版本号：1.04
2012-04-04

1. 前言

1.1. 概述

本文使用现有操作文档中的模板创建。[1] 本文描述Afilias对DNS区域的操作，因为它与DNS安全扩展有关。除非文中另有说明，这些准则适用于Afilias签署运营的所有顶级域区域。

1.2. 文档名称和ID

Afilias DNSSEC操作准则（DPS）V1.04

1.3. 社区与适用性

本节描述DNSSEC 和签署顶级域所提供的功能的各个“利益相关方”。

1.3.1. 顶级域注册局

Afilias采用两种不同的模式运营：1）作为一个注册局运营商（RO），ICANN将顶级域直接委派给Afilias；2）作为一个后端服务提供商（BESP），Afilias代表另一个实体（该实体扮演注册局运营商（RO）的角色）维护该区域。当Afilias是该区域的注册局运营商（RO）时，它同时也是BESP。

注册管理机构应履行以下职能：

- λ 为该区域生成关键签署密钥（KSK）。
- λ 为该区域生成区域签署密钥（ZSK）。
- λ 使用KSK签署ZSK。
  - o 使用KSK签署该区域的相关资源记录。
  - o 需要时更新 ZSK和KSK。
  - o 将授权签字人（DS）资源记录发送给ICANN，以便将其纳入到根区域中。
  - o 接收授权注册商发来的DS资源记录，并对区域进行相应更新。
  - o 对WHOIS信息进行相应更新。

1.3.2. 授权注 册 商

经某个顶级域注册局运营商（RO）授权认可的注册商需要使用以下两个机制之一修改该区域：1）通过EPP，或2） 通过一个web管理工具(Web Administration Tool)。web管理工具（Web Administration Tool）是Afilias为EPP提供的一个前端，因此，针对注册管理机构 的所有修改实际上都是通过EPP完成的。对于DNSSEC，注册商应代表他们的客户（注册人）与Afilias公共维护授权签字人（DS）记录。

1.3.3. 注册人

注册人负责确保他们的二级区域得到正确签署和维护。此外，他们还必须生成 签署区域的DS记录，并将它们上传给他们的注册商（后者将这些记录转发给Afilias）。

1.4. 规范管理

1.4.1. 规范管理机构

Afilias负责维护本规范。

1 本文中的众多术语在当前版本的互联网草案的第2节中定义，本文源于该草案（截止到这个修订版）。上述草案是：draft-ietf-dnsop-dnssec-dps-framework-07.txt。上述草案被改动或以RFC的形式出版时，参考资料将随之改变。

1.4.2. 联系信息

与本DPS或签署顶级域的操作有关的问题应发往Afilias客户支持中心：

电话：+1 416.646.3306

电子邮件：support@afilias.info

1.4.3. 规范修改程序

本DPS将被定期 审核，必要时将得到更新。

所有修改将由操作和安全团队审核，并发往管理团队进行审批。一旦获批后，程序将被更新，相关人员将接受有关新型操作的培训。所有准备工作完成后，DPS将被出版，并立刻生效。

2. 公布和知识库

2.1. 知识库

本DPS可在以下网站找到：http://www.afilias.info/dps。
只有Afilias操作团队才能更新该网站的内容。文件的ACL为只读。

2.2. 公布关键签署密钥

通过向ICANN发送DS记录，以便将其纳入到顶级域根区域中，Afilias 顶级域区域的“信任链”将得到维护。这些DS记录对应该区域中的至少1个活动KSK。因此，无需公布另一个信任锚。

3. 操作要求

3.1. 域名含义

指定区域中的域名限制政策由注册管理执行机构制定，并随顶级域的不同而不同。

3.2. 子区域管理者的身份验证

注册局运营商（RO）必需明确授权Afilias允许指定顶级域中的子区域的DNSSEC 。只有注册商（代表他们的注册人）才能激活某个子区域的DNSSEC。为了激活DNSSEC，注册商必须通过Web管理工具（Web Administration Tool）或EPP提交一条授权签字人（DS）记录（依照RFC 5910）。

对于EPP，每个注册商都有用于访问TLD注册局的唯一凭证，在执行任何EPP操作之前，这些凭证必须通过验证。对于Web Administration Tool，使用证书是唯一确定注 册 商 的 身 份 。

3.3. 注册授权签字人（DS）资源记录

注册商通过EPP（尤其是依照RFC 5910）将DS记录发送至注册局。提交到顶级域注册管局之后，WHOIS数据将被修改，区域修改将被自动传播到DNS基础设施。

3.4. 证明拥有私有密钥的方法

授权注册商负责确保提交给Afilias的数据的完整性。在向上级提交一条DS记录之前， 不要求某个区域中已经公布了一个对应的DNSKEY。这可以证明拥有私有密钥变得无法预测。

因此，Afilias不运行任何用于证明拥有私有密钥的测试。

3.5. 删除DS记录

3.5.1. 谁可以请求删除记录

只有相关域名的所属注册商才能添加、更改或删除该域名的DS记录。注 册 商 必 须 提 供 一 个 Auth-Info码，用于验证针对该域名的任何修改。

3.5.2. 删除请求程序

根据RFC 5910，可以使用相应的EPP命令删除记录。只有所属注册商有权请求删除某个记录，而且还必须提供正确的Auth-Info码。

3.5.3. 紧急删除请求

3.5.4. 由于是通过EPP操作，系统将得到持续更新，因此，没有为紧急删除请求另外制定程序。

4. 设施、管理和操作控制

4.1. 物理控制

Afilias使用两个位于不同国家的站点，而且它们不属于我们的办事处。这两个站点都是物理防护环境，能够阻止、防范和检测针对敏感信息和系统的 未经授权的使用、访问和披露。只有授权人员才能进入这两个站点。来访者必需在授权人员的陪同下才被允许进入，而且必需是为了某个具体的目的（如技术人员维修硬件）。

这两个站点均提供冗余和备用电源以及空调和消防设施。它们为对方相互提供冗余和备用DNSSEC服务，并采取合理措施减少Afilias系统与水接触。

Afilias的站点配有用于存储敏感信息的介质，并采用适当的物理和逻辑访问控制措施，用于限制未授权人员的访问。

在处理之前，敏感的文档、资料和存储介质已被粉碎，变为不可读。 Afilias定期备份重要的系统

数据，并使用一个第三方存储设施维护一个离线备份。

4.2. 程序控制

至少有两个操作团队负责维护签署系统。每个团队成员持有访问签署系统所需的密码的一部分。针对签署系统的任何任务都需要来自每个团队的一名授权代表在场才能执行。

4.3. 人员控制

Afilias要求参与某个可信角色的所有人员必需已在Afilias工作至少一年，而且必需拥有这一职务所要求的资格。

Afilias为所有员工提供入职培训以及履行工作职责所需的培训，并在必要时提供进修培训和更新。人员在必要时需要轮岗和换岗。

在特定情况下，承包商可以履行某个可信角色的职责。此类承包商被要求满足适用于相应职位的Afilias员工的相同标准。

Afilias为所有员工提供履行工作职责所需的资料和文件。

4.4. 审计日志记录程序

所有的重要生命周期事件，包括但不限于生成、激活、滚动、销毁和使用，无论它们成功与否，都将被记录到一个系统中，其中包含各种机制，用于防范未授权人员查看、更改、删除或以其它方式篡改日志文件。

对物理设施的访问将被设施记入日志，该日志只能由授权人员访问。

Afilias将监视所有日志条目，以找出异常和事故告警。Afilias安全团队每周至少查看一次所有审计日志，寻找可疑或异常活动。

4.5. 损坏和灾难恢复

如果遭遇重大损坏或灾难，Afilias的事故响应团队将会接到通知。该团队制订了调查、事故升级和响应程序，负责评估事态，制定行动方案，并在管理层批准后实施行动方案。

Afilias维护着冗余设施，以确保当某个站点不可用时，一个灾难恢复站点能够立即可用。重要数据均得到克隆和加密，并被发送到同一设施中的热备系统以及冗余设施中的两个备用系统。加解

密重要数据的能力被完全植入到每个系统的高安全性模块中，未在签署系统之外。

4.6. 实体终结

当签署服务的角色和职责必需转移给其它实体时，Afilias将采用一个DNSSEC终结方案。Afilias将与所有相关方开展合作，以安全透明地完成转移。

5. 技术安全控制

5.1. 密钥对的生成和安装

所有密钥对均在签署r系统中使用操作团队提供的参数生成。签署系统满足FIPS 140-2 level 3的要求。作为签署流程的一部分，公共密钥被当作一条DNSKEY资源记录被自动插入到顶级域区域文件中。一条DS记录被生成，并被提交到上级（根）区域。

签署系统保持KSK与ZSK分离，并管理密钥对的使用。每个密钥只用于一个区域。

5.2. 私有密钥保护和密码模块

工程控制

所有签署系统均通过FIPS 140-2 level 3认证。不允许对私有密钥进行加密访问。对签署系统的访问在程序控制和人员控制两节描述。

维护着多个冗余签署系统。这些系统包含一个机制，用于安全地相互备份密钥对和操作参数。私有密钥无法以其它方式备份、保存或存档。当某个私有密钥被去激活时，它将被签署系统销毁。

一个值得信赖的团队有权创建、激活和去激活密钥对，并根据相关政策和程序履行职责。

5.3. 计算机安全控制

Afilias将确保负责维护重要软件和数据文件的系统是值得信赖的系统，可阻止未经授权的访问。此外，Afilias还限制那些拥有合理有效的商业理由的个人访问生产用服务器。普通的应用用户在这些服务器上没有账户。

5.4. 网络安全控制

签署系统位于Afilias的生产系统之中，在逻辑上与其它系统分开。使用防火墙等常规网络安全机制减少进入威胁。只有那些受限角色用户才有权访问生产系统，而且他们的操作将被记入日志。

5.5. 时间戳

签字人系统能够安全地将系统时钟与Afilias 网络中的一个可信时间源进行同步。

5.6. 生命周期技术控制

Afilias开发和使用的应用均符合其开发与变更管理程序。可以使用版本控制系统追踪所有软件。生产期间的软件更新是一个打包更新机制的一部分，通过受限角色访问进行控制，并通过 自动配方进行更新。在部署前，所有更新和补丁都将通过全面验证。

Afilias在其签字人系统中使用一个第三方解决方案，以便在部署前在一个安全的实验室环境中测试所有更新。

6. 区域签署

6.1. 密钥长度和算法

关键签署密钥

Afilias使用2048位密钥长度和RSA生成算法。

区域签署密钥
Afilias使用1024位密钥长度和RSA生成算法.

6.2. 已验证的否认存在
将使用RFC 5155 [RFC5155]中描述的NSEC3记录提供已验证的否认存在。

6.3. 签名格式
SHA1，使用RSA

6.4. 区域签署密钥的滚动
Afilias将按照RFC 4641中 4.2.1.1节描述的一个公布前方案滚动ZSK。ZSK滚动每月进行一次。

6.5. 关键签署密钥的滚动
Afilias将按照RFC 4641中 4.2.1.2节描述的一个双签署方案滚动KSK。目前未定义KSK的滚动频率。

6.6. 签名的生命周期和再签署频率
区域每隔8天或9天签署一次（每月4次），签名的生命周期为20天。为防范签署期间的可能攻击，抖动将被引入。

6.7. 区域签署密钥集的验证
对区域签署密钥集的验证是通过验证密钥签署记录中的公共密钥数据完成的。

6.8. 资源记录的验证
所有RR签名在公布前均被验证。

6.9. 资源记录的存活时间

DNSKey	15分钟
NSEC3	SOA最少（24小时）
Delegation Signer（DS）	24小时
RRSIG	取决于所覆盖的RR

7. 合规审计

7.1. 实体合规审计频率
合规审计至少两年进行一次。

7.2. 审计机构的确定/资格
审计机构应是以下实体：精通所审计的技术，并独立于Afilias。

7.3. 审计机构与被审计方的关系
审计机构必需独立于Afilias。

7.4. 审计内容
环境、网络与软件控制、操作、重要的管理实践和操作。

7.5. 发现低效时所采取的措施
审计中所发现的任何差距都将导致我们创建一个行动图，列出消除差距所需采取的措施。管理人员将设计和实施旨在消除差距的各个步骤。

7.6. 公布结果
Afilias将在http://www.afilias.info/dps上公布结果。

8. 法律事务

本操作准则（DPS）适用于爱尔兰国内法，并按它们进行解释，不适用于任何可导致运用爱尔兰国内法以外的任何法律的法律条文。

以下资料应被视为保密：

- 私有密钥
- 用于获取/恢复私有密钥的信息
- 灾难恢复计划（DRP）
- 与DNS密钥管理有关的任何操作详情，包括但不限于网络、软件和硬件详情。

Afilias不会隐含或明确提供任何担保，而且对本DPS中的任何程序和职能不承担任何法律责任。Afilias不对使用密钥造成的财务或其它任何损失承担责任。请将所有法律问题发送至：legal@afilias.info。