构建可扩展的RPKI依赖方系统部署机制

Scaling RPKI Relying Party System

马迪/MA Di
（互联网域名系统国家地方联合工程研究中心，中国 北京 100102）
(Internet Domain Name System National Engineering Research Center, Beijing 100102, China)

DOI：10.12142/ZTETJ.202301008
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20230227.1253.004.html
网络出版日期：2023-02-27
收稿日期：2022-12-15

摘要：互联网码号资源公钥基础设施（RPKI）依赖方系统是各类网络运行机构开展RPKI应用实践的一个关键环节。RPKI依赖方系统的研发和部署，既需要处理RPKI核心功能的“普遍性”问题，又需要兼顾网络互联互通特征的“特殊性”问题。相关解决方案需要考虑RPKI依赖方系统应当有哪些组件，各个组件如何在网络上分布，以及以何种逻辑关系分布。面向RPKI依赖方系统的核心功能，梳理了影响RPKI依赖方系统运行效能的4对矛盾，并提出了一种可扩展的RPKI依赖方系统部署机制，包含软件层面的解耦机制和硬件层面的部署机制。

关键词：RPKI；路由安全；互联网码号资源管理

Abstract: The resource public key infrastructure (RPKI) relying party system is key to network operations with regard to the RPKI in practice. The development and deployment of the RPKI relying party system involves both the essential functionality of the RPKI universally and the networking condition where it operates particularly. The very resolution calls for the design of modularizing the RPKI relying party system and deploying those modules physically and logically. Four contradictions regarding the operation efficiency of the RPKI relying party system are summarized and a scheme of scaling the RPKI relying party system is proposed with respect to both the decoupling mechanism of software and the deployment principle of network hardware.

Keywords: RPKI; routing security; Internet number resource management

1 研究背景

自2012年国际互联网工程任务组（IETF[1]）完成基础协议的标准化工作以来，历经国际互联网体系结构委员会（IAB[2]）的背书[1]以及国际互联网路由安全自律协定（MANRS[3]）项目面向全球网络运行机构的推广倡议，互联网码号资源公钥基础设施（RPKI）已成为解决当前互联网域间路由安全问题的技术路线共识。RPKI的理念肇始于互联网安全协议专家S. KENT博士的论文[2]，并通过对传统的基于X.509公钥基础设施进行扩展[3]，进入到IETF的工业标准体系。

RPKI的部署和运行是一个复杂的系统工程，需要网络运行机构（网络运营商、互联网交换中心、内容分发网络服务商等）、RPKI数据服务机构（互联网IP地址注册机构、RPKI依赖方系统服务商等）以及路由器制造商等角色的配合和协调。其中，RPKI依赖方（RP）系统充当了地址管理系统和路由控制系统之间RPKI数据传递的桥梁，是连接RPKI数据供给侧和RPKI数据需求侧的RPKI生态关键环节。

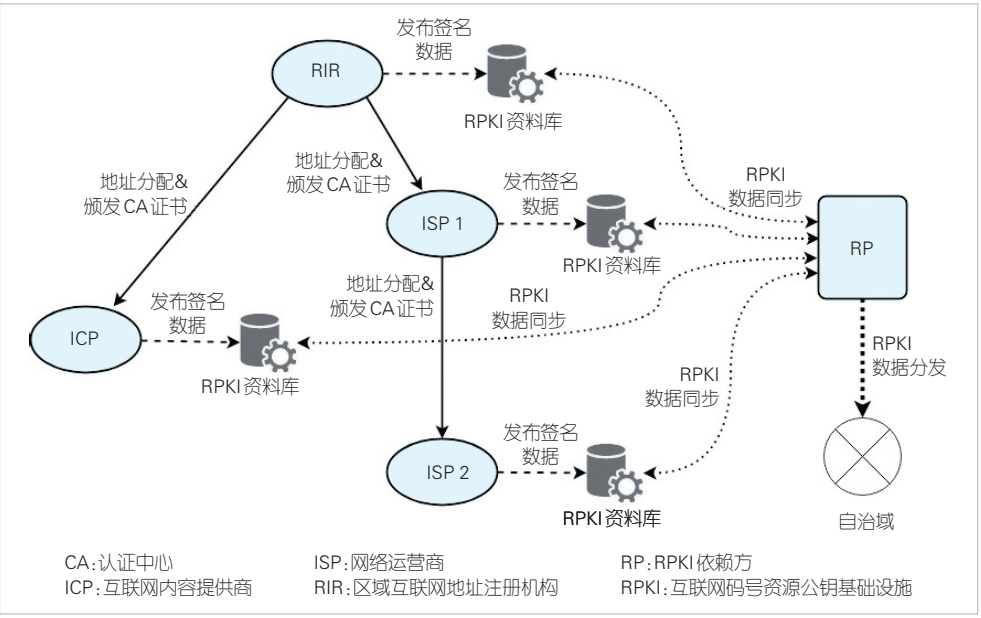
RPKI依赖方系统的部署，涉及网络运行机构的路由控制策略、安全保障策略和地址分配策略，需要统筹网络规模、拓扑结构、互联互通策略以及地址资源分配格局等要素。这些要素会因应业务和技术的演进而随之变化。设计一个既可以处理RPKI依赖方系统功能诉求的“普遍性”问题，又能兼顾具体网络（及其变化）“特殊性”问题的可扩展部署机制，是RPKI技术在网络运营商、互联网交换中心等网络运行机构落地应用的关键。

2 RPKI原理简介

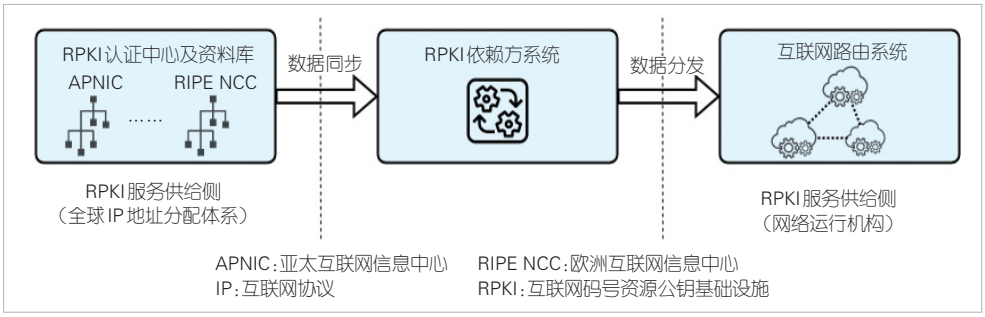
RPKI是一种公钥证书基础设施。基于当前全球的互联网码号资源分配关系，RPKI构建了一个面向IP地址及互联

1 IETF: Internet Engineering Task Force，国际互联网工程任务组（https://www.ietf.org/）
2 IAB: Internet Architecture Board，国际互联网体系结构委员会（https://www.iab.org/）
3 MANRS: Mutually Agreed Norms for Routing Security，国际互联网路由安全自律协定（https://www.manrs.org）

网自治系统（AS）号码的授权认证体系，并以X.509证书扩展及若干签名对象的形式加以呈现。如图1所示，RPKI体系中的码号资源分配者在分配资源的同时，为下游节点签发资源证书（基于X.509证书的扩展）。依托RPKI提供的认证功能，互联网码号资源（IP地址及AS号码）的最终用户单位（资源持有者）通过签发相关数据对象，来完成路由通告相关信息的发布（例如路由起源授权等）。作为RPKI认证体系的依赖方，参与域间路由交互的网络运行机构（例如网络运营商、互联网交换中心等）定期从RPKI资料库系统（基于码号资源分配关系组织起来的分布式数据存储体系）同步资源证书以及包括各类基于RPKI的数据对象，并将经过验证的信息推送给边界路由器，供其在接收路由通告时进行真伪判断。



▲图1 RPKI的工作原理



▲图2 RPKI的生态结构

概括地讲，RPKI生态有3个组成部分：RPKI供给侧、RPKI依赖方、RPKI需求侧。如图2所示，RPKI供给侧包含全球分布的RPKI认证中心（CA）以及用于存储RPKI资源证书和各类RPKI数据对象的分布式RPKI资料库系统。RPKI需求侧是当前互联网的域间路由系统，由部署在不同网络自治域的边界网关协议（BGP）路由器组成。RPKI依赖方是连接“供给”和“需求”的桥梁，负责收集RPKI供给侧产生的数据并加以验证后交付给RPKI需求侧参考使用。

RPKI数据尽可能快速、完整、准确地从供给侧扩散至需求侧的关键在于RPKI依赖方。全盘考察RPKI的运行机制，并结合相关RPKI依赖方系统的运行实践，笔者归纳了影响RPKI依赖方系统效能的4对矛盾：

矛盾1：RPKI资料库（发布点）越来越多，与实时感知全球RPKI数据更新情况之间的矛盾；

矛盾2：RPKI数据对象数量越来越多，与快速同步全球RPKI数据之间的矛盾；

矛盾3：RPKI数据授权链（深度和广度）越来越复杂，和快速构建全球RPKI数据认证路径之间的矛盾；

矛盾4：RPKI依赖方系统集中化趋势（远离网络边缘），和路由器快速获得RPKI认证数据之间的矛盾。

以上矛盾既有在“RPKI基本原理范畴”的普遍性，又有在“网络互联互通特征范畴”的特殊性，因此需要构建一个能够因应网络规模和信任模型变化而灵活调整的可扩展RPKI依赖方系统部署机制。该机制映射至解决方案层面，即RPKI依赖方系统应当有哪些组件，组件如何在网络上分布及以何种逻辑关系进行分布。

3 RPKI依赖方系统组件的功能解耦机制

可扩展RPKI依赖方系统部署机制在“RPKI基本原理范畴”的首要任务是，通过对RPKI依赖方系统核心功能实施解耦，形成彼此“正交”的RPKI依赖方系统的组件布局。按此原则，基于IETF RFC8897[4]，笔者从工程实践的角度梳理了RPKI依赖方系统在理论上的最低技术要求，包括：同

步RPKI资料库的数据、处理RPKI资源证书、处理RPKI数据签名对象、分发验证过的RPKI认证信息以及本地化控制。一个具备IETF RFC8897所列举功能的系统，可以称为RPKI依赖方系统。

RPKI依赖方系统在全球各个网络内的部署已逾10年，形成了一些运行实践和讨论。笔者在起草IETF标准和进行RPKI系统设计的工作中，有两点体会：在部署层面，RPKI依赖方系统的功能仍需要进一步模块化（正交化）；在运行层面，IETF RFC8897所列举的功能无法满足商用路由控制系统对RPKI依赖方系统的需求。为此，构建可扩展的RPKI依赖方系统的第一步是将其核心功能模块化，并给出各个模块彼此解耦之后的逻辑关系（接口关系）。图3是笔者对RPKI依赖方系统的设计思考和建议。

1）更新感知系统

将“更新感知”功能同“数据同步”功能进行解耦，是互联网内容分发范畴常见的工程设计思路。当这一思路被应用到RPKI体系时，更新感知系统便成为了一个独立的RPKI依赖方系统组件。该系统采用实时或不定时的方式获得RPKI资料库（RPKI数据发布点）的数据更新情况，并将这些更新信息传递给数据同步系统。

2）数据同步系统

数据同步系统以“全量”或“增量”的方式，将RPKI资料库内发布的各类RPKI资源证书及RPKI数字签名对象下载到本地网络，以形成与RPKI资料库一致的且具有一定时效的数据副本。在当前的RPKI生态中，数据同步系统和RPKI资料库之间的接口已经在IETF形成标准[5]。

3）数据验证系统

数据验证系统先后对相关证书及数据签名对象进行语法检查和RPKI逻辑验证。其中，语法检查包括检查相关数据格式是否符合技术标准、是否在有效期内等，RPKI逻辑验证包括验证PKI数字签名、验证相关的互联网码号资源包含关系[6]以及其他与RPKI授权体系相关的逻辑验证等。

4）数据分析系统

RPKI是一个分布式系统，因此位于不同RPKI授权体系子树上的数据可能存在冲突关系（码号资源分配、授权信息等）。数据分析系统旨在根据一定的算法，辅之以WHOIS数据、BGP广播存档数据等带外数据，对潜在的冲突关系进行检测，给出可能的（本地化）修正方案，并输出至本地控制系统。

5）本地控制系统

出于网络管理和安全保障的需求，网络运行机构可能希望以“本地过滤和添加”的形式建立RPKI路由认证数据的本地视图，对来自全球RPKI的数据进行覆盖。本地控制系统对“验证缓存”直接进行操作，增加或删减相关的路由认证数据条目。工业界将这种操作称为RPKI本地化控制（SLURM）。SLURM配置文件格式已经在IETF形成标准[7]。

6）数据分发系统

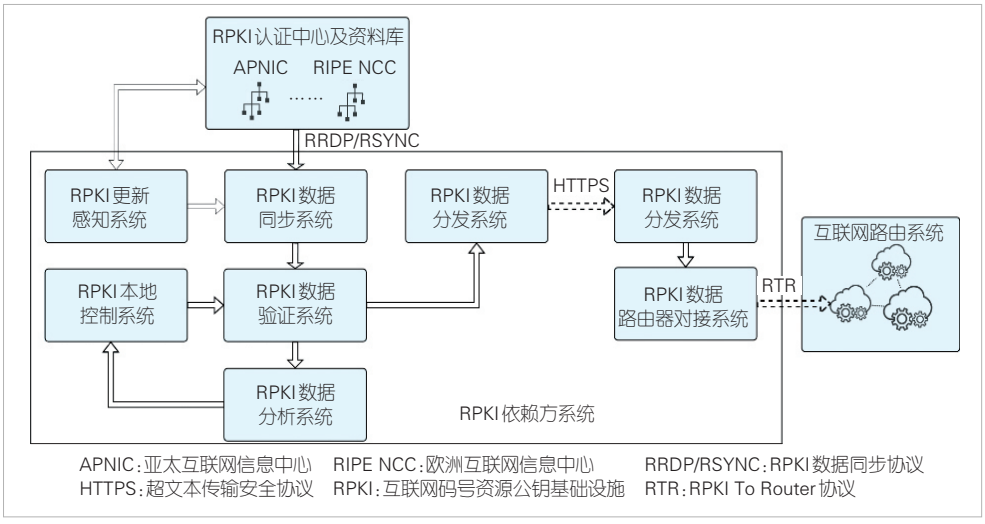
经过验证并最终可以供给路由器进行RPKI路由认证的数据称为“验证缓存”。基于“主从模型”，数据分发系统将“验证缓存”从一个网络节点分发至其他一个或多个有信任关系的网络节点，实现RPKI验证数据的共享。对于数据分发系统，RPKI意义上的数字签名已不复存在，其完整性依赖于传输信道（如超文本传输安全协议）。

7）路由器对接系统

RPKI供给侧形成的路由认证数据，通过同步、验证、分发、本地化处理，最终形成副本，然后经路由器对接系统，注入至BGP路由器。基于“客户端–服务器”操作模型，维护“验证缓存”的网络节点充当服务器，同时路由器充当客户端。两者之间的通信由一种RTR的IETF标准化协议承载[8]。

4 RPKI依赖方系统组件在规模网络上的编排机制

基于RPKI依赖方系统核心组件的解耦机制，本节探讨可扩展RPKI依赖方系统部署机制在“网络互联互通特征范

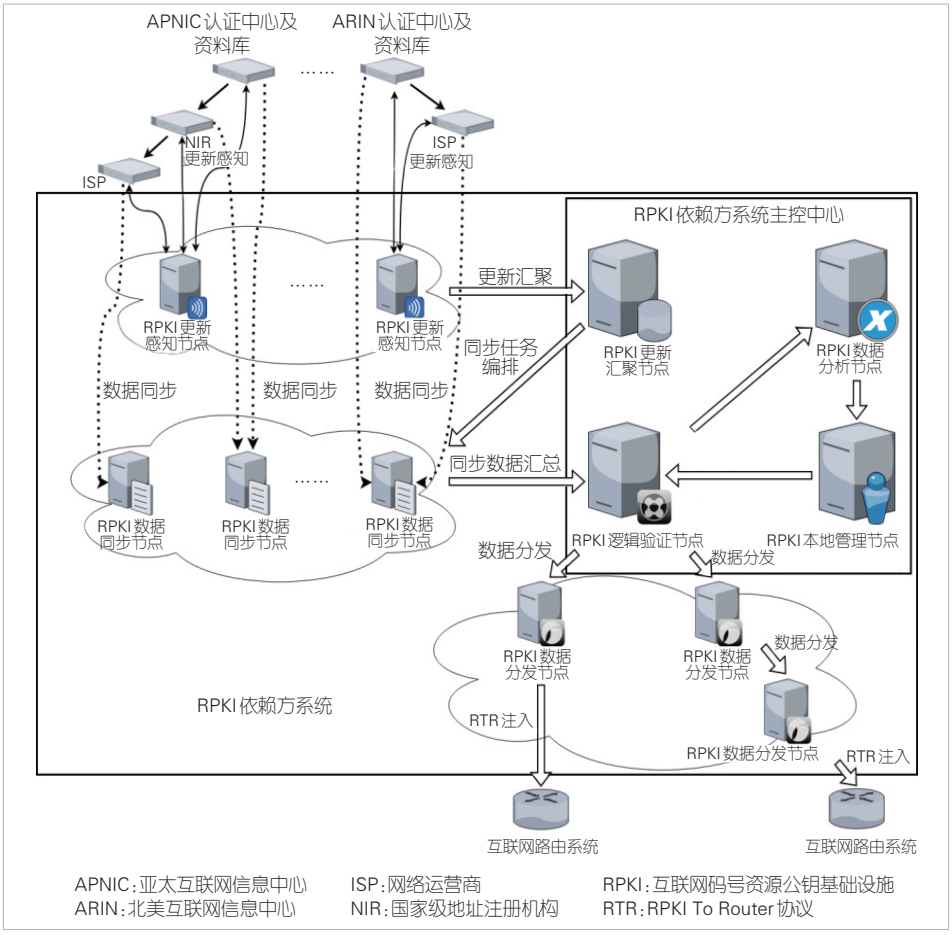


▲图3 RPKI依赖方系统组件

畴”的特殊性，就如何将相关组件编排在网络运行机构所管理的云和网的不同位置，设计一个能够适配各类规模网络（骨干网运营商、互联网交换中心、内容分发网络服务商等）的RPKI依赖方系统组件部署机制（框架）。

针对前文所述RPKI依赖方系统的4对矛盾，面向一个规模网络的一般特征，笔者建议在RPKI依赖方系统的组件颗粒度上展开相关设计，包括：一个RPKI依赖方系统北向分布式节点群组、一个RPKI依赖系统方南向分布式节点群组和一个RPKI依赖方系统主控中心。如图4所示，北向分布式节点群组面向RPKI供给侧，从分布式的RPKI资料库获取RPKI原始数据，包含RPKI更新感知节点和RPKI数据同步节点；南向分布式节点群组面向RPKI需求侧，将验证过的RPKI路由认证数据分发给分布式网络的边界路由器，即RPKI数据分发节点的集合；主控中心负责RPKI数据的验证和其他综合处理任务，包含RPKI更新汇聚节点、RPKI逻辑验证节点、RPKI本地管理节点、RPKI数据分析节点等。

RPKI依赖方系统的各个组件在该架构下的部署机制如下：



▲图4 规模网络上的RPKI依赖方系统组件部署示例

1）更新感知系统

鉴于RPKI资料库的全球分布特征，更新感知系统相应地采用分布式的更新获取方法。该系统拥有“更新感知模块”和“更新汇聚模块”。前者部署在分布式的“更新感知节点”之上。全体“更新感知节点”按照一定的编排算法各自分工，完成对RPKI资料库的遍历，并传递给负责整合更新信息的“更新汇聚节点”。“更新汇聚节点”再将更新信息传递至数据同步系统。

全球大型运营商（例如Tier 1 ISP）或头部流量的互联网交换中心，可以考虑将更新感知系统的寻址信息（域名、IP地址等）和接口方式公布出去，供相关的RPKI发布点主动推送更新信息。

2）数据同步系统

面向全球RPKI资料库的分布特征，数据同步系统也采用分布式的部署形态，根据一定的编排算法，将同步任务分散至不同的“数据同步节点”。“更新汇聚节点”负责运行该编排算法，在统筹更新任务来源、同步节点数量、同步节点分布位置等要素的前提下，实现同步任务的动态分配。多个“数据同步节点”的分布采用和“更新感知节点”类似的策略。

3）数据验证系统

面向RPKI的数据验证系统的核心是建立数据对象之间的关联，包括经典公钥基础设施（PKI）体系下的数字签名验证路径构建，以及RPKI特有的码号资源包含关系验证。这种“关联性”的验证任务（证书路径验证、资源包含关系验证）由数据验证系统的RPKI逻辑验证模块负责。该模块站在全局视角，以集中化的方式对来自不同“数据同步节点”的合规数据进行综合处理，并以“RPKI逻辑验证节点”的形式部署在网络运行机构的网运中心（NOC）。数据验证系统的语法检查模块不涉及对数据关联性的验证，可以部署在“数据同步节点”之上，对相关数据进行语法合规检查，实现“边同步，边语法检查”的高效机制。合规数据会汇聚至“RPKI逻辑验证节点”。

4）数据分析系统

数据分析系统承担的是RPKI数据同步、验证等任务之外的旁路功能，宜独立部署在专用的RPKI数据分析节点之中。

5）本地控制系统

本地控制系统将连同其他一些面向RPKI的互联网码号资源本地管理支撑系统（可视化、运行监控等），部署在专用的RPKI本地管理节点之中。

6）数据分发系统

鉴于数据分发系统的核心任务是将RPKI验证缓存从集中管理的RPKI依赖方系统主控节点分发至分布式部署的路由控制系统，其部署节点宜根据网络运行机构所辖自治域的数量和管理机制进行规划，以方便BGP边界路由器在就近获取RPKI验证缓存的同时，在网络运行机构的网络管理边界之内形成一致的RPKI数据视图。数据分发系统部署在数据分发节点之上，并根据该系统所定义的“主从模型”使相关节点（“分发服务器模块”与“分发客户端模块”）形成一个有序的数据共享体系。

7）路由器对接系统

路由器对接系统部署在面向路由器服务的末梢数据分发节点之上。

RPKI依赖方系统主控中心可部署在网络运行机构的NOC之中。北向分布式节点群组的节点数量和分布规则，可结合网络拓扑以及去RPKI资料库之“远近”（路由及寻址）情况量体裁衣。南向分布式节点群组的节点数量和分布规则，可参考网络运行机构的网络互联互通情况和管理机制进行规划设计。

5 总结与展望

RPKI依赖方系统连接RPKI供给侧和RPKI需求侧，是各类网络运行机构开展RPKI应用实践的一个关键环节。RPKI依赖方系统的研发和部署，既需要关注RPKI核心功能的“普遍性”问题，又需要兼顾网络互联互通特征的“特殊性”问题。相关解决方案需要考虑RPKI依赖方系统有哪些组件，各个组件如何在网络上分布，以及以何种逻辑关系分布。因此，各类网络运行机构使用RPKI依赖方系统实施路由认证，不仅是简单的软硬件集成，更需要设计能够“因地制宜”涵盖功能编排、部署方法及运行机制的一揽子解决方案。

面向RPKI依赖方系统的核心功能，本文梳理了影响RPKI依赖方系统运行效能的4对矛盾，并提出了一种可扩展的RPKI依赖方系统部署机制，包含软件层面的解耦机制和硬件层面的部署机制。本文相关论述是对RPKI依赖方系统在规模网络运行机构内进行服务模式设计的宏观思考。骨干网运营商、CDN服务商和互联网交换中心，在互联互通格局和码号资源管理等范畴具有不同特征。面向这些特征，探索如何在现有网络运维管理系统上增量部署RPKI依赖方系统组件以及对应的运行机制，是RPKI路由认证领域下一步值得深入研究的问题。

参考文献

[1] IAB. IAB statement on the RPKI [EB/OL]. [2022-11-25]. https://www.iab.org/documents/correspondence-reports-documents/docs2010/iab-statement-on-the-rpki/
[2] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP) [J]. IEEE journal on selected areas in communications, 2000, 18(4): 582-592. DOI: 10.1109/49.839934
[3] LYNN C, KENT S, SEO K X. 509 extensions for IP addresses and AS identifiers [EB/OL]. [2022-11-25]. http://mirror. cogentco. com/pub/rfc/pdf/rfc3779.txt.pdf
[4] MA D, KENT S. Requirements for resource public key Infrastructure (RPKI) relying parties [EB/OL]. [2022-11-25]. https://www.ietf.org/rfc/rfc8897.pdf
[5] BRUIJNZEELS T, MURAVSKIY O, WEBER B, et al. The RPKI repository delta protocol (RRDP) [EB/OL]. [2022-11-25]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8182.txt.pdf
[6] HUSTON G, MICHAELSON G, MARTINEZ C, et al. Resource public key infrastructure (RPKI) validation reconsidered [EB/OL]. [2022-11-25]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8360.txt.pdf
[7] MA D, MANDELBERG D, BRUIJNZEELS T. Simplified local Internet number resource management with the RPKI (SLURM) [EB/OL]. [2022-11-25]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8416.txt.pdf
[8] BUSH R, AUSTEIN B. RPKI to router protocol [EB/OL]. [2022-11-25]. https://www.rfc-editor.org/rfc/pdfrfc/rfc8210.txt.pdf

作 者 简 介

马迪，互联网域名系统国家地方联合工程研究中心（ZDNS）首席研究员、中国科学院大学研究生导师、国家（杭州）新型互联网交换中心高级顾问、中国电信集团“基于IPv6的电信网络技术北京市重点实验室”学术委员会委员、国际互联网码号资源理事会（NRO NC/ICANN ASO AC）委员、亚太互联网信息中心（APNIC）路由安全SIG联合创始人、国际互联网工程任务组（IETF）域名领域技术标准评审专家委成员、国际互联网名称与码号分配机构（ICANN）域名根服务器咨询委员会核心专家组成员；撰写了3项RPKI相关IETF RFC（RFC8211、RFC8416、RFC8897）；研究方向包括互联网体系结构、互联网寻址定位技术等。