



浅议互联网基础资源服务架构

王伟

ICANN公共技术标识符 (PTI) 董事

互联网基础资源，是支撑互联网上层应用算力、码号、协议、标准等要素的总和。从这个定义出发，它广义涵盖了传统的互联网物理基础设施（机房空间、网络带宽、计算存储、CDN等）、狭义针对以域名、IP、证书、时间为主的数字对象及其逻辑服务设施，也面向未来拥抱诸如分布式账本/区块链、开源代码等新兴要素。

互联网业务应用

电子商务、电子政务、网络游戏、视频通讯



互联网基础信息

IP服务、DNS服务、WEB证书、NTP服务等



互联网物理设施

基础网络、传输设备、互联设备、接入系统等



支撑网络实体（Cyber Entity）开展实际业务应用所必须的码号占用/释放、相互寻找识别、路选定位、验证信用信息等功能。

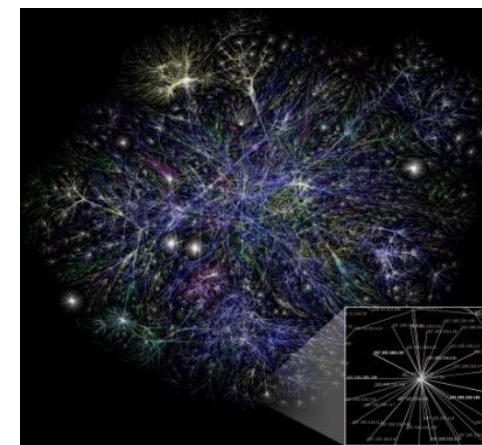
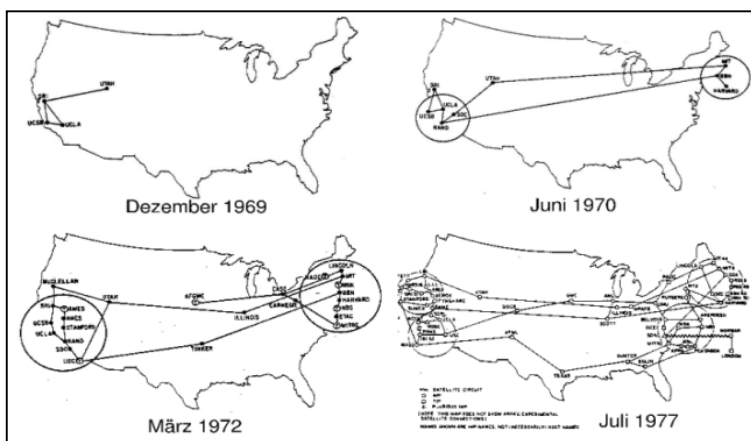
- 以地址分配和路由为代表的IP服务
- 以域名注册和查询为代表的DNS服务
- 以证书发放为代表的CA服务
- 以时间溯源和同步为代表的NTP服务

互联网重要的逻辑基础设施

互联网的中枢神经系统和调度支撑系统。

互联网基础资源的保障互联网稳定安全运行的基石，是促进互联网应用健康有序发展的杠杆，也是推动全球互联网治理工作的核心领域。

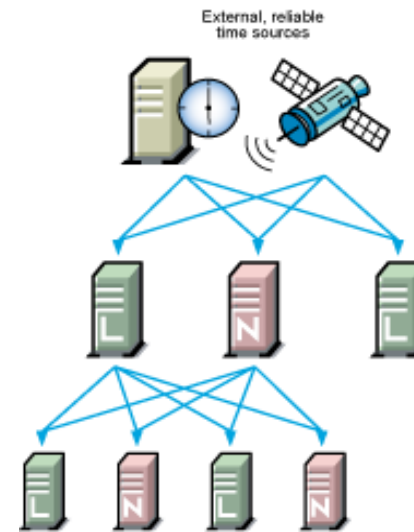
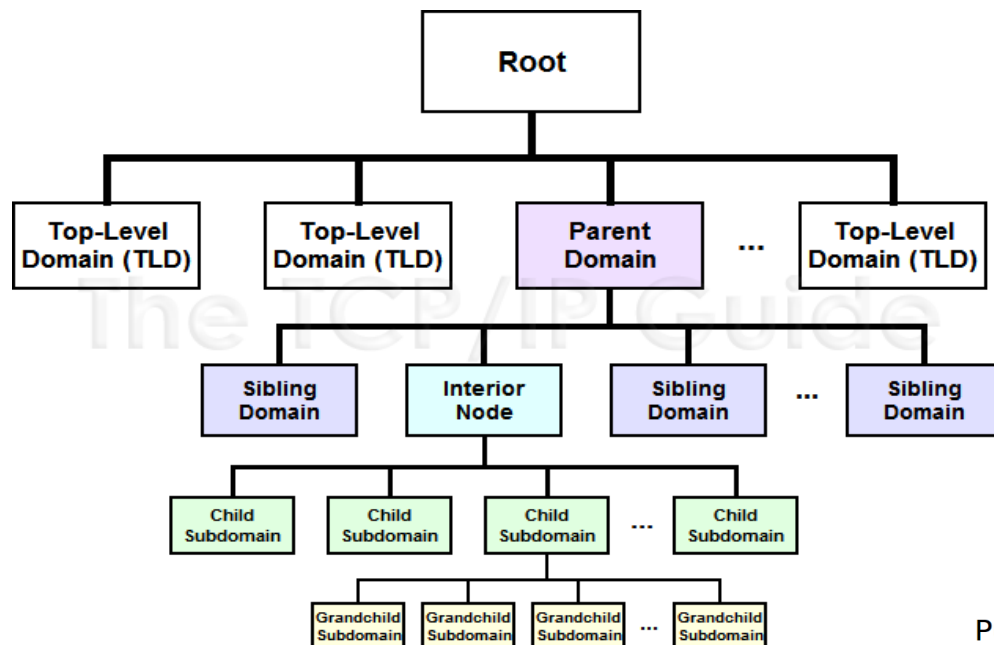
- 冷战催生的简化的、无需链路控制的、缺乏安全和信用机制网络，发展为支撑全球化的、跨边界的、与社会经济活动紧密融合的复杂环境。



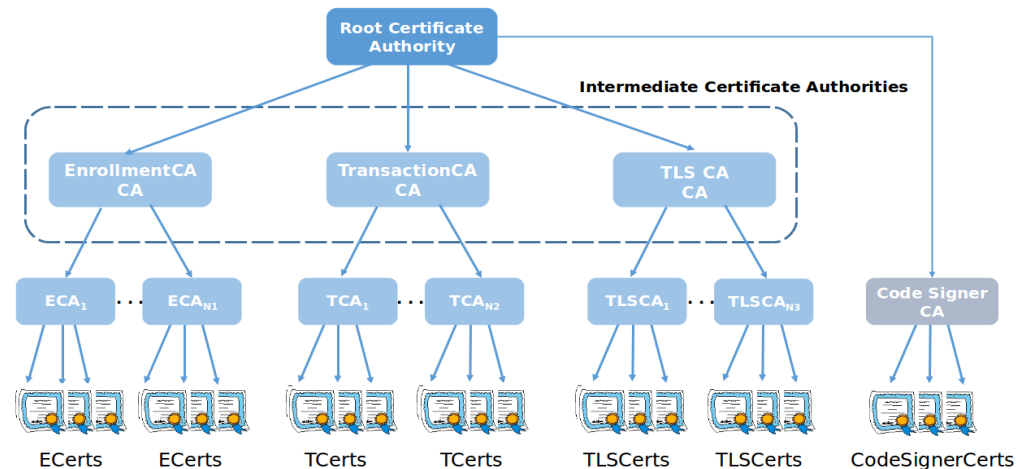
简化的、边界明晰的、用户互信的 >> 全球化的、无界的、紧密融合的

便于自顶向下的管控
树状结构的业务体系和管理架构

DNS

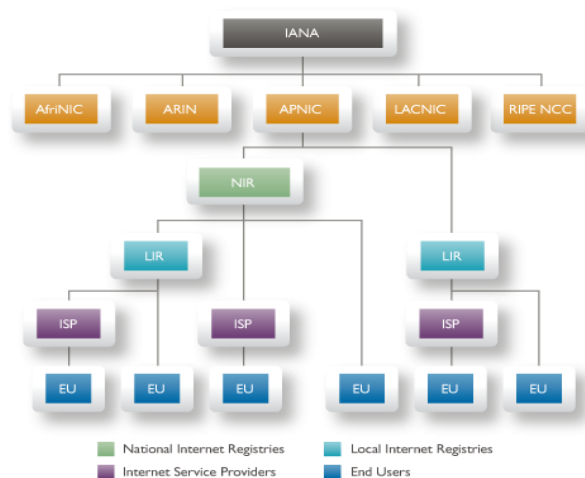


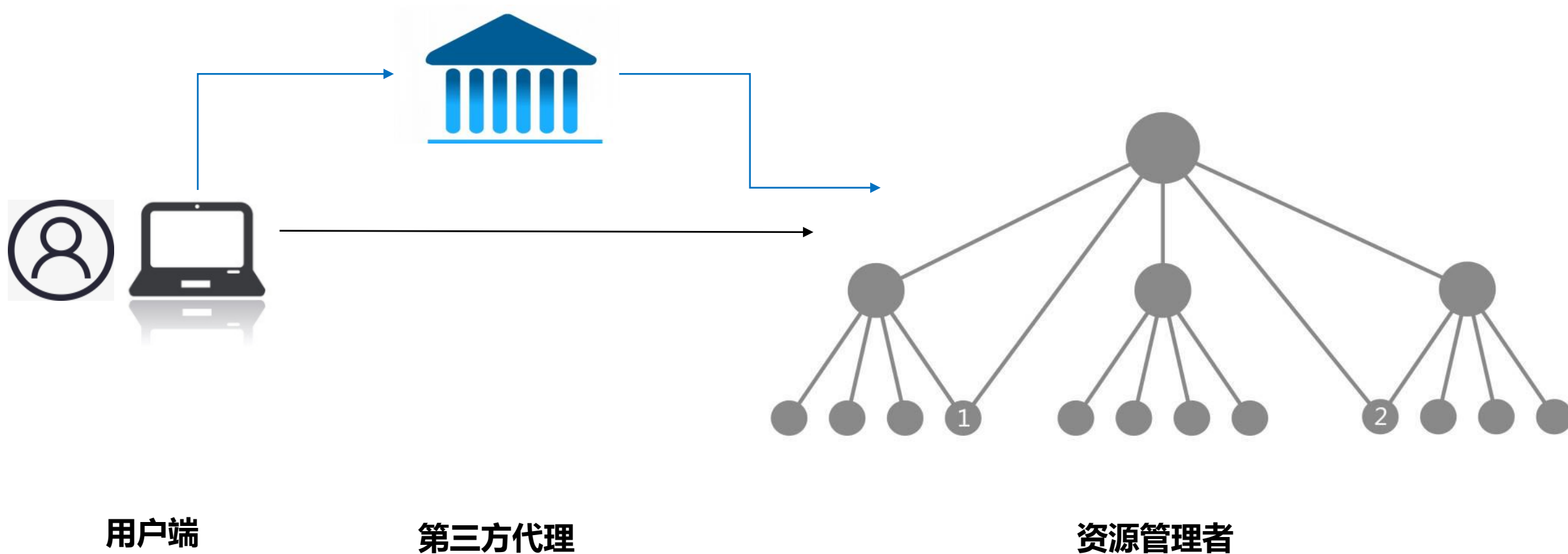
Public Key Infrastructure - Hierarchy



CA

IP地址





终极目标：用户端、第三方代理、资源管理者三方的权力平衡

- 资源管理者自顶向下的逐级分配和控制原则

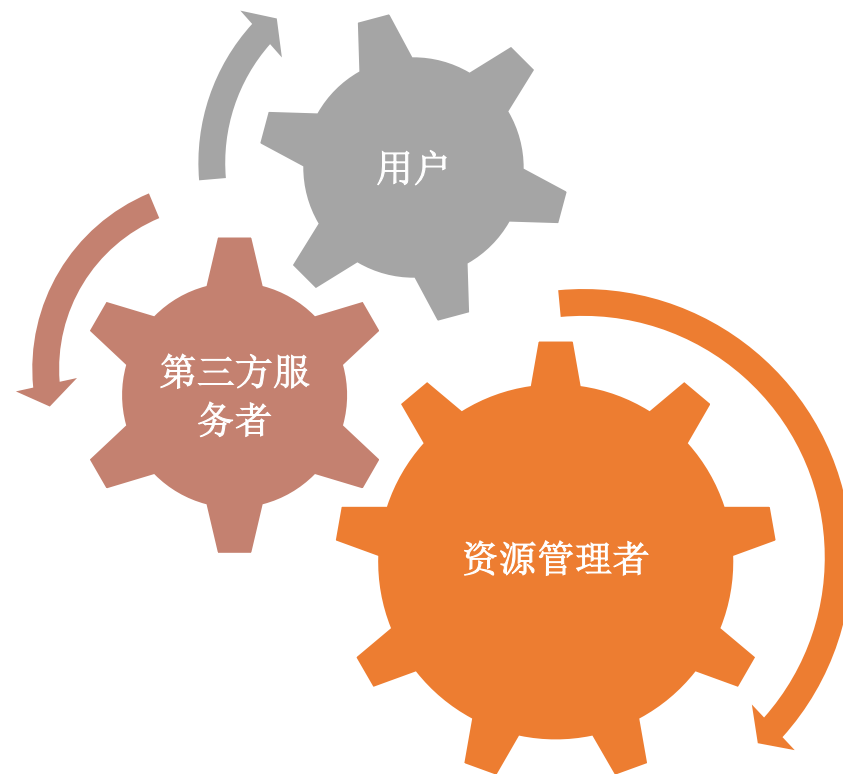
- 唯一、精确、完整、真实

- 最后一公里本地管辖和商业利益诉求

- 安全可控
- 服务水平SLA
- 客户价值

- 用户体验和个性化需求

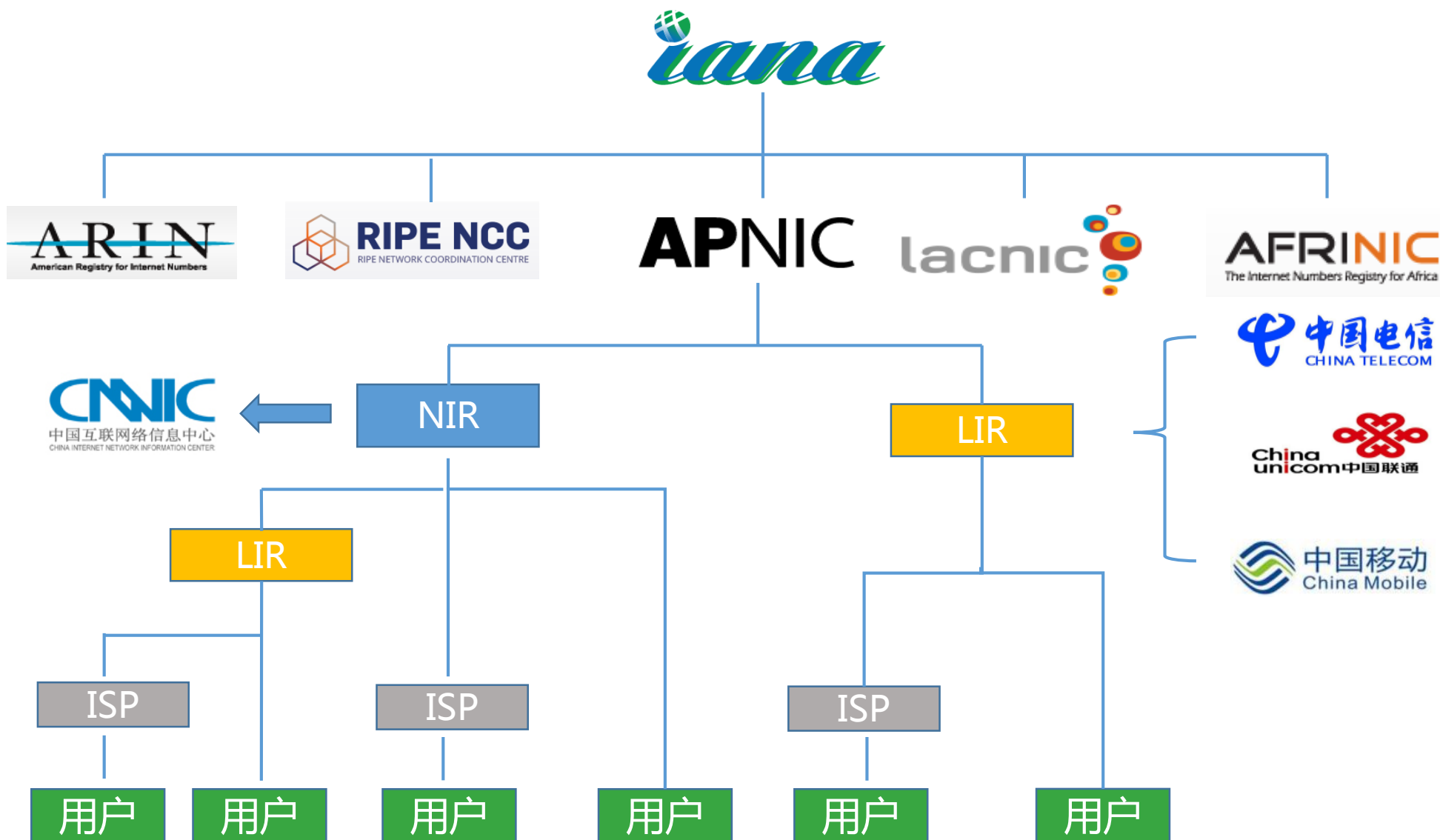
例子：来电号码助手



浅议互联网基础资源服务架构演进

➤ IP地址管理及服务





- 70年代，IP地址最初只在美国科研机构 and 大学内分配
- 80年代至90年代互联网向欧洲和亚洲扩展，在欧洲核子研究中心（CERN）网络协调机构的基础上形成了以欧洲互联网信息中心（RIPE NCC），在亚洲互联网先发国家日本和澳大利亚的网络社群内形成了亚太互联网信息中心（APNIC），同时非洲、拉美以及北美本土的IP地址分配服务也在萌芽酝酿。
- 美国政府在1998年强势宣布其对IANA的管理权，在加强对域名根服务器系统的管控力度同时，对互联网IP地址社群做出了妥协，非洲、拉美和北美社群加快成立各自的IP地址分配机构（ARFINIC、LANIC、ARIN）。



在IP地址分配业务上，五大洲地址分配机构为注册在各地区的独立法人，并不隶属于IANA。IANA仅对超大快IP地址进行大洲级的分配，五大机构对本地区内的终端用户进行实际IP地址分配，享有很大的自主运营和政策权，且自发成立了地址协调联盟机构NRO，独立于ICANN/IANA体系。

- RIPE NCC虽名为欧洲互联网信息中心，但是其业务政策已经向全球开放，不限于欧洲，任何国家的终端用户都可以RIPE NCC申请IP地址，也可以携带地址转移到APNIC等其他四家机构。
- 北美ARIN本质上也是欧洲模式，允许自由分配和转移，但在外围设计包装了更多政策门槛，属于“半自由”。
- 亚太APNIC和拉美LANIC只为本地区服务，不允许其它地区用户申请，但允许用户携带地址转移。
- 非洲AFRINIC既不允许其它地区用户申请，也不允许用户携地址转移出去，最为封闭。



- **随着全球IPv4地址的耗尽，各地区互联网发展规模及网民数量的不平衡，引发了如下现状：**
 - 大量新兴互联网国家（典型如中国）公司机构采用各种办法向其他大洲IP地址管理机构申请，最常见的方式是在各洲当地国家注册一批子公司或壳公司，以本地公司的名义申请、向原IP地址持有者发起溢价购买，待买入IP地址后，再转移回母公司所在地区，或者根本不转移直接在全球进行路由广播。
 - 我国对IP地址的管理较为严格，IP地址非备案不得用来广播和使用，备案系统需要应对这种趋势（除了传统的APNIC会员地址、CNNIC会员地址、工信部地址联盟会员地址外的碎片化国际来源IP地址）。

IP地址的全球流动和碎片化也进一步扩大了IP地址使用(运营商路由)过程中的安全威胁，引出了RPKI和BGPSEC技术。

RISK ASSESSMENT –

Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/28/2017, 4:20 AM

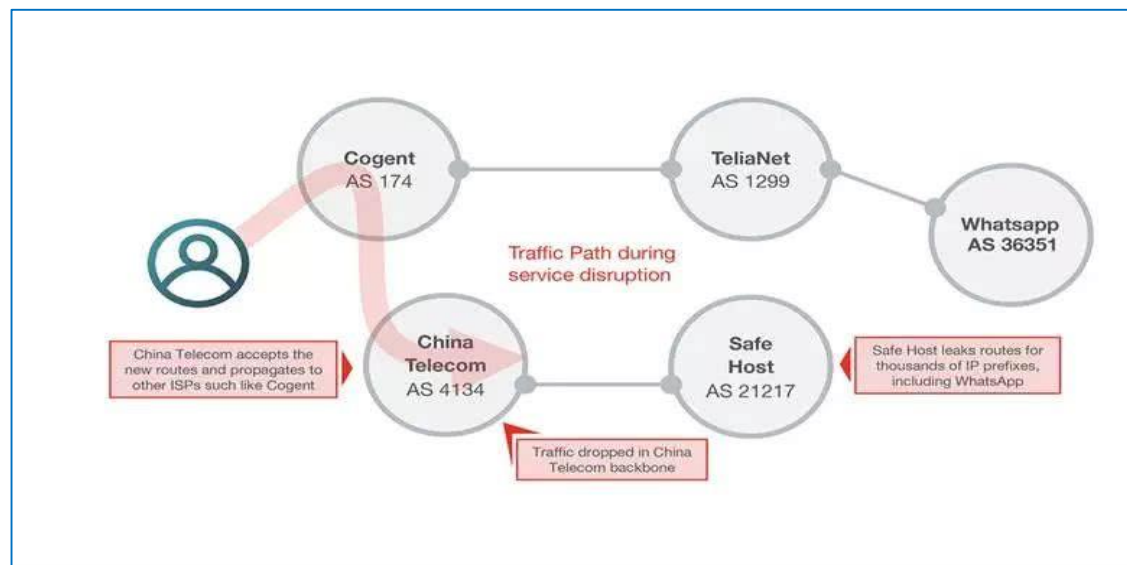
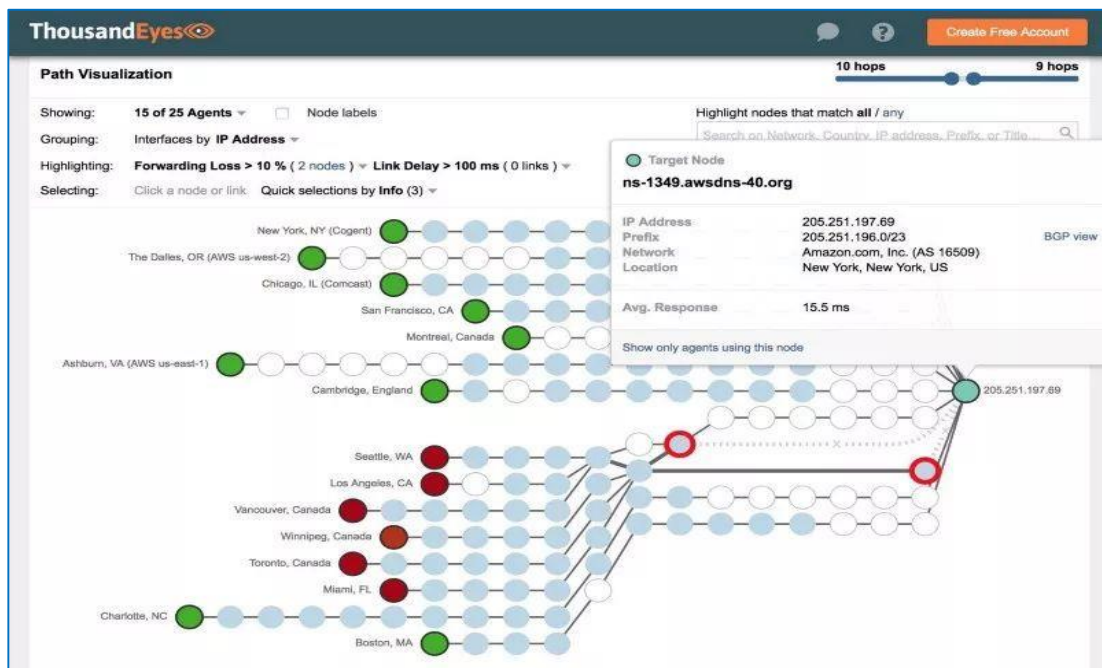
Google Error Causes Widespread Internet Outage in Japan

By Catalin Cimpanu

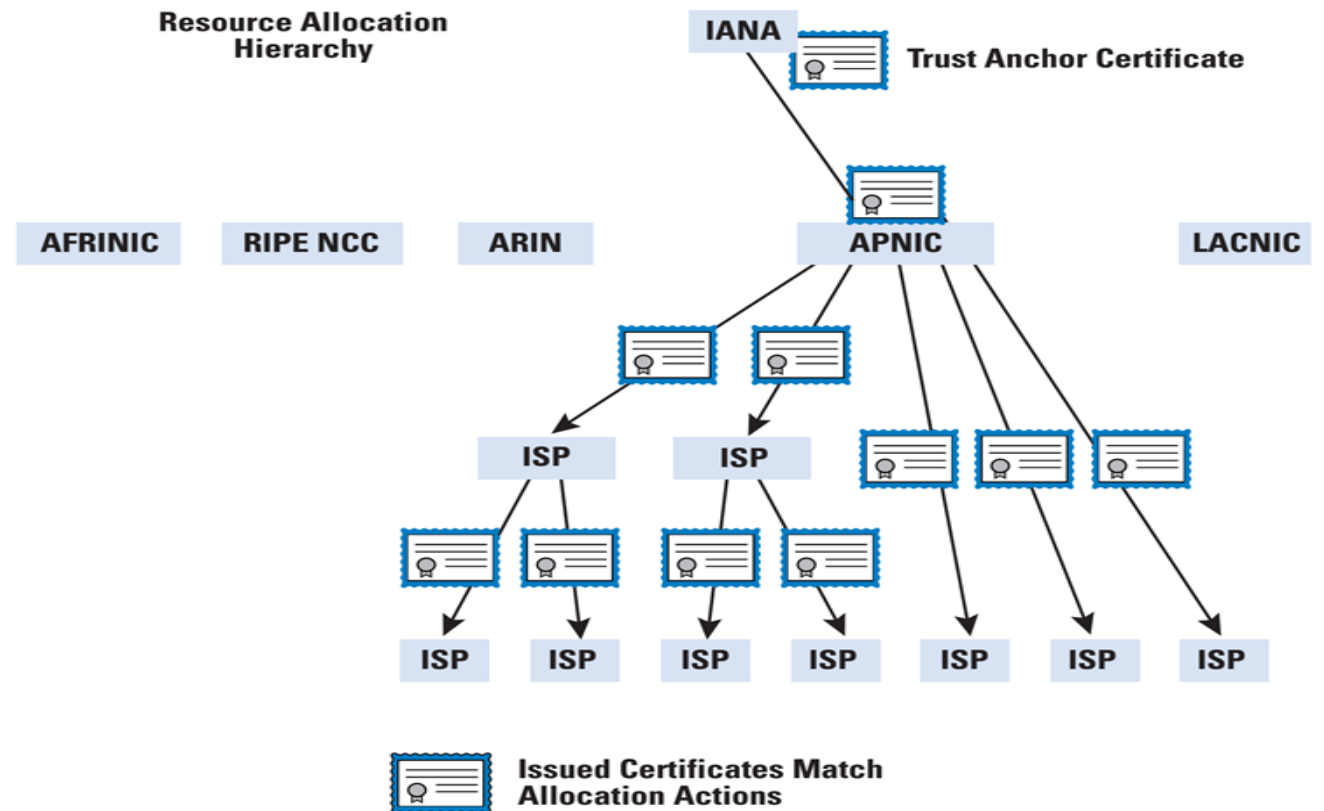
August 27, 2017 01:35 PM 0



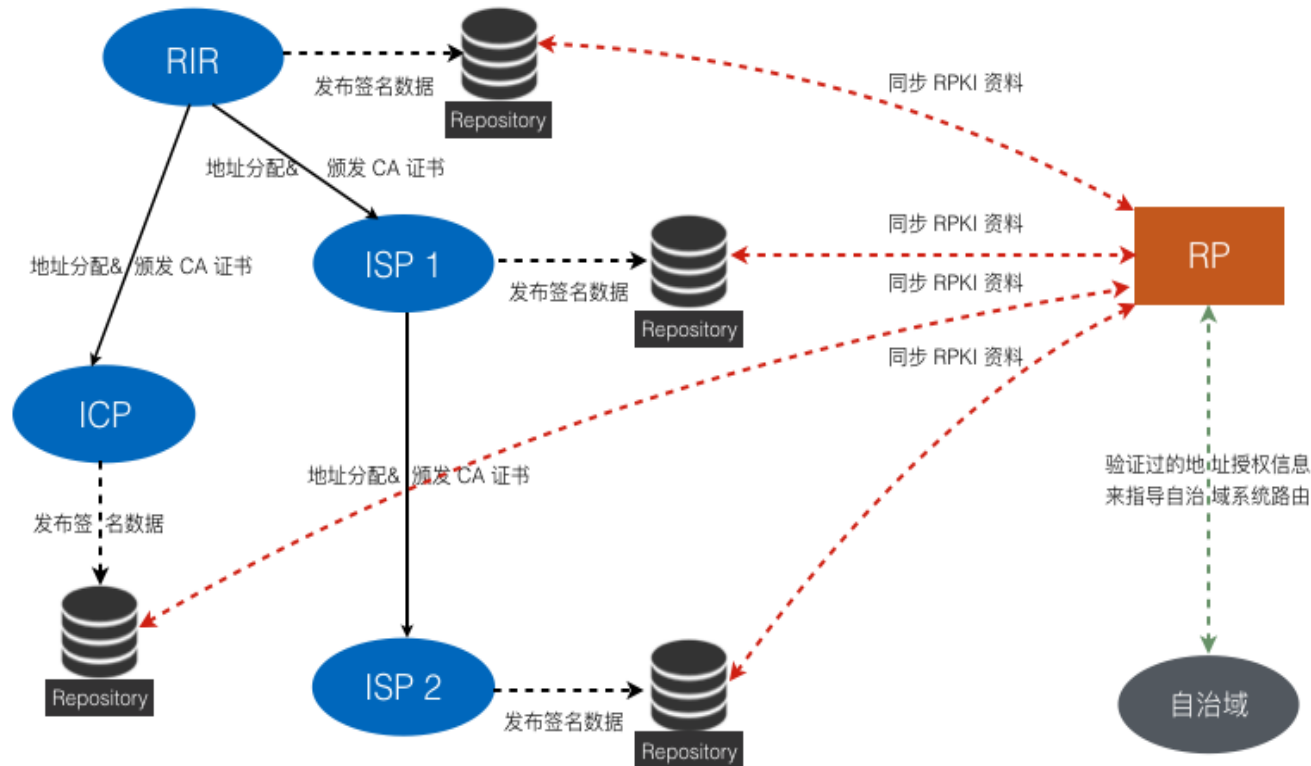
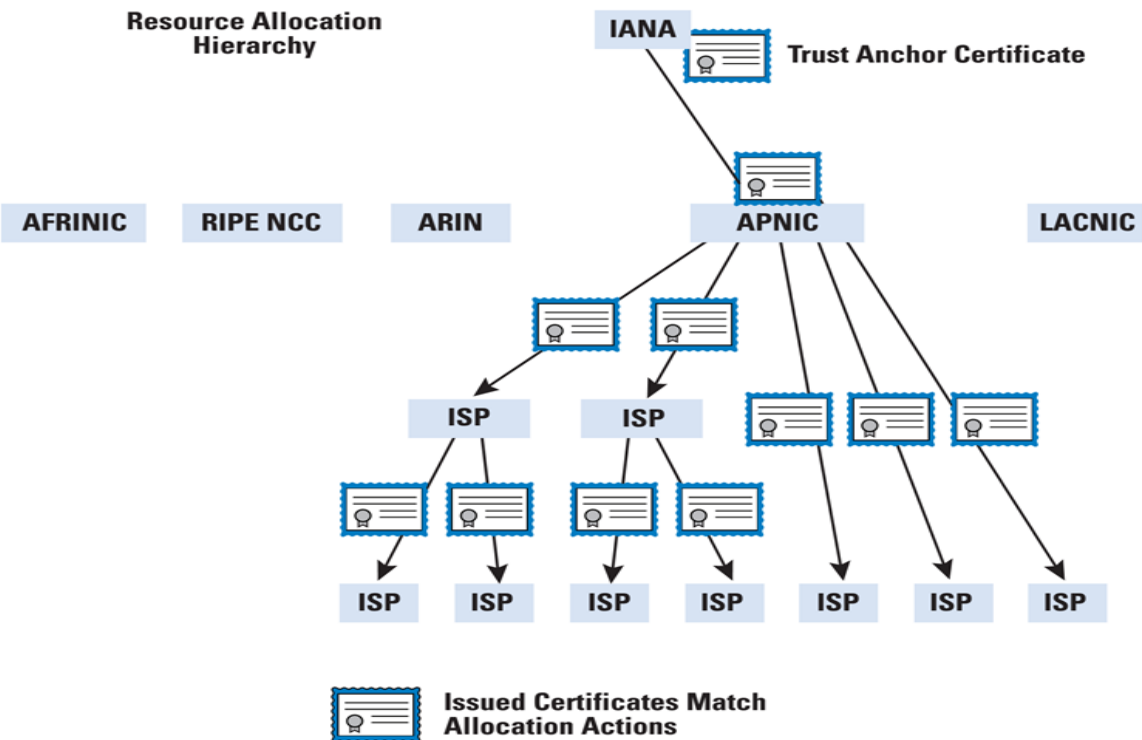
An error on Google's part has caused widespread Internet outages in Japan for about an hour, on Friday, August 25. The downtime was caused by a BGM route hijack that began at 12:22 PM local Japan time and was resolved by 1:01 PM.



- 五大机构无法阻止资本流动带来的IP地址使用权流动和应用流动，采用新型安全认证技术手段**RPKI**来确保IP地址的所有者和使用者一致；
- 而新型安全认证技术有可能进一步加大五大机构的独立性，冲击到IANA作为最高分配者和协调者的地位。

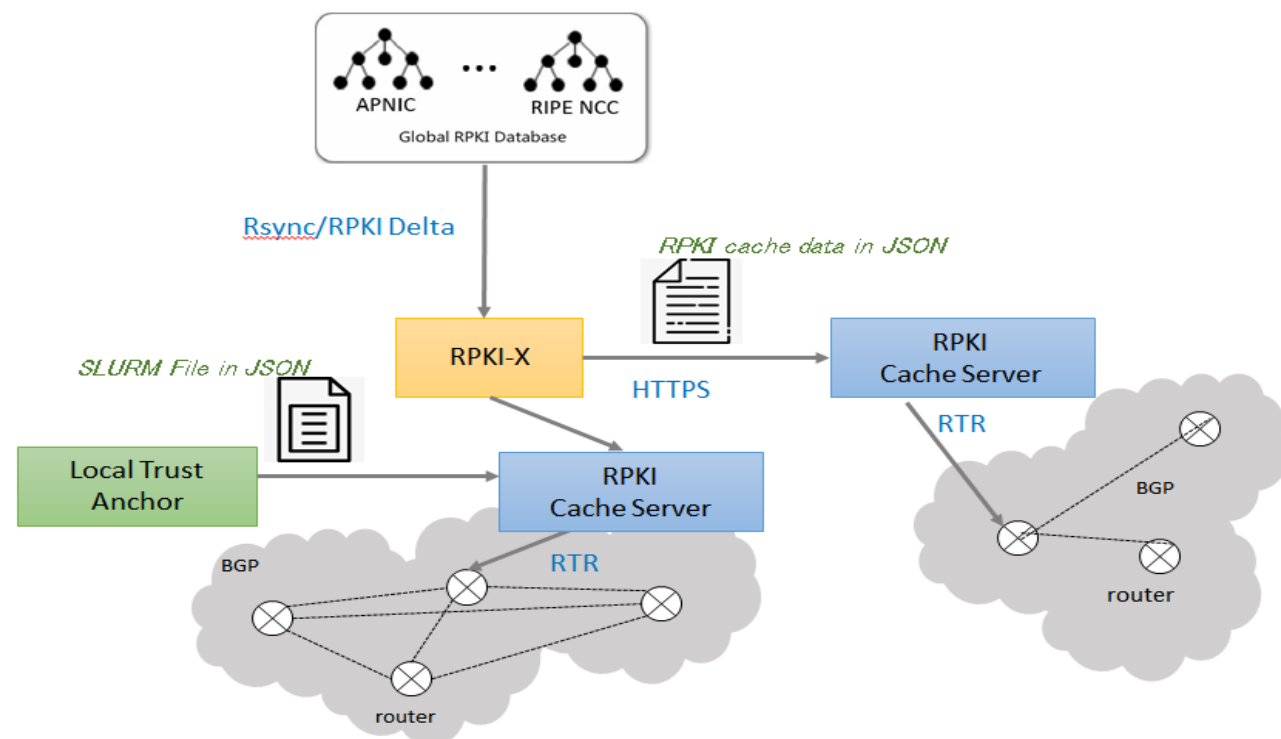


Resource Allocation Hierarchy



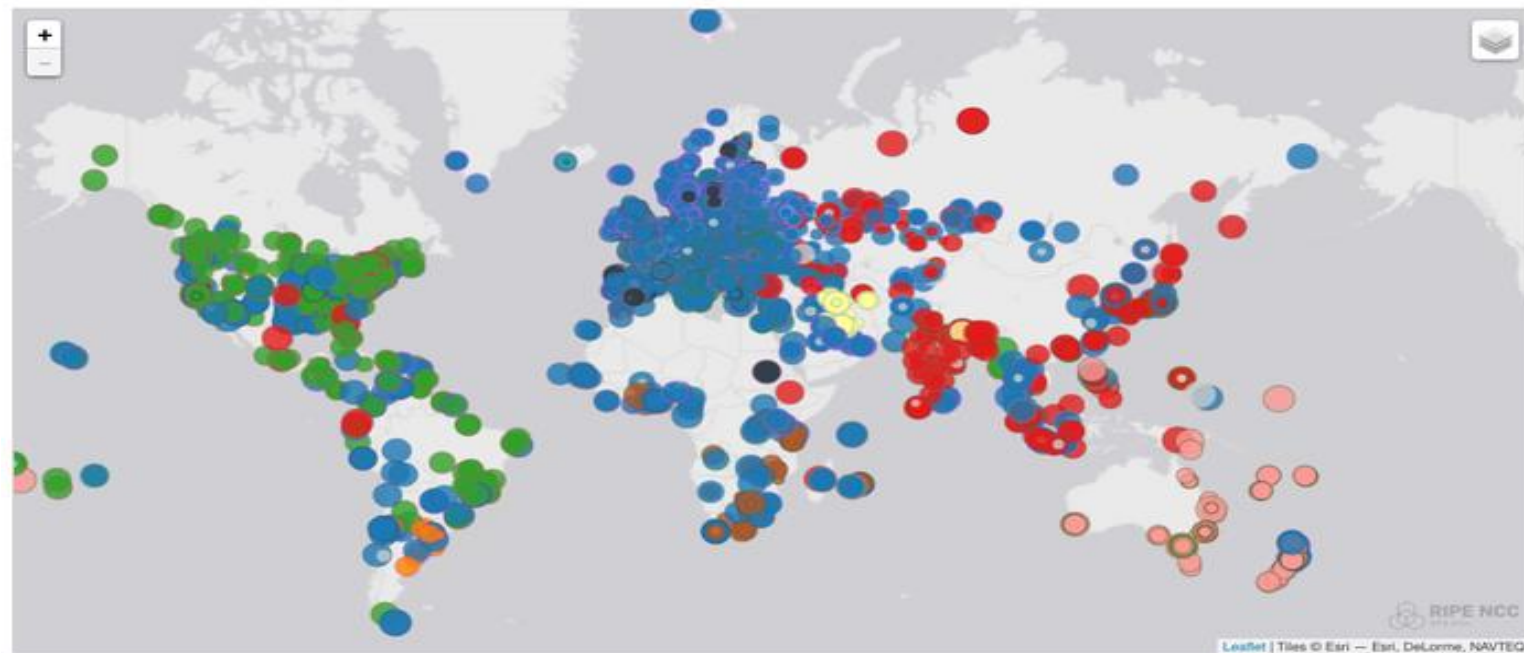
- RPKI引发了RIR和IANA的矛盾，未来互联网治理的新热点
- RPKI引入了“IP地址根”概念，RIR从IP地址分配机构变成了IP地址认证机构
- RPKI把IP地址路由技术风险转移成为RIR的管理风险
- RPKI要求ISP运营商的域间路由器进行升级，并搭建单独的认证系统

- 我国科研工作者贡献提出支持本地认证的RPSTIR方案和原型系统
- ICANN与NRO之间，各国本地RPSTIR与NRO RPKI服务器之间的关系有待厘清



浅议互联网基础资源服务架构演进

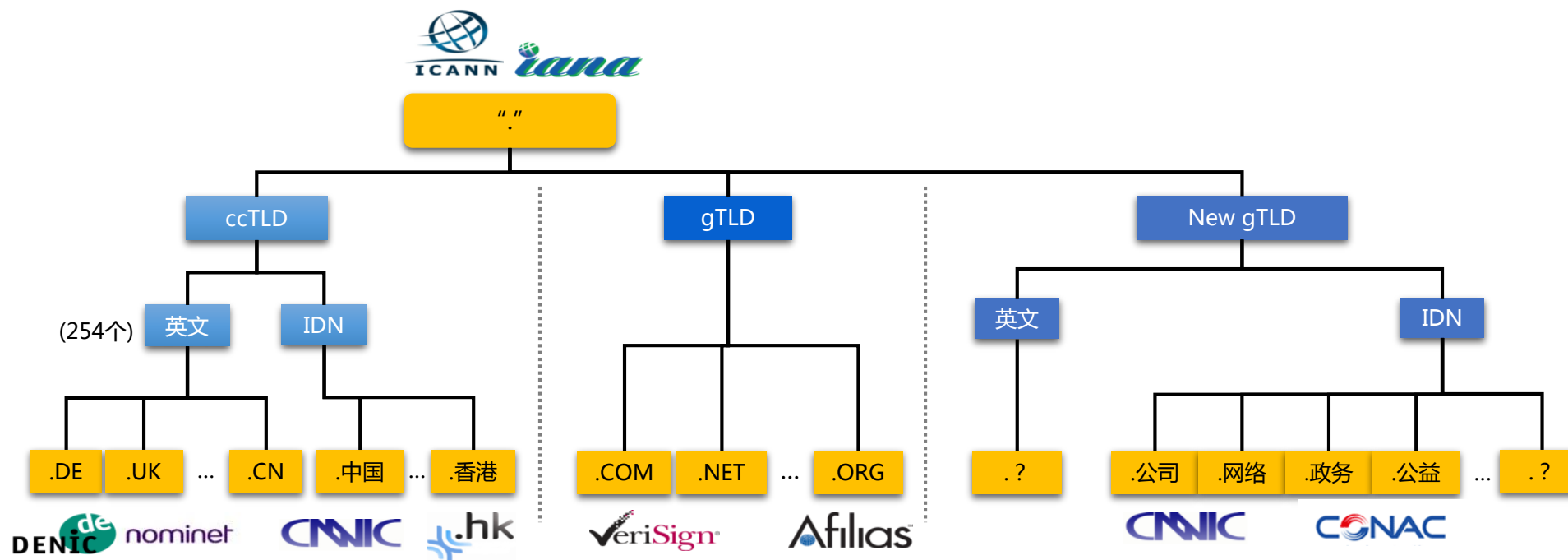
► 域名系统及根服务器体系

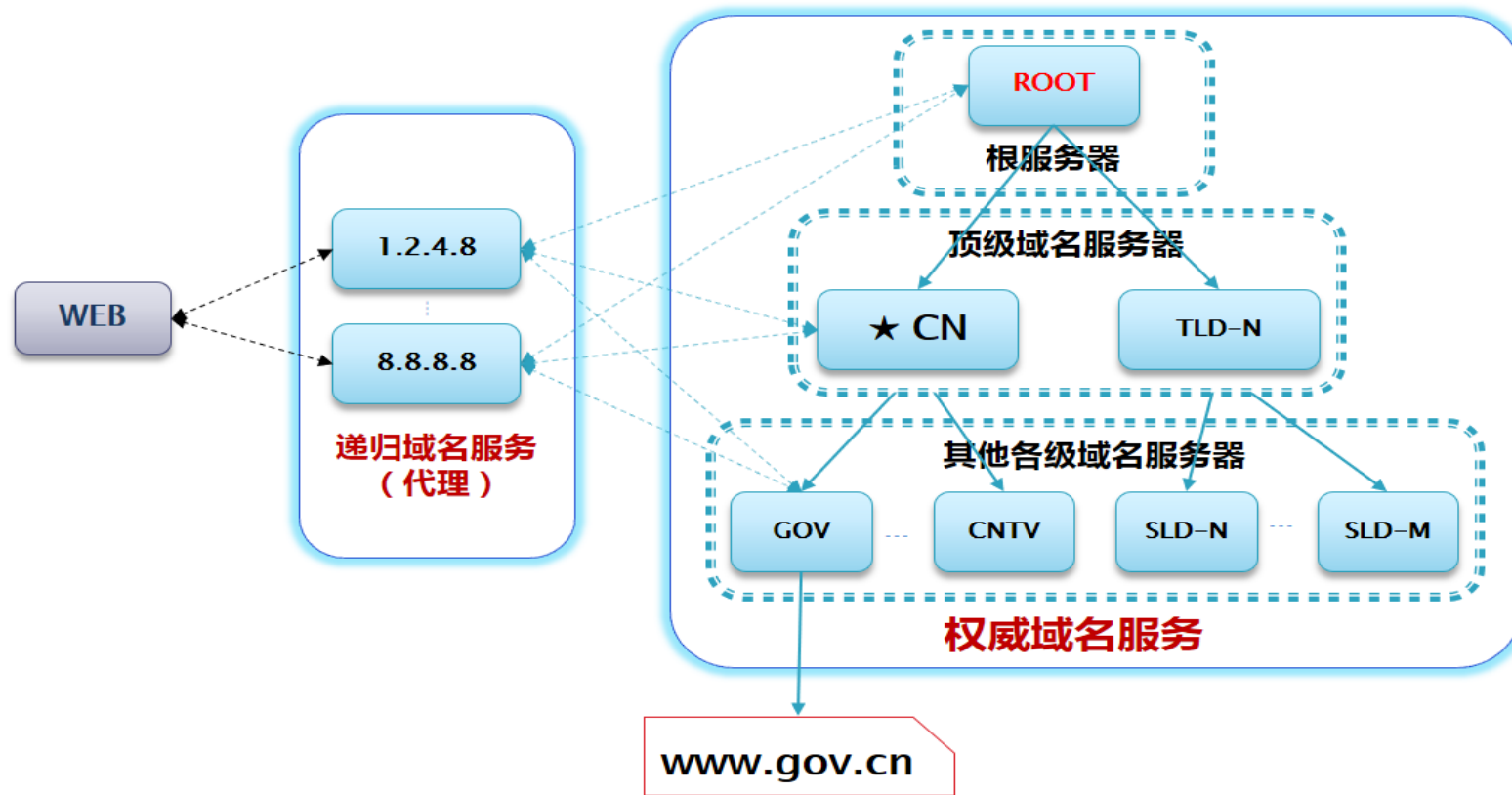


ICANN (The Internet Corporation for Assigned Names and Numbers 互联网名称与数字地址分配机构)

负责IP地址的分配、顶级域名 (TLD) 的管理、以及根服务器管理。

- 国家和地区顶级域, 属于主权范围, 政府授权, 自行管理
- 通用顶级域, 由ICANN批准, 并与注册管理机构签署协议授权其运营和管理
- 新通用顶级域, ICANN适时全面开放多语种顶级域, 并采取政策、技术、市场等多手段全面控制。





域名体系是通过最顶层的管理者逐级授权而不断延伸生长出的一棵数据树。作为这棵数的树根，域名根系统**理论上**具最高的**数据管理权**。

- **根区数据管理 (PTI/IANA)**

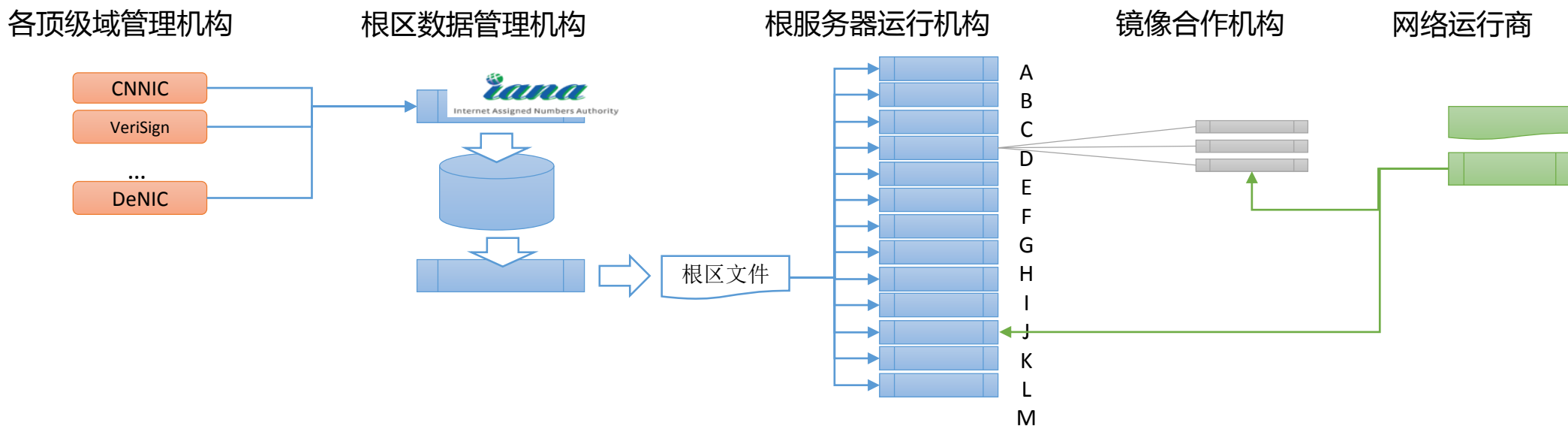
记录顶级域服务器名称及其IP地址的对应关系，完成根区文件的修订和编辑，是IANA的核心职能。

根区文件需要写入根区数据库服务器并分发给所有的根服务器，根区数据库不对外公开提供解析服务，相当于被隐藏的主根（或称母根）。

- **根服务器**

根服务器依据根区文件提供顶级域信息提供解析服务，并可根据需要与各国各地区的本地托管机构合作设立镜像服务器。

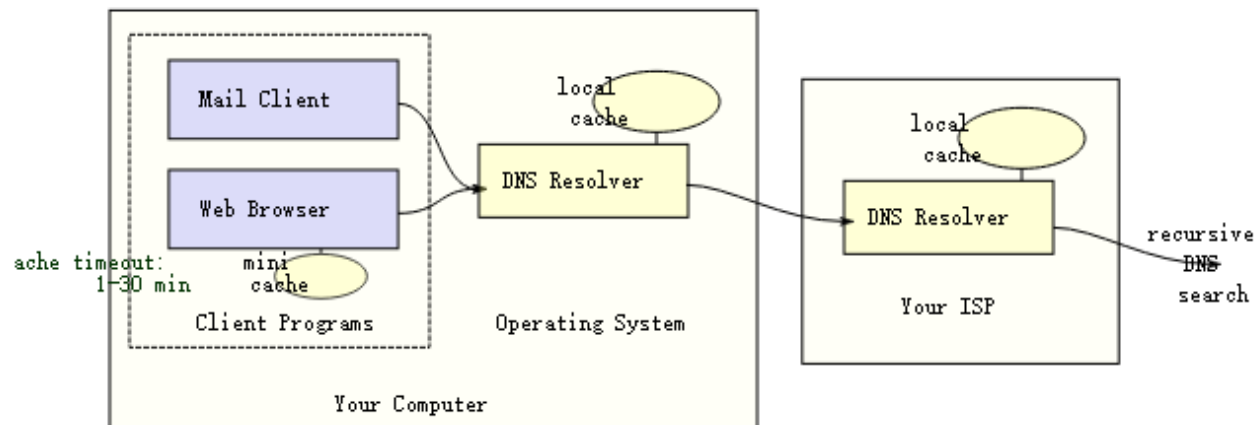
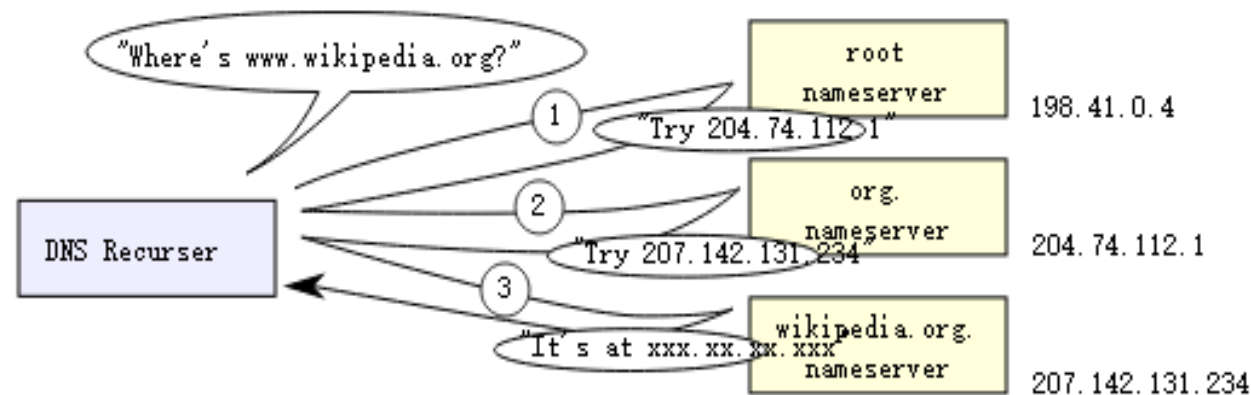
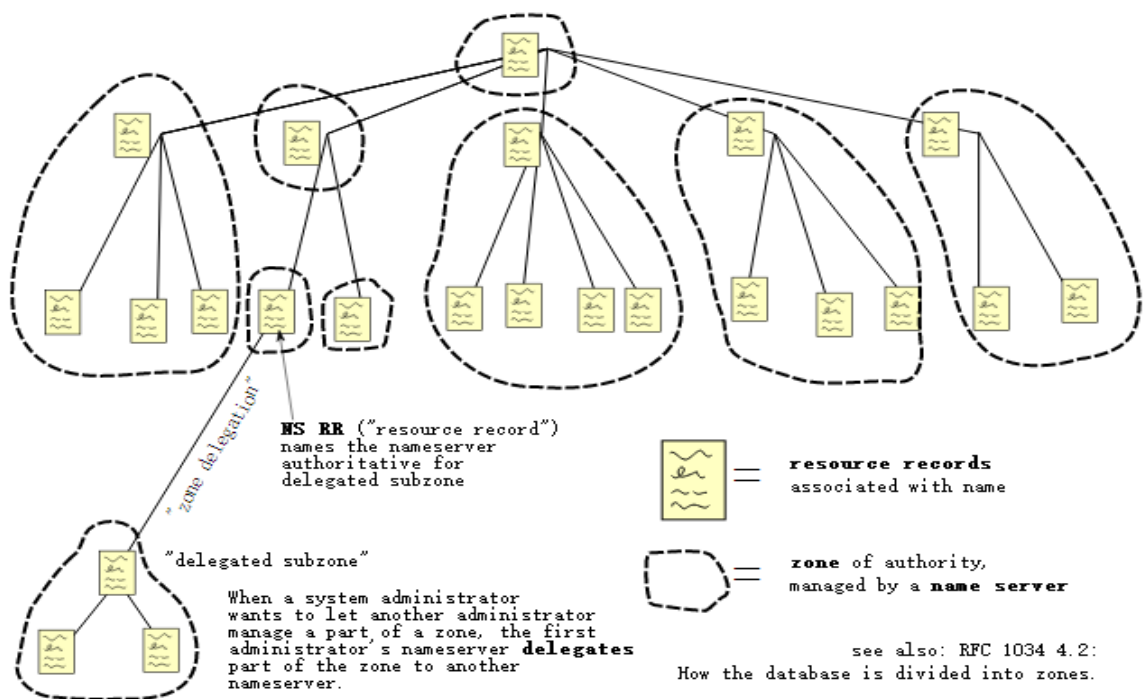
根服务器运行机构负责管理各自的根服务器，相互之间独立且地位平等，均以志愿者方式提供解析服务，与ICANN基于相互信任关系进行合作，但与ICANN互不隶属。



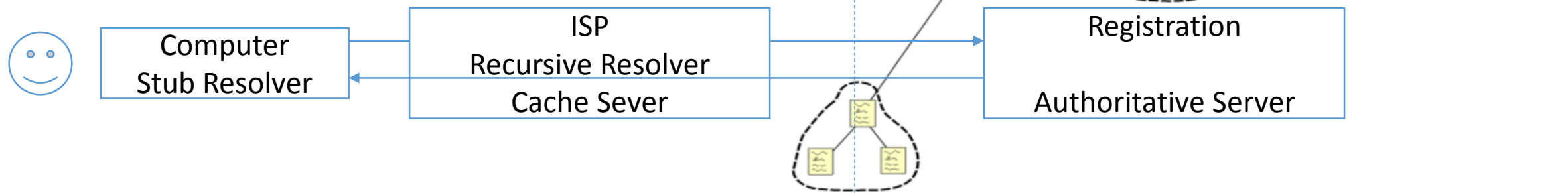
• 名字空间分级自治

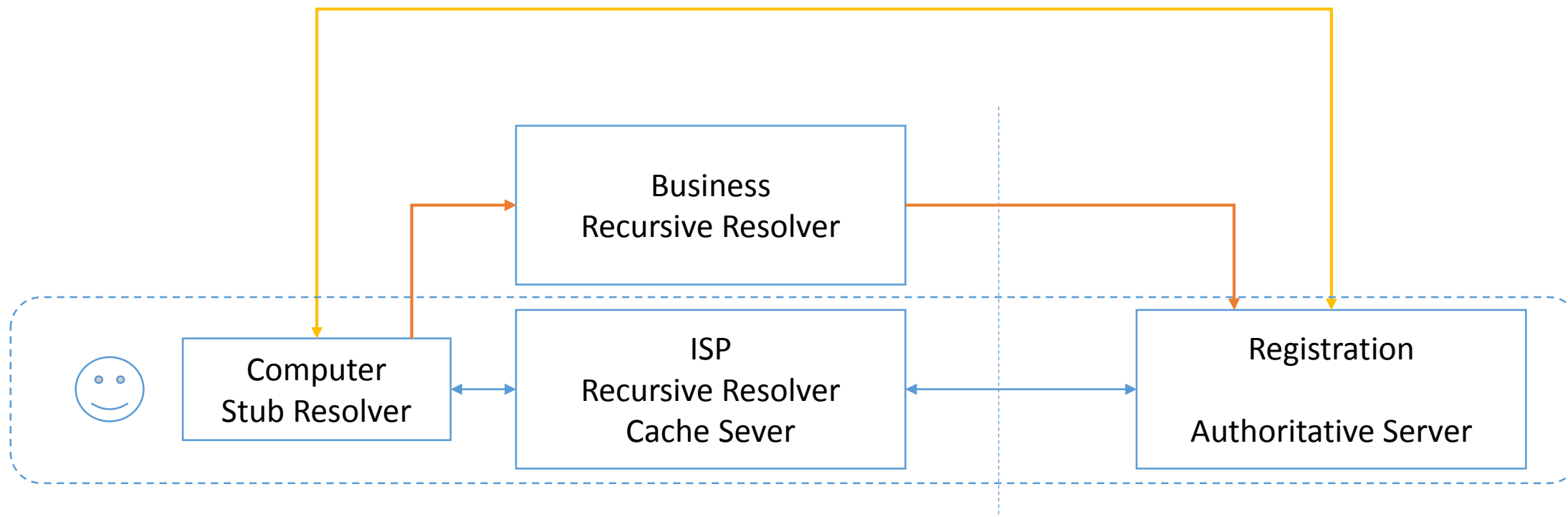
- 君上之君、非我之君
- 臣下之臣、非我之臣

Domain Name Space

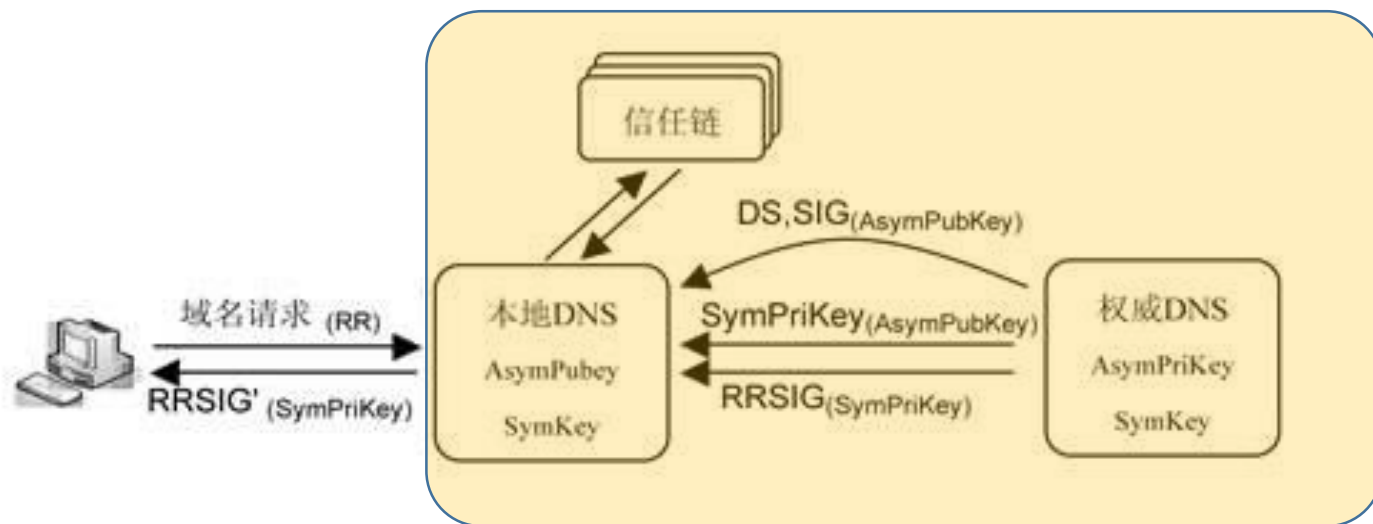


- **查询访问依靠代理**
 - 选择、授权、代议



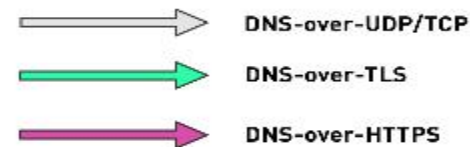
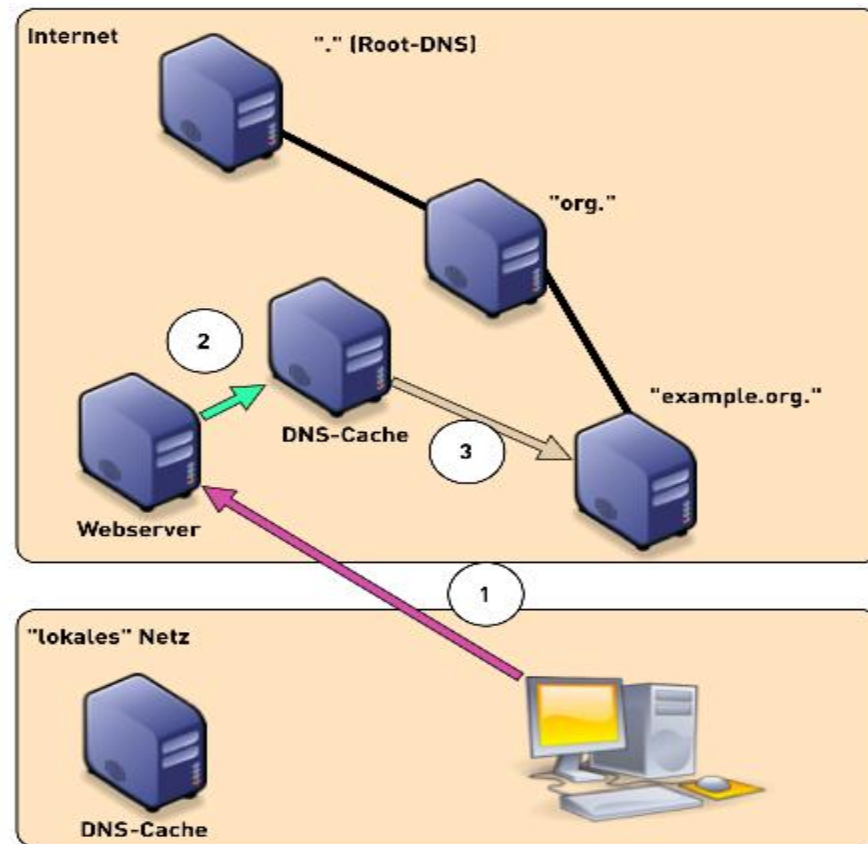
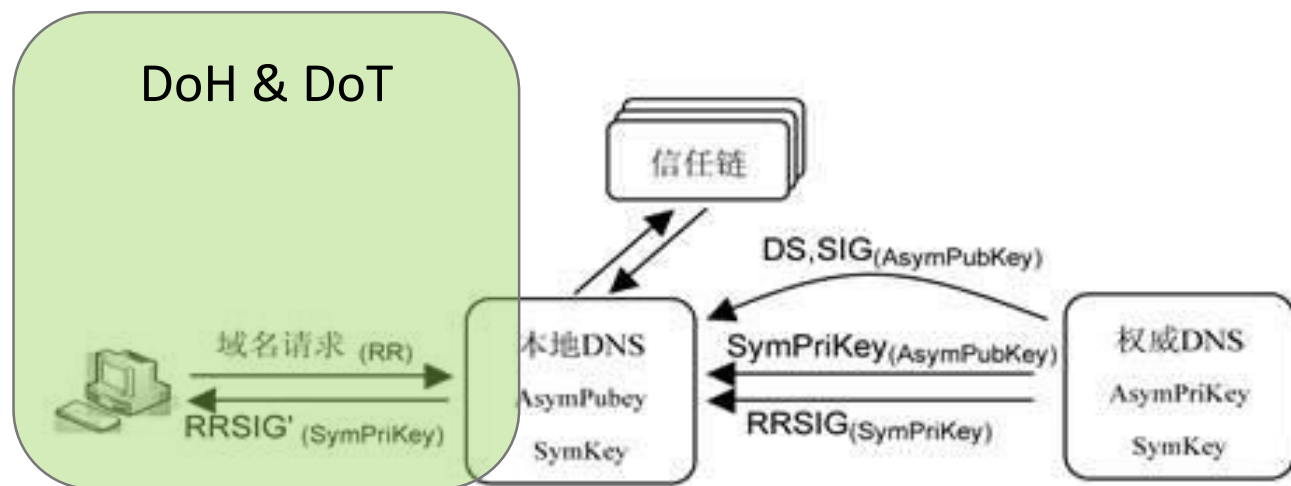


- 90年代后期，IETF成立了工作组专门研究DNSSEC安全扩展协议（DNS Security Extensions），利用经典的加密算法和签名机制，完善了原有DNS体系的不足之处，从而形成一整套的DNSSEC解决方案。



- **DNSSEC**赋予了根服务器一个新的角色，即，作为验证证书签名有效性的最高节点（通常被称作信任锚），进一步**推升了根服务器作为全球互联网核心基础设施的重要性**。全球的互联网域名用户，不仅依赖根系统完成域名解析，而且不得不依赖根系统对域名的完整性、真实性进行验证。
- 在无法保证域名访问路径可控的情况下，通用应用密码学PKI体系来加强数据可控。

- DNS over HTTPS
- DNS over TLS



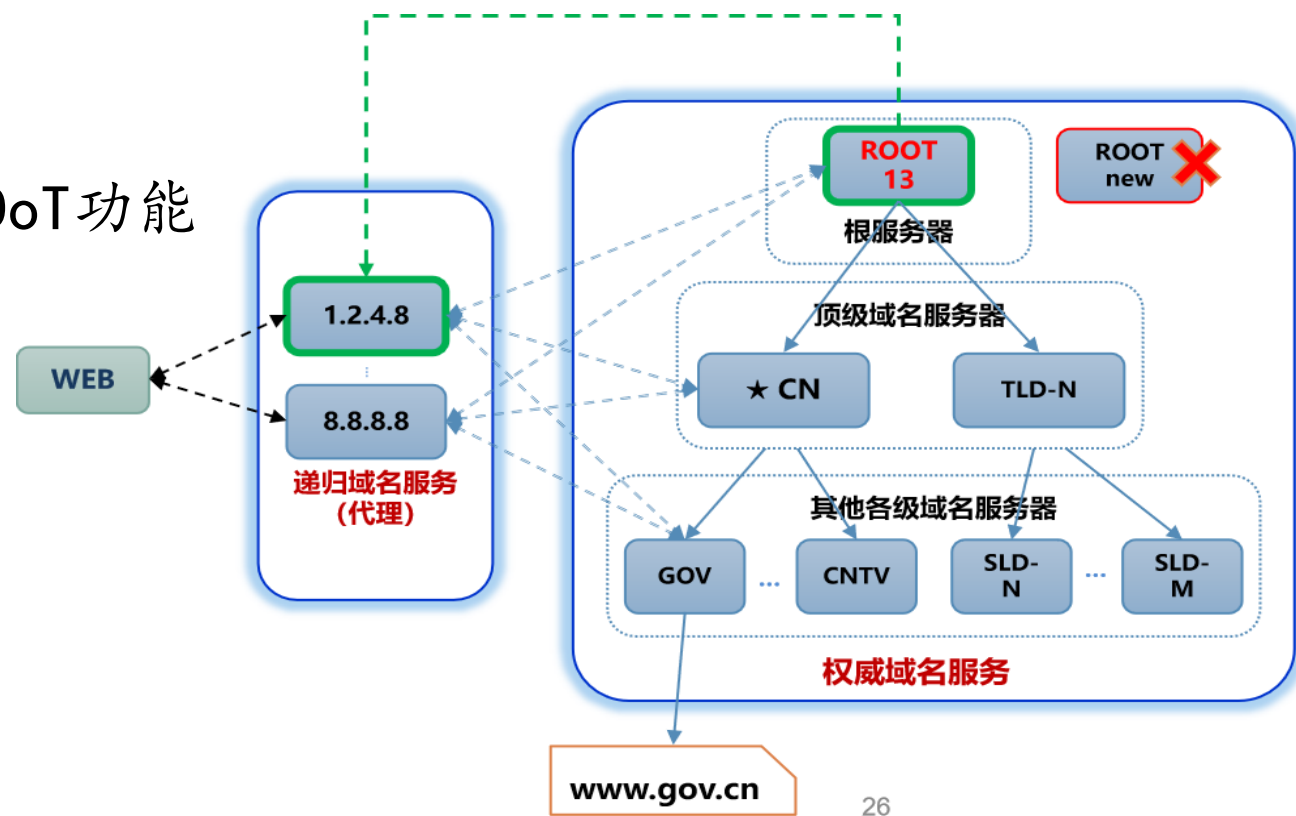
DNSSEC和DoH/DoT对本地DNS服务的机遇和挑战

- DNSSEC引发的递归本地根方案RFC7706

- 运营商拥有了合规合理的介入根管理的技术手段

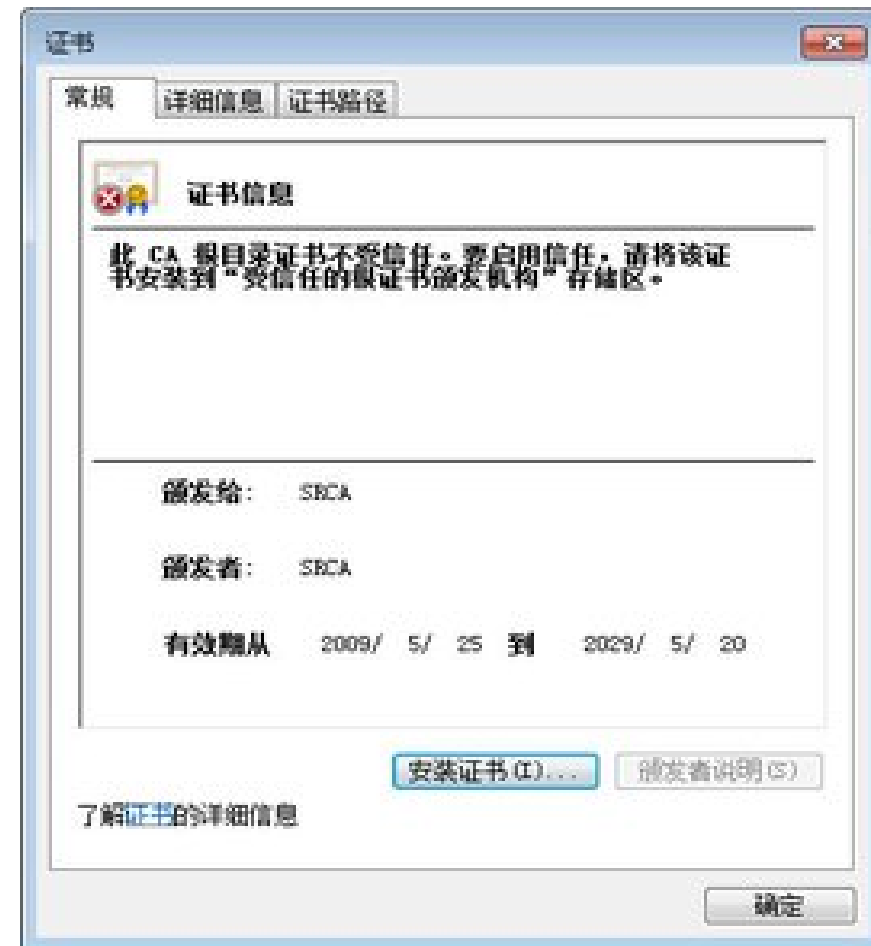
- DoH/DoT对运营商域名服务的旁路

- 冲击已有商业域名服务
- 浏览器甚至应用APP都可以嵌入DoH/DoT功能



浅议互联网基础资源服务架构演进

➤ CA证书WEB应用的管理模式变化



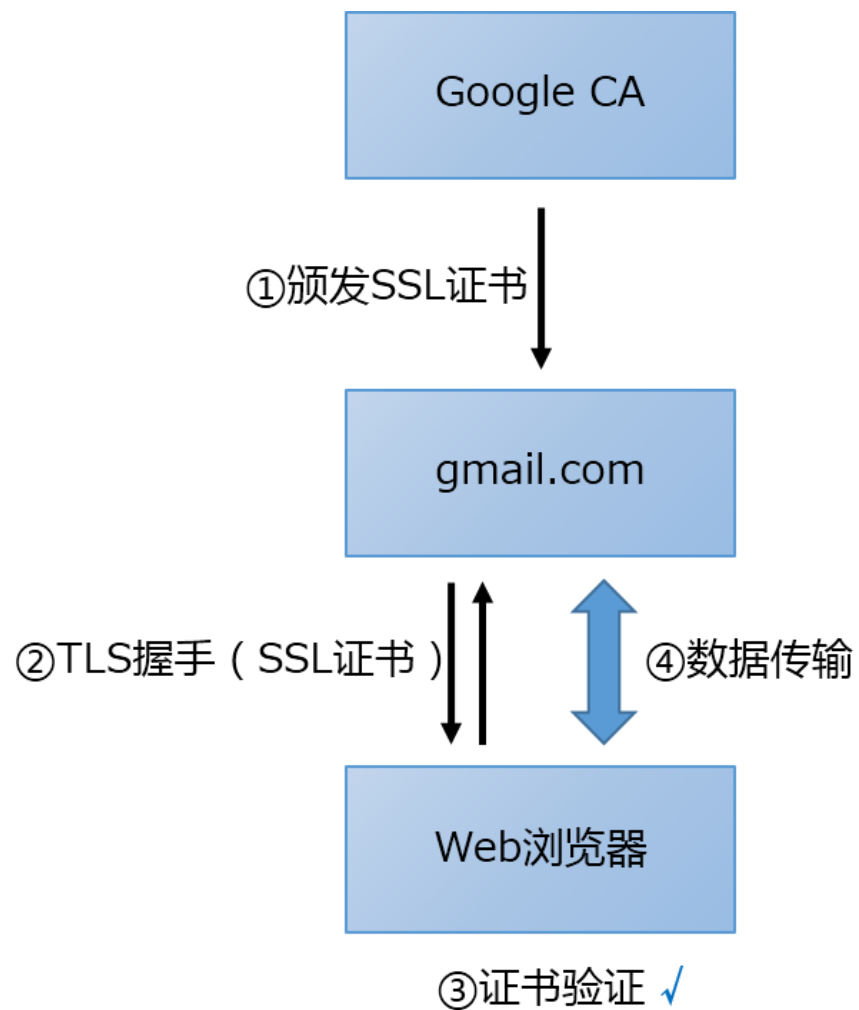


图 https连接的建立过程（正常）

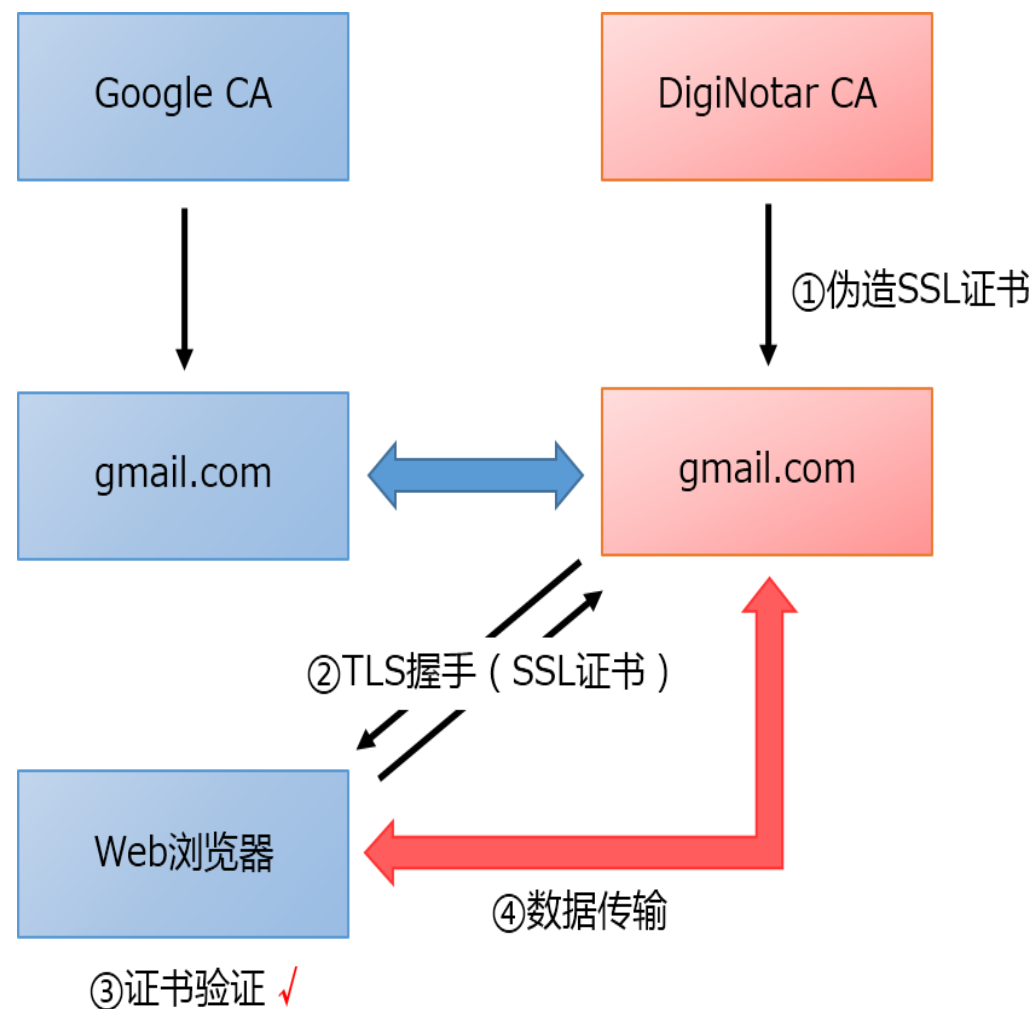
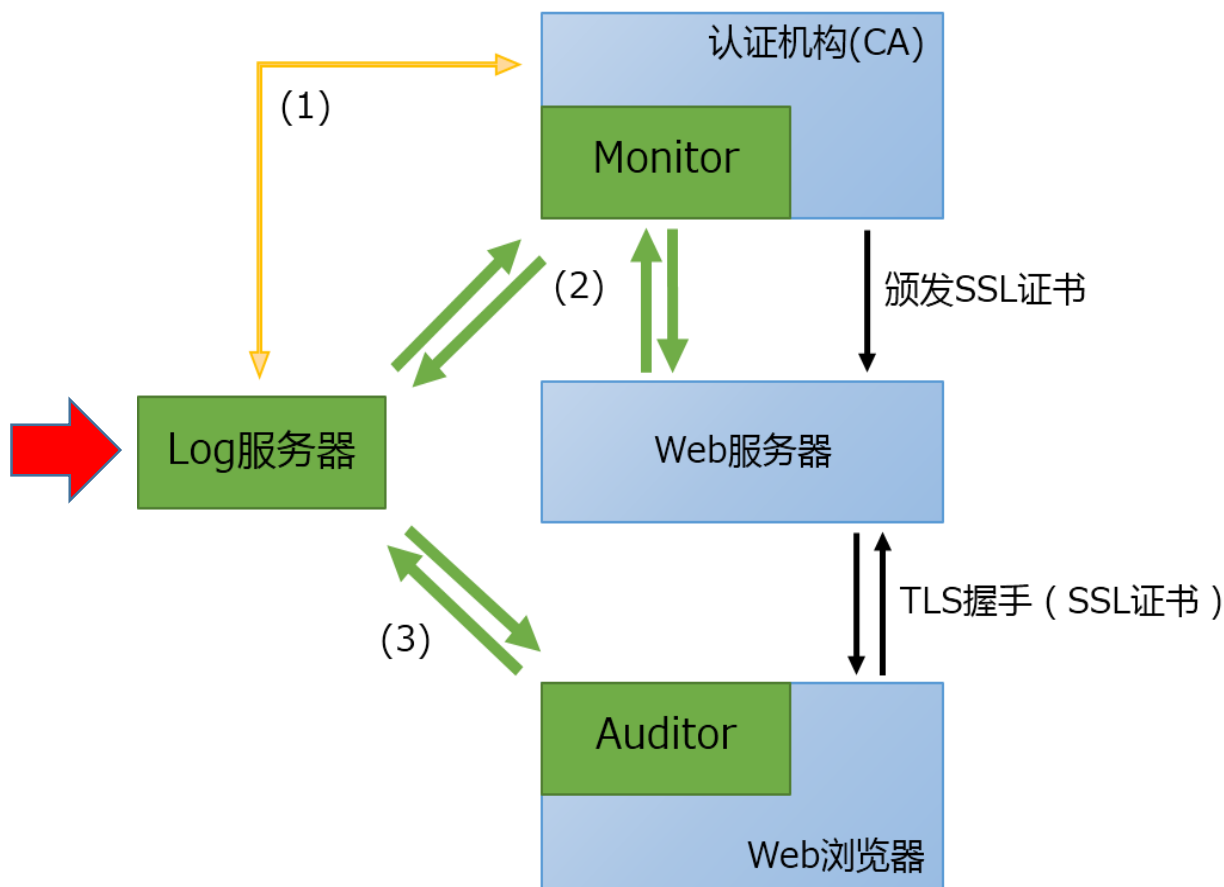
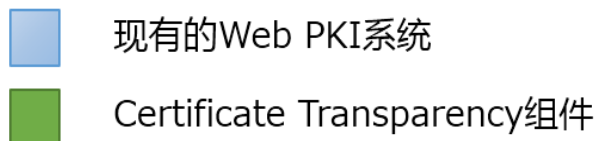


图 https连接的建立过程（中间人攻击）



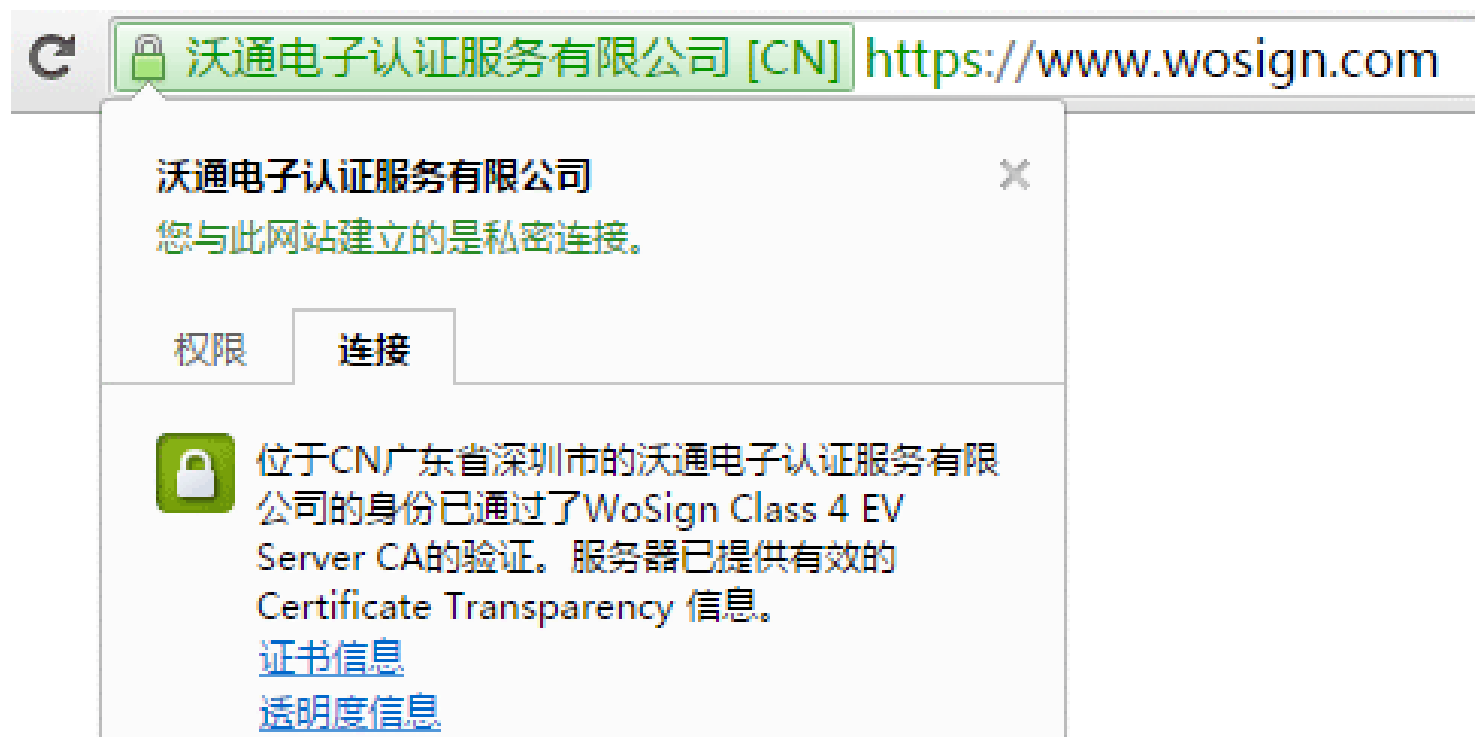
对现有的SSL证书系统的补充，并非替代
CT信任模型有三部分组成：

1. Certificate Log 证书日志
2. Certificate Monitor 证书监控
3. Certificate Auditor 证书审计



CT并不能阻止CA签发错误或虚假证书，但是它能让人们清楚看到CA签发所有证书，从而使检测这些证书的过程变得相对容易

- CA难以错发证书
- 公开、实时性的监督和审计，
确定证书是否错发
- 用户能够识别恶意 / 错误证书



- **CT机制出发点是通过引入审计，从而分散CA的权力**
 - 浏览器等终端的支持
 - 行业CT联盟（准入机制？）
 - 安全密码算法
- **DoH + CT ? !**
 - 如果未来DoH成为重要的DNS用户侧实现方式
 - 如果CT成为通用技术和安全模式
 - 域名问题叠加证书管理问题，证书成为基础资源的基础资源
 - IETF协议工作的泛PKI化

浅议互联网基础资源服务架构演进

➤ 其他




- DNS是一种分布式标识系统，但名字空间是等机制的，某一个名字的管辖权是明确的，在给定场景下必须有一个权威机构的存在；
- 现有BlockChain的域名方案聚焦在为某一个TLD提供业务支持，建立域名数据与分布式账本技术的联系，回避了互联网治理关注的焦点问题：
 - TLD的争夺博弈问题（.amazon）
 - 二级域的争夺博弈问题（weixin.com）
- 如果BlockChain无法提出比现实世界权威机构更合理的仲裁机制，则BlockChain只能给域名业务提供一个新的基础设施，或，为区块链提供一个新的应用场景。

- **网络时间源与国家时间源的不一致**
 - 各类NTP时间源 vs 北京时间时间源
- **传输过程中易遭攻击篡改**
 - UDP 123, 多为明文传输, 易遭到中间截获和篡改
- **网络时间SLA不一**
- **时间戳在各类证书应用的基础作用**
 - 在线交易
 - 工业互联网系统
 - Blockchain



- 互联网设计初衷，是对抗场景下、分布式去中心、简化信任机制的封闭网络。
- 互联网不断演变，发展为全球化的、跨边界的、与社会经济活动紧密融合的复杂网络空间环境。究其原因，实得益于“对等互联”的内在特性和协议。
- 凡事一利必有一弊。强调“对等互联”的网络架构无法有效地组织起一个集中式的管理权威来实施全局管理。各区域网络/自治域地位平等、并无相互隶属统属的责权关系，管理政策各行其是，**管控手段无法跨越区域网络边界**。
- 在不考虑推倒重来、暂不改变现有互联网基础协议的前提下，加强互联网管控治理的一个现实方案，是寻找**类似传统电信“支撑网”角色的关键元素**，IP地址、域名、证书体系恰恰是这种具有技术支撑与管理抓手双重属性的关键基础设施。
- 基于PKI的应用密码学技术给互联网基础资源管理带来了新的变化，也为我国互联网行业管理带来新的思路和新的挑战。



THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE