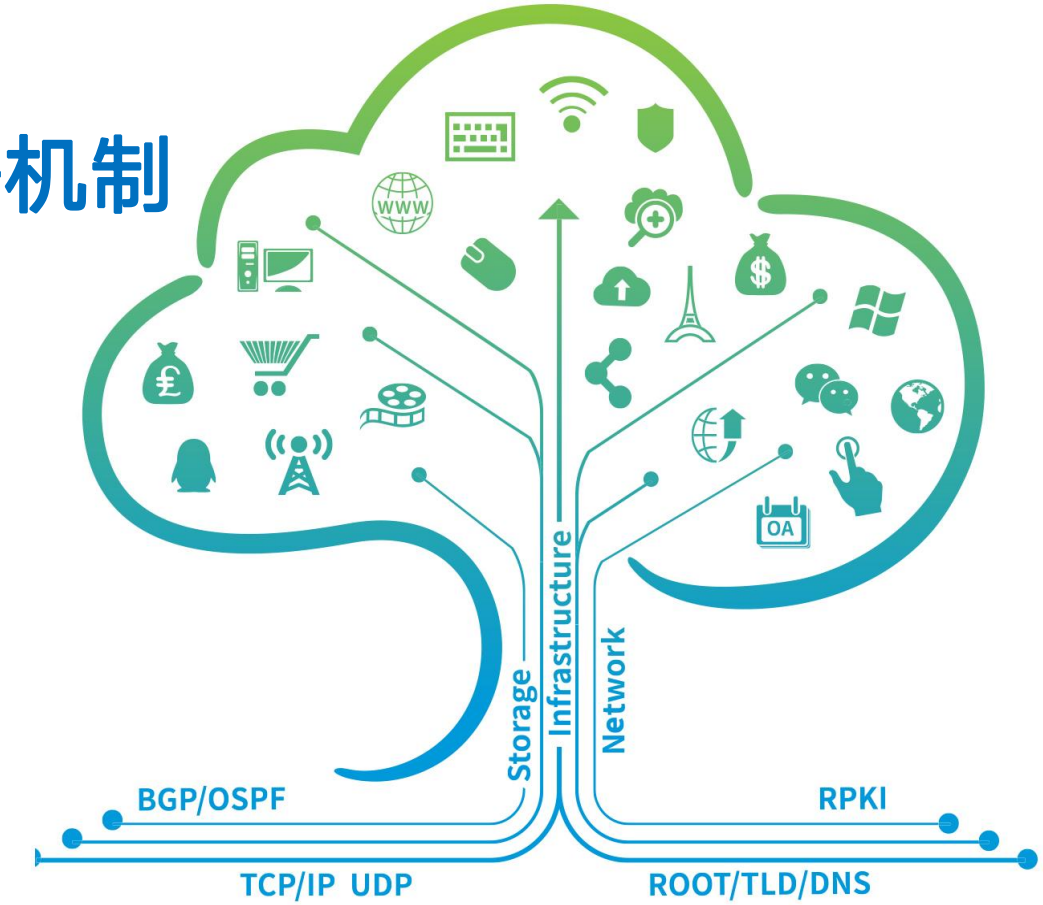
互联网域名系统国家工程研究中心

构建可扩展的RPKI依赖方系统部署机制

马　迪

互联网域名系统国家工程研究中心

madi@zdns.cn



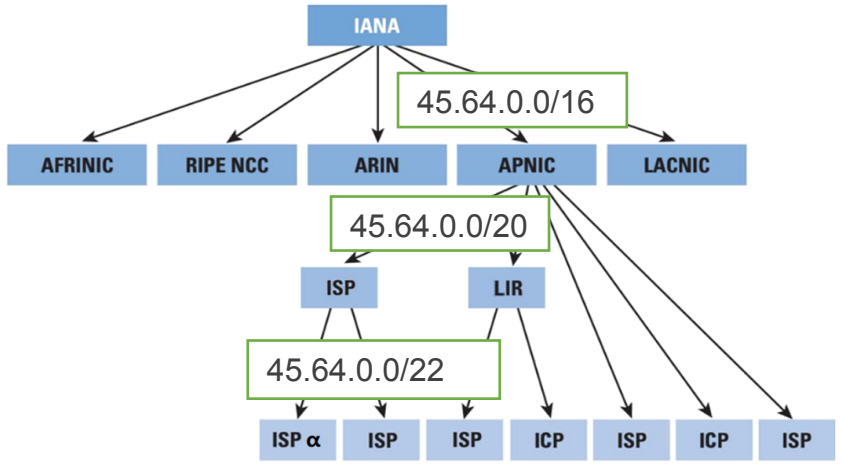
2023.11.28，福州

CERNET学术年会 2023

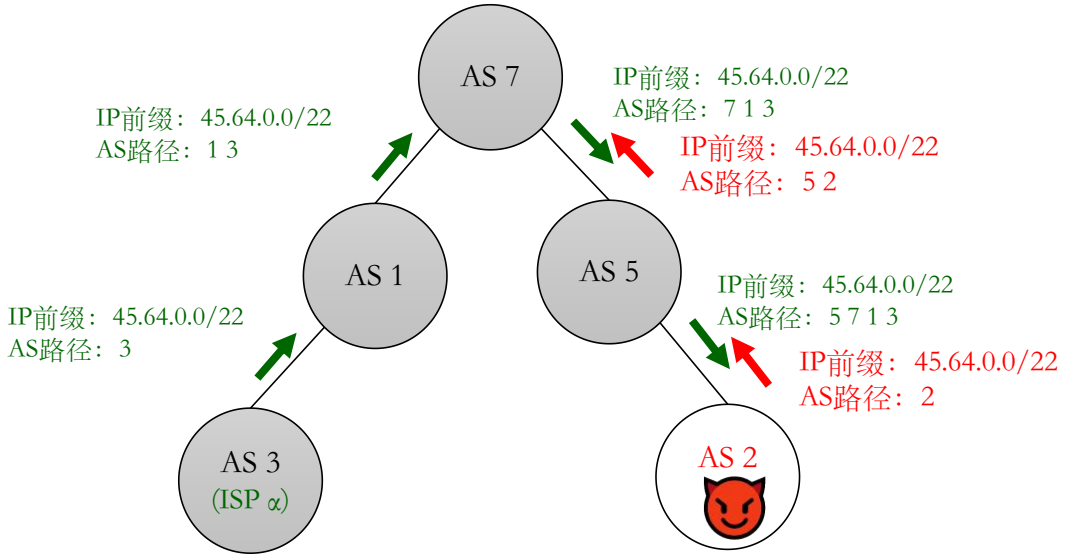
BGP的内生安全缺陷催生RPKI

互联网域名系统国家工程研究中心

地址分配示意图



路由通告示意图

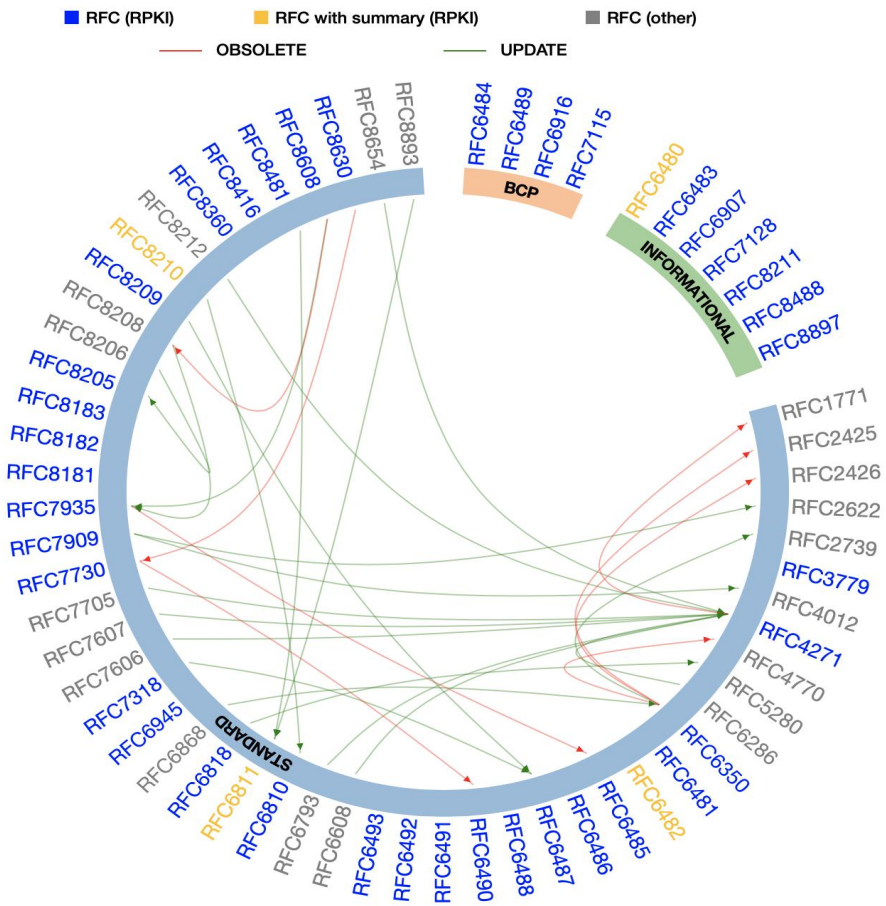


RPKI = Resource Public Key Infrastructure，　互联网码号资源公钥基础设施

IETF在技术标准层面定义RPKI

互联网域名系统国家工程研究中心

RPKI基础标准创制工作基本完成，相关标准化工作的重点迁移至RPKI部署运行机制。



Secure Inter-Domain Routing (sidr) Concluded WG

About | Documents | Meetings | History | Photos | Email expansions | List archive » | Tools »

Note: The data for concluded WGs is occasionally incorrect.

WG	Name	Secure Inter-Domain Routing
	Acronym	sidr
	Area	Routing Area (rtg)
	State	Concluded
	Charter	charter-ietf-sidr-04 Approved
	Status Update	Show update (last changed 2016-11-16)
	Dependencies	Document dependency graph (SVG)
	Additional Resources	- Issue tracker - Wiki
Personnel	Chairs	Chris Morrow Sandra Murphy
	Area Director	Alvaro Retana
	Tech Advisor	Steven Bellovin
Mailing list	Address	sidr@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/sidr
	Archive	https://mailarchive.ietf.org/arch/browse/sidr/

SIDR Operations (sidrops)

About | Documents | Meetings | History | Photos | Email expansions | List archive » | Tools »

WG	Name	SIDR Operations
	Acronym	sidrops
	Area	Operations and Management Area (ops)
	State	Active
	Charter	charter-ietf-sidrops-01 Approved
	Dependencies	Document dependency graph (SVG)
	Additional Resources	- Issue tracker - Wiki
Personnel	Chairs	Chris Morrow Keyur Patel
	Area Director	Warren Kumari
	Secretary	Nathalie Trenaman
Mailing list	Address	sidrops@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/sidrops
	Archive	https://mailarchive.ietf.org/arch/browse/sidrops/
Jabber chat	Room address	xmpp:sidrops@jabber.ietf.org?join
	Logs	https://jabber.ietf.org/logs/sidrops/

[2006] IETF SIDR（域间路由安全）工作组成立

[2012] IETF发布14个关于RPKI核心协议的RFC （RFC6480~RFC6493）

[2017] BGPsec相关标准发布（RFC8205~RFC8211）；IETF SIDR-OPS工作组成立

https://rpki-rfc.routingsecurity.net

RPKI是ISOC倡导的全球路由安全防护协定的关键条款

互联网域名系统国家工程研究中心

MANRS

Now, more than ever, we need a more resilient Internet. Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

Action 4: Facilitate routing information on a global scale – RPKI

A network operator should create a valid Route Origination Authorization (ROA) for each IP prefix or set of prefixes it is legitimately authorised and intends to originate.

Discussion:

The most secure method of facilitating validation on a global scale is through the RPKI system which allows their routing announcements to be cryptographically verified. Network operators can obtain RPKI certificates for their own IP prefixes from the RIRs that allocated them, and then generate, publish, and maintain Route of Origin Authorizations (ROAs) corresponding to the IP prefixes they announce. Network operators must also encourage their Customer Network operators to do so as well.

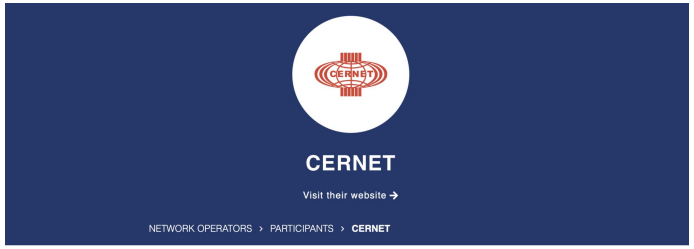
References:

- Origin Validation Operation based on the Resource Public Key Infrastructure (RPKI) – http://www.rfc-editor.org/bcp/bcp185.txt

ISOC（国际互联网协会）于2014年发起“互联网路由安全自律协定（MANRS）”，对ISP/ICP/IXP均作出支持RPKI 路由认证的要求。

中国大陆地区加入MANRS的网络运行机构

互联网域名系统国家工程研究中心



中国教育网

Participant Info

AREAS SERVED
CN

ASNS
4538

Implementation of MANRS Actions

- ACTION 1: PREVENT PROPAGATION OF INCORRECT ROUTING INFORMATION
- ACTION 2: PREVENT TRAFFIC WITH SPOOFED SOURCE IP ADDRESSES
- ACTION 3: FACILITATE GLOBAL OPERATIONAL COMMUNICATION AND COORDINATION
- ACTION 4: FACILITATE VALIDATION OF ROUTING INFORMATION ON A GLOBAL SCALE

国家互联网交换中心（杭州）

Participant Info

LOCATION
CN

NETWORK ASNS
139136

IX-F IDS

Implementation of MANRS Actions

- ACTION 1: FILTERING OF ROUTE ANNOUNCEMENTS
  https://www.nnix.cn/#/support/bgp We have applied the RPKI and whitelist filters to ensure the network security.
- ACTION 2-1: OFFER ASSISTANCE TO ITS MEMBERS TO MAINTAIN ACCURATE ROUTING INFORMATION IN AN APPROPRIATE REPOSITORY (IRR AND/OR RPKI)
  We have applied the RPKI and whitelist filters to ensure the network security. We can offer technical support if others required.
- ACTION 3: PROTECT THE PEERING PLATFORM
  We have published an official policy named "IXP access technology requirement": https://www.nnix.cn/#/knowledgeColumn/article1?id=28
- ACTION 4: FACILITATE GLOBAL OPERATIONAL COMMUNICATION AND COORDINATION BETWEEN NETWORK OPERATORS
  We have a member list available to all members of the exchange.
- ACTION 5: PROVIDE MONITORING AND DEBUGGING TOOLS TO THE MEMBERS
  Our looking glass is on the roadmap，we can provide several other tools on our website such as this link: https://www.nnix.cn/#/realOrFalseBGP

中国电信

Participant Info

AREAS SERVED
AE, AU, CN, DE, GB, HK, JP, KE, NL, RU, SG, US, ZA

ASNS
4134

Implementation of MANRS Actions

- ACTION 1: PREVENT PROPAGATION OF INCORRECT ROUTING INFORMATION
  CT/AS4134 prevents propagation of incorrect routing information.
- ACTION 2: PREVENT TRAFFIC WITH SPOOFED SOURCE IP ADDRESSES
  CT prevents traffic with spoofed source IP addresses.
- ACTION 3: FACILITATE GLOBAL OPERATIONAL COMMUNICATION AND COORDINATION
  CT facilitates global operational communication and coordination between network operators.
- ACTION 4: FACILITATE VALIDATION OF ROUTING INFORMATION ON A GLOBAL SCALE
  CT facilitates validation of routing information on a global scale.

中国科技网

Participant Info

AREAS SERVED
CN

ASNS
7497

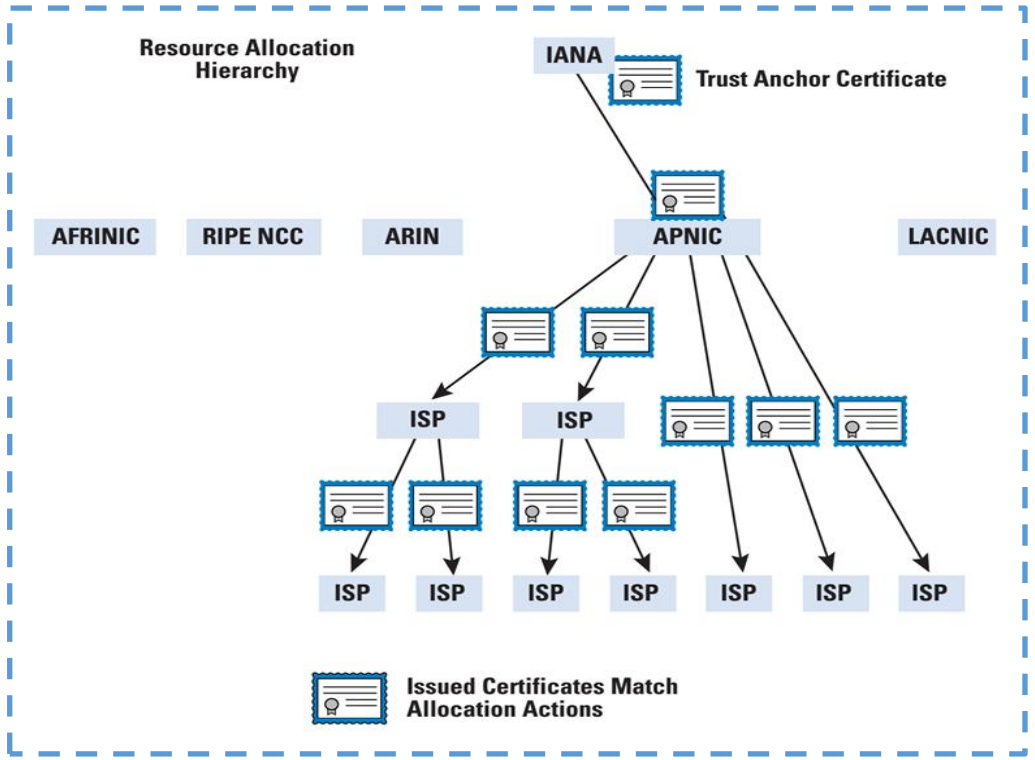
Implementation of MANRS Actions

- ACTION 1: PREVENT PROPAGATION OF INCORRECT ROUTING INFORMATION
- ACTION 3: FACILITATE GLOBAL OPERATIONAL COMMUNICATION AND COORDINATION
- ACTION 4: FACILITATE VALIDATION OF ROUTING INFORMATION ON A GLOBAL SCALE

RPKI技术原理

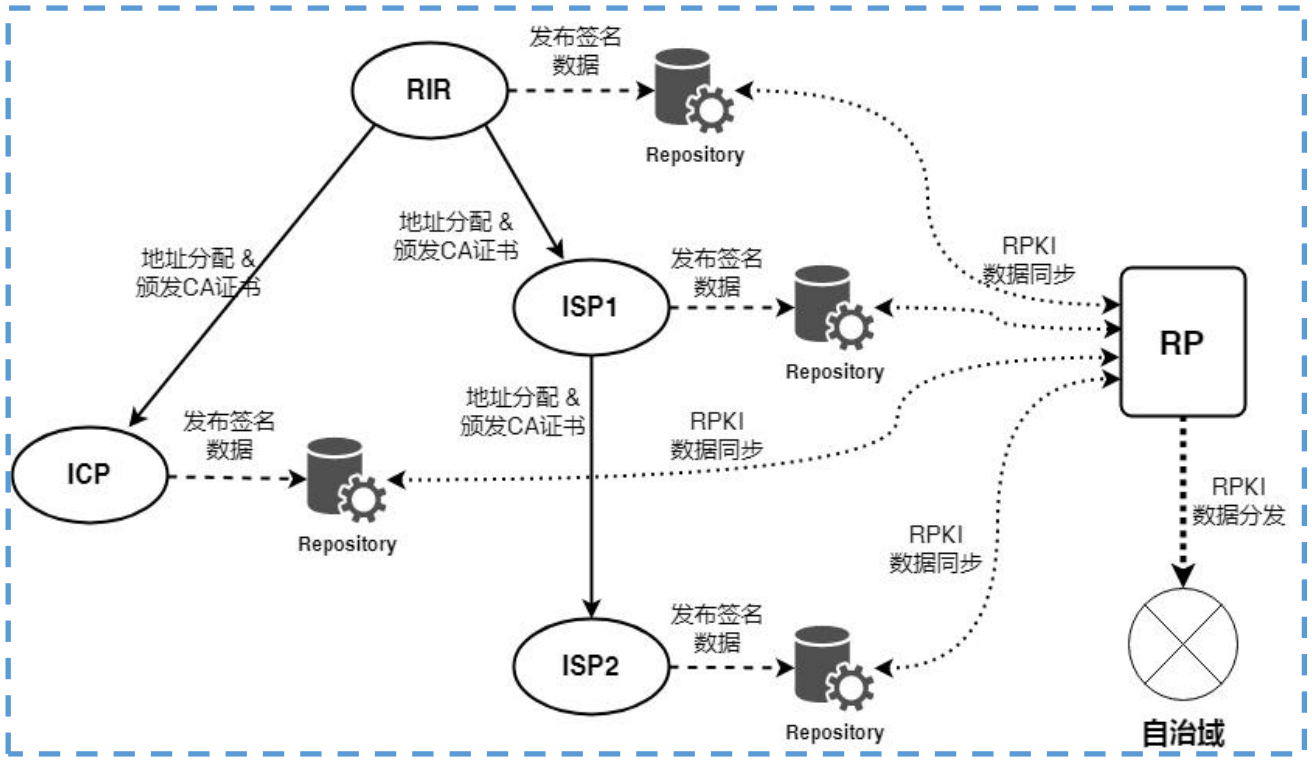
互联网域名系统国家工程研究中心

分配关系决定认证关系。



RPKI认证体系

第三方的带外信任锚点参与路由决策。



RPKI运行机制

- ✓ **基于RPKI的BGP路由起源验证: ROV (IETF RFC 6811)**
- ✓ **基于RPKI的BGP路径认证：BGPsec (IETF RFC 8205)，ASPA（draft-ietf-sidrops-aspa-verification-09）**

RPKI数据快速覆盖全球IP地址空间

互联网域名系统国家工程研究中心

RPKI启动部署10年以来，在IPv4和IPv6两个地址空间的覆盖率稳步上升

date	RIR	IPv4 adoption	IPv6 adoption
20231122	ripencc	0.6526	0.3745
20231122	arin	0.3102	0.6619
20231122	afrinic	0.2788	0.0764
20231122	apnic	0.3442	0.2351
20231122	lacnic	0.4983	0.4899

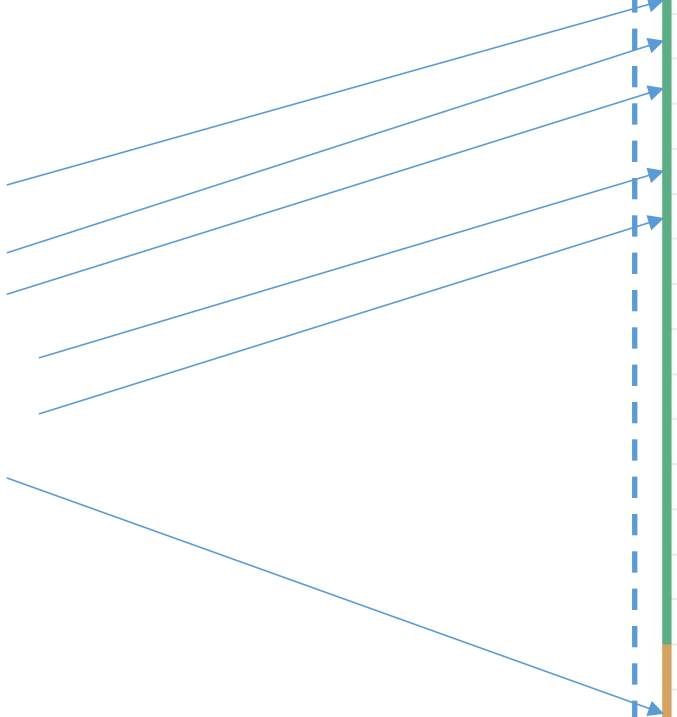
数据来源：国际互联网码号资源组织 NRO（截止到2023年11月22 日） https://www.nro.net/about/rirs/statistics

各类网络运行机构使用RPKI发布和验证路由

互联网域名系统国家工程研究中心

RPKI发挥作用的关键：网络运行机构“信任和依赖”它来验证彼此之间的“互联互通”信息。

Tier 1 ISP

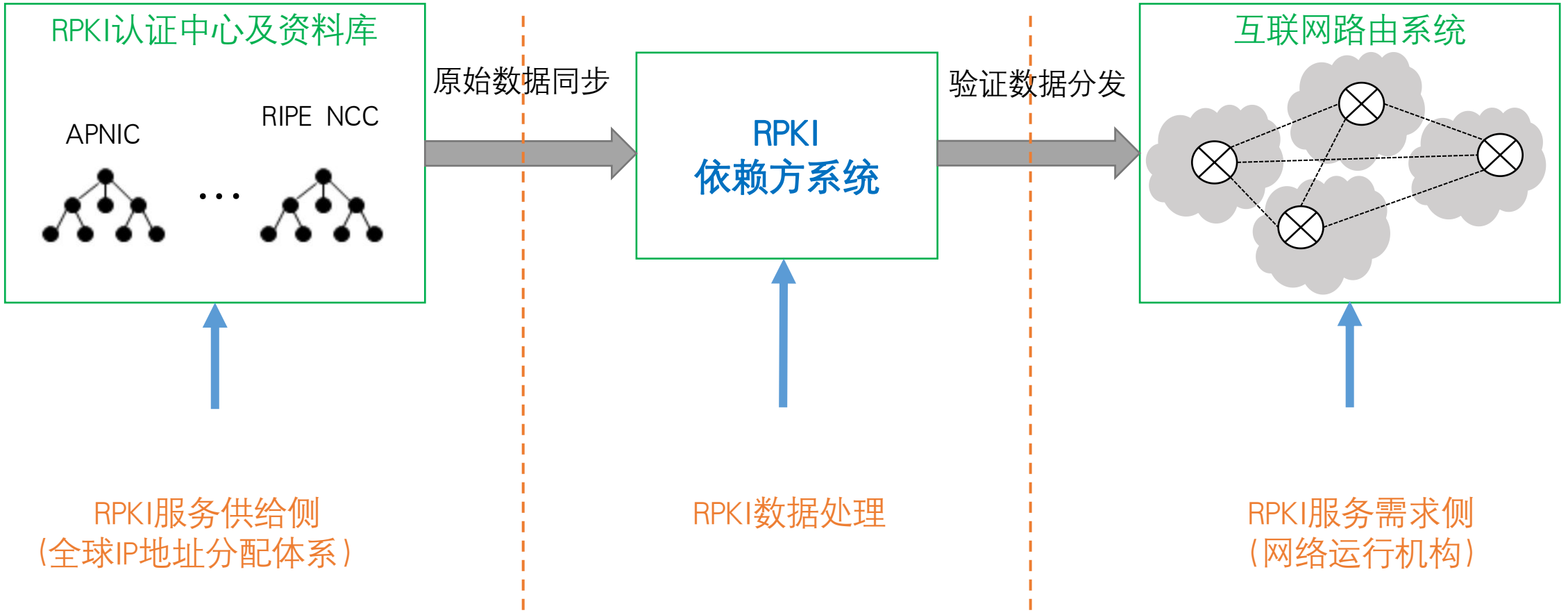


NAME	TYPE	DETAILS	STATUS
Lumen	transit	signed + filtering	safe
Arelion (Formally Telia)	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe
Telstra International	transit	signed	partially safe
AT&T	ISP	signed + filtering peers only	partially safe
Liberty Global	transit	signed + filtering peers only	partially safe
Google	cloud	signed	partially safe
DigitalOcean	cloud	filtering peers only	partially safe

数据来源：美国CDN服务商Cloudflare https://isbgpsafeyet.com

RPKI依赖方系统是连接供给和需求之间的桥梁

互联网域名系统国家工程研究中心



RPKI依赖方系统技术标准条款汇总：RFC8897

互联网域名系统国家工程研究中心

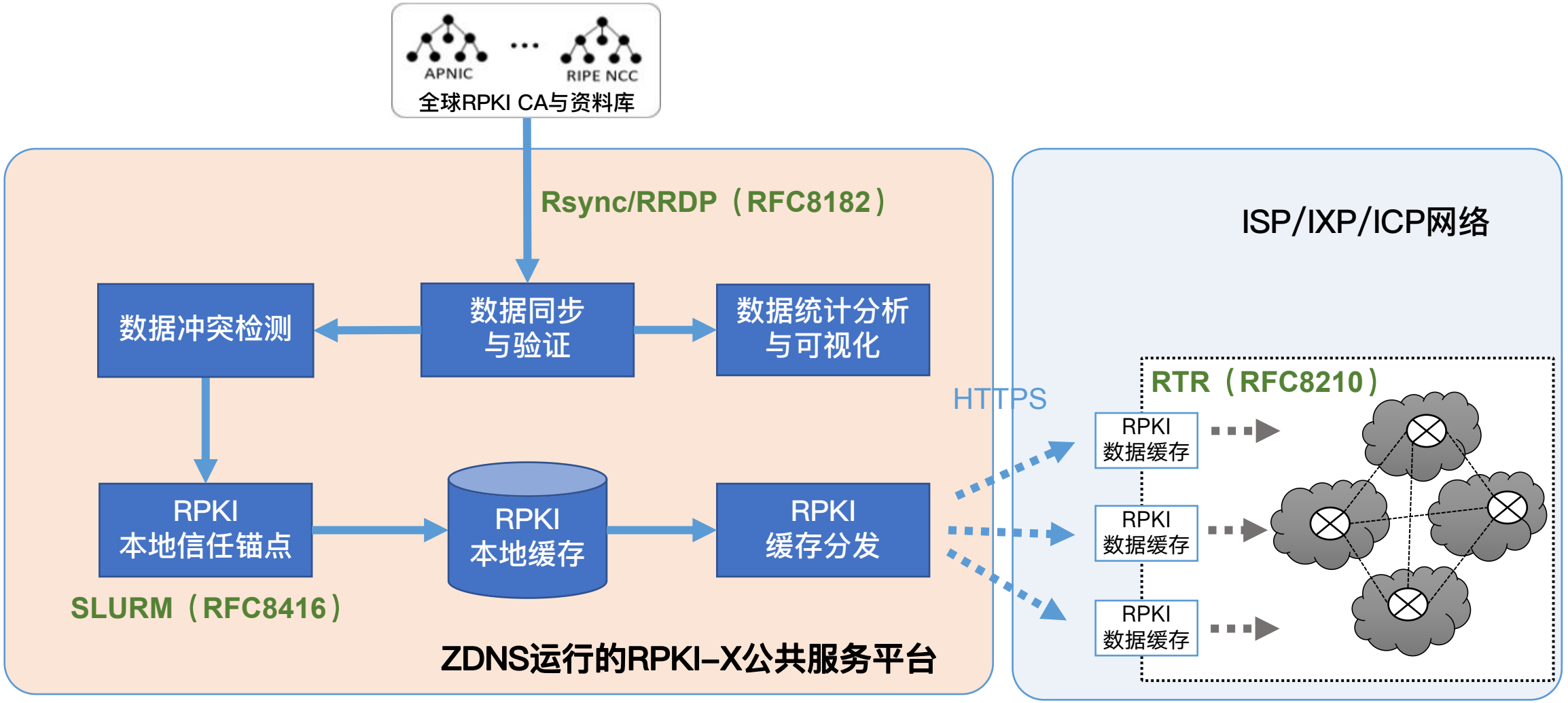
Stream: Internet Engineering Task Force (IETF)
RFC: 8897
Category: Informational
Published: September 2020
ISSN: 2070-1721

Authors: D. Ma *ZDNS* S. Kent *Independent*

RFC 8897
Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties

RPKI依赖方系统的云服务实践：RPKI-X

互联网域名系统国家工程研究中心



2019年，ZDNS和中国科技网进行了系统对接与测试。

2020年，ZDNS和国家新型互联网交换中心（杭州）进行了系统对接测试。

影响RPKI依赖方系统运行效能的四对矛盾

互联网域名系统国家工程研究中心

RPKI依赖方系统的核心目标：将RPKI数据尽可能快速、完整、准确地从供给侧扩散至需求侧。

- ✓ 矛盾1：RPKI资料库（发布点）越来越多，与实时感知全球RPKI数据更新之间的矛盾。
- ✓ 矛盾2：RPKI数据对象越来越多，与快速同步全球RPKI数据之间的矛盾。
- ✓ 矛盾3：RPKI认证链越来越复杂，与快速构建全球RPKI数据验证路径之间的矛盾。
- ✓ 矛盾4：RPKI依赖方系统越来越集中化，与路由器快速获得RPKI验证数据之间的矛盾。

化解RPKI依赖方系统运行效能矛盾的方法

矛盾在“RPKI基本原理范畴”的普遍性

模块组件设计

矛盾在“网络互联互通特征范畴”的特殊性

部署方案设计

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
逻辑关系分布。

可扩展的RPKI依赖方系统：功能组件正交 + 编排机制因应网络规模和特征差异

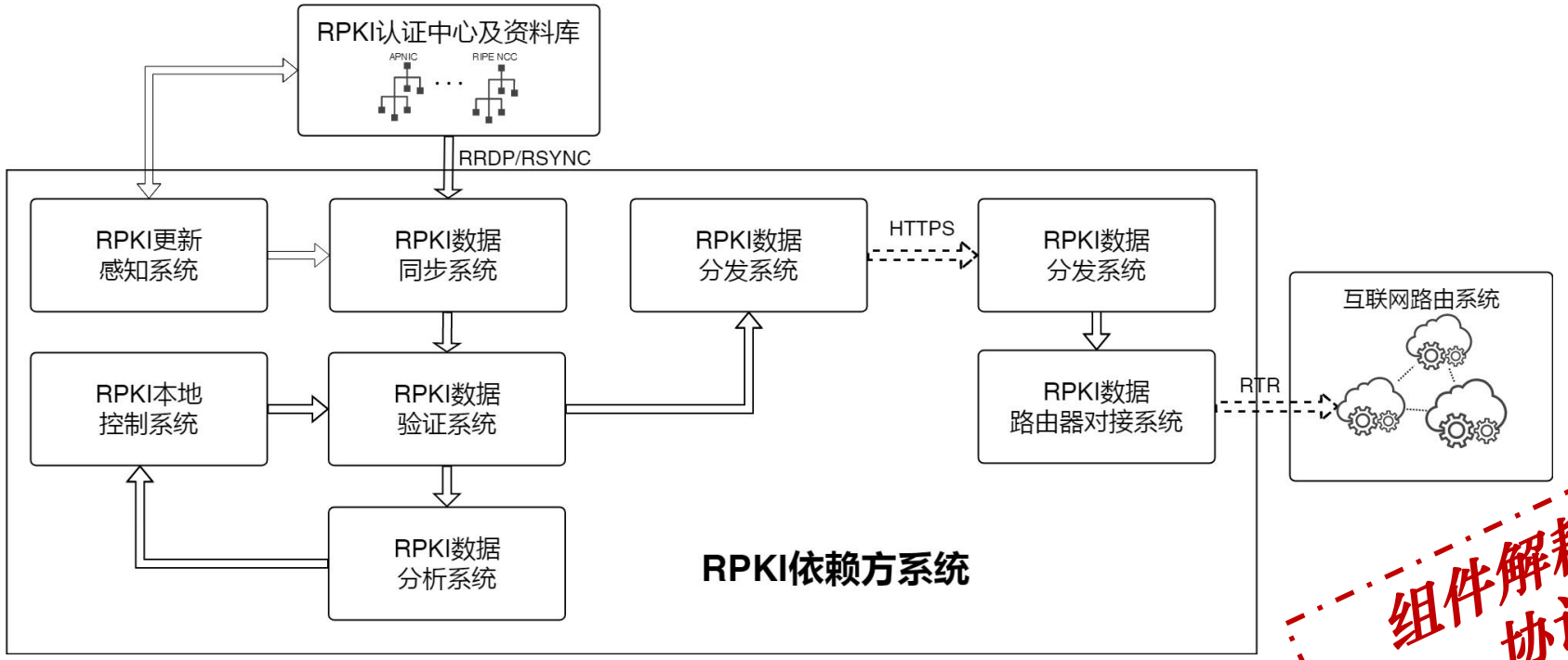
RPKI依赖方系统组件的功能解耦机制 1/2

互联网域名系统国家工程研究中心

可扩展的RPKI依赖方系统部署机制在“RPKI基本原理范畴”的任务：

通过对RPKI依赖方系统核心功能实施拆解，形成彼此“正交”的RPKI依赖方系统的组件集合。

- ✓ 更新感知系统
- ✓ 数据同步系统
- ✓ 数据验证系统
- ✓ 数据分析系统
- ✓ 本地控制系统
- ✓ 数据分发系统
- ✓ 路由器对接系统



组件解耦，支撑协议接口

RPKI依赖方系统组件的功能解耦机制 2/2

互联网域名系统国家工程研究中心

✓ **在组件解耦的基础上，实现组件之内功能模块之解耦。**

- 更新感知系统=“更新感知模块”+“更新汇聚模块”
- 数据验证系统=“语法检查模块”+“RPKI逻辑验证模块”
- 数据分发系统=“分发服务器模块”+“分发客户端模块”

✓ **在不同的网络节点上，对来自不同组件的功能模块进行适配。**

- 同一系统的不同模块，可以位于不同物理节点之上

模块解耦，支撑节点适配

RPKI依赖方系统组件在网络上的编排机制 1/2

互联网域名系统国家工程研究中心

可扩展的RPKI依赖方系统部署机制在“网络互联互通特征范畴”的任务：

面向规模网络的一般特征，在RPKI依赖方系统的“组件颗粒度”上实施功能模块的分布设计。

- ✓ 更新感知系统
- ✓ 数据同步系统
- ✓ 数据验证系统
- ✓ 数据分析系统
- ✓ 本地控制系统
- ✓ 数据分发系统
- ✓ 路由器对接系统

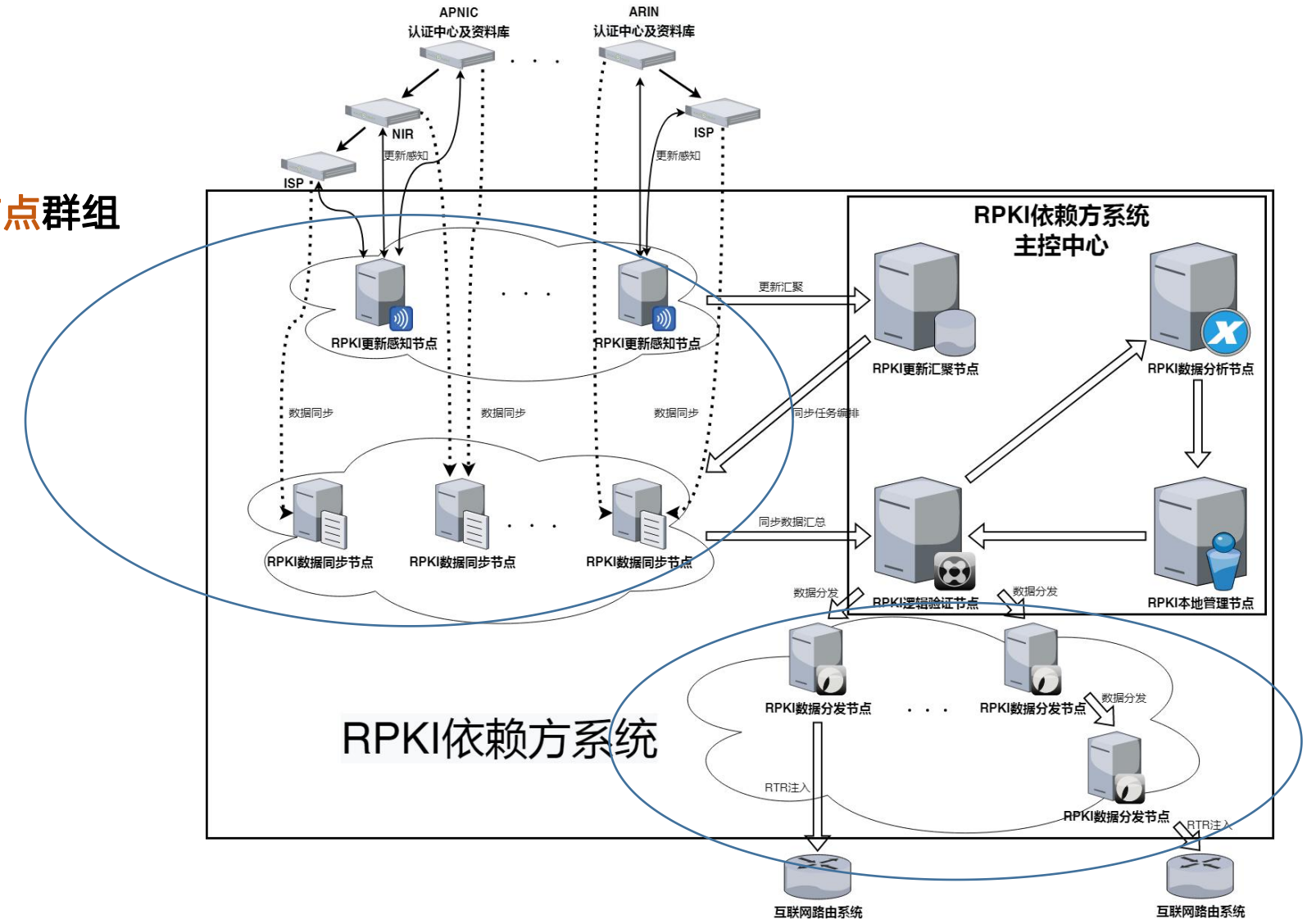
由“功能域” 至“网络域” 的映射

- ✓ 一个RPKI依赖方系统北向分布式节点 群组
  - 更新感知节点（群组）
  - 数据同步节点（群组）
- ✓ 一个RPKI依赖方系统南向分布式节点 群组
  - 数据分发节点（群组）
- ✓ 一个RPKI依赖方系统主控中心
  - 更新汇聚节点
  - 数据分析节点
  - 逻辑验证节点
  - 本地管理节点

RPKI依赖方系统组件在网络上的编排机制 2/2

互联网域名系统国家工程研究中心

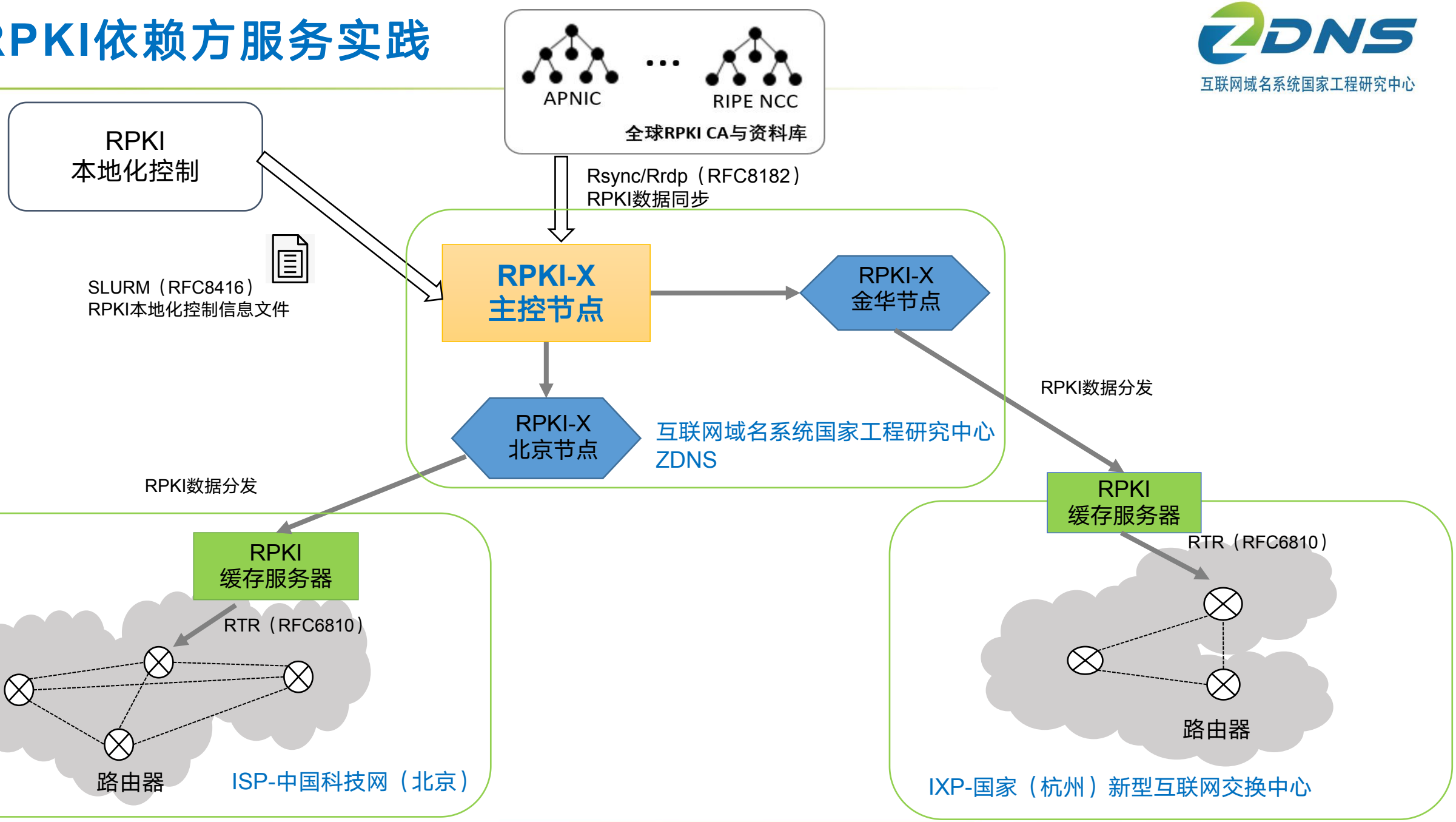
北向分布式节点群组



南向分布式节点群组

RPKI依赖方服务实践

互联网域名系统国家工程研究中心



总结

- ✓ 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“特殊性”问题。
  - ✓ 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及以何种逻辑关系分布。
- ✓ 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。

让网络服务更安全 更高效 更智能

Thanks !

欢迎关注官方微信
了解更多行业信息