INTERNATIONAL STANDARD

ISO/IEC 29164

First edition
2011-10-01

Information technology — Biometrics — Embedded BioAPI

Technologies de l'information — Biométrie — BioAPI incorporé

Reference number
ISO/IEC 29164:2011(E)

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
Web www.iso.org

Published in Switzerland

Contents

Page

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.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29164 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

Introduction

The environment for embedded systems differs in many ways from that of a more general computing environment. One difference is that the amount of processing power and/or memory/storage can be more limited in the embedded environment and operating system support and resources can also be more constrained. As a result, implementation of more general purpose interfaces might not be appropriate. In the case of embedded biometric technology, the algorithms and sensors are frequently packaged into hardware/firmware modules.

It can also be the case that the designer of the embedded system is not concerned with details of the biometric technology within its software and firmware and prefers to just integrate an external module that deals with some or all biometric functionalities.

This International Standard is not meant for applications where the integration of biometric functionality is going to be done within the software or firmware of the application. In such cases BioAPI (ISO/IEC 19784-1) is to be used, or its Frameworkless version (see ISO/IEC 19784-1 with Amd.2).

The interface defined in this International Standard provides a direct connection with such biometric modules. The definition of this interface is given by the services to be provided, as well as the message formats for commands to be sent to biometric modules and responses expected from them.

This International Standard is intended to provide a common interface for all those biometric systems where BioAPI (ISO/IEC 19784-1) cannot be implemented. From the historical point of view, as BioAPI does imply relatively large requirements both in processing power and memory capacity, some different approaches have been developed. One of those approaches is the use of BioAPI without the need of using the BioAPI framework, which is one of the most consuming parts of BioAPI. That version is called Framework free BioAPI, and is standardized in the 2nd Amendment to BioAPI. But even that approach, which can be of great help for several applications, such as Biometric Applets or Biometric services in mobile devices which run an Operating System, can be too demanding for embedded systems. Therefore a new approach is standardized in this International Standard, under the name of Embedded BioAPI, which should never be confused with the Framework free version of BioAPI.

Examples of applications where Embedded BioAPI might be used include remote controls, garage door openers, auto ignitions, physical access devices, memory sticks, authentication tokens, and handheld weapons. The utility of a standard interface in this environment is less obvious than for more general purpose processing environments, but addresses two important situations:

— It allows a device (unit into which the data capture device is embedded, e.g. a remote control device) manufacturer to use the same code base for multiple devices/units in his product line that differ only in embedded data capture device/biometric technology (e.g. Device A comes with a built-in fingerprint data capture device/algorithm and Device B comes with a built-in facial recognition camera/capability). This is a configuration management (CM) and efficiency issue (the single code base simplifying CM).

— It allows an OEM data capture device manufacturer who wants to build a single OEM unit/firmware to support multiple device vendors (the same firmware regardless of what device the data capture device unit is embedded within).

Throughout the text of this International Standard, devices suitable to be using Embedded BioAPI will be referred as “Embedded BioAPI subcomponents”. Noting that other kind of devices can also use this International Standard, this notation has been used for improving understanding of the standard. This International Standard does not state any requirement for those devices (e.g. Embedded BioAPI subcomponents) but those needed as to implement Embedded BioAPI.

Information technology — Biometrics — Embedded BioAPI

1 Scope

This International Standard provides a standard interface to hardware biometric modules designed to be integrated in embedded systems which can be constrained in memory and computational power. This International Standard specifies a full interface for such hardware-based biometric modules. This interface, called Embedded BioAPI, is defined by the specification of commands to be implemented by these modules. Such a specification is done in two levels:

— For low level implementations, a frame definition is provided, as well as the coding of all commands and their relevant responses. Being defined as a single-master/multiple-slave half-duplex protocol, these messages can be implemented over any communication interface at the physical and link layers. The definition of such communication interfaces is outside of the scope of this International Standard.

— A C-based function header description, for those manufacturers that want to provide a C-library for integration as a Software Development Kit for the overall embedded system.

Regarding security, this International Standard defines two kinds of devices:

— Type A: devices that, due to lack of processing capabilities, do not implement any kind of security mechanism.

— Type B: devices that implement security mechanisms for achieving confidentiality, integrity and/or authenticity. Use of the Type B kind of devices is recommended. For Type B devices a set of minimum requirements is defined, but the security mechanisms to be used are out of the scope of this International Standard.

Low level implementation is outside of the scope of the normative part of this International Standard, although an informative annex (see Annex B) is provided.

Security mechanisms, although considered in this International Standard, are outside of the scope of this International Standard, and are referred to other relevant standards. In particular, key management is outside of the scope of this International Standard, and is expected to be done prior to the application of this International Standard.

Specifications and requirements for Embedded BioAPI subcomponents, or any kind of devices suitable to implement Embedded BioAPI, are outside of the scope of this International Standard.

2 Conformance

A biometric module conforms to this International Standard by covering all mandatory items in the normative parts. A biometric module conformant to this International Standard can provide additional functionality as long as it does not modify the behaviour stated in this International Standard.

A more detailed list of all conformance requirements can be found in Annex A.

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 19784-1:2006, *Information Technology — Biometric application programming interface — Part 1: BioAPI specification*

ISO/IEC 19784-1/Amd.3:2010, *Information technology — Biometric application programming interface — Part 1: BioAPI specification — Amendment 3: Support for interchange of certificates and security assertions, and other security aspects*

ISO/IEC 19785-1:2006, *Information Technology — Common Biometric Exchange Formats Framework — Part 1: Data Element Specification*

ISO/IEC 19785-3:2007, *Information Technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794 (all parts), *Information Technology — Biometric data interchange formats*

ISO/IEC 24761:2009, *Information technology — Security techniques — Authentication context for biometrics*