ICS 35.020
L 80

中华人民共和国国家标准

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

Information security technology—Public key infrastructure—Certificate policy and certification practice statement framework

2011-07-29 发布　　2011-11-01 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、吉大正元信息技术股份有限公司。

本标准主要起草人:刘海龙、李伟平、何长龙、于海波、李丹、罗红斌、龙毅宏、姜玉琳。

引　言

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准中引用的 RSA 和 SHA-1 密码算法为举例性说明，具体使用时均须采用国家密码管理局批准的相应算法。

证书策略(CP)和认证业务声明(CPS)是公钥基础设施(PKI)建设中两份重要的文档。CP 是“一套指定的规则集，用以指明证书对具有相同安全需求的一个特定团体和(或者)应用类型的适用性”。依赖方可使用 CP 来帮助其决定一个证书(连同其中的绑定)是否足够可信、是否适用于特定的应用。CPS 是证书认证机构在颁发证书中所遵循的业务实践的声明。通常，CPS 也描述全部证书服务生命周期中的业务实践(如签发、管理、吊销、更新证书或密钥)，并且 CPS 提供其他业务、法律和技术方面的细节。

RFC3647 是由因特网工程任务组(IETF)制定的关于 CP 和 CPS 的框架标准，在国际上得到了广泛的认可。本标准是根据 RFC3647 制定的，主体框架与 RFC3647 一致，主要做了两方面修改：其一将与国内密码政策不符的部分进行了修改或删除；其二是将不必要的解释性文字删除，使标准更加简洁。此外，还将原标准中部分前后不一致的地方进行了改正。

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

1　范围

本标准规定了证书策略(CP)和认证业务声明(CPS)的概念,解释二者之间的区别,并规定了CP和CPS应共同遵守的文档标题框架,包括在标题中所应包含的信息类型。本标准提出的框架一般假设使用GB/T 16264.8—2005证书格式,但并不意味着此框架仅限于使用这种证书格式。此框架也可用于其他格式的证书。

本标准适用于CP和CPS的撰写和比较。本标准所给出的框架应作为一个灵活的工具来使用,用以指明在特定的CP或CPS中所应考虑的主题,而不是作为生成CP或CPS的固定公式。

本标准不适用于通用安全策略的定义,如组织安全策略、系统安全策略或数据标记策略。

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 13000.1—1993　信息技术　通用多八位编码字符集(UCS)　第1部分:体系结构与基本多文种平面(idt ISO/IEC 10646-1:1993)

GB/T 16264.2—2008　信息技术　开放系统互连　目录　第2部分:模型(ISO/IEC 9594-2:2005,IDT)

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 16284.1—2008　信息技术　信报处理系统(MHS)　第1部分:系统和服务概述(ISO/IEC 10021-1:2003,IDT)

GB/T 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

RFC 822:1982　ARPA因特网文本消息格式标准(Standard For The Format of ARPA Internet Text Messages)

RFC 5280:2008　因特网X.509公钥基础设施证书和证书撤销列表轮廓(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

3　术语和定义

GB/T 16264.8—2005确立的以及下列术语和定义适用于本文件。

3.1

激活数据　activation data

用于操作密码模块所必需的,并且需要被保护的非密钥数据值(例如PIN、口令或人工控制的密钥共享部分)。