



TRUNG TÂM INTERNET VIỆT NAM
VIETNAM INTERNET NETWORK INFORMATION CENTER - VNNIC



Lộ trình quốc gia triển khai DNSSEC - Đảm bảo an toàn hạ tầng Internet Việt Nam

Người trình bày: Nguyễn Trung Kiên

Email: ntkien@vnnic.vn

Đơn vị: Trung tâm Internet Việt Nam (VNNIC)



Nội dung

1

Hệ thống DNS & vấn đề ATAN

2

Công nghệ DNSSEC

3

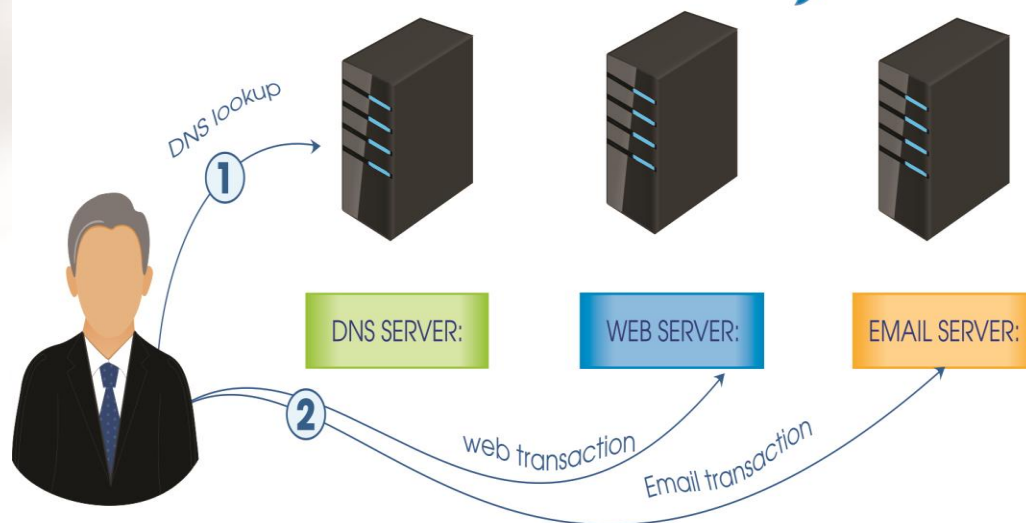
Lộ trình quốc gia triển khai DNSSEC



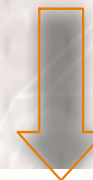
DNS – Trái tim mạng Internet

- DNS là hệ thống nền tảng giúp truy cập, sử dụng dịch vụ trên Internet

Sử dụng DNS để truy cập các dịch vụ trên Internet



TÊN MIỀN
MIC.GOV.VN
...



ĐỊA CHỈ IP

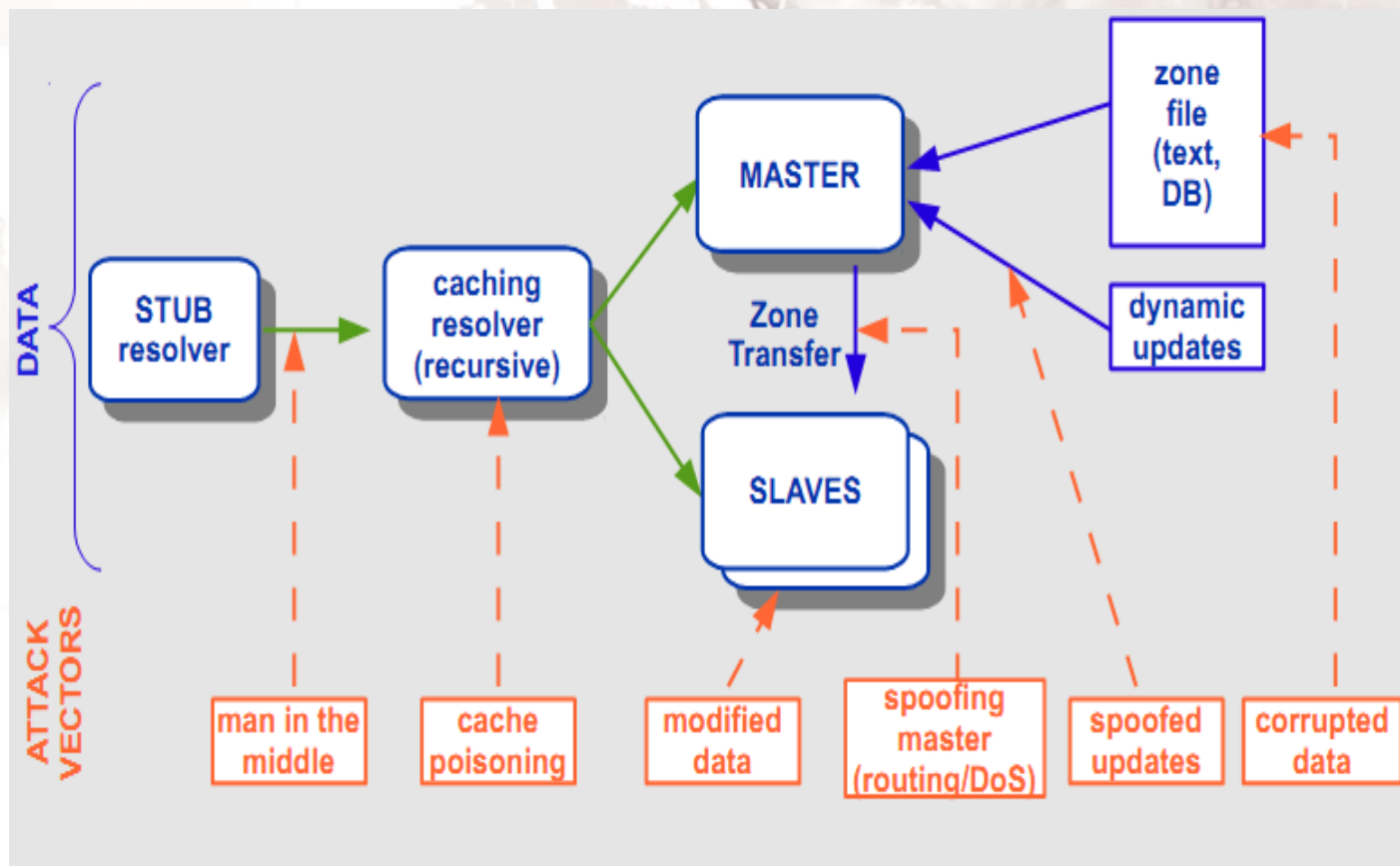
IPv4: 123.30.29.36

IPv6: 2001:ee0:0:8006::2



DNS & Vấn đề ATBM

- Các dạng tấn công DNS phổ biến



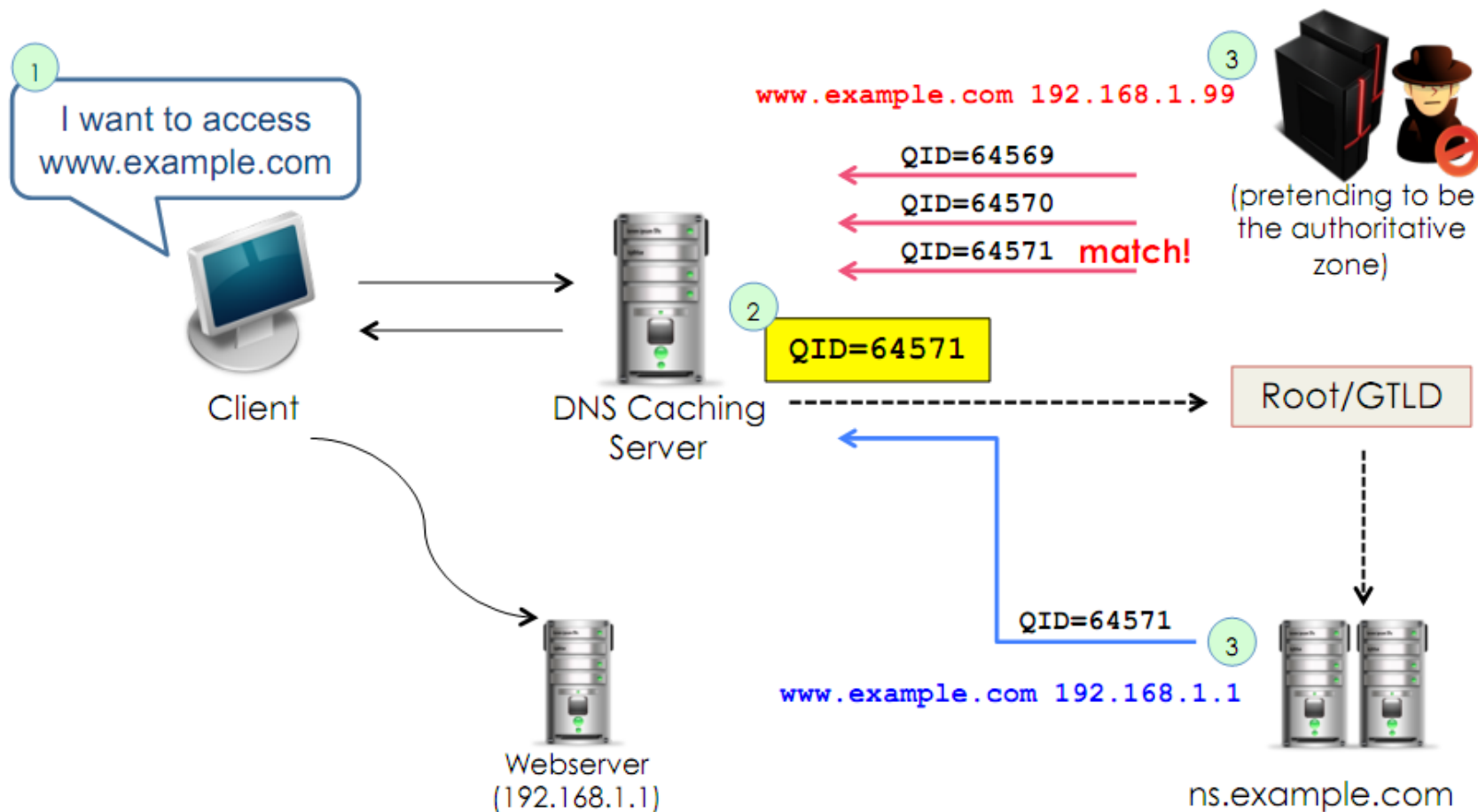


Tại sao DNS dễ bị tấn công?

- DNS sử dụng truyền tải UDP, vì vậy khi truy vấn, bất kỳ gói tin UDP trả về cũng có thể là câu trả lời.
- Gói tin UDP trả về chỉ cần đúng Source IP, Source port, Destination IP, Destination port, DNS query ID
→ Có thể vượt qua kiểm tra (bailiwick checking) !
- **Dễ dàng giả mạo ! Còn gọi là “DNS Pharming” hay “DNS Cache Poisoning”**



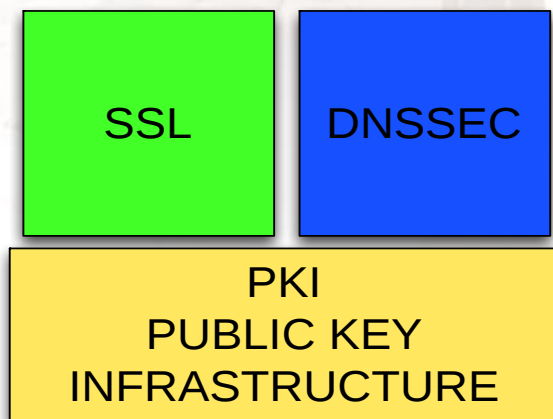
DNS Cache Poisoning





DNSSEC

- DNS Security Extensions (DNSSEC), tiêu chuẩn an toàn mở rộng của hệ thống DNS, được định nghĩa trong các RFC 4033, 4034, 4035.
- Sử dụng cơ sở hạ tầng mã hóa công khai PKI (private/public key).





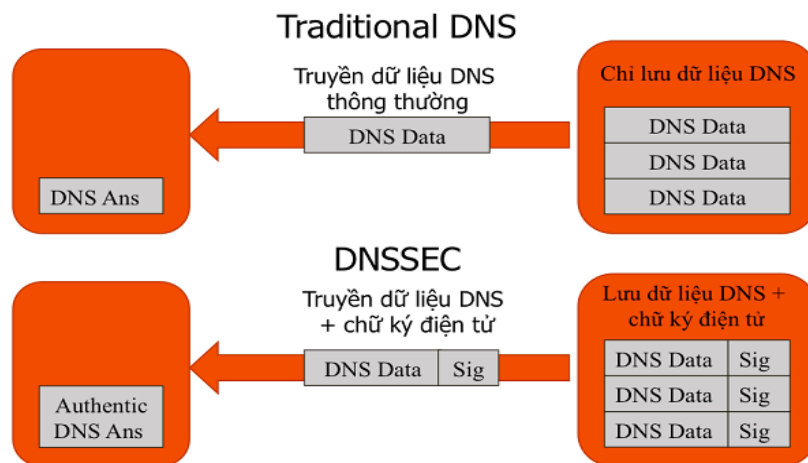
Tổng quan DNSSEC

- Thay đổi mô hình DNS từ mô hình mở (open) sang mô hình tin cậy (trusting) và xác thực (verifiable)
- DNSSEC cung cấp các khả năng:
 - ☐ Authentication of origin (xác thực nguồn gốc)
 - ☐ Data integrity (toàn vẹn dữ liệu)
 - ☐ Authenticated denial of existence (xác thực từ chối tồn tại)
- Không cung cấp confidentiality (không mã hóa)



DNS & DNSSEC

- Vì là tiêu chuẩn mở rộng, DNSSEC không làm thay đổi cấu trúc và nền tảng giao thức DNS (cùng tồn tại với hạ tầng hiện tại EDNS0)
- Thêm chữ ký số vào câu trả lời truy vấn



- Người dùng Internet sử dụng DNSSEC được kiểm tra xác thực, toàn vẹn dữ liệu, đảm bảo truy cập an toàn!



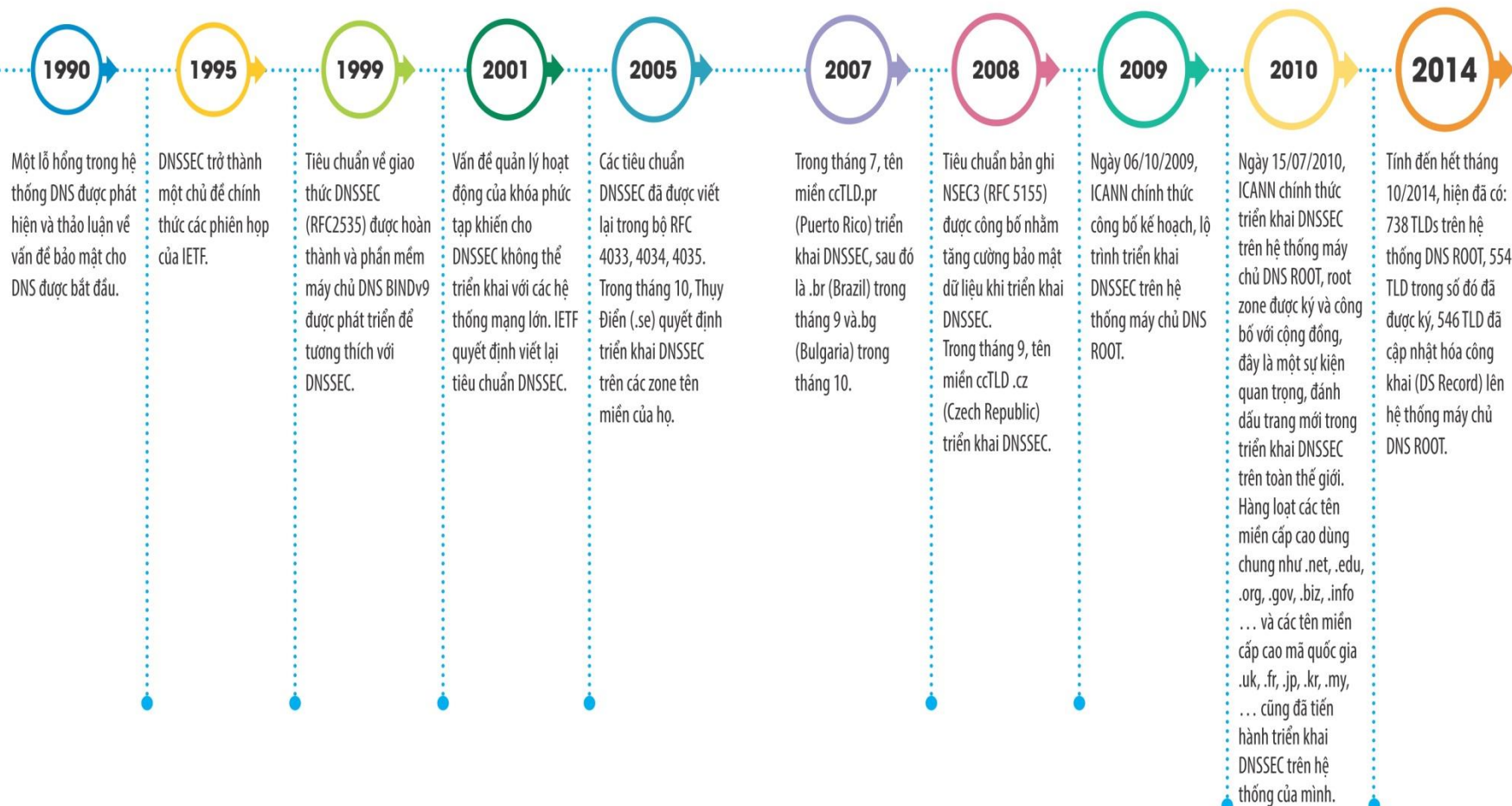
Các cập nhật trong DNSSEC

- DNSSEC đưa ra các loại bản ghi mới:
 - ❑ Bản ghi khóa công cộng DNS (DNSKEY)
 - ❑ Bản ghi chữ ký tài nguyên (RRSIG - Resource Record Signature)
 - ❑ Bản ghi bảo mật kế tiếp (NSEC/NSEC3).
 - ❑ Bản ghi ký ủy quyền (DS).
- Các trường thông tin mới trong giao thức (flag):
 - ❑ DO: DNSSEC OK
 - ❑ AD: Authenticated Data
 - ❑ CD: Checking Disable



Triển khai DNSSEC tại ROOT

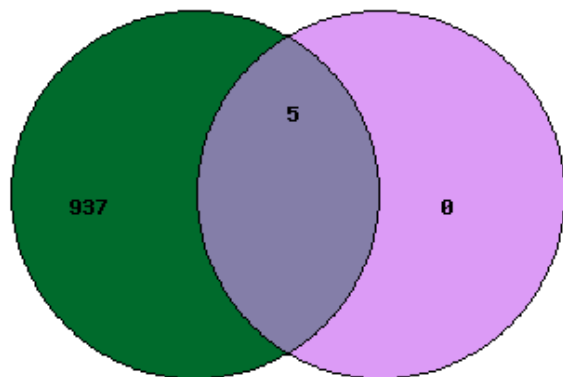
QUÁ TRÌNH TRIỂN KHAI DNSSEC TRÊN THẾ GIỚI





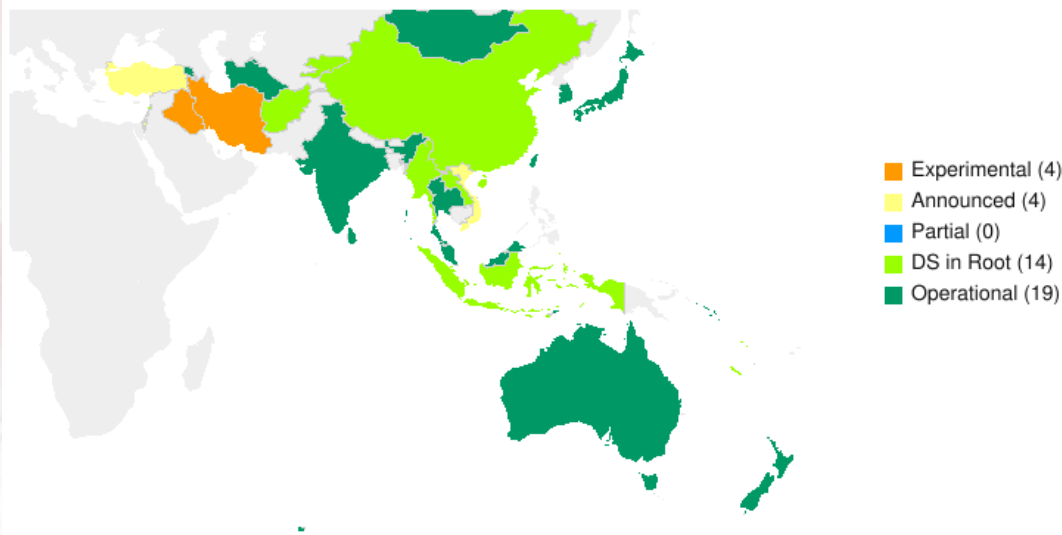
Triển khai DNSSEC tại TLD, ccTLD

Venn Diagram



■ Trust anchors in the Root Zone
■ Trust anchors in ISC's DLV

AP ccTLD DNSSEC Status on 2015-06-19



TLD DNSSEC Report (12/2015)
http://stats.research.icann.org/dns/tld_report/

AP ccTLD DNSSEC Status (06/2015)
<http://www.internetsociety.org/deploy360/dnssec/maps/>



Các TLD, ccTLD tiêu biểu

- Tên miền cấp cao: .com, .net, .org, .edu, .gov, .biz, .mil, ... Tên miền khu vực: .eu, .asia
- Các nước phát triển như: .us (Mỹ), .fr (Pháp), .cz (CH Séc), .se (Thụy điển), .br (Brazil), .ru (Nga), ...
- Châu Á: .kr (Hàn quốc), .jp (Nhật), .cn (TQ), .tw (Đài Loan), .in (Ấn độ), .my (Malaysia), .id (Indonesia), .th (Thailand), ...
- Toàn bộ hệ thống Google Public DNS đã triển khai xác thực DNSSEC





DNSSEC.vn 

**LỘ TRÌNH TRIỂN KHAI
DNSSEC TẠI VIỆT NAM**

<http://www.vnnic.vn>



Quá trình nghiên cứu, thử nghiệm

2001

- Tham dự diễn đàn, hội nghị
- Tìm hiểu tiêu chuẩn

2008

- Nghiên cứu, thử nghiệm
- Đào tạo nhân lực

2014

- Xây dựng đề án
- Công bố lộ trình



Lộ trình triển khai

- Ngày 23/10/2014, Bộ trưởng Bộ TTTT ký quyết định 1524/QĐ-BTTTT phê duyệt đề án triển khai DNSSEC
- Xác định rõ mục tiêu, phạm vi, nội dung và lộ trình triển khai gồm 3 giai đoạn
 - ❑ Giai đoạn chuẩn bị: 2015
 - ❑ Giai đoạn khởi động: 2016
 - ❑ Giai đoạn triển khai: 2017





Mục tiêu & phạm vi

- Xây dựng chuỗi tin cậy (chain of trust) của DNSSEC từ các DNS cấp cao xuống DNS cấp thấp hơn, kết nối liên thông quốc tế đảm bảo tin cậy.
- Phát triển hạ tầng Internet tại Việt Nam sẵn sàng cho việc đẩy mạnh phát triển các dịch vụ thương mại điện tử, chính phủ điện tử tại Việt Nam một cách an toàn.
- Triển khai đối với tất cả hệ thống máy chủ DNS của các ISP, các nhà đăng ký tên miền “.vn” và các cơ quan Đảng, Nhà nước, Tổ chức/Doanh nghiệp.



Nội dung thực hiện

- Thông tin, tuyên truyền.
- Đào tạo, chuẩn bị nguồn lực.
- Xây dựng, ban hành cơ chế, chính sách, văn bản, hướng dẫn, tiêu chuẩn.
- Hợp tác quốc tế.
- Xây dựng kế hoạch triển khai tại các đơn vị.
- Triển khai trên hệ thống DNS quốc gia.
- Triển khai trên hệ thống DNS của doanh nghiệp, tổ chức, Cơ quan Đảng, Nhà nước ...
- Kết nối liên thông, chính thức cung cấp dịch vụ.



Các giai đoạn triển khai DNSSEC

2015

- **Giai đoạn chuẩn bị**
 - Xây dựng kế hoạch
 - Chuẩn bị điều kiện: truyền thông, nhân lực, kỹ thuật, tài chính ...

2016

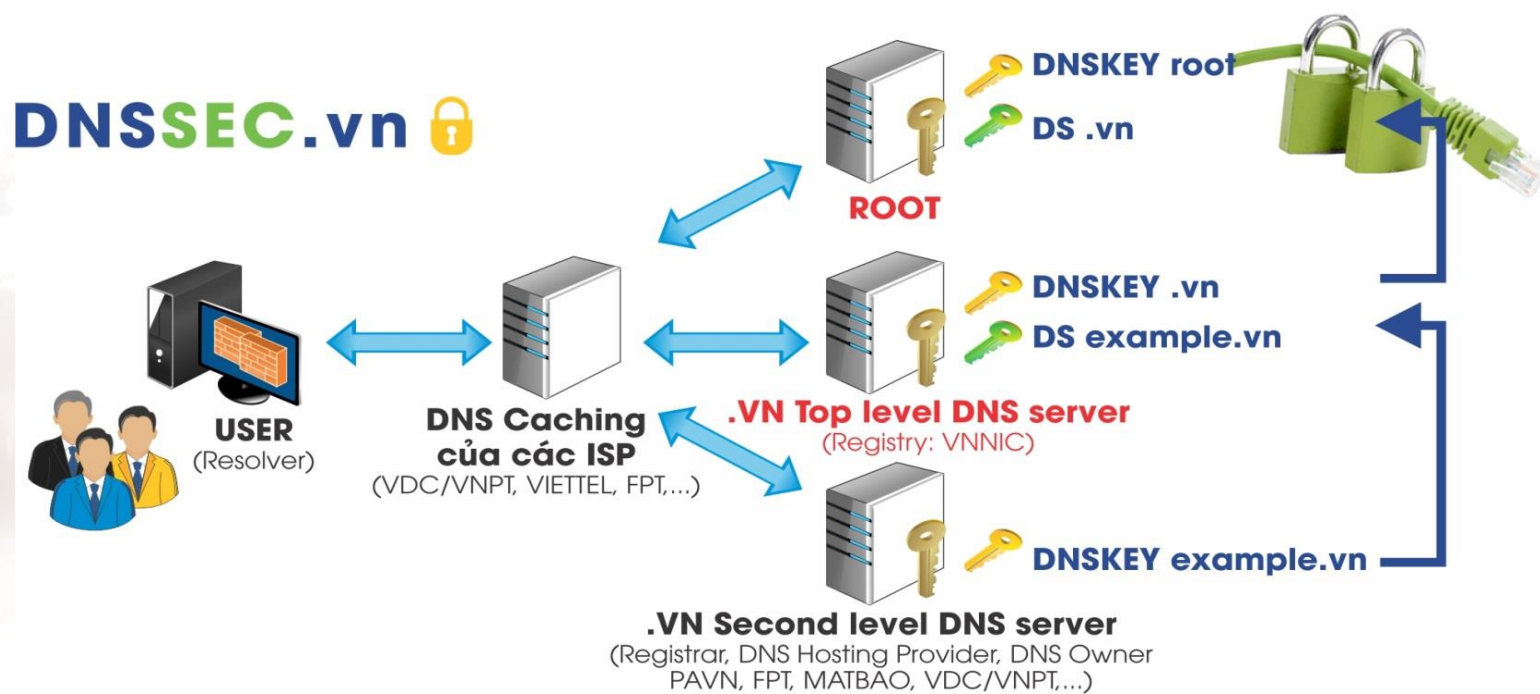
- **Giai đoạn khởi động**
 - Triển khai chính thức trên DNS quốc gia
 - Các DN, CQ, Tổ chức kết nối thử nghiệm

2017

- **Giai đoạn triển khai**
 - Triển khai chính thức trên DNS của DN, CQ, Tổ chức
 - Chính thức cung cấp dịch vụ DNSSEC



Mô hình triển khai DNSSEC



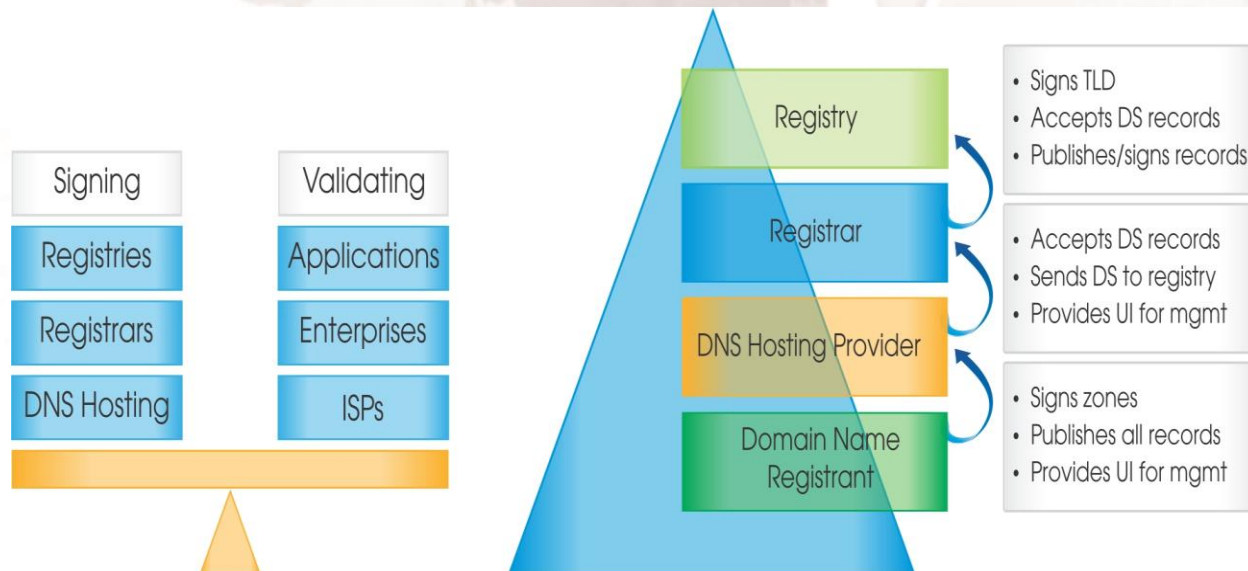
- Từng bước: ROOT → DNS TLD → DNS cấp dưới (IPS/Registrar/DNS Hosting/Ower)
- Gồm 5 giai đoạn: Experimental; Announced; Partial; DS in Root; Operational



Các đối tượng triển khai DNSSEC

○ 2 nhóm đối tượng chính:

- ❑ Nhóm ký sổ dữ liệu tên miền bao gồm: Registries, Registrars, DNS Hosting
- ❑ Nhóm kiểm tra dữ liệu tên miền: các ISP, các ứng dụng, các Enterprises





DNSSEC cho ISP

- DNS Recursive Caching: cầu nối khách hàng truy cập đến hệ thống DNS khác
- Không ký số tên miền (trừ các tên miền tự quản lý)
- Xác thực DNSSEC : Bật chế độ DNSSEC validation trong các phần mềm DNS có sẵn
- Sau khi triển khai DNSSEC:
 - ❑ Hệ thống hỗ trợ xác thực DNSSEC
 - ❑ Đảm bảo an toàn trong quá trình truy vấn của khách hàng



DNSSEC cho NĐK

- Xây dựng công cụ để hỗ trợ khách hàng cập nhật DNSSEC đảm bảo chuỗi xác thực tin cậy của hệ thống DNSSEC.
- Nâng cấp phần mềm, kết nối liên thông với hệ thống của VNNIC theo tiêu chuẩn kết nối giữa Registry- Registrar (RFC số 4310, RFC 5910) đồng bộ với việc triển khai hệ thống EPP của VNNIC.
- Hỗ trợ khách hàng trong triển khai DNSSEC.



DNSSEC cho DNS Hosting Provider

- Nâng cấp hệ thống DNS Hosting hỗ trợ DNSSEC.
- Bổ sung thêm thành phần tạo khóa, ký số tên miền
- Một số vấn đề lưu ý trong triển khai:
 - ☐ Hệ thống tạo khóa và ký zone
 - ☐ Quản lý và vận hành hệ thống theo quy trình



Kết luận

- Hệ thống DNS là cơ sở hạ tầng trọng yếu.
- Triển khai DNSSEC tại Việt Nam là rất cần thiết, phù hợp lộ trình, xu hướng thế giới.
- **Đảm bảo an toàn hạ tầng Internet Việt Nam!**



Trân trọng cảm ơn!