

# TWNIC DNS網路安全研討會

## 安全問題之解決對策 (DNSSEC)



TWCERT/CC

陳宗裕

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## Why do we need DNSSEC?

- Many application depend on DNS
- DNS is not secure
  - There are known vulnerabilities
- DNSSEC protect against data spoofing and corruptions

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

# TW Outline



- Introduction
- DNSSEC mechanisms
  - to authenticate communication between hosts
    - TSIG / SIG0
  - to establish authenticity and integrity of data
    - New RRs
    - Signing a single zone
    - Building chains of trust
    - Key exchange and key rollovers
    - NXT and wildcard issues
- Conclusions

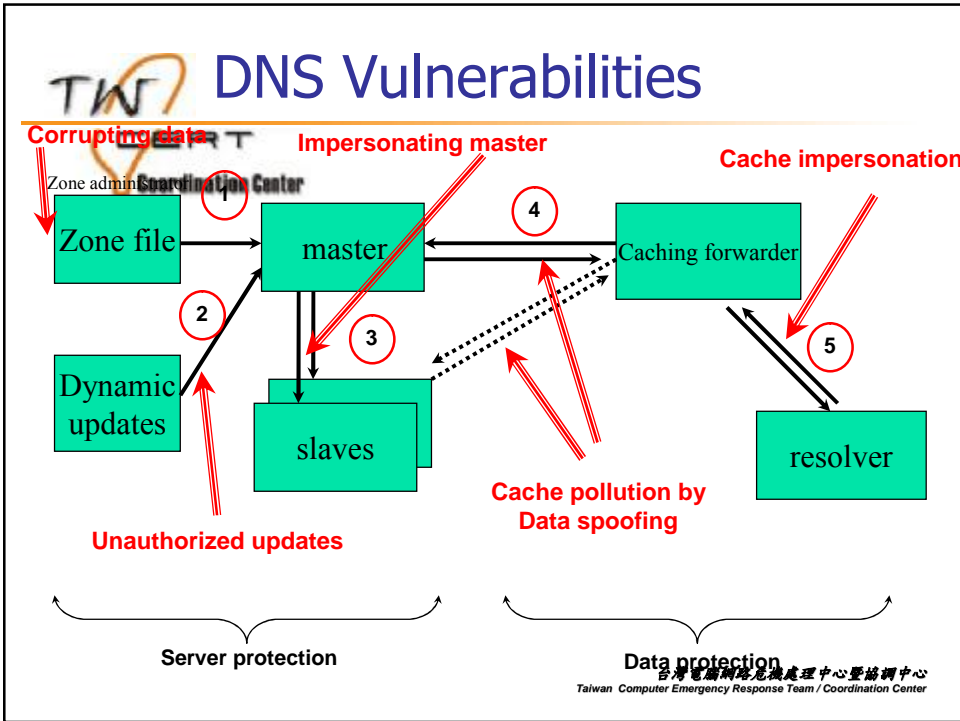
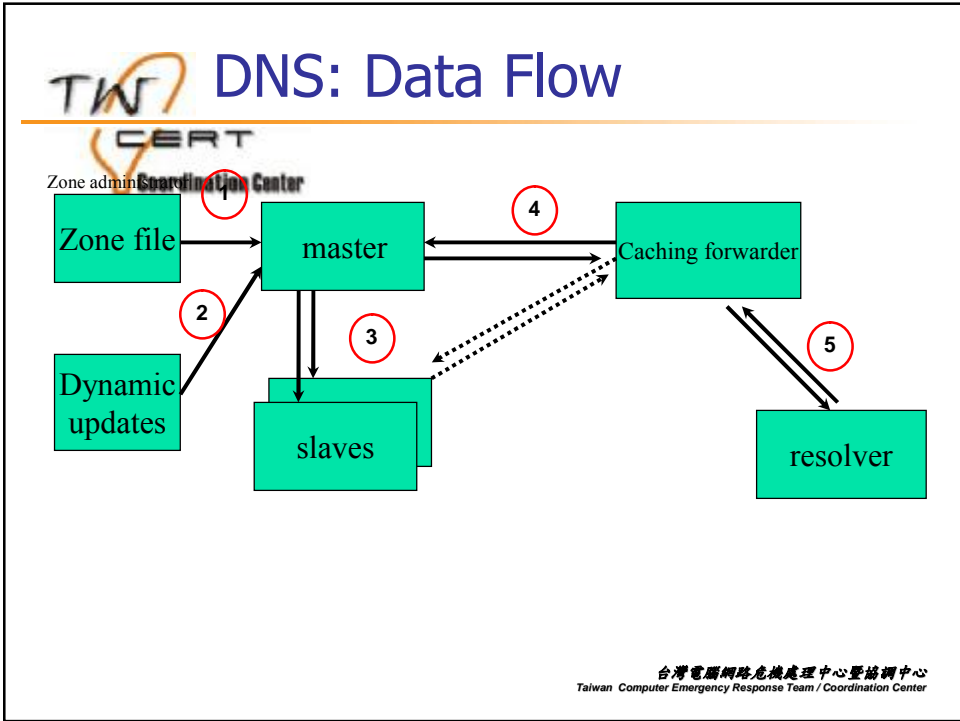
台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

# TW DNS: Known Concepts



- Known DNS concepts:
  - Delegation, Referral, Zone, RRs, label, RDATA, authoritative server, caching forwarder, stub and full resolver, SOA parameters, etc.

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center





## Motivation for DNSSEC

- DNSSEC protects against data spoofing and corruption
  - DNSSEC (TSIG/SIG0) provides mechanisms to authenticate communication between servers
  - DNSSEC (KEY/SIG/NXT) provides mechanisms to establish authenticity and integrity of data
  - DNSSEC (DS) provides a mechanism to delegate trust to public keys of third parties
- A secure DNS will be used as an infrastructure with public keys
  - However it is **NOT** a PKI

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

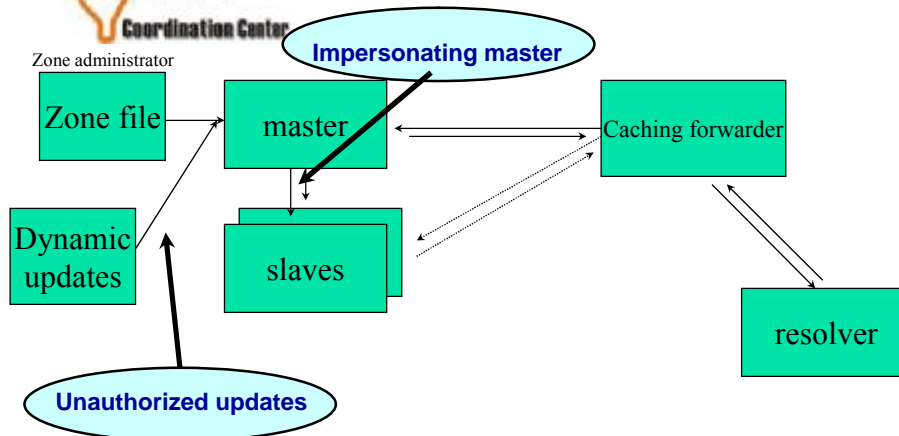


## DNSSEC Mechanisms to Authenticate Communication

- TSIG
- SIG0

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT TSIG Protected Vulnerabilities



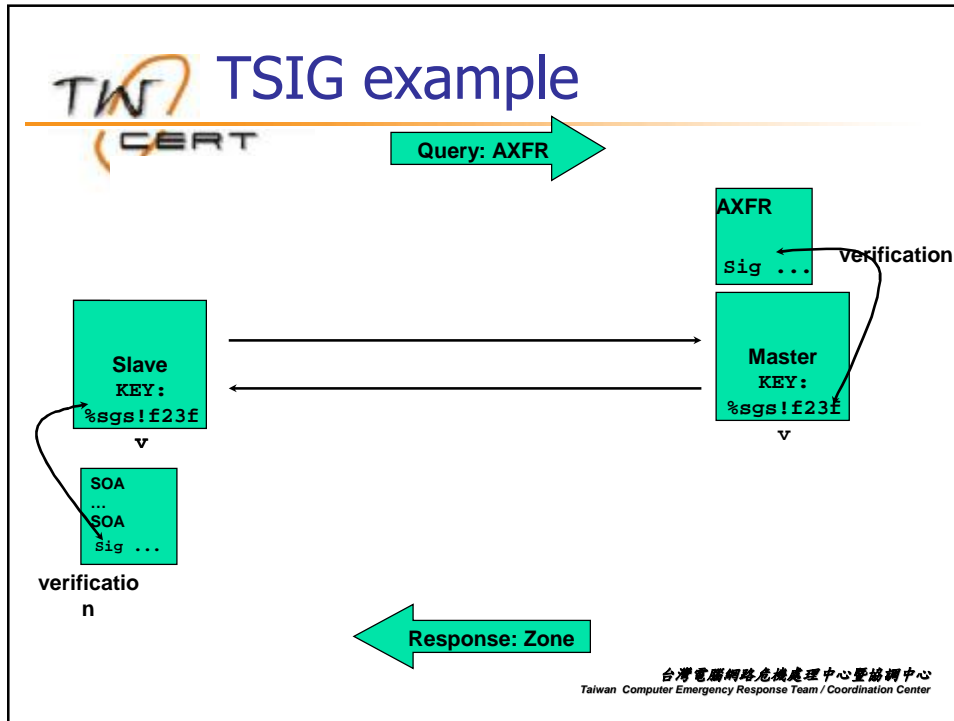
台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT Transaction Signature: TSIG



- TSIG (RFC 2845)
  - authorizing dynamic updates & zone transfers
  - authentication of caching forwarders
  - can be used without deploying other features of DNSSEC
- One-way hash function over:
  - DNS question or answer
  - & the timestamp
- Signed with "shared secret" key
- Used in server configuration, not in zone file

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



- 
- TW CERT** Summary:  
Coordination Center
- TSIG Configuration steps
- Configuring secure transfers between servers with TSIG
    1. Generate a key using “DNSSEC-keygen”
    2. Communicate key with your partner (off-band, PGP...)
    3. Configure your server to require the key for zone transfers
      - “key” statement to configure the key
      - “allow-transfer” statement in the “zone” statement
      - tip: use “include <file\_name>”
    4. Have your partners configure their servers to use the key when talking to you
      - Using the “server” statement
- 台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Authenticating Servers Using SIG0

- Alternatively its possible to use SIG0
  - Not widely used yet
  - Works well in dynamic update environment
- Public key algorithm
  - Authentication against a public key published in the DNS
- SIG0 specified in RFC 2931

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Importance of the Time Stamp

- TSIG/SIG0 signs a complete DNS request / response with time stamp
  - to prevent replay attacks
  - 'seconds since epoch'
  - currently hardcoded at 5 minutes
- Operational problems when comparing times
  - Make sure your local time zone is properly defined
  - `date -u` will give UTC time, easy to compare between the two systems
- Use NTP synchronization!!!

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



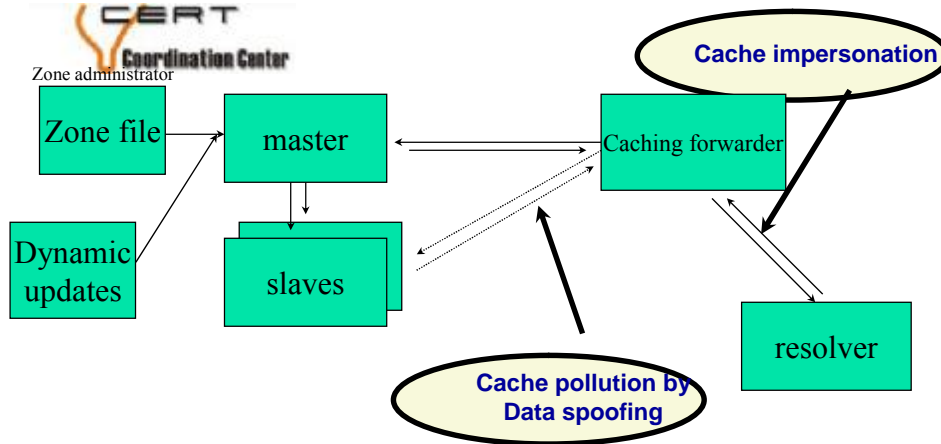
## DNSSEC Mechanisms to Establish Authenticity and Integrity of Data

1. New RRs
2. Using public key cryptography to sign a single zone
3. Delegating signing authority ; building chains of trust
4. Key exchange; Key rollovers
5. NXT and wildcard issues

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Vulnerabilities protected by KEY / SIG / NXT



台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT DNSSEC hypersummary



- Data authenticity and integrity by SIGNing the resource records with private key
- Public KEYS used to verify the SIGs
- Children sign their zones with their private key; The authenticity of their KEY is established by a SIGNature over that key by the parent (DS)
- In the ideal case, only one public KEY needs to be distributed off-band

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT Authenticity and Integrity of Data



- Authenticity: Is the data published by the entity we think is authoritative?
- Integrity: Is the data received the same as what was published?
- Public Key cryptography helps to answer these questions
  - signatures to check both integrity and authenticity of data
  - verifies the authenticity of signatures

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Public Key Crypto Reminder

- Key pair: a private (secret) key and a public key
- Simplified:
  - If you know the public key, you can verify a signature created with the private key
    - Usually an encrypted hash value over a published piece of information; the owner is the only person who can construct the secret. Hence this is a signature
  - If you know the public key, you can encrypt data that can only be decrypted with the private key
- DNSSEC only uses signatures
  - PGP uses both methods

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Public Key Crypto Issues

- Public keys need to be distributed
- Private keys need to be kept secret
- Public key cryptography is 'slow'
- Math:
  - The security of the cryptosystem is based on a set of mathematical problems for which guessing a solution requires scanning a huge solution space (*e.g.* factorization)
  - Algorithms *e.g.*: DSA, RSA, elliptic curve
  - RSA/SHA1 is a good choice

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



# 1. DNSSEC New RRs

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



# DNSSEC New RRs

- 3 Public key crypto related RRs
  - SIG      Signature over RRset made using private key
  - KEY      Public key, needed for verifying a SIG over a RRset
  - DS      Delegation Signer; 'Pointer' for building chains of trust
  
- One RR for internal consistency
  - NXT      Indicates which RRset is the next one in the zone
    - authenticated non-existence of data
  - NXT opt-in variety indicates next secure delegation
    - authenticated insecure delegations

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Other Keys in the DNS

- KEY RR should only be used for DNSSEC
  - keys for other applications should use other RR types
- CERT
  - For X.509 certificates
- Under discussion/development are application keys
  - IP-SEC
  - SSH

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## RR's and RRsets

- Resource Record:

name	TTL	class	type	rdata
<u>www.ripe.net.</u>	7200	IN	A	192.168.10.3

- RRset: RRs with same name, class **and** type:

<u>www.ripe.net.</u>	7200	IN	A	192.168.10.3
			A	10.0.0.3
			A	172.25.215.2

- RRsets are signed, not the individual RRs

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

# TW CERT KEY RDATA



- 16 bits: FLAGS
- 8 bits: protocol
- 8 bits: algorithm
- N\*32 bits: public key

Example:

```
ripe.net. 3600 IN KEY 256 3 5 (  
AQOvhvXXU61Pr8sCwELcqqq1g4JJ  
CALG4C9EtraBKVd+vGIF/unwigfLOA  
O3nHp/cgGrG6gJYe8OWKYNgq3kDChN)
```

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

# TW CERT NXT RDATA



- Points to the next domain name in the zone
  - also lists what are all the existing RRsets for "name"
  - NXT record for last RRset "wraps around" to first RRset after SOA
- N\*32 bit type bit map
- Used for authenticated denial-of-existence of data
  - authenticated non-existence of TYPEs and labels
- Example:

```
www.ripe.net. 3600 IN NXT ripe.net. A SIG NXT
```

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## NXT Record example



```

SO RIGIN ri pe. net.
SOA      ....
        NS      NS. ri pe. net.
        KEY     ....
        NXT     mail box. ri pe. net. SOA NS NXT KEY
SIG
mail box A      192. 168. 10. 2
        NXT     www.ripe.net. A NXT SIG
WWW      A      192. 168. 10. 3
'popserver' is missing NXT     ri pe. net. A NXT SIG

```

- Query for “popserver.ripe.net” would return:
 

```

aa bit set RCODE=NXDOMAI N
authority: mail box. ri pe. net. NXT www.ripe.net. A NXT
SIG

```
- Query for “[www.ripe.net](http://www.ripe.net) MX” would return: an empty answer section and the “www NXT” record in the authority section

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## NXT records



- If your query for data does not exist in a zone, the NXT RR provides proof of non-existence
- If after a query the response is:
  - NXDOMAIN: One, and maybe many more, NXT RRs indicate that the name or a wildcard expansion does not exist
  - NOERROR and empty answer section: The NXT TYPE array proves that the QTYPE did not exist
- NXT records are generated by tools
  - tools also alphanumerically order the zone

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## 2. Using public key cryptography to signing a single zone



台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

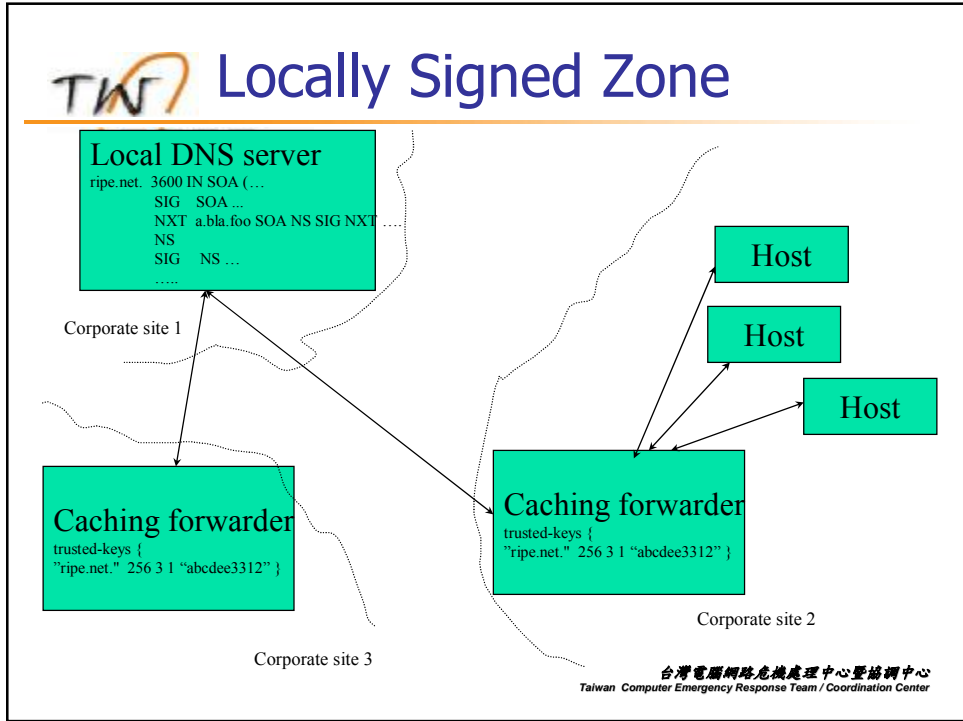
## Signing of a Local Zone - Steps

1. Generate keypair and include public key in the zone file
2. Sign your zone; signing will:
  - sort the zone
  - insert the NXT records
  - insert SIG records (signature over each RRset)
  - generate key-set file (used later)
  - insert DS records (for delegations with valid key-sets)
3. Distribute the Public KEY to those that need to be able to trust your zone
  - they configure your key in their resolver
  - thus configuring “secure entry point” in the tree

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



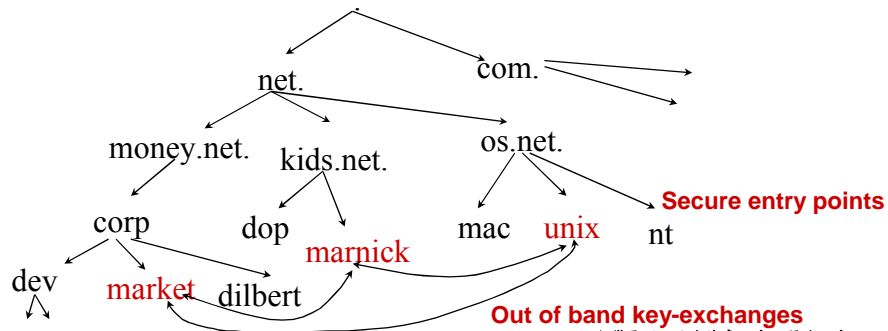
# Locally Signed Zone



# Locally Secured Zones



- Key distribution problem for distributing keys
  - It would be better if the whole tree would be secured!





## Notes on Secured Zones

- Only those records for which the server is authoritative for are signed
  - NS records in the APEX are signed
  - Delegating NS records and GLUE are not signed
    - DS RRs are

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## 3. Delegating Signing Authority

*building chains of trust*

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Using the DNS to Distribute Keys

- Secured islands make key distribution problematic
- Use the DNS itself to distribute keys:
  - one trusted key can be used to establish authenticity of other keys
  - Building chains of trust from the root down
  - Parents need to sign the keys of their children
- In an ideal world:
  - You would only configure one key (the root key)
  - Always delegate trust from parent to child

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Delegation Signer (DS)

- The parent delegates authority to sign DNS RRs to the child using the DS record
- DS is a pointer to the next key in the chain of trust
  - You may trust data that is signed using a key that the DS points to
- Introduced to solve problems with key-rollovers
  - More on that later

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## DS RRs for delegation

- Parent is authoritative for the DS record
  - It should not appear in the child's apex
- DS resource records are used for Delegation of Security
- DS is not backwards compatible with RFC2535
- Eases resigning
  - parent can sign often → short signature lifetime → shorter impact time when key gets compromised

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## DS RDATA

This field indicates which key is the next in the chain of trust

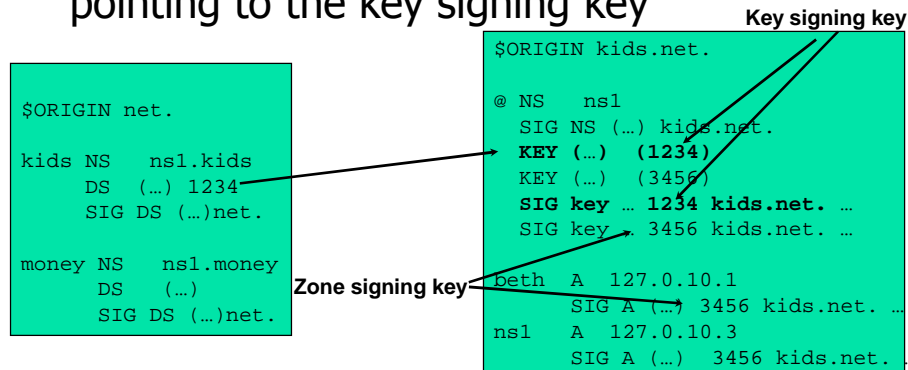
- 16 bits: key tag
- 8 bits: algorithm
- 8 bits: digest type
- 20 bits: SHA-1 Digest

```
$ORIGIN ripe.net.  
disi.ripe.net 3600 IN NS ns.disi.ripe.net  
disi.ripe.net. 3600 IN DS 3112 1 1 (  
  
239af98b923c023371b52  
  
1g23b92da12f42162b1a9  
  
)
```

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT Delegating Signing Authority

- Parent signs the DS record pointing to the key signing key



- The parent is authoritative for the DS RR of its children

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT Key / Zone Signing Keys

- Administrative distinction
- DS points to a key signing key (KSK)
- KSK signs ZSK
- The zone is signed with a zone signing key (ZSK)
  - (these keys may be the same)
- Key signing key may be long lived, and “bigger”
- Zone signing key may be short lived
  - can be “smaller” = “faster”

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Chain of Trust Verification, Summary

- Data in zone can be trusted if signed by a Zone-Signing-Key
- Zone-Signing-Keys can be trusted if signed by a Key-Signing-Key
- Key-Signing-Key can be trusted if pointed to by trusted DS record
- DS record can be trusted
  - if signed by the parents Zone-Signing-Key
  - or
  - DS or Key records can be trusted if exchanged out-of-band and locally stored (Secure entry point)

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Zone status terminology (RFC3090)

- Verifiable Secure
  - RRset and its SIG can be verified with a KEY that can be chased back to a trusted key, the parent has a DS record
- Verifiable Insecure
  - RRset sits in a zone that is not signed and for which the parent has no DS record (more next slide)
- BAD
  - RRset and its SIG can not be verified (somebody messed with the sig, the RRset, or the SIG expired)
  - A zone and its subzones are BAD when the parent's SIG over the Child's key is BAD

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



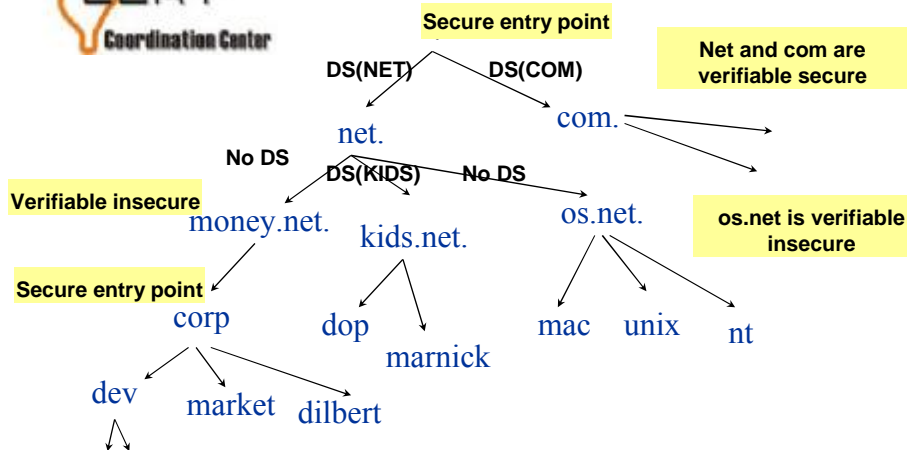
## Insecure Children

- Cryptographic evidence for the verifiably insecure zone status is given by parent
- If there is no DS record as proven by a NXT record with valid signature, the child is not secured
  - NXT opt-in only gives NXT RR for secure delegations
- A child may contain signatures but these will not be used when building a chain of trust
  - Secure island

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Illustrated Terminology



Resolver has key of root and corp.money.net configured as secure entry points

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## TW CERT Building the Chain of Trust



- The child has to:
  - be secure (see "Signing the local zone")
  - upload (off-band) the KSK to the parent
- The parent has to:
  - generate the DS record from the KSK of the child
  - sign the DS record with his own ZSK (re-sign his zone)
- Then the parent has to repeat the process, going to his own parent, and so on, till the "." (root)
- All of this could be done automatically
  - tools are being developed

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## 4. Key Exchange Considerations



台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Private Key Compromise

- You have to keep your private key secret
- Private key can be stolen
  - Put the key on stand alone machines or on bastion hosts behind firewalls and strong access control
- Private key reconstruction (crypto analysis)
  - random number not random
  - Leakage of key material (DSA)
  - Brute force attacks

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Key Rollovers

- Try to minimize impact
  - Short validity of signatures
  - Regular key-rollover
- Remember: KEYS do not have timestamps in them -- the SIG over the KEY has the timestamp
- Key rollover involves 2nd party:
  - State to be maintained during rollover
  - operationally expensive

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Short Signature Life Time

- Short parent signature over DS RR protects child
- Order 1 day possible

```
ripe.net. 3600 IN SIG DS 1 3 3600 20030304144523 (
20030204144523 3112 net.
VJ+8ijXvbrTLeoAiEk/qMrduRnYZM1VlqhN
vhYuAcYKe2X/jqYfMfjSUrnhPo+0/GOZjW
66DJubZPmNSYXw== )
```

Signature expiration

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## Key Rollover (part 1)

- Scheduled rollover of the child's Key Signing Key
- Child replaces key-1 with key-2 and wants parent to sign it

```
$ORIGIN net.
kids NS ns1.kids
DS (...) 1
SIG DS (...)net.
```

old parent zone

```
$ORIGIN kids.net.
@ NS ns1
KEY (...) (1)
KEY (...) (5)
SIG KEY (...) kids.net. 1
SIG KEY (...) kids.net. 5
ns1 A 127.0.10.3
SIG A (...) kids.net. 5
```

old child zone

```
$ORIGIN kids.net.
@ NS ns1
KEY (...) (1)
a) KEY (...) (2)
KEY (...) (5)
SIG KEY (...) kids.net. 1
b) SIG KEY (...) kids.net. 2
SIG KEY (...) kids.net. 5
ns1 A 127.0.10.3
SIG A (...) kids.net. 5
```

a) Create key 2

b) Sign key-set with key 1 and 2  
and send key 2 to parent

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## Key Rollover (part 2)



- c) Parent generates and signs DS record
- d) Child signs his zone with **only** key 2, once parent updated his zone

```
$ORIGIN net.  
  
kids NS    nsl.kids  
        DS    (...) 2  
        SIG DS (...)net.
```

```
$ORIGIN kids.net.  
  
@ NS     nsl  
  KEY (...) 2  
  KEY (...) 5  
  SIG KEY (...) kids.net. 2  
  SIG KEY (...) kids.net. 5  
nsl  A    127.0.10.3  
  SIG A   (...) kids.net. 5
```

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center

## Timing of the Scheduled Key Rollover



- Child should not remove the old key while there are still servers handing out the old DS RR.
- The new DS will need to be distributed to the slave servers
  - max time set by the SOA expiration time
- The old DS will need to have expired from caching servers.
  - Set by the TTL of the original DS RR.
- You (or your tool) can check if the master and slave have picked up the change

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Scheduled Key Rollover Issues

- Currently it is not possible to distinguish between KSK and ZSK
- Once that distinction can be made, the rollover can be fully automated.
  - <http://www.ietf.org/internet-drafts/draft-ietf-dnsexp-keyrr-key-signing-flag-05.txt>

台灣電腦網路危機處理暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Unscheduled Rollover Problems

- Needs out of band communication
  - with parent and pre-configured resolvers
- The parent needs to establish your identity again
- How to protect child delegations?
  - unsecured?
- There will be a period that the stolen key can be used to generate data useful on the Internet
  - There is no 'revoke key' mechanism
- Emergency procedure must be on the shelf

台灣電腦網路危機處理暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Key Rollover - Summary

1. Generate new KSK
2. Sign with old and new KSK's
3. Inform any resolvers that have you as a trusted entry point of the new key
  - trusted- keys configuration
4. Query for the parental DS and remember the TTL
  - you will need it later
5. Upload the new KSK to the parent
  - The parent will generate a new DS RR.
6. Check if **\*all\*** parental servers (slaves and masters) picked up the change
7. Wait another TTL before removing the old key

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## The DNS is not a Public Key Infrastructure (PKI)

- All procedures on the previous slide are based on local policy i.e. policy set by the zone administrator
- A PKI is as strong as its weakest link, we do not know the strength of the weakest link
  - Certificate Authorities control this by SLAs
- The DNS does not have Certificate Revocation Lists
- If the domain is under one administrative control you might be able to enforce policy

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## 5. NXT RR and Wildcard Issues

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Not just one NXT RR in your response

- If you query for data that does not exist in a zone, the NXT RR provides proof of non-existence
- The principle is simple, as explained before but there is a complication: WILDCARDS.
- Wildcards are needed and will need to be secured:  
\*.1.3.e164.arpa. NAPTR (redirection to some ldap server)

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## Recap Wildcards

- \*.ripe.net will provide an answer for:
  - Any label that is in the ripe.net zone
  - For labels not already known to exist between the query name and the wildcard domain
    - If B.X and \*.X appear in the zone with origin X then a query for Z.X would return the wildcard data. The wildcard answer would not apply for question for B.X, A.B.X or X.
  - The wildcard label sorts canonically before the alphabetical data
    - X
    - \*.X
    - B.X
    - A.B.X

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



## DNSSEC - Conclusions

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



- DNSSEC provides a mechanism to protect DNS
- DNSSEC implementation:
  - TSIG for communication between servers
  - SIG, KEY and NXT for data
- DNSSEC main difficulties:
  - keeping private key safe
  - distributing public keys

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center



- 資料來源
  - RIPE NCC: DNSSEC Training Course, <http://www.ripe.net/training/dnssec/>
  - DNSSEC, <http://www.dnssec.net>
- 資料參考
  - SANS Reading Room: DNS Issues, [http://www.sans.org/rr/catindex.php?cat\\_id=17](http://www.sans.org/rr/catindex.php?cat_id=17)
  - 交通大學 中文化DNS教學系統, <http://dnsrd.nctu.edu.tw>

台灣電腦網路危機處理中心暨協調中心  
Taiwan Computer Emergency Response Team / Coordination Center