ICS 35.240.15
CCS L 70

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 36094-2018

Information technology -- Biometrics -- Embedded BioAPI

Issued on: March 15, 2018 **Implemented on: October 1, 2018**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard uses the translation method equivalent to ISO /IEC 29164.2011 "Information Technology Biometrics Embedded BioAPI".

The documents of our country that have a consistent correspondence with the international documents referenced in this standard are as follows.

---GB/T 26237 (all parts) Information technology biometric identification data exchange format [ISO /IEC 19794 (all

section)];

--- GB/T 28826.2-2014 Information technology common biometric identification exchange format framework Part 2. Biometrics

Do not register the operating procedures (ISO /IEC 19785-2.2006, NEQ)

Introduction

There are many differences between embedded system environments and conventional computing environments. First, the embedded system is processing functions, memory (or storage) is empty

Between, operating system support and resource support are more limited. Therefore, the

practice of configuring more common interfaces for embedded systems may not

Suitable. For embedded biometrics, recognition algorithms and sensors are often packaged into hardware or firmware modules.

Second, embedded system designers do not care about the implementation of the system in biometrics when designing system software and firmware.

Details, but prefer to implement some or all of the biometric features by integrating an external module.

This standard does not apply to applications that integrate biometrics into software or firmware. Used in such applications

BioAPI (GB/T 30267.1-2013) or its frameless version (see ISO /IEC 19784-1 with Amd. 2).

The interfaces defined in this standard provide direct connection to such biometric modules. The interface definition takes into account the services provided by the interface.

And the message format of the command sent to the biometric module and the expected message format of the response from these modules.

This standard is intended to provide a common interface for all biometric systems that do not implement BioAPI (see GB/T 30267.1).

Previously, due to the considerable range of processing power and memory space requirements of BioAPI, there were some different solutions. One of them is

BioAPI is used directly without the BioAPI framework, which is one of the most expensive processing and memory components. This BioAPI version

Called the frameless BioAPI. However, this solution works for several types of applications (such as biometrics installed in mobile devices with an operating system).

Identifying applets and biometric services is a big help, but its requirements go beyond the capabilities of embedded systems. Therefore, this standard

A new solution called Embedded BioAPI was proposed, which is completely different from the above-mentioned frameless BioAPI.

Embedded BioAPI can be used for remote controls, garage openers, car ignitions, access control devices, memory cards, authentication tokens, and

Holding weapons and so on. Compared to the more common application scenarios, the usability of a standard interface in these application environments is not outstanding, but it has

The next two important advantages.

---When multiple devices or components on a manufacturer's product line (only devices or

components with built-in data acquisition devices, such as remote control devices)

Only when there is a difference in the built-in data acquisition device or biometric technology (for example, device A uses built-in fingerprint data)

Acquisition device or algorithm, while device B uses a face recognition camera or function), the standard interface can help the manufacturer to a single generation

The code library meets the needs of multi-device production. And because the single code library helps simplify configuration management, it can increase productivity;

--- Help data acquisition equipment OEMs implement multi-device vendor support with a single OEM component or firmware (ie no data to consider

What kind of equipment is built into the acquisition device).

In this standard, a device suitable for deploying an embedded BioAPI is called an "embedded BioAPI subcomponent." Please note that other types of settings

This standard can also be used, but for a better understanding of this standard, we will only describe it here around the embedded BioAPI. This standard

The requirements for devices such as embedded BioAPI subcomponents are not specified, but the requirements for implementing the embedded BioAPI devices are specified.

Information Technology Biometrics Embedded BioAPI

1 Scope

This standard provides a hardware biometric identification module designed for embedded systems that are integrated into memory space and limited computing power.

Standard interface. This standard specifies a complete interface for such hardware-based biometric modules. This interface is called an embedded BioAPI.

It is defined by the specification of the commands that these modules are to implement. The specification is divided into the following two layers.

--- Underlying implementation, which defines a framework for the underlying implementation and the encoding of all commands and their corresponding response pairs. Make

For a single-master/multi-slave half-duplex protocol, these messages can be implemented at any physical and link layer via any communication interface. This

The definition of some communication interfaces is not covered by this standard;

--- A header description of a C-based function for manufacturers who have the following ideas. Provide a C library as a whole

An integrated software development kit for embedded systems.

Regarding security, this standard defines two types of equipment.

--- Class A equipment. This type of equipment does not implement any security mechanism due to lack of processing power;

--- Class B equipment. This type of equipment implements a security mechanism to achieve confidentiality, integrity and/or authenticity and is recommended for use. This standard

A minimum set of requirements for Class B equipment is defined, but the safety mechanisms of the equipment are outside the scope of this standard.

The underlying implementation is not covered by the specification part of this standard, but is provided as an informative annex (see Appendix B).

Although the safety mechanism is considered in this standard, they are not within the scope of this standard. Please refer to other relevant standards. Especially the key

Management is also outside the scope of this standard and is expected to be addressed prior to the application of this standard.

Specifications and requirements for embedded BioAPI sub-components or any device suitable for implementing embedded BioAPI are outside the scope of this standard.

2 Compliance

A biometric module that claims to comply with this standard shall cover all mandatory requirements of the normative requirements of this standard. As long as the standard is not modified

Under the premise of the stated behavior, the biometric module conforming to this standard can provide additional functionality.

See Appendix A for a more detailed list of compliance requirements.

3 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article.

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 28826.1-2012 Information technology - Common biometric identification exchange format framework Part 1. Data element specification

(ISO /IEC 19785-1.2006, MOD)

GB/T 30267.1-2013 Information technology biometric identification application