6.7 Legitimate use of another identity.....	7
6.8 Other exceptions.....	8
6.9 Other issues of importance.....	8
<b>7 Implementation issues</b> .....	<b>8</b>
7.1 General.....	8
7.2 Aggregation of databases.....	8
7.3 Strengthening of token and knowledge based identity systems.....	9
7.4 Restrictions to accessing data.....	9
7.5 Privacy.....	9
7.6 Mechanisms for preventing abuse of systems.....	11
7.7 Multinational commercial organizations.....	11
<b>Bibliography</b> .....	<b>12</b>

## 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](http://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](http://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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](http://Foreword-Supplementary-information.standards.iteh.ai)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

<https://standards.iteh.ai/catalog/standards/sist/64f17a01-f6c2-456e-b809-096c9fb06089/iso-iec-tr-29144-2014>

## Introduction

This Technical Report provides support for the further development of ISO/IEC biometric standards in the context of cross-jurisdictional and societal applications of biometrics, including standardization of both existing and future technologies.

The contents of this Technical Report are recommended practices and guidelines and they are not mandatory. Legal requirements of the respective countries take precedence and biometric data should be obtained in accordance with local norms of behaviour. This Technical Report does not reduce any rights or obligations provided by applicable laws. Compliance with any recommendations in the Technical Report does not, in itself, confer immunity from legal obligations.

Examples of the benefits to be gained by following the recommendations and guidelines in this Technical Report are

- enhanced acceptance by subjects of systems using biometric technology,
- improved public perception and understanding of these systems,
- smoother introduction and operation of these systems,
- potential long-term cost reduction (whole life costs),
- adoption of commonly approved good privacy practice,
- interoperability both domestically and internationally, and
- implemented solutions having a greater degree of vendor independence.

The primary stakeholders are identified as

- users – those who use the results of the biometric data,
- developers of technical standards,
- subjects – those who provide the biometric sample,
- writers of system specifications, system architects, and IT designers, and
- public policy makers.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC TR 29144:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/64f17a01-f6c2-456e-b809-096c9fb06089/iso-iec-tr-29144-2014>

# Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes

## 1 Scope

### 1.1 In scope

This Technical Report will discuss

- concepts and considerations for the use of biometrics in a commercial Identity Management Solutions,
- items that need to be considered when integrating biometrics into a commercial Identity Management Solutions, and
- implementation Issues when implementing biometrics into commercial Identity Management Solutions.

### 1.2 Exclusions

**iTeh STANDARD PREVIEW**

This Technical Report will not **(standards.iteh.ai)**

- define an architecture and framework for IDM,
- discuss any specification or assessment of government policy,
- discuss the business need for a biometric database or process,
- discuss the specific biometrics and which ones are to be used in particular systems,
- consider the legality and acceptability in particular jurisdictions and cultures,
- analyse the general structure of identifiers and the global identification of objects (e.g. object identifiers), and
- discuss technical specifications in relation to the use of trusted biometric hardware and software.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012 apply.

## 4 Symbols and abbreviated terms

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

<b>DoB</b>	Date of Birth
<b>IDM</b>	Identity Management
<b>IDMS</b>	Identity Management System
<b>PIN</b>	Personal Identification Number
<b>TR</b>	Technical Report

## 5 Biometrics and Identity Management Systems

### 5.1 General

This Technical Report introduces concepts and considerations for the use of biometrics in a commercial IDMS.

It is not the intention of this Technical Report to outline how an IDMS works but only to provide guidance for the use of biometrics. Multipart standard ISO/IEC 24760-1:2011 describes concepts in a suggested IDM framework and this Technical Report will complement the International Standard

### 5.2 Biometrics and identity

A biometric capture subject, such as a human being, can be described by many different attributes and different sets of these attributes can form different identities.

The identity of a human can be characterized uniquely in a biometric system. The term “identifier” is used to refer to one or more attributes in an identity that express uniqueness. This aspect of uniqueness is widely understood as the essence of identity. In the context of IDM, uniqueness is just one of the many aspects to be considered.

While an identity can be unique in one system, the individual can still have unique but different identity in one or more other biometric systems. The set of attributes used as an identifier should always be sufficient to distinguish the biometric capture subject from any other biometric capture subject within a particular system.

ISO/IEC 24760 describes a range of identities that a biometric capture subject can have in various circumstances. These include biological identities such as biometrics. If a given biometric identifier is shared with multiple systems, it is possible to match data in different (or separate) biometric systems about the same identity.

When a biometric is introduced into an IDMS, it can only confirm with a level of confidence whether the biometric capture subject is or is not the same person who enrolled the biometric previously. In this sense, it is quite misleading to state that a biometric confirms an identity as it can only confirm that the biometric capture subject is the person previously associated with a set of data.

### 5.3 Identity and biometric identification

Biometric identification is the process of comparing a biometric sample to an enrolled biometric database and returning a list of records from the database (typically ordered by the probability that the person who enrolled the record is the same person who has provided the sample). The matching probability



thresholds, comparison process and the business rules for the system will determine whether the sample is a match of an existing enrolled sample. This process will enable

- Identification of a biometric capture subject whose biometric(s) have already been registered in the biometric database (one-to-many or 'identification'). This does not require any biographic information,
- Confirmation of an identity when an individual provides a claim of identity (e.g. a passport) is compared to a biometric reference sample (one-to-one or 'verification.'), and
- Comparison of a biometric capture subject with a list of biometric reference samples selected using a list of identification references provided by the system where the biometric capture subject sample is compared with each reference sample in turn (watch list matching).

Before implementing biometrics into an IDMS, it is essential to determine the required identification process along with the associated levels of identity assurance. Identity should be defined according to the identification requirements. Consideration should be given to the following which is not exhaustive:

- a) The identity reference that the biometric capture subject will use;
- b) Whether the reliance on evidence of identity is dependent upon the level of activity or access granted, and whether the evidence is based on recent or old activity;
- c) Identification documents and tokens can be appropriated by others or used with the owner's permission, for example a membership card or discount card;
- d) Naming information can change with marriage or in witness protection schemes;
- e) Biometric data of the biometric capture subject can change over time;
- f) Biometric capture subject cannot provide a particular biometric if the biometric is missing or damaged due to injury or disease;
- g) Behavioural biometric data can vary with each attempt.

The risk management approach, in conjunction with appropriate policies and procedures, could provide an acceptable level of assurance when using a biometric identification system.

#### 5.4 Biometric identifiers

A wide range of identifiers can be used in a biometric system. The suitability of an identifier has to be assessed to ensure that it will meet the needs of all the system users and deliver a workable solution.

There are a number of key discriminators to consider when choosing a particular biometric modality. These can include the following:

- **Stability:** A biometric should preserve enough features to ensure that any changes will have minimal impact on the system's ability to identify a candidate correctly;
- **Usability:** The convenience and ease of use of a biometric is a key driver in the adoption and acceptance of a biometric system. Where possible, sensors should be situated so that all people can use them effectively. The system should respond in a timely fashion and should be easy to manage and maintain;

NOTE Further guidance on usability/privacy is given in ISO/IEC TR 24714-1:2008.

- **Privacy:** With increasing scrutiny and public awareness of biometric systems, the privacy of identities stored within a biometric system should be of the utmost importance. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the biometric data subject;

NOTE Further guidance is given in ISO/IEC TR 24714-1:2008

- Cost: The cost of a biometric system should be weighed against the benefit the system will deliver. If the inclusion of a particular biometric identifier is cost prohibitive, and provides little benefit to the overall system, it could be beneficial to look for an alternative;
- Vulnerability: The biometric chosen should be hard to defraud, and the system and sensor devices should be both hardened against attack and alert if tampered with. Also, policies and human monitoring should be employed to mitigate attacks and vulnerabilities where possible.

## 5.5 Human role in biometrics

When integrating a biometric modality into a recognition system, consideration needs to be given to the human role. The solution should consider how a human could process comparisons, the quality of the image (or data), and how the requirements will be different to the automated comparison process. The organization should consider who is allowed to look at the comparison results and different workflow solutions for the human operator. The organization should consider the following:

- Staff qualifications, training, and competencies;
- Screen display;
- Workflow for comparisons;
- Exception handling;
- Data quality required for biometric comparison processes.

## 5.6 Assuring the integrity of the database

It is important to assure the integrity of the database when integrating biometrics into an IDMS and the implementation of a data cleansing process should be undertaken where possible.

Data in an inconsistent state can be a result of a single identity having more than one unique identifier or multiple unique identities having the same identifier. This can arise because of human error, system error, process failure, or because of fraud.

As part of the database assurance process, organizations should be aware that a large amount of data will be created.

An organization or agency accepting biometric data from another body with an enrolment process of a standard lower than the one they themselves use in establishing identities should be aware of the risks associated with the data and take appropriate measures where required.

# 6 Biometric considerations in Identity Management Systems

## 6.1 General

This clause describes items that need to be considered when integrating biometrics into a commercial IDMS.

## 6.2 Capturing and recording biometric characteristics

The value of the biometric sample to the identity system is dependent upon the accuracy and quality of the biometric data captured, and the matching process for linking it to a reference set. The following subclauses explore some of the issues that impact upon the value of the biometric.

### 6.2.1 Capture

All biometric solutions will require a quality capture process, this can include data coming from other systems where the capture process can be controlled, or it might include setting up a full capture

environment. A biometric system can only be as good as the data within it and it is important to ensure that the best possible sample is obtained and quality checked. Items to consider when capturing biometrics include the following:

- Standards – Biometric capture should meet international standards;
- Environment – factors should be considered e.g. lighting, dark walls, safety hazards;
- Quality check – it is highly desirable that the system carries out a quality assessment at the time the data is captured;
- Remote capture – The organization should consider how to capture biometric samples in remote locations or locations that are not within the normal operation of the system (e.g. disaster scene/area);
- Failure to capture – the organizations should consider how it will capture data in a situation where the process cannot be executed.

More information can be retrieved from ISO/IEC 29794-1:2009 and ISO/IEC 19794 (all parts).

### 6.2.2 Process stability and repeatability

As part of the biometric integration into an IDMS solution, the biometric capture process is important and a stable, repeatable capture process is essential. All biometric modalities are subject to variability due to a range of factors, including those connected with the environment, such as lighting, temperature, noise, and the ergonomics of the biometric readers. It is important to consider all affecting factors and mitigate the risks wherever possible. Further variability is introduced by aspects of human behaviour and conditions including pose, facial expression, skin, and medical conditions.

### 6.2.3 Retention and longevity of biometric records

A biometric characteristic can weaken in quality over time. Ageing is a particular issue for most, if not all, biometric modalities, and increase in time since enrolment tends to be associated with an increase in failure to match the biometric correctly.

### 6.2.4 Stability of biometric records

Human factors, such as emotion, fatigue, health, and stress can affect the stability of the biometric record.

## 6.3 Adhesion of biometric characteristics

### 6.3.1 General

It is important for organizations to assess the integrity of the linkage of the biometric data to the identity. If data is coming from multiple sources, there could be different confidence levels for the biometric and identity source of data.

The confidence of information and the constraints on the handling of identity information need to be clearly described in an agreed convention for the IDMS. This is particularly important with data coming from other systems. Biometric data is no different and can have its own confidence rating. As an example, the IDMS can have a high confidence but the biometric data might not be as trusted due to poor quality control at capture. It is important that the whole biometric process, in conjunction with the identity system, is assessed and an appropriate rating given.

An example convention can be as follows:

- A — ALWAYS CONSISTENT — There is no doubt about the authenticity, trustworthiness, and competence of the source. The system or organization supplying the information is consistently