ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37935—2019

信息安全技术　可信计算规范
可信软件基

Information security technology—Trusted computing specification—Trusted software base

2019-08-30 发布　　2020-03-01 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

本标准按照 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。

本标准起草单位:北京可信华泰信息技术有限公司、北京工业大学、中标软件有限公司、全球能源互联网研究院有限公司、中国人民大学、中国船舶重工集团公司第七〇九研究所、北京新云东方系统科技有限责任公司、华大半导体有限公司、北京得安信息技术有限公司、浪潮(北京)电子信息产业有限公司。

本标准主要起草人:孙瑜、宁振虎、胡俊、赵保华、董军平、沈楚楚、吴欣、黄坚会、洪宇、张建标、王涛、梁鹏、宋元、周晓刚、宗栋瑞、田健生、王志皓、徐宁、马洪富、杨紫东、王昱波、徐明迪、张敏健、王振宇、黄磊、王大海、夏攀。

信息安全技术　可信计算规范
可信软件基

1　范围

本标准规定了可信软件基的功能结构、工作流程、保障要求和交互接口规范。

本标准适用于可信软件基的设计、生产和测评。

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 29827—2013　信息安全技术　可信计算规范　可信平台主板功能接口

GB/T 29828—2013　信息安全技术　可信计算规范　可信连接架构

GB/T 29829—2013　信息安全技术　可信计算密码支撑平台功能与接口规范

IETF RFC 5209　网络终端评估：概述和要求[Network Endpoint Assessment (NEA): Overview and Requirements]

3　术语和定义

GB/T 29827—2013、GB/T 29828—2013、GB/T 29829—2013 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 29829—2013 中的一些术语和定义。

3.1

可信计算平台　trusted computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

[GB/T 29829—2013，定义 3.1.1]

3.2

宿主基础软件　legacy fundamental software

可信计算平台中实现常规功能部分(如操作系统)软件的总称。

3.3

可信软件基　trusted software base

为可信计算平台的可信性提供支持的软件元素的集合。

3.4

基本信任基　fundamental trusted software

负责宿主基础软件的可信启动及可信软件基其他部件完整性度量的部件。

3.5

可信基准值　trusted baseline value

表示对象可信特性的数据，作为判断对象是否可信的参照。

3.6

可信基准库　trusted baseline value database

可信基准值的集合。