# Domain Name System Security Extensions

กฤต วิทวิยะรุจ
บริษัท ไทย เนม เซิฟเวอร์ จำกัด

# DNS

- ในการเข้าถึงข้อมูลใน Internet เราจำเป็นต้องระบุ Address (ที่อยู่) ในการเข้าถึงข้อมูล
- Address จะเป็น ชื่อ หรือ ตัวเลข ก็ได้ แต่ที่อยู่จะต้องไม่ซ้ำกัน
- Address ที่เป็นชื่อจะถูกแปลงให้เป็นตัวเลข IP โดยระบบที่เรียกว่า DNS
- ระบบ DNS ถูกออกแบบมาให้เป็นระบบจัดเก็บข้อมูลชื่อ Domain/Host แบบกระจาย
- ข้อมูลใน DNS จะถูกแบ่งออกเป็นลำดับขั้น หรือ Domain หรือ Zone
- ในแต่ล่ะ Zone จะมีผู้ดูแล/เจ้าของ Domain เป็นคนจัดการ/แก้ไขข้อมูล
- โดยกรรมสิทธิ์ในการจัดการ Domain จะถูกถ่ายทอดเป็นลำดับขั้นจากแม่ไปสู่ลูก
- ระบบ DNS ทำงานบนพื้นฐานของความไว้วางใจซึ่งกันและกัน
- DNSSEC คือความพยายามที่จะเพิ่มความปลอดภัยให้กับระบบ DNS

# ทำไม DNS จึงเป็นเป้าหมายในการโจมตี

- DNS มีอยู่ทุกที่ เกือบทุกๆ Client ในปัจจุบันนั้นต้องอาศัย DNS ในการทำงาน
  - โทรศัพท์, Laptop, PC, ATM?
- DNS ทำงานผ่านช่องทางที่ไม่ได้มีการเข้ารหัสใดๆ plain text
  - มีหลายวิธี/ช่องทางในระบบ DNS ที่เปิดโอกาสให้ผู้ไม่ประสงค์ดีจะเข้ามาแก้ไขข้อมูล
- การโจมตี DNS จะส่งผลต่อกระทบผู้ใช้จำนวนมาก

# DNSSEC คืออะไร

- DNSSEC เป็นส่วนขยายเพิ่มเติมของระบบ DNS
  - เริ่มต้นตั้งแต่พัฒนาครั้งแรก 1997, ออก RFC มาแล้วสามครั้งในปี 1999, 2005, 2008
- สามารถใช้ร่วมกับระบบเดิมได้ Backward compatible
- ข้อมูล DNSSEC ไม่ได้ถูกเข้ารหัส
- ข้อมูล DNS ในระบบ DNSSEC จะถูกทำการประทับตรารับรองจากผู้ดูแลโดเมนด้วยการลงนามอิเล็กโทรนิคส์ เพื่อสร้างเป็น Digital signature
- Client สามารถตรวจสอบและยืนยันความถูกต้องและสมบูรณ์ของข้อมูลที่ได้รับจาก DNS Server โดยใช้การตรวจสอบ Digital signature
  - ข้อมูลไม่ถูกปลอมแปลงโดยบุคคลอื่น
  - ข้อมูลที่ไม่ถูกต้องจะถูกทิ้งไป

# ประโยชน์ของ DNSSEC

- ระบบ DNS ทำงานบนพื้นฐานของความไว้วางใจซึ่งกันและกัน
- DNSSEC จะคอยปกป้องส่วนสำคัญในโครงสร้างพื้นฐานของ Internet
- DNSSEC ทำให้ข้อมูลในระบบ DNS มีความน่าเชื่อถือและตรวจสอบได้
- ด้วยการระบุ Public Key หรือ Fingerprint ของอุปกรณ์สื่อสารไว้ในระบบ DNS เราสามารถยืนยันตัวตนที่ถูกต้องของอุปกรณ์สื่อสารที่เราต้องการติดต่อด้วยได้
- ด้วยการนำไปใช้งานร่วมกับระบบรักษาความปลอดภัยอื่นๆ เช่น SSL จะเป็นการช่วยเสริมความปลอดภัยให้กับระบบยิ่งขึ้น

# DNSSEC ทำงานอย่างไร

- ทำงานด้วยกลไกการลงนามอิเล็กโทรนิคส์แบบใช้กุญแจสาธารณะ (public-key cryptography)
- ข้อมูล DNS records ที่จำเป็นในการตอบคำถาม DNS แต่ละชุดจะถูกนำไปแปลงให้เป็นตัวเลขสั้นๆที่เปรียบเสมือนลายนิ้วมือของชุดข้อมูลนั้นๆ
- ลายนิ้วมือของข้อมูลจะถูกลงนามอิเล็กโทรนิคส์ด้วย Private key ของผู้ดูแล Domain
- Client ในระบบ DNSSEC จะได้รับข้อมูล DNS พร้อมกับลายเซ็นของข้อมูลชุดนั้น
- ข้อมูลที่ได้รับจะถูกนำมาคำนวณหาลายนิ้วมือเพื่อนำมาใช้เปรียบเทียบกับตัวเลขที่ได้มาจากการถอดรหัสลายเซ็นด้วย Public key ที่อยู่ในระบบ DNS
- เพื่อเสริมความปลอดภัย DNSSEC ยังมีกลไกไว้สำหรับตรวจสอบการไม่มีตัวตนของข้อมูลในระบบ DNS อีกด้วย

# DNSSEC Trust anchors

- ในการตรวจสอบความถูกต้องของ Public keys ในระบบ DNSSEC เราจำเป็นจะต้องกำหนด Public key ของจุดเริ่มต้นที่เรียกว่า Trust anchors
- Trust anchors จะถูกตรวจสอบ/ติดตั้งไว้ก่อนโดยใช้ช่องทางอื่นที่ไม่ใช่ DNS
  - ติดตั้งโดยผู้ดูแล หรือ ติดตั้งผ่านระบบ update อัตโนมัติของโปรแกรม Nameserver
- Trust anchors สามารถติดตั้งได้หลายตัวตามที่ต้องการ
- โดยปกติเราต้องการ Trust anchor ของ root zone เพียงตัวเดียวเพื่อใช้งาน DNSSEC
- Trust anchor ของ root zone เริ่มประกาศใช้งานครั้งแรกเมื่อ 15 กรกฎาคม 2553 (15 July 2010)

  https://data.iana.org/root-anchors/root-anchors.xml

# การตรวจสอบ Public keys / Chain of Trust

- ในการตรวจสอบลายเซ็นของข้อมูล client จำเป็นต้องทราบ Public keys ที่ถูกต้อง
- DNS เป็นระบบข้อมูลแบบกระจายที่แบ่งเป็นลำดับขึ้นโดยแบ่งตามโดเมน
- Public Keys ของแต่ล่ะโดเมนจะถูกใส่ไว้ใน DNS และจะถูกทำลายเซ็นกำกับไว้ด้วย
- การตรวจสอบความถูกต้องของ Public keys มีสองขั้นตอน
  - ตรวจสอบลายเซ็นอิเล็กโทรนิกส์เหมือนข้อมูล DNS ทั่วไป
  - ตรวจสอบกับโดเมนแม่เกี่ยวกับ Public key ที่มีการลงทะเบียนไว้ในรูปแบบของ Digital Signer (DS) โดยตรวจสอบไล่ขึ้นไปจนถึง root zone.
- ในการใช้งาน DNSSEC โดเมนที่เกี่ยวข้องทั้งหมดจะต้องสามารถใช้งาน DNSSEC ได้
  - ถ้าโดเมนแม่ไม่สามารถใช้งานหรือ มีปัญหาที่โดเมนแม่ โดเมนลูกก็จะไม่สามารถใช้งาน DNSSEC ได้
    - www.cs.ait.ac.th = www.cs -> ait -> ac -> th -> .root

# DNSSEC กับผู้ที่เกี่ยวข้อง

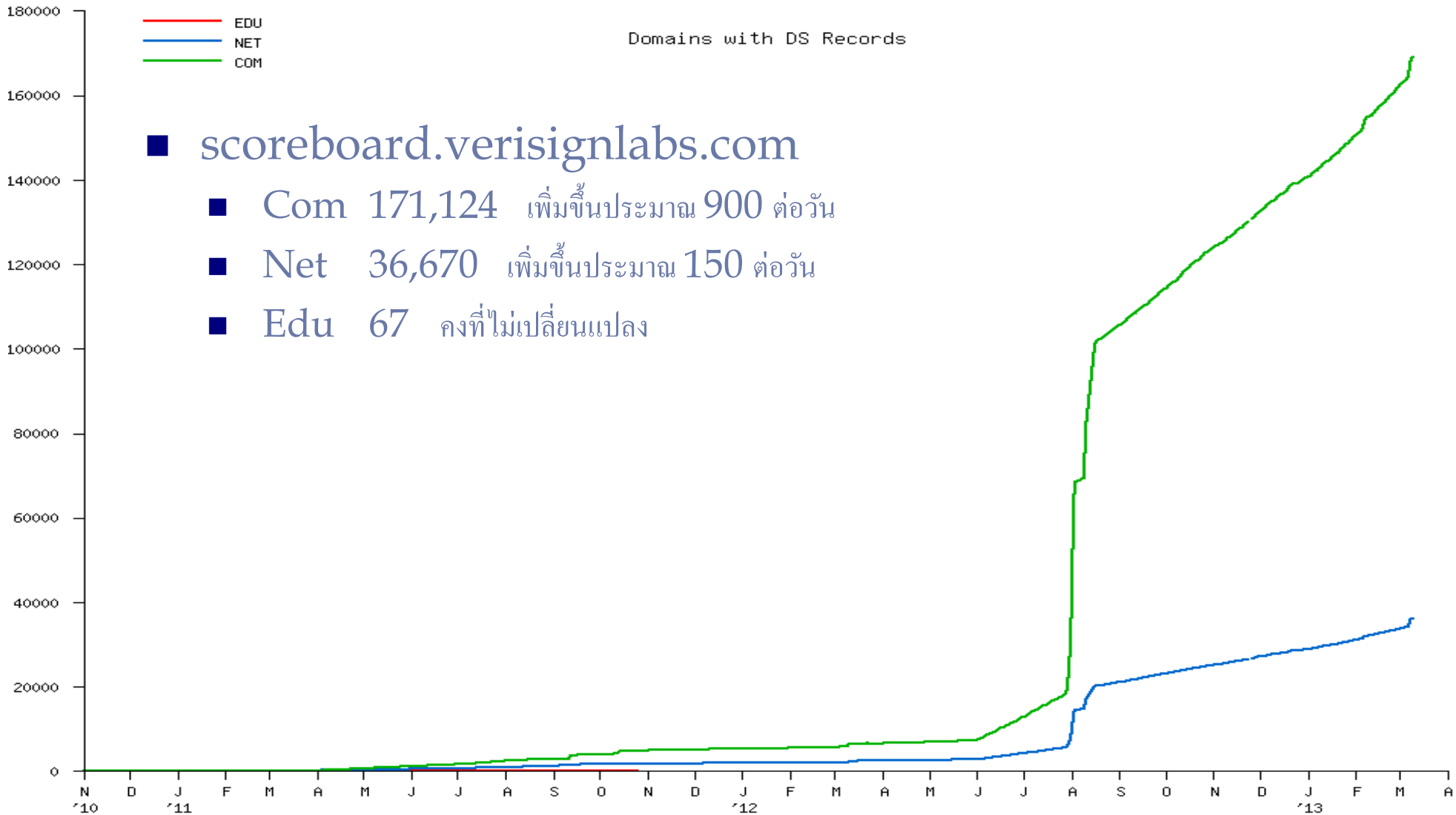
- ISP
  - DNSSEC เป็นการเพิ่มมูลค่าการให้บริการให้กับลูกค้าของ ISP ที่ต้องการความมั่นใจและปลอดภัยในการใช้งาน Internet
  - ช่วยสร้างภาพลักษณ์ที่ดี ปกป้องธุรกิจด้วยการสร้างความเชื่อมั่น รักษาฐานลูกค้าที่ใส่ใจในเรื่องของความปลอดภัย
  - ISP มีบทบาทที่สำคัญ ต่อการทำงานของ Internet
    - เป็นผู้บริหารจัดการ Recursive name servers ที่เป็นเป้าหมายหลักที่จะถูกโจมตี
  - ผู้ให้บริการ DNS Hosting ต้องรองรับ/ให้บริการ DNSSEC
- เจ้าของกิจการ/ผู้ดูแล Website
  - ช่วยเพิ่มการปกป้องการใช้งาน Online ให้แก่ลูกค้าและเจ้าของกิจการ
  - ช่วยปองกันการโจรกรรม Website จากการถูกลักลอบแก้ไขข้อมูล DNS
- ผู้พัฒนา Software
  - ขณะนี้ Software ที่สามารถใช้ประโยชน์จาก DNSSEC ยังมีไม่มากนัก
  - DNS client ไม่สามารถแยกความแตกต่างระหว่าง NXDOMAIN กับ DNSSEC fail ได้
  - พัฒนา Software ที่รองรับ DNSSEC จะช่วยให้ผู้ใช้มีความปลอดภัยมากขึ้น

# TLD ที่เริ่มมีการใช้งาน DNSSEC

- DNS ณ ปัจจุบันมีทั้งหมด 316 TLD
- 101 TLD มีการใช้งาน DNSSEC
  - 77 ccTLDs, 11 idn ccTLDs, 13 gTLDs
- gTLD ที่เริ่มใช้งาน DNSSEC
  - arpa, asia, biz, cat, com, edu, gov, info, museum, net, org, pro, mil
- TH เริ่มให้บริการ DNSSEC
  - โดยไม่คิดค่าใช้จ่ายตั้งแต่วันที่ 1 มีนาคม 2552 (2009)
  - ใช้งานร่วมกับ root anchor ได้ตั้งแต่ 23 กันยายน 2553 (2010)
  - รายละเอียดเพิ่มเติม

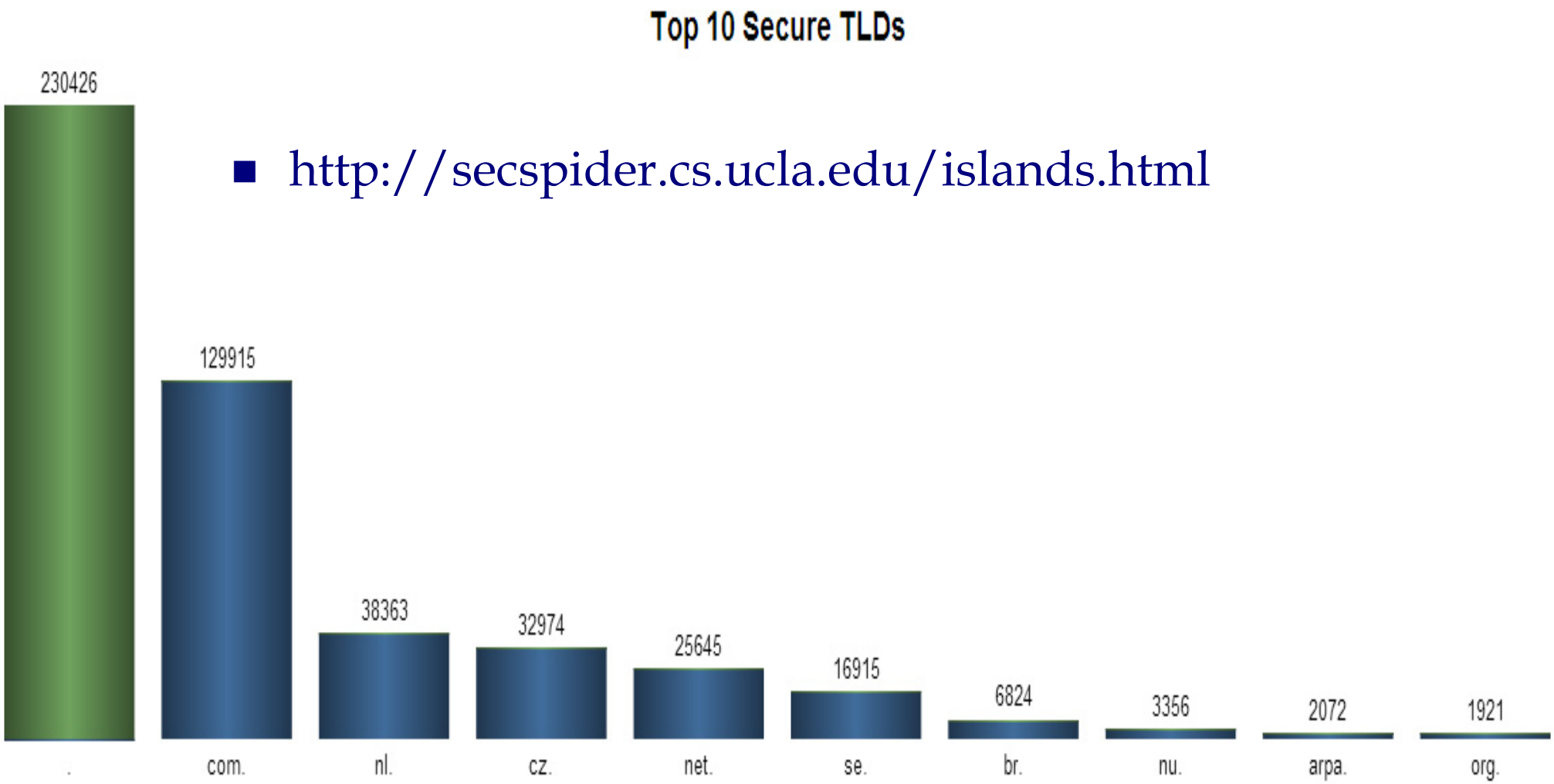
    https://www.thnic.co.th/index.php?page=dnssec

# สถิติ .COM/.NET/.EDU ข้อมูลจาก verisignlabs




- scoreboard.verisignlabs.com
  - Com 171,124 เพิ่มขึ้นประมาณ 900 ต่อวัน
  - Net 36,670 เพิ่มขึ้นประมาณ 150 ต่อวัน
  - Edu 67 คงที่ไม่เปลี่ยนแปลง

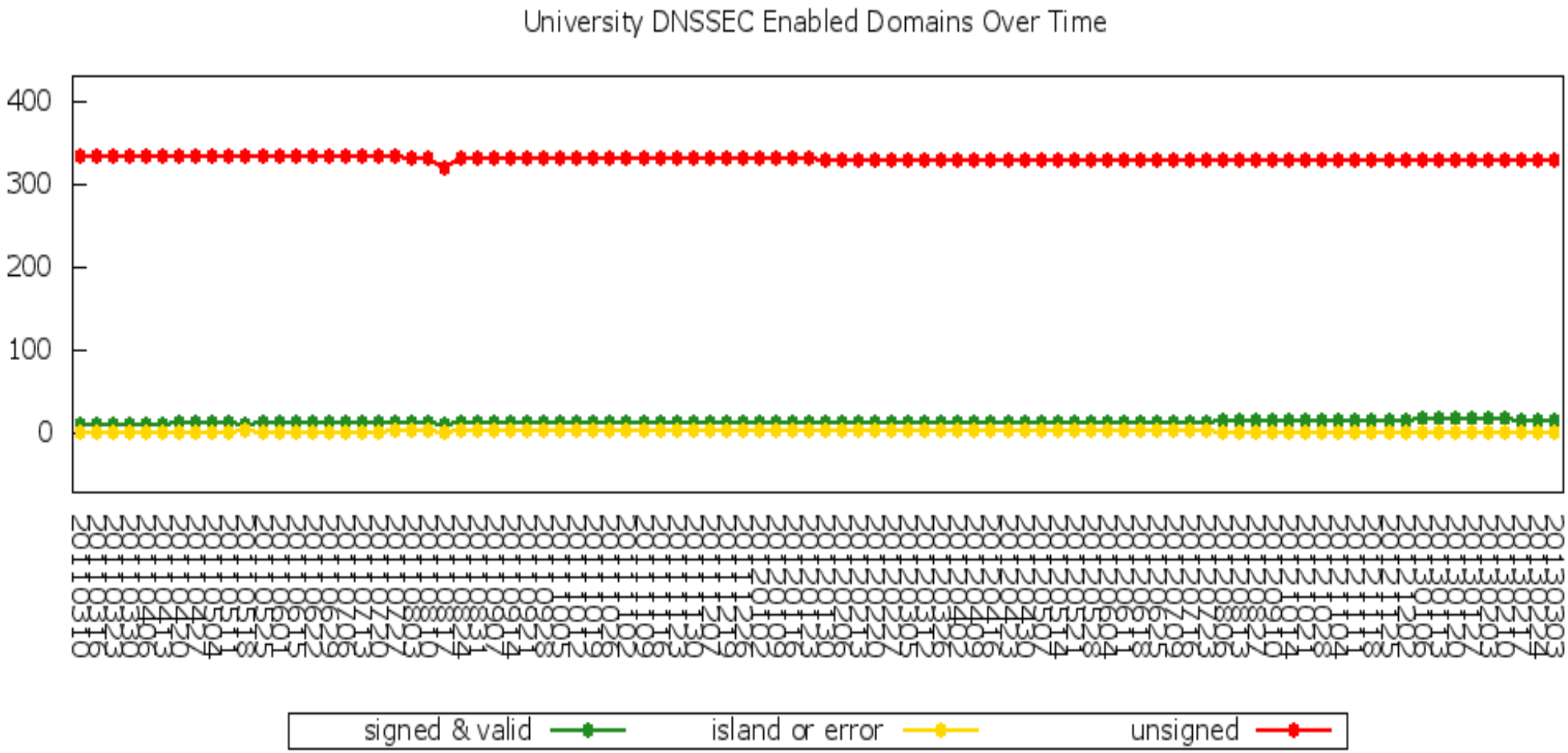
# สถิติ TOP TLDs ข้อมูลจาก secspider ucla.edu




- http://secspider.cs.ucla.edu/islands.html

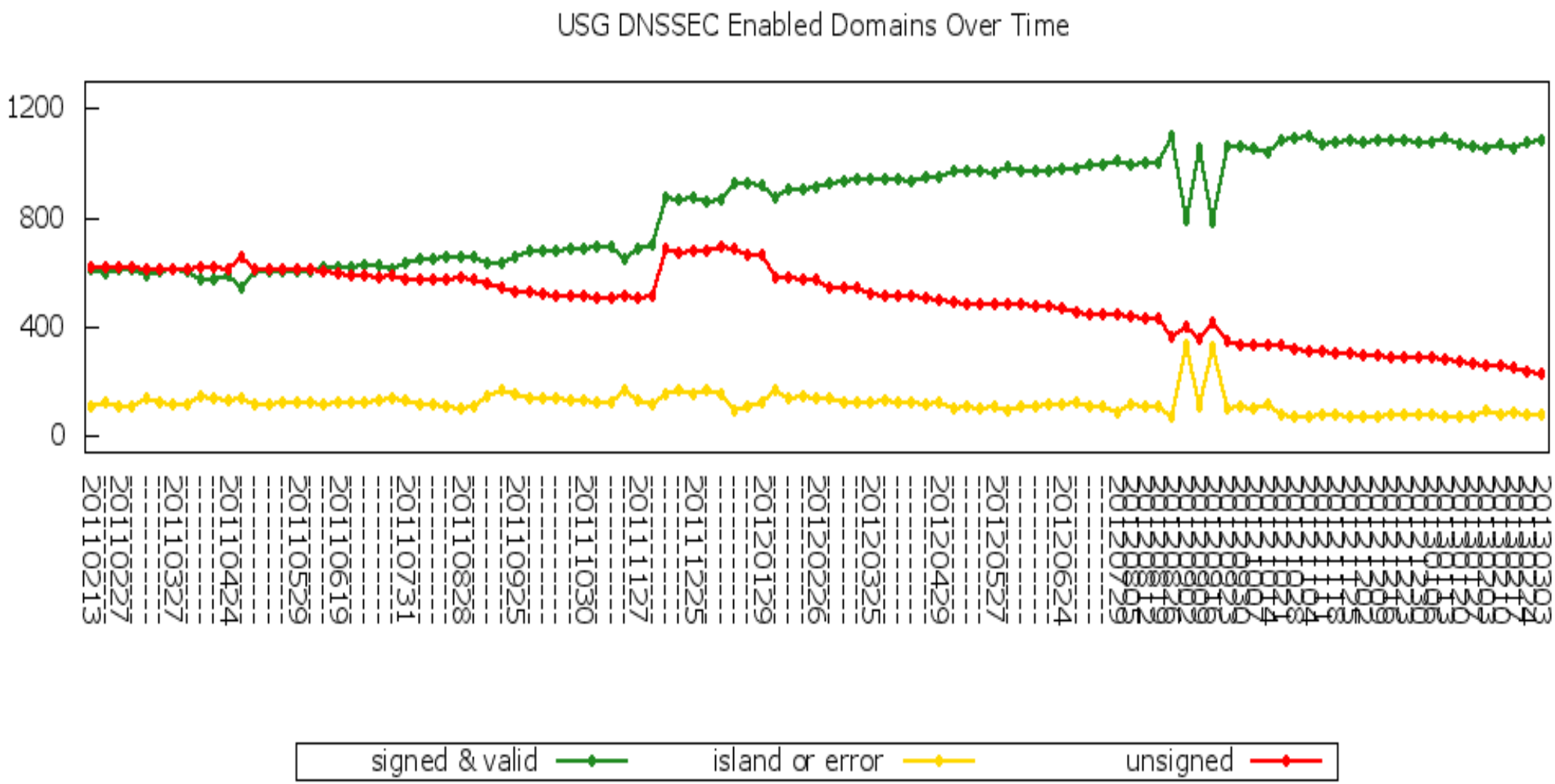
# สถิติ .EDU ข้อมูลจาก NIST 346 ตัวอย่าง

- US National Institute for Standards and Technology
- http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-edu

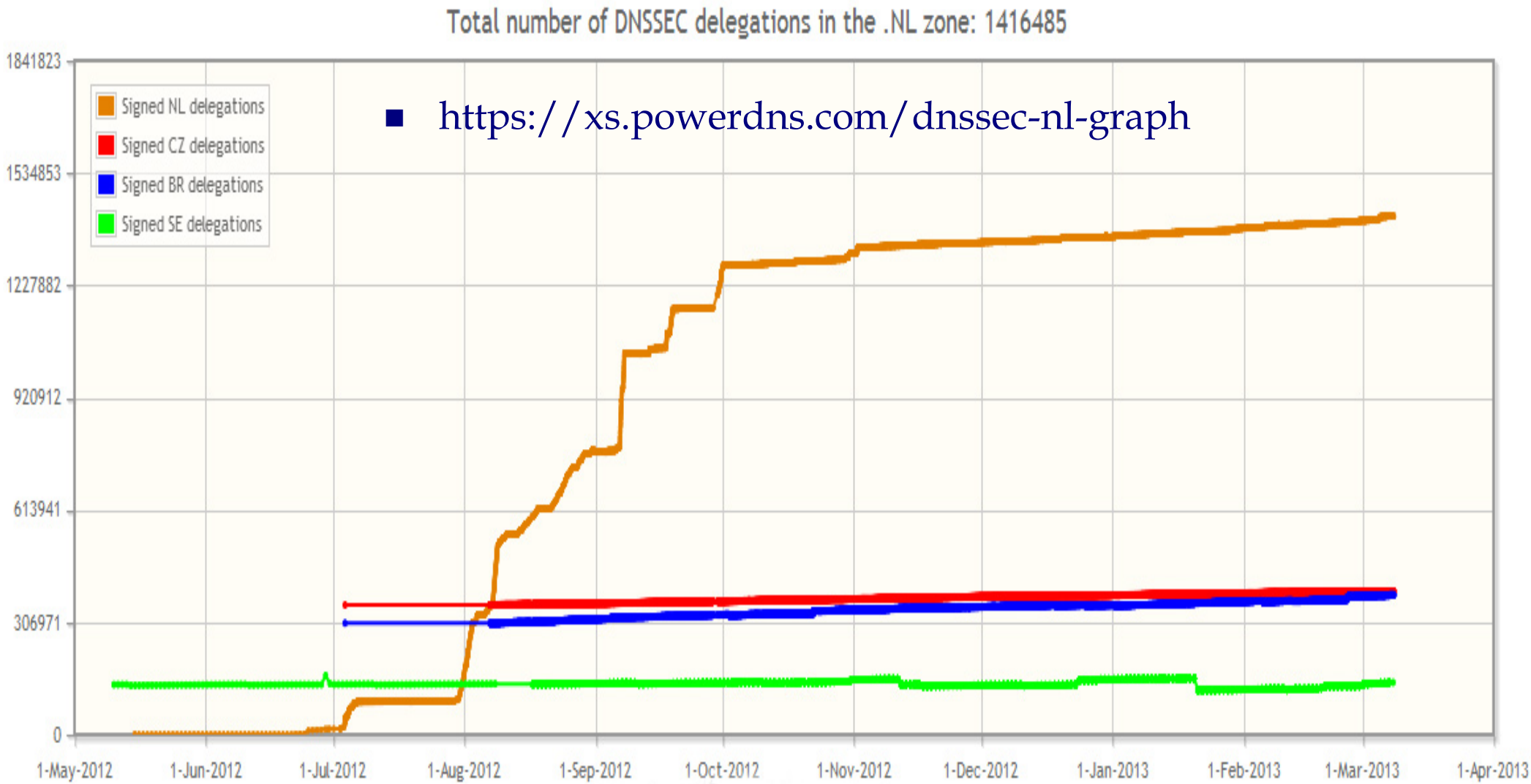


# สถิติ .GOV ข้อมูลจาก NIST 1384 ตัวอย่าง

- http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov



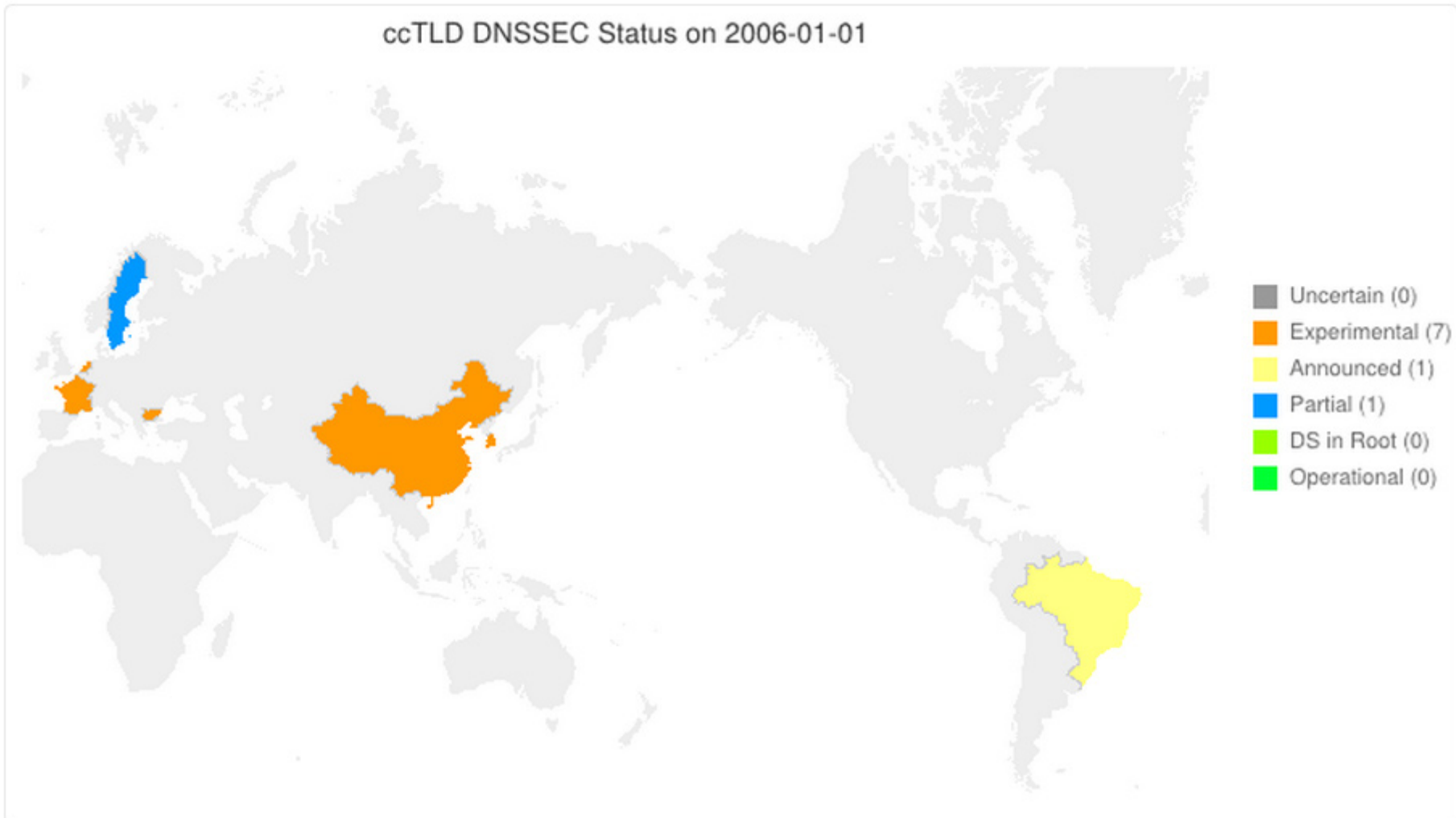
# สถิติ .NL/.CZ/.BR/.SE ข้อมูลจาก powerdns



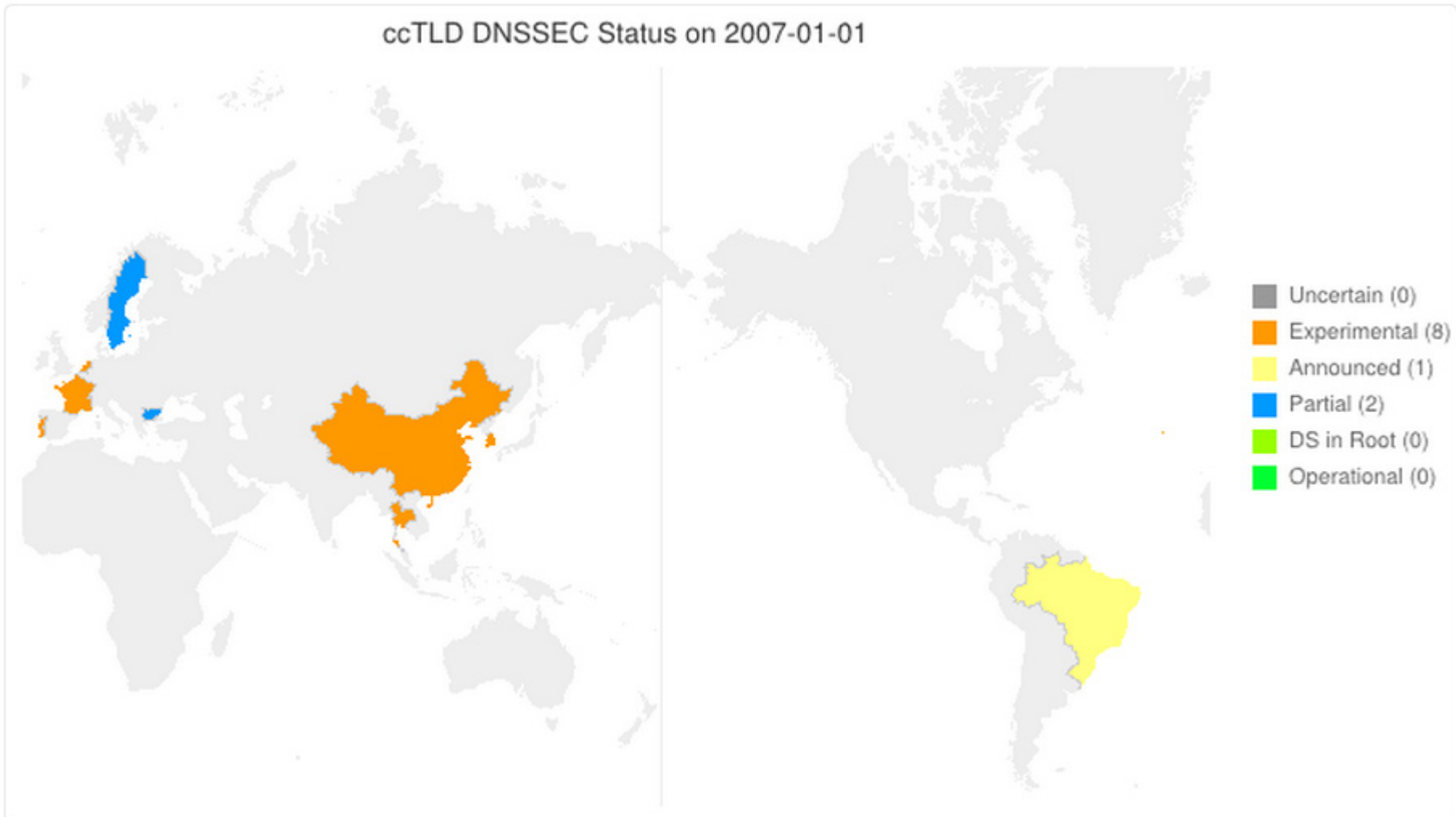

- https://xs.powerdns.com/dnssec-nl-graph

# DNSSEC กับ ccTLD

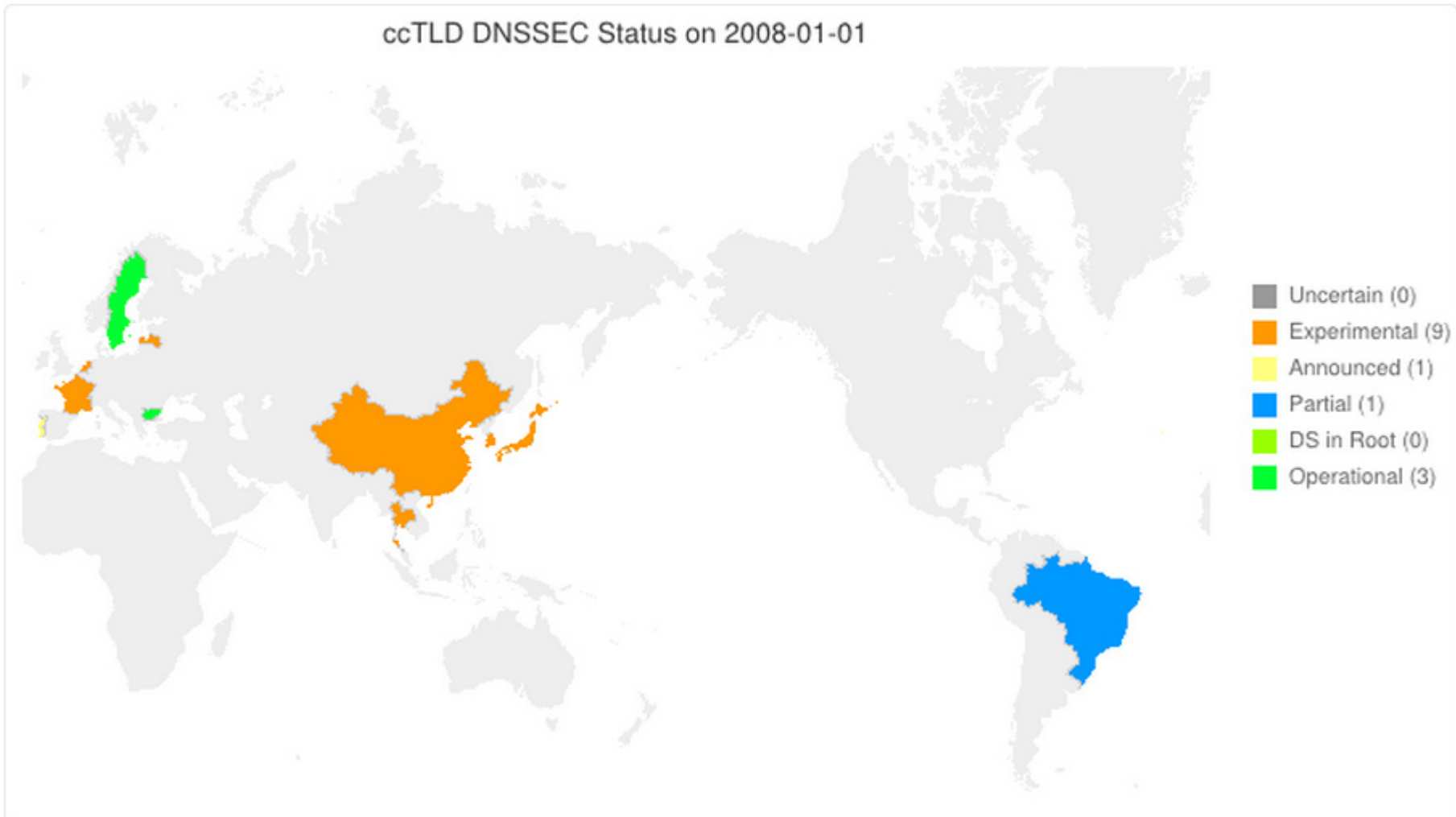
ข้อมูลจาก www.dnssec-deployment.org



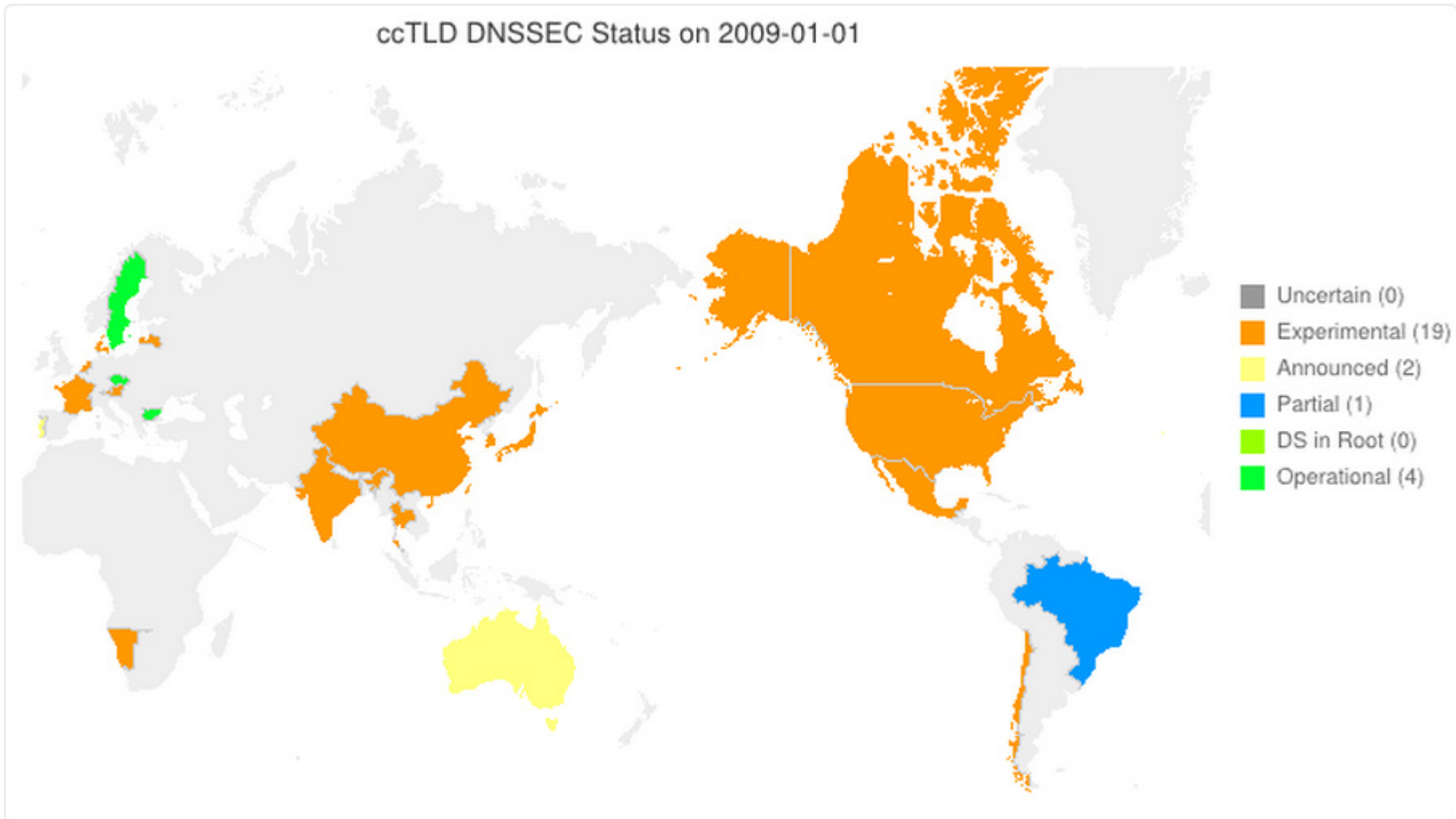
# DNSSEC กับ ccTLD



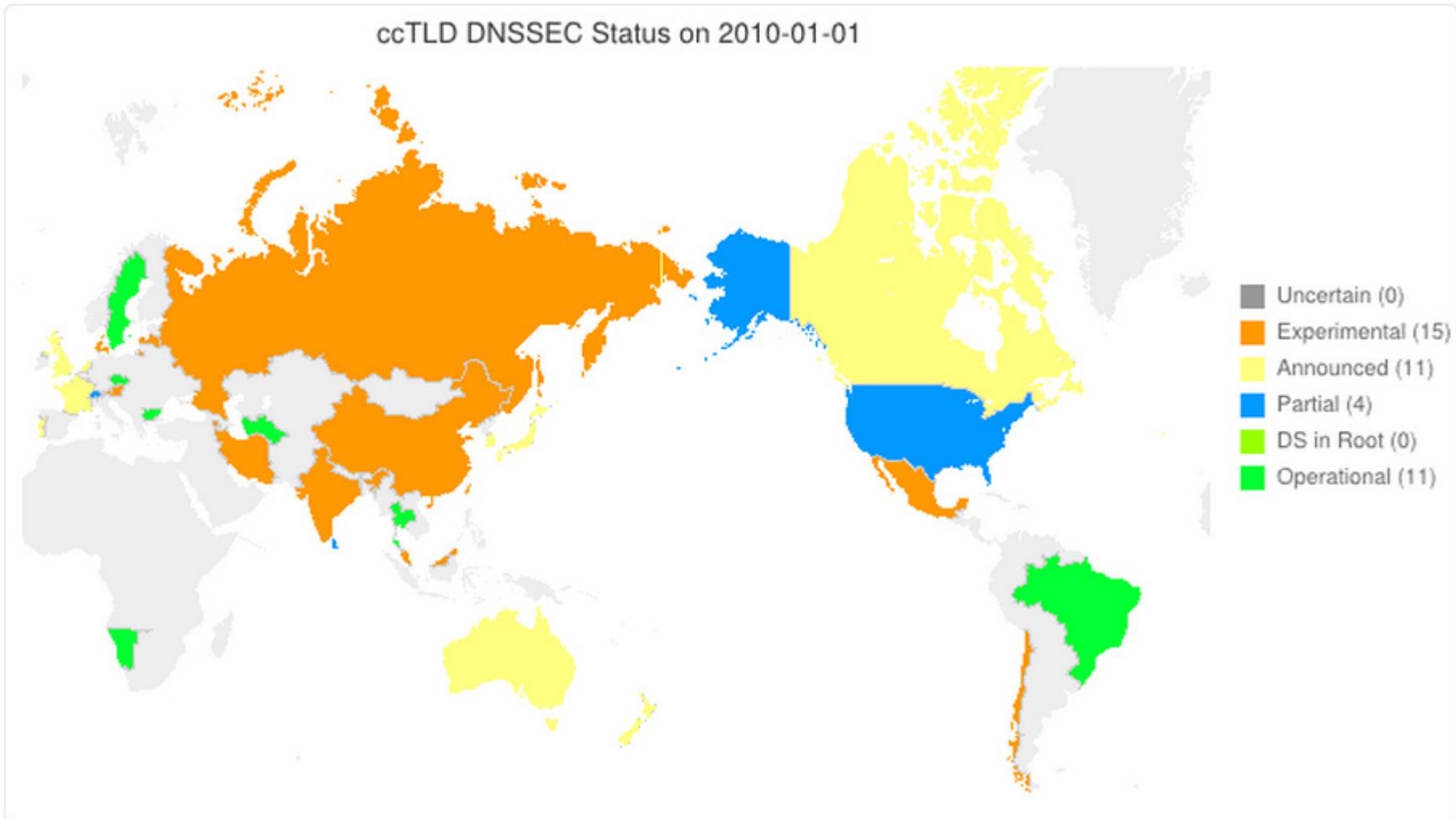
# DNSSEC กับ ccTLD



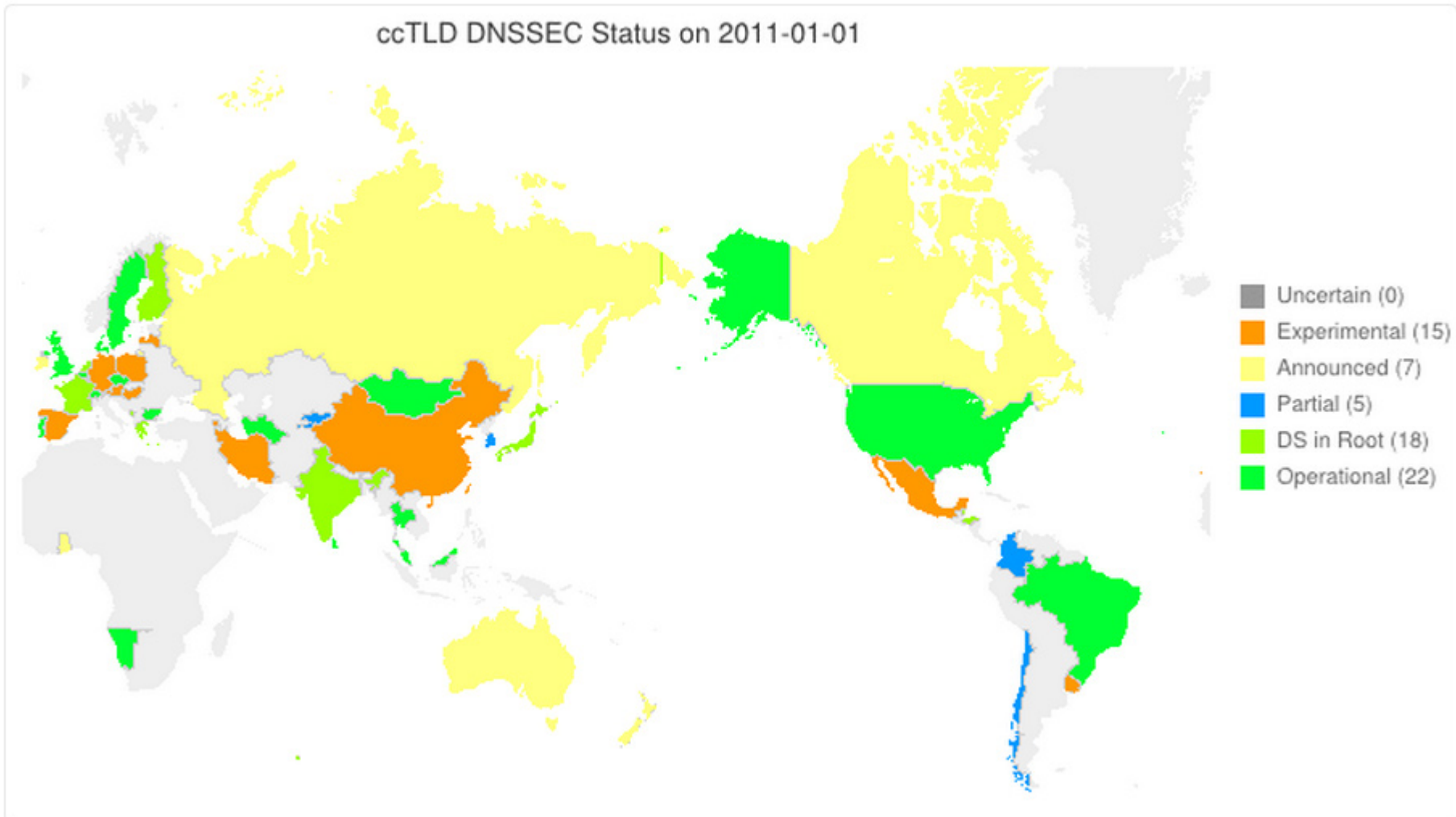
# DNSSEC กับ ccTLD



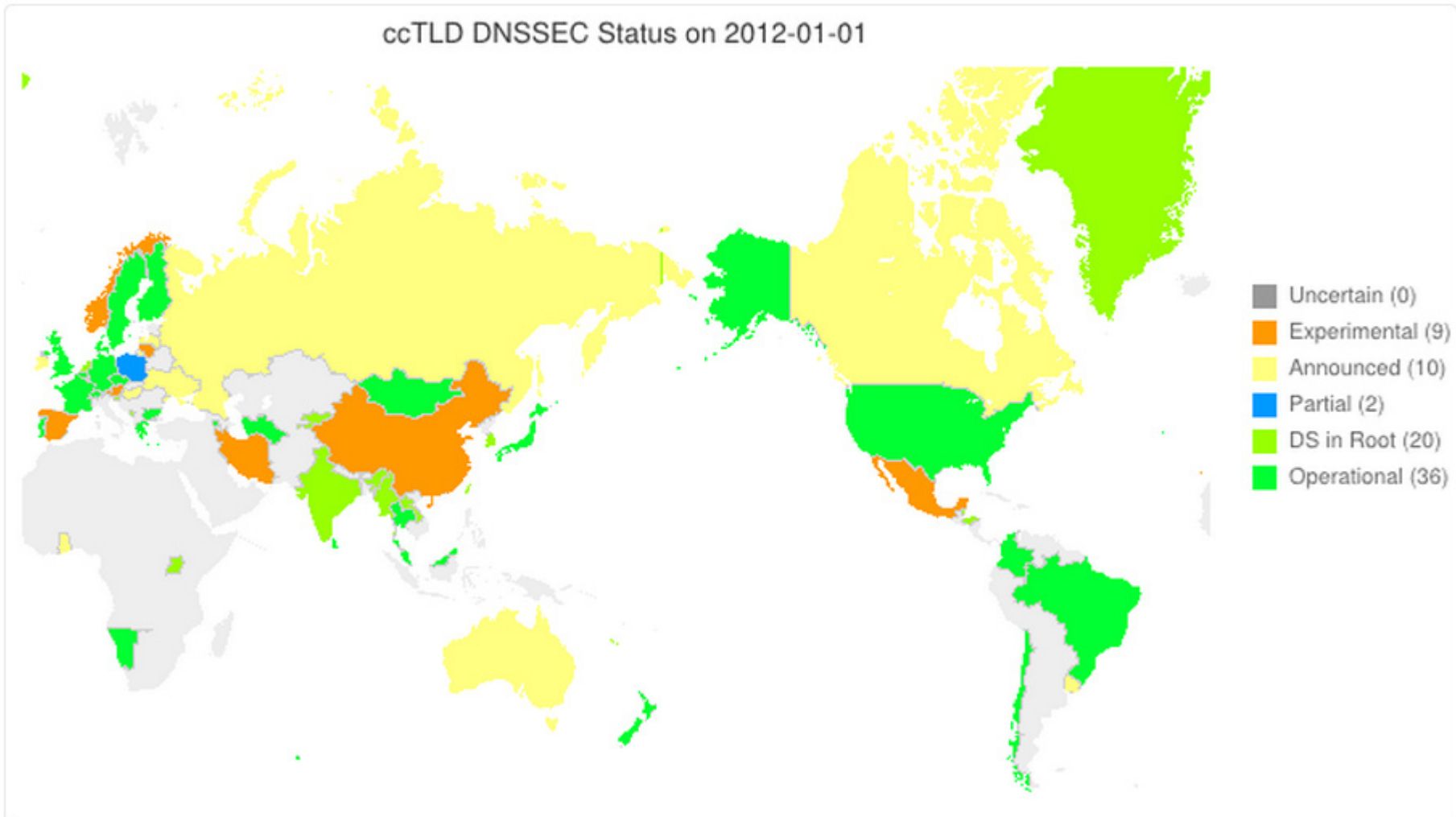
# DNSSEC กับ ccTLD



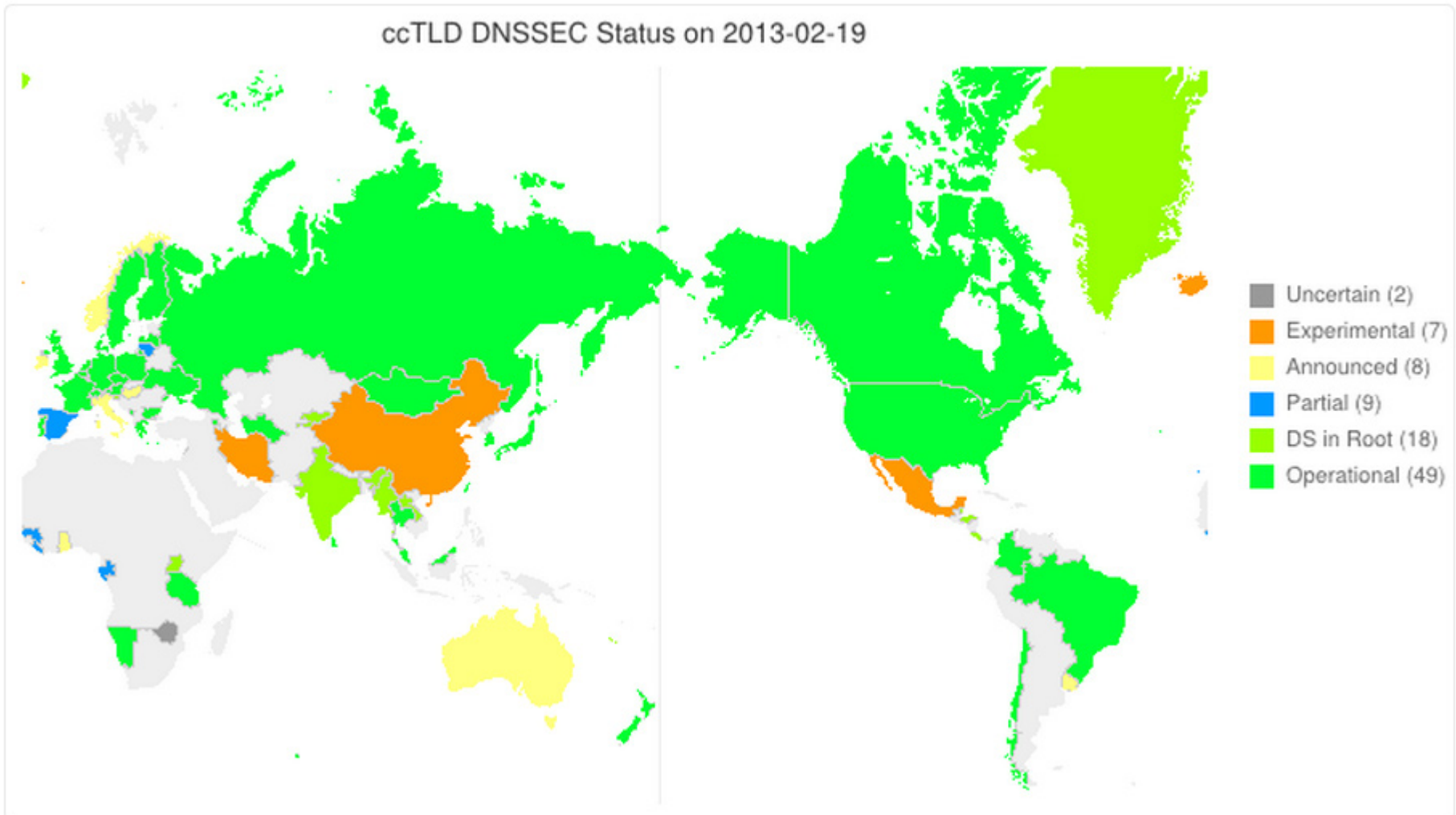
# DNSSEC กับ ccTLD



# DNSSEC กับ ccTLD



# DNSSEC กับ ccTLD



# สถิติ .TH

- 2009 & 2010
  - Thains.co.th / Thnic.co.th
  - Dotarai.co.th / Dotarai.in.th
  - Uni.net.th สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา
- 2011
  - Paypal.co.th จ่ายเงิน โอนเงิน ออนไลน์ 2011-09
- 2012
  - Ega.or.th สรอ. สำนักงานรัฐบาลอิเล็กทรอนิกส์ 2012-01
  - Eclipse.co.th ร้านอาหาร 2012-12
- 2013
  - Thnic.or.th มูลนิธิศูนย์สารสนเทศเครือข่ายไทย 2013-03
  - Thairen.net.th สมาคมเครือข่ายไทยเพื่อการศึกษาวิจัย 2013-03
  - Thailis.or.th เครือข่ายความร่วมมือพัฒนาห้องสมุดสถาบันอุดมศึกษาไทย 2013-03

# ชนิดของข้อมูลในระบบ DNSSEC

- RRSIG
  - ข้อมูลลายเซ็นอิเล็กโทรนิคส์ของชุดข้อมูล (ข้อมูลที่ถูกจัดเรียงตามลำดับและจัดเป็นกลุ่มตามชนิดของข้อมูล)
- DNSKEY
  - ข้อมูลกุญแจสาธารณะของ Domain/Zone
- DS (Delegated Signer)
  - ชุดตัวเลขสั้นๆที่ใช้แทนลายนิ้วมือของ DNSKEY
  - จะถูกใส่ไว้ ณ จุดที่ทำการส่งต่อกรรมสิทธิ์ในการดูแล Domain หรือ Domain แม่
  - เพื่อไว้ค้นหาและตรวจสอบ DNSKEY ที่ถูกต้องสำหรับการใช้งาน
- NSEC
  - NSEC/NSEC3/NSEC3PARAM
  - ข้อมูลเอาไว้ตรวจสอบการไม่มีตัวตนของข้อมูลใน Domain นั้นๆ

# DNSSEC Timing Parameters

- ข้อมูลใน DNS แต่ละอันจะมีกำหนดเวลาที่ใช้สำหรับ Caching
  - TTL และ Negative-TTL
- SOA ของ zone จะมีกำหนดระยะเวลา
  - Refresh, Update retry, Expiry, Neg-TTL
- DNSSEC keys ไม่มีกำหนดวันหมดอายุไว้ใน zone/DNS
  - ผู้ดูแลจะต้องเป็นคนพิจารณาความเหมาะสมว่าควรจะเปลี่ยน keys ใหม่เมื่อไหร่
  - ความยาวของ key ความถี่ของการใช้งาน key และ จำนวนข้อมูลที่ต้องสร้างลายเซ็นกำกับ
- ข้อมูล RRSIG แต่ละอันจะมีวันเวลาที่ลายเซ็นจะหมดอายุกำกับไว้ (และมีวันเวลาที่เริ่มใช้งาน)
  - ผู้ดูเลเป็นคนกำหนดระยะเวลาที่เหมาะสมของแต่ละ Domain/zone
  - โดยทั่วไปลายเซ็นจะมีอายุใช้งานอยู่ระหว่าง 1 อาทิตย์ ถึง 3 เดือน
  - เมื่อ RRSIG หมดอายุ จำเป็นต้องมีการสร้าง RRSIG ใหม่ / Re-Sign Zone

# Key Algorithm

- Algorithm ที่ใช้ได้กับ DNSSEC
  - RSA | RSAMD5 | DSA | RSASHA1 | NSEC3RSASHA1 | NSEC3DSA | RSASHA256 | RSASHA512 | ECCGOST | DH | HMAC-MD5 | HMAC-SHA1 | HMAC-SHA224 | HMAC-SHA256 | HMAC-SHA384 | HMAC-SHA512
- การเปลี่ยน Algorithm สำหรับ DNSSEC นั้นเป็นเรื่องค่อนข้างยุ่งยาก
  - การเลือกใช้ Algorithm ที่เหมาะสมจึงควรกระทำตั้งแต่เริ่มต้น
- Algorithm ที่นิยมใช้กันสำหรับ DNSSEC (สถิติจาก257,929 secured zones)
  - RSASHA1 152,169
  - NSEC3RSASHA1 461,715
  - RSASHA256 213,687
  - RSASHA512 1,826

# ขนาดของ Key

- ด้วยเหตผลในการบริหารจัดการในระบบ DNSSEC เราจะใช้ key สองชุดสำหรับแต่ล่ะ Zone
  - Key Signing Key (KSK) ชุดกุญแจสำหรับข้อมูล DNSKEY
  - Zone Signing Key (ZSK) ชุดกุญแจสำหรับข้อมูลทั่วไป
- Key ที่มีขนาดเล็กจะมีความเสี่ยงที่จะถูกถอดรหัสด้วยการคำนวนได้
- ขนาดของ key ที่เลือกใช้จะมีผลต่อขนาดของ ข้อมูล RRSIG (ลายเซ็น)
  - ZSK ที่มีขนาดใหญ่จะกินทรัพยากรระบบมาก, ในบางกรณีข้อมูลอาจจะใหญ่เกินกว่าที่ UDP จะรองรับได้
  - การใช้ TCP จะทำให้ประสิทธิภาพในการทำงานของระบบลดลงอย่างมาก
- ขนาดของ key ที่นิยมใช้กันมาก
  - 2048 bits สำหรับ KSK
  - 1024 bits สำหรับ ZSK, ไม่แนะนำให้ใช้ ZSK ขนาดใหญ่เกินความจำเป็น

# การเก็บรักษา Key

- การเก็บและใช้งาน Key แบบ Off-line ความเสี่ยงที่จะถูกขโมยจากภายนอกก็มีน้อย
  - เก็บ key ไว้ในเครื่องที่ไม่ได้ต่อ Network, Removable Storage, Smart card.
  - สำหรับ Domain ที่มีการแก้ไขข้อมูลบ่อยๆการเก็บ Key แบบ Off-line อาจไม่ใช่ทางเลือก
- การเก็บ Key แบบผสม
  - เก็บ Key ที่สำคัญนั่นก็คือ KSK แบบ Off-line และเก็บ ZSK แบบ On-line
  - จะเพิ่มความเสี่ยงแต่ยังให้ความสะดวกแก่การใช้งาน
  - พร้อมใช้งาน ZSK ได้ทันที สำหรับการแก้ไขข้อมูลภายใน Zone
- การเก็บ Key แบบ On-line ทั้งหมดจะมีความเสี่ยงสูงที่สุด
  - เก็บ key ไว้ในไฟล์ที่อยู่เครื่องที่มีการต่อ Network สู่ภายนอก
- การป้องกันรักษาตัว Zone File เองก็เป็นสิ่งจำเป็น
  - ปกติ Zone File จะอยู่ในเครื่องที่ On-line จึงมีความเสี่ยงสูง

# EDNS0 คืออะไร

- ระบบ DNS จำกัดขนาดข้อมูลของ UDP packet ไว้ที่ 512 bytes
- EDNS เป็นข้อกำหนดเพื่อเพิ่มขนาด parameter/flag ต่างๆของ DNS
- สามารถใช้ร่วมกับระบบเดิมได้ Backward compatible
- เพิ่มเติม option-code/flag และ option-data
  - ทำให้สามารถส่งข้อมูล DNS ผ่าน UDP ด้วยขนาดใหญ่ถึง 4096 bytes
- DNSSEC ต้องอาศัย EDNS0 ในการทำงาน
  - ข้อมูลขนาดใหญ่ บวกกับ flag ใหม่สำหรับ DNSSEC
- DNSSEC อาจมีปัญหากับการใช้งานร่วมกับ Firewall ที่จำกัดขนาดของ UDP packet

  *และ/หรือ packets ที่ถูก Fragment
  - ข้อมูลที่ Authoritative server ถูกต้อง แต่ Validate ไม่ได้

# DNSSEC servers

- Authoritative DNS/DNSSEC server
  - Server ที่เก็บข้อมูลของ zone/signed zone
  - ตอบคำถามที่เกี่ยวกับ zone ที่รับผิดชอบ/DNSSEC records
- Recursive DNS/DNSSEC server
  - Server ที่คอยส่ง DNS query หาข้อมูลในระบบ DNS
  - ทำหน้าที่ Caching ข้อมูลเพื่อเพิ่มประสิทธิภาพในการทำงาน
  - ทำหน้าที่ตรวจสอบความถูกต้องของข้อมูล DNSSEC (Validate data)
- Client คือคนที่ส่งคำถาม DNS ไปยัง Local Name Server (Recursive Server)
  - Client เป็นคนกำหนดว่าต้องการให้ Name Server ทำการ Validate DNSSEC ด้วยหรือไม่

*Client ต้องรองรับการใช้งาน DNSSEC

# DNS recursive server ที่รองรับ DNSSEC

- ISC BIND
- Unbound
- Simple DNS Plus
- Nominum Vantio
- Secure64 DNS Cache

# วิธีการติดตั้ง DNSSEC validator ด้วย BIND

- Recursive server ที่มีการสั่งให้ทำการตรวจสอบผลลัพธ์ของข้อมูล DNSSEC
  - DNSSEC-validation enabled
- ติดตั้ง ISC BIND server ที่รองรับ openssl
  - BIND 9.9.0, 9.8.1-p1 หรือใหม่กว่า
- เปิดการใช้งาน DNSSEC และ การตรวจสอบ DNSSEC
  - โดยแก้ไข Config file named.conf เพิ่มสองบรรทัดในส่วน ของ options

    dnssec-enable yes;

    dnssec-validation yes;

    ตัวอย่าง

```
options {
    dnssec-enable yes;
    dnssec-validation yes;
};
```

# วิธี download Root Public Key

- Download ผ่าน DNS ได้โดยตรง
  - Query root dnskey ด้วยคำสั่ง dig
  - Save ผลลัพท์ที่มี keyflag เป็น 257 ไว้ใน Temp file **! ชื่อไฟล์ลงท้ายด้วย .key**

dig . dnskey หรือ

dig . dnskey +noall +answer | grep 257 > temp-root.key

. 170914 IN DNSKEY 257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9…

# วิธีตรวจสอบ Root Public Key

- Run คำสั่ง dnssec-dsfromkey โปรแกรมที่มาพร้อมกับ ISC BIND

  dnssec-dsfromkey temp-root.key

  . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200F ….

- นำผลลัพธ์ไปเปรียบเทียบกับที่ประกาศไว้ในเว็บของ IANA

  https://data.iana.org/root-anchors/root-anchors.xml

```
<Zone>.</Zone>
 <KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
     <KeyTag>19036</KeyTag>
     <Algorithm>8</Algorithm>
     <DigestType>2</DigestType>
     <Digest>
       49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
     </Digest>
 </KeyDigest>
```

# วิธีการติดตั้ง root DNSSEC key ใน BIND

- ระบุ public key ของ root ลงใน named.conf นอกส่วนของ options

```
managed-keys {
  "."   initial-key  257 3 8
    "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
     FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
     bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
     X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
     W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
     Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
     QxA+Uk1ihz0=";
};
```

# วิธีการติดตั้ง DNSSEC validator ด้วย unbound

- ติดตั้ง unbound จาก source code หรือ package
  - Unbound 1.4.18 หรือใหม่กว่า
- เปิดการตรวจสอบ DNSSEC
  - โดยแก้ไข Config file unbound.conf กำหนดค่าการทำงานให้ตรวจสอบ DNSSEC

    module-config: "validator iterator"
  - กำหนดชื่อไฟล์ที่ให้ unbound เก็บ root key โดยกำหนดค่า

    auto-trust-anchor-file: /usr/local/etc/unbound/root-trust-anchor
  - กำหนด trust-anchor เริ่มแรก โดยกำหนดค่า trust-anchor:

    trust-anchor: ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32 F24E8FB5“

# ทดลองใช้งาน validator

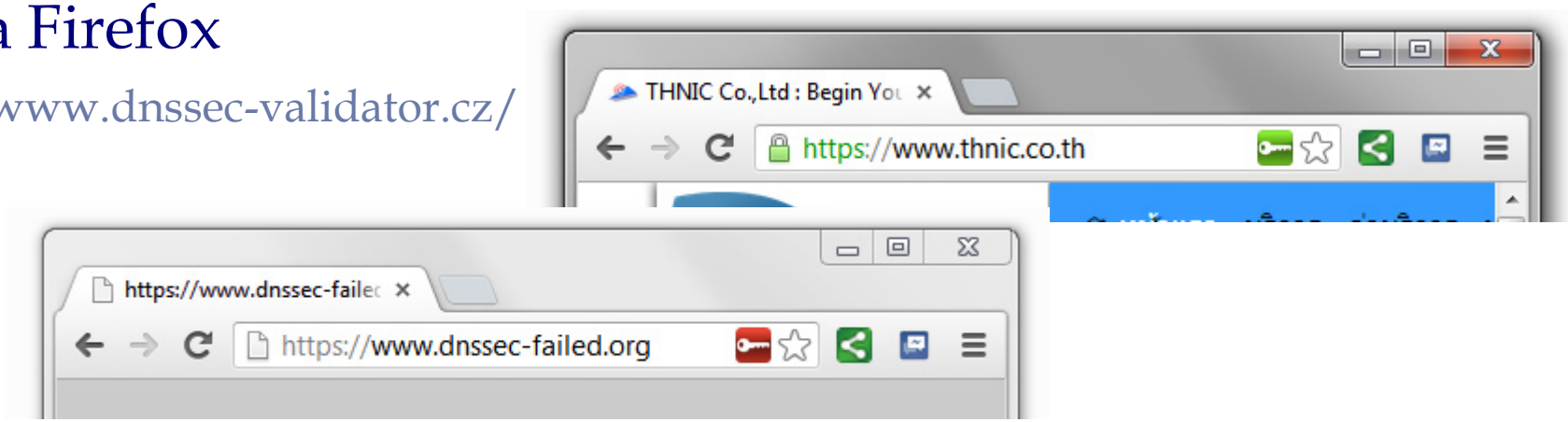
- ทดสอบการใช้งานด้วยคำสั่ง dig
  - Dig version > 9.9.0 จะมีการ set AD bit มาให้ (สนใจแต่ผลการ Validate)
  - Dig version < 9.9.0 สั่งใช้งาน DNSSEC โดยการใส่ option +dnssec หรือ +ad

dig @validator's_ip thnic.co.th +dnssec

```
; <<>> DiG 9.9.0 <<>> @xx.xx.xx.xx   thnic.co.th   +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,  id: 61994
;; flags:  qr  rd  ra  ad; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
```

# Validator ใน Browser (Plugin โดย .CZ NIC)

- สามารถติดตั้งโปรแกรมเสริมลงใน Browser เพื่อทำการตรวจสอบ DNSSEC
  - สำหรับ Debug หรือไว้เพื่อให้ผู้ใช้ตรวจสอบดูโดยผู้ใช้งานเท่านั้น
  - ติดตั้งผ่านหน้าเว็บผู้พัฒนาโปรแกรมเสริม หรือ หน้าติดตั้งโปรแกรมเสริมของ Browser ที่ต้องการ
- Internet Explorer
  - http://www.dnssec-validator.cz/ie/
- Google Chrome
  - https://labs.nic.cz/page/990/dnssec-validator-extension-for-google-chrome/
- Mozilla Firefox
  - http://www.dnssec-validator.cz/



# ข้อควรระวังสำหรับเครื่อง validator

- โปรแกรม Resolver ควรรองรับ RFC 5011 auto update Trust anchor
  - ควรตรวจสอบ Trust anchor ก่อนเริ่มใช้งานในกรณีติดตั้งเอง ควรตรวจสอบ Trust anchor เป็นระยะๆ
- ในมุมมองของโปรแกรม ชื่อที่ validate ไม่ผ่าน จะไม่ต่างกับการค้นหาชื่อไม่พบ
  - ถ้า DNSSEC มีปัญหาด้วยปัญหาทางเทคนิคหรือด้วยความตั้งใจจะทำให้ใช้งาน Domain ไม่ได้
  - ถ้าผู้ใช้งานเจอปัญหากรุณาแจ้งเจ้าของ Domain โดยเร็วที่สุด
    - ISC BIND ไม่สามารถเลือกปิดการใช้งาน DNSSEC เป็นราย Domain ได้
    - Unbound สามารถเลือกปิดการใช้งาน DNSSEC สำหรับบาง Domain ที่มีปัญหาได้
    - Unbound มี option ให้เลือก return ผลลัพธ์แม้จะValidate ไม่ผ่านได้ด้วย *(ใช้ในการ debug DNSSEC เท่านั้น)
    - Google public-dns สามารถ validate ได้ถ้า client ระบุว่าต้องการให้ validate ข้อมูล
      - ใช้งานได้ดีเมื่อติดตั้ง plug-in ใน browser ที่ทำการ validate DNSSEC
      - สามารถใช้งาน web ได้แม้ validate ไม่ผ่าน (ไม่สนใจความปลอดภัย)
- การใช้งานควบคู่ไปพร้อมกันระหว่าง DNS กับ DNSSEC validator
  - ใช้งาน nameserver 2 ตัว client จะได้รับคำตอบจากเครื่องที่ไม่ได้ validate DNSSEC (ไม่ใช่คำตอบที่ปลอดภัย)
    *ใน Windows 7, server 2008 R2 สามารถกำหนด NRPT เพื่อบังคับให้มีการ validate สำหรับ Domain ที่ต้องการได้

# ทำไมเราต้อง sign zone

- เพราะว่า Website เป็นทรัพย์สมบัติที่เป็นหน้าตาขององค์กร
- เพื่อป้องการการถูกทำ Redirect หน้าเว็บ, email, VoIP และ อื่นๆ
- เพื่อป้องกันผู้ใช้งานที่เกี่ยวข้อง ไม่ให้ตกเป็นเหยื่อถูกขโมยข้อมูลส่วนบุคคล
- เพื่อเสริมสร้างมาตราการความปลอดภัยอื่นๆ โดยใช้ DNSSEC
  - เก็บ SSH fingerprint ของ server
  - เก็บ SSL certificate ต่างๆ
- Website ที่เกี่ยวกับธุรกรรมทางการเงินต่างๆ
  - หน่วยงานที่มีกฎหมายควบคุมพิเศษ
  - นโยบายภาครัฐส่งเสริมให้มีการ sign zone ของหน่วยงานราชการกันมากขึ้น
- เพื่อนำหน้า/ทำตาม คู่แข่งทางธุรกิจ

# เครื่องมือในการ sign zone

- Open source software
  - OpenDNSSEC
  - DNSSEC-TOOLS
  - BIND 9.x
  - PowerDNSSEC
  - ZoneKeyTool
- Commercial solution/software
  - Secure64 DNS signer http://www.secure64.com
  - Xelerance DNS-X signer http://www.xelerance.om
  - IPAM vendors
    - Men & Mice, Infoblox, BlueCat networks

# การทำ DNSSEC zone signing

- โดยปกติ ในแต่ละ zone ที่ต้องการทำ DNSSEC เราต้องใช้ Key 2 ชุด

1. Key Signing Key
   - ใช้ในการสร้างลายเซ็นสำหรับ DNSKEY
   - ใช้เป็น Key ที่เอาไว้ใช้ในการสร้าง Chain of trust
   - เป็น Key ที่ เป็น Secure Entry Point (SEP) ของ Zone
2. Zone Signing Key
   - ใช้ในการสร้างลายเซ็นสำหรับข้อมูลต่างๆใน Zone

- Algorithm ที่นิยมสำหรับใช้งานในขณะนี้คือ RSASHA256

# วิธีการสร้าง key ด้วย BIND

- ตัวอย่างการสร้าง key ด้วยคำสั่ง dnssec-keygen สำหรับ zone “example.co.th”
  - สร้าง Key-Signing-Key (KSK) -f KSK (กำหนด SEP flag ให้เป็น 1)

```
dnssec-keygen -K /var/named/dnssec-keys -a RSASHA256 –b 2048 –f KSK example.co.th
Generating key pair.....................+++ .............+++
Kexample.co.th.+008+07186
```

  - สร้าง Zone-Signing-Key (ZSK)

```
dnssec-keygen -K /var/named/dnssec-keys -a RSASHA256 –b 1024 example.co.th
Generating key pair.........++++++ ............++++++
Kexample.co.th.+008+45399
```

  - Key ที่ถูกสร้างจะถูกเก็บไว้ที่ directory ที่ระบุไว้ใน option -K /var/named/dnssec-keys

# วิธีการ sign zone ด้วย BIND

- Sign zone ด้วยตนเอง
  - การ Sign zone ด้วยตนเอง ผู้ดูแล zone จะต้องบริหารจัดการ key เอง
  - include หรือใส่ DNSKEY records ที่ต้องการใช้งานเข้าไปใน zone
    - Validator จำเป็นต้องใช้ DNSKEY ในการ validate ข้อมูล
  - สั่ง sign zone ด้วยคำสั่ง dnssec-signzone

```
dnssec-signzone -K /var/named/dnssec-keys -o example.co.th db.example.co.th
```

  - Zone ที่ถูก sign แล้วจะอยู่ใน file .signed (db.example.co.th.signed)

- เปิดการใช้งาน DNSSEC โดยแก้ไข named.conf
  - กำหนด dnssec-enable yes; ในส่วน ของ options
  - ต้องทำการ reload zone/config หลังทำการ sign zone/แก้ไข config ก่อนเริ่มใช้งาน

# วิธีการ sign zone แบบอัตโนมัติ

- ได้มีการเพิ่มความสามารถในการ sign zone แบบอัตโนมัติขึ้นใน BIND 9.7.0
  - 9.9.0 เพิ่มการทำงานในแบบ inline-signing
- เพิ่ม option ใน named.conf ให้ระบุการทำงาน auto-dnssec ได้สองรูปแบบ
  - เมื่อกำหนดค่า auto-dnssec เป็น allow เราจะสามารถทำงานสั่ง sign zone แบบกึ่งอัตโนมัติได้

    rndc sign <zone>
  - ในโหมด maintain โปรแกรม nameserver จะ sign zone อัตโนมัติโดยการตรวจสอบ metadata ที่อยู่ใน keys ของแต่ละ Zone
    - สร้าง key แบบระบุวันเวลาการใช้งานของ key
    - จะทำการตรวจสอบการเปลี่ยนแปลงของ key ทุกๆ 60 นาที
    - ตั้งค่าความถี่ได้ด้วย option dnssec-loadkeys-interval
    - สามารถสั่ง rndc loadkeys เพื่อทำการตรวจสอบได้ทันที

    rndc loadkeys <zone>

# วิธีการติดตั้ง auto-dnssec ใน named.conf

- การใช้งาน auto-dnssec ต้องเปิดใช้งาน dynamic update
  - allow-update หรือ update-policy

  *inline-signing ไม่จำเป็นต้องเปิดใช้งาน dynamic update
- กำหนด Directory ที่เก็บ key
  - key-directory "/var/named/dnssec-keys";

```
zone “example.co.th” {
        type            master;
        file            “db.example.co.th”;
        update-policy   local;
        key-directory   “/var/named/dnssec-keys”;
        auto-dnssec     maintain;
};
```

- เริ่มใช้งาน ด้วยการ start server หรือ rndc reconfig

# การดูแล secured zone

- ข้อมูลในระบบ DNS เดิมไม่ต้องการการดูแลจาก Admin
- DNSSEC ได้กำหนดให้ข้อมูล RRSIG มีเวลาหมดอายุ
  - เราสามารถกำหนดวันหมดอายุของ RRSIG ได้เอง
  - ระยะเวลาการใช้งานของ RRSIG อยู่ในช่วง 1 อาทิตย์ ถึง 3 เดือน
- RRSIG ที่หมดอายุจะไม่สามารถใช้งานได้ (ไม่สามารถ validate ข้อมูลได้)
  - Domain ไม่อาจใช้งานได้ ถ้ามีการเปิดใช้งาน DNSSEC ไว้ที่ recursive DNS server และ/หรือที่เครื่อง client
- ผู้ดูแลจะต้องคอยทำการ Re-sign zone เป็นระยะๆ แม้ว่าจะไม่ได้มีการแก้ไขข้อมูลใน zone*
  - ปกติ BIND จะตั้งเวลาการใช้งานของ RRSIG อยู่ที่ 30 วัน โดยมีผลย้อนหลัง 1 ชม ก่อนการ sign
  - ในการทำงาน Sign zone แบบอัตโนมัติ BIND จะทำการ re-sign zone ก่อนวันหมดอายุจริง (เมื่อถึง 3/4 ของอายุการใช้งานของ RRSIG หรือ ก่อนหมดอายุ 7.5 วันโดยปกติ)

# เครื่องมือสำหรับตรวจสอบ DNSSEC ผ่านทางหน้า Web

- ควรตรวจสอบ secured zone จาก network ภายนอกองค์กร
- Signed zone check
  - http://dnsviz.net
  - http://dnssec-debugger.verisignlabs.com
- Validator check
  - http://www.dnssec-failed.org
  - http://dnssec.vs.uni-due.de
  - http://test.dnssec-or-not.com
  - http://dnssectest.sidn.nl/test.php
- DNS (Nameservers & Zone) check
  - http://dnscheck.iis.se
- Network Check
  - http://netalyzr.icsi.berkeley.edu/index.html

# การดูแล secured zone และการแจ้งเตือน

http://dns.comcast.net/index.php/categories/listings/dnssec-news

This site provides you with the Comcast DNS server status, IP addresses, and troubleshooting tools. As part of our ongoing efforts to protect our customers and provide great security features, DNSSEC validation is now included as part of Comcast Constant Guard™ from Xfinity.

## DNSSEC News

Subscribe to feed  80 posts in this category

### coffeecupmonument.com Failing DNSSEC Validation

**Posted by Comcast on March 11, 2013 in DNSSEC News**

The domain coffeecupmonument.com is currently failing DNSSEC validation. This is because there are published DS records, but no corresponding DNSKEY records. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/coffeecupmonument.com/UT3dOQ/dnssec/.

Tags: DNSSEC

### uspto.gov Failing DNSSEC Validation

**Posted by Comcast on March 01, 2013 in DNSSEC News**

The domain uspto.gov is currently failing DNSSEC validation. This is because the RRSIGs covering the domain have expired. The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/uspto.gov/UTEOsQ/dnssec/.

Tags: DNSSEC

# การดูแล secured zone และการแจ้งเตือน

## nsopw.gov Failing DNSSEC Validation

**Posted by** Comcast **on February 14, 2013 in** DNSSEC News

The domain nsopw.gov is currently failing DNSSEC validation. This is because the domain was signed by DNSKEYs that do not correspond to the DS records in parent domain (.gov). The domain owners have been contacted and made aware of the issue. The DNSViz report of this failure can be found at http://dnsviz.net/d/nsopw.gov/URwiqQ/dnssec/

Tags: DNSSEC

## www.clinicaltrials.gov Failing DNSSEC Validation

**Posted by** Comcast **on February 13, 2013 in** DNSSEC News

The domain www.clinicaltrials.gov is currently failing DNSSEC validation in some areas. This is because the domain rolled it's keys and the old ones are still cached. The domain owners contacted us to make us aware of the issue. We will be flushing the platform and resolution should resume shortly.

Tags: DNSSEC

## www.medlineplus.gov Failing DNSSEC Validation

**Posted by** Comcast **on February 13, 2013 in** DNSSEC News

The domain www.medlineplus.gov is currently failing DNSSEC validation in some areas. This is because the domain rolled it's keys and the old ones are still cached. The domain owners contacted us to make us aware of the issue. We will be flushing the platform and resolution should resume shortly.

Tags: DNSSEC

## faa.gov Failing DNSSEC Validation (Fixed)

**Posted by** Comcast **on February 13, 2013 in** DNSSEC News

# การบริหารจัดการ keys

- ในการใช้งาน DNSSEC เราต้องบริหารจัดการ key ที่ใช้
  - สถานที่จัดเก็บ
  - วันเวลาที่ใช้งาน
  - ประกาศ public key ทาง web หรือ ใน DNS
  - เปลี่ยน key ใหม่
- วิธีการเปลี่ยน Key ใหม่และขั้นตอนการเปลี่ยน key
  - ประเภทของ key ที่จะเปลี่ยน KSK หรือ ZSK
  - เปลี่ยน algorithm ของ key ด้วยหรือไม่
  - อ่านเพิ่มเติมใน RFC 6781

# เครื่องมือบริหารจัดการ keys

| Component | BIND 9.7.0 | DNSSEC-TOOLS | OpenDNSSEC |
|---|---|---|---|
| DNSSEC key lifecycle | Metadata stored in DNSSEC Keys | zone keyrec file | signconf XML datafile |
| Zone Signing | Smart Sign/ Automatic | zonesigner CLI | ods-signzone CLI |
| DNSSEC key rollover | Not fully implemented | rollerd daemon | ods-signerd daemon |

# Conclusions

- เริ่มมีการใช้งาน DNSSEC มากยิ่งขึ้น หลังจาก root และ top TLD เปิดให้บริการ
- DNSSEC ถูกออกแบบให้สามารถใช้ร่วมกับระบบ DNS เดิมได้
- Infrastructure ณ ปัจจุบันรองรับการใช้งาน DNSSEC
- สามารถเริ่มติดตั้ง validator หรือ เปิดใช้งาน validation ที่เครื่อง server ที่มีอยู่ได้ทันที
  - ผู้ให้บริการ ISP ราย ใหญ่ ใน US เช่น Comcast เริ่มให้บริการ DNSSEC มาตั้งแต่ต้นปี 2012
- เริ่มวางแผนในการ sign zone / ให้บริการ sign zone แก่ลูกค้า