



中华人民共和国国家标准

GB/T 36342—2018

智慧校园总体框架

Smart campus overall framework

2018-06-07 发布

2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 智慧校园总体系统架构	3
5.1 智慧校园的总体架构	3
5.2 基础设施层	3
5.3 支撑平台层	4
5.4 应用平台层	4
5.5 应用终端	5
5.6 信息系统安全体系	5
6 智慧教学环境	5
6.1 概述	5
6.2 智慧教学环境的类型与分级	5
6.3 智慧教学环境总体架构	6
7 智慧教学资源	8
7.1 概述	8
7.2 智慧教学资源总体架构	8
8 智慧校园管理	11
8.1 概述	11
8.2 智慧校园管理类型与分级	11
8.3 智慧校园管理总体架构	11
9 智慧校园服务	15
9.1 概述	15
9.2 智慧校园服务总体架构	15
10 信息安全体系	18
10.1 概述	18
10.2 信息安全防护要求	19
10.3 信息安全防护架构	20
10.4 网络安全防护要求	20
10.5 应用访问控制	21
10.6 数据安全防护要求	21
10.7 移动访问安全防护	21
参考文献	22

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

标准主要起草单位:清华大学、华南理工大学、国家开放大学、中央民族大学、浙江大学、北京大学、北京工业大学、中国人民大学、上海交通大学、南京大学、中国教育技术协会、深圳锐取信息技术股份有限公司、北京同方艾威康科技有限公司、上海金桥信息技术股份有限公司、湖南青果软件有限公司、北京康邦科技有限公司、北京外国语大学、苏州科技大学、中国电子技术标准化研究院。

主要起草人:钟晓流、丁泉龙、单从凯、郑道林、肖波、董榕、蒋家傅、左渠、周恕义、张秋、葛萌、刘培柱、李海霞、聂风华、郑莉、毕雄、何全、张光铎、陈学林、沈宏兴、钱震、宋述强、杜婧、王峻京、余云涛、李莹。

智慧校园总体框架

1 范围

本标准规定了智慧校园建设的总体框架,包括智慧教学环境、智慧教学资源、智慧校园管理、智慧校园服务、信息安全体系等的系统架构及基本要求。

本标准适用于智慧校园建设的设计与实施。

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 22240—2008 信息安全技术 信息系统安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字校园 digit campus

在传统校园基础上构建一个数字空间,实现从环境信息(包括教室、实验室等)、资源信息(如图书、讲义、课件等)到应用信息(包括教学、管理、服务、办公等)等全部数字化,从而为资源和服务共享提供有效支撑。

3.2

智慧校园 smart campus

物理空间和信息空间有机衔接,使任何人、任何时间、任何地点都能便捷地获取资源和服务。

注:智慧校园是数字校园的进一步发展和提升,是教育信息化的更高级形态。

3.3

智慧教学环境 smart instructional environment

集智能化感知、智能化控制、智能化管理、智能化互动反馈、智能化数据分析、智能化视窗等功能于一体的用以支持教学、科研活动的现实空间环境或虚拟空间环境。

3.4

智慧教学资源 smart instructional resources

能通过自动分类与编目、检索与导航、汇聚与策展、共享与推送等方式实现跨终端获取和应用的资源。

3.5

智慧校园管理 smart campus management

集智能化感知、智能化控制、智能化管理、智能化互动反馈、智能化数据分析、智能化视窗等功能于一体的用于实现校园信息管理的系统。

3.6

智慧校园服务 smart campus service

集智能化感知、智能化控制、智能化管理、智能化互动反馈、智能化数据分析、智能化视窗等功能于

10.4.2 外网的防护功能

对于外网的安全防御,需在外网与核心交换设备之间部署相应的防火墙设备,并部署相关策略。外网防护功能包括结构安全、访问安全、安全审计、入侵防范、恶意代码防护等。

针对互联网对校园网内业务系统访问,执行严格的访问控制策略,可依据源、目标地址、协议、端口,以限制互联网不同级别的终端,按照权限访问不同服务器的不同应用,并有效禁止非法的访问。

10.4.3 VPN 访问控制

对于内网用户通过公众网络访问智慧校园内部系统,配置 VPN 功能,对数据进行机密性、完整性保护,避免数据被窃取,及保障数据在传递过程中不被非法篡改。

10.5 应用访问控制

部署的防火墙设备还根据具体的应用类型来配置访问控制策略,针对用户多业务的特点,区分不同的业务类型,确定外网终端可进行的具体应用,杜绝非法的访问,保障业务访问的合规性。

10.6 数据安全防护要求

数据中心出口针对具体应用,部署入侵防御系统,对访问数据包的内容进行深度检测,提升对攻击检测的准确性。

10.7 移动访问安全防护

10.7.1 移动身份认证

移动身份认证管理服务为智慧校园系统移动端提供统一身份认证管理,实现移动端的应用系统单点登录。

10.7.2 移动数据安全传输

移动数据安全防护是通过控制移动用户访问智慧校园内部数据资源,宜对受信任的移动应用建立 SSL 安全传输通道,进行数据的传输和访问。

10.7.3 移动应用控制

根据智慧校园应用系统的保护等级,对移动应用进行相应的应用接入控制。只有经过系统认证的移动应用 APP 才能通过安全网关访问授权管理智慧校园的资源和服务。对非法的应用 APP 访问,拒绝访问并宜给出相应提示。

参 考 文 献

- [1] GB/T 2887—2011 计算机场地通用规范
 - [2] GB/T 13745—2009 学科分类与代码
 - [3] GB/T 14198—2012 传声器通用规范
 - [4] GB/T 19391—2003 全球定位系统(GPS)术语及定义
 - [5] GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式
 - [6] GB/T 21062.2—2007 政务信息资源交换体系 第2部分:技术要求
 - [7] GB/T 21671 基于以太网技术的局域网系统验收测评规范
 - [8] GB/T 28049—2011 厅堂、体育场馆扩声系统设计规范
 - [9] GB/T 29808—2013 信息技术 学习、教育和培训 高等学校管理信息
 - [10] GB/T 31068—2014 普通高等学校安全技术防范系统要求
 - [11] GB/T 31778—2015 数字城市一卡通互联互通 通用技术要求
 - [12] GB/T 33745—2017 物联网 术语
 - [13] GB 50052—2009 供配电系统设计规范
 - [14] SJ/T 11343 数字电视液晶显示器通用规范
 - [15] SJ/T 11346 电子投影机测量方法
 - [16] YD/T 2437—2012 物联网总体框架与技术要求
 - [17] YD/T 2877.1—2015 智能终端支持个人健康管理的技术要求 第1部分:总体
 - [18] ISO 8601:2004 Data elements and interchange formats—Information interchange—Representation of dates and times
 - [19] ISO 55001:2014 Asset management—Management systems—Requirements
 - [20] ISO/IEC 14496-3:2009 Information technology—Coding of audio-visual objects—Part 3:Audio
 - [21] ISO/IEC 14496-10:2014 Information technology—Coding of audio-visual objects—Part 10:Advanced Video Coding
 - [22] IETF RFC 2048:1996 Multipurpose Internet Mail Extensions (MIME) Part Four:Registration Procedures
-