Chinastandards.org

ICS 35.240.40
CCS A 11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21078.3-2011

Banking -- Personal identification number (PIN) management and security -- Part 3: Guidelines for PIN handling in open networks

银行业务 个人识别码的管理与安全 第3部分：开放网络中PIN处理指南

(English Translation)

Issued on: December 30, 2011 **Implemented on: February 1, 2012**

Issued by: Standardization Administration of China

Preview: page 1 of 4 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-21078-3-2011

Chinastandards.org

Table of Contents

Foreword

Introduction

1 Scope

2 Terms and definitions

Foreword

GB/T 21078 "Banking - Personal Identification Number management and security" is divided into the following three parts.

--- The first part 1. ATM and POS systems basic principles and requirements for online PIN processing;

Part --- Article 2. ATM and POS systems offline PIN processing requirements;

--- Part 3. Guidelines for PIN handling in open networks.

This section GB/T 21078 Part 3.

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

This part identical with ISO/T R9564-4.2004 "Banking - Personal Identification Number management and security - Part 4. Open network Network in PIN Processing Guide "(in English).

This part of ISO foreword deleted.

This section proposed by the People's Bank of China.

This part of the National Standardization Technical Committee on Finance (SAC/TC180) centralized.

This section is responsible for drafting units. China Financial Computerization Corporation.

Participated in the drafting of this section. Industrial and Commercial Bank of China, Bank of China, Bank of Communications, China People's Bank branch in downtown Xinghua, China silver Union Company.

Introduction

Open Network Environment is a high-risk environment. For PIN-based transactions, especially so because the card issuer or acquirer of PIN Input devices are uncontrollable. In many cases, the cardholder is to decide what kind of network access equipment.

Preview: page 2 of 4 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-21078-3-2011

This section provides a guide to help reduce the payment system participant PIN leakage risks in an open network system, and to prevent fraud that may occur in the payment system GB/T 21078.1 and GB/T 21078.2 covered by the disclosure with the PIN. Its purpose PIN is to define a minimum safety standards in an open network environment. If the PIN data in this environment of inadequate security, the card also is compromised, then both (card data and PIN) there is a high likelihood of being fraudulent used in ATM, POS or open network environment.

Authentication mechanism depends on the integrity of confidential PIN and cardholder data. In the open network environment, due to the lack of control makes PIN protection becomes difficult, therefore, to protect cardholder data is necessary, which can be in an open network environment and PIN card data theft Leakage caused by the risk of fraud is minimized.

Banking - Personal Identification Number management and security Part 3. Guidelines for PIN handling in open networks

1 Scope

This section provides an open network system processing guidelines of PIN; PIN no direct management control in issuer and acquirer Under the system environment, or prior to the occurrence of the transaction PIN input device and the acquirer does not matter the situation, for the management and processing of PIN debit cards issued the transaction provides best practices from the financial services security measures.

This section applies to the need to verify the PIN debit card transactions initiated and apply to be responsible for end-use in an open network system and PIN PIN input device implemented organizational management techniques.

This section does not apply to.

PIN management and security --- online PIN environment, GB/T 21078.1 and GB/T 21078.2 contains the contents;

--- Approved PIN encryption algorithm;

--- Prevent the user or card issuer and its agents authorized employee misuse lost or intentionally taken with PIN protection;

--- Privacy of non-PIN transactions;

--- Protection of transaction messages against modification or replacement, such as online authorization response;

--- Prevent replay PIN or transaction;

--- Specific key management;

--- By the server-based applications (for example. Wallet) to access and card data;

Preview: page 3 of 4 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-21078-3-2011

--- Financial institutions laying cardholder activation, secure PIN entry device.

2 Terms and definitions

The following terms and definitions apply to this document.

Acquirer

From the square by the card to obtain transaction-related data and data submitted to the agency or its agent switching system.

Leak compromise

destruction of privacy and (or) security.

Encryption encipherment Using some encoding mechanism to translate text to an unauthorized person can not understand the form.

Integrated circuit card (IC card) integratedcircuitcard (ICC) ID-1 card type, defined according to GB/T 14916, GB/T 15120, GB/T 15694 and GB/T 17552, in which is embedded a One or more integrated circuits.

Note: Refer to GB/T 16649.1.

Issuer

Have a primary account organization identified.

Preview: page 4 of 4 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-21078-3-2011