ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31508—2015

信息安全技术　公钥基础设施 数字证书策略分类分级规范

Information security techniques—Public key infrastructure—Digital certificate policies classification and grading specification

2015-05-15 发布　　2016-01-01 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。

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:中国科学院数据与通信保护研究教育中心、北京数字证书认证中心有限公司、中国科学院软件所。

本标准主要起草人:荆继武、高能、林璟锵、王展、马存庆、向继、王跃武、夏鲁宁、查达仁、王平建、王琼霄、詹榜华、连一峰。

引　言

使用电子认证服务进行电子交易的实体主要关心两个问题：一是交易对象的合法公钥是什么；二是交易对象的数字证书的安全性能否用于本交易。为了体现第二方面的信息，数字证书中包含了一个由电子认证服务机构提供的证书策略标识，它表明了证书持有者（公钥所对应的用户）的安全属性。数字证书的依赖方可以通过阅读相应的证书策略文档来评估证书的安全程度，以便正确使用或依赖该证书（如：仅用于测试的，或者仅用于访问网络，或者可用于金融交易并有10万元担保）。因此，证书策略的实施是数字证书实际应用中不可缺少的一部分，也是提供分层次可靠的电子认证服务的基础之一。

目前，我国的电子认证服务机构签发的数字证书均未包含证书策略的内容，即在证书中没有说明公钥可以应用在什么场景，适用于什么样的安全需求。这导致了证书的使用者对于证书的用途十分茫然，限制了数字证书的广泛应用。另外，由于缺乏数字证书使用范围或质量的标准，各电子认证服务机构证书签发的安全措施（如：证书签发过程中的身份鉴别、物理设备安全、责任和赔付等）也存在较大差距。这种不一致导致了证书依赖方的许多困惑，阻碍了数字证书的跨区域跨行业应用，限制了应用程序直接获得证书的安全信息，对证书进行自动地验证。而标准化的证书策略能够使用户清晰地认识到证书的质量和安全通途，方便应用系统的开发设计。因此，对证书策略进行规范和标准化，是推进电子商务、电子政务系统之间互联互通的重要一步。

通过证书策略的标准化，设计数字证书策略的分级分类规范，可以为电子认证服务市场规划出分级的、多层次的服务质量体系，为不同应用系统实现适度的安全服务，从而促进电子认证服务机构之间的良性竞争，提升服务质量，推动电子认证服务市场的有序发展。另外，随着证书策略的分级分类逐步的实施，也可以促进电子认证服务机构评估和许可工作的规范化，即审查电子认证服务机构是否真正地按照其证书策略要求的规范来运营，是否提供相应的安全保障，这也是构建证书策略分级分类体系的重要意义。

信息安全技术　公钥基础设施
数字证书策略分类分级规范

1　范围

本标准通过分类分级的方式，规范了用于商业交易、设备和公众服务领域的电子认证服务中的8种数字证书策略。

本标准适用于我国电子商务和公众服务中所涉及的数字证书。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 26855—2011　信息安全技术　公钥基础设施　证书策略与认证业务声明框架

GB/T 29241—2012　信息安全技术　公钥基础设施　PKI互操作性评估准则

3　术语和定义

下列术语和定义适用于本文件。

3.1

证书签发机构　certification authority

负责签发证书和维护证书状态的实体。

3.2

订户注册机构　registration authority

负责订户的标识和鉴别，批准或拒绝订户的证书申请、撤销申请和挂起申请，发起证书的撤销和挂起的实体。

3.3

电子认证服务机构　certification service provider

依据《电子签名法》和《电子认证服务管理办法》获得《电子认证服务许可证》向公众提供电子认证业务的机构，一般包含有证书签发机构和订户注册机构。

3.4

订户　subscriber

与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的实体。订户应能对证书对应的私钥的使用负有法律责任。

3.5

依赖方　relying party

接受电子认证服务机构的依赖方协议，独立地判断证书的安全性是否满足其应用的安全需求，并验证证书和相应签名的实体。