ICS 35.240.15
CCS L 64

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 30001.4-2013

Information technology - Mobile payment based on radio frequency - Part 4: Card application management and security

信息技术 基于射频的移动支付 第4部分：卡应用管理和安全

Issued on: October 10, 2013 **Implemented on: May 1, 2014**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;
Standardization Administration of the PRC

Table of Contents

Foreword

GB/T 30001 "Information technology based on radio frequency mobile payment" is divided into five parts.

--- Part 1. RF interface;

--- Part 2. card technology requirements;

--- Part 3. Technical Requirements;

--- Part 4. Card application management and security;

--- Part 5. RF interface test methods. This section GB/T 30001 Part 4. This section drafted in accordance with GB/T 1.1-2009 given rules. Please note that some of the content of this document may involve patents. Release mechanism of the present document does not assume responsibility for the identification of these patents. This part of the National Information Technology Standardization Technical Committee (SAC/TC28) and focal points. This section drafted by: China Electronics Standardization Institute, Wuhan Tianyu Information Industry Co., Ltd., China UnionPay has shares Ltd., Shanghai Fudan Microelectronics Group Co., Ltd., Beijing Watchdata System Co., Ltd., Beijing Tongfang Microelectronics Co., Ltd., China Mobile Communications Corporation, China Telecom Group, China United Network Communications Group Company Limited, Putian Information Technology Research Institute. The main drafters of this section. Geng force, Zhao Bo, Chai Hongfeng, Dongfeng Hua, Gao Lin, single undefeated, Feng Jing, Li Jie, Qian Jin, Ding Yimin, Li Wei, Yan Guangwen. IT RF-based mobile payment Part 4. The card application management and security

1 Scope

China's national standard for the card application management and security of radio frequency mobile payment. It is Part 4 of GB/T 30001 and specifies how payment applications are loaded onto, managed on and removed from the secure element, and the security requirements governing those operations. This is the part that decides how mobile payment actually works as a business. The secure element is a piece of hardware in someone's pocket, and a bank that wants to put its payment application onto it has to do so remotely, over the air, through infrastructure it does not own, onto an element owned by a mobile operator or a handset manufacturer. That operation - provisioning - is the thing that makes mobile payment different from a plastic card, which is personalised once in a factory. Everything that follows from it is a security problem. The element has to be able to tell a legitimate provisioning request from an attacker's; the issuer has to be able to load an application without the element's owner reading its keys; the element's owner has to be able to manage the space without the issuer's application being altered; an application has to be revocable when a card is cancelled or a phone is lost; and none of the applications on the element may reach any other. The standard therefore specifies the roles and the key hierarchy that separates them, the security domains within the element, the secure channel over which a management operation is carried out, the commands for loading, installing, locking and deleting an application, and the lifecycle of both the element and each application on it. Issued on 10 October 2013 and in force since 1 May 2014.

This section GB/T 30001 specifies the RF-based mobile payment card security unit multi-unit management application security, and more Channel management, life cycle

management, system security unit and multi-application platform security requirements for managing security requirements. This section applies to RF-based mobile payment card design, production and use.

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.

GB/T 30001.1 pay Part 1 RF interface RF-based mobile

3 Terms and Definitions

GB/T 30001.1 defined and the following terms and definitions apply to this document.

3.1 Safety unit securityelement The main devices composed of mobile payment card radio frequency based primarily responsible for transaction security storage and computing capabilities critical data.

3.2 Application application To meet the specific functions required data structures, data elements and program modules. [GB/T 16649.4-2010, the definition 3.3]

3.3 Application provider applicationprovider Provide physical security unit application components.

3.4 Safety Unit Platform systemplatformonsecurityelement The component responsible for the basic functions of the security unit.

3.5 Security domain securitydomain Provides control, security and communications support to the card application provider entity.

4 Abbreviations

The following abbreviations apply to this document. ADF application definition file (ApplicationDefinitionFile) AID Application Identifier (ApplicationIdentifier)