DNSSEC
at a glance

Fan-Chieh Lin
8th,10 ,2020

About Me

HiNet

DNS

- 168.95.1.1 (resolver)
- DNS hosting (auth.)
- DNS for national elections, tax filing etc.

TAIPEI 2017 29th SUMMER UNIVERSIADE

CDN

About Today

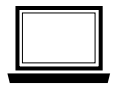
I 背景介紹
- How does DNS work?
- What might go wrong?
- Core concept

II 現況盤點
- DNSSEC Statistics
- Efforts having been put in

III 未來規劃與建議
- Progressive activation
- Improper setup or maintenance
- Amplification attack

IV Q&A
opinions & suggestions

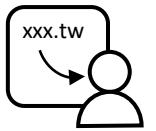
How does DNS work? (& roles involved)



Client

DNS Resolver
(ISP / Public DNS)

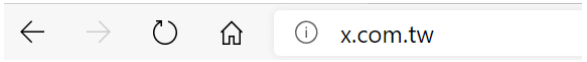
Authoritative Name Server



registrar

2. **X company** arranges **DNS servers** to manage and publish DNS records

1. **X company** **Registers** a domain



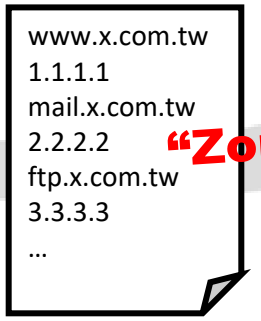
3. **Client** sends DNS queries while surfing the net

4. The **default DNS** resolves queries (by calling out)

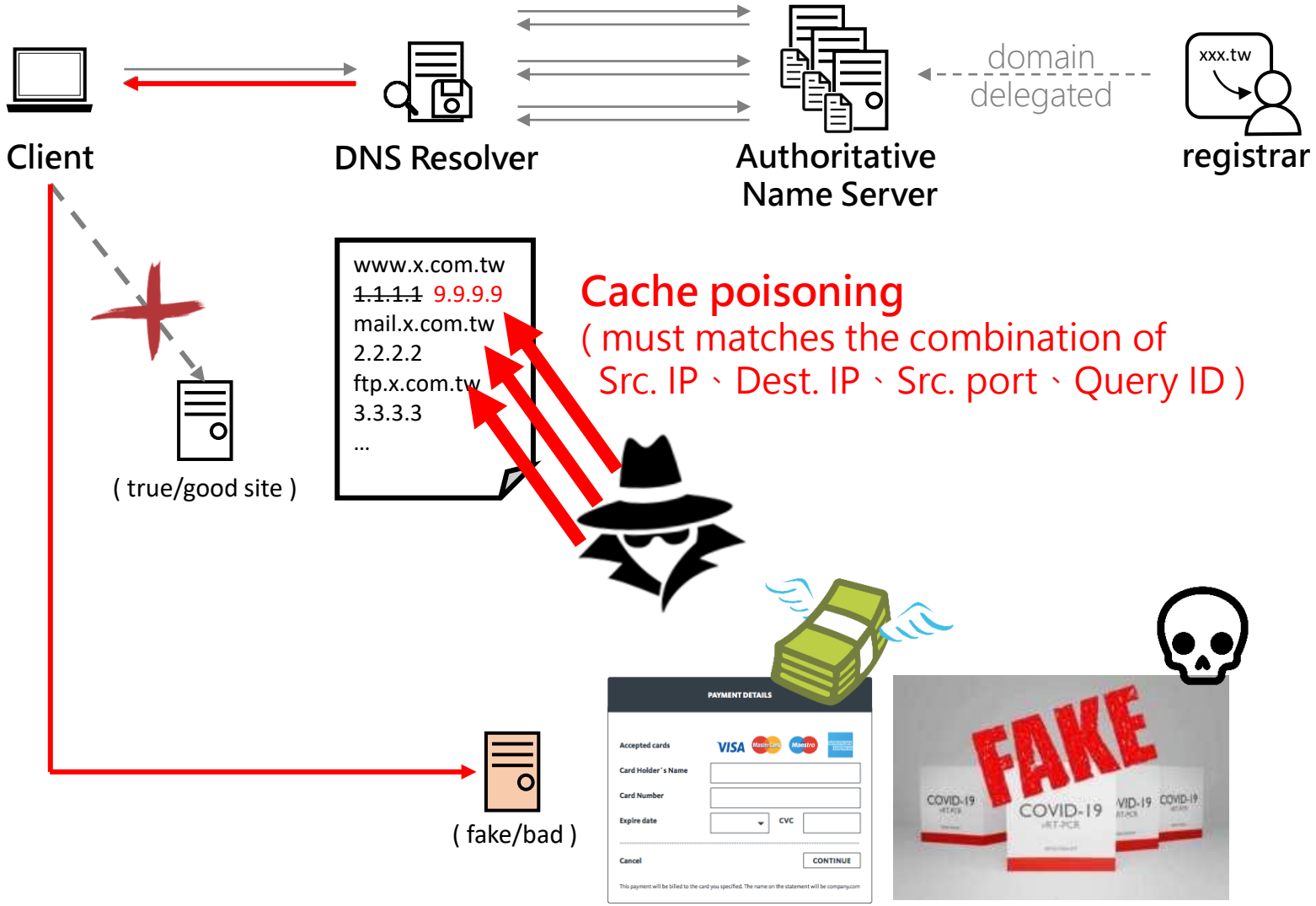
5. The **DNS servers** in charge of the DNS records answers

7. **Client** connects according to the DNS answer/response

6. The **default DN** returns what it finds



What might go wrong? (& impact)

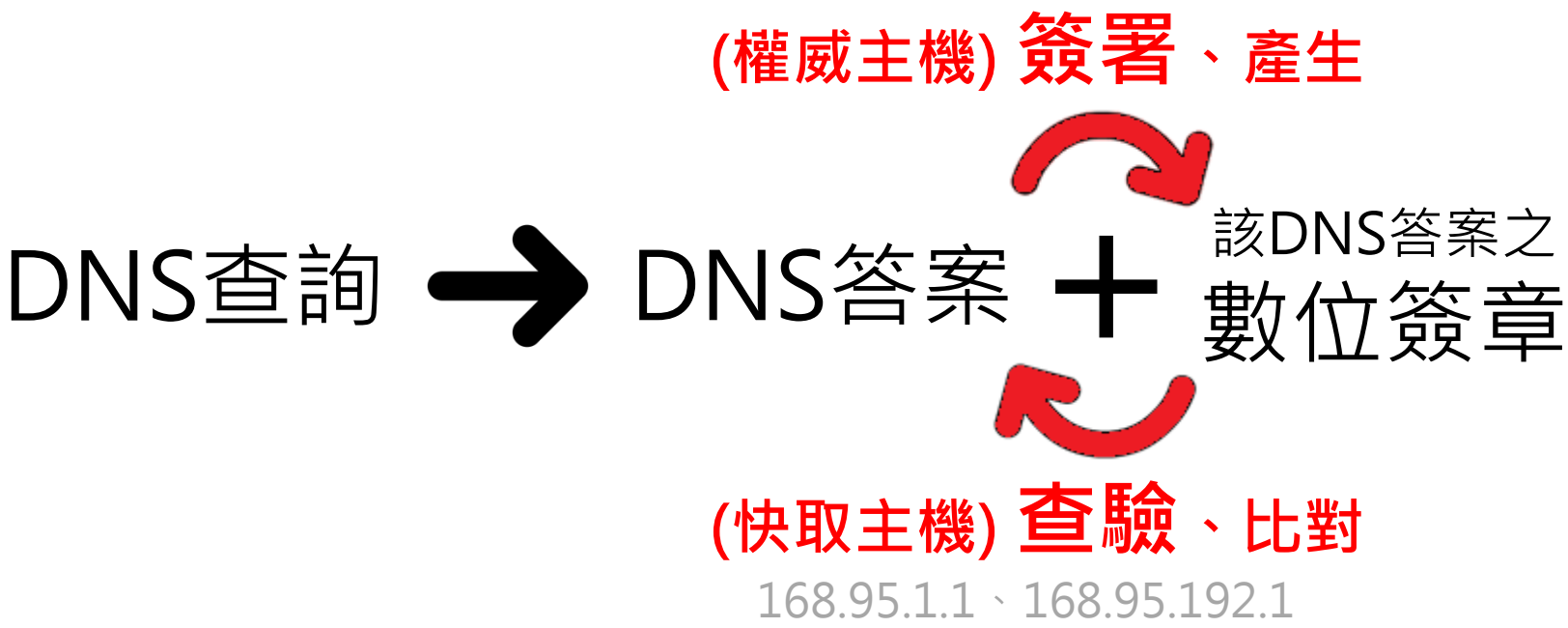


圖源
https://www.paymill.com/en/blog/9-ways-to-make-online-payment-easy-for-your-customers/
https://scvnews.com/fda-warns-of-fake-covid-19-home-test-kits/
https://www.cleanpng.com/png-logo-computer-icons-clip-art-white-hat-hacker-icon-5595839/download-png.html

DNSSEC Core Concept

Q. 如何確定所收到的答案是「對」的？

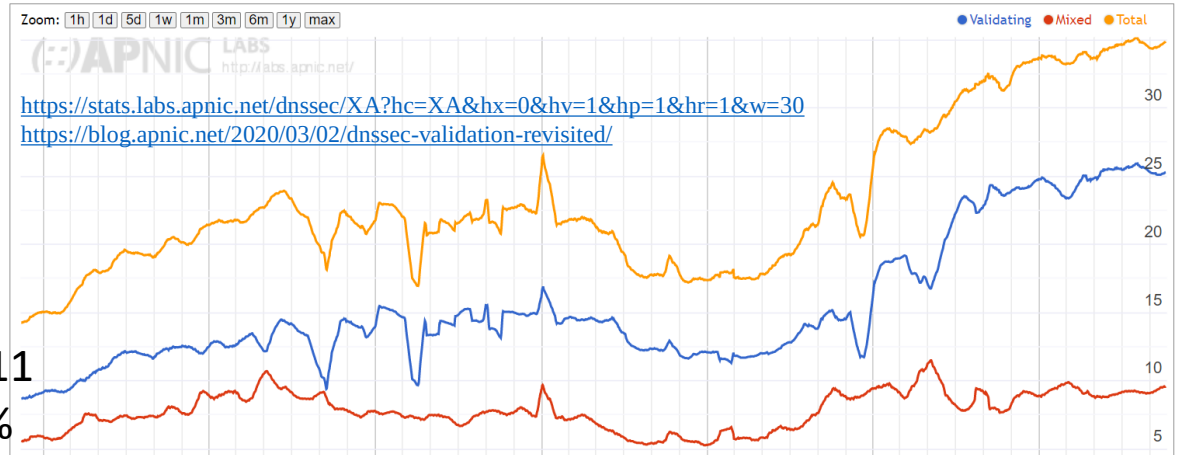
A. 資料管理者提供「答案」+「答案專屬的數位簽章」
資料需求者查驗兩者是否成對



II 現況 DNSSEC Validating Users

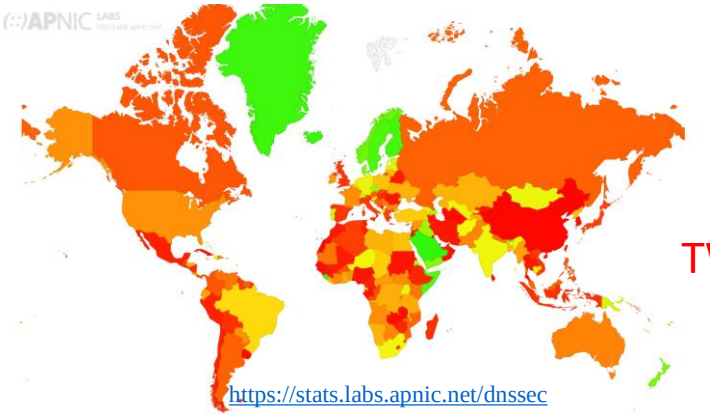
2020/10
34.86%

2013/11
14.25%



https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=1&hr=1&w=30
https://blog.apnic.net/2020/03/02/dnssec-validation-revisited/

Code	Region	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
XA	World	25.05%	9.50%	8,698,057	1	8,698,057
XF	Oceania	34.21%	10.61%	35,333	1.74	61,338
XE	Europe	30.56%	6.01%	1,524,791	0.83	1,264,740
XC	Americas	27.23%	5.70%	2,209,844	0.7	1,540,243
XD	Asia	23.21%	9.87%	4,224,360	1.18	4,969,704
XB	Africa	22.98%	19.16%	703,724	1.22	861,850
XG	Unclassified	0	0	76	2.44	185



https://stats.labs.apnic.net/dnssec

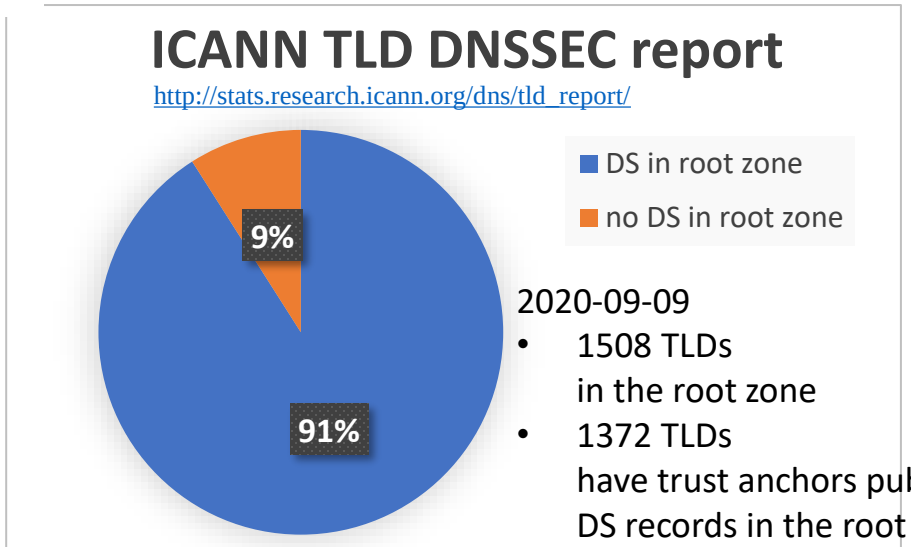
TW, 4.42%

No. 187
(total 236)

CC	Country	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
SA	Saudi Arabia, Western Asia, Asia	97.46%	2.08%	57,884	1.19	68,726
AD	Andorra, Southern Europe, Europe	97.37%	2.26%	266	0.6	159
SL	Sierra Leone, Western Africa, Africa	97.33%	2.19%	2,097	1.5	3,142
IS	Iceland, Northern Europe, Europe	96.98%	1.75%	1,026	0.67	687
GI	Gibraltar, Southern Europe, Europe	95.48%	3.23%	155	0.52	79
GL	Greenland, Northern America, Americas	94.20%	5.80%	207	0.4	83
DJ	Djibouti, Eastern Africa, Africa	94.16%	5.42%	719	3.34	2,399
FI	Finland, Northern Europe, Europe	92.78%	2.62%	5,334	1.87	9,997
FO	Faeroe Islands, Northern Europe, Europe	91.89%	6.49%	185	0.55	101
TC	Turks and Caicos Islands, Caribbean, Americas	90.62%	9.38%	256	0.17	43
SE	Sweden, Northern Europe, Europe	90.31%	2.44%	12,728	1.71	21,808
SO	Somalia, Eastern Africa, Africa	87.20%	11.73%	11,318	0.06	721
FM	Micronesia (Federated States of), Micronesia, Oceania	86.40%	12.00%	125	0.74	92
AI	Anguilla, Caribbean, Americas	86.38%	8.96%	279	0.09	26
FJ	Fiji, Melanesia, Oceania	84.89%	14.16%	1,165	0.91	1,064
EU	European Union, Western Europe, Europe	84.75%	5.93%	118	0	0
BT	Bhutan, Southern Asia, Asia	82.67%	16.89%	1,847	0.5	927
NO	Norway, Northern Europe, Europe	81.45%	7.56%	5,359	1.98	10,618
DM	Dominica, Caribbean, Americas	81.25%	5.83%	240	0.46	110
DK	Denmark, Northern Europe, Europe	79.91%	8.90%	6,547	1.77	11,588
YE	Yemen, Western Asia, Asia	78.66%	15.78%	8,103	2.27	18,389
LU	Luxembourg, Western Europe, Europe	74.75%	4.98%	1,085	1.17	1,266
PF	French Polynesia, Polynesia, Oceania	74.69%	13.28%	482	0.97	469
NZ	New Zealand, Australia and New Zealand, Oceania	73.43%	19.78%	4,626	2.01	9,313
IQ	Iraq, Western Asia, Asia	72.52%	13.19%	92,839	0.83	76,895
BS	Bahamas, Caribbean, Americas	71.70%	2.20%	1,498	0.5	754
CZ	Czech Republic, Eastern Europe, Europe	71.56%	7.68%	17,366	1.04	18,079
PS	State of Palestine, Western Asia, Asia	67.45%	12.75%	17,230	0.45	7,705
AZ	Azerbaijan, Western Asia, Asia	67.21%	5.38%	27,920	0.6	16,817
SC	Seychelles, Eastern Africa, Africa	66.67%	24.95%	549	0.23	128
KM	Comoros, Eastern Africa, Africa	65.96%	32.45%	188	0.92	172
CH	Switzerland, Western Europe, Europe	64.02%	2.72%	6,957	2.59	17,991
BB	Barbados, Caribbean, Americas	61.84%	29.30%	1,976	0.26	515
PT	Portugal, Southern Europe, Europe	60.29%	3.18%	29,785	0.56	16,709
AM	Armenia, Western Asia, Asia	60.00%	14.64%	5,678	0.87	4,934
EE	Estonia, Northern Europe, Europe	59.77%	11.50%	2,053	1.18	2,427
LV	Latvia, Northern Europe, Europe	55.77%	14.68%	5,736	0.56	3,239
HT	Haiti, Caribbean, Americas	55.32%	4.49%	4,546	0.64	2,904
...						
MA	Morocco, Northern Africa, Africa	5.21%	1.81%	83,749	0.61	51,199
ME	Montenegro, Southern Europe, Europe	4.84%	35.26%	7,190	0.13	959
KG	Kyrgyzstan, Central Asia, Asia	4.72%	7.47%	6,628	0.94	6,239
VC	Saint Vincent and the Grenadines, Caribbean, Americas	4.58%	2.29%	393	0.48	188
TW	Taiwan, Eastern Asia, Asia	4.42%	4.87%	124,609	0.44	55,144
SN	Senegal, Western Africa, Africa	4.32%	6.38%	20,056	0.65	13,090
TH	Thailand, South-Eastern Asia, Asia	4.27%	26.19%	99,325	0.96	95,348
RO	Romania, Eastern Europe, Europe	4.27%	1.81%	35,162	0.81	28,552
TT	Trinidad and Tobago, Caribbean, Americas	4.17%	2.92%	6,449	0.38	2,466

II DNSSEC Signed Domains

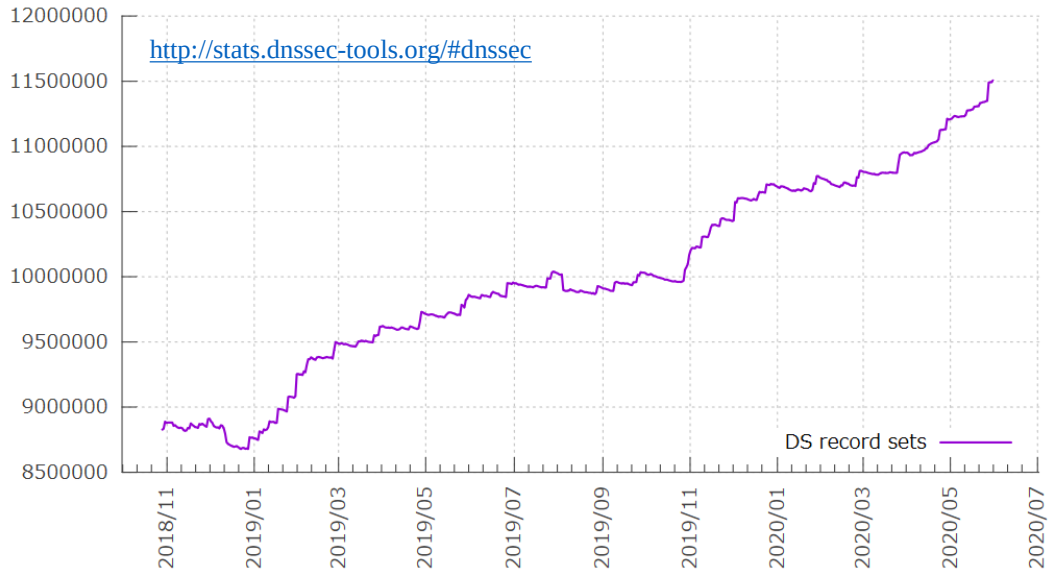
現況



2020-09-09
- 1508 TLDs
  in the root zone
- 1372 TLDs
  have trust anchors published as
  DS records in the root zone

DS Record count growth

The following graph shows the growth of observed DS record sets over time (i.e. the number of signed zones):

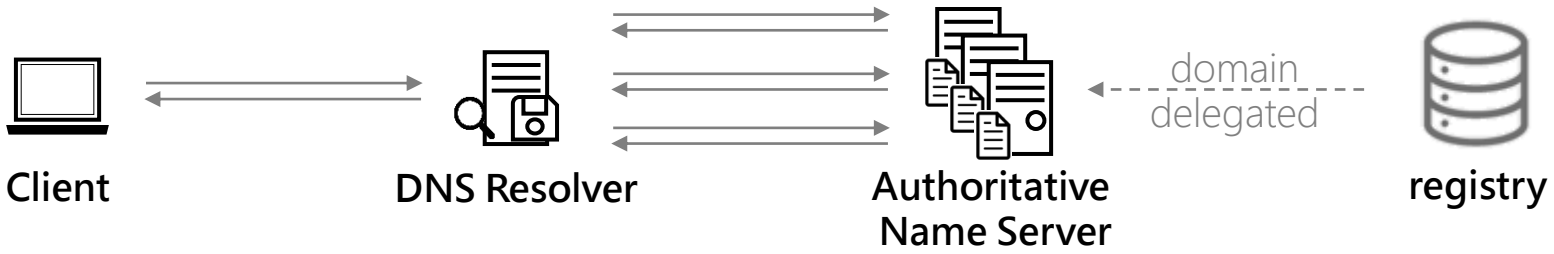


域名類別	DNSSEC 啟用(域名)數量	百分比
edu.tw	30	2.09%
gov.tw	76	1.99%
game.tw	3	1.8%
ebiz.tw	1	1.64%
club.tw	1	0.53%
net.tw	5	0.41%
org.tw	19	0.16%
idv.tw	102	0.10%
com.tw	240	0.11%
tw	506	0.05%
Total	983	0.08%

2020-08-18 TWNIC「DNSSEC部署」推廣的引言報告

II 現況

Effort has been made (From GSN's point of view)



- ✓ 積極**科普** (while)
  - 申告查測
  - 技術諮詢
- ✓ 提供與維護指引**文件**
  - *政府網域名稱 DNSSEC DS 設定步驟說明*
  - *Bind DNSSEC 簽署教學(自動簽署)*
  - *Bind DNSSEC 簽署教學(手動簽署)*

- ✓ 持續**優化體質**，以因應訊務質&量的改變
  - 硬體升級、擴容
  - 監控防護 (月報 etc.)
  - 軟體功能、彈性

(DNSSEC validation)
- ✓ 技術面：功能就緒
- ✓ 策略面：配合政策與國際趨勢

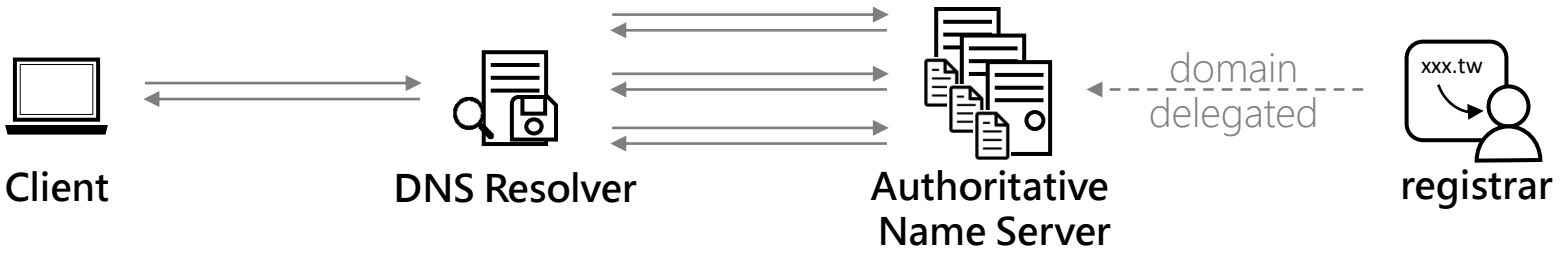
(DNSSEC signing)
- ✓ 技術面：功能就緒
- ✓ 策略面：依客戶需求提供服務

- ✓ 支援gov.tw層級的DNSSEC **signing**
- ✓ 受理**DS紀錄**的提交
- ✓ 更新域名註冊受理與管理機制
  - 整合eGov單一登入(SSO)掌握域名/機關聯絡窗口、代理人
  - 更新域名相關之申請與受理機制
  - (系統、制度優化有利於DNSSEC等進階服務的推廣)

https://gsn.nat.gov.tw/upload/domain/1451cb5f26d000003e70.pdf
https://gsn.nat.gov.tw/upload/domain/1451cb6a7b1000004b9e.pdf
https://gsn.nat.gov.tw/upload/domain/1451cb5b299000005ddd.pdf

II 現況

Effort has been made (From CHT's point of view)



✓ 積極**科普** (while)
- 申告查測
- 客戶拜訪
- 舉辦說明會

✓ 健全**客服**體系
- 企客專案經理
- 消客客務專線
- ticketing system 申告處理與跟催機制

✓ 持續**優化體質**，以因應訊務質&量的改變
- 硬體升級、擴容
- 縱深防禦 (與骨幹網路深度合作)
- 軟體功能、彈性

(DNSSEC validation)
✓ 技術面：功能就緒
✓ 策略面：**漸進**推廣 "progressive activation"

(DNSSEC signing)
✓ 技術面：功能就緒
✓ 策略面：依客戶需求提供 (DNS hosting) 服務方案

✓ 受理**DS紀錄**的提交

II 現況

How CHT Progressively Activate (DNSSEC Validation)

effect (mind the flags)

edu.tw

```
C:\Users>dig @168.95.1.1 edu.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 edu.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14638
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

AD bit

```
C:\Users>dig @8.8.8.8 edu.tw soa

; <<>> DiG 9.12.3-P1 <<>> @8.8.8.8 edu.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10554
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

AD bit

com.tw

```
C:\Users>dig @168.95.1.1 com.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 com.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60681
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

~~AD bit~~

```
C:\Users>dig @8.8.8.8 com.tw soa

; <<>> DiG 9.12.3-P1 <<>> @8.8.8.8 com.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48888
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

AD bit

II 現況

How CHT Progressively Activate (DNSSEC Validation)

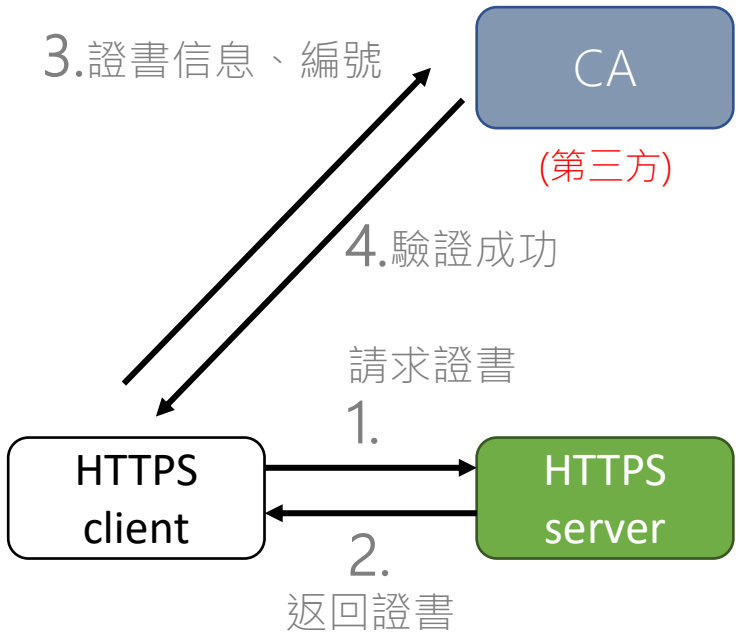
rationale (an analogy)

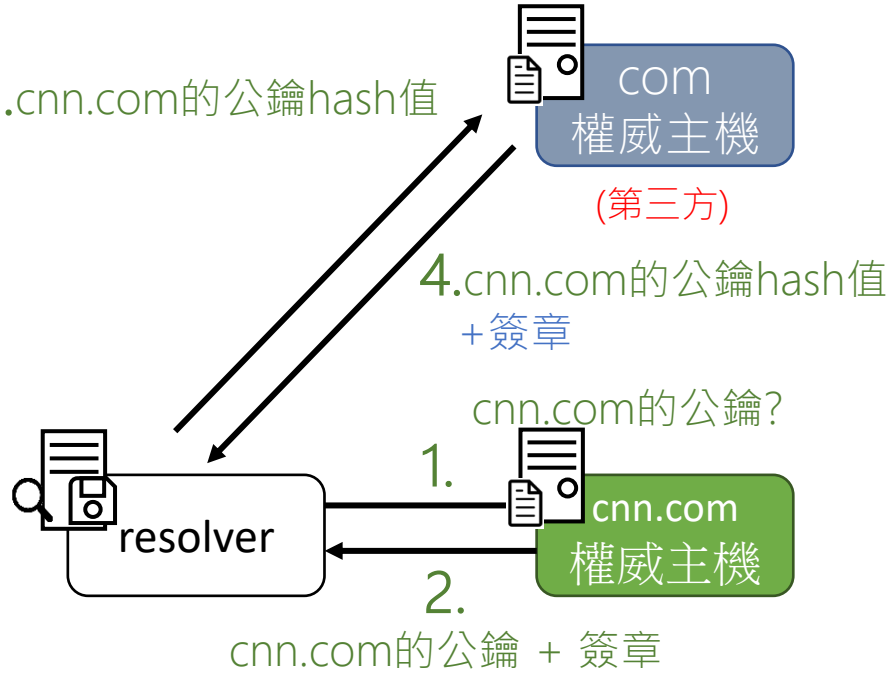
- client 需要 (server’s) public key，以安全同步對稱加密傳輸所需的 shared key
- resolver 需要 (權威主機’s) public key 以驗證 DNS data 的數位簽章

為了確保 public key 是對的，由「第三方」協助佐證：
取 public key 的 hash 值 + 以第三方**私鑰**加密該 hash 值

（確保內容完整） （確保來源正確）

PS:
在DNS架構中「上層」權威主機即是現成的第三方，不需要 CA 機構

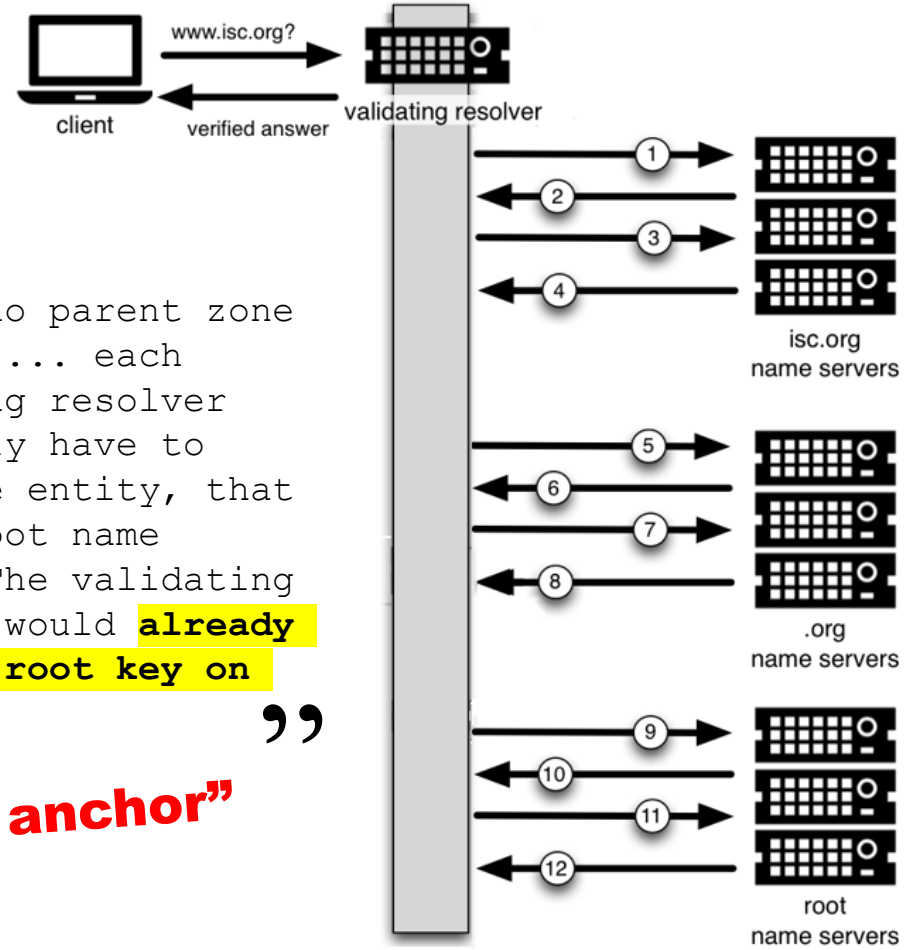




II How CHT Progressively Activate (DNSSEC Validation)

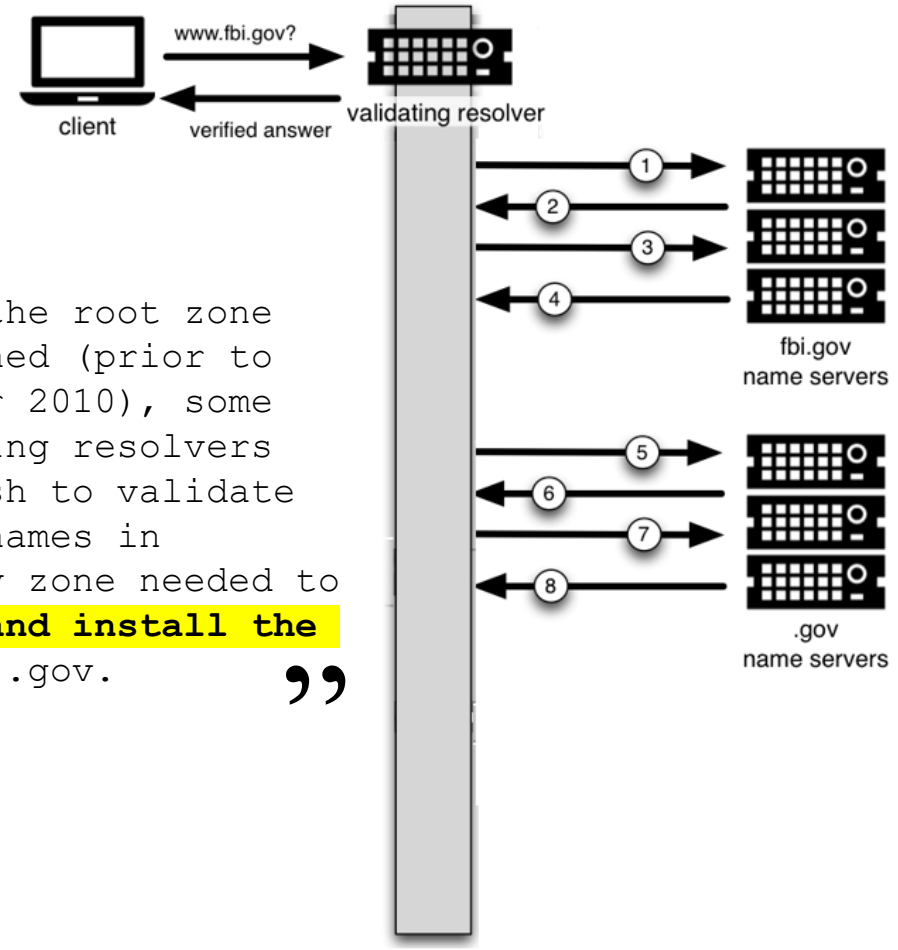
現況

rationale (cont.)



"There's no parent zone for root ... each validating resolver would only have to trust one entity, that is the root name server. The validating resolver would **already have the root key on file**."

"trust anchor"



"before the root zone was signed (prior to the year 2010), some validating resolvers that wish to validate domain names in the .gov zone needed to **obtain and install the key** for .gov."

ISC BIND DNSSEC Guide

https://ftp.eenet.ee/pub/isc/dnssec-guide/html/dnssec-guide.html#trust-anchors

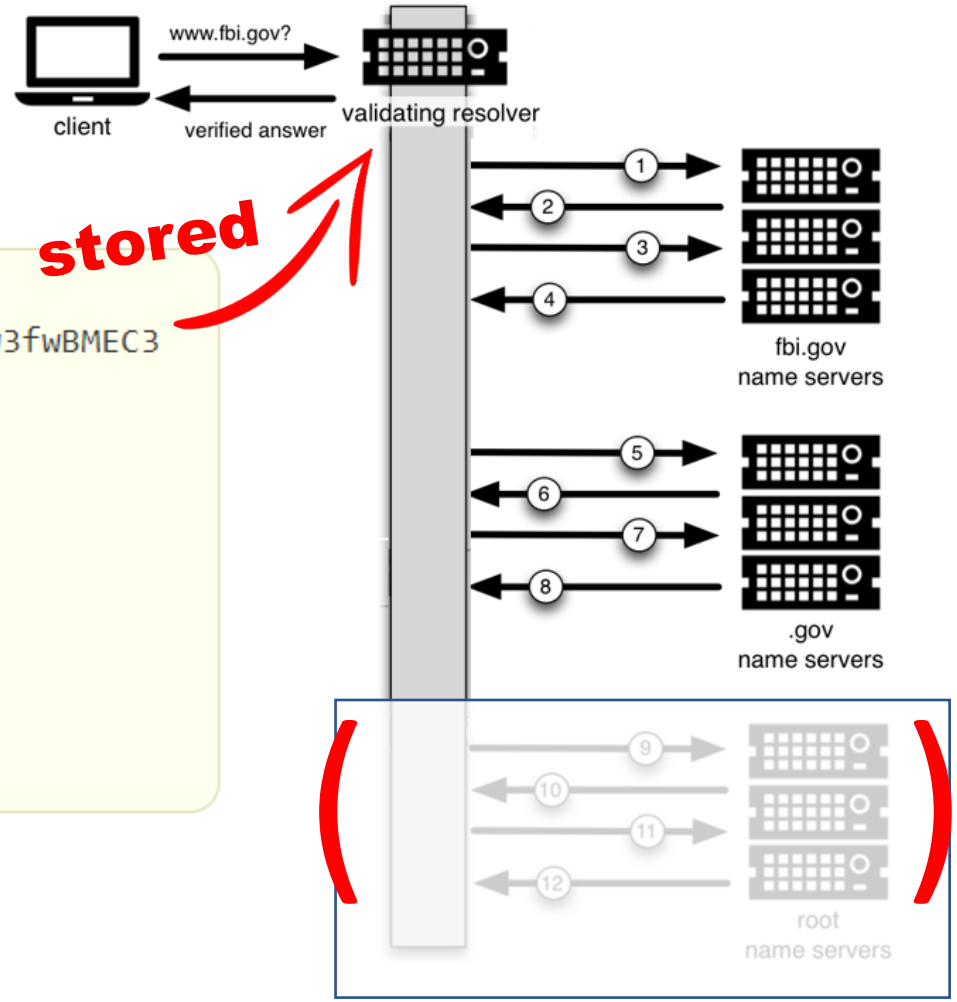
III 未來 Plans & Suggestions (about the “progressive activation”)

(trusted) key management

change!

```
trusted-keys {
    gov. 257 3 8 "AQO8daaz7B+yshOfL60rytKd9aOSujgponEw3fwBMEC3
    /+e9XzHw2k+VKnbJTZ+QaVtpfUd1q9HKZIv/ck83Gl5T
    jYKE5jtUZ2kpEDZfVNGv6yx0smtWAXv1nCJS9ohnyOTd
    397eMojGDHqkEC+uojEScZheEkMxzgCZwDAs+/CSU7mS
    uHtCRZn19xlZUd5Gv7yDQ3mbOUwuy30oSk0z1Q5UUPpo
    ihOugIZHFX6Jk7NLiW2wlqfq9qhV4zj7TiBiJY0mCc4z
    HN8/aq2VKDHp2Na7mWzvKyTy+SYQkBQ/08LbPwj9YMc+
    uCzKL6sU/ObHv17EFhD8aPDftTHZvV9L+OZr";
};
```

stored

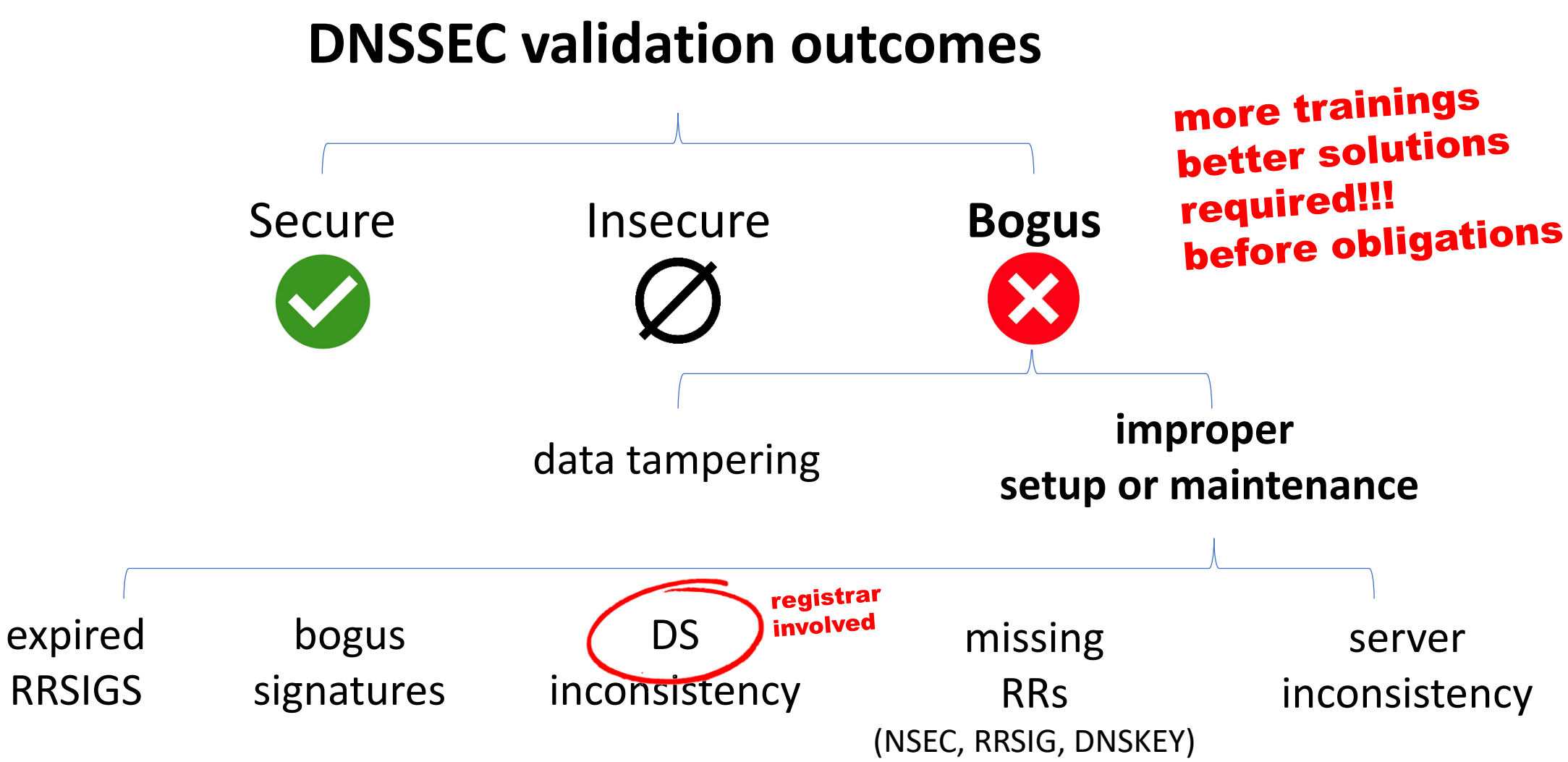


take

- monitoring
- notifying? (by TWNIC?)

III Plans & Suggestions (about setup and maintenance)

未來



https://www.osti.gov/servlets/purl/1110294

III 未來 Plans & Suggestions (about security threat)

“amplification attack”

```
;; QUESTION SECTION:
;ghmn.ru.                       IN      ANY

;; ANSWER SECTION:
ghmn.ru.                17794   IN      A       5.135.4.1
ghmn.ru.                17794   IN      A       5.135.4.10
ghmn.ru.                17794   IN      A       5.135.4.11
ghmn.ru.                17794   IN      A       5.135.4.12
ghmn.ru.                17794   IN      A       5.135.4.13
ghmn.ru.                17794   IN      A       5.135.4.14
ghmn.ru.                17794   IN      A       5.135.4.15
ghmn.ru.                17794   IN      A       5.135.4.16
ghmn.ru.                17794   IN      A       5.135.4.17
ghmn.ru.                17794   IN      A       5.135.4.18
ghmn.ru.                17794   IN      A       5.135.4.19
ghmn.ru.                17794   IN      A       5.135.4.2
ghmn.ru.                17794   IN      A       5.135.4.20
ghmn.ru.                17794   IN      A       5.135.4.21
ghmn.ru.                17794   IN      A       5.135.4.22
ghmn.ru.                17794   IN      A       5.135.4.23
ghmn.ru.                17794   IN      A       5.135.4.24
ghmn.ru.                17794   IN      A       5.135.4.25
ghmn.ru.                17794   IN      A       5.135.4.26
ghmn.ru.                17794   IN      A       5.135.4.27
ghmn.ru.                17794   IN      A       5.135.4.28
ghmn.ru.                17794   IN      A       5.135.4.29
ghmn.ru.                17794   IN      A       5.135.4.3
ghmn.ru.                17794   IN      A       5.135.4.30
ghmn.ru.                17794   IN      A       5.135.4.4
ghmn.ru.                17794   IN      A       5.135.4.5
ghmn.ru.                17794   IN      A       5.135.4.6
ghmn.ru.                17794   IN      A       5.135.4.7
ghmn.ru.                17794   IN      A       5.135.4.8
ghmn.ru.                17794   IN      A       5.135.4.9

...
;; MSG SIZE  rcvd: 4016
```

```
C:\Users\FJ Lin>dig @168.95.1.1 fjlin.tw soa

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 fjlin.tw soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4300
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0c04fb91afed982a859c38325f5f2d730259950aac1ab9c8 (good)
;; QUESTION SECTION:
;fjlin.tw.                      IN      SOA

;; ANSWER SECTION:
fjlin.tw.               3600    IN      SOA     nspl.hinet.net. hostmaster.hinet.net. 2009141640 3600 1800 1209600 3600

;; Query time: 5 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Mon Sep 14 16:44:36 Taipei Standard Time 2020
;; MSG SIZE  rcvd: 126
```

more protections required!!!

126 byte

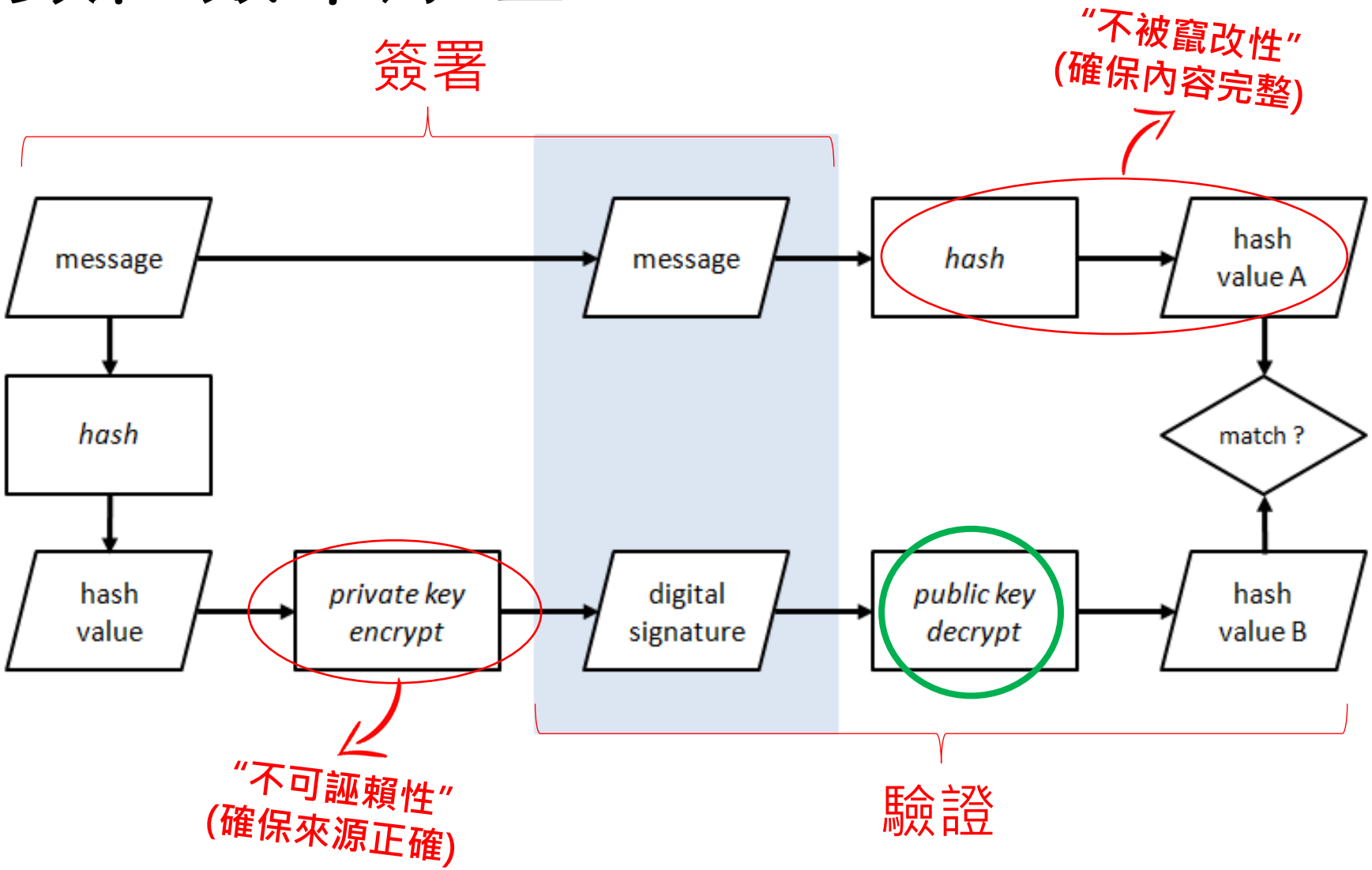
```
C:\Users\FJ Lin>dig @168.95.1.1 fjlin.tw soa +dnssec

; <<>> DiG 9.12.3-P1 <<>> @168.95.1.1 fjlin.tw soa +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47248
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 4f4d69b5aab2d9cd552fa47d5f5f2d773268aeab2e39ea7b (good)
;; QUESTION SECTION:
;fjlin.tw.                      IN      SOA

;; ANSWER SECTION:
fjlin.tw.               3600    IN      SOA     nspl.hinet.net. hostmaster.hinet.net. 2009141640 3600 1800 1209600 3600
fjlin.tw.               3600    IN      RRSIG   SOA 8 2 3600 20201001000000 20200825000000 681 fjlin.tw. ZScpTCvxJiw4MsL
F0I1JfUeEcpUbI2UVo5JQKu8iPaEo5M+Xen5/vfdq 8JTec2Zay5VTpFpMeqByejSlyeEYhTzg/RpuhQgXI6y+zBqZfIhN/d0p XFpRfvu5WekEpwDvWOXuS
Xjse7x56aQaoFDLGTiFle/VH+pzasC7wczq +SX4OXTE7mdTYKWabv378LFHOo7Gg2gdPEDNRgTSNdwNaJty6GeBDIIc QcCjF2ZbbkBGD/0IRb98TBIqTvR
HNjad1/09ejryadfH6TSkZKmTa/Q0 GzQFeVBosWyj9TlykOSvQDzBx845GPSc+pGjw6qJfFJBOLPn1g0xwDkK QFx7/A==

;; Query time: 3 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Mon Sep 14 16:44:39 Taipei Standard Time 2020
;; MSG SIZE  rcvd: 422
```

422 byte (+dnssec, magnified)

Any questions?

PS
備註

數位簽章原理

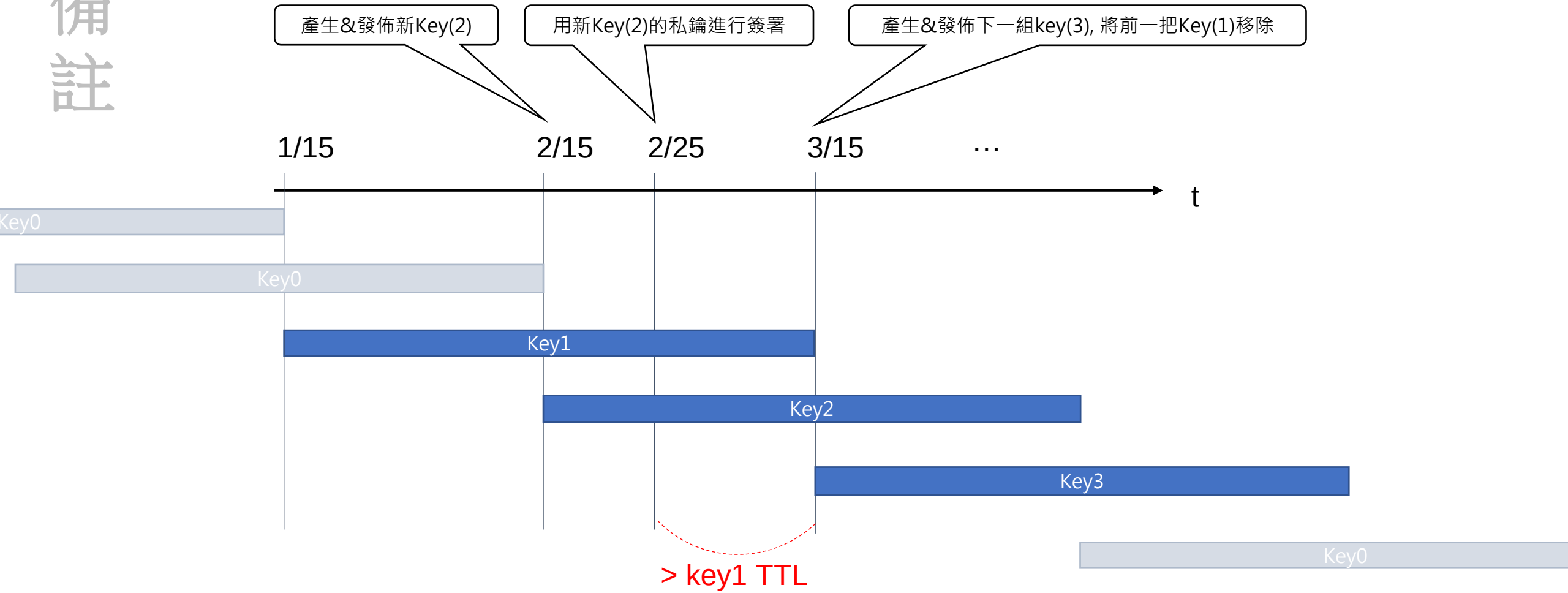


Q：怎確保public key是對的？　A：由第三方掛保證

PS

備註

key (ZSK) rollover plan



ZSK 生命週期, 2個月；KSK 生命週期, 1~5年 (依客戶偏好)