约翰内斯堡 – 关于 KSK 滚动更新计划的 GAC 会议
2017 年 6 月 29 日（星期四）- 12:00 - 12:30（约翰内斯堡时间）
ICANN59 | 南非，约翰内斯堡

施耐德 (SCHNEIDER) 主席：我们赶在午餐休息前再召开一场会议，本次会议的主题是 KSK 滚动更新计划。ICANN 强烈要求传达一项重要信息。我们有幸请到了戴维·康纳德 (David Conrad)，稍后他将会做自我介绍，并说明出席本次会议的缘由。

未知身份的发言者：[关闭麦克风]。

施耐德主席：请随意选择一个座位，或者也可以坐到中间，戴维。

戴维·康纳德：大家好，我叫戴维·康纳德，目前担任 ICANN 首席技术官。今天来到这里想跟大家谈谈密钥签名密钥滚动更新计划，我们正在开展这项工作。密钥签名密钥是在 DNSSEC 中使用的一种密钥，主要用于对所谓的域签名密钥进行签名。接着，继续使用域签名密钥对根区进行签名。以上就是 DNSSEC 的实施过程。2010 年，当我们首次对根区进行签名时，曾向社群宣布，5 年后将会更改密钥，称之为密钥滚动更新。今年是 2017 年，我们正在做出相关更改。在 Adobe 的帮助下，我打算展示几张幻灯片。

注：以下内容为针对音频文件的誊写文本。尽管文本誊写稿基本准确，但也可因音频不清晰和语法纠正而导致文本不完整或不准确。该文本仅为原始音频文件的补充文件，不应视作权威记录。

内容十分笼统，请大家谅解。我记得，我们曾面向 180 个国家/地区的监管机构发布了一封公开函，并且抄送给这些国家/地区的相应 GAC 代表。在这封信函中，我们希望提醒广大监管机构，即将推行密钥滚动更新计划，如有关监管机构准备迎接此次调整，应向网络运营商咨询相关情况。

下面简要介绍几个概念。根区 DNSSEC 密钥签名密钥是用于保护 DNS 数据的最顶层密钥。由公钥部分和私钥部分共同组成。私钥部分存储于所谓的安全密钥管理设施中。目前共设有两个安全密钥管理设施。一个设在美国东海岸，另一个设在美国西海岸。

二者建于 2009 年，当时与美国商业部签订了合同。这些设施的安全性相对较高。其中设有安全室。安全室内设有安全柜。安全柜中装有保险箱。保险箱中设置了所谓的硬件安全模块。这些专业设备用于承载加密信息。根区的私钥就存储在支持访问控制的协同定位设施的安全室安全柜保险箱的 HSM 中。

公钥/私钥对的公钥部分将被复制到执行 DNSSEC 全球验证的各个 DNS 解析器中。据我们估计，全球共有大约 1 亿解析器，其中仅有一小部分实际执行 DNSSEC 验证。不过，我们仅与存有配置信息的大约几百万解析器开展通信。密钥滚动更新——DNSSEC 使用密钥构建信任链，连结 DNS 直至最后一个节点，实际查找树叶信息，务必确保域所有者对数据进行了

DNSSEC 签名，中间人攻击、网络钓鱼及其他攻击形式无法随意修改相关数据。请切换到下一张幻灯片。

为什么要滚动更新密钥？目前有一种常用的安全做法：如果设置密码，需要不时做出更改，防止有人悄悄攻陷密码，确保更改密码所需的必要基础设施正常运行，以防出于某种不明原因被迫更改密码。

DNSSEC 也是如此。大家可以将密钥签名密钥想象成为 DNSSEC 密码，因而必需确保更改密钥所需的基础设施切实正常运行。一旦需要更改密钥，必需立即做出响应。众所周知，倘若加密信息分解技术取得重大突破，很可能需要更改密钥，或者声明在某种程度上密钥已经受损。问题在于，需要更新的设备数量十分庞大，操作过程必须极为谨慎而且十分缓慢。与此同时，在操作过程中，还会尽量避免摧毁互联网。关键在于，如果密钥滚动更新出现错误，那么将意味着，计算机、服务器以及使用互联网查找名称的最终用户对签名区域开展的一切操作将瞬间戛然认知。由于根区经过签名，该网络的全体用户将不得不面对现实。我们不希望出现这种场景。所以，我们会慎之又慎，尽量多方开展测试，务必杜绝一切重大风险，避免互联网 DNSSEC 验证出错。基本上，整个过程需要花费两年半的时间。请切换到下一张幻灯片。

就是这一张。我们列出了一些密钥滚动更新重要事件日期，有些已经发生，有些尚未发生。9 月 19 日，密钥规模有所增

加，因为我们不得不在 DNS 中插入新密钥，供即将举办的所谓密钥仪式使用。在密钥仪式上，我们需要进入这些安全设施，提取私钥并对用于执行根区签名的 VeriSign 域签名密钥进行签名。每季度都会开展这项工作。这意味着，每季度的密钥仪式基本上都要定时举办所有这些活动。上一次密钥仪式是在 9 月，确切地说是 2017 年 9 月 19 日。DNS 密钥的规模还会不断壮大，因为我们还会继续增添新的密钥。今年 10 月 11 日，我们会将密钥首次投入使用。

这一天，很可能会出现一些奇特的现象。奇特之处在于，如果人们未在 10 月 11 日前使用解析器更改密钥，将无法完成验证。届时查找域名，将会显示“找不到主机”或错误 404，诸如此类。

1 月 11 日，我们将回收旧密钥并进行设置，提示不可再使用密钥。3 月 22 日，将从根区中全面清除旧密钥。紧接着，2018 年 8 月，我们将彻底销毁旧密钥，保障所有信息安全可靠。

请切换到下一张幻灯片。

这将会对哪些群体带来影响？DNS 软件开发人员和分销商必需获取新密钥，将新密钥输入软件和分销系统。系统集成商，如获取并部署相关软件，必需确保在集成系统中使用最新密钥。网络运营商往往负责运行解析器，必需确保系统支持更改密钥。

根服务器运营商需要保持清醒，我们会一直与他们保持密切联络，如果人们未更改密钥，他们很可能会议遇到麻烦。通常情况下，如果 DNSSEC 验证失败，解析器将会多次尝试执行解析。因此，通信量将会有所增加。

互联网服务提供商几乎必然会接到求助电话。如果网络运营商未更新密钥，必然会遇到某种麻烦，ISP 势必会致电求助。

如果网络运营商未更新密钥，最终用户将会受到影响，因为用户将瞬间无法访问任何互联网站点。

请切换到下一张幻灯片。

显而易见，我们需要做大量准备工作。我们一直提醒网络运营商确定是否启用 DNSSEC 验证。如果启用了 DNSSEC 验证，务必确保能够更新密钥。从历史角度而言，一旦开始运行解析器，将无需再过多关注。倘若人们将解析器部署到只读文件系统，如尝试更改密钥，势必引发问题，因为您根本无法对磁盘执行写入操作。

请切换到下一张幻灯片。

那么，解析器运营商又该怎样做呢？他们需要确定是否启用 DNSSEC。务必确保了解如何评估系统信任度。必需测试并验证解析器能否更改密钥，检测配置文件，保证将数据写入适当的位置。如果已经启用 DNSSEC 验证或者计划在网络中启用 DNSSEC 验证，则需制定密钥滚动更新实施计划。比方说，仔

细监测 10 月 11 日的行为，确定故障表现。通常，若解析器尚未更新密钥，将开始显示服务器失败——每当有人查询受保护的名称，都会提示服务器发生故障。

请切换到下一张幻灯片。

十分令人遗憾。在蓝色小方框中显示的是我们发出的公开函图像。我刚刚说过，我们面向各个国家/地区的监管机构和 GAC 代表发布公开函，建议他们咨询网络运营商，务必确保全面掌握密钥滚动更新计划。请切换到下一张幻灯片。

差不多就是这样。欢迎大家广泛提问，非常乐意提供相关信息，帮助您与网络运营商开展相关讨论。再次声明，我是戴维·康纳德，我的联系方式是 david.conrad@icann.org。感谢大家观看本次演示。

施耐德主席： 谢谢，戴维。首先，我想提一个问题：可不可以提供一个模拟电话热线号码？一旦整个互联网发生瘫痪，我们可以致电寻求帮助。热线全天候运行吗？

美国代表想要提问或者发表评论。

戴维·康纳德： 先来回答这个问题：是的，ICANN 全球支持中心提供了相关信息，我们已经通过各种渠道发布号码。

美国代表： 谢谢，戴维。这项演示很有帮助。我本人很关心这个问题，因为我自认是一位不折不扣的计算机谜。不过，我们并没有接到 Goran 的来信。非常感谢。老实说，我的第一反应是需要与 ISP 携手合作。身为政府机构，我们通常会依赖决议规范商业 ISP。

但从提供指导的角度而言，我们是否需要以政府机构的名义开展工作？除了确保 ISP 开展必要工作以外，可否提出一些内部工作建议保证业务正常运转？谢谢。

戴维·康纳德： 好的。在任何网络中——无论是政府内部网络还是 ISP 网络，都需要在某个位置安装解析器。也可能安装到外部。例如，Google 提供了公共 DNS 服务 8.8.8.8。很多用户使用这项服务。

所有这些都必需确保能够支持密钥滚动更新计划。

据我所知，Google 坚决支持密钥滚动更新计划。毫无疑问，我丝毫不表示怀疑。

至于其他 ISP 和网络运营商，特别是企业级网络运营机构，只能逐一询问确定是否留意密钥将会发生更改。如果了解相关情况，应首先检查确定是否启用 DNSSEC 并鼓励启用 DNSSEC，如果可能的话。如果已经启用 DNSSEC，则检查确定是否留意密钥将会发生更改。如果不了解相关情况，则建议他们参与 ICANN 公布的密钥滚动更新计划。

在本次会议中，我们希望说明众多地区开展的工作，切实加强人们对相关工作的认识；不过，显然根本不可能亲自传达到每一个人。因此，我们强烈呼吁政府机构开展一定的工作，确保网络运营商意识到即将实施密钥滚动更新计划。

施耐德主席： 伊朗代表请讲。

伊朗代表： 非常感谢您所做的陈述。有没有设立反馈渠道，确保切实落实您所提出的具体措施，避免陷入不利困境？不是所有人都熟悉相关措施并快速落实。只想提一个反馈问题。我们已经接到公开函，并且正在落实相关工作。有什么潜在困难要说明吗？又或者，根本没有部署反馈系统？谢谢。

戴维·康纳德： 通常，无论在任何情况下，我们都会鼓励人们与我们联系，提出可能存在的问题，或者表达可能希望表达的担忧。

我们并未确立明确机制要求人们提出反馈意见。不过，我们会一直与各大网络运营机构、TLD 组织及有关机构携手合作，切实提供平台，从而建立通信渠道，便于大家向我们提出相关反馈意见。

施耐德主席： 谢谢。下面有请埃及代表、挪威代表、英国代表，还有荷兰代表发言，抱歉。

埃及代表： 谢谢，托马斯。感谢戴维的精彩演示。我想就第 5 张幻灯片提一个问题。与此同时，如果理解无误的话，还有提供了某种工具执行检查，我认为有必要进行相关了解。

戴维·康纳德： 是的。我们创建了试验床，解析器运营商可以通过试验床参与 KSK 滚动更新实时测试。遗憾的是，这个幻灯片中并未对试验床进行介绍。我们倾向于在技术性较强的幻灯片中进行相关说明，但我可以向 GAC 成员提供信息，以便他们向其所在国家/地区的网络运营商做出介绍。

埃及代表： 是的，谢谢。我认为这非常有帮助。

请谈谈我就第 5 张幻灯片提出的问题。

我想确定一下，这是否会对特定解析器造成影响？我发现，ccTLD——我是指 TLD 注册管理机构和运营商并未出席本次会议。是否推荐特定解析器？谢谢。

戴维·康纳德： 好的。DNS 端用户将会受到影响，DNS 端需要从 TLD 运营商处获取信息。TLD、ccTLD、gTLD 将不会受到密钥滚动更新计划的影响。不必采取任何措施。他们提供的功能不会受到影响，当然，内部系统及其在内部系统中运行的解析器除外。

施耐德主席： 谢谢。

有请荷兰代表发言。

荷兰代表。 感谢戴维的细致说明。我想核实几点。我认为，政府机构在这方面不需要承担正式责任。之所以邀请政府机构参与，纯粹是为了举办外展活动，与 ISP 建立联系。比方说，完全不存在政府责任？

戴维·康纳德： 确实如此。我们将会探寻所有可以联络的通信渠道，是的。

荷兰代表。 其次，还提供了 DNS 解析器和递归解析器列表，用于对每个字母执行 DNSSEC 验证。在我们的示例中，我记得大约有七八个的样子。当然，据我推测，同样存在直接联系。这些元素与更改息息相关，属于实际系统更改。其他受影响的各利

益相关方确实会产生一定的效应，但真的一定要做出系统更改吗？谢谢。

戴维·康纳德： 关于密钥更改的实际操作方式，实际上采用的是自动模式。如果某位解析器运营商运行的是最新软件，并且已经启用自动更新，那么不必采取任何措施。或许应该谨慎使用试验床，务必确保在实施密钥滚动更新计划时，不会发生任何奇特现象。总而言之，将会自动内置到现代解析器，从而自动完成密钥滚动更新。

如果并未运行旧——抱歉，并未运行新版软件，或者尚未启用自动滚动更新，则必须更改配置数据点。公钥已经与 KSK 建立关联，必需复制到配置文件。在这种情况下，解析器运营商将不得不采取一定的措施。

施耐德主席： 谢谢。英国代表请讲，请保持简洁。

英国代表： 好的，谢谢。感谢戴维参加本次会议并说明相关情况。

我还没有来得及与 ISP 选区 ISPCP 的英国成员开展讨论。基本上，他们都与此有关，所以要核实一下。假设将会积极联络，

面向全球 ISP 开展关键外展活动。您对活动成效有信心吗？如果做出相关保证，将会很有帮助。

实际上，我并未收到公开函，所以也必须进行核实。我不知道结果会怎样。

但是，我记得您还曾指出，需要与全球政府网络提供商进行核实，这对我们意义重大。就我个人而言，面对的是伦敦内阁府。10 月 11 日，您将会做些什么？您期待这一天的到来吗？我的意思是，如果因为人们未能落实必要的转换工作而造成麻烦，一旦出现这种状况，是否需要依靠政府采取恢复措施为解决事态保驾护航？或者说，一旦 10 月 11 日出现问题，如何应对这种严重态势？嗯，抱歉。

戴维·康纳德： 我们一直与 ISPCP 积极联络，鼓励他们派遣选区成员出席会议，并广泛邀请其他机构参加网络运营小组会议。

至于“是否会引发混乱局面”，我们一直在设置精细观察系统，严密监测根服务器通信，根服务器通信可以率先提示糟糕问题。同时，我们还制定了回退计划，一旦检测到某个重要事件表明滚动更新失败，将会实施回退计划。

我们十分肯定，政府机构不太可能会遭到最终用户和网络运营商的愤怒对待。据我预计，人们势必会将怒火指向 ICANN，更

确切地说是我本人。正因如此，我一直勤勤恳恳地竭力获取相关信息。保证人们更新密钥至关重要。

施耐德主席： 抱歉！请不要离开会议室。稍后，我将会宣布一项重要事件。下面先请坐在后排的那位男士发言。我记得你是尼日利亚代表，对吗？

尼日利亚代表： 尼日利亚代表，是的。

施耐德主席： 谢谢。请不要离开会议室。这是我们安排的最后一次发言，然后发言到此结束，尽管结束发言有些困难。尼日利亚代表，请讲。

尼日利亚代表： 感谢精彩的 DNSSEC 滚动更新演示。

我有一个疑问：对于未启用 DNSSEC 的网络服务提供商，滚动更新后将会面临哪些问题？起初网络中并未启用 DNSSEC。谢谢。

戴维·康纳德： 好的。不会发生任何变化。如果尚未启用 DNSSEC，密钥滚动更新将不会带来任何影响。如果未来某一时刻决定启用 DNSSEC，则必需确保获取最新密钥。如果未获取最新密钥，验证将会失败，继而造成混乱。综上所述，他们只需确保获取最新密钥或者最新软件版本，实际上很可能会自动获取最新密钥。

施耐德主席： 现在必须结束了——一些代表希望保持会议简明扼要，我们深表理解——还有一个重要事件需要宣布。众所周知，这是本届会议的最后一次午餐，这意味着也是欧勒夫 (Olof) 在任的最后一次午餐——

你的确切职务是什么？ICANN 外派 GAC 支持人员，无论白天黑夜，总是在召开电话会议时讲一些幽默笑话，热衷提供支持是关键。

事实上，茱莉亚 (Julia) 或许还像往常一样隐藏在某个角落，一直在帮助我们为欧勒夫准备小礼物。

[笑声]

你很快会看到礼物——我们将会联络技术人员，看看怎样把它运回家。我记得有一张卡片，这是礼物。不是很重，应该可以搬动。同样，最后我们衷心地对你表示感谢，欧勒夫。

后排藏有一些玻璃杯，请大家喝些饮料吃些点心，与欧勒夫共同庆祝担任这一职务的最后时光。非常感谢，欧勒夫。

[掌声]

欧勒夫·诺德林 (OLOF NORDLING)：非常感谢。我一直想要一块铁砧 -

[笑声]

——作为随身行李。

噢，好极了！非常感谢。希望随时保持联系，尽管我即将退休。

我将会一直待到 7 月末，现在还不能完全摆脱我，但依然非常感谢大家。

施耐德主席： 是的。请大家前往后排——

巴西代表： 托马斯，我可以提一个要求吗？

施耐德主席： 好的。

巴西代表： 午餐结束后，我们将继续召开会议讨论地理名称，需要达成哪些目标？我认为，我们还需要就公报开展一定程度的讨论，或者根本没必要这样做？在此情况下会发生什么事情？昨天，我们曾提出要在 3:00 举行会晤或者进行某种互动。

施耐德主席： 我们将会简单讨论当前或过去获取的文本。汤姆将对此进行概括介绍。我们会在午餐时间开展相关讨论，接着大约 3:00 准备好一切，然后占用 5 分钟左右确定最终文本，但愿可以圆满达成目标。谢谢你提醒我们。

不要离开，工作尚未完成。谢谢。

不过，现在不要谈工作，先为欧勒夫干杯。谢谢。

[休息]