ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20520—2006

信息安全技术　公钥基础设施 时间戳规范

Information security technology—Public key infrastructure—Time stamp specification

2006-08-30 发布　　2007-02-01 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提出并归口。

本标准起草单位：中国科学院信息安全国家重点实验室。

本标准主要起草人：冯登国、张凡、荆继武、庄湧、张立武、路晓明。

引　言

本标准主要对时间戳协议的请求响应消息格式做出了规定，并在此基础上增加了对时间戳的产生和颁发方式、时间戳系统组成、时间戳管理、时间戳系统安全的要求。

本标准参考了国内外的相关时间戳规范，最大程度地保证标准的互操作性，保证了 TSA 的互操作性、TSA 和时间戳的安全性以及 TSA 的时间精确性，为开发时间戳产品提供了可依据的标准。

本标准凡涉及密码算法相关内容，按国家密码管理部门相关规定执行。

本标准例子中提及的密码算法均为举例性说明，具体使用时均须采用国家密码管理部门批准的相应算法。

信息安全技术　公钥基础设施
时间戳规范

1　范围

本标准规定了时间戳系统部件组成、时间戳的管理、时间戳的格式和时间戳系统安全管理等方面的要求。

本标准适用于时间戳系统的设计和实现，时间戳系统的测试和产品采购亦可参照使用。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999　计算机信息系统安全保护等级划分准则

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 20273—2006　信息安全技术　数据库管理系统安全技术要求

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

RFC 2630　加密消息语法

3　术语和定义

下列术语和定义适用于本标准。

3.1

时间戳　time stamp

使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。TSA 对此对象进行数字签名产生时间戳，以证明原始文件在签名时间之前已经存在。

3.2

可信时间　trusted time

准确的、值得信赖的当前时间值，这个时间值的来源应是高度权威的。

3.3

时间戳机构　time stamp authority

用来产生和管理时间戳的权威机构。

3.4

时间戳协议　time stamp protocol

由本标准规定的一系列规范，包括时间戳的格式、各部件交流的消息格式、时间戳的颁发方式等内容。

3.5

时间戳服务　time stamp service

时间戳机构给用户提供的颁发时间戳服务，由用户提供文件，时间戳机构给此文件签发时间戳。

3.6

请求方　requester

向 TSA 系统发出申请时间戳请求的人、硬件或者软件。