How DNSSEC Works

กฤต วิทวิยะรุจ
บริษัท ไทย เนม เซิฟ เวอร์ จำกัด

DNSSEC ทำงานอย่างไร

- ข้อมูล DNS records ที่จำเป็นในการตอบคำถาม DNS แต่ละชุดจะถูกนำไปแปลงให้เป็นตัวเลขสั้นๆที่เปรียบเสมือนลายนิ้วมือของชุดข้อมูลนั้นๆ

```
thnic.or.th.        86400   IN      A       203.150.1.139
```

```
3ab28b19a55e1021b9605cc7d738745115e59b46
```

- ลายนิ้วมือของข้อมูลจะถูกลงนามอิเล็กโทรนิคส์ด้วย Private key ของผู้ดูแล Domain

```
RRSIG  A  5  3  3600  20130413022859  20130314022859 58941    thnic.or.th.
dWrk4hHP3/vdvLept3aTCLWQWNnahDg/wC//RNW00kKbVu4m0IeH6Q1X
smQ1HDYDLc3HuiibNJxtrTib0ZbeYoYteSB/4MdOz5BDj26Tdm/SdQFn
UqSzozhFR3dCSnzP6B7+YddK95YJF/LLcmOancSUOUiRvk4FhlgVr9CA pQU=
```

DNSSEC ทำงานอย่างไร

- ลายเซ็นของข้อมูลจะถูกถอดรหัสโดยอาศัย Public key ของ Damain

RRSIG A 5 3 3600 20130413022859 20130314022859 58941 thnic.or.th.
dWrk4hHP3/vdvLept3aTCLWQWNnahDg/wC//RNW00kKbVu4m0IeH6Q1X
smQ1HDYDLc3HuiibNJxtrTib0ZbeYoYteSB/4MdOz5BDj26Tdm/SdQFn
UqSzozhFR3dCSnzP6B7+YddK95YJF/LLcmOancSUOUiRvk4FhlgVr9CA pQU=

+

DNSKEY 256 3 5 AwEAAcvTyZ1w6QNuuyXoZS+/ArNrOxGOprv9KjqdeqX6Iu2lt7Q8QOFH
sVwJF/Gh5abGllnBGJYykLXqJQnrMninyPW/2YdyKEdP1XJwtkCwKcsK
hBP+ACD5cvJey7QOh3GyDZCWjlE2POgSltg0jXd2sHqzqF8yaagogz5q HG6u5cJ9

3ab28b19a55e1021b9605cc7d738745115e59b46

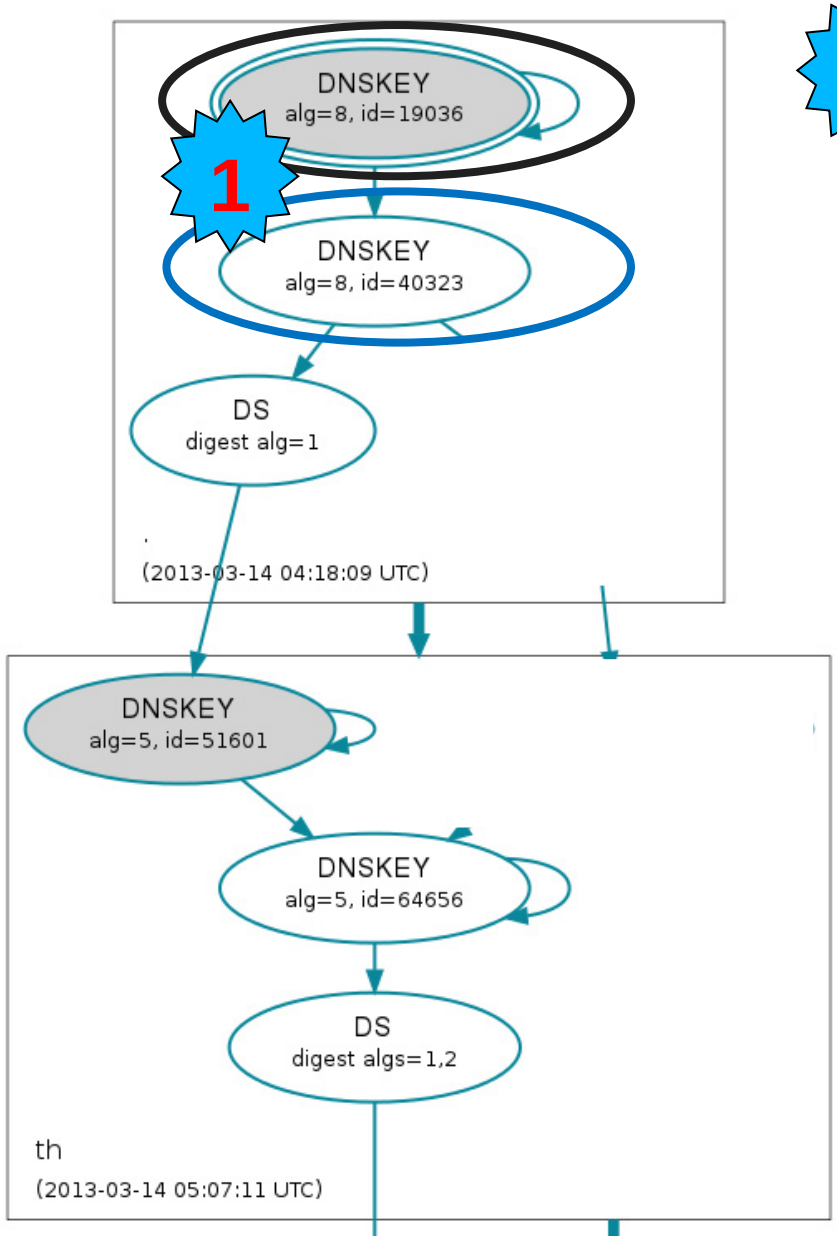
=

3ab28b19a55e1021b9605cc7d738745115e59b46

Trust anchor (กุญแจที่ไว้วางใจ)

- ในการตรวจสอบความถูกต้องของ Public keys ในระบบ DNSSEC
- เราจำเป็นจะต้องกำหนด Public key ของจุดเริ่มต้นที่เรียกว่า Trust anchors
- Trust anchors จะถูกตรวจสอบ/ติดตั้งไว้ก่อนโดยใช้ช่องทางอื่นที่ไม่ใช่ DNS
  - ติดตั้งโดยผู้ดูแล หรือ ติดตั้งผ่านระบบ update อัตโนมัติของโปรแกรม Nameserver
- โดยปกติเราต้องการ Trust anchor ของ root zone เพียงตัวเดียวเพื่อใช้งาน DNSSEC

การตรวจสอบ Public keys / Chain of Trust



1 www.thnic.or.th A ?

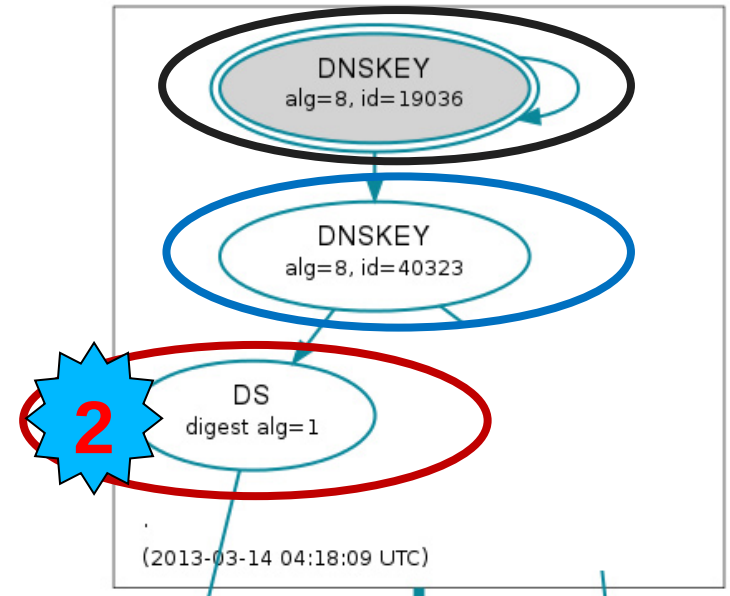
เริ่มต้นจากการขอข้อมูล DNSKEY ของ root zone ในระบบ DNSSEC

DNSKEY 19036 DNSKEY 40323 ✓

ลายเซ็นกำกับเซ็นโดย key 19036 ✓

Trust anchor key/DS 19036

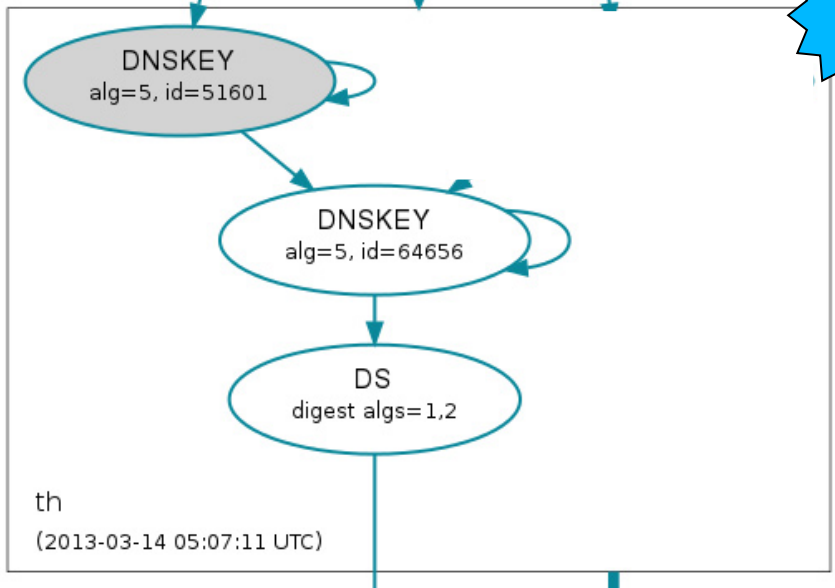
การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
เริ่มต้นจากการขอข้อมูล DNSKEY ของ root zone ในระบบ DNSSEC

DNSKEY 19036 DNSKEY 40323

ลายเซ็นกำกับเซ็นโดย key 19036



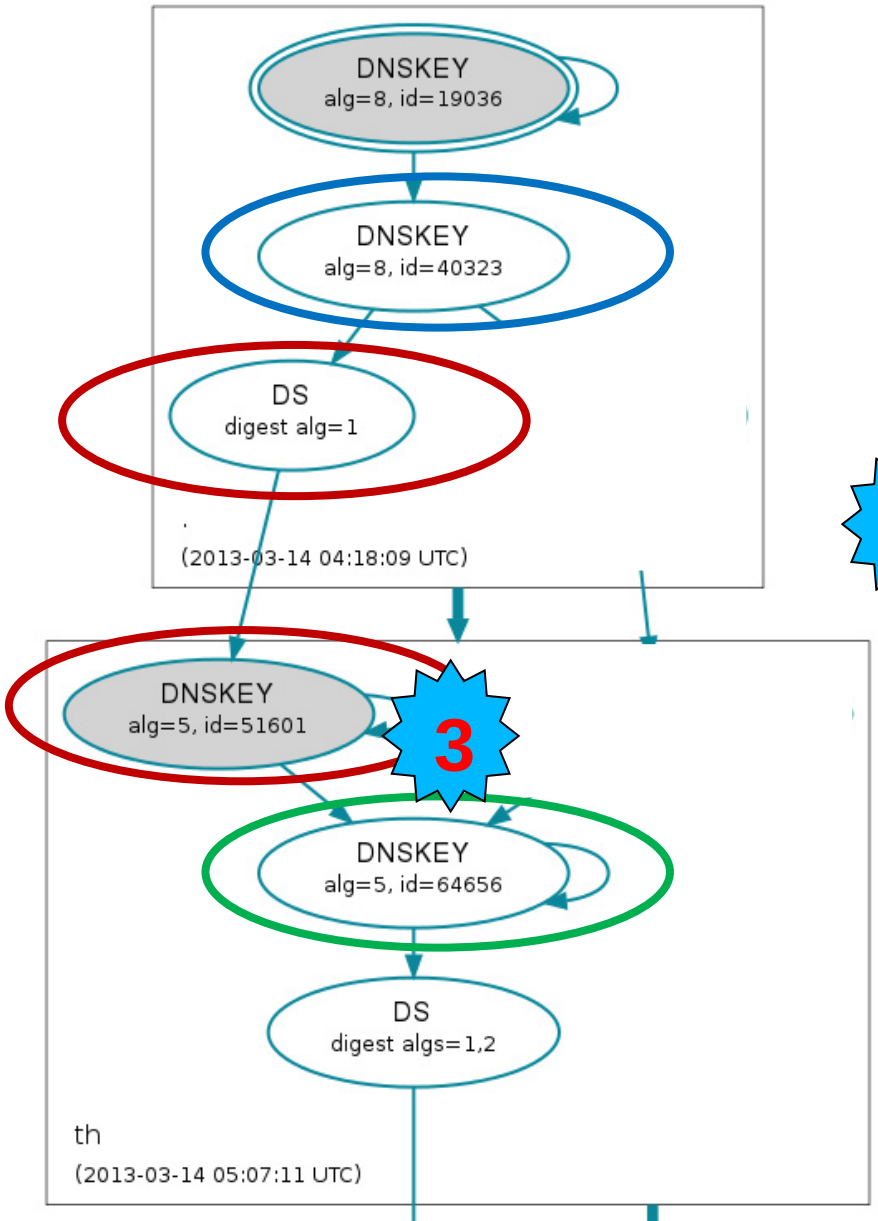
2

www.thnic.or.th A ?
ขอข้อมูล DS ของ TH ในระบบ DNSSEC จาก root

DS 51601 ✓

ลายเซ็นกำกับเซ็นโดย key 40323 ✓

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DS ของ TH ในระบบ DNSSEC จาก root

DS 51601

ลายเซ็นกำกับเซ็นโดย key 40323

3

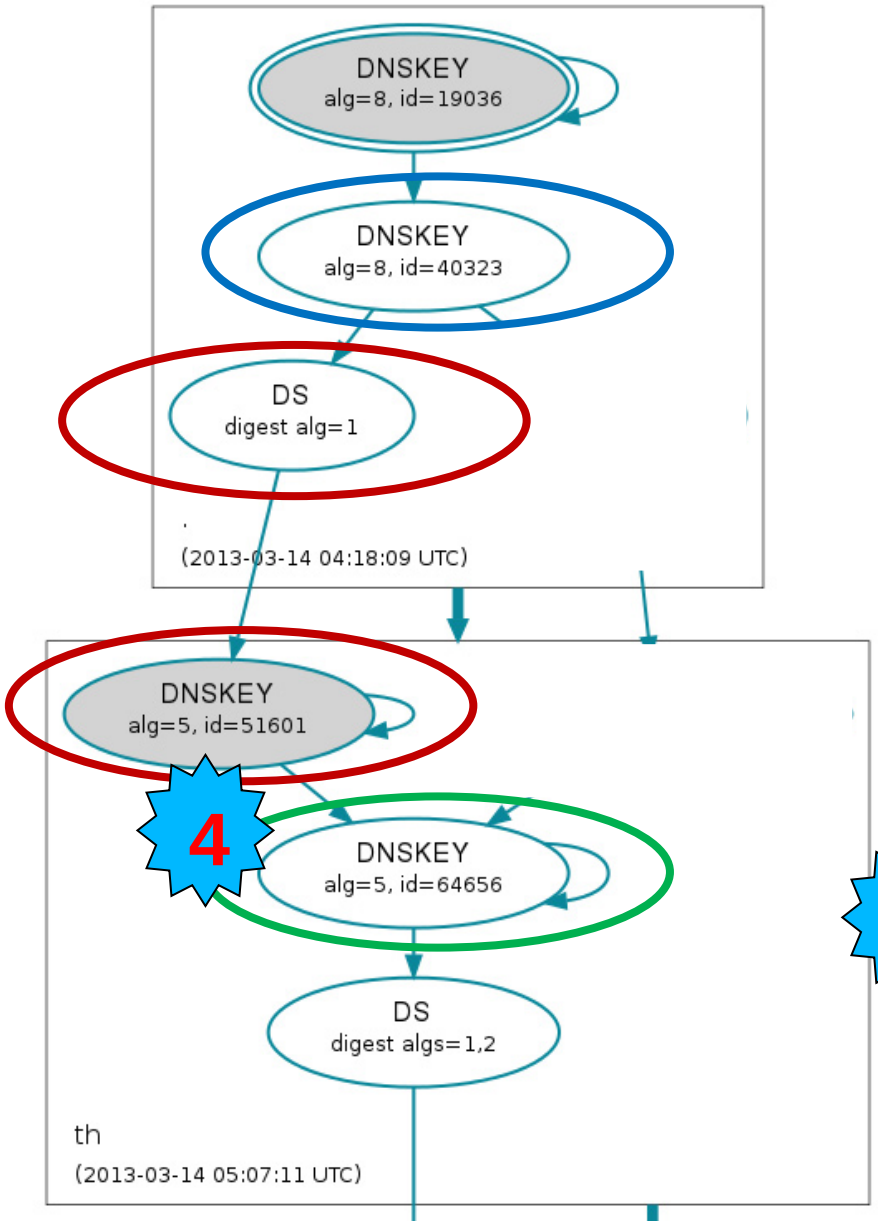
www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ TH zone ในระบบ DNSSEC

DNSKEY 51601 สามารถแปลงค่าเป็น DS 51601
ที่ตรงกับข้อมูลใน root zone ที่ได้ในขั้นตอนที่ 2

DNSKEY 51601 ✓ DNSKEY 64656

ลายเซ็นกำกับเซ็นโดย key 51601

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DS ของ TH ในระบบ DNSSEC จาก root

DS 51601

ลายเซ็นกำกับเซ็นโดย key 40323

www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ TH zone ในระบบ DNSSEC

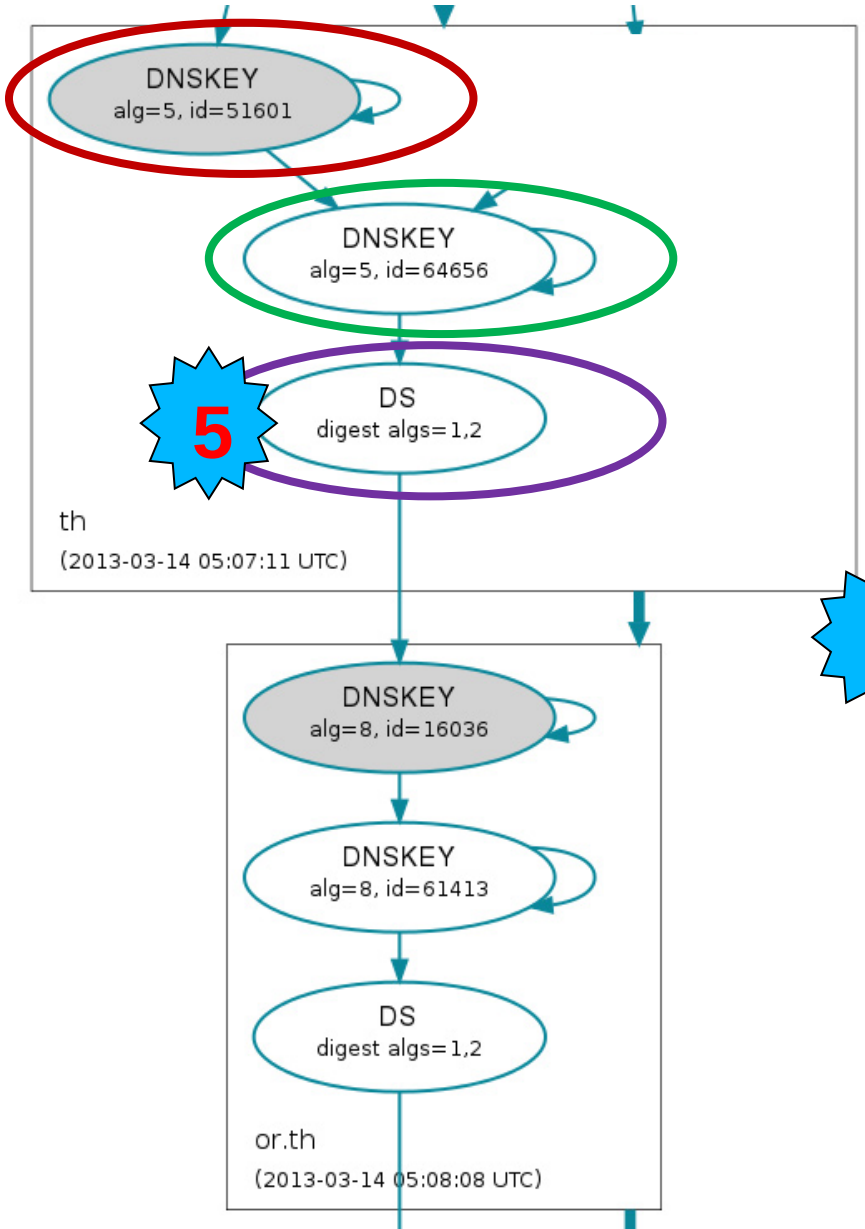
DNSKEY 51601 สามารถแปลงค่าเป็น DS 51601
ที่ตรงกับข้อมูลใน root zone ที่ได้ในขั้นตอนที่ 2

4

DNSKEY 51601 ✓ DNSKEY 64656 ✓

ลายเซ็นกำกับเซ็นโดย key 51601 ✓

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ TH zone ในระบบ DNSSEC

DNSKEY 51601 DNSKEY 64656

ลายเซ็นกำกับเซ็นโดย key 51601

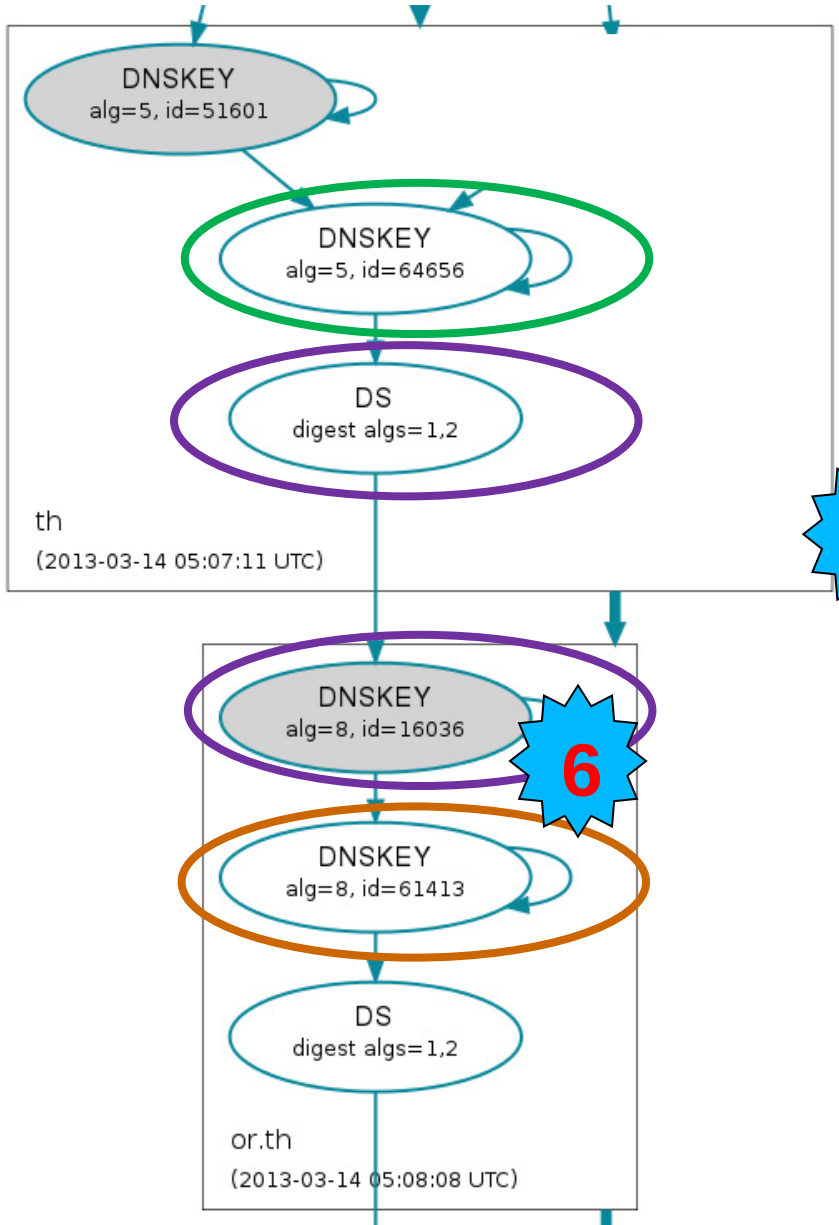
5

www.thnic.or.th A ?
ขอข้อมูล DS ของ OR.TH ในระบบ DNSSEC จาก TH zone

DS 16036

ลายเซ็นกำกับเซ็นโดย key 64656

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DS ของ OR.TH ในระบบ DNSSEC จาก TH zone

DS 16036

ลายเซ็นกำกับเซ็นโดย key 64656

6

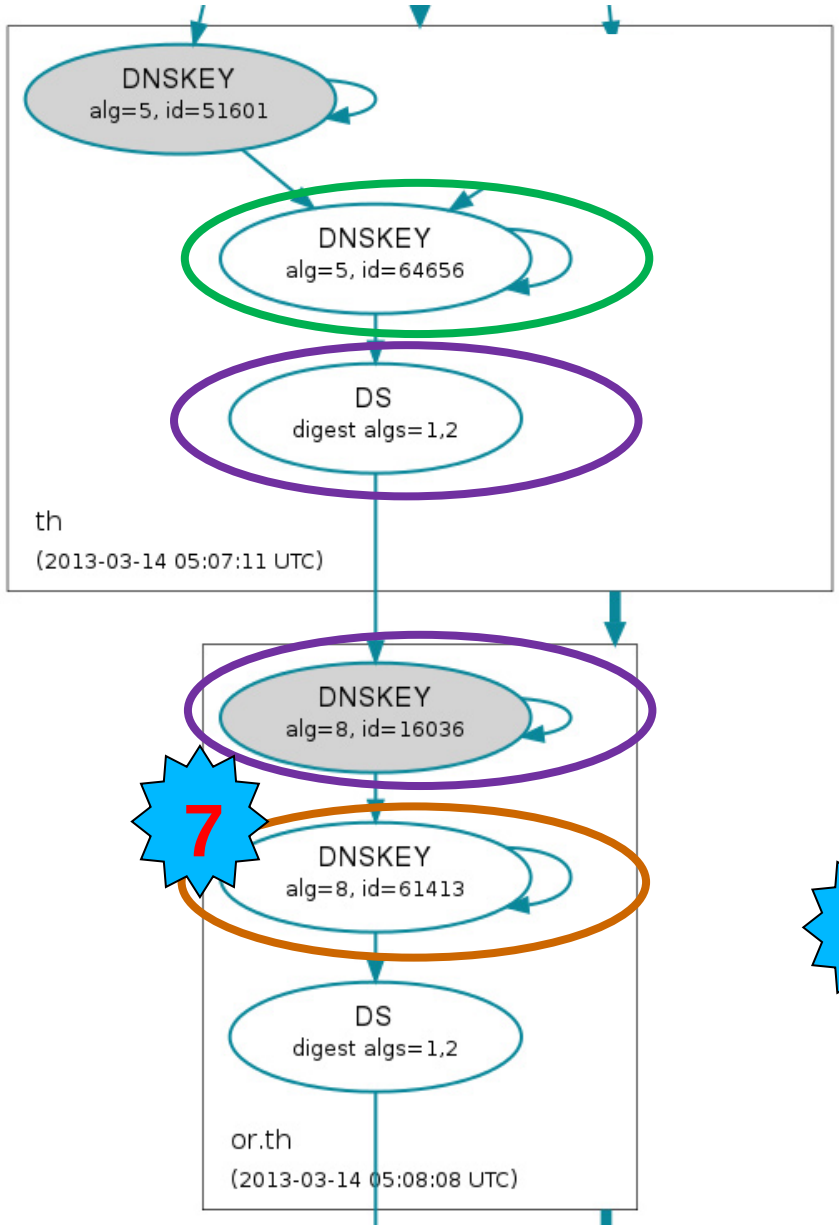
www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ OR.TH zone ในระบบ DNSSEC

DNSKEY 16036 สามารถแปลงค่าเป็น DS 16036
ที่ตรงกับข้อมูลใน TH zone ที่ได้ในขั้นตอนที่ 5

DNSKEY 16036 ✓ DNSKEY 61413

ลายเซ็นกำกับเซ็นโดย key 16036

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DS ของ OR.TH ในระบบ DNSSEC จาก TH zone

DS 16036

ลายเซ็นกำกับเซ็นโดย key 64656

www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ OR.TH zone ในระบบ DNSSEC

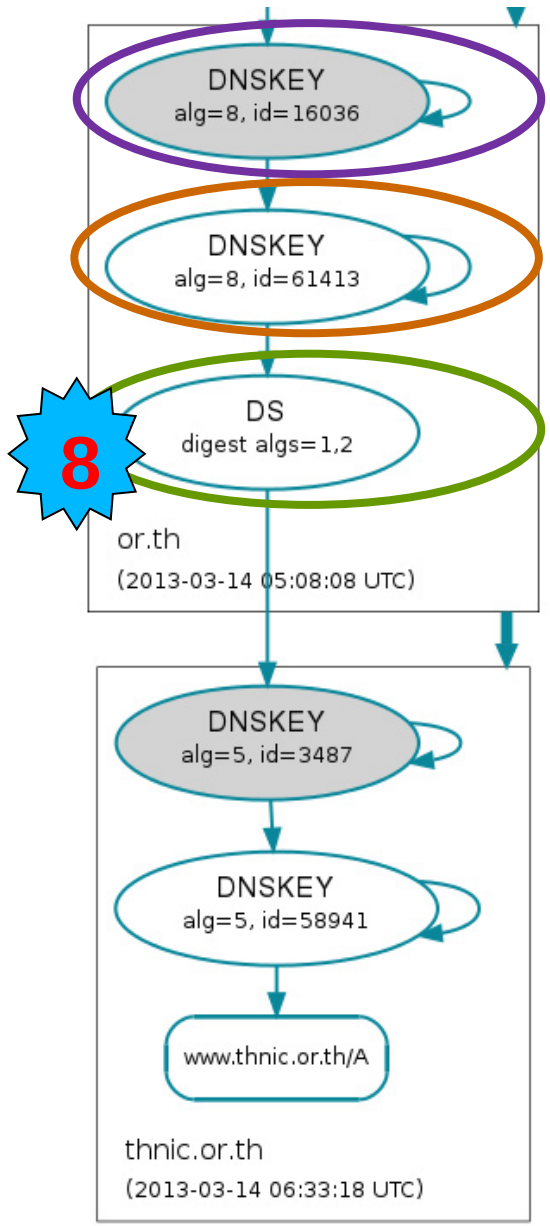
DNSKEY 16036 สามารถแปลงค่าเป็น DS 16036
ที่ตรงกับข้อมูลใน TH zone ที่ได้ในขั้นตอนที่ 5

7

DNSKEY 16036 ✓ DNSKEY 61413 ✓

ลายเซ็นกำกับเซ็นโดย key 16036 ✓

การตรวจสอบ Public keys / Chain of Trust



www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ OR.TH zone ในระบบ DNSSEC

DNSKEY 16036 DNSKEY 61413

ลายเซ็นกำกับเซ็นโดย key 16036

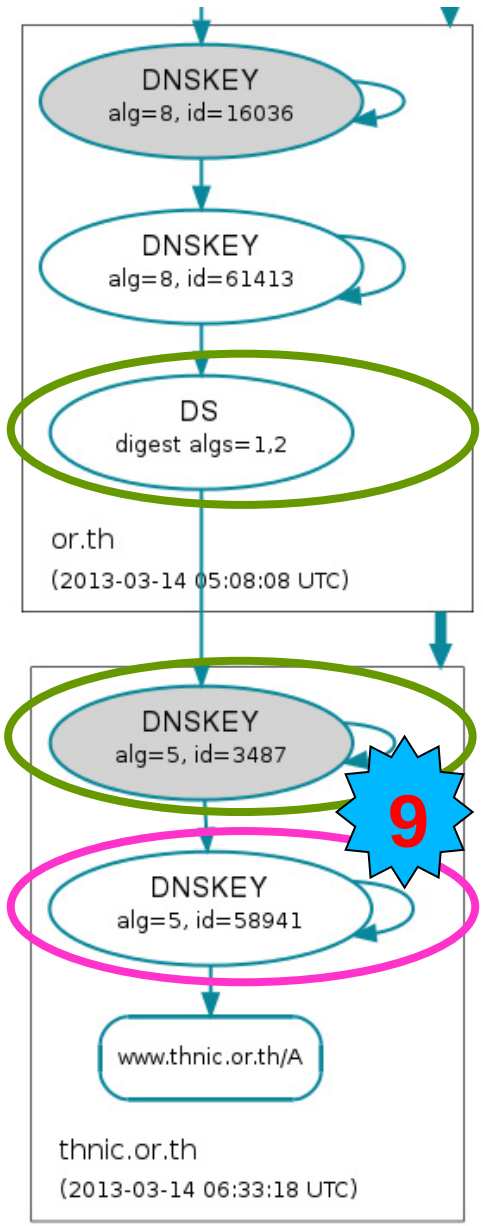
8

www.thnic.or.th A ?
ขอข้อมูล DS ของ THNIC.OR.TH จาก OR.TH zone

DS 3487 ✓

ลายเซ็นกำกับเซ็นโดย key 61413 ✓

การตรวจสอบ Public keys / Chain of Trust



9 www.thnic.or.th A ?

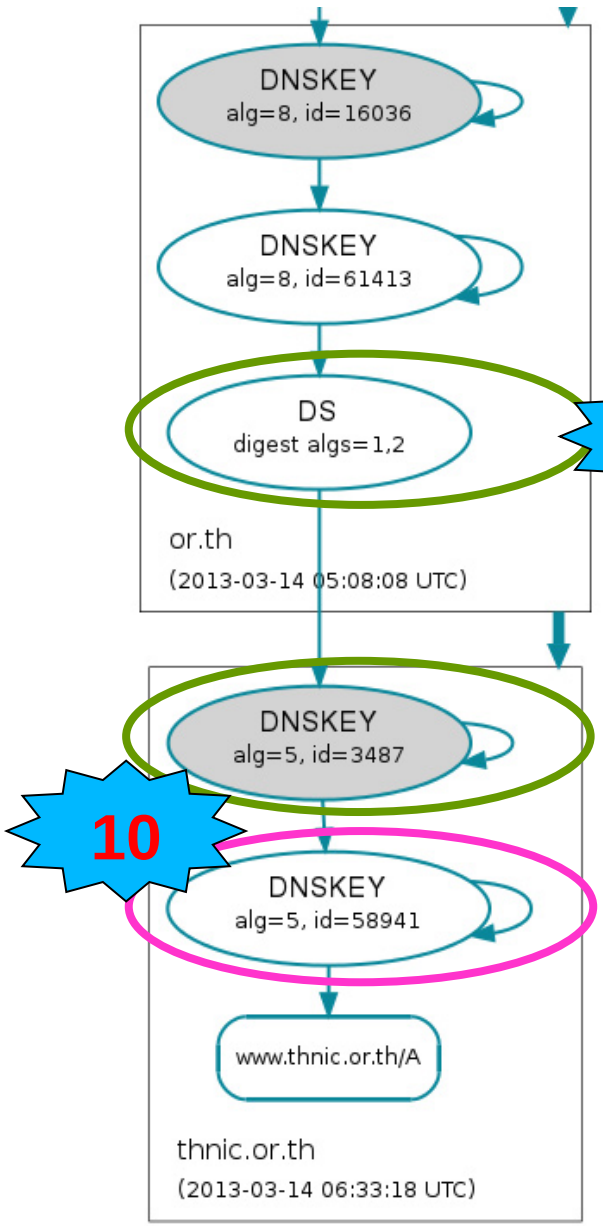
ขอข้อมูล DNSKEY ของ THNIC.OR.TH zone

DNSKEY 3487 สามารถแปลงค่าเป็น DS 3487 ที่ตรงกับข้อมูลใน OR.TH zone ที่ได้ในขั้นตอนที่ 8

DNSKEY 3487 ✓ DNSKEY 58941

ลายเซ็นกำกับเซ็นโดย key 3487

การตรวจสอบ Public keys / Chain of Trust



10

10

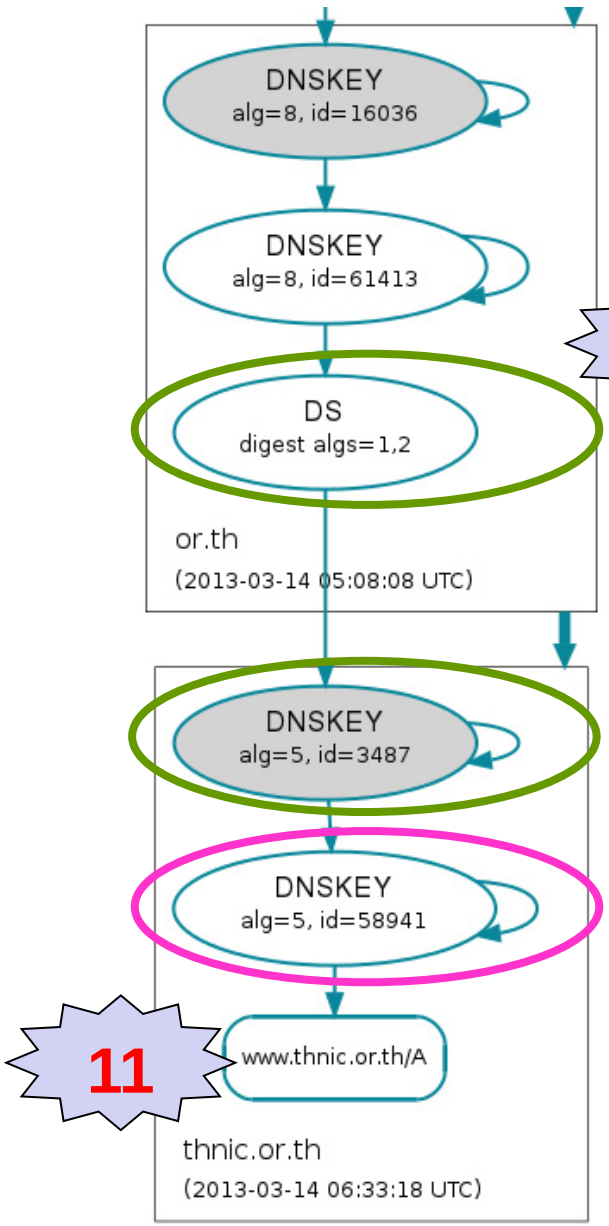
www.thnic.or.th A ?
ขอข้อมูล DNSKEY ของ THNIC.OR.TH zone

DNSKEY 3487 สามารถแปลงค่าเป็น DS 3487
ที่ตรงกับข้อมูลใน OR.TH zone ที่ได้ในขั้นตอนที่ 8

DNSKEY 3487 ✓ DNSKEY 58941 ✓

ลายเซ็นกำกับเซ็นโดย key 3487 ✓

การตรวจสอบ DNS data ในระบบ DNSSEC



DNSKEY 3487 DNSKEY 58941

ลายเซ็นกำกับเซ็นโดย key 3487

11

www.thnic.or.th A ?

ขอข้อมูล A record ของ www.thnic.or.th

A 203.150.1.139

ลายเซ็นกำกับเซ็นโดย key 58941

SUCCESS