ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31502—2015

信息安全技术
电子支付系统安全保护框架

Information security technology—
Security protect framework of electronic payment system

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号与缩略语 …… 2
4.1　符号表示 …… 2
4.2　缩略语 …… 3
5　电子支付系统描述 …… 3
5.1　电子支付系统模型 …… 3
5.2　电子支付系统工作模式 …… 7
5.3　受保护资产 …… 8
6　安全问题定义 …… 10
6.1　概述 …… 10
6.2　威胁 …… 10
6.3　组织安全策略(SOP) …… 14
6.4　假设(SAS) …… 17
6.5　安全问题定义理由 …… 17
7　安全目的 …… 17
7.1　概述 …… 17
7.2　针对评估对象[TOE]的安全目的(OET) …… 18
7.3　针对评估对象[TOE]运行环境的安全目的(OTE) …… 18
8　安全功能要求 …… 19
8.1　概述 …… 19
8.2　安全审计(FAU 类) …… 19
8.3　通信(FCO 类) …… 32
8.4　密码支持(FCS 类) …… 35
8.5　用户数据保护(FDP 类) …… 35
8.6　标识和鉴别(FIA 类) …… 40
8.7　安全管理(FMT 类) …… 40
8.8　TSF 保护(FPT 类) …… 42
9　安全保证要求 …… 43
10　国家相关标准的部分依从性分析 …… 43
11　组织安全策略示例 …… 43
附录 A（资料性附录）　电子支付系统的行为模型 …… 44

附录 B（规范性附录） 安全问题定义理由 …… 69
附录 C（规范性附录） 安全目的理由 …… 74
附录 D（规范性附录） 安全保证要求 …… 78
附录 E（规范性附录） 对国家相关标准的部分依从性分析 …… 80
附录 F（资料性附录） 组织安全策略示例:可疑交易预警规则 …… 82
参考文献 …… 87

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京多思科技工业园股份有限公司、中国农业银行、中国金融电子化公司、国家信息安全工程技术研究中心、东方集团网络信息安全技术有限公司、北京大秦兴宇电子有限公司、北京天宏绎网络技术有限公司、北京科蓝软件系统有限公司、长城瑞通(北京)科技有限公司、重庆银行、南充市商业银行。

本标准主要起草人:刘大力、李宽、沈敏锋、韩琳琳、吴义章、吴铮、刘运、文仲慧、沈昕立、康伟、张磊、于敬新、崔新杰、罗勇、夏鹏轩、闫凤如、陈辉武、王庆元、左小波、邱岩、张春阳、黄光伟、邢呈礼、高艳芳、王州府。

引　言

本标准以国际通行的信息技术安全性评估准则为基础，结合我国现阶段电子支付系统的特点，按照我国有关法律、法规和政令的要求，以自主可控为原则，为公共类电子支付系统的信息安全提供一个公共框架；是进一步完善相关国家标准及行业标准的重要步骤；为构建、运行公共电子支付系统，提供支撑。

信息安全技术
电子支付系统安全保护框架

1 范围

本标准在给出电子支付系统模型的基础上，为公共类电子支付系统的信息安全提供了一个公共框架，主要包括安全问题定义、安全目的、安全功能需求和安全保障需求。

本标准适用于安全构建、运行公共类电子支付系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

GB/T 18336.2 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件

GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保障组件

3 术语和定义

GB/T 18336.1 界定的以及下列术语和定义适用于本文件。

3.1

电子支付 electronic payment

采用数字化方式，在电子终端、信息传输通道以及相关系统的支持下，进行支付的行为。

3.2

支付通道 transaction channel

在电子支付交易过程中，电子支付凭据与支付终端以及支付终端与支付安全前置之间实现信息传输的途径。

3.3

公共网络通道 public network channel

支持电子支付交易的公共网络基础设施。在电子支付领域通常简称为**网络**。

3.4

接触通道 contact channel

支持电子支付交易的实体直接连接方式。

3.5

电子支付凭据 electronic payment credential

在电子支付过程中，用以最终确定支付相关账户的凭据。

电子支付凭据可能是有载体的，也可能是无载体的，同一电子支付凭据可能记载在不同的载体中。

3.6

电子支付凭据载体 electronic payment credentials carrier

记载电子支付凭据的介质。不同的电子支付凭据载体，其安全性是不同的。