



# 中华人民共和国国家标准

GB/T 36631—2018

---

## 信息安全技术 时间戳策略和时间戳业务操作规则

Information security technology—  
Time stamp policy and time stamp practice rules

2018-09-17 发布

2019-04-01 实施

---

国家市场监督管理总局  
中国国家标准化管理委员会 发布

# 目 次

前言 .....	I
引言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	2
5 时间戳策略 .....	2
5.1 概述 .....	2
5.2 时间戳策略标识 .....	2
5.3 应用实体 .....	3
5.4 适用性 .....	3
5.5 符合性 .....	3
6 时间戳业务操作规则 .....	3
6.1 业务实体 .....	3
6.2 策略管理 .....	3
6.3 时间戳管理 .....	3
6.4 时间同步管理 .....	4
6.5 密钥信息 .....	4
6.6 机构证书生成方式 .....	4
6.7 备份机制 .....	4
6.8 业务连续性 .....	4
6.9 操作管理 .....	4
7 责任与义务 .....	4
7.1 责任 .....	4
7.2 义务 .....	5
参考文献 .....	6

## 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:中国电子技术标准化研究院、中国信息安全研究院有限公司、中国科学院软件研究所、重庆邮电大学、中国科学院国家授时中心、北京数字认证股份有限公司、北京联合信任技术服务有限公司、北京科技大学、华东师范大学、国家信息安全工程技术研究中心、长春吉大正元信息技术股份有限公司、北京天威诚信电子商务服务有限公司、北京锐安科技有限公司、北京航空航天大学、西安电子科技大学、河南科技大学、中国传媒大学、中国平安保险(集团)股份有限公司、北京工业大学、北京邮电大学、北京中电普华信息技术有限公司、安徽科技学院。

本标准主要起草人:王惠莅、杨晨、张立武、黄永洪、范科峰、郭伟、詹榜华、张昌利、宁焕生、刘虹、何道敬、袁峰、赵丽丽、马文平、裴庆祺、陈晓峰、杨力、伍前红、许东阳、李琳、刁春飞、杨震、曹浩、马占宇、曹占峰、万月亮、毛剑、姜正涛、张志勇、蔡伟。

## 引 言

随着信息技术的发展,越来越多的传统应用被网络应用所代替,如电子商务、数字出版等网络应用,传统的记录时间方式在互联网环境下已不适用于证明时间是否发生在某一时刻,引发对可信第三方时间戳服务的需求。为此,国内多家证书认证机构及专业公司陆续开展了时间戳相关的业务服务,为电子取证、版权保护、电子商务等业务提供权威的、可信赖的、公正的第三方的时间戳服务。2003年,《电子签名法》颁布,为时间戳业务服务的进一步发展提供了法律保障。

为规范时间戳业务发展,本标准针对第三方时间戳服务机构,在时间戳策略、时间戳业务操作规则等应包含的时间戳标识、时间戳管理、时间戳关联方的责任与义务等内容进行规范。本标准在制定过程中参考了国内外的相关规范,结合我国时间戳服务、应用的特点进行了调整和扩充。

# 信息安全技术

## 时间戳策略和时间戳业务操作规则

### 1 范围

本标准规定了时间戳策略、时间戳业务操作规则以及责任与义务等内容。  
本标准适用于时间戳机构编制时间戳策略和时间戳业务操作规则等活动。

### 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 16262.1—2006 信息技术 抽象语法记法—(ASN.1) 第1部分:基本记法规范

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

### 3 术语和定义

GB/T 20520—2006 界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 20520—2006 中的一些术语和定义。

#### 3.1

**时间戳策略 time stamp policy**

用以指明时间戳对一个特定团体和/或具有相同安全需求的应用类型适用性的一套指定的规则集。

#### 3.2

**时间戳业务操作规则 time stamp practice**

时间戳机构针对订户和依赖方在签发、管理、删除和销毁时间戳与 TSU 密钥管理过程中所采用的业务实践。

#### 3.3

**依赖方 relying party**

时间戳接收方。

#### 3.4

**订户 subscriber**

需要由时间戳机构提供时间戳服务的实体。

#### 3.5

**时间戳机构 time stamp authority**

用来产生和管理时间戳的权威机构。

[GB/T 20520—2006,定义 3.3]

#### 3.6

**时间戳服务 time stamp service**

时间戳机构向订户提供的颁发时间戳的服务。

注:由订户提供文件,时间戳机构给此文件签发时间戳。