



中华人民共和国国家标准

GB/T 20520—2025

代替 GB/T 20520—2006

网络安全技术 公钥基础设施 时间戳规范

Cybersecurity technology—Public key infrastructure—
Specification for time stamp

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目次

前言 III

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 时间戳系统组成、内容及申请颁发..... 2

 5.1 时间戳系统组成 2

 5.2 时间戳内容 3

 5.3 时间戳申请和颁发 3

6 时间戳基本要求 3

 6.1 申请和颁发方式要求 3

 6.2 可信时间产生要求 4

 6.3 时间同步要求 4

 6.4 请求和响应消息格式要求 4

7 时间戳系统安全要求 4

 7.1 安全管理要求 4

 7.2 安全技术要求 6

8 测试评价方法 8

 8.1 申请和颁发方式 8

 8.2 可信时间产生 8

 8.3 时间同步 8

 8.4 请求和响应消息格式 8

 8.5 时间戳系统安全管理要求 8

 8.6 时间戳系统安全技术要求 11

附录 A（规范性） 时间戳请求与响应消息格式的 ASN.1 描述 13

 A.1 基本要求 13

 A.2 时间戳请求格式 13

 A.3 时间戳响应格式 13

 A.4 KeyUsage 扩展域 OID 定义 16

参考文献 17

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 20520—2006《信息安全技术 公钥基础设施 时间戳规范》。与 GB/T 20520—2006 相比,除结构调整和编辑性改动外,主要技术变化如下:

- a) 更改了标准的范围(见第1章,2006年版的第1章);
- b) 将“时间戳系统的组成”更改为“时间戳系统组成、内容及申请颁发”(见第5章,2006年版的第5章、6.4、第8章);
- c) 将“时间戳的产生和颁发”更改为“时间戳基本要求”,在“申请和颁发方式要求”中增加了使用 SOAP 的方式(见 6.1),更改了“可信时间的产生方法”的部分要求(见 6.2,2006年版的 6.2);
- d) 将“对 TSA 的要求”更改为“通用要求”(见 7.1.1,2006年版的 8.1),并删除了部分要求[见 7.1.1,2006年版的 8.1 c)、d)];
- e) 删除了“在用户方的保存”(见 2006年版的 7.1.2);
- f) 删除了备份介质、异地备份和备份密码算法的要求[见 2006年版的 7.2 b)、c)、f)];
- g) 将“物理安全”“软件安全”更改为“通用安全”,增加了通信网络、区域边界、计算环境和管理中心相关要求(见 7.2.1,2006年版的 9.1、9.2);
- h) 更改了“签名系统”密码应用安全的要求(见 7.2.2,2006年版的 9.2.3);
- i) 删除了“时间戳数据库”的安全要求(见 2006年版的 9.2.4);
- j) 删除了“保存文件”文件扩展名的要求(见 2006年版的 8.2.5);
- k) 增加了“测试评价方法”,给出了与安全要求对应的测试评价方法(见第8章);
- l) 更改了时间戳请求与响应消息格式的 ASN.1 结构及其描述(见附录 A,2006年版的 8.4)。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国科学院软件研究所、中国科学院大学、长春吉大正元信息技术股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、北京数字认证股份有限公司、中电科网络安全科技股份有限公司、北京中关村实验室、公安部第三研究所、工业和信息化部网络安全产业发展中心(工业和信息化部信息中心)、广东省电子商务认证有限公司、北京天融信网络安全技术有限公司、博雅中科(北京)信息技术有限公司、数安时代科技股份有限公司、同智伟业软件股份有限公司、亚数信息科技有限公司(上海)有限公司、上海市数字证书认证中心有限公司、国网区块链科技(北京)有限公司、陕西省信息化工程研究院、郑州信大捷安信息技术股份有限公司、杭州海康威视数字技术股份有限公司、长扬科技(北京)股份有限公司、北京时代新威信息技术有限公司、北京芯盾时代科技有限公司、北京天融信网络安全技术有限公司、深圳市电子商务安全证书管理有限公司、江南信安(北京)科技有限公司、浙江大华技术股份有限公司、奇安信网神信息技术(北京)股份有限公司、浙江九州量子信息技术股份有限公司、中孚信息股份有限公司、工信通(北京)信息技术有限公司、中国电子信息产业集团有限公司第六研究所。

本文件主要起草人:冯登国、张严、张立武、荆继武、杨领波、张宝欣、刘丽敏、胡建勋、赵松、李官麟、孟佳颖、陈妍、潘毅、陈子雄、肖臻、张超、程科伟、邓钊汉、焦正坤、魏一才、王玉林、高振鹏、杨珂、赵晓荣、刘为华、王滨、赵华、杜云浩、王在方、梁珍权、汪海洋、陈芳、黄亮、於建江、陈腾、王斌、陈怀凤。

本文件及其所代替文件的历次版本发布情况为:

——2006年首次发布为 GB/T 20520—2006;

——本次为第一次修订。

网络安全技术 公钥基础设施 时间戳规范

1 范围

本文件给出了时间戳系统组成、时间戳的内容和申请颁发流程,规定了时间戳安全要求,描述了相应的测试评价方法。

本文件适用于时间戳系统及其应用的设计、开发与测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 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 20518—2018 信息安全技术 公钥基础设施 数字证书格式
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

时间戳 time stamp

时间戳令牌 time stamp token

对包括原始数据信息、签名参数、签名时间等确认后,使用数字签名技术产生的以证明原始数据在签名时间之前已经存在的数据。

3.2

可信时间 trusted time

准确的、可信赖的当前时间值。

3.3

时间戳机构 time stamp authority

用来产生和管理时间戳的可信服务机构。

[来源:GM/Z 0001—2013,2.101]

3.4

时间戳服务 time stamp service

用以证明原始数据在某一时刻前已存在的服务。



注:由请求方提供数据,时间戳系统为此数据签发时间戳。

[来源:ISO/IEC 18014-1:2008,3.18,有修改]

3.5

请求方 requester

向时间戳机构(3.3)发出申请时间戳请求的实体。

3.6

时间戳系统 time stamp system

公钥基础设施密码应用技术体系中实现时间戳申请接收、申请合法性验证、时间戳产生和颁发、时间戳管理等功能的信息系统。

3.7

公钥基础设施 public key infrastructure

基于公钥密码技术,具有普适性,可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。

[来源:GB/T 25069—2022,3.212]

4 缩略语

下列缩略语适用于本文件。

DER:可辨别编码规则(Distinguished Encoding Rules)

HTTP:超文本传输协议(Hyper Text Transfer Protocol)

HTTPS:超文本传输安全协议(Hyper Text Transfer Protocol Secure)

SFTP:安全文件传输协议(Secure File Transfer Protocol)

SOAP:简单对象访问协议(Simple Object Access Protocol)

TSA:时间戳机构(Time Stamp Authority)

TST:时间戳令牌(Time Stamp Token)

UTC:协调世界时(Universal Time Coordinated)

5 时间戳系统组成、内容及申请颁发

5.1 时间戳系统组成

公钥基础设施密码应用技术体系中的时间戳系统组成见图 1,包括以下三个部分。

- 可信时间源:时间戳系统的时间来源,负责为系统颁发的时间戳提供可信的时间来源,在颁发时间戳时,依据可信时间源填写时间。
- 签名系统:负责接收时间戳申请,验证申请合法性,产生和颁发时间戳。
- 时间戳数据库:负责保存签名系统颁发的时间戳。

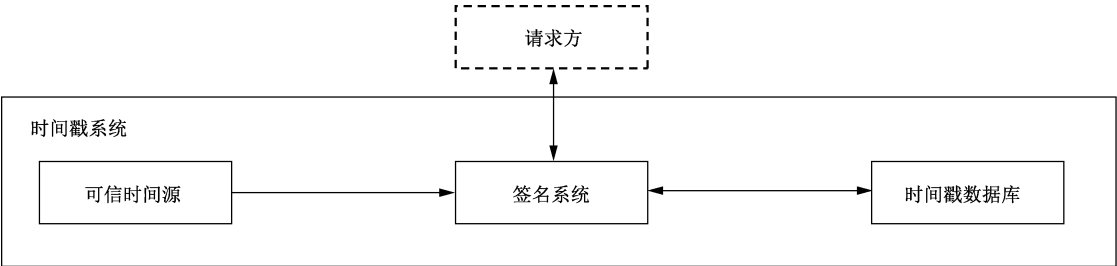


图 1 时间戳系统组成

5.2 时间戳内容

时间戳中包括以下内容：

- 时间戳的版本号；
- 表明时间戳生成时的安全策略的唯一标识符；
- 生成该时间戳时的可信时间值；
- 与可信时间值绑定的数据的杂凑值；
- 该时间戳的序列号；
- TSA 使用其签名密钥对待签名数据的签名；
- 计算数据杂凑时使用的杂凑算法的对象标识符；
- 时间戳的可能误差及排序条件(可选项)；
- TSA 的名称(可选项)；
- TSA 支持的,与请求方通过申请消息扩展域内提出的额外要求对应的扩展信息(可选项)。

5.3 时间戳申请和颁发

请求方与 TSA 交互进行时间戳申请和颁发过程包括以下步骤。

- a) 请求方向 TSA 提交申请请求,TSA 的签名系统接收到申请请求后,对请求消息的合法性进行检验。
- b) 如果请求消息格式不正确或者由于某种内部原因 TSA 无法颁发这个时间戳,TSA 产生时间戳失败响应,并在响应中详细描述申请被拒绝的原因。
- c) 如果请求消息合法,TSA 的签名系统填写时间戳并进行签名,同一个 TSA 可在不同场景下使用多个不同签名密钥的私钥进行签名,例如:为适应不同的策略、不同的算法、不同的密钥长度和不同的性能要求。
- d) TSA 的签名系统通过可信信道把新生成的时间戳发送给时间戳数据库,由时间戳数据库将其归档保存,对于申请被拒绝而产生的时间戳失败响应,由 TSA 本身的策略决定是否将其保存。
- e) TSA 通过与用户申请方式对应的颁发方式,将新生成的时间戳发给用户。
- f) 用户在收到时间戳后,使用 TSA 的证书验证时间戳的合法性,并检验时间戳内容是否有错误。如果时间戳不合法或者有错误,用户通过 TSA 提供的用户反馈渠道向 TSA 管理者报告异常情况,如果时间戳有效,用户自行保存此时间戳。

6 时间戳基本要求

6.1 申请和颁发方式要求

TSA 应支持采用以下一种或多种方式接收时间戳申请并颁发时间戳。

- 通过电子邮件方式。用户使用电子邮件向一个 TSA 指定的电子邮件地址发送时间戳申请,TSA 将颁发的时间戳通过电子邮件返回给用户。
- 通过文件传输方式。用户将申请消息编码存储在一个扩展名为.tsr 的文件中传送给 TSA,TSA 将产生的响应消息编码保存在一个扩展名为.tsr 的文件中返回给用户,文件的传送可使用任意可信赖的方法,例如:SFTP 协议等。
- 通过套接层连接方式。TSS 通过某个端口监听用户发来的申请,而用户在与这个端口建立一个安全的套接层连接后,与 TSS 传输申请消息和响应消息。
- 通过 HTTP/HTTPS 方式。用户通过 HTTP/HTTPS 协议将申请消息发送给 TSA,TSA 通过 HTTP/HTTPS 协议返回时间戳响应消息。

——通过 SOAP 方式。用户通过 SOAP 协议将申请消息的 DER 编码发送给 TSA, TSA 通过 SOAP 协议返回时间戳的 DER 编码响应消息。

6.2 可信时间产生要求

在产生可信时间时,对时间来源、准确性和安全性保障等方面的要求包括:

- a) 可信时间源产生的时间应能溯源至标准时间,可从标准时间的发布机构(例如:国家授时中心等)使用某种硬件或软件授时方法获得,包括使用无线装置通过长波信号、卫星信号等获得,使用某种时间同步协议从发布机构指定的网络地址通过安全信道获得等;
- b) 在获取标准时间时,应采取完整性保护措施抵御传输错误和篡改攻击;
- c) 应根据所采用的授时方法评估所产生的可信时间与标准时间的误差,并公布最大可能误差作为可信程度的一个标志;
- d) 可信时间源可首先使用多种方法分别产生多个时间值,然后依据每种方法的可能误差和可信程度使用特定方案(例如:计算加权平均)产生最终的时间值;
- e) 应采用措施确保从可信时间源到签名系统的传输过程中时间信息的完整性,使得签名系统有能力发现对时间信息的篡改,并向 TSA 管理者发出警告。

6.3 时间同步要求

时间戳系统根据可信时间源对各组件进行时间同步时,满足以下要求:

- a) 应定期从可信时间源获得可信时间,再根据可信时间进行时间同步;
- b) 在获得可信时间后,应根据可信时间对所有组件的时间进行调整,时间同步的优先级应高于其他操作(例如:时间戳请求的处理);
- c) 每次同步的间隔时间不应长于 30 min,可根据运行策略以及运行的硬件或软件时钟的可靠性等因素使用更短的同步间隔;
- d) 每次同步的间隔时间应可配置;
- e) 时间戳系统各个组件应采取统一行动检验并同步时间;
- f) 在启动时间戳系统的过程中,可信时间源应在开始提供时间戳服务之前启动,可信时间源启动后,TSA 在开始提供时间戳服务之前应先等待一段时间,以保证开始颁发时间戳时,各组件已经完成了与可信时间源的同步;
- g) 在定期同步时间的过程中,如果获得可信时间失败或者发现收到的时间信息被篡改,应立即停止时间同步和接收时间戳申请,同时向管理者发出警报并写入审计日志。

6.4 请求和响应消息格式要求

请求者与 TSA 间发送的时间戳请求和响应消息格式应符合附录 A 的要求。

7 时间戳系统安全要求

7.1 安全管理要求

7.1.1 通用要求

通用要求包括以下内容。

- a) 应拥有可信时间源,并保证除可信时间源以外的其他实体(包括签名系统和时间戳请求方等)无法对时间源进行控制。
- b) 应确保每一个时间戳中都包含一个来自可信时间源的时间值。

- c) 在生成时间戳时,应在其中包含表明了该时间戳生成时采用的安全策略的对象标识符。
- d) 应只对数据的杂凑值生成时间戳,使用的杂凑函数应拥有唯一的对象标识符。
- e) 应检验杂凑函数的标识符,并且验证数据的杂凑值长度是否符合该杂凑函数预期的结果长度。
- f) 不应应对杂凑值数据进行除杂凑值长度以外的任何检验。
- g) 应检验在时间戳请求中表示的杂凑算法是否符合国家或密码行业相关标准,如果无法识别给出的杂凑算法或该杂凑算法不符合国家或密码行业相关标准,应拒绝提供时间戳服务,并在返回消息中包含相关信息,例如:设置 pkiStatusInfo 域中的 PKIFailureInfo 结构数据为 badAlg (0)。
- h) 时间戳内不应包含任何请求方的标识,如果需要鉴别请求方的身份,应另外进行双向身份鉴别。
- i) 应使用专门的签名密钥对时间戳签名,时间戳签名密钥的数字证书格式应符合 GB/T 20518—2018 的规定,且证书的扩展密钥用途中应包含 id-kp-timeStamping,扩展密钥用途的格式见 GB/T 20518—2018 中 5.2.4.2.5。
- j) 如果请求方在申请消息的扩展域内提出了请求并且时间戳系统支持这些扩展,应在生成的时间戳内包含相应的额外信息,如果时间戳系统不支持其中的某些扩展,应返回错误信息。
- k) 应对用户异常报告具有完备的处理预案,当管理员收到用户的异常报告时,通过检验审计日志和时间戳数据库等找出错误原因。

7.1.2 时间戳的保存

时间戳保存的要求包括:

- a) 时间戳数据库应负责保存由 TSA 产生的所有时间戳;
- b) 时间戳数据库可在一定时间后或者数据库中的数据达到一定的量后,将数据库中的所有或部分数据转移到他处保存,这一过程应配置为仅能由管理员执行,并且转移后数据的保存应符合 7.1.3 对时间戳备份的要求;
- c) 对于每一个时间戳,时间戳数据库在保存它们时至少应保存时间戳入库的时间、时间戳的序列号与时间戳的完整编码数据。

7.1.3 时间戳的备份

时间戳备份的要求包括:

- a) 管理员应定期执行备份操作,对时间戳数据库的所有数据进行备份;
- b) 备份数据应以方便检索的方式存放;
- c) 备份数据的访问应仅在管理员在场并对其进行身份鉴别后才能执行。

7.1.4 时间戳的恢复

时间戳恢复的要求包括:

- a) 应支持通过时间戳备份数据恢复时间戳;
- b) 时间戳恢复操作应仅在管理员在场并对其进行身份鉴别后才能执行。

7.1.5 时间戳的检索

时间戳检索的要求包括:

- a) 应向请求方提供能方便地检索时间戳的方法,使请求方可通过网络或者面对面的方式检索和获得时间戳;
- b) 向请求方提供的可检索的时间戳应包括时间戳数据库中保存的时间戳和以前备份的时间戳;

- c) 应至少支持通过以下三种信息检索时间戳,并满足下列要求:
- 根据时间戳入库的时间检索,该方式可返回多个结果,再由用户自行选择;
 - 根据时间戳的序列号检索,该方式应返回至多一个结果;
 - 根据时间戳的完整编码检索,该方式应返回至多一个结果。

7.1.6 时间戳的删除

时间戳删除的要求包括:

- a) 应支持对时间戳数据库中错误时间戳数据的删除;
- b) 所有即将从时间戳数据库中删除的时间戳数据应先进行备份,因删除而备份的错误数据应与正常备份数据区分并单独存放,并符合 7.1.3 中对时间戳数据备份的要求;
- c) 应及时通过公开渠道公布所有被删除时间戳的详细信息;
- d) 时间戳的删除操作应配置为仅能由管理员执行。

7.1.7 时间戳的销毁

在确定时间戳已经丧失其价值后,可完全销毁时间戳,时间戳的销毁包括从时间戳数据库和时间戳备份中同时删除。时间戳销毁的要求包括:

- a) 时间戳应只在 TSA 证书失效后被销毁;
- b) TSA 可根据策略决定时间戳的保存时间,这一保存时间应足够长,以确保在超过保存时间时,时间戳已丧失使用价值,TSA 应在用户申请时间戳时向用户详细说明时间戳保存时间的策略;
- c) 时间戳的销毁操作应配置为仅能由管理员执行。

7.1.8 时间戳的查看

应向请求方提供查看已颁发的时间戳的方式,使请求方可凭借此方法查看时间戳中所有可查看的内容,例如:提供查看软件等。

7.1.9 时间戳的验证

时间戳验证的要求如下。

- a) 应向请求方提供对时间戳进行验证的方式,使请求方可对已颁发的时间戳的正确性和有效性进行验证,例如:提供验证软件或者通过互联网验证等。
- b) 应向用户提供 TSA 证书及验证该证书所需的必要数据,确保证验时间戳前,用户能验证 TSA 证书的有效性。
- c) 提供的验证服务应包括对以下内容的验证:
 - 使用 TSA 证书验证用户给定的时间戳是否是由该 TSA 签发;
 - 使用用户提供的时间戳和源文件,验证该时间戳是否对应该文件。

7.2 安全技术要求

7.2.1 通用安全

时间戳系统的物理环境、通信网络、区域边界、计算环境和管理中心安全应满足 GB/T 22239—2019 中第 7 章的要求。

7.2.2 签名系统

签名系统的密码应用应满足 GB/T 39786 第二级或以上要求。

7.2.3 时间戳文件保存

通过文件对时间戳进行保存时,存储时间戳申请和响应消息内容的文件中应只包含消息的 DER 编码,不应有额外的消息头和消息尾。

7.2.4 日志审计

日志审计的要求包括以下内容。

- a) 签名系统应通过审计功能组件提供日志审计功能,对审计功能的启动和结束以及表 1 中的事件产生审计记录。
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功,以及表 1 中附加信息栏中的相应内容。

表 1 审计事件及审计记录内容

功能	事件	附加信息
安全审计	对审计变量的修改	
	对审计记录进行删除或尝试删除的操作	
	审计日志签名	审计日志的数字签名、杂凑值或消息鉴别码
本地数据输入	所有安全相关数据的输入	
远程数据输入	所有被系统接受的安全相关信息	
数据输出	对关键或安全相关信息进行输出的请求	
私钥载入	组件私钥的载入	
私钥存储	对为密钥恢复而保存的证书主体私钥的读取	
公钥的输入、删除和存储	对公钥的改变	公钥和与公钥相关的信息
私钥和秘密密钥的输出	对私钥和秘密密钥的输出,包括一次性会话密钥	
时间戳申请	所有的时间戳申请请求	若申请成功,保存申请请求和所产生的时间戳的拷贝 若申请失败,保存申请请求和所产生的时间戳响应的拷贝
组件的配置	所有与安全相关的配置	
可信时间的获取和同步	根据可信时间源同步时间	可信时间与本地时间不匹配时,对本地时间的改变 同步过程中发生的所有错误
审计日志时间戳生成	为审计日志生成时间戳	生成的时间戳

- c) 审计记录中的秘密密钥、私钥和其他安全相关的秘密参数不应以明文形式出现。
- d) 审计功能组件应能将可审计事件与发起该事件的系统用户身份相关联。

- e) 审计功能组件应为审计员提供查看日志信息的能力,并以适于阅读和解释的方式显示。
- f) 审计功能组件应在审计事件存储过程中防止对审计记录的非授权修改,并可检测对审计记录的修改。
- g) 当审计日志存储已满时,审计功能组件应能阻止除由管理员发起以外的所有审计事件的发生,以防止审计数据丢失。
- h) 审计功能组件应确保每一条审计记录都具有正确、可信的时间。
- i) 审计功能组件应定期为审计日志生成时间戳,时间戳中签名的对象包含上次生成时间戳后加入的所有审计日志条目以及上次生成的时间戳的值,为审计日志生成时间戳的周期应可配置。

8 测试评价方法

8.1 申请和颁发方式

申请和颁发方式的测试评价方法如下。

- a) 测试方法:对照 6.1 的申请和颁发方式,进行时间戳申请,检验时间戳系统是否支持 6.1 中列出的申请和颁发方式。
- b) 预期结果:时间戳系统支持 6.1 中规定的至少一种申请和颁发方式。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.2 可信时间产生

可信时间产生的测试评价方法如下。

- a) 测试方法:对照 6.2 的可信时间产生要求,检验时间戳系统的时间来源是否可溯源至标准时间、是否能抵御传输错误和篡改攻击、是否公布了授时方法的误差。
- b) 预期结果:TSA 产生的时间能溯源至标准时间,采取了抵御传输错误和篡改攻击的措施,并公布了可信时间与标准时间的最大可能误差。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.3 时间同步

时间同步的测试评价方法如下。

- a) 测试方法:对照 6.3 的时间同步要求,检验时间戳系统的时间同步。
- b) 预期结果:TSA 采用 6.3 中给出的方式,在 TSS 各组件之间实现了时间同步。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.4 请求和响应消息格式

时间戳请求和响应消息格式的测试评价方法如下。

- a) 测试方法:尝试进行时间戳申请,获取时间戳请求和响应消息,检验时间戳系统的时间戳请求和响应消息的内容格式是否与附录 A 要求一致。
- b) 预期结果:时间戳请求和响应消息与附录 A 要求一致。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5 时间戳系统安全管理要求

8.5.1 通用要求

通用要求的测试评价方法如下。

a) 测试方法:

- 1) 检验时间戳系统是否具有可信时间源;
- 2) 查看时间戳系统生成的时间戳,检验其中是否都包含一个可信时间值;
- 3) 查看时间戳系统生成的时间戳,检验其中是否都包含表明了该时间戳生成时采用的安全策略的对象标识符;
- 4) 查看时间戳系统生成的时间戳,检验时间戳是否只对数据的杂凑值生成,杂凑函数是否拥有唯一的对象标识符;
- 5) 查看时间戳系统生成的时间戳,检验数据的杂凑值长度是否符合杂凑函数标识符对应的杂凑函数的结果长度;
- 6) 检验时间戳系统对杂凑值数据的验证机制,是否符合 7.1.1 f) 的要求;
- 7) 检验时间戳系统是否对时间戳请求中表示的杂凑算法进行验证,当请求中给出无法识别或不符合国家或密码行业相关标准时,是否能拒绝提供时间戳服务,并在返回消息中包含相关信息;
- 8) 查看时间戳系统生成的时间戳,检验其中是否包含任何请求方的标识,并符合 7.1.1 h) 的要求;
- 9) 检验时间戳系统的时间戳签名密钥的用途以及具有的证书,是否符合 7.1.1 i) 的要求;
- 10) 检验时间戳系统对时间戳请求中扩展域的处理机制是否符合 7.1.1 j) 的要求;
- 11) 检验时间戳系统是否具有应对用户异常报告的处理预案,预案是否符合 7.1.1 k) 的要求。

b) 预期结果:

- 1) 时间戳系统具有可信时间源,并符合 6.2 的要求;
- 2) 生成的时间戳均包含可信时间值;
- 3) 生成的时间戳均包含表明了该时间戳生成时采用的安全策略的对象标识符;
- 4) 生成的时间戳均只对数据的杂凑值生成,且杂凑函数拥有唯一对象标识符;
- 5) 生成的时间戳中数据的杂凑值长度与杂凑函数标识符对应的杂凑函数的结果长度;
- 6) 时间戳系统具有对杂凑值数据的检验机制,并符合 7.1.1 f) 的要求;
- 7) 时间戳系统对时间戳请求中表示的杂凑算法进行检验,当请求中给出无法识别或不符合国家或密码行业相关标准时,能拒绝提供时间戳服务,并在返回消息中包含相关信息;
- 8) 时间戳系统生成的时间戳中均包含请求方的标识,并符合 7.1.1 h) 的要求;
- 9) 时间戳系统的时间戳签名密钥具有有效证书,证书中的密钥用途符合 7.1.1 i) 的要求;
- 10) 时间戳系统对时间戳请求中扩展域的处理机制符合 7.1.1 j) 的要求;
- 11) 时间戳系统具有应对用户异常报告的处理预案,预案符合 7.1.1 k) 的要求。

c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.2 时间戳的保存



时间戳的保存的测试评价方法如下。

- a) 测试方法:对照 7.1.2 的要求,检验时间戳的保存方式、位置和存储的内容。
- b) 预期结果:时间戳保存的方式、位置和存储的内容请求符合 7.1.2 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.3 时间戳的备份

时间戳的备份的测试评价方法如下。

- a) 测试方法:对照 7.1.3 的要求,检验时间戳的备份机制。

- b) 预期结果:时间戳备份的方式、位置和存储的内容请求符合 7.1.3 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.4 时间戳的恢复

时间戳的恢复的测试评价方法如下。

- a) 测试方法:对照 7.1.4 的要求,检验时间戳的恢复机制。
- b) 预期结果:时间戳系统支持对备份的时间戳进行恢复,操作的访问控制符合 7.1.4 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.5 时间戳的检索

时间戳的检索的测试评价方法如下。

- a) 测试方法:对照 7.1.5 的要求,检验是否提供了时间戳检索方法。
- b) 预期结果:时间戳系统提供了时间戳检索方法,可检索时间戳的范围和支持的用于检索时间戳的信息符合 7.1.5 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.6 时间戳的删除

时间戳的删除的测试评价方法如下。

- a) 测试方法:对照 7.1.6 的要求,检验是否具备时间戳删除机制。
- b) 预期结果:时间戳系统具备时间戳删除机制,删除机制中备份信息、公开信息和删除操作的访问控制符合 7.1.6 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.7 时间戳的销毁

时间戳的销毁的测试评价方法如下。

- a) 测试方法:对照 7.1.7 的要求,检验是否具备时间戳销毁机制。
- b) 预期结果:时间戳系统具备时间戳销毁机制,销毁机制的执行策略和销毁操作的访问控制符合 7.1.7 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.8 时间戳的查看

时间戳的查看的测试评价方法如下。

- a) 测试方法:对照 7.1.8 的要求,检验是否提供了时间戳查看方法。
- b) 预期结果:时间戳系统提供了时间戳查看方法,可通过该机制查看到的时间戳信息符合 7.1.8 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.5.9 时间戳的验证

时间戳的验证的测试评价方法如下。

- a) 测试方法:对照 7.1.9 的要求,检验是否提供了时间戳验证方法。
- b) 预期结果:时间戳系统提供了时间戳验证方法,支持的验证内容符合 7.1.9 的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.6 时间戳系统安全技术要求

8.6.1 通用安全

通用安全的测试评价方法如下。

- a) 测试方法:通过时间戳系统开发者提供的证明材料,检验时间戳系统的物理环境、通信网络、区域边界、计算环境和管理中心是否满足 GB/T 22239—2019 等级保护第二级或以上的要求。
- b) 预期结果:时间戳系统的物理环境、通信网络、区域边界、计算环境和管理中心满足 GB/T 22239—2019 等级保护第二级或以上的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.6.2 签名系统

签名系统的测试评价方法如下。

- a) 测试方法:通过时间戳系统开发者提供的证明材料,检验签名系统的密码应用是否满足 GB/T 39786 第二级或以上的要求。
- b) 预期结果:签名系统的密码应用满足 GB/T 39786 第二级或以上的要求。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.6.3 时间戳文件保存

时间戳文件保存的测试评价方法如下。

- a) 测试方法:访问时间戳数据库,检验保存存储时间戳申请和响应消息的文件的内容。
- b) 预期结果:存储时间戳申请和响应消息的文件是否只包含消息的 DER 编码,没有额外的消息头和消息尾。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。

8.6.4 日志审计

日志审计的测试评价方法如下。

- a) 测试方法:对以下内容进行测试。
 - 1) 签名系统是否具备日志审计功能,以及审计记录的范围。
 - 2) 签名系统的审计记录中是否包含了 7.2.4 b) 中列出的所有应记录的内容。
 - 3) 审计记录中涉及秘密密钥、私钥和其他安全相关的秘密参数是否进行了加密等措施,不以明文形式出现。
 - 4) 审计功能组件是否能将可审计事件与发起该事件的系统用户身份相关联。
 - 5) 审计功能组件是否为审计员提供了查看日志信息的能力,并以适于阅读和解释的方式显示。
 - 6) 审计功能组件是否提供了防篡改机制,在审计事件存储过程中防止对审计记录的非授权修改,并可检测对审计记录的修改。
 - 7) 当审计日志存储已满时,审计功能组件是否能阻止除由管理员发起以外的所有审计事件的发生,以防止审计数据丢失。
 - 8) 审计功能组件是否能确保每一条审计记录都具有可信时间。
 - 9) 审计功能组件是否能定期通过 TSA 为审计日志生成时间戳,并确认时间戳对应的数据内容。
- b) 预期结果:

- 1) 签名系统具备日志审计功能,能对审计功能的启动和结束以及表 1 中的时间产生审计记录;
 - 2) 审计记录包含了 7.2.4 b)中列出的所有应记录的内容;
 - 3) 审计记录中涉及秘密密钥、私钥和其他安全相关的秘密参数均进行了加密等措施,不以明文形式出现;
 - 4) 审计功能组件能将可审计事件与发起该事件的系统用户身份相关联;
 - 5) 审计功能组件为审计员提供了查看日志信息的能力,并以适于阅读和解释的方式显示;
 - 6) 审计功能组件提供了防篡改机制,在审计事件存储过程中防止对审计记录的非授权修改,并可检测对审计记录的修改;
 - 7) 当审计日志存储已满时,审计功能组件能阻止除由管理员发起以外的所有审计事件的发生,以防止审计数据丢失;
 - 8) 审计功能组件能确保每一条审计记录都具有可信时间;
 - 9) 审计功能组件能定期通过 TSA 为审计日志生成时间戳,时间戳中签名的对象包含上次生成时间戳后加入的所有审计日志条目以及上次生成的时间戳的值,并支持对审计日志生成时间戳周期的配置。
- c) 结果判定:上述预期结果均满足判定为符合,其他情况判定为不符合。



附录 A
(规范性)

时间戳请求与响应消息格式的 ASN.1 描述

A.1 基本要求

应采用 GB/T 16262.1 规定的抽象语法规法 (ASN.1) 对时间戳请求和响应消息格式进行描述。

A.2 时间戳请求格式

```
TimeStampReq ::= SEQUENCE{
    version                INTEGER{ v2(2) },
    messageImprint         MessageImprint,
    reqPolicy              TSAPolicyId OPTIONAL,
    nonce                  INTEGER OPTIONAL,
    certReq                BOOLEAN DEFAULT FALSE,
    extensions              [0]IMPLICIT Extensions OPTIONAL
}
```

其中：

- version 域表示时间戳申请消息格式的版本号，依据本文件生成的申请消息版本为 2。
- messageImprint 域包含需要加盖时间戳的数据的摘要值。该摘要值的类型是 OctetString，长度是相应杂凑算法的杂凑值长度。具体格式为：
MessageImprint ::= SEQUENCE{
 hashAlgorithm AlgorithmIdentifier,
 hashedMessage OCTET STRING
}
- reqPolicy 域表示安全策略，安全策略由 TSA 提供。如果用户需要指明时间戳应在什么样的安全策略下生成，用户可设置 reqPolicy 域说明需要的安全策略。reqPolicy 的类型是 TSAPolicyId，TSAPolicyId 的定义为：
TSAPolicyId ::= OBJECT IDENTIFIER
- nonce 域是一个随机数，用于在没有可靠的本地时钟的情况下检验响应消息的合法性并防止重放攻击。
- certReq 域用于请求 TSA 公钥证书。如果请求消息中有 certReq 域并且为 true，则 TSA 在其响应消息中给出其公钥证书，该证书由响应消息中 SigningCertificate 属性的 ESSCertID 指出，证书存放在响应消息中 SignedData 结构的 Certificates 域中。
- extensions 为扩展域，用于为申请消息添加额外信息。对于其中任何一个扩展，无论其是否是关键扩展，当它在请求消息中出现且又无法被 TSA 识别时，TSA 应不为该请求生成时间戳并返回一个失败信息 (unacceptedExtension)。

A.3 时间戳响应格式

TSA 在收到申请消息后，应给请求方返回响应消息。该响应消息包含签发的时间戳，或是与时间戳申请相对应的失败信息。

时间戳响应消息的 ASN.1 数据格式如下。

```
TimeStampResp ::= SEQUENCE{
    status PKIStatusInfo,
    timeStampToken TimeStampToken OPTIONAL
}
```

其中:

```
PKIStatusInfo ::= SEQUENCE{
    status PKIStatus,
    statusString PKIFreeText OPTIONAL,
    failInfo PKIFailureInfo OPTIONAL
}
```

其中:

```
PKIStatus ::= INTEGER{
    granted (0),
    grantedWithMods (1),
    rejection (2),
    waiting (3),
    revocationWarning (4),
    revocationNotification (5)
}
```

当且仅当 PKIStatusInfo 中的 status 值为 0 或者 1 时,响应消息中应包含 TimeStampToken。
status 不应有除 PKIStatus 外的其他值。

如果申请失败,则用 statusString 给出一个说明失败原因的字符串。statusString 的类型是 PKIFreeText,其定义为:

```
PKIFreeText ::= SEQUENCE SIZE (1..MAX) OF UTF8String
```

failInfo 用来说明时间戳请求被拒绝的具体原因,其值如下。

```
PKIFailureInfo ::= BIT STRING{
    badAlg (0),--申请使用了不支持的算法
    badRequest (2),--非法的申请
    badDataFormat (5),--数据格式错误
    timeNotAvailable (14),--TSA 的可信时间源出现问题
    unacceptedPolicy (15),--不支持申请消息中声明的策略
    unacceptedExtension (16),--申请消息中包括了不支持的扩展
    addInfoNotAvailable (17),--有不理解或不可用的附加信息
    systemFailure (25),--系统内部错误
}
```

failInfo 不能有 PKIFailureInfo 外的其他值,请求方如果收到一个不识别的值,应报告错误。

TimeStampToken 是一个 ContentInfo 结构,当使用的公钥算法为 SM2 时,ContentInfo 结构定义见 GB/T 35275。当公钥算法为 SM9 时,ContentInfo 结构定义见 GM/T 0081。该结构中 content type 是一个 signedData content type,具体值如下。

```
TimeStampToken ::= ContentInfo
--content type 为 id-signedData
--content 为 SignedData
```

当使用的公钥算法为 SM2 时,SignedData 结构定义见 GB/T 35275。当公钥算法为 SM9 时,

SignedData 结构定义见 GM/T 0081。

TimeStampToken 不应含有除 TSA 签名以外的任何其他数字签名。TSA 证书的证书标识符(Es-sCertID 或 EssCertIDv2)作为 SignedInfo 的属性包含在 SigningCertificate 属性里。

TSTInfo 的具体定义如下。

TSTInfo ::= SEQUENCE{
 version INTEGER{ v2(2) },
 policy TSAPolicyId,
 messageImprint MessageImprint,
 serialNumber INTEGER,
 genTime GeneralizedTime,
 accuracy Accuracy OPTIONAL,
 ordering BOOLEAN DEFAULT FALSE,
 nonce INTEGER OPTIONAL,
 tsa [0]GeneralName OPTIONAL,
 extensions [1]IMPLICIT Extensions OPTIONAL
}

对于 TSTInfo 的各项解释如下。

- version 域指明了时间戳的版本号。
- policy 域指明响应消息是根据 TSA 的哪个策略生成的。如果类似的域出现在 TimeStampReq 中,该域具有相同的值;否则需要返回 unacceptedPolicy 错误。policy 域中包含的信息包括:
 - 该时间戳的使用条件;
 - 时间戳日志的有效性,可用于后续增强时间戳的可信度。
- messageImprint 同 TimeStampReq 中类似的域有相同的值,前提是杂凑值的长度与 hashAlgorithm 标记的算法预期的长度相同。
- serialNumber 域是 TSA 分配的一个整数。对一个给定的 TSA 发出的每一个时间戳,serialNumber 应是唯一的。即使经历一个可能的服务中断(例如崩溃)后,该特性也应保留。
- genTime 是 TSA 创建时间戳的时间。应用 UTC 时间表示,以减少使用本地时区用法造成的混乱。时间表示的语法结构为:YYYYMMDDhhmmss[.s...]Z。
- accuracy 表示时间可能出现的最大误差,genTime 加上 accuracy 的值,可得到 TSA 创建这个时间戳的时间上限;同理,减去 accuracy 就是 TSA 创建时间戳的时间下限。具体定义如下:

Accuracy ::= SEQUENCE{
 seconds INTEGER OPTIONAL,--s
 millis [0]INTEGER(1..999)OPTIONAL,--ms
 micros [1]INTEGER (1..999) OPTIONAL --μs
}

如果 seconds、millis 或者 micros 未出现,则未出现域的值应被赋为 0。当 accuracy 这个可选项不出现时,精确度可从别的途径得到,例如 TSAPolicyId。

- ordering 表示时间戳排序条件。如果 ordering 域不出现,或者 ordering 域出现但被置为 false,那么 genTime 域只表示 TSA 创建时间戳的时间。在这种情况下,当两个时间戳中第一个的 genTime 与第二个的 genTime 之差大于这两个 genTime 的精确度的和,同一个 TSA 或者不同的 TSA 签发的时间戳标志才有可能排序。如果 ordering 域出现并被置为 true,同一个 TSA 发的每一个时间戳都可依据 genTime 排序,而不必考虑 genTime 精确度。

- 如果在 TimeStampReq 中出现了 nonce 域,则此处也应出现 nonce 域,其值应等于 TimeStampReq 中的值。
- tsa 域的目的是为鉴别 TSA 的名称提供的一个线索。如果出现,应与用于验证时间戳的证书里的主体名称中的一个相同。
- extensions(扩展)域是为将来增加额外的信息而采用的一种通常的做法。特殊的扩展类型可由组织或者团体自行定义并声明注册。

A.4 KeyUsage 扩展域 OID 定义

用于时间戳消息签名的密钥证书的 KeyUsage 扩展域中 KeyPurposeID 的 OID 定义如下,该域的使用方式见 GB/T 20518—2018 中 5.2.4.2.5。

```
id-kp-timeStamping OBJECT IDENTIFIER ::= {  
    iso(1)  
    identified-organization(3) dod(6)  
    internet(1) security(5) mechanisms(5) pkix(7)  
    kp (3) timestamping (8)  
}
```

参 考 文 献

[1] GB/T 15851(所有部分) 信息技术 安全技术 带消息恢复的数字签名方案


[2] GB/T 17902(所有部分) 信息技术 安全技术 带附录的数字签名

[3] GB/T 25069—2022 信息安全技术 术语

[4] GB/T 29842—2013 卫星导航定位系统的时间系统

[5] GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

[6] GM/Z 0001—2013 密码术语

[7] GM/T 0081 SM9 密码算法加密签名消息语法规范 

[8] JJF 1180—2007 时间频率计量名词术语及定义

[9] ISO/IEC 18014-1:2008 Information technology—Security techniques—Time-stamping services—Part 1: Framework
