ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 28455—2026
代替 GB/T 28455—2012

网络安全技术　引入可信第三方的实体鉴别及接入架构规范

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

2026-05-25 发布　　2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替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》，与GB/T 28455—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了术语“非对称密码算法”“可信第三方”“散列函数/杂凑函数”“数字签名/签名”“原子密钥建立与实体鉴别”（见第3章）；

b) 增加了符号（见4.1）；

c) 删除了缩略语“ASF”“CBAP”“CHAP”“CMAP”“DHCP”“FDDI”“IBAP”“TP”“Port”“PCAP”“OUI”“VLAN”（见2012年版的第4章）；

d) 增加了缩略语“BK”“DCK”“DRK”“EEP”“EIAK”“EKey”“EMK”“IAK”“IVK”“KDF”“MAK”“MEK”“MIK”“PK”“PRF”“PSK”“SPK”（见4.2）；

e) 增加了对TAEP协议封装的扩展（见6.3.1、6.3.2）；

f) 删除了“对等鉴别访问控制协议”“端口接入控制管理”“端口接入控制MIB定义”三章（见2012年版的第7章、第8章、第9章）；

g) 增加了“原子密钥建立与实体鉴别技术要求”一章（见第8章）；

h) 增加了“测试评价方法”一章（见第9章）；

i) 增加了附录“密钥产生”（见附录A）；

j) 删除了附录“PICS形式表”（见2012年版的附录A）。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：西安西电捷通无线网络通信股份有限公司、北京数字认证股份有限公司、国家信息技术安全研究中心、陕西省信息化工程研究院、北京时代新威信息技术有限公司、湖北省数字证书认证管理中心有限公司、中国科学院信息工程研究所、中电信量子信息科技集团有限公司、联通在线信息科技有限公司、长扬科技（北京）股份有限公司、国家无线电监测中心检测中心、浙江齐安信息科技有限公司、中关村无线网络安全产业联盟、中国南方电力调度控制中心、中国电力科学研究院有限公司、天翼安全科技有限公司、大唐高鸿信安（浙江）信息科技有限公司、国网山东省电力公司、广西通量能源技术有限公司、西安芯语慧联信息科技有限公司、深圳鑫润星智能有限公司、兴唐通信科技有限公司、华为技术有限公司、微位（深圳）网络科技有限公司、中汽研软件测评（天津）有限公司、用友网络科技股份有限公司。

本文件主要起草人：李琴、王月辉、杜志强、张国强、张变玲、黄振海、侯鹏亮、赵晓荣、徐震、张璐璐、隋忻、铁满霞、曹军、杜云浩、陈诚、刘勇、程福兴、颜湘、芦亮、井经涛、郑骊、王立华、尹玉昂、于双双、赵华、张宙、谢俊毅、陈宝仁、肖红阳、程武阳、孙晓童、蔡子凡、贾世杰、赖晓龙、陈维刚、马丹丹、肖龙、管荑、苑超、童伟刚、潘文博、王浩、王云飞、张明远、季晨荷、刘海洁、张勇、梁浩军、鲍博武、李子阳、梁斌、孙梁、季晟宇、周晓刚、高鹏、侯昕田。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为GB/T 28455—2012；

——本次为第一次修订。

引　言

网络通信中，经常会出现非授权或者非预期的访问，包括未授权的终端设备物理连接到网络上、授权的终端设备所连接的网络不是它所期望的等各种情况。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并进行访问控制，以保证通信的安全。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。

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。本文件将采用密码技术，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。

本文件主要内容是：

——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；

——本文件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。

本文件的发布机构提请注意，声明符合本文件时，可能涉及到 5.4 与“一种三元结构的对等访问控制系统”“一种三元结构的对等访问控制方法”，第 8 章与“一种身份鉴别方法和装置”等相关的专利的使用。

本文件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文件的发布机构承诺，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文件发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：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

请注意除了上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

网络安全技术　引入可信第三方的实体鉴别及接入架构规范

1　范围

本文件确立了引入可信第三方的实体鉴别及接入总体架构，规定了协议封装要求、原子密钥建立与实体鉴别技术要求，描述了对应的测评方法。

本文件适用于无线网络、有线网络的数据链路层，以及网络层的访问控制系统设计、开发、测试等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2014　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　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

GB/T 15629.15—2010　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15部分：低速无线个域网（WPAN）媒体访问控制和物理层规范

GB/T 15843.3—2023　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

GB/T 15852.2—2024　网络安全技术　消息鉴别码　第2部分：采用专门设计的杂凑函数的机制

GB/T 17901.3—2021　信息技术　安全技术　密钥管理　第3部分：采用非对称技术的机制

GB/T 25068.5—2021　信息技术　安全技术　网络安全　第5部分：使用虚拟专用网的跨网通信安全保护

GB/T 28925—2012　信息技术　射频识别　2.45 GHz空中接口协议

GB/T 29828—2013　信息安全技术　可信计算规范　可信连接架构

GB/T 30001.1—2013　信息技术　基于射频的移动支付　第1部分：射频接口

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 33746.2—2017　近场通信（NFC）安全技术要求　第2部分：安全机制要求

3　术语和定义

GB/T 15843.3—2023界定的以及下列术语和定义适用于本文件。