ICS 35.040
L 80

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

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 抽象语法记法一(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。

3.7

时间戳令牌　time stamp token

时间戳机构对包括原始文件信息、签名参数、签名时间等信息进行数字签名后产生的数据，以证明原始文件在签名时间之前已经存在。

3.8

时间戳签发单元　time stamp unit

调用时间戳机构私钥对包括原始文件信息、签名参数、签名时间等信息进行数字签名的软硬件集合。

3.9

协调世界时　universal time coordinated

以国际制秒(SI)为基准，用正负闰秒的方法保持与世界时相差在 1s 以内的一种时间。

3.10

国家授时中心协调世界时　national time service center universal time coordinated

由中国科学院国家授时中心产生并保持的协调世界时。

注：我国标准时间北京时间是通过 UTC(NTSC)计算得到的，记为北京时间＝UTC(NTSC)＋8 h。

4　缩略语

下列缩略语适用于本文件。

NTSC：中国科学院国家授时中心(National Time Service Center)

TSA：时间戳机构(Time Stamp Authority)

TSP：时间戳策略(Time Stamp Policy)

TST：时间戳令牌(Time Stamp Token)

TSU：时间戳签发单元(Time Stamp Unit)

UTC：协调世界时(Universal Time Coordinated)

UTC(NTSC)：国家授时中心协调世界时(National Time Service Center Universal Time Coordinated)

5　时间戳策略

5.1　概述

TSA 应在其颁发的时间戳中使用 5.2 定义的 TSP 标识。TSA 可以依据自己的 TSP，如果一个 TSA 能够提供比 1s 更高精度的时间，且该 TSA 所有的 TSU 均能提供此种精度，TSA 应告知此信息。

凡涉及密码算法的相关内容，按国家有关法规实施；凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

5.2　时间戳策略标识

TSP 标识：

itu-t(0)组织标识(4)etsi(0)时间戳策略(2023)策略标识号(1)基本-ts-策略(1)

itu-t(0)identified-organization(4)etsi(0)time-stamp-policy(2023)policy- identifiers(1)baseline-ts-policy(1)。

TSP 标识的编码应符合 GB/T 16262.1—2006。

5.3 应用实体

时间戳的应用实体包括订户和他们的依赖方。

5.4 适用性

适用于具有长期合法性电子签名资格的实体对时间戳的需求，通常也适用于类似性的需求。TSA签发的时间戳用以证明数据电文在申请时间戳时已经存在。

5.5 符合性

TSA 应使用 5.2 中的 TSP 标识。

TSA 应声明是否与其他更严格的 TSP 相符。

6 时间戳业务操作规则

6.1 业务实体

时间戳业务的相关实体包括：

——时间戳机构；

——订户；

——依赖方。

6.2 策略管理

应明确策略管理部门、联系人等，包括负责起草、注册、维护和更新策略和操作规则文档的部门的名称和邮件地址，以及联系人的姓名、电子邮件地址、电话号码和传真号码。

作为一种替代方案，可不指定真实人，在策略和操作规则文档中可以定义一个称谓或角色、一个电子邮件别名或其他通用联系信息。

6.3 时间戳管理

6.3.1 时间戳申请

TSA 应明确：

——提交申请的方法；

——提交申请过程中各方的责任。

6.3.2 时间戳签发

TSA 应明确：

——签发过程及方法；

——对订户的通告机制。

6.3.3 时间戳使用

TSA 应明确：

——时间戳的时间精度及时效；

——TST 的保管及期限；

——TST 验证方法。

6.3.4 时间戳销毁

在确认时间戳已经丧失其价值或订户时间戳服务期满后，TSA 可以销毁时间戳数据库或时间戳备份中的时间戳。TSA 应明确：

——时间戳销毁机制；

——时间戳销毁的通告机制。

6.3.5 时间戳异常处置

当 TSA 内部提供时间戳服务的系统由于内部错误或者外部攻击导致产生错误的时间戳时，应对错误时间戳数据进行标识。TSA 应明确：

——时间戳异常标识机制；

——时间戳异常的通告机制。

6.4 时间同步管理

TSA 应明确提供的时间戳服务的 UTC(NTSC)时间精度。

TSA 应明确保护获取时间安全的机制。

6.5 密钥信息

TSA 应支持国产密码算法，明确 TSU 密钥更新策略，并保证所有密钥在受控情况下产生：

——TSA 提供的密钥算法及密钥长度；

——TSU 使用的密钥算法及密钥长度。

6.6 机构证书生成方式

TSA 应明确时间戳机构证书的生成方式。

6.7 备份机制

TSA 应建立运营中时间戳相关信息的备份机制。

6.8 业务连续性

TSA 应明确业务连续性、可靠性等服务机制，声明其内部提供时间戳服务的系统的安全控制措施。

6.9 操作管理

TSA 应遵循以下操作管理要求：

——TSA 保证 TSU 安全、正确操作，最小化风险；

——TSA 保证其提供时间戳服务系统的接入被限制在适当的授权人员之间；

——TSA 使用可信赖的系统和产品以防止篡改。

7 责任与义务

7.1 责任

TSA 应明确业务中各方的责任，应按照与订户约定的协议条款来操作。

7.2 义务

7.2.1 TSA 义务

TSA 应在提供时间戳服务过程中：

——制定服务策略与业务操作规则，明确业务费用、争议处理、赔偿条款等；

——确保系统运行风险的可控；

——保证订户与依赖方能够得到服务策略及相关的文件；

——保障订户的商业秘密或敏感信息的安全；

——遵从国家有关法律法规和管理规定；

——确保提供与其业务操作规则相一致的时间戳服务。

7.2.2 订户义务

订户应通过使用 TSA 提供或认可的方式获取时间戳服务，履行时间戳服务协议中规定的义务。

7.2.3 依赖方义务

依赖方应通过使用 TSA 发布的方法验证 TST。

参 考 文 献

[1] GB/T 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范

[2] 工业和信息化部[2015]29号 电子认证服务管理办法

[3] RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)

[4] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities Version 1.2.2