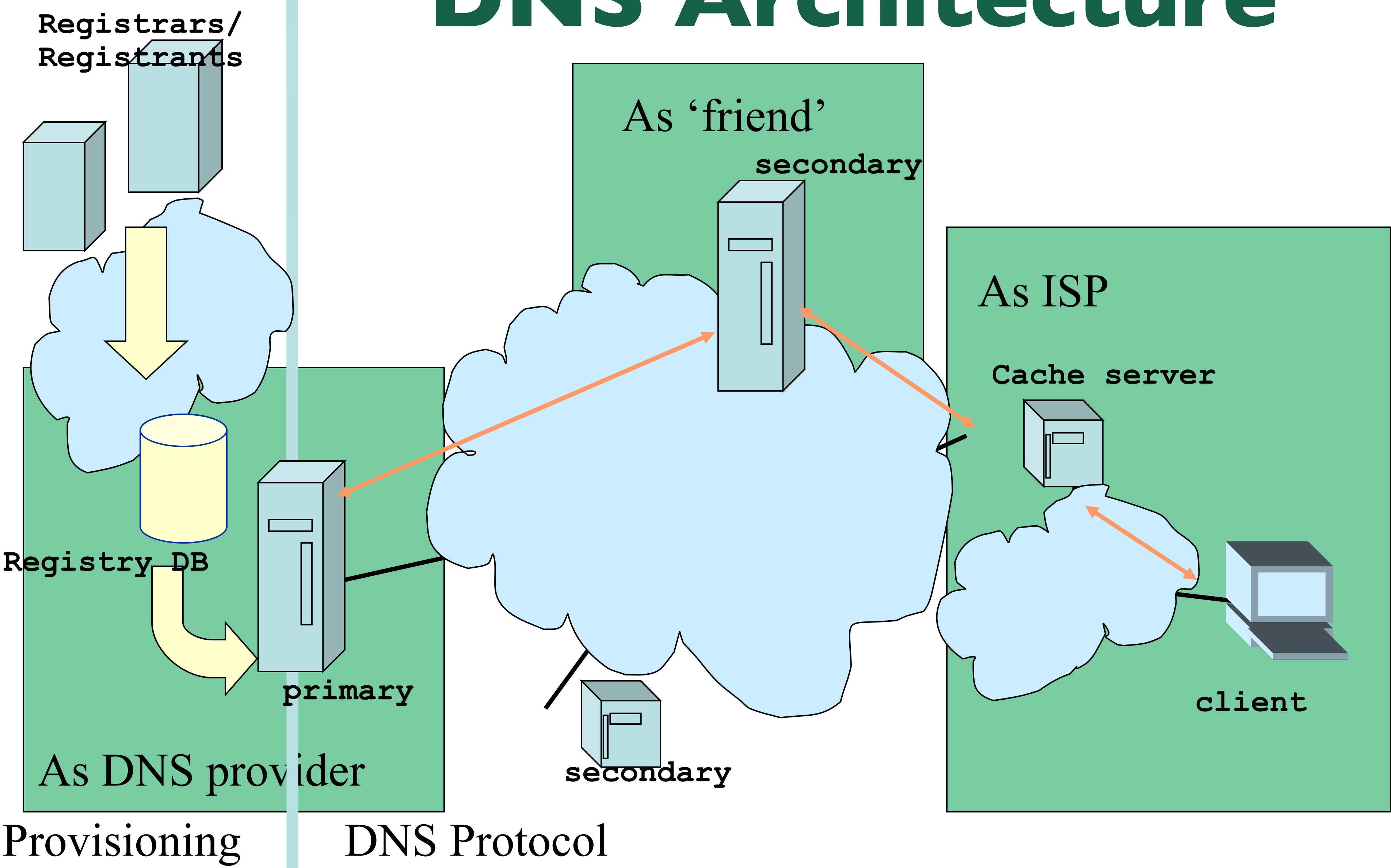
DNSSEC

Part1: DNSSEC: Why and How

DNSSEC Tutorial

AfriNIC-15
Yaounde, 11/21/2011

DNS Architecture



Why DNSSEC

- Good security is multi-layered
  - Multiple defense rings in physical secured systems
  - Multiple ‘layers’ in the networking world
- DNS infrastructure
  - Providing DNSSEC to raise the barrier for DNS based attacks
  - Provides a security ‘ring’ around many systems and applications

The Problem

- DNS data published by the registry is being replaced on its path between the "server" and the "client".

- This can happen in multiple places in the DNS architecture
  - DNS uses UDP, much easier to spoof
  - Some places are more vulnerable to attacks then others
  - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)

- Deficiencies in the DNS protocol and in common deployment create some weaknesses
  - Query ID is 16 bits (0-65535)
  - Lack of UDP packet Source Port (16 bits) and Query ID randomization in some deployments

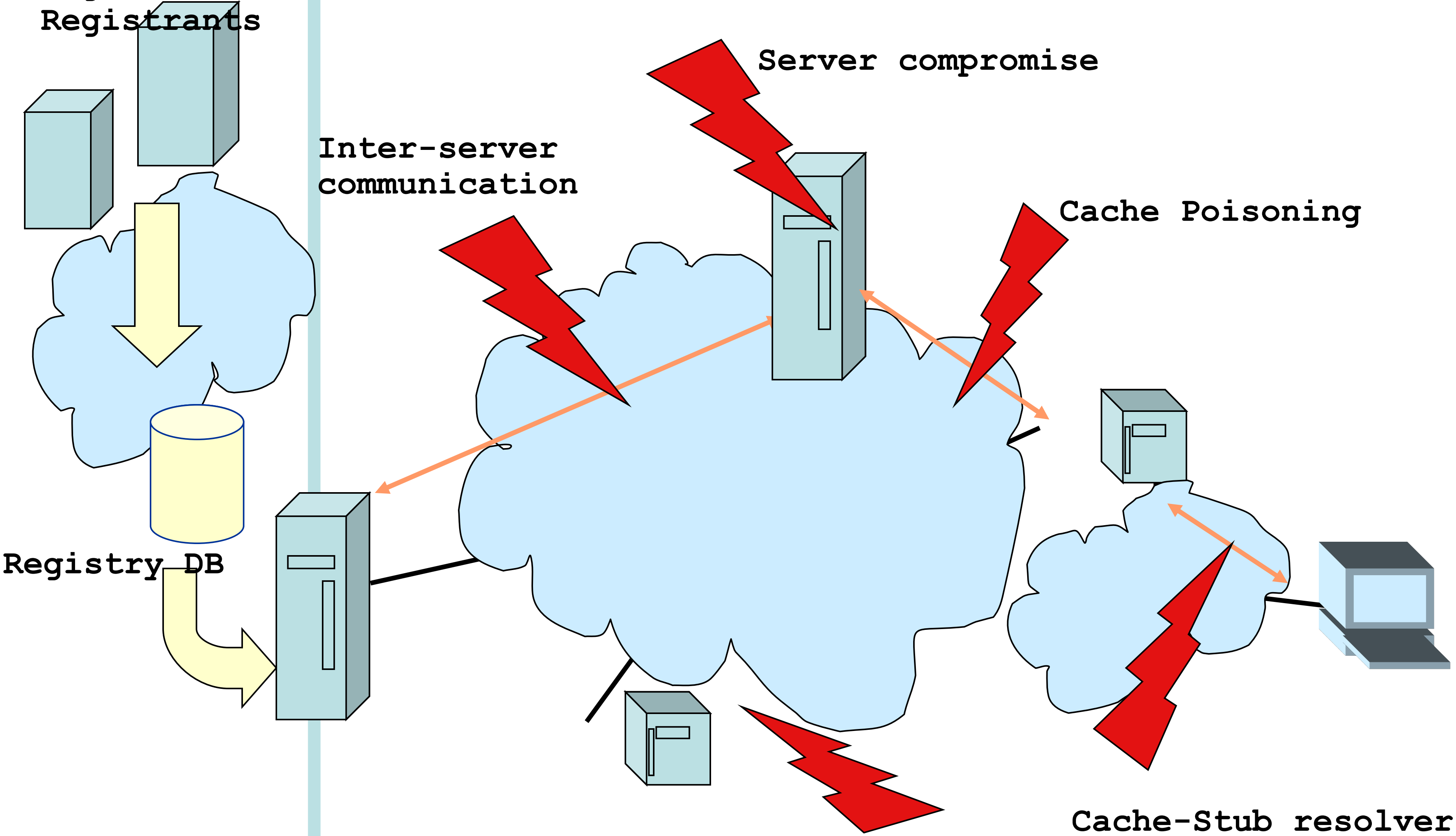
The Problem(cont'd)

- Kaminsky Attacks published in 07/2008 showed how these weaknesses can be exploited for cache poisoning attacks
  - Panic (although all of this is known for a long !!!)
  - Workarounds to contain the situation
    - Source port/Query ID randomization
    - Recommendations for DNS deployment

      http://www.kb.cert.org/vuls/id/800113
  - The Solution ????
    - DNSSEC

And so, DNSSEC is now known as a critical component of DNS Security

DNS Vulnerabilities



Registrars
Registrants

Registry DB

Inter-server
communication

Server compromise

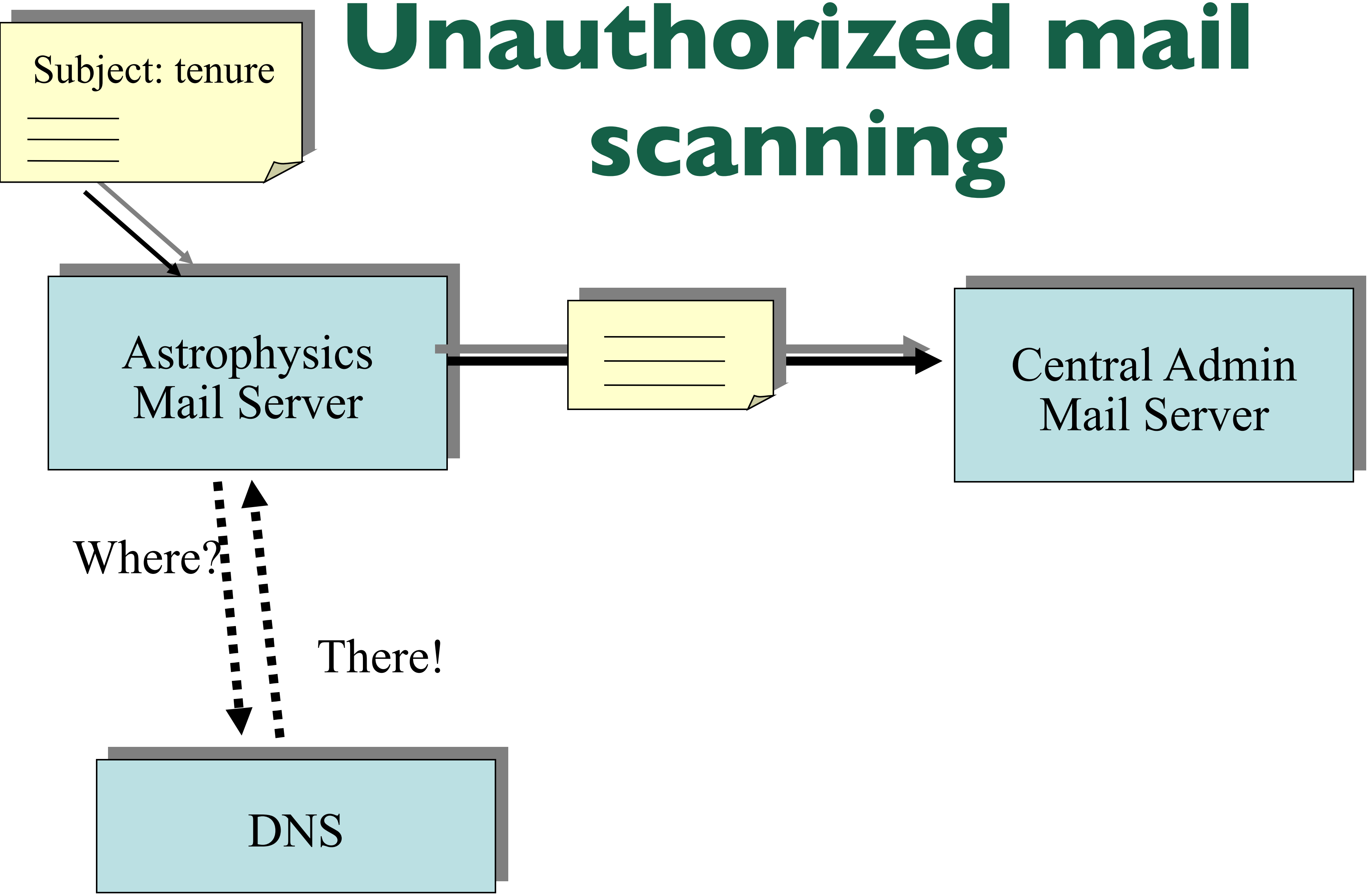
Cache Poisoning

Cache-Stub resolver
communication

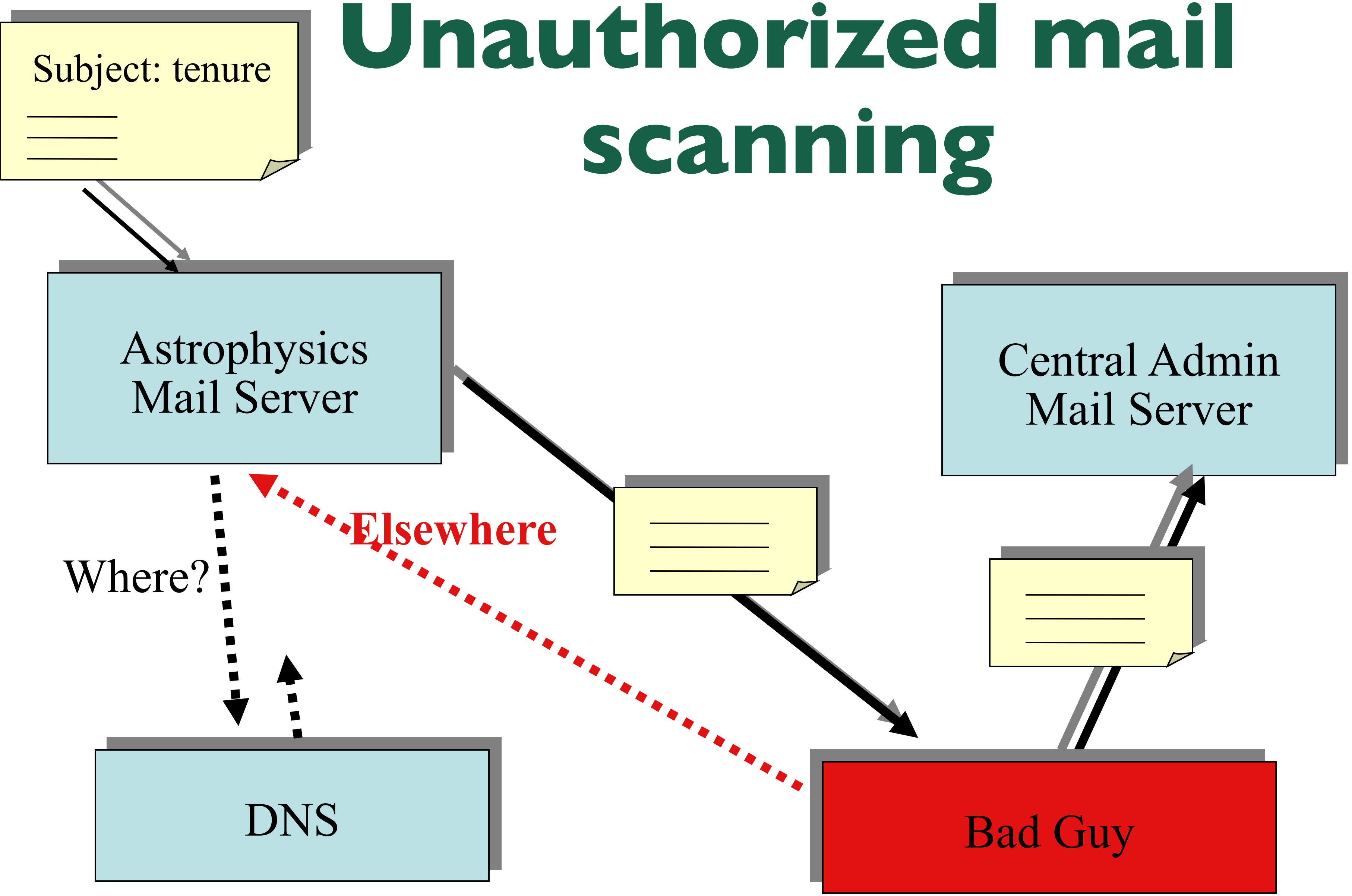
Provisioning

DNS Protocol

Example: Unauthorized mail scanning



Example: Unauthorized mail scanning



Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
  - Tranport and Application security are just other layers.

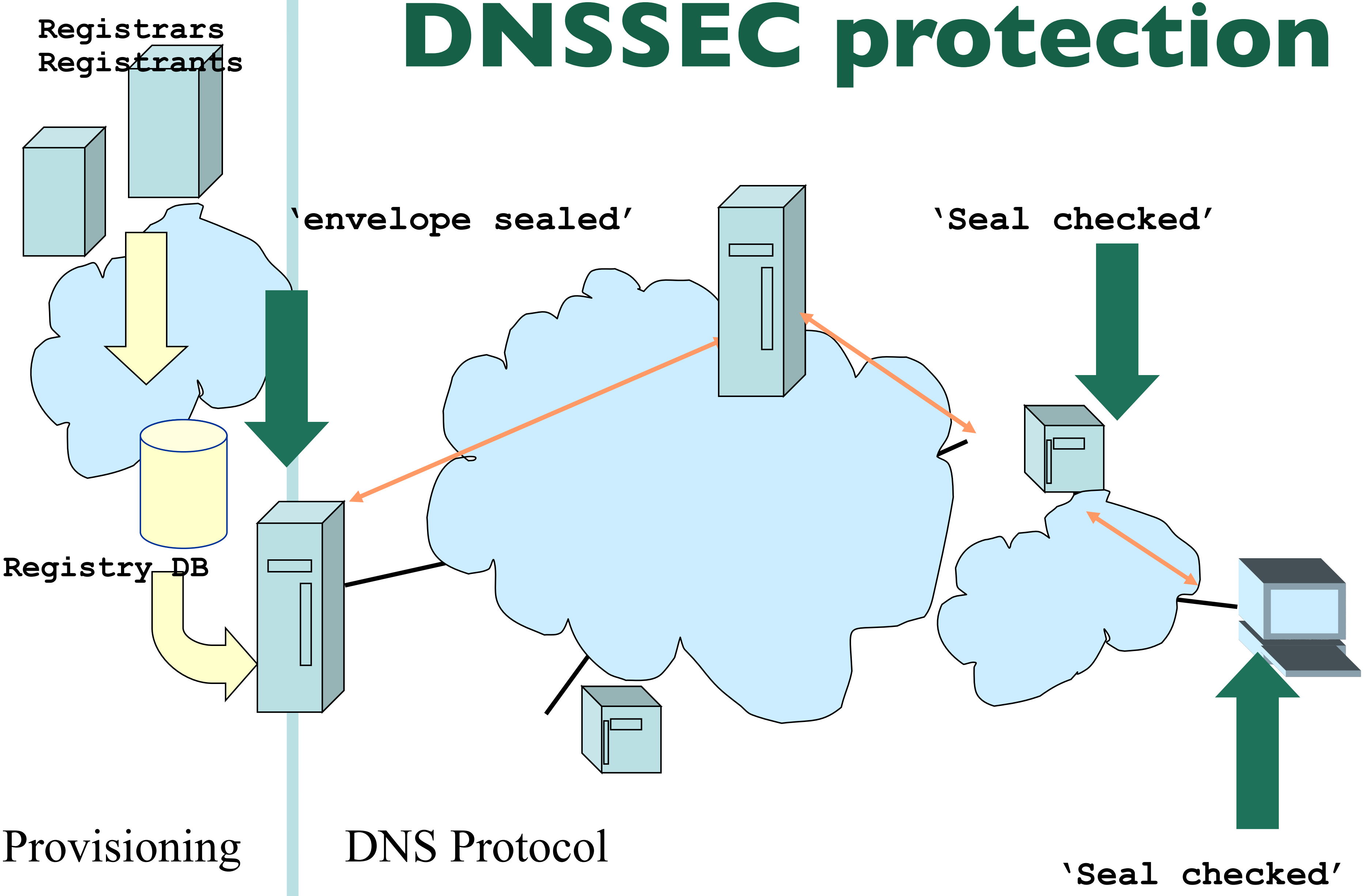
Authenticity and Integrity

- We want to check authenticity and integrity of DNS 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
  - use signatures to check both integrity and authenticity of data
  - Verify the authenticity of signatures

DNSSEC properties

- DNSSEC provides message authentication and integrity verification through cryptographic signatures
  - Authentic DNS source
  - No modifications between signing and validation
- It does not provide authorization
- It does not provide confidentiality

DNSSEC protection



Registrars
Registrants

'envelope sealed'

'Seal checked'

Registry DB

Provisioning

DNS Protocol

'Seal checked'

DNSSEC hypersummary

- Data authenticity and integrity by signing the Resource Records Sets with private key

- Public DNSKEYs used to verify the RRSIGs

- Children sign their zones with their private key
  - Authenticity of that key established by signature/checksum by the parent (DS)

- Ideal case: one public DNSKEY distributed

DNSSEC secondary benefits

- DNSSEC provides an “independent” trust path
  - The person administering “https” is most probably a different from person from the one that does “DNSSEC”
  - The chains of trust are most probably different
  - See acmqueue.org article: “Is Hierarchical Public-Key Certification the Next Target for Hackers?”

More benefits?

- With reasonable confidence perform opportunistic key exchanges
  - SSHFP and IPSECKEY Resource Records
- With DNSSEC one could use the DNS for a priori negotiation of security requirements.
  - "You can only access this service over a secure channel"

A signed zone

```
[...]

trstech.net.   86400 NS      ns.trstech.net.

trstech.net.   86400 NS      rip.psg.com.

trstech.net.   86400 RRSIG      NS 5 2 86400 20061227191027 (20061127191027 33888
        trstech.net.pVlziETr5b3RjBR86rHTdgrJVEkL9QfHoUoR3mepL5wGlH8leJpeZQNjQPZM/AMzcEtiDmIi2RXvpYLxTdBpdg
        == )

 [....]

trstech.net.   86400 DNSKEY 257 3 5
        ( AwEAAZrwNevGbMaT+yW9K+XlLk6WqN3F1heks/tfUCjAVWLKYHKtB5+2GdCC7QW4MA3dwAKbpqv+4NSg/6yLwQz
        BnF6gSRW3PhzIR53u8FdGF3yuYzTOd8HSL04otKZfmXAWnDSJfLY0WkZyycxB+tMWUWqEYWMhC5aZuTL7kHJndiz
        3) ; key id = 36472

[.....]

trstech.net.   86400          RRSIG      DNSKEY 5 2 86400 20061227191027 ( 20061127191027 33888 trstech.net.

J82iBTiEZOoheOMigH52SLtltXHij9jT12RIepZr9+EAeW/24wjJqvkicWLRN1DFYXTbK1V24F9NzkUh5TfeFw== )

[...]

trstech.net.   3600   NSEC       aalain.trstech.net. NS SOA MX RRSIG NSEC DNSKEY

trstech.net.   3600   RRSIG      NSEC 5 2 3600 20061227191027 (20061127191027 33888 trstech.net.

TE9+FGO2Yr5fwOu3/uXyW/Ub4M6YobJNkhhTWW835Ff2qmZrpraFLp5ZNAK200M901uY7XI20O8nvRDv8XXb9Q== )

[...]
```

Using the DNS to Distribute Keys

- Secured islands make key distribution problematic
- Distributing keys through DNS:
  - Use one trusted key to establish authenticity of other keys
  - Building chains of trust from the root down
  - Parents need to sign the keys of their children
- Only the root key needed in ideal world
  - Parents always delegate security to child
  - ... but it doesn't help to sign if your parent doesn't sign, or isn't signed itself...

Trust Anchors repositories

- Root is signed and receiving DS records from TLDs
  - www.root-dnssec.org
- Incremental deployment of DNSSEC with multiples isldans
- Use of Trust Anchors
  - *A DNS resource record store that contains SEP keys for one or more zones.*
- Two initiatives exist to provide these Trust Anchor Repositories.

  - for TLDs
  - for other domains

Trust Anchor Repositories... DLV

DLV: DNSSEC Lookaside Validation

- Alternative method for chain of trust creation and verification in a disjointed signed space (islands of trust)
- DLV functions automatically (if the resolver is configured to do so) by looking up in a preconfigured "lookaside validation" zone
  - no need to fetch a list of anchors
  - ISC Initiative: https://www.isc.org/solutions/dlv

Trust Anchor Repositories… ITAR(no longer used:root is signed)

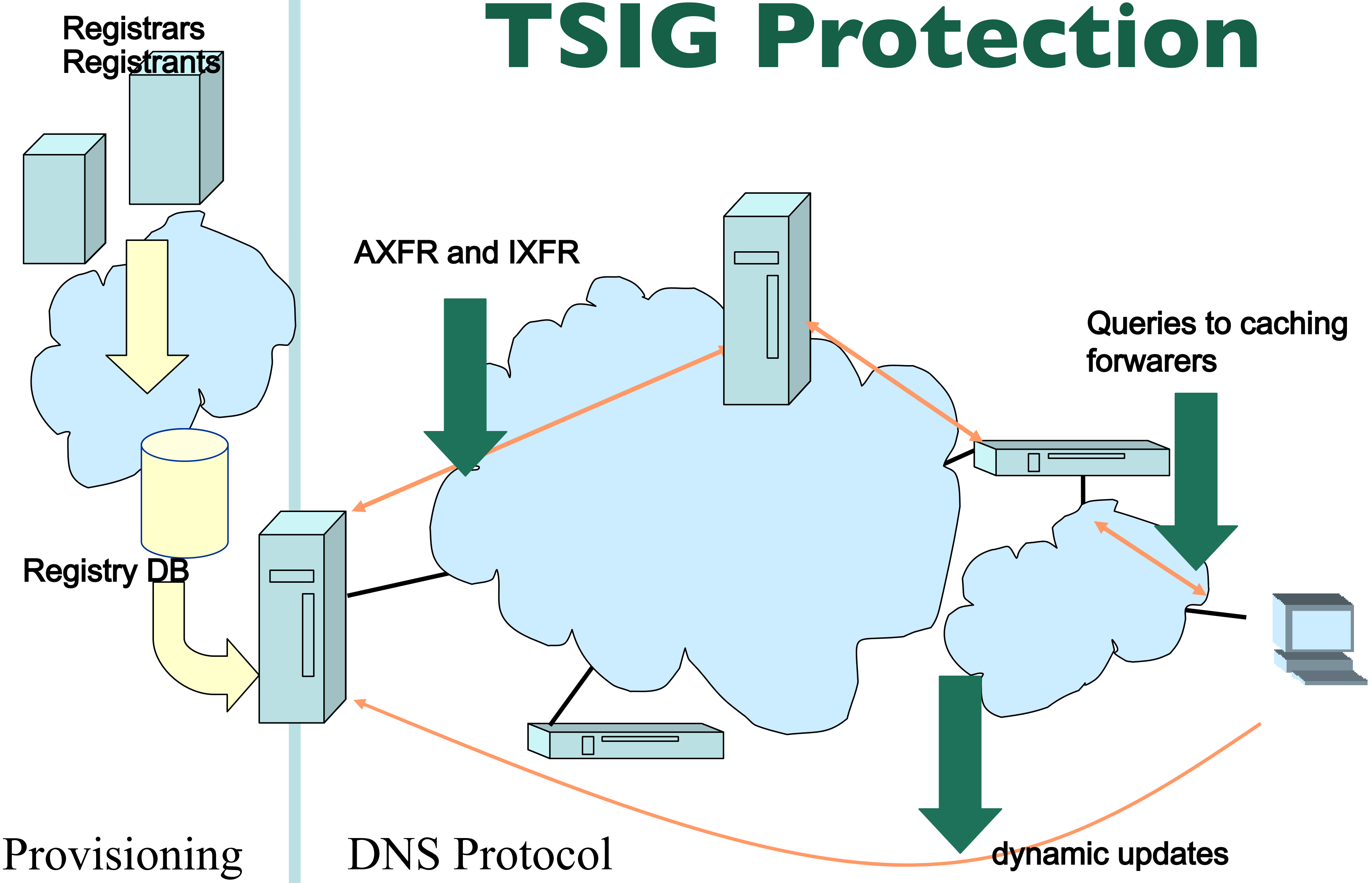
ITAR: Interim Trust Anchor Repositories

- Interim Trust Anchor Repository
- IANA Trust Anchor Repository (Until The Root Is Signed)
  - Is targeted at TLDs
  - Lookup is not automatic
    - list of anchors must be retrieved (one more operational constraint)
  - Already a beta program, several TLDs have already registered
  - https://itar.iana.org/

Other DNS security

- We talked about data protection
  - The sealed envelope technology
  - RRSIG, DNSKEY, NSEC and DS RRs
- There is also a transport security component
  - Useful for bilateral communication between machines
  - TSIG or SIG0

TSIG Protection



Transaction Signature: TSIG

- TSIG (RFC 2845)
  - Authorising dynamic updates and zone transfers
  - Authentication of caching forwarders
  - Independent from other features of DNSSEC
- One-way hash function
  - DNS question or answer and timestamp
- Traffic signed with "shared secret" key
- Used in configuration, **NOT** in zone file

TSIG for Zone Transfers

- Generate secret
- Communicate secret
- Configure servers
- Test

Importance of the Time Stamp

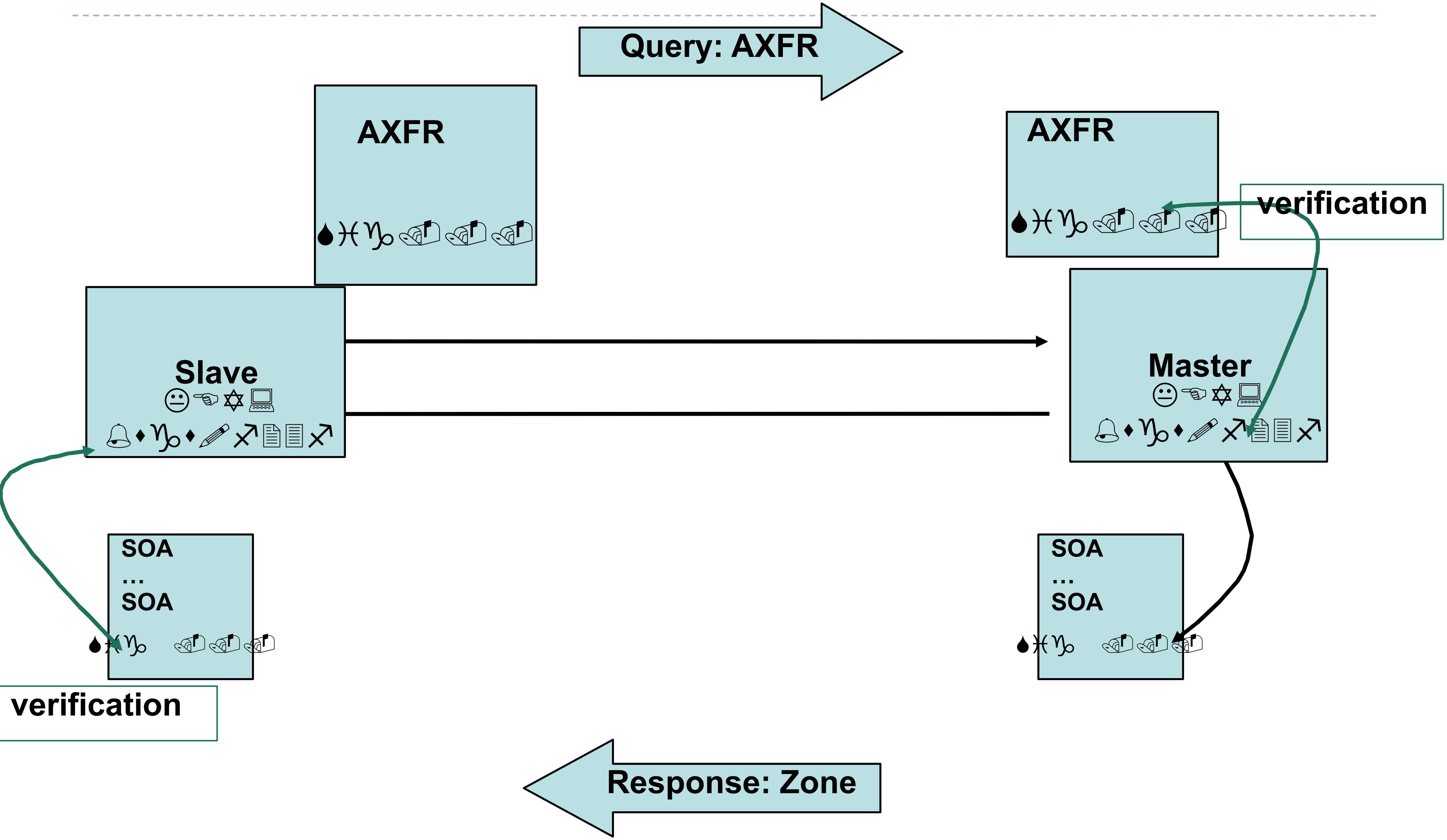
- TSIG/SIG(0) signs a complete DNS request / response with time stamp
  - To prevent replay attacks
  - Currently hardcoded at five minutes

- 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 synchronisation!

Authenticating Servers Using SIG(0)

- Alternatively, it is possible to use SIG(0)
  - Not yet widely used
  - Works well in dynamic update environment
- Public key algorithm
  - Authentication against a public key published in the DNS
- SIG(0) specified in RFC 2931

TSIG Example



Query: AXFR

AXFR

AXFR

verification

Slave

Master

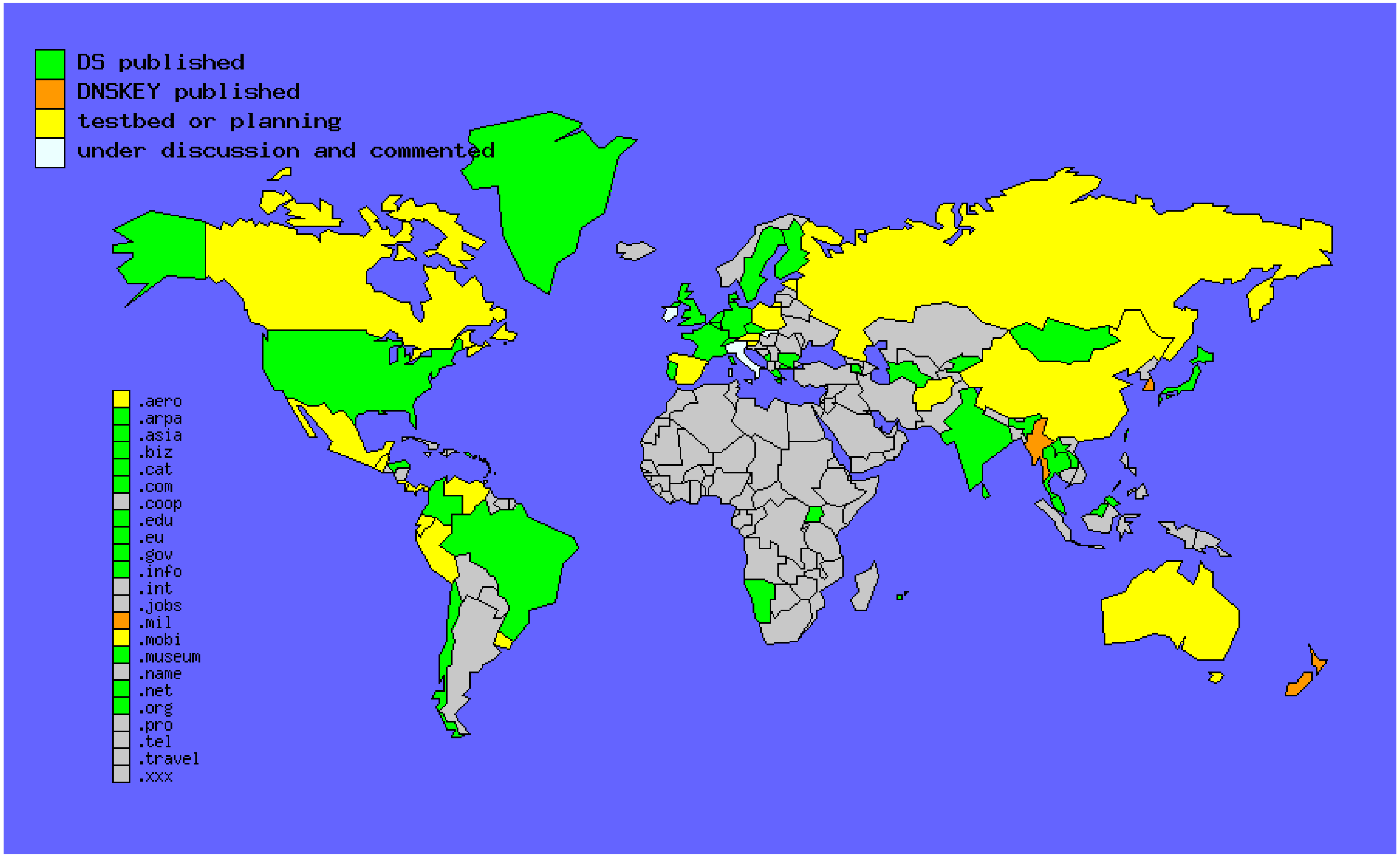
SOA
…
SOA

SOA
…
SOA

verification

Response: Zone

DNSSEC Adoption

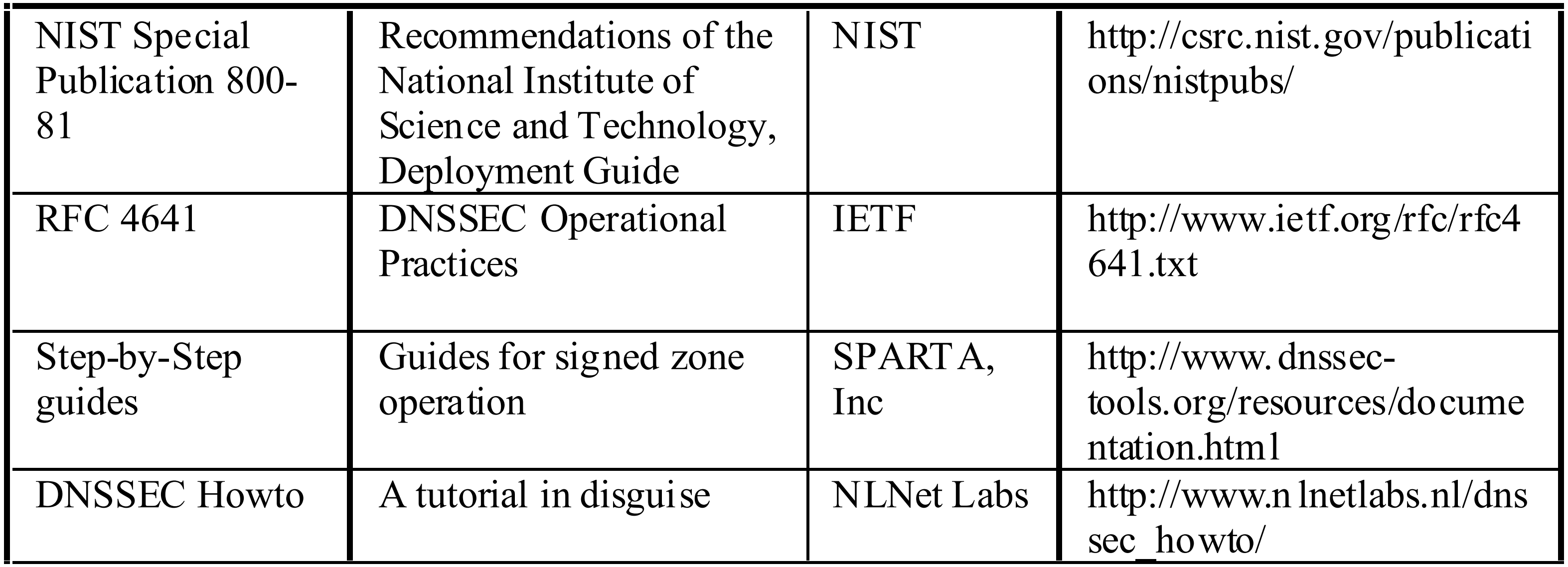


http://www.ohmo.to/dnssec/maps/ seen today

Testing Resources

maketestzone	useful for generating test data which DNSSEC aware software can be tested against	SPARTA, Inc	www.dnssec-tools.org
Querysim	A DNS traffic replay tool	NIST	http://snad.ncsl.nist.gov/dnssec/
Packet Server	A tool that helps crafting packets with various settings to test the behavior of validating resolvers	Roy Arends	http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/

Operator Guidance Documentation



NIST Special Publication 800-81	Recommendations of the National Institute of Science and Technology, Deployment Guide	NIST	http://csrc.nist.gov/publications/nistpubs/
RFC 4641	DNSSEC Operational Practices	IETF	http://www.ietf.org/rfc/rfc4641.txt
Step-by-Step guides	Guides for signed zone operation	SPARTA, Inc	http://www.dnssec-tools.org/resources/documentation.html
DNSSEC Howto	A tutorial in disguise	NLNet Labs	http://www.nlnetlabs.nl/dnssec_howto/

RFC4641bis http://tools.ietf.org/wg/dnsop/draft-ietf-dnsop-rfc4641bis/

Resources

www.dnssec-deployment.org

Includes monthly newsletter, DNSSEC This Month

DNSSEC Deployment Mailing list

dnssec-deployment-subscribe@shinkuro.com

www.dnssec-tools.org/

www.dnssec.net/

www.isc.org

Internet Systems Consortium – BIND, DLV

www.nlnetlabs.nl

NLnet Labs – NSD, Unbound

www.opendnsssec.org

DNS visualization tool (http://dnsviz.net/)

Questions?

ASK