ICS 35.040

CCS

CMA

中 国 计 量 协 会 团 体 标 准

T/CMA ZK 159—2024

计量数据及计量证书报告的时间戳规范

The Specification oftime stamp for metrology data and metrology certification or reports

2024－XX－XX 发布

2024－XX－XX 实施

中 国 计 量 协 会发 布

目录

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。

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。

本文件由中国计量协会提出。

本文件由中国计量协会智库工作委员会归口。

本文件起草单位：

本文件主要起草人：

计量数据及计量证书报告的时间戳规范

1.范围

本文件规定了计量数据及计量证书报告的时间戳需要满足的技术要求与质量测评方法,以实现可信时间戳。

本文件适用于计量数据及计量证书报告的时间戳的生成、使用和质量测评，其他领域或对象的时间戳的技术要求可以参照本标准。

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 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 35276 信息安全技术 SM2密码算法使用规范

JJF1001通用计量术语及定义

JJF1033计量标准考核规范

JJF1069法定计量机构考核规范

3.术语和定义

GB/T 20520界定的以及下列术语和定义适用于本文件。

3.1

可信时间戳 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、签名可信时间等信息。TSA 对此对象进行数字签名产生的时间戳,以证明原始文件在签名时间之前已经存在。

3.2

可信时间 Trustable time

经计量溯源具有一定不确定度水平的时间。

3.3

可信度 Trustable level

对象所具有的必要的信任。

4 格式要求

4.1 时间戳

规定时间戳的格式，包括包含哪些字段，每个字段的含义、属性、长度等。对一个完整的时间戳，其应包含如下信息：

a） 可信时间信息，可信时间的最初源头应来源于国家权威时间部门（如国家授时中心），或者使用国家权威时间部门认可的硬件和方法获得的时间。

b） 在每个新生成的时间戳中都要包含一个一次性随机整数，以保证在没有可靠本地时钟的情况下校验相应信息的合法性并防止重放攻击。

c） 当从一个请求者处收到一个合法请求时，应尽可能地根据这个请求内容生成一个时间戳。

d） 只在数据散列（Hash）值上盖时间戳，散列函数拥有一个唯一的对象标识符（OID）。

e） 时间戳生成时要包含能够体现时间戳生成时的安全策略的唯一标识符。

f） 时间戳申请信息格式可表示如下：

TimeStampReq := SEQUENCE {
version INTEGER(v1(1)),
messageImprint MessageImprint,
reqPolicy TSAPolicyId OPTIONAL,
nonce INTEGER OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
extensions [0] IMPLICIT Extension OPTIONAL
}

其中，version：表示时间戳申请消息格式的版本号。

messageImprint包含需要加盖时间戳的数据的散列值，其类型是 Oetet String，长度应是相应散列算法的结果长度。具体格式为：

MessageImprint := SEQUENCE {
hashAlgorithm hashedMessageAlgorithmIdentifier,
OCTET STRING
}

hashAlgorithm：表示的散列算法应该是一个已知的散列算法（一个单向函数），TSA 会检查其是否符合国家密码管理部门的相关规定。若不认识或不符合规定，将拒绝提供时间服务并在返回消息中设置 “bad_ald” 的 pkiStatusInfo 结构。

reqPolicy：OPTIONAL（可选），如果用户需要指明时间戳应该在什么样的安全策略下生成，可通过该字段说明需要的安全策略。

nonce：INTEGER 类型，OPTIONAL（可选）。在没有可靠的本地时钟的情况下，用于检验响应消息的合法性并防止重放攻击。它是一个很大的随机数，且以很高的概率不被重复（例如一个 64 比特的整数）。若请求消息中有该字段，响应消息中应包含相同的值，否则响应消息应被拒绝接受。

certReq：BOOLEAN 类型，DEFAULT FALSE（默认值为假）。如果该字段为 true，则 TSA 应在其响应消息中给出它的公钥证书，该证书由响应消息中 SigningCertificate 属性的 ESSCertID 指出，证书本身则存放在响应消息中 SighedData 结构的 Certificates。若请求消息中未给出或设为 false，则响应消息中不必给出上述证书。

Extensions：IMPLICIT Extension 类型，OPTIONAL（可选），是未来给申请消息添加额外信息的一种方法，扩展在 GB/T 20518 - 2006 中定义。对于一个扩展，无论是否是关键扩展，只要在请求消息中出现且无法被 TSA 识别，TSA 应不生成时间戳并返回一个失败信息（unaceptedExtension）。

g）时间戳服务响应消息可采用如下格式：

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

其中，status：PKIStatusInfo 类型，具体定义为：

PKIStatusinfo ::= SEQUENCE {
status PKIStatus,
statusString PKIFreeText OPTIONAL,
faillnfo PKIFailureInfo OPTIONAL
}

status：PKIStatus 的取值决定了响应消息的类型，其定义为：

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

如果 PKIStatusinfo 中的 status 值为 0（granted）或者 1（grantedWithMods）时，响应消息中的 TimeStampToken 就应出现，否则 TimeStampToken 就不能出现。status 不能有除 PKTStatus 外的其他值，若请求方收到不认识的值，查看时间戳时应报告错误。

statusString：OPTIONAL（可选），如果申请失败，用该字段给出一个说明失败原因的字符串。

faillnfo：OPTIONAL（可选），也用于说明时间戳请求被拒绝的具体原因，其取值为：

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
}

faillnfo 不能有除 PKIFailureInfo 外的其他值，若请求方收到不认识的值，查看时间戳时应报告错误。

timeStampToken：TimeStampToken 类型，OPTIONIONAL（可选）。当 status 值为 0 或 1 时出现，实际上它应该是一个 Contentinfo 结构，该结构在 RFC2630 中定义，且其 content type 应该是一个 signed data content type。其定义为：

TimeStampToken ::= ContentInfo {

contentType 为 RFC2630 所定义的 id - signedData

content 为 RFC2630 定义的 SignedData

}

在 SignedData 结构中，EncapsledConetno 类中的域有如下含义：

cContentType：是一个对象标识符唯一指定内容的类型，对于时间戳，定义为：

id_ct - TSTInfo OBJECT IDENTIFIER := {iso (1) member - body (2) us (840) rsadsi (113549) pkcs (1) pkcs - 9 (9) smime (16) ct (1) 4}

eContent：就是时间戳内容本身，是一个 octet sting，内容应该是下面说明的 TSTnfo 的 DER 编码。关于 TSTInfo 的具体定义如下：

TSTInfo := SEQUENCE {

version INTEGER (v1 (1)),

policy TSAPolicyId,

messageImprint MessageImprint,

serialNumber INTEGER,

genTime Generalized Time,

accuracy Accuracy OPTIONAL,

ordering BOOLEAN DEFAULT FALSE,

nonce INTEGER OPTIONAL,

tsa [0] GeneralName OPTIONAL,

extensions [1] IMPLICIT Extensions OPTIONAL

}

version：说明了时间戳的版本号，依据本标准写成的时间戳版本号为 1。

policy：应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 TimeStampReg 中，这里应有相同的值，否则应返回错误（unacceptedPolicy），该策略可以包含如时间戳在什么条件下使用、时间戳日志的有效性等信息（但不全面）。

messageImprint：应同 TimeStampReg 中类似的域有相同的值，前提是散列值的长度与 hashAlgorithm 标记的算法预期的长度相同。

serialNumber：是 TSA 分配给每个时间戳的一个整数，对一个给定的 TSA 发出的每一个时间戳它都应是唯一的（即 TSA 的名字和序列号可以确定一个时间戳标志），即使经历服务中断后该特性也应保留。

genTime：是 TSA 创建时间戳的时间，用 UT 时间表示，格式应遵守 8.3 的规定。

accuracy：表示时间可能出现的最大误差，genTime 加上 accuracy 的值可求得 TSA 创建这个时间戳的时间上限，减去 accuracy 的值就是时间下限，其定义为：

Accuracy := SEQUENCE {

seconds INTEGER OPTIONAL, -- s

millis INTEGER (1..999) OPTIONAL, -- ms

micros [1] INTEGER (1..99) OPTIONAL -- us

}

如果 seconds、milis 或者 micros 没出现，其值应被赋为 0。当 accuracy 可选项不出现时，精确度可从别的途径（如 TSAPolicyld）得到。

ordering：表示时间排序条件。若不出现或被置 false，genTime 只表示 TSA 创建时间戳的时间，此时只有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 或不同 TSA 签发的时间戳标志才有可能排序；若出现并被置为 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。

nonce：若在 TimeStampReq 中出现，在这里也应出现且值等于 TimeStampReq 中的值。

tsa：目的是为鉴别 TSA 的名字提供一个线索，若出现应与验证时间戳的证书里的 subjet naes 中的一个相同。

extensions：为将来增加额外信息而采用的一种通常做法，特殊扩展类型可由组织或团体自行定义并声明注册。

4.2 嵌入时间戳的对象

嵌入时间戳的对象主要为计量数据及计量证书、报告。

a）规定嵌入时间戳的计量数据所应满足的格式和特征。

可嵌入时间戳的计量数据应包括检校过程中获取的数据、计算过程、附加信息（如图谱等）和结论等内容。数据内容可参考表1。

表1 计量数据类型及格式

序号	数据类型	数据格式
1	计量参数	文本
2	样品特性	文本
3	技术要求	文本
4	检测数据	文本
5	示值误差	文本
6	不确定度	文本
7	单项判定	文本
8	附加说明	文本

b）规定嵌入时间戳的计量证书、报告所应满足的格式和特征。

可嵌入时间戳的计量证书、报告应包括证书报告信息数据项应包含委托方信息、样品信息、检测任务试验数据信息、原始记录信息等必要的数据项，同时还包括证书编号、证书类型、CNAS资质等其他证书报告信息。

5 技术要求

5.1 时间戳的权限

规定时间戳的溯源关系、权属、签发等权限。

时间戳由时间戳签发机构（TSA）生成并签发，可以通过不同的方式接收时间戳申请和颁发时间戳，包括通过电子邮件申请、通过文件传输申请、通过网络请求（HTTP）申请等。

时间戳所用可信时间信息可以使用以下的一种或多种方法获得：

a)使用某种无线接收装置，通过无线手段获得国家权威时间部门的时间发布，如长波信号、卫星信号等。

b）使用某种时间同步协议从一个指定网络地址获得时间。该网络地址发布的时间和使用的时间同步协议都应是可信的，且通过了国家权威时间部门认可。

c）使用某种通过国家权威时间部门认证的硬件获得时间，如使用原子钟等。

考虑到任何一种方法都可能产生误差，时间戳生成系统可以使用多种方法产生可信时间，以保证时间的精确度。通过多种方法产生最终可信时间应该是产生的多个可信时间的折衷。TSA应该给出一个可靠方案，该方案要考虑每种方法的可能误差和可信程度，对它们的结果做出一个加权平均，获得最终结果。

5.2 时间戳的生成

TSA收到4.1中格式的时间戳申请信息，经审核符合要求，可向用户反馈4.1中格式的时间戳响应信息，响应信息中包含相应时间戳信息。

5.3 时间戳的申请与签发

规定时间戳的申请、签发的权限。

时间戳的申请和颁发过程应该包括如下流程：

a）用户提交申请请求：用户通过上述任一种申请方式，向 TSA 提交申请请求，请求消息格式应符合第 8 章规定。

b）TSA 检查请求合法性：TSA 的签名系统接收到申请请求后，根据第 8 章对时间戳格式的说明，检查请求消息的合法性。

c)处理不合法或异常请求:如果请求消息不合法或者由于内部原因 TSA 无法颁发时间戳,TSA 应产生时间戳的失败响应，并详细填写申请被拒绝的原因。

如果请求消息合法且系统正常运转，进入下一步。

d）TSA 生成并签名时间戳：TSA 的签名系统根据第 8 章说明的时间戳格式，填写正常的时间并签名。

e）存储时间戳：TSA 签名系统通过可信通道把新生成的时间戳发送给时间数据库，由时间数据库将其归档保存。对于申请被拒绝产生的时间戳失败响应，由 TSA 策略决定是否保存。

f）TSA 发送时间戳给用户：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。

g）用户验证时间戳：用户收到时间戳后，使用 TSA 的证书验证时间戳的合法性，并检查时间戳内容是否有错误。如果时间戳不合法或有错误，用户立即向 TSA 管理者报告异常情况，TSA 应提供用户反馈渠道。如果时间戳正常，用户自行保存以备后用。

h）管理员处理异常报告（如有）：如果管理员收到用户的异常报告，应立即检查审计日志和时间戳数据库，找出错误原因所在，TSA 应准备完备的处理预案。

5.4 时间戳的使用

a）时间戳使用所需具备的条件

1）可信时间源

TSA 应拥有可信时间源，其可以是国家权威时间部门发布的时间，或者是用国家权威时间部门认可的硬件和方法获得的时间。TSA 应估算从可信时间源到 TSA 的时间传递过程中的误差，并公布最大可能误差作为可信程度标志。

2）符合格式要求的申请消息

申请消息应按照4.1中规定格式(TimeStampReq)构建，包含版本号、数据散列值(Messagelmprint，散列算法需符合规定）等字段。

3）支持的申请和颁发方式

TSA 应至少支持电子邮件申请、文件传输申请、HTTP 申请这三种方式中的一种，以接收时间戳申请和颁发时间戳。

b）时间戳使用的方法

1）可信时间获取方法

可通过多种方式获取可信时间，如使用无线接收装置接收国家权威时间部门的时间发布（如长波、卫星信号）；利用国家权威时间部门认可的时间同步协议从指定网络地址获取时间；使用国家权威时间部门认证的硬件（如原子钟）获取时间等。为保证时间精确度，可综合使用多种方法，并通过加权平均等可靠方案得出最终可信时间。

2）时间同步方法

TSA 系统各部件根据可信时间同步自身时间，获得可信时间后，TSA 应迅速调整所有部件时间（尤其是签名系统)，保证过程快速且不被打断；定期从可信时间源获取可信时间检查自身时间；在启动 TSA 系统时，可信时间源先启动，且在开始工作前先进行一段时间的时间同步。若同步过程中获取可信时间失败或发现时间信息被篡改，TSA 系统应停止接受时间戳申请和同步，并向管理者发出警报并写入审计日志。

3）申请消息构建方法

按照 TimeStampReq 格式构建申请消息，明确各字段含义和取值规则。如正确设置版本号，准确计算并填充数据散列值（使用符合规定的散列算法），根据需要设置安全策略、随机数、证书请求标识和扩展信息等。

（4）响应消息处理方法

用户收到 TSA 的响应消息后，根据消息中的 status 字段判断申请结果。

c）时间戳使用的流程

1）申请流程

用户选择支持的申请方式（电子邮件、文件传输、 HTTP 申请），按照格式要求构建并提交时间戳申请消息，其中包含待时间戳数据的散列值等必要信息。

2）处理流程

TSA 的签名系统收到申请后，检查请求消息合法性。若合法且系统正常，根据可信时间源生成时间戳，签名后发送给时间数据库归档保存，并通过相应方式将时间戳返回给用户；若不合法或无法颁发，生成包含拒绝原因的失败响应返回给用户。

3）验证流程

用户收到时间戳后,先使用 TSA 证书验证时间戳的合法性,再检查时间戳内容(如对比散列值等)。若合法无误，自行保存以备后续使用；若发现异常，向 TSA 管理者报告，管理员检查审计日志和时间戳数据库查找原因。

d）时间戳使用的规章制度

1）安全相关规章制度

物理安全：时间戳系统的物理安全应遵循 GB/T20271 - 2006 中 4.1 的要求，保障环境、设备和记录介质安全。

2）软件安全

运行环境：TSA 部件运行的计算机环境安全等级应达到或高于 GB17859 - 1999 中规定的第二级“系统审计保护级”，具备完善的反毒、防火墙解决方案，不运行无关程序和服务，严格控制操作人员和访问口令密码。

可信时间源：时间源应为国家标准时间，获取过程保证时间信息完整性，防止篡改，接收软件检查时间连续性和有效性，发现异常向管理者报警。

签名系统：对密钥的使用和访问严格遵照国家密码管理局规范，具备完整审计系统，符合相关审计要求。

时间戳数据库：安全等级应达到或高于 GB/T 20273－2006 中规定的第二级 “系统审计保护级”。

审计相关规章制度

审计数据产生：TSA 签名系统应对多种事件（如审计功能启动和结束、安全相关数据输入输出、密钥操作、时间戳申请等）产生审计记录，记录应包含事件日期时间、用户、事件类型、成功与否及附加信息，日志中不得出现明文私钥等安全相关参数，审计功能部件应关联事件与用户身份。

审计查阅：审计功能部件应为审计员提供查看日志所有信息的能力，并以适于阅读和解释的方式提供日志信息。

审计事件存储：具备受保护的审计踪迹存储能力（防止非授权修改并检测修改）和防止审计数据丢失能力（审计踪迹存储满时阻止非审计员发起的事件）。

可信的时间：在每条审计记录上加上来源于可信时间源的正确时间。

审计日志签名：审计功能部件应定期让 TSA 给审计日志加盖时间戳，签名对象为上次签名后新增日志条目和上次时间戳值，时间戳周期可配置，且该事件应写入日志。

3）数据管理规章制度

时间戳保存：

TSA 方保存：时间戳数据库负责保存 TSA 产生的所有时间戳，符合数据库安全要求，可在一定条件下转移数据，保存时间戳入库时间、序列号、完整编码等信息，考虑用户查询和取证需求。

用户方保存：用户收到时间戳后自行保存，自行保证安全性，若保存问题可向 TSA 申请取回。

时间戳备份：管理员定期备份时间戳数据库所有数据，使用符合要求的介质，采用异地备份方式，以方便检索的方式存放，备份数据访问需管理员在场，可选择是否加密或签名（算法需符合规定）。

时间戳检索：TSA 为用户提供检索环境，支持通过时间戳入库时间、序列号、完整编码等信息检索，检索结果可通过多种方式（如申请方式对应的颁发方式、IC 卡、光盘等）发给用户。

时间戳删除和销毁：

删除：因内部错误或外部攻击产生错误时间戳时，TSA 管理员可删除，删除前先备份（与正常备份区分存放），并在公开渠道公布详细信息。

销毁：确定时间戳丧失价值后，TSA 管理员可销毁（从数据库和备份中删除），但需在时间戳生成足够长时间且 TSA 证书失效后进行，保存时间可由 TSA 策略决定并向用户说明。

6 质量测评要求

时间戳的质量测评应满足如下要求：

a）系统中的时间均需经过计量校准，成为可信时间。

b）可信时间的准确性以时间偏差和计量不确定度表示。一般应满足：

平均时间偏差：0.1 ms；

不确定度：1.3ms（k=2）。

7 质量测评方法

时间戳所用时间（含时间戳服务器）的测评按JJF 1206、GB/T 20520相关方法执行。具体的时间戳质量测评方法应包括如下内容：

a）可信时间源检查

确认 TSA 的时间来源是否为国家权威时间部门发布的时间，或者是否使用国家权威时间部门认可的硬件和方法获得时间。例如，查看其是否采用如长波信号、卫星信号接收装置，或者是否通过国家认证的时间同步协议从指定网络地址获取时间，以及是否使用原子钟等硬件获取时间。

评估 TSA 时间精度的可靠性、时间格式与精度验证。

b）系统安全性测评

运行环境检查：验证 TSA 部件运行的计算机环境安全等级是否达到或高于 GB17859 - 1999 中规定的第二级 “系统审计保护级”，查看是否具备完善的反毒、防火墙解决方案，以及是否严格控制了可运行的程序和服务，同时检查操作 TSA 部件计算机的人员和访问口令密码的管理是否严格。

可信时间源完整性验证：考察从可信时间源获取时间的过程中，是否采用了严格措施保证时间信息的完整性,防止被篡改,并且检查用于接收时间的软件是否能有效检查时间的连续性、完整性和真实性。

签名系统安全性审查：确认签名系统对密钥的使用是否严格遵照国家密码管理局有关规范，包括密钥的生成、存储、使用和销毁等环节；检查对签名系统的访问控制是否严格，是否有完善的审计系统记录相关操作，且审计系统是否符合 9.2.5 对审计的要求。

时间戳数据库安全评估：检查时间戳数据库的安全等级是否达到或高于 GB/T 20273 - 2006 中规定的第二级 “系统审计保护级”，确保数据存储的安全性。

c）可追溯性测评

检查时间戳中的序列号（serialNumber）是否对于每个 TSA 发出的时间戳是唯一的，即使经历服务中断后该特性是否仍能保留，并且验证结合 TSA 名称是否能唯一确定一个时间戳标志，方便对时间戳进行准确追溯。同时，检查时间戳中包含的策略、生成时间、扩展信息等相关信息之间是否相互关联且合理，便于在后续使用中准确追溯时间戳生成时的背景和条件。

d）合规性测评

核对时间戳系统的设计、实现和运行是否全面遵循了JJF 1206、GB/T 20520等的相关要求，确保系统在技术架构、安全管理、数据处理等方面符合国家规范。

检查涉及密码算法的部分是否严格按照国家密码管理部门的相关规定执行,所用算法是否为国家批准的相应算法，保证密码算法使用的合规性。

消息格式与流程合规审查：详细审查时间戳申请和响应消息格式是否严格符合文档中的定义，确保信息交互的规范性。按照文档规定的时间戳申请、颁发、管理、验证等流程，检查 TSA 和用户是否严格遵循相应流程，保证整个时间戳服务流程符合行业标准和规范要求。

附录 A
时间戳测评（使用安全性）参考指标

（资料性）

A.1 准确性

A.1.1 可信时间源的精度保障

可信时间源是时间戳准确性的基础，其应来源于国家权威时间部门（如国家授时中心）或使用经认可的硬件和方法获取时间。通过多种获取时间的方法（如无线接收装置、时间同步协议、认证硬件等）并采用加权平均等方案得出最终可信时间，以减少误差，保证时间戳所标记时间的准确性。

TSA 需估算从可信时间源到自身的时间传递误差，并公布最大可能误差，使用户能了解时间戳的时间精度范围。

A.1.2 时间戳内时间表示的规范性

时间戳中使用的时间应为 UTC 时间，精度至少精确到秒，语法结构需严格遵循“YYYYMMDDhhmmss....2” 的格式规定，如 “20031101001326.343522”，确保时间表示的准确性和统一性，避免因时间格式混乱导致的时间解读错误。

A.2 可靠性

A.2.1 系统组件的稳定性与安全性

物理安全：时间戳系统的物理环境（包括设备和记录介质等）需遵循相关安全标准（如 GB/T20271 - 2006 中 4.1 的要求），保障系统运行的稳定性，防止因物理因素（如硬件损坏、环境干扰等）影响时间戳服务的可靠性。

软件安全

运行环境达到一定安全等级（如 GB17859 - 1999 中规定的第二级 “系统审计保护级”），具备完善的反毒、防火墙措施，严格控制运行程序和人员访问，确保软件运行环境稳定可靠，避免外部恶意软件入侵和内部误操作对时间戳系统的影响。

可信时间源的完整性保护机制，包括从获取到传递过程中的严格措施，防止时间信息被篡改，以及接收软件对时间连续性和有效性的检查，保证时间戳基于可靠的时间源生成。

签名系统对密钥的规范使用和严格访问控制，以及完整的审计系统，有助于确保时间戳生成和管理过程的可靠性，防止因密钥管理不善或操作不规范导致时间戳不可信。

时间戳数据库的高安全等级（如 GB/T 20273 - 2006 中规定的第二级 “系统审计保护级”）保障数据存储的可靠性，防止数据丢失、损坏或被非法篡改。

A.2.2 时间同步的稳定性与准确性

TSA 系统各部件需根据可信时间源定期同步自身时间，同步间隔应尽可能短（不超过 30min 且可配置），保证各部件时间与可信时间源的一致性，防止因时间不同步导致时间戳记录的时间不准确或不一致。

在获取可信时间失败或发现时间信息被篡改时，TSA 系统能及时停止服务并报警，避免生成错误的时间戳，体现了系统在异常情况下保障可靠性的能力。

A.3 完整性

A.3.1 数据处理的完整性保障

在时间戳生成过程中，仅对数据的散列值进行处理，且散列函数有唯一的对象标识符（OID），TSA 能检查散列函数标识符并验证散列值长度，确保处理的数据完整性和准确性，防止数据在传输或处理过程中被篡改或损坏而影响时间戳的有效性。

对于输入的散列值数据，除规定的长度检查外不做其他修改，保证数据的原始性和完整性。

A.3.2 时间戳信息的完整性

时间戳中包含必要的信息，如可信时间值、一次性随机整数（nonce 域）、唯一标识符（表明安全策略）、数据散列值等，确保时间戳记录的信息完整，能够全面反映时间戳生成时的相关情况，便于后续的验证和使用。

审计功能记录时间戳申请和处理过程中的关键信息（如申请请求、时间戳拷贝、失败原因等），保证整个时间戳服务流程的可追溯性和信息完整性，有助于在出现问题时进行排查和分析。

A.4 安全性

A.4.1 密钥管理安全性

TSA 使用专门的密钥对时间戳签名，密钥在相应证书中明确其用途（KeyUsage 的扩展域为 Id－kp－timestamping），且密钥的使用和访问严格遵照国家密码管理局规范，防止密钥泄露和滥用，确保时间戳的签名安全，防止时间戳被伪造或篡改。

A.4.2 防止重放攻击和数据混淆

支持使用 nonce 域（一次性随机数）来检验响应消息的合法性并防止重放攻击，同时建议请求方采用局部时钟和时间窗口等方法防止重放攻击，保障时间戳服务的安全性，防止同一时间戳被重复使用或恶意利用。

对于可能因相同数据和散列算法导致的时间戳混淆问题，TSA 系统和客户端应采取措施进行处理，如对不同实体或多次申请同一对象的情况进行合理管理，确保每个时间戳的独立性和安全性，避免因混淆导致时间戳的可信度降低。

A.5 可追溯性

A.5.1 审计功能的完备性

TSA 签名系统具备完善的审计功能，对多种关键事件（如审计功能操作、安全相关数据处理、密钥操作、时间戳申请与处理等）产生详细审计记录，记录包括事件的日期时间、用户、类型、成功与否及相关附加信息，且审计记录与用户身份相关联，实现对时间戳服务全流程的有效追溯，便于在出现问题时定位责任和查找原因。

审计日志的存储受到保护（防止非授权修改和检测修改），且在每条审计记录上加上可信时间源的时间，保证审计记录的真实性和时间顺序的准确性，进一步增强了时间戳服务的可追溯性。

审计日志定期加盖时间戳，签名对象涵盖新增日志条目和上次签名值，且时间戳周期可配置，确保审计日志的完整性和连续性，为长时间的追溯提供可靠依据。

A.5.2 时间戳信息的可识别性与关联性

时间戳中的序列号（serialNumber）对于每个 TSA 发出的时间戳是唯一的，即使系统中断后该特性也应保留，结合 TSA 名称，可唯一确定一个时间戳标志，方便对时间戳进行识别和追溯。

时间戳中包含的相关信息（如策略、生成时间、扩展信息等）之间相互关联，形成一个完整的信息集合，便于在后续验证和使用过程中，根据这些信息准确追溯时间戳生成时的背景和条件，确保时间戳的有效性和可信度。

A.6 合规性

A.6.1 信息加密合规性

时间戳信息加密涉及密码算法相关内容，需使用经批准的算法，保障时间戳在密码学层面的安全性和合规性。

A.6.2 消息格式和处理流程的规范性

时间戳申请和响应消息格式（如 TimeStampReq 和 TimeStampResp）有明确的定义和规范，包括各字段的含义、类型、取值范围等，TSA 和用户需严格按照格式进行消息的构建和处理，保证信息交互的准确性和规范性，有助于提高时间戳服务的质量和互操作性。

时间戳的申请、颁发、管理、验证等流程均有详细规定，如申请方式、处理步骤、数据保存与检索、异常处理等，各环节需遵循相应流程，确保时间戳服务的有序开展，符合行业规范和标准，从而保障时间戳的质量。

A.7 可用性

A.7.1 申请和颁发方式的多样性与便利性

TSA 支持多种时间戳申请和颁发方式（如电子邮件、文件传输、套接字、HTTP 申请等），用户可根据自身需求和实际情况选择合适的方式，方便快捷地获取时间戳服务，提高时间戳的可用性。

对于时间戳的检索，TSA 提供多种检索途径（如根据入库时间、序列号、完整编码等），并可通过多种方式（如申请方式对应的颁发方式、IC 卡、光盘等）将检索结果提供给用户，方便用户获取所需时间戳，增强了时间戳服务的可用性。

A.7.2 系统的稳定性与容错性

TSA 系统各部件在运行过程中遵循严格的安全和同步要求，保证系统的稳定性，减少因系统故障导致时间戳服务中断的可能性。同时，在出现内部错误或外部攻击等异常情况时，系统具备相应的处理机制（如删除错误时间戳、备份数据、报警等），提高系统的容错能力，确保时间戳服务在一定程度上的持续可用性。

对于用户在使用时间戳过程中可能遇到的问题（如时间戳验证不合法或有错误等），TSA 提供用户反馈渠道，并有相应的管理员处理预案，保障用户能够及时解决问题，进一步提高时间戳服务的可用性和用户体验。