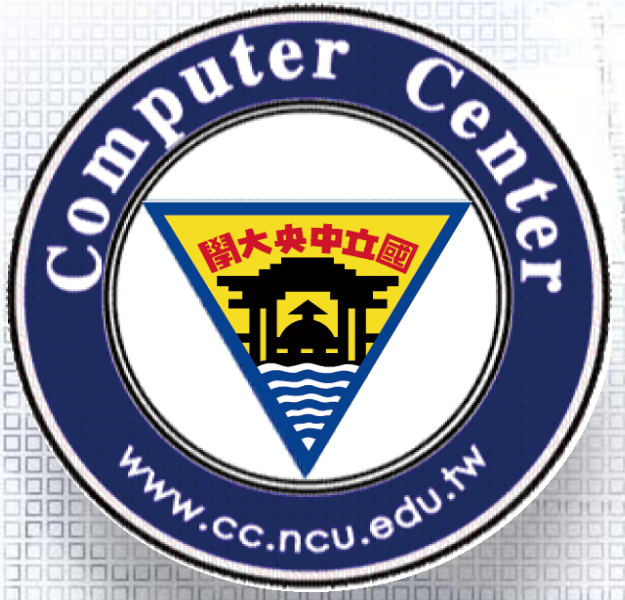


DNSSEC介紹

技術研發組
108/06/10

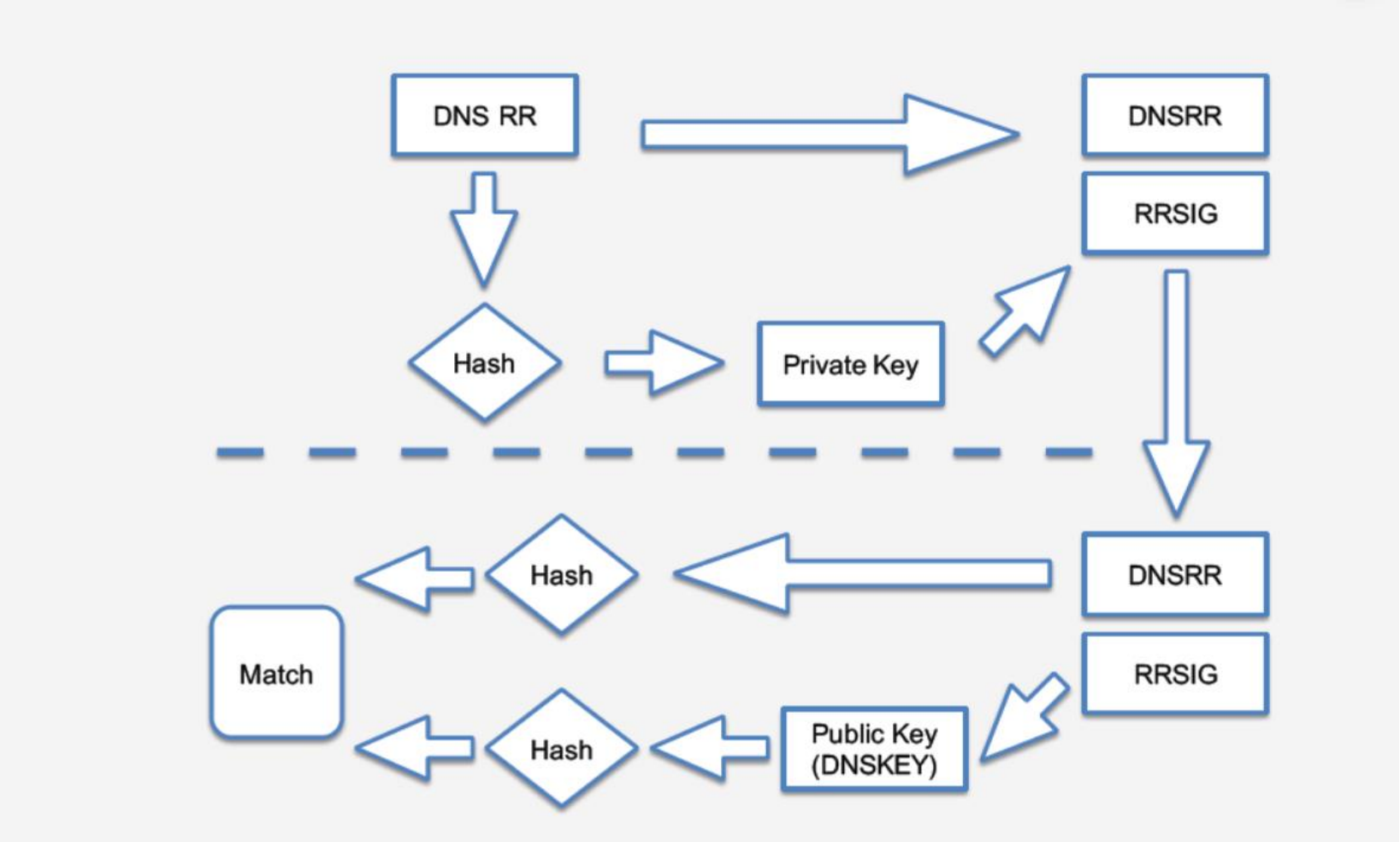
報告大綱

- DNSSEC介紹
- DNSSEC設定與部署
- 注意事項

DNSSEC介紹

- DNSSEC(DNS Security Extensions)是一個DNS的安全強化技術，針對原本的DNS標準做了許多安全上的延伸，以電子簽章技術為基礎，可以完全兼容現行的DNS，目的在於改善DNS的安全性問題。
- DNSSEC提供的安全性功能
  - 資料完整性 (Data Integrity)
  - 來源可驗證性 (Origin Authentication of DNS Data)
  - 可驗證之不存在性 (Authenticated Denial of Existence)

DNSSEC運作原理


DNS RR
DNSRR
RRSIG
Hash
Private Key
DNSRR
Hash
Match
RRSIG
Hash
Public Key
(DNSKEY)

DNSSEC 新增RRs

- Public Key
  - DNSKEY Public key，用來驗證RRSIG
- Private Key
  - 非公開鑰匙，用來簽署網域資料
- Digital signature
  - RRSIG 使用Private key對現有RRs所作的簽章
  - DS Delegation Signer; 上層與下層的簽章
- 負面回應
  - NSEC/NSEC3 在zone中的下一個域名

DNSSEC負擔

- 膨脹數倍的區域檔案
- 增加回應訊息大小
- 查詢次數增加
- 用戶端/伺服端負載加重
- 易造成DNS區域管理上的錯誤

DNSSEC設定與部署

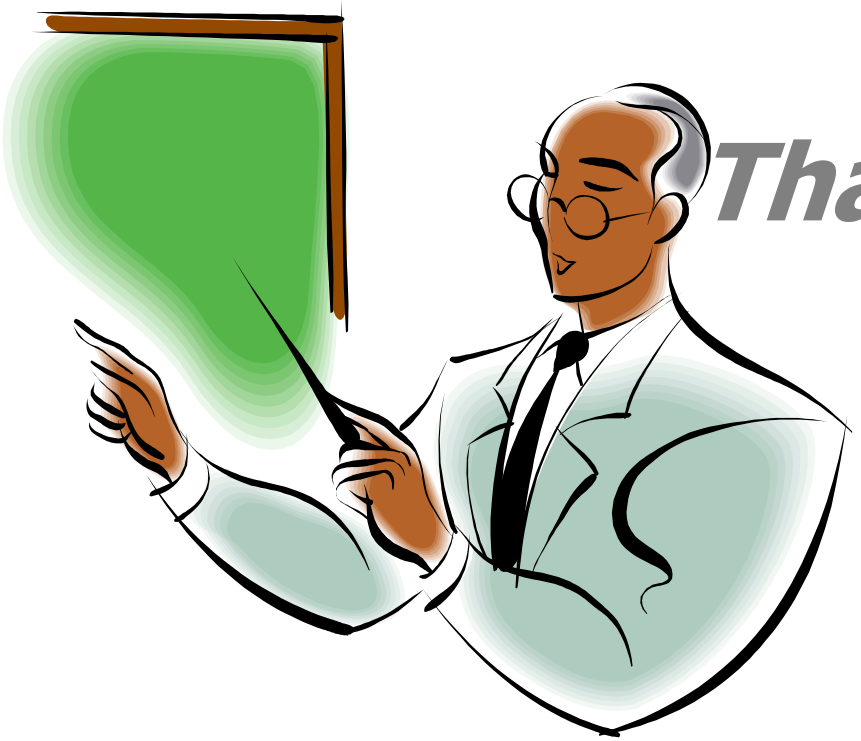
1. 產生金鑰 (ZSK / KSK)
2. 將DNSKEY加入Zone File
3. 簽署網域
4. 啟用.signed檔案
5. 重新啟動DNS Server
6. 檢查log及使用dig檢查
7. 將DS紀錄上傳

DNSSEC設定-DS紀錄上傳

- 請將DS記錄新增至上層的DNS伺服器
  - 請mail 至cloud-service@ncu.edu.tw ，信件標題“XXX單位-DNSSEC DS RECORD“

注意事項

- DNSSEC檢核
  - http://dnsviz.net/
  - https://dnssec-analyzer.verisignlabs.com/
- RRSIG 有效期間預設30天，可設crontab 每周簽屬網域一次
- 備份DNSKEY
- Key rollover



Thank You!