ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28455—2012

信息安全技术　引入可信第三方的实体鉴别及接入架构规范

Information security technology—Entity authentication involving a trusted third party and access architecture specification

2012-06-29 发布　　2012-10-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:西安西电捷通无线网络通信股份有限公司、国家密码管理局商用密码检测中心、信息安全国家重点实验室、中国电子技术标准化研究所、国家无线电监测中心检测中心、西安电子科技大学、西安邮电学院、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、中国信息安全认证中心、国家信息安全工程技术研究中心、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、公安部第一研究所、工业和信息化部通信计量中心、公安部信息安全等级保护评估中心、国防科技大学、北京市政务网络管理中心、重庆邮电大学、宇龙计算机通信科技(深圳)有限公司、中国人民大学、中国人民解放军信息安全测评认证中心、中国电信集团公司、国家信息中心、北京大学深圳研究生院、中国电力科学研究院、北京中电华大电子设计有限责任公司、东南大学、中国移动通信集团设计院有限公司、中国人民解放军信息工程大学、江南计算技术研究所、北京邮电大学、上海龙照电子有限公司、北京五龙电信技术公司、北京网贝合创科技有限公司、深圳市宏电技术股份有限公司、北大方正集团公司、海尔集团公司、北京广信融科技术有限公司、北京六合万通微电子技术有限公司、弘浩明传科技(北京)有限公司、北京城市热点资讯有限公司、北京华安广通科技发展有限公司、迈普通信技术有限公司、长春吉大正元信息技术股份有限公司、清华大学、北京天一集成科技有限公司、桂林电子工业学院、西安立人科技股份有限公司、宽带无线 IP 标准工作组、WAPI 产业联盟等。

本标准主要起草人:黄振海、赖晓龙、李大为、冯登国、宋起柱、铁满霞、曹军、李建东、林宁、舒敏、朱志祥、陈晓桦、郭晓雷、李京春、余亚莉、王育民、张变玲、肖跃雷、高波、高昆仑、潘峰、胡亚楠、蒋庆生、肖雳、朱建平、贾焰、施伟年、李琴、李广森、吴亚非、梁朝晖、梁琼文、罗旭光、龙昭华、沈凌云、张伟、徐平平、马华兴、高峰、仇洪冰、朱跃生、王雅辉、兰天、王志坚、杜志强、张国强、田小平、田辉、张永强、寿国梁、毛立平、曹竹青、郭志刚、高宏、韩康、王钢、白国强、陈志峰、李建良、李大伟、王立仁、高原、岳林、井京涛。

引　言

网络通信经常处于这样的环境，非授权的终端设备可以物理地连接到网络上，授权的终端设备所连接的网络也不一定是它所期望的，因此在终端和网络通信前，需要通过鉴别和授权功能互相鉴别对方身份的合法性，以保证通信的安全。对此通信和信息技术业界一直在寻找经济有效的安全解决方案，安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。

因此本文件的主要目标是提出一套适用于网络访问控制和身份管理的、支撑上层业务的、具有普遍适用性的实体鉴别与安全接入协议和结构。本标准将采用非对称密码技术，并引入在线的可信第三方，构建鉴别协议，并定义网络安全接入架构。

本标准主要内容是：

——引入可信第三方的实体鉴别及接入架构采用三元结构，将参加鉴别和授权的实体置于对等的角色，利用逻辑的端口控制方法完成双方的鉴别和授权；

——本标准确定的访问控制方法可应用于无线网络访问控制、有线网络访问控制以及 IP 自适应移动访问控制系统等。

本标准的使用者是通信行业的生产企业、检测机构和科研机构。

本标准的发布机构提请注意，声明符合本标准时，可能涉及到 5.4.5.4 与“一种三元结构的对等访问控制方法”、“一种三元结构的对等访问控制系统”等相关的专利的使用。

本标准的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本标准的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本标准发布机构备案。相关信息可通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电　　话：029-87607836

传　　真：029-87607829

网　　址：http://www.iwncomm.com

请注意除了上述专利外，本标准的某些内容仍可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

信息安全技术　引入可信第三方的实体鉴别及接入架构规范

1　范围

本标准规定了引入可信第三方的实体鉴别及接入架构的一般方法。包括：

a）　引入可信第三方的实体鉴别及接入架构的框架；

b）　引入可信第三方的实体鉴别及接入架构的基本原理；

c）　定义引入可信第三方的实体鉴别及接入架构的不同级别以及相应收发数据时端口的行为；

d）　定义引入可信第三方的实体鉴别及接入架构的参与实体间的消息交互协议；

e）　定义使用消息交互协议完成引入可信第三方的实体鉴别及接入架构的过程；

f）　规定协议交互消息中的数据编码；

g）　建立引入可信第三方的实体鉴别及接入架构管理的需求，识别管理对象，定义管理操作；

h）　描述远程管理者利用简单网络管理协议（SNMP）所能进行的管理操作；

i）　描述符合本标准的设备应满足的需求，见附录A。

本标准适用于无线网络访问控制、有线网络访问控制和IP网络访问控制系统等。

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 15629.2—2008　信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第2部分：逻辑链路控制

GB/T 15629.3—1995　信息处理系统　局域网　第3部分：带碰撞检测的载波侦听多址访问（CSMA/CD）的访问方法和物理层规范

GB 15629.11—2003　信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第11部分：无线局域网媒体访问控制和物理层规范

ISO/IEC 9798-3：1998/Amd.1：2010　信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制　修改单1（Information technology—Security techniques—Entity authentication—Part 3：Mechanisms using digital signature techniques—Amendment 1）

IEEE Std 802.3™-2005　局域网和城域网规范　第3部分：带检测冲突的载波检测多址存取（CSMA/CD）方法和物理层规范[IEEE Standard for Local and Metropolitan Area Networks—Part 3：Carrier Sense Multiple Access with Collision Detection（CSMA/CD）　Access Method and Physical Layer Specifications]

IEEE Std 802.1D™-2004　局域网和城域网规范　媒体访问控制桥[IEEE Standard for Local and Metropolitan Area Networks—Media Access Control（MAC）Bridges]

IEEE Std 802.1Q™-2003　局域网和城域网规范　局域网虚拟桥（IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks）

IEEE Std 802.1x™-2004　局域网和城域网规范　基于端口的网络访问控制（IEEE Standards for Local and Metropolitan Area Networks—Port-Based Network Access Control）