



中华人民共和国国家标准

GB/T 34994.1—2017

教育卡应用规范 第 1 部分：教育卡技术要求

Application specifications for education card—
Part 1: Technical requirements for education card

2017-11-01 发布

2018-05-01 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
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	4
5 总则	5
6 教育卡文件系统	5
6.1 文件总则	5
6.2 文件引用	5
6.3 文件结构	5
6.4 数据元定义	8
7 教育卡命令	8
7.1 命令总则	8
7.2 命令报文格式	9
7.3 命令响应报文格式	9
8 教育卡应用流程	10
8.1 应用流程概述	10
8.2 应用预处理	10
8.3 身份鉴别	12
8.4 卡片鉴别	14
8.5 信息读取	16
8.6 信息变更	16
8.7 学籍注册	17
8.8 营养改善计划用餐登记	19
8.9 交通优惠信息写入	20
8.10 电子学位证信息写入	21
8.11 电子学位证信息读取	22
8.12 电子毕业证/电子结业证信息写入	23
8.13 电子毕业证/电子结业证信息读取	24
8.14 ESN 读取	25
8.15 交易认证	26
8.16 联机圈存	27
8.17 联机消费	28
8.18 教育卡芯片认证码读取	30
8.19 应用维护功能	30
8.20 防拔	31
9 教育卡卡面信息	31

10	教育卡应用安全要求	31
10.1	总体要求	31
10.2	加密机制	32
10.3	公钥鉴别	34
10.4	安全报文	38
10.5	卡片安全	39
10.6	密钥管理	41
10.7	密码算法	43
11	教育卡应用接口	43
附录 A (规范性附录)	教育应用文件定义	44
附录 B (规范性附录)	教育卡存储的数据元	59
附录 C (规范性附录)	命令	71
附录 D (规范性附录)	安全报文	120
附录 E (规范性附录)	AC 和 ARPC 生成方法	122
附录 F (规范性附录)	卡面信息	124
附录 G (规范性附录)	算法标识	131
附录 H (规范性附录)	C/S 应用接口函数	133
附录 I (规范性附录)	B/S 应用接口函数	147

前 言

GB/T 34994《教育卡应用规范》分为 14 个部分：

- 第 1 部分：教育卡技术要求；
- 第 2 部分：教育卡发卡发证流程；
- 第 3 部分：教育卡数据处理要求；
- 第 4 部分：教育卡个人化写卡写证制作系统技术要求；
- 第 5 部分：教育卡应用安全保障体系技术要求；
- 第 6 部分：教育卡终端安全模块应用技术要求；
- 第 7 部分：教育卡应用技术要求；
- 第 8 部分：教育卡网上副本应用技术要求；
- 第 9 部分：教育电子证件技术要求；
- 第 10 部分：教育电子证件制作系统技术要求；
- 第 11 部分：教育电子证件验证终端技术要求；
- 第 12 部分：教育卡产品测试要求；
- 第 13 部分：教育卡系统测试要求；
- 第 14 部分：教育卡可信电子档案应用技术要求。

本部分为 GB/T 34994 的第 1 部分。

本部分按照 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。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位包括：教育部教育管理信息中心、中国电子技术标准化研究院、中育至诚科技有限公司、南方城墙信息安全科技有限公司、公安部第一研究所、中国银联股份有限公司、上海复旦微电子集团股份有限公司、苏博云科数字认证有限公司、长城信息产业股份有限公司、东方新诚信数字认证中心有限公司、广东楚天龙智能卡有限公司、华南理工大学、长沙理工大学。

本部分主要起草人员：罗方述、蔡燕、马亮、颜星、张鹏、余云涛、王刚、程和、丁林润、钟梁、杨清贵、程聂、李莹、欧阳晖、李春欢、陈朋、陈安新、张纲、倪以金、谭武征、齐德昱、罗晓奔、傅明、李峰、罗继东、王瑾、邵飞、蒋才平。

教育卡应用规范

第 1 部分：教育卡技术要求

1 范围

GB/T 34994 的本部分规定了教育卡应用相关的文件系统、命令、应用流程、卡表面信息、安全体系以及应用接口的技术要求。

本部分适用于规范教育卡的设计、制造、检测、发行、开发、应用与管理。

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。凡是未注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 2260—2013 中华人民共和国行政区划代码

GB/T 14916—2006 识别卡 物理特性

GB/T 16649.4—2010 识别卡 集成电路卡 第 4 部分：用于交换的结构、安全和命令

GB/T 16649.5—2002 识别卡 带触点的集成电路卡 第 5 部分：应用标识符的国家编号体系和注册规程

GB 18030—2005 信息技术 中文编码字符集

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议

GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法

GB/T 33190—2016 电子文件存储与交换格式版式文档

JY/T 1001—2012 教育管理信息 教育管理基础代码

JY/T 1002—2012 教育管理信息 教育管理基础信息

JY/T 1003—2012 教育管理信息 教育行政管理信息

3 术语和定义

下列术语和定义适用于本文件。

3.1

教育卡 **education card**

面向在校学生、毕业生、教职员工以及教育行政部门的人员等对象发放的集成电路卡与网上副本。教育卡是满足教育应用安全性要求、具备身份鉴别功能、具有可识别的全国唯一的教育电子身份号，又能同时支持教育管理应用、学校应用、智慧教育应用、网络空间应用、社会化应用的可信电子化教育身份证。

注：根据教育卡的存在形态，教育卡分为无触点集成电路卡与网上副本。根据教育卡的应用功能，教育卡分为学生教育卡、教师教育卡、毕业生教育卡、教育电子证件、电子校徽等类型。