交通大學DNSSEC維運經驗
2013/08/08

國立交通大學　資訊技術服務中心
蘇俊憲

2013/07/16

Outline

- 了解DNSSEC
  - Resolver(解析) Server
  - Authoritative(授權) Server
- 維運經驗
- 結論

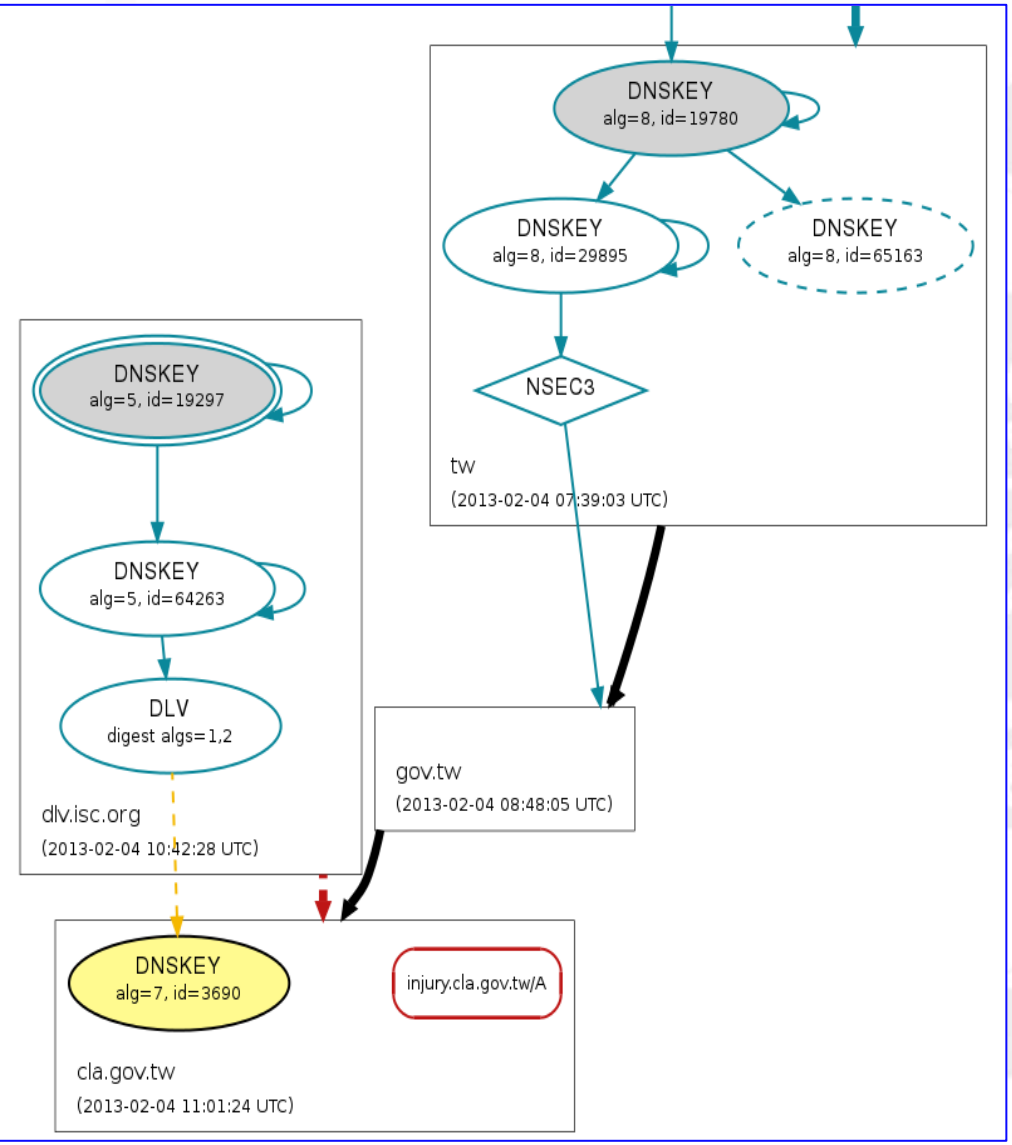
了解DNSSEC

- DNSSEC Resolver(解析) Server
  - 提供使用者DNS查詢的伺服器
  - 8.8.8.8(2013/3/19)、168.95.1.1(未支援DNSSEC)
  - 新版的bind預設已啟用DNSSEC
- Authoritative(授權) Server
  - 儲存負責網域的zone file，提供給外界查詢

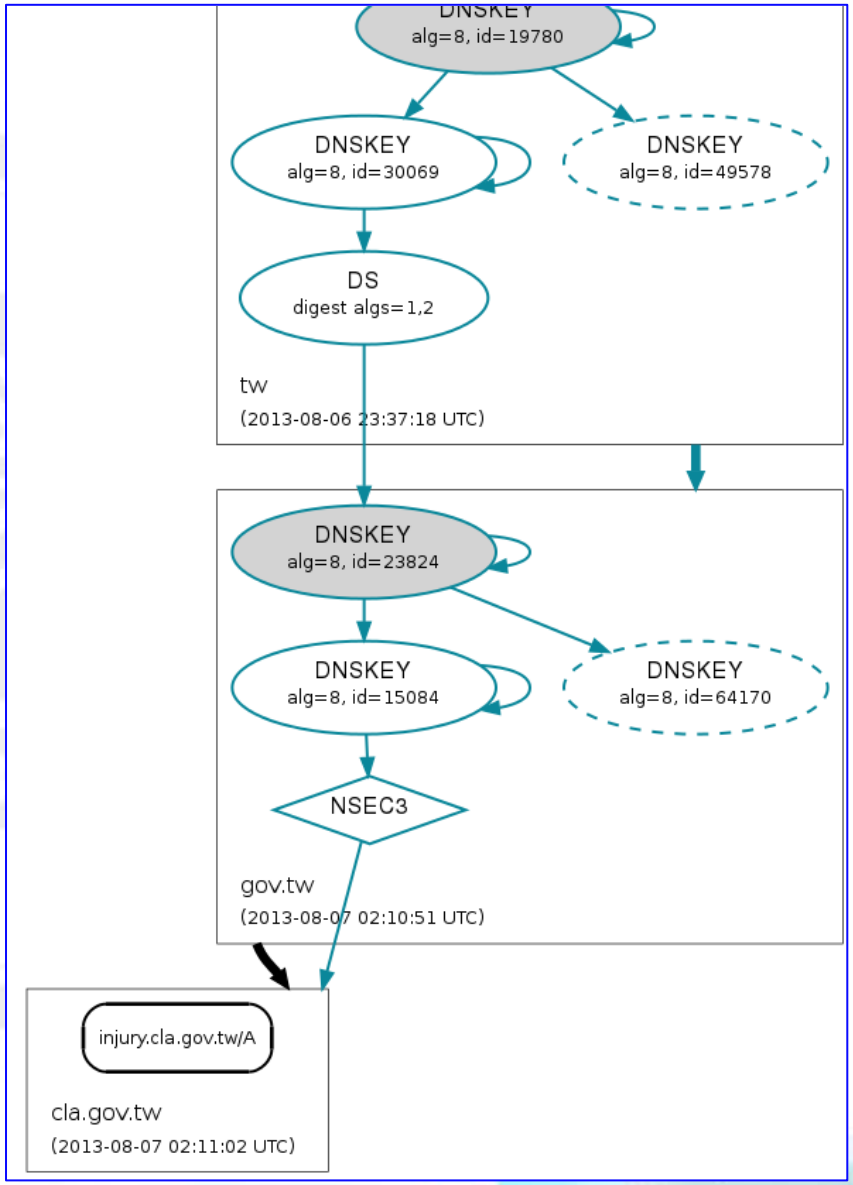
```
root@ns2[/usr/home/chsu]#dig nctu.edu.tw ns

; <<>> DiG 9.8.1-P1 <<>> nctu.edu.tw ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43132
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;nctu.edu.tw.                   IN      NS

;; ANSWER SECTION:
nctu.edu.tw.            300     IN      NS      ns2.nctu.edu.tw.
nctu.edu.tw.            300     IN      NS      ns1.nchc.org.tw.
nctu.edu.tw.            300     IN      NS      ns.nctu.edu.tw.
```

維運經驗

- 2013/2/4 無法查詢injury.cla.gov.tw(勞委會)
  - 影響：
    - 140.113.1.1(DNSSEC)查詢不到IP
    - 168.95.1.1(沒有DNSSEC)查的到
    - 使用者抱怨用學校提供的DNS查不到，用中華電信的DNS就可以
  - 原因：
    - 勞委會授權伺服器設定錯誤，與DLV銜接有問題
  - 解決方式：
    - 通知GSN DNS負責人後修復



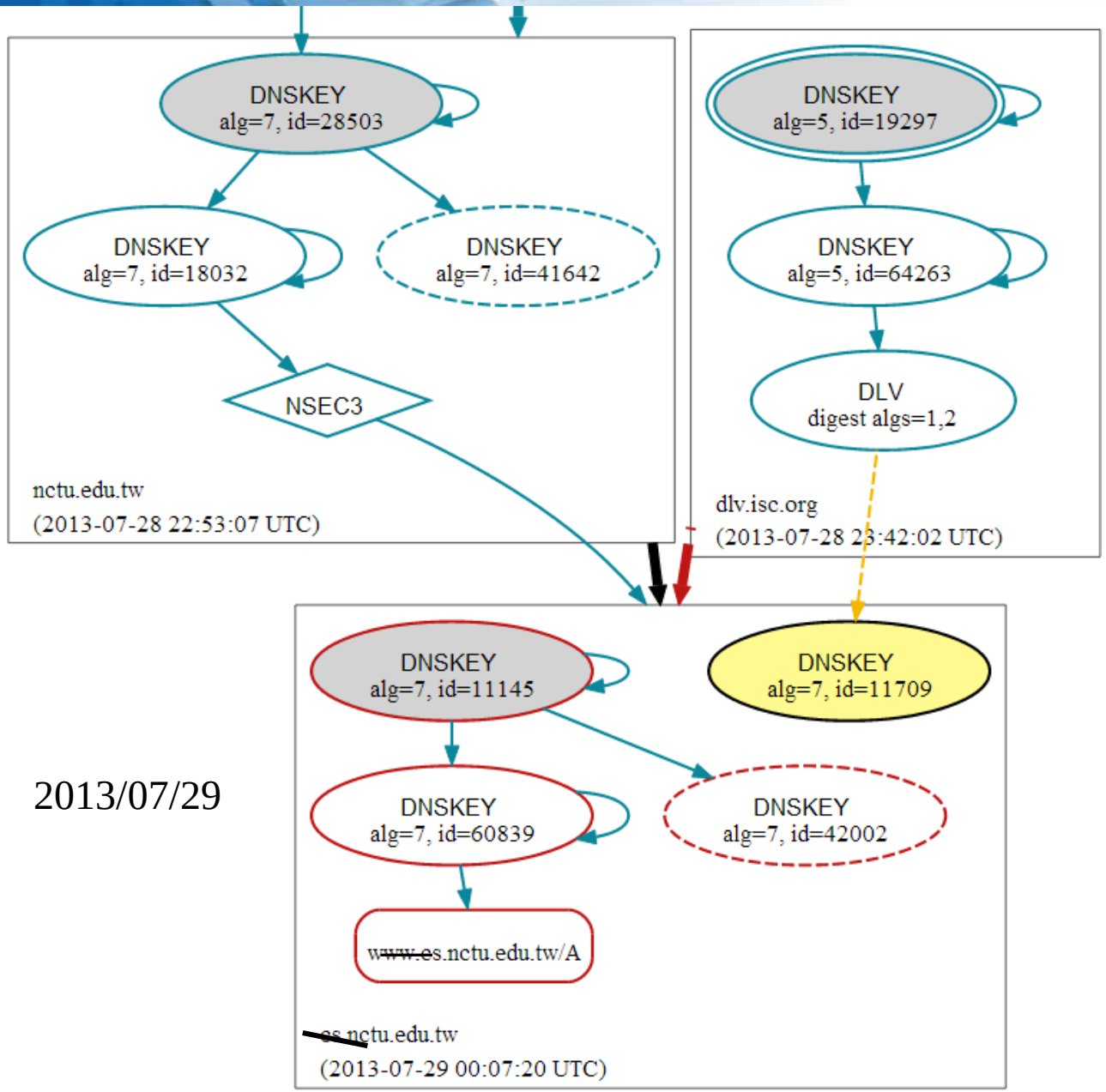
2013/02/24



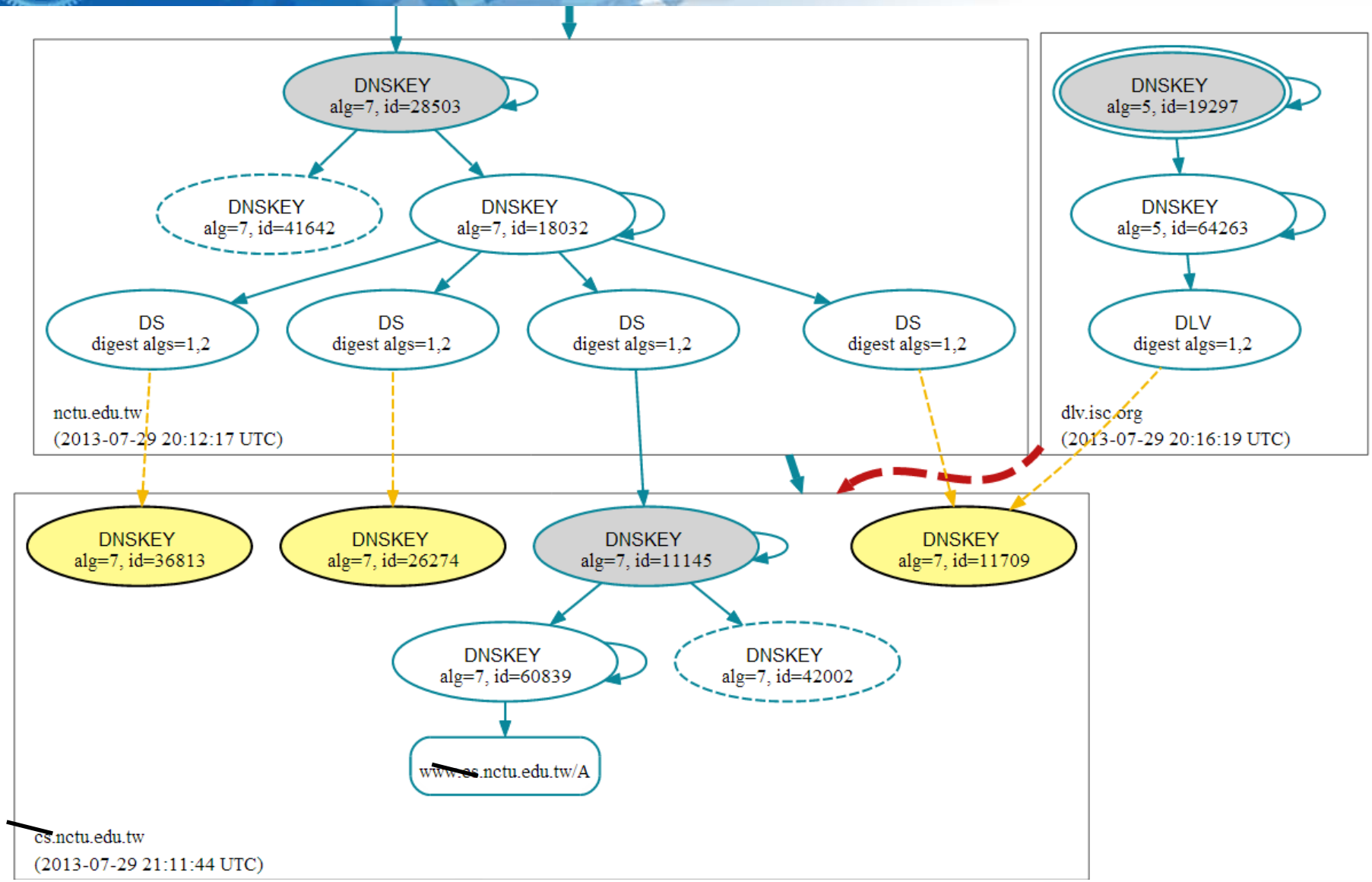
2013/08/07

維運經驗

- 2013/07/29校內單位DNSSEC授權伺服器出錯
  - 影響：
    - 外界DNS(啟用DNSSEC)無法正常查詢到校內單位Domain -> IP Address
  - 原因：
    - 舊的KSK於2013/7/28到期，未向DLV更新KSK
  - 解決方式：
    - 改用DS驗證，提供DS資訊給資訊中心


DNSKEY
alg=7, id=28503
DNSKEY
alg=7, id=18032
DNSKEY
alg=7, id=41642
NSEC3
nctu.edu.tw
(2013-07-28 22:53:07 UTC)
DNSKEY
alg=5, id=19297
DNSKEY
alg=5, id=64263
DLV
digest algs=1,2
dlv.isc.org
(2013-07-28 23:42:02 UTC)
DNSKEY
alg=7, id=11145
DNSKEY
alg=7, id=11709
DNSKEY
alg=7, id=60839
DNSKEY
alg=7, id=42002
www.es.nctu.edu.tw/A
es.nctu.edu.tw
(2013-07-29 00:07:20 UTC)

2013/07/29


DNSKEY
alg=7, id=28503
DNSKEY
alg=7, id=41642
DNSKEY
alg=7, id=18032
DS
digest algs=1,2
DS
digest algs=1,2
DS
digest algs=1,2
DS
digest algs=1,2
nctu.edu.tw
(2013-07-29 20:12:17 UTC)
DNSKEY
alg=5, id=19297
DNSKEY
alg=5, id=64263
DLV
digest algs=1,2
dlv.isc.org
(2013-07-29 20:16:19 UTC)
DNSKEY
alg=7, id=36813
DNSKEY
alg=7, id=26274
DNSKEY
alg=7, id=11145
DNSKEY
alg=7, id=11709
DNSKEY
alg=7, id=60839
DNSKEY
alg=7, id=42002
www.cs.nctu.edu.tw/A
cs.nctu.edu.tw
(2013-07-29 21:11:44 UTC)

2013/07/29

結論

- 若DNSSEC Resolver查詢不到某些Domain Name，需注意是否為DNSSEC問題(與沒啟用DNSSEC的Resolver交叉比對)
- 建置Authoritative需注意KSK與ZSK的到期時間，避免出問題時外界找不到Domain，本身渾然不知
- 注意：新版Bind預設啟用DNSSEC
- 是否要建置DNSSEC?
  - 了解->測試->建置
- 檢測DNSSEC網站
  - http://dnsviz.net/

報告完畢

Thanks!