Amazon Registry Services, Inc.

.TUSHU 区域 DNS 实践声明

第 2 版

目录

1.1 概述 6
1.2 文件名称和标识 6
1.3 团体和适用范围 6
1.3.1 区域经理 6
1.3.2 区域管理员 6
1.3.3 服务器运营商 6
1.3.4 注册中心 6
1.3.5 注册商 7
1.3.6 注册人 7
1.3.7 .TUSHU 区域密钥签名密钥运营商 7
1.3.8 根区域区域签名密钥运营商 7
1.3.9 依赖方 7
1.4 规范管理 7
1.4.1 规范管理机构 7
1.4.2 联系信息 7
1.4.3 规范变更程序 7
2 发布和资源库 8
2.1 DPS 资源库 8
2.2 发布密钥签名密钥 8
2.3 资源库访问权限控制 8
3 运营要求 8
3.1 域名的含义 8
3.2 激活子区域 DNSSEC 8
3.3 识别和认证子区域管理员 8
3.4 注册授权签名者（DS）记录 9
3.5 证明密钥所有权的方法 9
3.6 清除 DS 记录 9
4 设施、管理和运营控制 9
4.1 物理控制 9
4.1.1 现场位置和结构 9
4.1.2 物理访问 9
4.1.3 电源和空调 10
4.1.4 水分接触 10
4.1.5 消防和保护措施 10
4.1.6 介质存储 10
4.1.7 废物处置 10
4.1.8 异地备份 10
4.2 规程控制 10

4.2.1 可信任角色 10
4.2.2 执行各项任务的规定人数 11
4.2.3 识别和认证各个角色 11
4.2.4 要求分工执行的任务 11
4.3 人员控制 11
4.3.1 资质、经验和许可要求 11
4.3.3 培训要求 11
4.3.4 再培训频率和要求 12
4.3.5 岗位轮换频率和顺序 12
4.3.6 未经许可采取行动的处罚 12
4.3.7 承包人员要求 12
4.3.8 向相关人员提供的文件 12
4.4 审计记录规程 12
4.4.1 记录的事件类型 12
4.4.2 处理日志的频率 12
4.4.3 审计日志信息的保留期限 13
4.4.4 保护审计日志 13
4.4.5 审计日志备份规程 13
4.4.6 审计采集系统 13
4.4.7 通知引起事件的对象 13
4.4.8 漏洞评估 13
4.5 攻击和灾难恢复 13
4.5.1 事故和攻击处理规程 13
4.5.2 计算资源、软件和/数据崩溃 13
4.5.3 实体私钥泄密应对规程 14
4.5.4 业务连续性和 IT 灾难恢复能力 14
4.6 实体终止 14
5 技术安全控制 14
5.1 生成和安装密钥对 14
5.1.1 生成密钥对 14
5.1.2 交付公钥 15
5.1.3 生成公钥参数和质量检查 15
5.1.4 密钥用途 15
5.2 私钥保护和密码模块工程控制 15
5.2.1 密码模块标准和控制 15
5.2.2 多人控制私钥 15
5.2.3 私钥托管 15

5.2.4 私钥备份 15
5.2.5 私钥存储在密码模块中 15
5.2.7 密码模块中的私钥转移 15
5.2.8 激活私钥的方法 16
5.2.9 停用私钥的方法 16
5.2.10 销毁私钥的方法 16
5.3 其他密钥对管理事项 16
5.3.1 公钥存档 16
5.3.2 密钥使用期限 16
5.4 激活数据 16
5.4.1 生成和安装激活数据 16
5.4.2 保护激活数据 16
5.5 计算机安全控制 16
6 区域签名 17
6.1 密钥的长度和算法 17
6.2 存在性验证 18
6.3 签名格式 18
6.4 区域签名密钥更新 18
6.5 密钥签名密钥更新 18
6.6 签名有效期和重新签名的频率 18
6.7 区域签名密钥集验证 18
6.8 资源记录验证 18
6.9 资源记录生存时间 18
7 合规审计 18
7.1 实体合规审计的频率 19
8 法律问题 19
8.1 费用 19
8.2 经济责任 19
8.3 商业信息保密 19
8.3.1 机密信息的范围 19
8.3.2 机密信息范围以外的信息 20
8.3.3 保护机密信息的责任 20
8.4 个人信息隐私 20
8.4.1 私人信息 20
8.4.2 非私人信息类型 20
8.4.3 保护私人信息的责任 20
8.4.4 依据司法或行政程序进行披露 20
8.5 责任限制 21
8.6 有效期和终止 21
8.6.1 有效期 21

8.6.2 终止 21
8.6.3 争议解决规定 21
8.6.4 准据法/管辖权 21

1 引言

本文件“关于.TUSHU 区域的 DNSSEC 实践声明”（DPS）阐述了 Amazon Registry Services, Inc. 关于.TUSHU 区域 DNSSEC 运营的政策和实践。

1.1 概述

DPS 旨在提供 Amazon Registry Services, Inc.管理下的.TUSHU 区域 DNSSEC 的相关运营信息。本文件依照 IETF 域名系统运营（DNSOP）工作组提议的 DPS 框架制定而成。

1.2 文件名称和标识

.TUSHU 区域的 DNSSEC 实践声明（.TUSHU DPS）

版本号：第 2 版

可用日期：根区域授权日期

生效日期：根区域授权日期

1.3 团体和适用范围

.TUSHU DNSSEC 服务的利益干系人及其承担的角色和职责如下。

1.3.1 区域经理

.TUSHU 的区域经理是 Amazon Registry Services, Inc.

1.3.2 区域管理员

.TUSHU 的区域管理员是 Neustar。

1.3.3 服务器运营商

Neustar 是唯一的服务器运营商。

1.3.4 注册中心

Amazon Registry Services, Inc.是.TUSHU 域名注册的注册运营商。作为 DNS 服务的一部分，Amazon Registry Services, Inc.向注册商提供 DNSSEC 服务，注册商再将这些服务提供给注册人。注册中心使用 ZSK 和 KSK 组合密钥作为区域签名密钥。KSK 密钥的 DS 记录注册并发布在根区域后，使启用 DNSSEC 的解析器在根与.TUSHU 注册中心之间维护一条信任链。

1.3.5 注册商

注册中心为.TUSHU 域名注册系统注册商提供服务。注册商与注册中心订立了合同业务关系，为注册人提供域名注册和维护服务。注册商提供.TUSHU 区域中的 DS 记录等域名信息。

1.3.6 注册人

注册人是通过.TUSHU 注册商在注册中心注册的.TUSHU 域名的所有人。注册人选择的注册商或 DNS 提供商负责提供注册域名的 DS 记录。向注册中心提交这些记录后，即在注册中心与注册人获得许可的子区域间确立一条信任链。

1.3.7 .TUSHU 区域密钥签名密钥运营商

Neustar 是.TUSHU 区域密钥签名密钥运营商，负责生成.TUSHU 区域的密钥签名密钥（KSK）和使用 KSK 签发.TUSHU 密钥集，同时还负责安全生成和存储私人密钥以及分配公开的 KSK。

1.3.8 根区域区域签名密钥运营商

Neustar 是.TUSHU 区域签名密钥运营商，负责生成.TUSHU 区域的区域签名密钥（ZSK）和使用 ZSK 签发.TUSHU 区域文件。

1.3.9 依赖方

依赖方包括 DNS 解析器，例如解析区域域名的浏览器或主机，DNS 提供商、ISP，以及使用或依赖于.TUSHU DNSSEC 服务使用 DNSSEC 协议安全解析域名的任何用户。

1.4 规范管理

1.4.1 规范管理机构

.TUSHU DPS 的管理员是 Amazon Registry Services, Inc.

1.4.2 联系信息

Neustar 代表 Amazon Registry Services, Inc.：Reg-support@neustar.biz

1.4.3 规范变更程序

DPS 的内容每年审查一次，必要时也可增加审查次数。修订可在现行文件中进行，或者发布新文件。所有修订文件必须发布在以下资源库中。Amazon Registry Services, Inc.保留随时发布修订文件的权利，恕不另行通知。

2 发布和资源库

2.1 DPS 资源库

DPS 发布在 Amazon Registry Services, Inc.网站的 NIC.TUSHU:资源库中。

2.2 发布密钥签名密钥

KSK 发布在根区域中。使用根密钥作为信任锚可获得信任链。

2.3 资源库访问权限控制

DPS 公开发布在 DPS 资源库中，所有人均可访问和查看。如有变更请求，须提交给 Amazon Registry Services, Inc.进行审查。已设置权限控制，防止未经许可变更 DPS。

3 运营要求

3.1 域名的含义

域名可公开注册。在某些情况下，如果注册违法政策规定，注册中心保留删除或拒绝注册的权利。

3.2 激活子区域 DNSSEC

.TUSHU 区域发布子区域的签名 DS 记录后，即在.TUSHU 区域与子区域间确立一条信任链。确立信任链后，子区域 DNSSEC 激活。

3.3 识别和认证子区域管理员

注册中心与子区域管理员之间没有直接关系，因此无法识别和认证子区域管理员。

3.4 注册授权签名者（DS）记录

注册商代表注册人连接注册中心，提供和管理域名注册数据，包括 DS 记录。

3.5 证明密钥所有权的方法

注册中心无法验证子授权区域私钥的所有权。

3.6 清除 DS 记录

注册商可随时请求清除注册商管理下的域名的 DS 记录。注册中心收到注册商的有效请求后，将清除区域中的 DS。

4 设施、管理和运营控制

4.1 物理控制

.TUSHU 注册中心位于数据中心设施中，满足或超出一个任务关键型平台的所有环境规定。

4.1.1 现场位置和结构

.TUSHU 注册中心和 DNSSEC 服务的运营地点位于美国弗吉尼亚州斯特林和北卡罗来纳州夏洛特的多个充分冗余的数据中心。这些设施位置提供不同的网络连接和必要的网络能力，可有效支持注册中心的全面运营，防止遭受自然和人为灾难。两个数据中心的加密密钥存储在 FIPS 140-2 第 3 级硬件安全模块（HSM）中。

4.1.2 物理访问

Neustar 运营高度安全的数据中心，提供最高级别的安全性和服务。对这些设施的物理访问受到严密控制。物理安全机制包括保安、闭路电视监控摄像机和入侵侦测系统。NOC 全天 24 小时监控所有位置的出入情况。

访问 HSM 至少需要获得两把密钥，分别由管理员和安全审计员持有。密钥备份放在 PIN 输入设备（PED）密钥上，锁在 2 小时安全防火柜中。

4.1.3 电源和空调

每个数据中心由多个电源提供运行支持，包括备用发电机和蓄电池电源。每个设施处都安装多个空调装置控制温度和湿度。

4.1.4 水分接触

Amazon Registry Services, Inc.和 Neustar 已采取预防措施尽量避免系统由于接触水分而遭到损害。

4.1.5 消防和保护措施

Amazon Registry Services, Inc.和 Neustar 已采取消防预防措施以及其他防烟防火措施。所有系统都配备了自动灭火系统。

4.1.6 介质存储

Neustar《数据保护政策》规定了介质存储和处理规程。

4.1.7 废物处置

Neustar 信息安全政策和规程中规定了根据信息敏感性适当处置过时资料的方针。规程中规定将过时的纸质信息粉碎后存放在 Neustar 场所中印有特殊标记的处置箱中。电子数据必须彻底删除或清除或者彻底销毁实体介质。不需要的硬盘和备份磁带须消磁。

4.1.8 异地备份

安装和使用备份所有重要系统的备份软件，备份介质定期轮流存放在异地位置。另外，所有重要系统备份须按照 Neustar 备份政策的规定依照确定的流程进行半年一次的备份恢复测试。

4.2 规程控制

4.2.1 可信任角色

Neustar 规定了有限数量的可信任角色负责 DNSSEC 管理和运营。可信任角色包括：

密钥管理人

- 生成密钥和 DS 记录
- 管理密钥滚动更新事件

安全审计员

- 监督安全审计
- 确保遵从规定/规程

DNSSEC 专员

- 参加团体会议和研讨会
- 熟练掌握 DNSSEC 技术
- 充当 Neustar 与外部人员之间的协调员

4.2.2 执行各项任务的规定人数

密钥签发仪式和 HSM 激活至少需要两名密钥管理员和一名安全审计员。

4.2.3 识别和认证各个角色

仅允许授权人员访问.TUSHU DNSSEC 系统所在的数据中心物理地址。仅授权上述角色成员访问系统。

4.2.4 要求分工执行的任务

要求分工执行的任务包括密钥生成、执行和清除。

4.3 人员控制

4.3.1 资质、经验和许可要求

上文第 4.2.1 节所述的 DNSSEC 角色仅可分配给员工。分配每项角色时应单独进行经验和资质评估，但所有角色都必须具备广泛的 DNS 运营和安全技术相关知识。

4.3.2 背景调查程序

背景调查内容包括审查申请人的资质、工作经历、推荐信、教育背景以及与岗位职责相关的其他信息。

4.3.3 培训要求

相关人员将持续接受 DNSSEC 运营和管理培训。培训内容包括但不限于.TUSHU 的具体规定和规程以及相关技术。相关人员将参加 DNSSEC 研讨会和会议。

4.3.4 再培训频率和要求

再培训根据实际情况单独安排。

4.3.5 岗位轮换频率和顺序

不适用本文件。

4.3.6 未经许可采取行动的处罚

不适用本文件。

4.3.7 承包人员要求

不适用本文件。

4.3.8 向相关人员提供的文件

参加 DNSSEC 相关活动的所有相关人员将获得含有该服务适用的操作规程、规定和政策内容的文件。

4.4 审计记录规程

4.4.1 记录的事件类型

.TUSHU 注册中心记录与事件相关的所有信息（人物、事件和时间），包括：

- 访问存储 DNSSEC 服务的数据中心
- 访问服务器和 HSM
- 修改文件和文件系统
- 密钥操作：
    - 密钥生成/删除以及与密钥使用周期相关的其他事件
    - 生成 DS 记录并提交到根区域

4.4.2 处理日志的频率

定期监查审计日志，确保.TUSHU DNSSEC 服务的运营完整性。标记异常事件，以便 DNSSEC 安全审计员作进一步调查。

4.4.3 审计日志信息的保留期限

注册中心的日志在网上保留至少 3 个月。日期更早的日志归档后最多保存 5 年。

4.4.4 保护审计日志

仅允许授权人员访问审计日志，以防非法查看、修改、删除或其他篡改操作。审计日志中不含有可能损害私钥完整性的信息。

4.4.5 审计日志备份规程

审计日志按照预定的频率定期备份在离线存储系统中。仅 DNSSEC 授权人员可请求访问和查看这些档案。

4.4.6 审计采集系统

注册中心利用软件和应用程序将基本事件自动记录在审计日志中。除了系统记录以外，还会记录并存储应用程序日志。

4.4.7 通知引起事件的对象

不适用本文件。

4.4.8 漏洞评估

自动和人工漏洞评估部分通过监查审计日志完成。注册中心工作人员也参与评估，并与团体的其他成员共享安全性相关信息。

4.5 攻击和灾难恢复

4.5.1 事故和攻击处理规程

如果检测到事故和攻击，应确定问题的影响范围。如果密钥泄露，应立即启动紧急密钥更新。注册中心制订了 KSK 和 ZSK 紧急更新策略。

4.5.2 计算资源、软件和/数据崩溃

注册中心建立了备份系统和失效备援站点，以便应对资源、软件和/或数据崩溃的情况。注册中心将根据问题的具体性质，依照注册中心恢复计划采取适当的措施。

4.5.3 实体私钥泄密应对规程

注册中心 KSK 泄密后，将采取以下措施：

- 生成并激活新的 KSK 或者激活注册中心区域现有的试用版 KSK。激活过程中，DNSKEY 设置将重新签名。
- 使用根区域中新的 DS 记录替换已泄露密钥的 DS 记录。
- 尽快取消并删除注册中心区域中被泄露的 KSK，以免无法安全删除。

注册中心 ZSK 泄密后，将采取以下措施：

- 生成并激活新的 ZSK 或者激活注册中心区域现有的试用版 ZSK。激活过程中，所有签名将重新签名。
- 签名失效后尽快删除注册中心区域中被泄露的 ZSK。

4.5.4 业务连续性和 IT 灾难恢复能力

注册中心维护一个全面运营的备份/失效备援站点。发生故障时，失效备援/备份站点将取代 DNSSEC 运营。

4.6 实体终止

注册中心终止后，注册中心将全力协助完成有序过渡。

5 技术安全控制

5.1 生成和安装密钥对

5.1.1 生成密钥对

一年一次的签名仪式上生成 KSK 和 ZSK 密钥对，必要时可增加次数。一般情况下，按照预定的密钥更新周期，签名仪式上会生成足够数量的密钥对，足以支持.TUSHU DNSSEC 服务运营数月。密钥生成由授权人员在 FIPS 140-2 第 3 级硬件安全模块上进行。

5.1.2 交付公钥

注册中心 DNSKEY 资源记录集（RR 集）提供注册中心 KSK 和 ZSK 使用的公钥。除此以外，不通过其他方式分配。

5.1.3 生成公钥参数和质量检查

定期对公钥进行验证。

5.1.4 密钥用途

密钥用于注册中心区域中生成签名，除此以外，不用于其他用途。

5.2 私钥保护和密码模块工程控制

5.2.1 密码模块标准和控制

FIPS 140-2 第 3 级硬件安全模块上生成并存储 ZSK 和 KSK。

5.2.2 多人控制私钥

生成密钥时，必须至少有 DNSSEC 密钥管理员的两名授权成员在场。

5.2.3 私钥托管

.TUSHU 区域的私钥不受托管。

5.2.4 私钥备份

私钥备份位于符合 FIPS 140-2 标准的 PCMCIA 卡上，存放在异地和 2 小时安全防火柜中。

5.2.5 私钥存储在密码模块中

不适用本文件。

5.2.6 私钥存档

私钥不归档存储，除非在备份站点用作失效备援用途。

5.2.7 密码模块中的私钥转移

在 HSM 中生成的 ZSK 和 KSK 以加密形式转移到备份站点中。

5.2.8 激活私钥的方法

密钥管理员在安全审计员在场的情况下向硬件安全模块提供 PIN 后，即可激活私钥。

5.2.9 停用私钥的方法

系统关机后，私钥停用。

5.2.10 销毁私钥的方法

KSK 和 ZSK 私钥在系统中删除后便无法再使用。

5.3 其他密钥对管理事项

5.3.1 公钥存档

已过时的公钥不再存档。

5.3.2 密钥使用期限

KSK 在注册中心区域中的有效期约为一年加上发布和停用时的过渡期。由于 ZSK 的签名数量较大，ZSK 的有效期约为三年加上发布和停用时的过渡期。注册中心在必要时可更改期限。

5.4 激活数据

5.4.1 生成和安装激活数据

密钥管理员在安全审计员在场的情况下向 PIN 输入设备提供 PIN 即可激活 HSM。

5.4.2 保护激活数据

密钥管理员有责任保护 PIN 和 PED 的安全。必要时可取消或修改访问权限。

5.5 计算机安全控制

授予不同的授权人员访问 DNSSEC 不同部分和执行特定操作的权限。记录访问和操作事件并写入审计日志。监视并记录违反规定的行为或恶意行为，以便进一步调查。

5.6 网络安全控制

DNSSEC 服务的所有操作均在 Neustar 数据中心中进行托管和执行。内部网络受到多层物理和网络保护措施的保护，并且依照网络和物理安全性政策保护网络安全。

5.7 时间戳

DNSSEC 服务的所有时间戳均采用世界协调时间，并且通过 NTP（网络时间协议）服务器同步。

5.8 使用周期技术控制

5.8.1 系统开发控制

DNSSEC 服务的所有部分在部署前遵循严格的开发指导原则，确保实现可靠、高品质的可复制结果。

5.8.2 安全管理控制

注册中心建立了服务器软件更改监控机制，每日生成报告，供授权人员核查。

5.8.3 使用周期安全控制

注册中心根据反馈和团队最佳实践不断改进控制。对软件或安全政策和规程进行的更改将先经过评估、测试和批准后再进行部署。

6 区域签名

6.1 密钥的长度和算法

注册中心的 KSK 和 ZSK 均为 RSASHA256。KSK 采用 2048 位加密，ZSK 采用 1024 位加密。

6.2 存在性验证

注册中心使用 RFC 4034 中规定的 NSEC 记录进行存在性验证。

6.3 签名格式

.TUSHU 区域记录的签名格式为 RFC 5702 中规定的 RSA/SHA-2 格式。

6.4 区域签名密钥更新

.TUSHU ZSK 每 3 个月更新一次。

6.5 密钥签名密钥更新

.TUSHU KSK 每 12 个月更新一次。

6.6 签名有效期和重新签名的频率

ZSK 和 KSK 签名的有效期均为 30 天。签名到期前 7 天左右重新签名。

6.7 区域签名密钥集验证

签名仪式中按照一组明确的程序生成 ZSK。生成后的公钥及其元数据再进一步通过另一组自动验证工具进行验证。

6.8 资源记录验证

注册中心定期对区域中的所有资源记录进行在线验证，记录区域中的所有资源记录并验证所有签名。

6.9 资源记录生存时间

DNSKEY、DS 及各自的资源记录签名（RRSIG）的生存时间设置为 518400（6 天）。NSEC 及其 RRSIG 的生存时间为 86400（1 天）。将来如有必要，可更改生存时间。

7 合规审计

使用保留日志和其他相关信息进行审计，确保始终遵循和严格执行适当的规程。

7.1 实体合规审计的频率

审计由注册中心执行，至少每年一次，如果技术注册服务外包给第三方服务提供商，则由第三方执行。

7.2 审计员身份和资质

合规审计由精通安全审计、安全工具、DNS 和 DNSSEC 的独立安全咨询公司执行。

7.3 审计员与受委托方的关系

尽量委托注册中心和/或注册服务提供商以外的外部审计员执行审计。

7.4 审计涵盖内容

审计范围包括审查审计期间发生的事件，包括关键管理操作、基础架构/管理控制、KSK 和 ZSK 以及签名使用周期管理和实践披露。

7.5 缺陷应对措施

如果在审计时发现重大异常，将立即通知注册中心和/或注册中心外包服务提供商，并由受影响方制定和执行纠正措施。

7.6 传达结果

每次审计结束后 30 天内，将审计结果以书面报告的形式提交给注册中心和/或注册中心外包服务提供商。

8 法律问题

8.1 费用

接受、签名和发布授权签名者资源记录或 DNSSEC 的其他相关功能不收取任何费用。

8.2 经济责任

对于不当使用 DPS 签名的行为，Amazon Registry Services, Inc.不承担任何经济责任。

8.3 商业信息保密

8.3.1 机密信息的范围

以下信息应保密（机密/私人信息）：

- 私钥及恢复私钥所需的信息
- 将要发布的密钥集签名
- 交易记录（交易的完整记录和审计跟踪）
- Neustar 创建或保留的审计跟踪记录
- Neustar 或其各自的审计员（内部或公开）创建的审计报告（维护的报告），除非该报告已公开发布
- 应急计划和灾难恢复计划
- 管理 Neustar 硬件和软件操作及 DNS 密钥管理的安全性措施

8.3.2 机密信息范围以外的信息

关于 Neustar 运营的域名数据库的信息属于公开信息，例如公钥其他状态信息。

8.3.3 保护机密信息的责任

不适用

8.4 个人信息隐私

8.4.1 私人信息

不适用。

8.4.2 非私人信息类型

不适用。

8.4.3 保护私人信息的责任

不适用。

8.4.4 依据司法或行政程序进行披露

如果 Amazon Registry Services, Inc.在基于善意的原则上认为在民事或行政诉讼的取证程序中有必要依照司法、行政或其他法律程序（例如传票、质询、要求承认和要求复制文件）披露机密/私人信息，则有权进行披露。

8.5 责任限制

针对 Amazon Registry Services, Inc.在履行本文件义务时造成的经济损失或者由于附带性损失或损害而引起的其他损失，Amazon Registry Services, Inc.不承担任何责任，且不承担其他任何暗示或明示责任。

8.6 有效期和终止

8.6.1 有效期

DPS 发布在 Amazon Registry Services, Inc.资源库后开始生效。本 DPS 修订内容发布在 Amazon Registry Services, Inc.资源库后开始生效。

8.6.2 终止

DPS 及其不时经过修订的内容在被新版本取代之前一直有效。

8.6.3 争议解决规定

DNSSEC 参与者之间的争议应依照各参与者之间签订的适用协议的规定进行解决。

8.6.4 准据法/管辖权

本 DPS 受美国华盛顿州法律和管辖权的支配。