

ICS 35.240.40

CCS A 11



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

GB/T 27927-2011

**Banking and related financial services -- Triple DEA-Modes of
operation -- Implementation guidelines**

银行业务和相关金融服务 三重数据加密算法操作模式 实施指南

(English Translation)

Issued on: December 30, 2011

Implemented on: May 1, 2012

Issued by: Standardization Administration of China

Table of Contents

Preface

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviations

5 5 Specification

6 3-DEA operation modes

Appendix A (Informative Appendix) 3-DEA operation mode ASN.1 syntax

Password Characteristics Appendix B (Informative Appendix) 3-DEA operation mode

Aspects of Annex C (informative) key group encryption should be noted that

References

Foreword

This revised standard adopts ISO/T R19038.2005 "Banking and related financial services - Triple Data Encryption Algorithm operation mode Implementation Guide "(in English).

This standard is based on ISO/T R19038.2005 redrafted with ISO/T R19038.2005 technical differences are as follows.

- a) The standard "TDEA" According to China habits changed to "Triple Data Encryption Algorithm" (referred to as the "3-DEA" herein) (superscript Quasi-body part of the need to distinguish between reservations "triple DEA" argument);
- b) To facilitate the user's understanding of the standard text, add a term. "error propagation" (see 3.20);
- c) 5.5 for unnumbered, untitled Table number. Table 1DEA function block execution schedule, the following table No. postponed.
- d) in 6.6.1.1, the 7.4 TCFB with only difference is fed back to the data block shift function is not Oi Ci " Amended to read "and 6.4 TCFB only difference is fed back to the data block shift function is not Oi Ci" (errata);
- e) For ease of understanding, B.3.2 title in the "streamcipher" translated as "pseudo-random sequence of vectors {Oi}".

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

- a) the original text of the "technical report" to the "standard";
- b) Delete ISO/T R19038.2005 Foreword by modifying the ISO/T R19038. Introduction 2005.

This standard Annex A, Annex B, Annex C is informative appendix.

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

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

Introduction

To strengthen the DEA (Data Encryption Algorithm) strength and prolong its life cycle, it is recommended to use the Triple Data Encryption Algorithm (3-DEA) operation mode. 3-DEA mode of operation greatly enhance the strength of a password-protected, since these algorithms based on DEA, therefore, users and vendors can Faster familiar with them. Since the 3-DEA operation mode can be backward compatible with existing DEA mode of operation, financial institutions can use 3-DEA extended Long DEA safety lifecycle investment protection standard DEA technology.

Each operating mode has its advantages and characteristics. Selection of a particular mode of operation, implementation and use depends on the security to financial institutions Seeking, risk acceptance and operational requirements, which are not within the scope of this standard. If participants use the same mode of operation and shared secret Key, then the need to use this standard as defined herein 3-DEA operation mode according to the parties to provide the basis for interoperability.

This standard does not replace the standard 3-DEA DEA algorithm and ISO/IEC 18033 as specified. DEA is a 3-DEA operation mode Type foundation. 3-DEA uses advanced computing technology and cryptanalysis techniques, provides greater security. 3-DEA available hardware, Software, or a hybrid implementation.

This standard provides implementation guidance ISO/IEC 10116 in the specified operating mode.

Financial institutions have a responsibility to establish a comprehensive security process that includes the necessary control measures to ensure that the above process in a secure way real Shi, and respond to audit the implementation process to confirm that the process of compliance with safety procedures.

Banking and related financial services Triple Data Encryption Algorithm Operation mode Implementation Guide

1 Scope

This standard provides the user with the enhanced data encryption and secure effective implementation of the technical support 3-DEA operation mode and details data. The mode of operation of the 3-DEA operation described for the encryption and decryption operations. The standard mode is described using ISO/IEC 18033-3 specified in the block cipher mode of operation to achieve (in ISO/IEC 10116 as specified) of 3-DEA operation.

3-DEA operation mode can be used to finance wholesale and retail financial services applications. This standard enables interoperability and products with 3-DEA operation mode of application of standards development provides the foundation. The standard will use DEA and other ISO standards used together.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

Data integrity mechanisms ISO/IEC 9797-1 Information technology - Security techniques used block cipher algorithm cryptographic check function ISO/IEC 10116 Information technology - Security techniques n-bit block cipher mode of operation ISO/IEC 18033-3 Information technology - Security techniques - Encryption algorithms - Part 3. Block operator

3 Terms and Definitions

The following terms and definitions apply to this document.

Birthday phenomenon There are a relatively small group of n members of at least two people may have a common phenomenon birthday.

Example. When $n = 23$, the probability of more than $1/2$. If a person from the m digital alternative to each other may randomly pick one of the subjects in the n $p = 1 - e^{-n^2/2m}$ in the above experiments, the expected number of trials before the same value was found to be approximately $(\pi m/2)^{1/2}$. Which indicates that the use of hybrid key 64-bit block encryption operation, if a person owns 232 plaintext/ciphertext pairs and 232 generated by the random input ciphertext block of text dictionary, it should be considered an unknown cipher text block will be searched from the dictionary (see Ref. [11]).

Block; grouping block Binary string Example. divided into a given length of plaintext or ciphertext, each fragment is called a block (packet). Plaintext (ciphertext) from left to right by-block encryption (decryption). In the present Standard, for TCBC, TCBC-I, TOFB and TOFB-I mode, plaintext and ciphertext is divided into 64-bit block, but for

TCFB and TCFB-P mode, it supports an 8-bit and 64-bit plaintext message and to encrypt and decrypt ciphertext block.