

ICS 35.240.15

CCS L 70



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 28826.4-2022

**Information technology - Common biometric exchange formats
framework - Part 4: Security block format specifications**

Issued on: October 12, 2022

Implemented on: May 1, 2023

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

Table of Contents

Preface	
Introduction	
1 Scope	1
2 Normative references	1
3 Terms and Definitions	2

foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1. Structure and Drafting Rules for Standardization Documents" drafting.

This document is part 4 of GB/T 28826 "Framework for Public Biometric Identification Interchange Formats for Information Technology". GB/T 28826

The following parts have been released.

- Part 1. Data element specification;
- Part 2. Operating procedures for biometric identification registration agencies;
- Part 4. Security block format specification.

This document is modified to adopt ISO /IEC 19785-4.2010 "Information Technology Public Biometric Identification Interchange Format Framework Part 4

Sub. Security Block Format Specification".

Compared with ISO /IEC 19785-4.2010, this document has made the following structural adjustments.

a) 5.8.2.1 corresponds to the suspension section of 5.8.2 of ISO /IEC 19785-4.2010, and 5.8.2.2~5.8.2.3 corresponds to ISO /IEC 19785-

4.5.8.2.1~5.8.2.2 of.2010;

b) 5.8.3.1 corresponds to the suspension section of 5.8.3 of ISO /IEC 19785-4.2010, and 5.8.3.2~5.8.3.3 corresponds to ISO /IEC 19785-

4.5.8.3.1~5.8.3.2 of.2010.

The technical differences between this document and ISO /IEC 19785-4.2010 and their reasons are as follows.

a) The general security block format of domestic commercial ciphers (see Chapter 1) has been added in "Scope" to facilitate the understanding and application of this document;

b) In "Terms and Definitions" specifically listed "biometric identification (of), biometric identification (of), biometric identification, biometric number

Data block, biometric information record, CBEFF biometric organization, security block, security block format, security block format identification

character, security block format owner, standard biometric data header, BioAPI unit, ACBio instance, biometric authentication

Context, biometric processing unit, and message authentication code" are definitions of 15 terms (see Chapter 3), so as to facilitate the definition of this document

Understanding and application; "Biometric Organization Identifier" (3.6) and "Object Identifier" (3.15) have been added to facilitate the identification of 2

differentiated understanding and application of terminology;

c) The "Abbreviations" specifically reflect the eight abbreviations "ACBio, BDB, BPU, CBEFF, CRL, MAC, SB, SBH"

The full name and Chinese interpretation are used to facilitate the understanding and application of this document (see Chapter 4), so ISO /IEC is no longer cited

19785-1, ISO /IEC 24761, ISO /IEC 9798-6 and REC3852;

d) Added 6 abbreviations "ASN.1, BER, BioAPI, DER, PER, XER" in "Abbreviations" (see Chapter 4), so that

for the understanding and application of this document;

e) Replaced ISO /IEC 8824-1 (see 5.8.1.1, 7.8.1.1) with the normatively quoted GB/T 16262.1 to adapt to my country's technical standards

technical conditions;

f) Replaced ISO /IEC 8825-1 (see 5.4, 6.4, 6.8, 7.4) with the normatively quoted GB/T 16263.1 to adapt to my country's

Technical conditions;

g) Replaced ISO /IEC 8825-2 (see 5.4, 6.4, 7.4) with the normatively quoted GB/T 16263.2 to adapt to my country's technology

condition;

h) Replaced ISO /IEC 8825-3 (see 5.4, 6.4, 7.4) with the normatively referenced GB/T 16263.4 to modify

The quotation of ISO /IEC 19785-4:2010 is wrong, and adapt to the technical conditions of our country;

i) Replaced ISO /IEC 19785-1 (see 5.8.1.3) with the normative referenced GB/T 28826.1 to adapt to my country's technology

condition;

j) The normative reference document GB/T 28826.2-2020 (see 7.2, 7.4) is added to standardize the general security block of domestic commercial ciphers

format for registration requirements;

k) The normative reference document GB/T 32918.2 (see 7.8.3.1) has been added to standardize the registration of the general security block format of domestic commercial ciphers.

record requirements;

l) The normative reference document GB/T 33560-2017 (see 7.8.3.2.1, 7.8.3.2.2) is added to standardize domestic commercial encryption

Registration requirements in secure block format;

m) The normative reference document GB/T 35275-2017 (see 7.8.3.2.1, 7.8.3.2.2) is added to standardize domestic commercial encryption

Registration requirements in secure block format;

n) The normative reference document GB/T 38635.2 (see 7.8.3.1) has been added to standardize the registration of the general security block format of domestic commercial ciphers.

record requirements;

o) Modify ISO /IEC 19785-2 from an informative reference to a normative reference, because the registration operation specified in ISO /IEC 19785-2

Operating procedures are normative requirements;

p) Added support for domestic commercial encryption algorithms, in order to apply the national encryption system (see Chapter 7);

q) Added "ASN.1 code of general security block format for domestic commercial ciphers" (see Appendix B), to illustrate that ASN.1 domestic commercial ciphers

The specific content of the code security block format.

The following editorial changes have been made to this document.

a) The ISO /IEC 19785-4:2010/CORR1:2013 "Information Technology Public Biometric

Identification Interchange Format Framework No. 4

Part. Technical Corrigendum 1 of "Security Block Format Specification" is incorporated into the corresponding clauses, and the outer margin of the modified clauses

The position is marked with a vertical double line (||), and the original Appendix B is deleted according to the technical corrigendum;

b) Deleted the reference to ISO /IEC 19785-2 "Information technology public biometric identification exchange format framework - Part 2.Biometrics

Informative references to the Operating Procedures for Sign Identification and Registration Agencies.

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

Introduction

Biometric-based authentication systems and applications are expected to support multiple biometric devices from different vendors. male

The Biometric Exchange Format Framework (CBEFF) facilitates biometric data exchange developed by different vendors by simplifying the exchange of biometric data.

Interoperability of signature recognition applications and systems.

GB/T 28826 "Information Technology Public Biometric Identification Interchange Format Framework" is proposed to be composed of 4 parts.

--- Part 1.Data element specification. The aim is to define a standardized project enabling the exchange of biometric data.

--- Part 2.Operating procedures for biometric registration agencies. The purpose is to stipulate the biometric identification registration mark used in the country

Requirements for identifiers, registration agencies, registration procedures, registration applications, and registration maintenance.

--- Part 3.Maintainer format specification. The purpose is to CBEFF biometric identification organization ISO /IEC JTC1/SC37

Defined and described according to the three maintainer format specifications registered in ISO /IEC 19785-2.

--- Part 4.Security block format specification. The purpose is to CBEFF biometric identification organization ISO /IEC JTC1/SC37

Two security block formats defined and registered according to ISO /IEC 19785-2, and the National Information Technology Standardization Committee biological