ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29828—2013

信息安全技术　可信计算规范
可信连接架构

Information security technology—Trusted computing specification—Trusted connect architecture

2013-11-12 发布　　2014-02-01 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 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:北京工业大学、西安西电捷通无线网络通信股份有限公司、瑞达信息安全产业股份有限公司、西安电子科技大学、北京理工大学、武汉大学、北京天融信科技有限公司、北京电子科技学院、北京金奥博数码信息技术有限责任公司、中国电子科技集团公司第三十研究所、国家无线电监测中心、北京网贝合创科技有限公司、中国航天科工集团二院七 O 六所、郑州信大捷安信息技术有限公司、上海格尔软件股份有限公司、西安邮电大学、江南计算机技术研究所、国家广播电影电视总局广播科学研究院、中国电子技术标准化研究院、华为技术有限公司、深圳长城电脑有限公司、中安科技集团有限公司、长春吉大正元信息技术股份有限公司、北京鼎普科技股份有限公司、成都卫士通信息产业股份有限公司、北京密安网络技术股份有限公司、中国电力科学研究院、无线网络安全技术国家工程实验室。

本标准主要起草人:沈昌祥、肖跃雷、曹军、张立强、张兴、韩永飞、方娟、李海鹏、黄振海、陈曦、祝烈煌、李兆斌、刘彤、冷冰、宋起柱、陈志浩、张焕国、秦志强、段丽娟、李晖、张龙、铁满霞、赖晓龙、常超稳、谭武征、韩勇桥、刘智君、姚琦、裴庆祺、张子剑、葛莉、鞠磊、赵桂芳、朱林、朱志祥、蒋炎河、王磊、邹冰玉、赖英旭、马卓、张变玲、杜志强、胡亚楠、刘卫国、池亚平、吴素研、苑克龙、王晓程、于昇、李兴华、王轲、张国强、李琴、刘贤刚、位继伟、尹瀚、秦晰、魏占祯、李瑛、刘了、梁晋春、公备、邵存金、李大东、何长龙、万俊、贾科、张世雄、王明坤、高昆仑、许胜伟、姚金利、王勇、侯亚荣、任兴田、杨宇光、赵国磊、韩培胜、曹慧渊、郭沛宇、郎风华。

引　言

随着信息化的逐渐发展，网络安全面临严峻的考验，各种计算机网络遭受的攻击和破坏80%是来自于内部。目前业内的安全解决方案往往侧重于先防外后防内，先防服务设施后防终端设施。而可信计算技术则逆其道而行之，首先保证所有终端的可信赖性，通过可信赖的组件来组建更大的可信系统。可信计算平台在底层进行防护，通过可信硬件对上层进行保护，为用户提供更强的安全防护。可信网络连接本质上包含两个方面的内容：第一方面需要创建一套在网络内部系统运行状况的策略；第二方面，只有遵守网络设定的策略的终端才能访问网络，网络将隔离和定位那些不遵守策略的设备。

本标准的主要目标是提出一个实现终端连接到网络的双向用户身份鉴别和平台鉴别，进而实现可信网络连接的可信连接架构，并定义其层次、实体、组件、接口、实现流程、评估、隔离和修补以及各个接口的具体实现。

本标准主要内容是：

——可信连接架构，实现终端连接到网络的双向用户身份鉴别和平台鉴别。

——定义可信连接架构中各个接口的具体实现。

本标准的使用者是可信计算的生产企业、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，可能涉及第5章与“一种基于三元对等鉴别的可信网络连接方法”、“一种基于三元对等鉴别的可信网络连接系统”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　可信计算规范
可信连接架构

1　范围

本标准规定了可信连接架构的层次、实体、组件、接口、实现流程、评估、隔离和修补以及各个接口的具体实现，解决终端连接到网络的双向用户身份鉴别和平台鉴别问题，实现终端连接到网络的可信网络连接。

本标准适用于具有可信平台控制模块的终端与网络的可信网络连接。

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 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

GB 15629.11—2003/XG1—2006　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　第1号修改单

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

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　第1号修改单：引入在线可信第三方的机制(Information technology—Security techniques—Entity authentication—Part 3：Mechanisms using digital signature techniques—Amendment 1：Mechanisms involving an on-line trusted third party)

ISO/IEC 18028-5：2006　信息技术　安全技术　IT网络安全　第5部分：使用虚拟专用网的跨网通信安全保护(Information technology—Security techniques—IT network security—Part 5：Securing communications across networks using virtual private networks)

IETF RFC 2138　远程认证拨入用户服务 (Remote Authentication Dial In User Service)

IETF RFC 2246　TLS协议1.0版本(The TLS Protocol Version 1.0)

IETF RFC 2547　边界网关协议/多协议标签交换 虚拟专用网(BGP/MPLS VPNs)

IETF RFC 2675　Ipv6 巨型包(IPv6 Jumbograms)

IETF RFC 2865　远程认证拨入用户服务(Remote Authentication Dial In User Service)

IETF RFC 2866　远程认证拨入用户服务的计费(RADIUS Accounting)

IETF RFC 3280　X.509公钥基础设施证书和证书撤销列表轮廓(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile)

IETF RFC 3539　认证、授权和计费传输轮廓(Authentication Authorization and Accounting Transport Profile)

IETF RFC 3588　Diameter基础协议(Diameter Base Protocol)

IETF RFC 3589　3GPP的Diameter命令代码(Diameter Command Codes for Third Generation Partnership Project Release 5)

IETF RFC 4346　TLS协议1.1版本(The TLS Protocol Version 1.1)