

ICS 03.360; 35.240.40
CCS A 11



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

GB/T 27912-2011

Financial services -- Biometrics -- Security framework

金融服务 生物特征识别 安全框架

(English Translation)

Issued on: December 30, 2011

Implemented on: February 1, 2012

Issued by: Standardization Administration of China

Table of Contents

Preface	
Introduction	
1 Scope	
2 Compliance	
3 Normative references	
4 Terms and definitions	
5 Acronyms	
6 Biometrics Overview	
10 7 technical considerations	
The basic principle of structure 8 Biometrics	
9 Management and security requirements	
22 10 Security Infrastructure	
11 Biometric identification of control objectives	
Appendix A (informative) Event Log	
Appendix B (normative) Biometric Registration	
Annex C (normative) Security Considerations	
Annex D (normative) Safety requirements for biometric devices	
Annex E (informative) existing applications	
References	

Foreword

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

This revised standard adopts ISO 19092-1:2006 "Financial Services Biometrics - Part 1. Safety Framework" (in English).

This standard and ISO 19092-1:2006 technical differences are as follows.

Content a) delete the text involved in ISO 19092-2 (ISO 19092-2 by ISO proposal has been aborted, and delete content and it does not affect the integrity of the standard);

b) delete the original standard 10.1.2, because the key name in this section has been terminated all from ISO 19092-2;

c) 10.1.2 (original standard 10.1.3) digital signature "hash algorithm should meet the relevant ISO standards (or an equivalent national standard) Specific requirements "is

replaced by" hashing algorithm should meet the specific requirements of the relevant national standards ";

d) Remove 10.1.2 (formerly Standard 10.1.3) digital signature column item "should be hashed through plain text data by the text and one or more values

BiometricHeader BiometricData type of composition, in addition to the type and BiometricHeader Outside BiometricData value it should also include the value of a IntegrityBlock type ";

e) "key management, as shown in 10.1.2 and 10.1.3 (former standard 10.1.3 and 10.1.4) in Table 1, shall be in accordance with the relevant ISO , specific provisions of ISO/IEC standards (or an equivalent national standard) implementation, such as ISO 11568, or ISO/IEC 11770 "to" key management techniques should be specific provisions related to the implementation of national standards ";

f) delete the original standard in Table 1 (subsequent table numbers are minus 1);

g) 10.1.3 encryption-based data confidentiality purposes of "encryption algorithm should be relevant ISO standards (or equivalent national standard) Specific provisions "with" specified in the national standard encryption algorithm should be related to the implementation of ";

h) 11.3.1 12 tables (13 tables in the original standard) of 147. "key generation using key generation algorithm, as specified in ISO standard (or National standards are equivalent) "to" key generation algorithm using the key generation, particularly in the relevant national standards ";

i) Appendix A.3.4 column item d) the "reference template description (for example, biometric OID)" was changed to "reference template described (Example for example, biometric target identifier) ";

j) Remove ISO 19092-1:2006 Annex B.2, because the individual identification criteria as described in the premises not suitable for China's national conditions.

This standard also made the following editorial changes.

--- The original text of the "international standard", "ISO 19092", "this part of ISO 19092," and "this part" to "this standard";

--- Delete foreword international standards;

--- For the sake of full unity, to define the equal error rate of 4.21 in the "crossover rate (crossoverrate)" was renamed "crossover error rate (Crossovererrorrate) ";

--- 9.3.3 column item a) re-registration requirements mentioned. "The use of raw materials credentials, rather than existing biometric template. This method can provide adequate assurance level, depending on the existing biometric templates and technical reliability and Usability "to" use the original voucher material, rather than existing biometric template. This method provides sufficient Guaranteed level, depending on the original certificate of

reliability and availability of materials "(errata);

--- Table 22 11.4.5 Integrated Circuit Card (ICC) life cycle control 300 "Unless CDF active or re when active, otherwise the IC can not be used for financial transactions "to" unless CDF active or re-active, Otherwise ICC can not be used for financial transactions "(errata);

--- C.8 in the "single-factor biometric identification system using a simple probabilistic model [20], the system does not appear in the wrong N users Pr is the probability of mismatch "to" single-factor biometric identification system using a simple probabilistic model [20], with the N System error probability Pr of matching households appear as "(errata).

The standard proposed by the People's Bank of China.

This standard by the National Standardization Technical Committee on Finance (SAC/TC180) centralized.

Introduction

With the introduction of computer technology, the business model has changed significantly. Replace the previous paper electronic trading transactions, reduces costs this improves the efficiency. These transactions are in an open network environment, there is a risk of data corruption, the financial sector needs to take appropriate Measures to deal with these risks.

Biometrics, the "who you are or what to do," the means of identification, there have been a number of years, including such as fingerprint recognition, voice recognition Do not, eyes scanning, face recognition like. Biometrics in increased reliability at the same time, gradually reduce the cost to the financial industry Implementation possible.

This standard describes the use of biometric identification technology as a mechanism to protect remote electronic access to the financial industry or local physical access Mechanisms and processes.

Biometrics can be used as a physical or logical access to personnel identification. Can include logical access to applications, services or grant Access. This standard promotes biometric applications in the financial industry, and promote the biometric information of a commercial management Part of the organization's information security management. This standard through the use of biometric technology to provide higher strength and more a result of differential mode Sub-authentication mechanism, public key infrastructure (PKI) to provide stronger authentication mechanism. In addition, the standard allows duplicate acknowledgment generate digital signatures People actually have access to the private person.

Widely used biometric recognition system built on a number of factors, existing biometric technology on these factors table Now different, these factors include.

--- Convenience and ease of use;

- External level of safety;
- performance;
- Non-invasive.

The standard authentication mechanisms discussed limited to closed user groups, community members have agreed to use biometric technology for identity Recognition. These agreements may be the dominant form (such as service agreements), or implicit form (such as access to a facility that is shown to have a transaction executed Motivation). Uncertain regulatory system personnel are not within the scope of this standard discussion.

This standard describes a technique for maintaining the integrity and confidentiality of biometric information, and provide authentication mechanism. However, the standard does not Ensure implementation of an adequate safety. Financial institutions have a responsibility to set the appropriate whole business processes and make the necessary controls to ensure business Process safe operation. In addition, in order to verify compliance with this standard of consistency, control measures should include appropriate audit tests.

Financial Services Biometrics Security Framework

1 Scope

This standard specifies the use of the financial industry biometric identification mechanisms personnel identity security framework introduces biometric identification technology Type describes the relevant application problems. This standard also describes the implementation architecture, details the minimum requirements for safe and effective management, but also for Professional provides control objectives and recommendations.

The criteria include.

- Using biometric recognition technology, by verifying the claimed identity or identify their individual identity of persons involved in financial services and Employee identity identification;
- Based on the risk management requirements of the registration certificate submitted by the user for confirmation to support authentication;
- Throughout the life cycle, including registration, transmission, storage, identification, and termination processes, biometric letter Information management;
- Biometric information security in their life cycle, including data integrity, origin authentication and confidentiality;
- Biometric mechanism in logical and physical access control applications;
- Protect financial institutions and their customers control measures;
- Throughout the biometric information life cycle used in the physical hardware security.