DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 30124

ISO/IEC JTC **1**/SC **37** Secretariat: **ANSI**

Voting begins on:
2015-11-26

Voting terminates on:
2016-02-26

Code of practice for the implementation of a biometric system

Titre manque

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT 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.

Reference number
ISO/IEC DIS 30124:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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

Contents

Page

Foreword 5
Introduction 6
1 Scope 1
2 Conformance 1
3 Normative references 1
4 Terms and definitions 1
5 Symbols (and abbreviated terms) 7
6 General 7
6.1 About recognition systems 7
6.2 About biometric systems 8
6.3 Uses of biometric systems ..... **Error! Bookmark not defined.**
7 Planning for the implementation of a biometric system 10
7.1 General 11
7.2 Biometric modality ..... **Error! Bookmark not defined.**
7.3 Performance parameters 12
7.4 Security 15
7.5 Privacy and data protection 16
7.6 Usability 20
7.7 Accessibility 19
7.8 User Acceptance ..... **Error! Bookmark not defined.**
7.9 Data Capture 26
7.10 Exception Handling 28
8 Acceptance testing a biometric system ..... **Error! Bookmark not defined.**
9 Operating a biometric system 27
9.2 Maintenance 27
9.3 Change management 27
9.4 Management information system data 28
9.5 Fallback arrangements 28
Annex A (informative) Basic principles of a biometric system 29
A.1 General 29
A.2 What is a biometric system? 29
A.3 Biometric recognition 33
Annex B (informative) Relationship between security and false acceptance rates 32
Annex C (informative) Examples of security risks and countermeasures associated with a biometric system 33
C.1 Spoofing 33
C.2 Capture replay 33
C.3 Biometric reference integrity and confidentiality 33
Annex D (informative) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 35
Bibliography 36

EDITORS NOTE CONTENTS TO BE UPDATED PRIOR TO PUBLICATION

© ISO/IEC 2012– All rights reserved

© ISO/IEC 2012– All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 30124 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 37, *Biometrics*.

© ISO/IEC 2012– All rights reserved

Introduction

This International Standard is intended for organizations considering the procurement and implementation of a biometric recognition system.

It provides recommendations and guidance that such organizations can follow to demonstrate good practice in their implementation.

In particular, it helps organizations decide what performance requirements are needed and how to maximize the chances of a successful implementation: it also aids organizations in understanding their duties in respect of the use and governance of biometric data. Biometric recognition systems can be expensive to implement therefore collaboration and joint procurement should be considered between appropriate organizations. Biometric recognition systems frequently need to be interoperable with other systems and this interoperability can be facilitated by use of ISO/IEC 19785 Common Biometric Exchange Formats Framework.

Some countries will have laws or practices in place relating to biometric data that should be considered.

© ISO/IEC 2012– All rights reserved

Information Technology — Code of practice for the implementation of a biometric system

1. Scope

This Code of Practice provides recommendations and guidance for the implementation of a biometric system. In particular it covers:

a) planning for the implementation of a biometric system;
b) acceptance testing a biometric system; and
c) operating a biometric system.

This document focuses on the specific aspects related to the inclusion of a biometric system at the core of a recognition system (where the recognition of people is an important requirement of an application). It should be noted that biometrics is one element of the recognition system

This document has applicability across a wide range of applications that incorporate a biometric system. The recommendations and guidance are intended to support the needs of users in small to medium size organizations without biometric expertise but in charge of requirements capture, planning, procuring and accepting the biometric system whose development is outsourced to a system developer.

The recommendations are equally applicable to off-the-shelf applications that incorporate a biometric system (such as a time and attendance system), as well as bespoke applications where the biometric system requires integration with other systems.

2. Conformance

Although there are no specific requirements in the Code of Practice, it is still important to demonstrate that the organization has followed the guidance in Clauses 7-9. It is also recommended that this be documented through the completion of the Checklist in Annex D (or an equivalent).

3. Normative references

The following referenced documents are indispensable for the application 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 TR 24714-1:2008 Information technology - Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General guidance
- ISO/IEC TR 24741:2007 Information technology - Biometrics Tutorial

4. Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012, Information Technology – Vocabulary – Part 37: Biometrics and the following apply:

4.1
access control
function to determine whether to grant an individual access to systems, resources, facilities, services or information based on pre-established rules and specific rights or authority associated with the requesting party

4.2
accessibility
possibility for everyone, regardless of physical capability or technological readiness, to access resources and

© ISO 2012– All rights reserved

use technologies and services

4.3
application
set of inter-related software components, policies, business processes and information designed to fulfill a particular purpose

4.4
attack potential
measure of the effort to be expended in attacking an IT system, expressed in terms of an attacker's expertise, resources and motivation

NOTE a physical attack on system components can be as or more effective than cyber attacks on the system

4.5
biometric attendant
Agent of the biometric system operator who directly interacts with the biometric capture subject

4.6
authentication
The act of proving or showing to be of undisputed origin or veracity

NOTE 1 Use of this term as a synonym for "biometric verification" or "biometric identification" is deprecated: the term biometric recognition is preferred.

NOTE 2 In this document this term refers to the general act of rather than a specific biometric identification application and biometric identification function

4.7
biometric characteristic
biometric (deprecated)
biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.

NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 2 Distinguishing does not necessarily imply individualization.

4.8
biometric claim
claim that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference

NOTE 1 A biometric claim can be made by any user of the biometric system.

NOTE 2 The phrase "claim of identity" is often used to label this concept.

NOTE 3 Claims may be positive sitive is often used to label this concept..stem.cified or unspecified biometric referencerencecombinations of any of these.y of these.f any of these.the hand, ridge structure of the palm, reled as a specified biometric enrollee; or non-specific – i.e. that the biometric capture subject is or is not among the set or subset of biometric enrollees.

NOTE 4 Biometric claims are not necessarily made by the biometric capture subject.

© ISO 2012– All rights reserved