



中华人民共和国国家标准

GB/T 29234—2012

基于公用电信网的宽带客户网络 安全技术要求

Security technical requirements for broadband customer network based on
telecommunication network

2012-12-31 发布

2013-06-01 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

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。

本标准由中华人民共和国工业和信息化部提出。

本标准由中国通信标准化协会归口。

本标准起草单位：工业和信息化部电信研究院。

本标准主要起草人：程强、敖立、刘谦、陆洋。

基于公用电信网的宽带客户网络 安全技术要求

1 范围

本标准规定了基于公用电信网的宽带客户网络的安全威胁、安全需求、安全机制和安全算法、设备认证证书轮廓以及安全功能。

本标准适用于电信网络提供的业务和应用通过网关在宽带客户网络内部实现的情况,对仅在宽带客户网络内部设备之间信息流通的情况也可参考使用。

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。

YD/T 1448—2006 基于公用电信网的宽带客户网络总体技术要求

ITU-T X.509 信息技术 开放系统互连 号码簿:公钥和属性鉴别框架(Information technology—Open systems interconnection—The directory:Public-key and attribute certificate frameworks)

ITU-T X.805 提供端到端通信的系统的体系(Security architecture for systems providing end-to-end communications)

ITU-T X.1121 移动端到端数据通信的安全技术框架(Framework of security technologies for mobile end-to-end data communications)

Broadband Forum TR-069 Amendment 1(2006) CPE WAN 管理协议(CPE WAN Management Protocol)

3 术语和定义

下列术语和定义适用于本文件。

3.1

授权证书 authorization certificate

用于为对象授权的一个签名物。它至少包括一个发放者和一个对象。它可以包括有效性条件、授权和委托信息。通常,证书可以分为三类:身份证书、属性证书和授权证书。身份证书用于映射对象的名字和公钥,属性证书用于映射对象的名字和授权,授权证书用于映射对象的授权和公钥。获得一个授权证书或属性证书可以代表对象从发放者获得所有或部分权限。

3.2

身份证书 ID certificate

一段信息,其中至少声明了授权发放者名称、证书对象身份、该对象公钥、证书有效期、序号和认证中心的数字签名。

3.3

设备证书 device certificate

身份证书的一种,在宽带客户网络中,它是一个符合 ITU-T X.509 版本 3 的证书,用于认证宽带客