ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29767—2013

信息安全技术　公钥基础设施 桥CA体系证书分级规范

Information security techniques—Public key infrastructure—Bridge Certification Authority leveled certificate specification

2013-09-18 发布　　2014-05-01 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 给出的规则起草。

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。

本标准起草单位:国家信息中心、中国科学院信息安全国家重点实验室。

本标准主要起草人:吴亚非、任金强、罗红斌、张凡、高能。

引　言

本标准对桥CA证书策略的安全保证级别规定了分级标准，将桥CA体系证书划分为四个应用级别和测试级共五个等级，并说明了对各级别的技术要求。四个应用级别是：初级、基本级、中级、高级，其安全级别逐次增高。测试级证书是用于交叉认证测试的证书。

本标准参照RFC 3647，对各级别的证书策略做出了明确说明，用以指导设计者如何设计和实现相应级别的证书策略。每个级别针对九个方面的不同内容做出了要求，保证了证书策略从初级到高级，其安全程度随之递增，其适应的安全环境也随之更加严格。

信息安全技术　公钥基础设施
桥 CA 体系证书分级规范

1　范围

本标准规定了桥 CA 体系证书安全等级划分。

本标准适用于桥 CA 体系证书策略的设计与实现。桥 CA 系统的研制、开放、测试和产品采购也可参照使用。

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。

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第 8 部分：公钥和属性证书框架(ISO/IEC 9594-8：2001，IDT)

GB/T 20518—2006　信息安全技术　公钥基础设施数字证书格式

RFC 3647　互联网 X.509 公钥基础设施：证书策略和证书运行框架(Internet X.509 Public Key Infrastructure：Certificate Policy and Certification Practices Framework)

3　术语和定义

GB/T 16264.8—2005 界定的以及下列术语和定义适用于本文件。

3.1

公钥基础设施　public key infrastructure

支持公钥管理体制并提供鉴别、加密、完整性和不可否认性服务的基础设施。

3.2

交叉认证　cross certification

两个 CA 之间建立信任关系，以使它们可以互相信任和依赖任何一方发放的证书的过程。

3.3

交叉认证协议备忘　cross-certification memorandum of agreement

确定两个 CA 之间关系、规定了双方互通后享有的信任程度的协议。

3.4

证书策略　certificate policy

一组指定的规则，指出证书对具有公共安全要求的特定团体和/或应用的适用范围。

3.5

实体 CA　entity CA

要求帮助交叉认证的具体根 CA。

3.6

订户　subscriber

从 CA 接收数字证书的实体。