



# 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 发布  
中国国家标准化管理委员会

## 目 次

前言 .....	V
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
4 缩略语 .....	3
5 总体描述 .....	5
5.1 概述 .....	5
5.2 实体 .....	6
5.3 层次 .....	6
5.4 组件 .....	6
5.5 接口 .....	7
5.6 实现过程 .....	8
5.7 评估、隔离和修补 .....	9
6 网络访问控制层 .....	11
6.1 概述 .....	11
6.2 网络传输机制 .....	11
6.3 访问控制机制 .....	51
7 可信平台评估层 .....	52
7.1 概述 .....	52
7.2 平台鉴别基础设施 .....	53
8 完整性度量层 .....	115
8.1 概述 .....	115
8.2 IF-IM 消息协议 .....	115
9 IF-IMC 和 IF-IMV .....	120
9.1 概述 .....	120
9.2 IF-IMC .....	120
9.3 IF-IMV .....	129
附录 A (资料性附录) 完整性管理框架 .....	134
附录 B (资料性附录) 安全策略管理框架 .....	136
附录 C (资料性附录) 数字信封 .....	138
图 1 可信连接架构(TCA) .....	5
图 2 TCA 的实现过程 .....	8
图 3 具有隔离修补层的可信连接架构 .....	10

图 4	TCA 的序列 TAEP 鉴别实现一的层次模型	12
图 5	序列 TAEP 鉴别实现一的 TAEP 交互过程	14
图 6	TCA 的序列 TAEP 鉴别实现二的层次模型	15
图 7	序列 TAEP 鉴别实现二的 TAEP 交互过程一	18
图 8	序列 TAEP 鉴别实现二的 TAEP 交互过程二	19
图 9	FLAG	21
图 10	EWAI 协议的证书鉴别过程	21
图 11	消息 1 的数据字段格式	22
图 12	消息 2 的数据字段格式	22
图 13	消息 3 的数据字段格式	23
图 14	消息 4 的数据字段格式	24
图 15	消息 5 的数据字段格式	27
图 16	消息 6 的数据字段格式	30
图 17	消息 7 的数据字段格式	33
图 18	消息 8 的数据字段格式	36
图 19	消息 9 的数据字段格式	36
图 20	TCA 的隧道 TAEP 鉴别方式层次模型	38
图 21	隧道 TAEP 鉴别实现的 TAEP 交互过程一	41
图 22	隧道 TAEP 鉴别实现的 TAEP 交互过程二	42
图 23	ETLS 协议的握手协议分组格式	43
图 24	ETLS 协议的握手过程	44
图 25	消息 1 的数据字段格式	44
图 26	FLAG	45
图 27	消息 2 的数据字段格式	46
图 28	消息 3 的数据字段格式	48
图 29	消息 4 的数据字段格式	49
图 30	全端口控制实现方式下的端口控制系统结构	52
图 31	PAI 协议基本流程	54
图 32	PAI 协议分组格式	56
图 33	标识 FLAG 格式	57
图 34	组件类型级平台完整性度量请求参数	58
图 35	组件属性级平台完整性度量请求参数条目	58
图 36	组件类型级平台完整性评估策略条目	59
图 37	组件产品级平台完整性评估策略条目	59
图 38	组件属性级平台完整性评估策略条目	60
图 39	组件类型级平台完整性度量值条目	60
图 40	IF-IM 级平台完整性度量值条目	61
图 41	组件类型级 Quote 数据值条目	61
图 42	IF-IM 级 Quote 数据值条目	61
图 43	组件类型级平台配置保护策略条目	62
图 44	组件产品级平台配置保护策略条目	62
图 45	组件属性级平台配置保护策略条目	63
图 46	组件类型级平台修补信息条目	63