

ICS 03.060
CCS A 11



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

GB/T 21080-2007

**Banking and related financial services -- Sign-on authentication
based on symmetric algorithm**

银行业务和相关金融服务 基于对称算法的签名鉴别

(English Translation)

Issued on: September 5, 2007

Implemented on: December 1, 2007

Issued by: Standardization Administration of China

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms, Definitions and Abbreviations
4 Signature Verification
5 Protection
6 Interoperability Protocol Specification
Appendix A (informative) The limitations of the standard

Foreword

This standard is identical with ISO 11131:1992 "Banking and related financial services signature verification" (in English).

For ease of use, this standard made the following editorial changes.

- a) Remove ISO foreword;
- b) "this International Standard" be replaced by "this standard";
- c) According to the current actual development of the computer industry, increasing the informative Appendix B.

Appendices A and B are informative appendices.

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

This standard by the National Standardization Technical Committee on Finance.

Introduction

Financial institutions are increasingly using electronic communication technology to provide more timely and accurate services to its customers to meet individual customers' demand. The technology continues to strengthen customers direct access to computer applications (or log) financial institutions. Specific examples include funds Transfer and cash management services.

Historically, the financial industry commonly used user (user identification name) Personal identifiers used in combination with a secret password as provide consumers direct Then

access to the standard method of service provider systems.

However, the effectiveness of the password system has limitations. Authenticate the user can use a variety of methods to crack passwords, for example, it can be speculated Out, he was tapped or publicly displayed. Counterfeiting and reproduction are also two possible threats.

--- Counterfeiting is to steal passwords for entities by displaying imitation, counterfeiting is usually accompanied by other attacks, such as data tampering;

--- Is the playback recently recorded once again demonstrated effective exchange used to produce unauthorized effect.

The two sides shared common key security signature verification procedures need to achieve a large number of conditions, including the following.

- a) holding identification system nodes complete the hardware and software;
- b) maintaining the authentication information between the supplicant and the complete authorized person, such as. assign a user identifier (user name), password selection, mouth Change orders, disrupting access method, the signature failed attempts audit;
- c) after a successful login to keep the entire session identified during continuity;
- d) maintain the ability to audit failed login attempts;
- e) ensure the integrity and resistance to crack misuse of Key Management System;
- f) ensure the confidentiality of transmitted authentication information;
- g) to provide detection reproducing method validation of authentication information.

GB/T 21080-2007/ISO 11131:1992 Banking and related financial services Signature-based identification of symmetric algorithms

1 Scope

This standard implements the introduction of conditions f) and conditions g). It specifies the entity requesting access and authorization to allow access to three entities Species Signature Verification mode.

- a) by personal password authentication information (PAI) to authenticate the user, such as;
- b) by a unique user key to authenticate the user;
- c) key node by node unique identification.

This standard uses a symmetric (key) algorithm, and the requesting party licensors symmetric algorithms use the same key.

Chapter 6 gives an agreement to meet the requirements of this standard instance can be

obtained interoperability instance. Appendix A describes the present standard Some limitations exist. Appendix B describes some of the limitations of the standard specification.

2 Normative references

The following documents contain provisions which, through reference in this standard and become the standard terms. For dated references, subsequent Amendments (not including errata content) or revisions do not apply to this standard, however, encourage the parties to the agreement are based on research Whether the latest versions of these documents. For undated reference documents, the latest versions apply to this standard.

GB/T 15277-1994 Information processing 64bit block cipher algorithm works (eqv ISO 8372. 1987) ISO 8730:1990 requirements for banking message authentication (wholesale) ISO 8732. 1988 Banking - Key Management (Wholesale) ISO 10126-1:1991 Banking packet encryption program (wholesale) - Part 1. General principles ISO 10126-2:1991 Banking packet encryption program (wholesale) - Part 2. DEA algorithm

3.1 Terms and Definitions

The following terms and definitions apply to this standard.

3.1.1

Used to identify the key.

3.1.2

Encrypted information.

3.1.3

One key is available to authorized time period, or in a given system remain valid key for a specified period of time.

3.1.4

Ciphertext (unreadable) is converted to plain text (readable) process.

GB/T 21080-2007/ISO 11131:1992