ALISHA GURUNG
alisha.gurung@bt.bt
BHUTAN TELECOM LIMITED

Dnssec and .bt signing

Agenda

- Recap: How dns works?
- DNS Vulnerabilities
- Dnssec concepts
- Signing “.bt”

DNS??

- Distributed database
- Ip address→ domain name and vice versa
- Types of DNS Servers
    a) Authoritative DNS

    -Master

    -Slaves

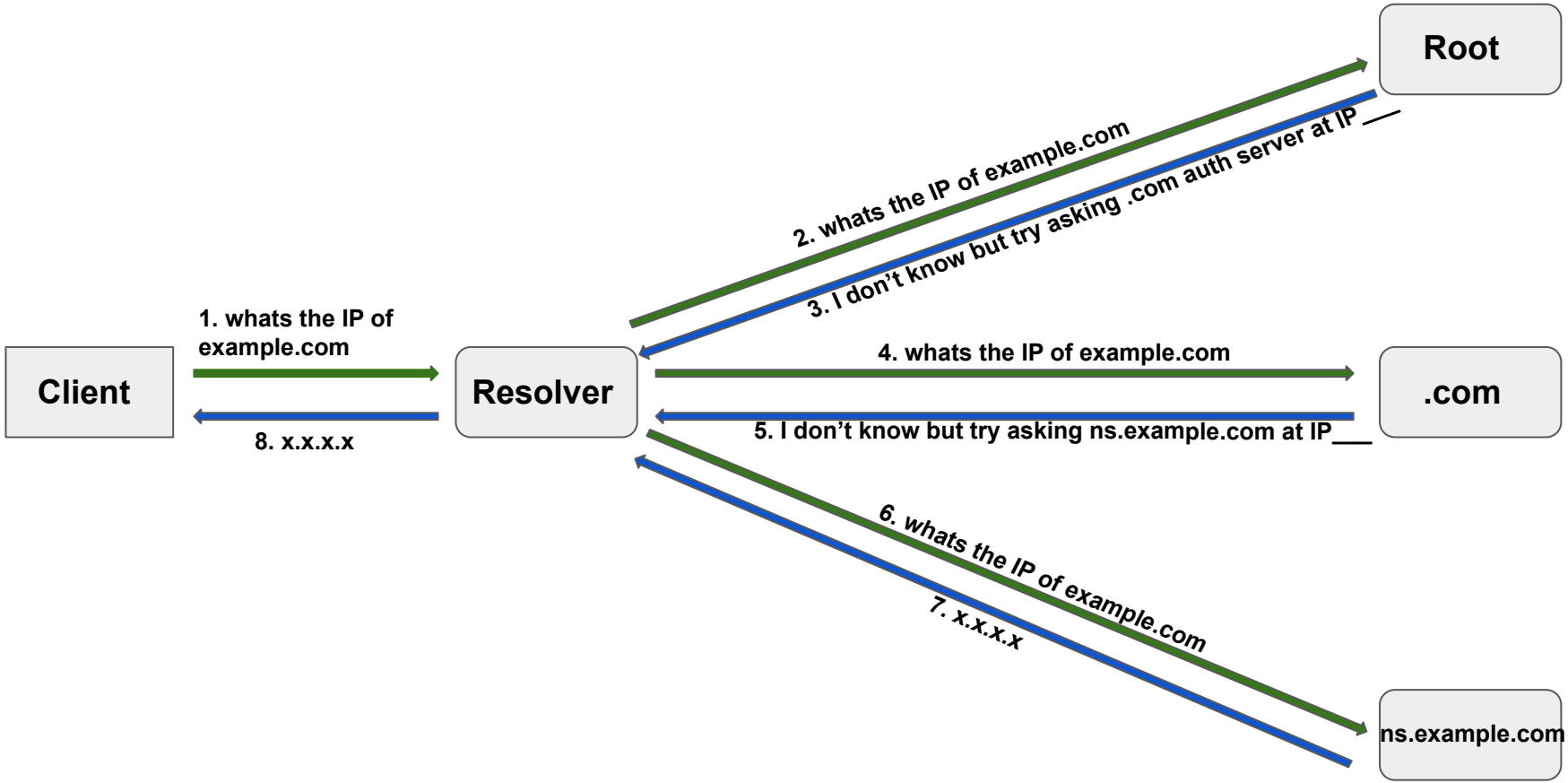
    b) Resolvers

    -Recursive

    -Cache

    -Stub resolver

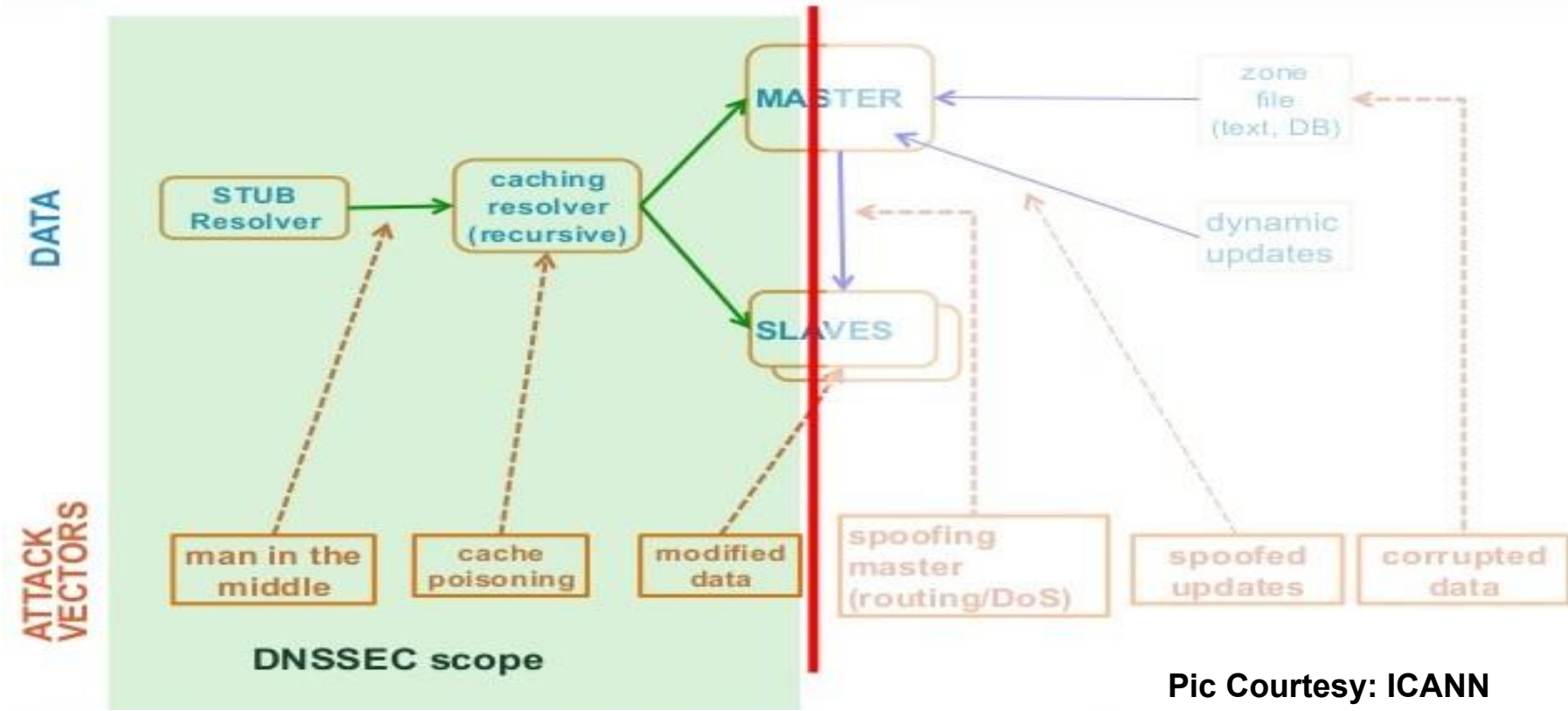
Normal Dns Flow



Resource Records and Zone Sample

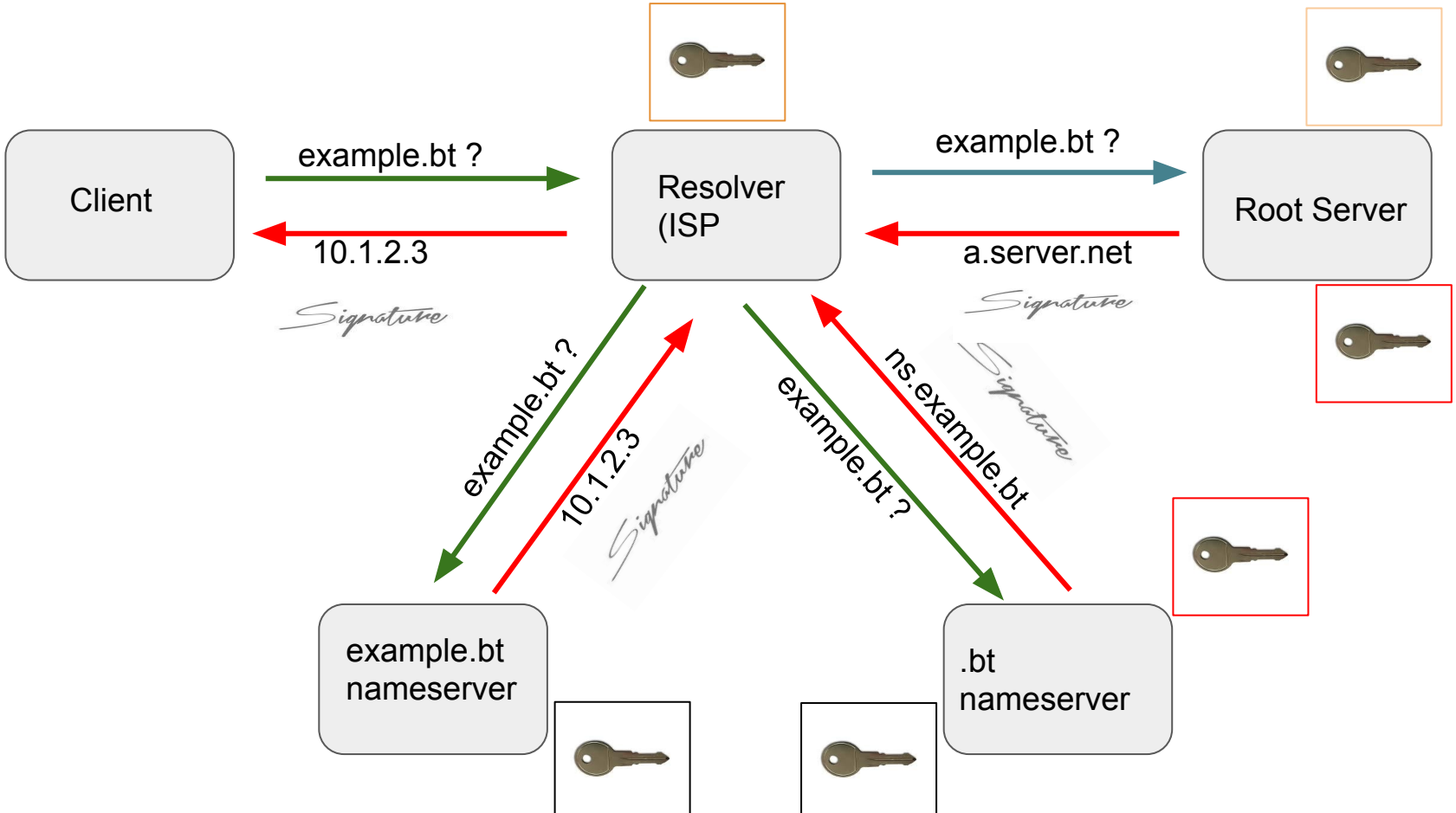
```
1  @              SOA      ns.mydomainname.com. myhostname.mydomainname.com. (
2                              1448207972       ; Serial
3                              10800     ; Refresh
4                              3600      ; Retry
5                              604800    ; Expire
6                              10800 )   ; Minimum
7
8  mydomainname.com.                              NS     ns1.mydomainname.com.
9  mydomainname.com.                              NS     ns2.mydomainname.com.
10 ns1.mydomainname.com.                          A      194.23.253.196
11 ns2.mydomainname.com.                          A      194.23.254.196
12 mydomainname.com.                              A      194.23.253.196
13 www.mydomainname.com.                          A      194.23.253.196
14 mydomainname.com.                              AAAA      4001:41d0:2:80c4::
15 www.mydomainname.com.                          AAAA      4001:41d0:2:80c4::
16 mail.mydomainname.com.                         A      194.23.253.196
17 webmail.mydomainname.com.                      A      194.23.253.196
18 ftp.mydomainname.com.                          CNAME          mydomainname.com.
19 mydomainname.com.                              MX   10 mail.mydomainname.com.
20 _domainkey.mydomainname.com.                   TXT    "o=-"
21 default._domainkey.mydomainname.com.           TXT    "p=;"
22 mydomainname.com.                              TXT    "v=spf1 +a +mx -all +a:myhostname.mydom
```

DNS Vulnerabilities



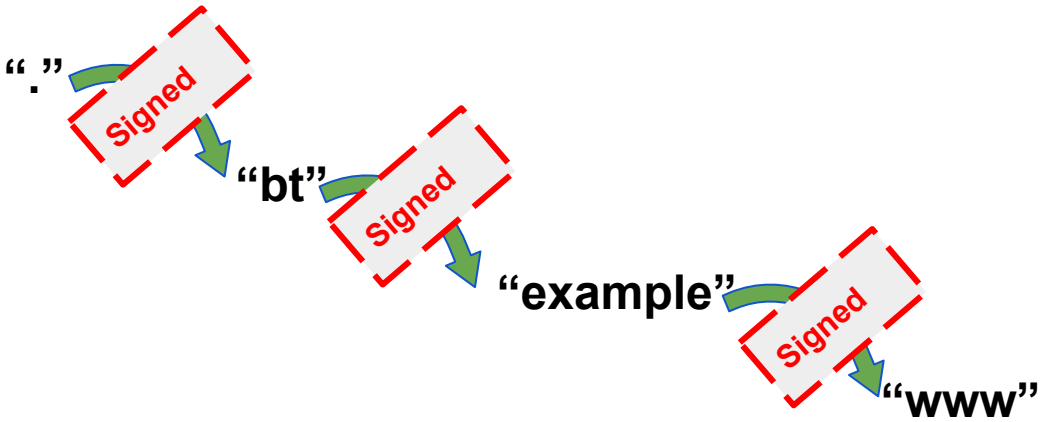
Pic Courtesy: ICANN

How Dnssec works?



How Dnssec works?(continued…)

- Using the existing delegation based model of distribution
- Don’t sign the entire zone, sign a RRset
- Parent DOES NOT sign the child zone.
- The parent signs a pointer (hash) to the key used to sign the data of the child zone (DS record)
- Example with www.example.bt.



Signing of .bt

- BCP & RFCs
- Test Bed Server
- IANA portal update
- Only signing ,no publishing
- Several testing from different networks
- Finally the DS record
- Subsequently signing of edu.bt, gov.bt, org.bt, etc
- Drawback: No portal like many other tld operators for uploading Ds
- But upcoming and ongoing future project

Signing of .bt (Continued)

- Checked that signatures are updated according to the applicable configuration.[R45]
- Checked that all name servers respond with the correct authenticated positive responses for the zone’s SOA, NS and DNSKEY records.
- Verified that all name servers respond with the correct authenticated denial of existence.
- Checked that all name servers are updated with current data.
- Checked that all name servers are accurately synchronized with a correct time source.
- Separate second level tld servers for less computational load.

Difficulties

- What could go wrong?The “risk” factor
- Starting point….
- IANA Portal
- Ipv6 address Change for secondaries
- Signing issues
- Sensitivity towards human/technical error which could make the whole cctld(.bt) unavailable or the secondary tlds.

Some RFCs

- The signing system MUST support DNSSEC in compliance with RFC4033 [13],RFC4034 [15] and RFC4035 [14].
- [R23]The signing system MUST support signing with the following algorithms:RSA/SHA-1 as specified in RFC3110 [11], as well as RSA/SHA-256 and RSA/SHA-512as specified in RFC5702 [19].
- The signing system SHOULD support signing with the following algorithms: ECDSAP-256/SHA-256 and ECDSA P-384/SHA-384 as specified in RFC6605 [18].
- The signing system MUST support NSEC3 as specified in RFC5155 [21].
- The signing system MUST support DS records published with SHA-256 as specified inRFC4509 [17].

End User/Organization Signing their zone?

- Check if you have a validating resolver
- What's your domain?.bt?.com?.gov.bt?.... Parent needs to be signed first
- Where is the auth dns?
- If with your ISP, ask them.
- If within your premises, sign your zone as per your requirement and RFCs and send the DS record to the parent (for .bt to Bhutan Telecom)
- Until the portal/key management system is up, via email for those having their own auth dns (same for many cctld operators)
- Would require capacity building/workshop for dnssec if the auth is with the customers.
- Customers coming up and interested in signing their domains.
- Lack of awareness and competency
- **DNSSEC DOES NOT** provide encryption, only adds authentication and data integrity.
- Looking into last mile dns, dot and doh?

Dnssec Validation Statistics for Bhutan

CC	Country	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
FM	Micronesia (Federated States of), Micronesia, Oceania	93.72%	37.30%	1,386	0.71	980
LR	Liberia, Western Africa, Africa	93.68%	20.70%	14,509	0.79	11,449
KI	Kiribati, Micronesia, Oceania	93.05%	37.16%	331	1.39	458
FO	Faeroe Islands, Northern Europe, Europe	92.63%	5.74%	2,197	0.54	1,186
BT	Bhutan, Southern Asia, Asia	92.62%	12.07%	13,774	0.81	11,153
NR	Nauru, Micronesia, Oceania	91.65%	98.10%	683	0.21	145
IS	Iceland, Northern Europe, Europe	90.46%	9.88%	6,481	1.22	7,900
PW	Palau, Micronesia, Oceania	88.54%	43.51%	1,248	0.23	287
DJ	Djibouti, Eastern Africa, Africa	87.18%	58.29%	7,307	3.5	25,553
BJ	Benin, Western Africa, Africa	85.82%	83.81%	37,656	1.27	47,783

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