网证通

时间戳机构策略声明

V1.1 版

www.cnca.net

广东省电子商务认证有限公司

Guangdong Electronic Certification Authority

修 订 历 史

版本	修订日期	修订说明
V1.0	2019 年 5 月 29 日	为提供时间戳服务编写首个版本。
V1.1	2020 年 1 月 10 日	新增支持国密算法的说明。

目录

介绍

目前，在电子政务和电子商务中，为了解决保密性、完整性、防抵赖等信息安全问题，使用了数字证书技术。在信息交换的过程中，通过数字签名能够保证内容完整性和签发人的抗抵赖性，但仍无法确认行为发生的真实时间、数据生成、发生或接收的真实时间。数字时间戳服务作为解决该问题的有效手段，可以保证数据在某一时间（之前）的存在性，同时为数字签名服务提供了可供验证的时间凭证。

广东省电子商务认证有限公司（以下简称“NETCA [1]”）是依据《中华人民共和国电子签名法》及《电子认证服务管理办法》，首批通过信息产业部审批成立的第三方电子认证服务机构(《电子认证服务许可证》编号 :ECP44010615006）。

NETCA 数字时间戳遵循 RFC3161 时间戳协议。

NETCA 数字时间戳系统的密码模块符合国家规定的标准要求。

1.概述

本文档定义了 NETCA 作为时间戳机构（TSA）对时间戳服务进行操作和管理的策略要求，以便订户或者依赖方可以通过本文档判断 NETCA 所提供的时间戳服务是否可信。

NETCA 时间戳的时间与协调世界时同步，并且所颁发的时间戳带有 NETCA 的数字签名。

2. 参考规范

[1] RFC 3628 Policy Requirements for Time-Stamping Authorities(TSAs)
[2] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol(TSP)
[3] 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
[4] GB/T 20520-2006 信息安全技术 公钥基础设施时间戳规范

[1] NETCA 在表示机构时为“广东省电子商务认证有限公司”简称，在表示产品和服务时为品牌名称。“网证通”与“NETCA”具有相同的含义。

[5] GM/T 0033-2014 时间戳接口规范

3. 定义和缩写

3.1. 定义

1. 时间戳

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，以证明原始文件在签名时间之前已经存在。

2. 可信时间

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. 时间戳机构

用来产生和管理时间戳的权威机构。

4. 时间戳服务

时间戳机构向订户提供的颁发时间戳的服务。

5. TSA 系统

颁发和管理时间戳的管理系统。

6. 订户

需要由时间戳机构提供时间戳服务的实体。

7. 依赖方

时间戳接收方。

8. 时间戳策略

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。

9. TSA 披露声明

需要向订户和依赖方特别强调或披露的关于TSA策略和实践的一系列陈述。

10. TSA 实践声明

TSA 颁发时间戳的做法声明。

11. 时间戳签发单元

调用时间戳机构私钥对包括原始文件的唯一性属性、签名参数、签名时间等信息进行数字签名的软硬件集合。

12. 协调世界时

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。

3.2. 缩写

1. TSA

Time Stamp Authority，时间戳机构。

2. TSU

Time Stamp Unit，时间戳签发单元。

3. UTC

Coordinated Universal Time，协调世界时。

4. CA

Certificate Authority，证书颁发机构。

5. ETSI

European Telecommunications Standards Institute，欧洲电信标准协会。

4. 一般概念

4.1. 时间戳服务

为了对要求进行分类，本文档把 NETCA 所提供的时间戳服务分为以下组成部分：

- 生成服务：此组件负责生成时间戳。
- 管理服务：此组件负责监视和控制时间戳服务的操作，以确保提供的服务符合 NETCA 规定。此组件还负责生成服务的启动和停止。此组件确保时间戳的时钟与 UTC 同步。

这种服务细分仅用于澄清本文档中规定的要求，并不对 NETCA 服务实现的细分方式进行限制。

4.2. 时间戳机构

时间戳机构 NETCA 对本文档章节 4.1 提供的时间戳服务负有全面责任。

NETCA 的密钥用于签署时间戳证书，并在时间戳中被标识为颁发者。

4.3. 订户

订户可以是包括若干最终用户的组织，亦可以是个人最终用户。

当订户是组织时，适用于该组织的义务也必须适用于最终用户。无论如何，如果最终用户的义务没有得到正确履行，组织将承担责任。因此组织应该恰当地告知其最终用户。

当订户是个人最终用户时，如未正确履行其义务将直接承担责任。

4.4. 时间戳策略和时间戳实践声明

4.4.1. 目的

本文档有版权保护，对公众公开，但不得随意分发或复制。

本文档有 3 个用途：

1) 策略：向公众显示 NETCA 遵循什么准则；
2) 实践：向公众显示 NETCA 如何遵循这些准则；
3) 披露：向公众提供关于时间戳服务的策略和实践的一系列声明。

4.4.2. 声明程度

本文档会以某种恰当的方式向公众传达 NETCA 作为时间戳机构要遵循的内容，但不会列出 NETCA 所遵循的所有政策、标准、流程、实践等。

5. 时间戳策略

5.1. 概述

时间戳策略表示 NETCA 在颁发和管理时间戳时所遵守的一系列规则。

NETCA 时间戳的精度为秒。

每个时间戳都包含对应的 NETCA 策略标识符（请参考本文档章节 5.2）。

5.2. 策略标识符

以下策略标识符 OID 会被包含在 NETCA 时间戳的时间戳策略属性值中。生成的时间戳符合 RFC3161 要求。

序号	策略 OID	名称
1	1.3.6.1.4.1.18760.1.8.3	网证通时间戳机构策略声明

本策略和披露声明可从 NETCA 网站（www.cnca.net）中下载查阅。

5.3. 用户群体和适用性

时间戳用于证明某些数据（例如合同、研究数据、医疗记录、数字签名……）在某个时间点之前已经存在。因为时间戳时间可以被系统精确显示，因此通常被用于支持法庭证据。NETCA 的时间戳策略还可以满足电子签名对时间戳的要求，以确保电子签名的长期有效性。

此策略和 NETCA 时间戳服务可用于公共组织的时间戳服务。

5.4. 一致性

NETCA 颁布的时间戳包括本文档章节 5.2 中描述的策略标识符。

NETCA 确保所提供的服务符合本文档章节 6.1 所规定的要求，亦确保其管理机制的可靠性符合本文档章节 7 所规定的要求。

6. 义务和责任

6.1. TSA 义务

6.1.1. 概述

NETCA 确保所选的时间戳策略完全符合本文档章节 7 所描述的所有要求。

NETCA 确保时间戳运行程序完全符合本文档所描述的内容。

NETCA 确保提供的所有时间戳服务完全符合本文档要求。

6.1.2. TSA 对订户的义务

NETCA 保证时间戳服务的可用性和精确性符合本文档要求。

NETCA 保证时间戳服务可被正常访问，除了系统维护的计划性任务或者 NETCA 不可控的其他因素（如基于 Internet 访问的依赖性等）之外。

NETCA 保证所颁发的时间戳符合通用标准：RFC3161、X.509。

NETCA 保证时间戳操作符合本文档所描述的策略和实践声明。

6.2. 订户义务

订户需要对数字签名、证书和计算机技术知识有足够的了解，以便选择并恰当使用软件验证数字签名。

订户有责任根据订户事项、当地法律和习俗来确认当地法院是否承认数字时间戳的真实性和可受理性。

NETCA 强烈要求订户一旦收到时间戳后马上验证其数字签名，验证方法请查阅 RFC3161 章节 2.2 ,验证内容包括各种数据字段和数字签名的有效性 ,如：

- 验证带有时间戳的内容对应得上请求加盖时间戳的内容。
- 验证其包含正确的 TSA 策略标识符。
- 验证其相关的策略字段能够被应用接受。
- 考虑协议或其它地方规定的任何其它预防措施。

6.3. 依赖方义务

依赖方除了承担本文档章节 6.2 的所有订户义务之外，还需要：

- 验证时间戳证书未被注销。如果时间戳证书被注销，则在注销时刻之后的所有时间戳均无效，具体情况可关注 NETCA 网站相关内容。
- 考虑时间戳策略提出的任何时间戳使用限制。
- 验证时间戳使用的哈希函数仍然安全，如有必要则进行更新。
- 确保 TSA 密钥的算法仍然被认为是安全的。

6.4. 责任

6.4.1. 偿付责任及其限制

6.4.1.1. NETCA 的赔偿责任

若 NETCA 违反本策略声明，导致订户或依赖方遭受损失的，对于一个时间戳的所有当事人（包括但不限于订户、依赖方）的合计赔偿责任，不超过该时间戳的最高赔偿限额。NETCA 声明的一个时间戳对所有时间戳相关受损方法律赔偿责任之最高限额合计为该时间戳相应服务费用的 10 倍。

6.4.1.2. 订户和依赖方的赔偿责任

订户和依赖方在使用和信赖时间戳时，如有任何行为或疏忽导致 NETCA 产生损失，则订户或依赖方应承担赔偿责任。

1. 订户的赔偿责任情况

- 订户申请时间戳时，因故意、过失提供非法时间戳请求，造成 NETCA 或者其他方遭受损失的。
- 订户在收到 NETCA 返回的时间戳后没有按照本文档章节 6.2 所要求的方法进行对时间戳的验证或明知时间戳验证失败依旧使用而没有告知 NETCA，造成 NETCA 或其他方遭受损害的。

2. 依赖方的赔偿责任情况

- 未按本策略声明或其他相关协议承担依赖方义务，而造成 NETCA 或其他方遭受损失的。

7. TSA 实践

NETCA 已采取至少满足以下声明的控制措施（本文档章节 7）。

对于超过 NETCA 与订户协议所约定的服务水平的请求，NETCA 保留拒绝为其颁发时间戳的权利。

7.1. 实践和披露声明

7.1.1. TSA 实践声明

7.1.1.1. 概述

NETCA 创建并实施一系列策略、标准和管理办法，用于管理与时间戳服务相关的所有人员及事项。NETCA 章节 7.1.1 的实践声明和章节 7.1.2 的披露声明都会随本文档发布在官网上，以便订户和依赖方随时查阅。

7.1.1.2. 策略管理

网证通时间戳机构策略声明由 NETCA 认证（安全）策略管理委员会负责起草、注册、维护和更新，版权由 NETCA 完全拥有。

时间戳策略声明起草后，交由 NETCA 法律顾问审核通过，认证（安全）策略管理委员会通过后形成决议，在 NETCA 网站（www.cnca.net）发布后，该策略声明正式生效。

在 NETCA 时间戳相关政策和操作规范做出任何变动之前，NETCA 认证（安全）策略管理委员会将对提供的变动建议进行研究，做出变更决定，并根据决策结论按需要遵循上述流程更新并发布 NETCA 时间戳策略声明。

NETCA 将对 NETCA 时间戳策略声明进行严格的版本控制，由 NETCA 认证（安全）策略管理委员会制定专人负责版本控制及发布。

所有时间戳策略声明相关公告和通知需获得认证（安全）策略管理委员会批准，方能在 NETCA 网站（www.cnca.net）上公布。

7.1.1.3. 风险评估

NETCA 定期进行风险评估和/或业务影响分析，重复评估安全控制和操作程序的充分性以消除或减少对 NETCA 运营资产的威胁。这些风险评估包括重新审视所有策略和标准，以确保它们是最新的并符合相应的行业法规。

NETCA 向公众和任何审计组织提供适当的策略和实践声明，证明符合相关标准如 RFC 3628 的要求。

7.1.2. TSA 披露声明

7.1.2.1. TSA 联系信息

电话：(+8620)38861746
电子邮件：TSA@cnca.net
地址：广东省广州市越秀区建设五马路 1 号德安大厦 3 楼

7.1.2.2. 时间戳类型和用法

NETCA 在策略标识符 1.3.6.1.4.1.18760.1.8.3 下提供 RSA 2048 和 SM2 算法时间戳。NETCA 接受以下哈希算法：

SHA-1
SHA-256
SHA-384
SHA-512
SM3

NETCA 时间戳使用 RSA 2048 或 SM2 密钥签名，每个时间戳包含时间戳证书公钥，订户可以根据时间戳证书公钥验证时间戳，时间戳证书可从 NETCA 网站或 LDAP 查询下载。

NETCA 时间戳的签名有效期依赖于签名算法的安全性，订户可关注相关标准，自行评估。

7.1.2.3. 依赖限制

NETCA 数字时间戳提供的时间精度为秒。
TSA 事件日志将在 NETCA 存储库保存 10 年。
NETCA 签发的时间戳由用户自行保管，NETCA 不存储、备份时间戳。

7.1.2.4. 订户的义务

请参阅本文档的章节 6.2。

7.1.2.5. 依赖方的义务

请参阅本文档的章节 6.3。

7.1.2.6. 有限保证和免责声明

网证通仅提供与时间戳相关的数字证书、数字签名、时间戳的技术验证等调查及取证的服务，对于其他各方之间的纠纷以及提交诉讼的证据等，网证通不作任何保证。

如因网证通原因致使订户就时间戳服务遭受直接损失的，网证通将对遭受直接损失的各方承担赔偿责任，但是该赔偿责任合计最高不超过时间戳相应服务费用的 10 倍。

属于以下情形之一，应当免除网证通的责任：

1) 因网络原因致使时间戳出现延迟或其他异常的；
2) 网证通遭受黑客或病毒攻击，导致时间戳出现延迟或其他异常的，但是网证通保证对时间戳服务系统及密钥进行符合《网证通时间戳机构策略声明》的保护；
3) 因意外事件或不可抗力造成的服务延迟、错误、暂停或终止的。不可抗力包括但不限于自然灾害、政府行为、战争、罢工等不可预见、不可避免、无法克服的客观情况。

7.1.2.7. 适用协议和实践声明

相关内容可在 NETCA 网站（www.cnca.net）找到。

适用的协议包括 TSA 策略声明和实践声明中描述的订户义务和依赖方义务，亦包括本文档章节 7.1.2.6 的有限保证及免责声明。

7.1.2.8. 隐私保密策略

请参阅本文档的章节 7.4.9。

7.1.2.9. 偿付责任及其限制

请参阅本文档的章节 6.4.1。

7.1.2.10. 适用法律及争议处理

本协议的解释适用中华人民共和国法律。若订户与网证通之间发生任何纠纷或争议，应先通过友好协商解决，协商不成的，任何一方可提请广州仲裁委员会按照该会仲裁规则在广州进行仲裁。仲裁裁决是终局的，对双方均具有约束力。

7.2. 密钥生命周期管理

7.2.1. TSA 密钥生成

NETCA TSA 密钥对由国家密码主管部门检测达到安全要求的密码设备或模块生成。密钥算法和长度符合时间戳标准。

7.2.2. TSA 私钥分发

NETCA TSA 私钥必须在经过认证的加密模块中创建（参阅本文档章节 7.2.1），NETCA TSA 私钥是在设定的程序下，由可信的授权人员产生，并对每个环节进行记录和签名。

NETCA 不对私钥进行备份，因此没有分发。

7.2.3. TSA 公钥分发

TSA 公钥用于验证当使用时间戳服务时所创建的时间戳的真实性。公钥作为 X.509 证书发布。公钥证书可从 NETCA 网站或 LDAP 查询下载。

7.2.4. 更新 TSA 密钥

TSA 密钥对在硬件设备中更换频率为 1 年，更新 TSA 密钥的同时会销毁先前的时间戳私钥。每次更新 TSA 密钥都会申请签发新的时间戳证书，其有效期为 1 年。

7.2.5. TSA 密钥生命周期结束

NETCA TSA 密钥生命周期结束时，加密模块中的私钥将以不能检索的方式进行销毁。私钥没有备份，也没有导出或分发。

如果签名私钥已过期或已损坏，NETCA 将拒绝颁发时间戳。

7.2.6. 签发时间戳的密码模块的生命周期管理

硬件安全模块的初始化会确保私钥始终在模块中保存，以此达到创建可信时间戳的目的。初始化过程创建了验证数据，便于在未来证明硬件安全模块仍旧处于有效、未被改变状态。硬件安全模块初始化过程可被审计。这些审计记录可用于审计、审查和争议解决。

当时间戳设备废弃使用时，会通过制造商规定的方法来销毁安装的时间戳软件和 TSA 私钥。

7.3. 时间戳

7.3.1. 时间戳的申请与颁发

NETCA 目前只支持 HTTP 的申请方式。

订户向 NETCA 提交符合 RFC3161 标准的申请请求，当 NETCA 接收到请求后，对请求消息的合法性进行检查，无论消息是否合法，都通过与申请请求相同的方式返回响应给订户。

7.3.2. 时间戳的内容格式

NETCA 在收到订户的有效请求后生成时间戳，时间戳的内容格式符合 RFC 3161 要求。简而言之，时间戳就是将用户数据的哈希值与当前时间相结合，然后在此基础上加以数字签名。

NETCA 确保安全发放时间戳并且每个时间戳包含正确的时间。时间戳密钥对专门用于创建时间戳，每个时间戳都包含一个唯一的正整数序列号。

时间戳包含的时间与 UTC 同步，精度为秒。如果 NETCA TSA 由于任何原因无法与 UTC 保持同步，则不会颁发时间戳。

每个时间戳中包含 NETCA 的时间戳策略标识符。若订户的请求不包含策略标识符， NETCA 默认使用 OID 为 1.3.6.1.4.1.18760.1.8.3 的策略响应，除非 NETCA 与订户之间的协议另有规定。

7.3.3. 时间同步

NETCA 使用 GPS 北斗双模时钟系统获取 GPS/北斗卫星时间，时间精度为秒。

在获得可信时间后 ,NETCA 迅速根据可信时间对所有部件的时间进行调整。为了保证各个部件的时间精确性，NETCA 根据可信时间定期检查自身时间，与可信时间源保持时间同步，每次同步的间隔时间不长于 30 分钟。

NETCA 充分考虑闰秒的影响 ,NETCA 会将已知的闰秒清单作为配置参数写入时间处理模块，当遇到闰秒时，系统会自动分析并处理以确保时间正确同步。

7.4. TSA 管理和运营

7.4.1. 安全管理

NETCA 执行一系列的管理措施来满足时间戳服务的维护及安全 ,例如以下：

NETCA 由其认证(安全)策略管理委员会负责制定和实施适当的安全策略，确保其方向符合 NETCA 的主要业务目标。该委员会亦负责管理和发布 NETCA 的所有策略、管理办法和指南，并监控与 NETCA 相关的所有安全事项，以确保时间戳服务不会因安全问题而中断。

NETCA 维护一系列策略、管理办法和指南（包括风险评估、灾难恢复计划等），并根据实际实施情况作出调整。这些策略的目的主要在于计划并记录业务目标，评估潜在威胁，以最大限度地减少预期之内或之外事件的负面影响，同时最大限度地提供可靠的时间戳服务。

7.4.2. 资产分类和管理

NETCA 承诺提供必要的资源，以确保信息和资产得到保护，例如以下：

NETCA 维护资产清单，根据其性质对资产进行分类，并定义和实施适当的控制措施。同时，NETCA 对这些资产进行定期风险分析以确保充分了解当前风险并作出适当的监督。

7.4.3. 人员安全

7.4.3.1. 人员资格要求

NETCA 在录用担任可信角色的人员之前，除需满足一般的技能和经验要求外，必须按 NETCA 可信人员背景调查管理的相关操作指南要求，对录用岗位的可信人员进行对应调查级别的背景调查，符合要求方予录用。可信人员背景调查至少包括以下方面：

- 学历、学位、职称
- 过往的就业情况

对于较高可信等级的调查可能还包括社会关系、奖惩记录、犯罪记录、社会保险记录、交通违章记录、征信记录等。

7.4.3.2. 背景调查程序

拟录用担任信任角色的人员需同意 NETCA 作背景调查。NETCA 采取调阅人事档案、访问过往就读学校和就职单位的人事主管或同事、参阅政府相关部门的个人记录等方式，核实拟录用人所声明和未声明的信息，并作出评估。评估通过后需签署保密协议和就业限制协议，始可录用。

新入职的员工必须经过三个月的观察期，观察期通过后才可独立上岗。

NETCA 不定期进行可信人员背景调查，以便能够持续验证人员的可信程度和工作能力。

7.4.3.3. 培训要求

NETCA 为员工提供必要的培训，帮助员工胜任其目前的工作并为将来的发展做准备。NETCA 根据需要对员工进行职责、岗位、技术、政策、法律和安全等方面的培训。

NETCA 根据各岗位要求对员工进行相应的培训 ,包括但不限于 :企业文化、规章制度、岗位职责等基本培训；《中华人民共和国电子签名法》;《网证通时间戳机构策略声明》；NETCA 的安全原则和机制；NETCA 的系统运行、维护、安全；NETCA 的政策、标准、管理办法；以及岗位技能、行为方式等其他必要的培训。

NETCA 对具有 TSA 管理职责的员工培训以下知识：

- 时间戳技术知识
- 数字签名技术知识
- UTC 校准和同步时钟的机制
- 安全人员负责的安全程序
- 信息安全和风险评估经验

7.4.3.4. 对未授权操作的处理

NETCA对所有涉及到业务操作安全的操作均有记录。记录由NETCA安全审计员审查。员工涉嫌未授权行为、未授予的权力使用和对系统的未授权使用等，一经发现，NETCA将立即中止该员工进入NETCA证书认证体系各系统。当事人的证书和操作权限即时冻结或注销，所做的未授权操作将立即被注销失效。同时根据情节严重程度，对当事人作出相应处罚，包括内部处分、辞退、解雇等，涉及犯罪的将送司法机关处理。

7.4.4. 物理和环境安全

NETCA 采用以下措施来确保物理和环境安全，包括机房建筑物的选址和建设、物理访问、电源和空调、水患防治、火灾预防和保护、入侵侦测报警系统、介质存储、废物处理、异地备份等各方面。

NETCA 机房采用符合国家标准的防水材料建造；机房内部根据业务功能划分不同区域，并相应设置双因素门禁系统和双人双因素控制策略；电源确保不间断供电，空调符合机房温度和湿度的控制要求；设置火灾自动报警系统和灭火系统；部署入侵侦测报警系统；妥善控制和保管存储有敏感信息的各类介质，在它们作废前或保存期满后按照信息不可恢复的原则进行销毁。

7.4.5. 操作管理

7.4.5.1. 可信角色

所有涉及时间戳业务操作和维护管理的人员，可能是 NETCA 雇员或代理人员、承包人员、顾问等，都属于可信人员。这些可信人员担任的角色包括但不限于以下部分：

1. 安全管理人员：负责管理安全实践的全面责任；
2. 系统维护人员：负责 TSA 系统的正常运行；
3. 系统审计人员：查看 TSA 系统的档案和审计日志。

7.4.5.2. 角色要求的人数

NETCA 对于涉及敏感信息的操作任务，要求采取双人控制策略，并为担任该任务角色至少配置 3 人。某些涉及敏感信息的区域的进入也是采取双人控制策略（见本文档章节 6.4.4.2）；核心秘密（如时间戳密钥）分管者和操作的物理访问控制者由不同的人员担任角色。

7.4.5.3. 可信角色的鉴别

所有担任可信角色的人员需持有经授权的智能门禁卡（或智能门禁卡+指纹）进入相应的活动区域，或在有进入该区域权限的可信人员的陪同下进入，并持有经授权的电子密匙和证书进入系统进行相应业务的操作和管理。

7.4.5.4. 职责需分离的角色

NETCA 建立并执行严格的控制流程，根据工作要求和工作安排采取职责分离措施，建立互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。NETCA 进行职责分离的角色，包括但不限于下列人员：

1. 系统维护；
2. 密钥管理；
3. 安全审计。

7.4.6. 可信赖系统部署和维护

7.4.6.1. 系统开发控制

NETCA的TSA系统符合国家的相关标准和规范。

NETCA要求其内部或外包的软件开发项目符合ISO9001、ISO27001等质量要求，并遵守国家的法规和签署的项目保密条款。

7.4.6.2. 系统改进控制

NETCA对TSA系统生命周期内的任何补丁和升级版本进行控制，并只有授权的工程实施人员才能访问；TSA系统的重大升级需由NETCA认证（安全）策略管理委员会批准。

NETCA在安装系统补丁或系统升级之前对代码进行验证，包括测试和版本核对。

7.4.6.3. 安全管理控制

NETCA TSA系统的配置以及任何修改都会记录在案，并制定相关的管理办法和监督机制，包括确定TSA系统的访问角色、制定网络安全策略、制定TSA系统的访问机制、制定TSA系统的审计机制等，来保障TSA系统配置的安全，防止未授权的修改。

7.4.7. TSA 服务主要风险及应对

NETCA 认为主要风险点在于 TSA 私钥泄露和时间戳时间失准。如果发生该类事件，NETCA 将停止颁发时间戳，直到恢复程序完成。

当时间戳私钥被攻破或泄露，NETCA 启动应急事件处理程序，由 NETCA 认证（安全）策略管理委员会和相关的专家进行评估，指定行动计划。NETCA 将执行以下操作：

- 撤销“私钥泄露”密钥对所对应的时间戳证书。
- 在 NETCA 网站或其他通信方式发布关于注销时间戳证书的处理通报。
- 重新生成新的私钥并签发新的时间戳证书。

7.4.8. TSA 服务终止

因各种原因，NETCA 计划暂停或终止 TSA 服务的情况下，NETCA 将按国家相关法律法规的要求进行 TSA 服务终止操作。NETCA 终止 TSA 服务后，有权根据自身情况决定是否告知相关方。

7.4.9. 个人隐私保密

NETCA TSA 不存储、不收集用户的隐私信息，因此不存在隐私保密事项。

7.4.10. 时间戳审计日志程序

7.4.10.1. 记录事件的类型

NETCA TSA日志记录的事件包括但不限于以下内容：

- 涉及TSA密钥发生的事件。包括密钥生成、销毁，密码设备的启用、停用、转移和销毁。
- 涉及TSA证书发生的事件。包括证书的申请、更新、密钥更新、变更、注销。
- 涉及时钟同步的事件。包括同步时钟源，同步时刻，同步失准，重新校准等信息。
- 涉及网络安全的事件。包括防火墙、路由器、入侵检测记录的信息，以及被攻击的相应处理记录。

- 其它安全事件。包括各系统的登录、退出，系统的各种配置及其修改，业务处理的成功或失败，系统部件的安装、升级、维修，人员在各区域的访问记录，敏感信息的取阅。

每个事件的记录至少包括以下信息：

- 发生的日期和事件
- 事件的内容
- 事件相关的实体
- 事件的标识

7.4.10.2. 日志的处理周期

NETCA审计人员每月对日志进行一次审查，识别可疑的事件，核实系统和操作人员是否按规定操作，并记录和报告审查的结果。

7.4.10.3. 审计日志的保存期限

对于纸质日志，现场保存至少1个月，归档保存期限为10年以上，满足本文5.5.2要求的档案保存期限。

对于系统自动记录的日志，分在线保存和离线保存，其中在线保存是把日志留在运行的数据库或文件中保存；离线保存则是把数据库或文件中某段时间的日志以文件转储的方式分开保存。在线保存期限为1年，离线保存的保存期限为10年以上。

7.4.10.4. 审计日志的保护

只有被NETCA授权的人员才能对日志进行查看和处理，NETCA对系统的日志设有访问控制权限。

7.4.10.5. 审计日志的备份

NETCA每月对纸质日志实施归档；对于审计日志，NETCA每天对审计日志进行备份，并且每周对审计日志做一次全备份并异地保存。NETCA采取严格的物理和逻辑访问控制措施，防止所有的审计日志和记录被未经授权的浏览、修改、读取、删除等。

7.4.10.6. 审计日志的采集

NETCA 的审计日志分手工采集和自动采集两种方式。自动采集的主要是电子日志，通过 TSA 系统、网络设备、各计算平台产生并记录；手工采集的主要是纸质日志，通过操作或出入人员的手工记录产生。

7.4.10.7. 对导致事件实体的通告

NETCA将依据法律、法规的监管要求，可能对一些恶意行为，如网络和病毒攻击等，通知相关的主管部门，并且NETCA保留进一步追究责任的权利。

7.4.10.8. 脆弱性评估

审计人员对日志进行日常审计，如发现引起安全事故的事件或可能的隐患，将写入审计报告。NETCA 认证（安全）策略管理委员会指定专业人员对审计报告进行评审，确定需要改进的安全措施。同时，NETCA 每年进行一次信息安全的风险评估。

7.5. 其他声明

NETCA 采取以下措施确保对可靠时间戳服务产生积极影响：

1. NETCA 的政策、标准和管理办法都是非歧视性的。
2. NETCA 向任何同意遵守披露声明中规定的订户义务的客户提供服务。
3. NETCA 遵守国家法律要求。
4. NETCA 采取一系列有效措施来确保其系统能够提供可靠的时间戳服务。
5. NETCA 有足够资金安排以应对万一出现的风险和以及相关责任。
6. NETCA 雇佣具备必要的时间戳相关知识和经验的足够数量的员工。