DNSSEC: Why and How

DNSSEC Tutorial

AfNOG XI
Kigali, 30/05/2010

aalain@trstech.net

The Material

- Based on material I used with Olaf KOLKMAN for many DNSSEC workshops and tutorials
- We also borrowed heavily from other sources
  - Organizations and individuals
- They are acknowledged for allowing me to re-use this material

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

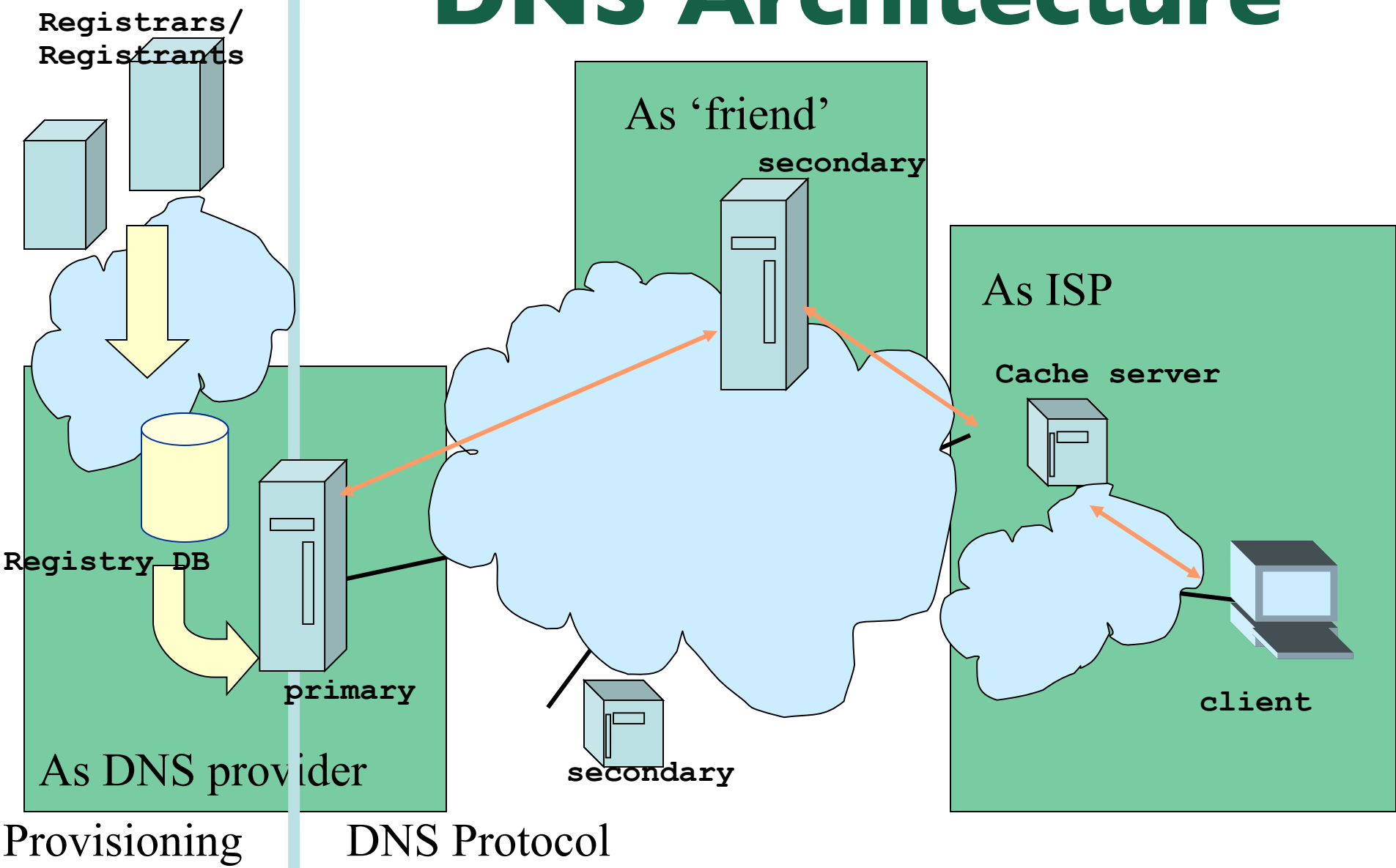
The Problem(cont'd)

- 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

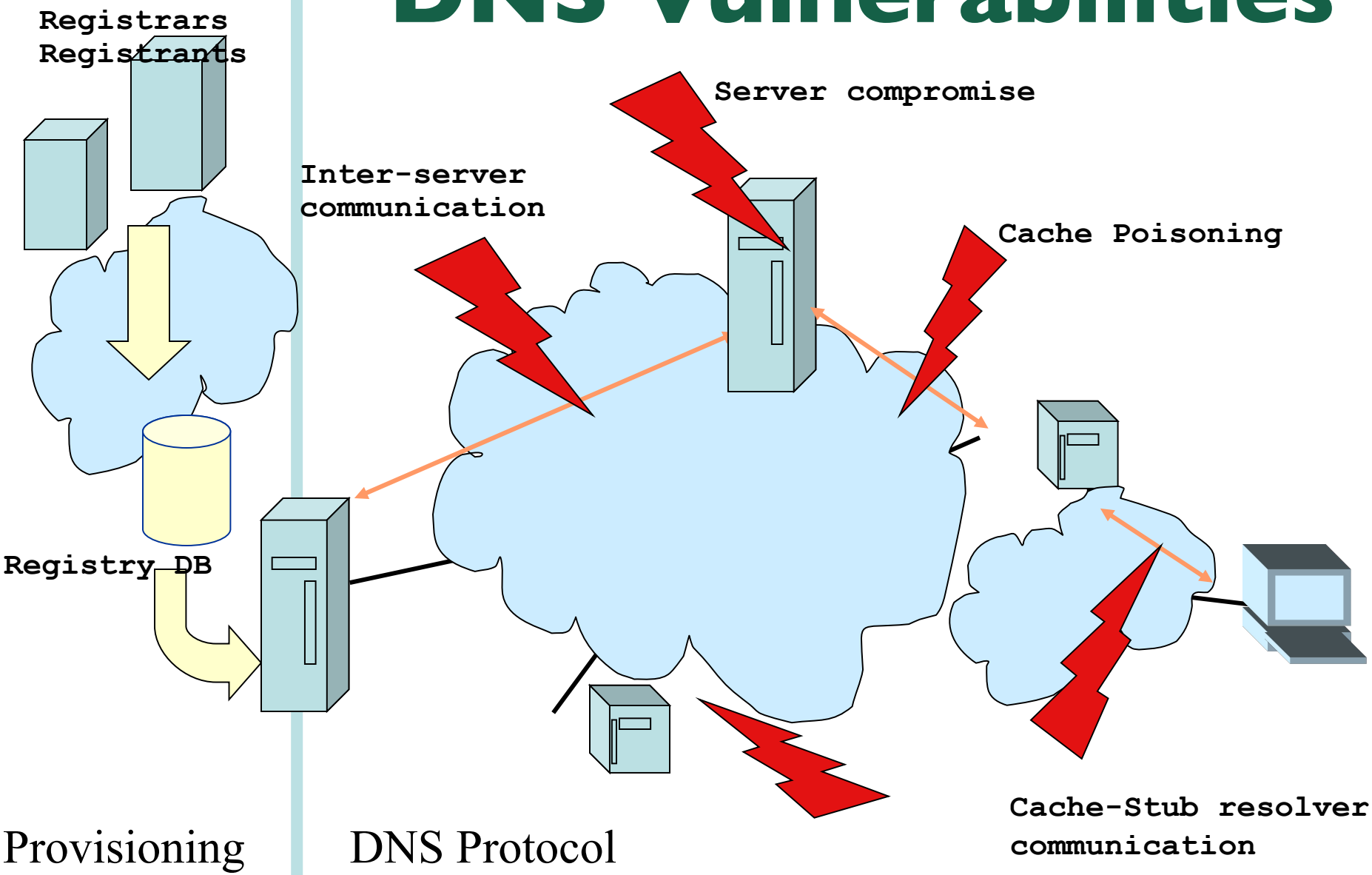
      http://www.kb.cert.org/vuls/id/800113
  - The Solution ????
    - DNSSEC

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

DNS Architecture



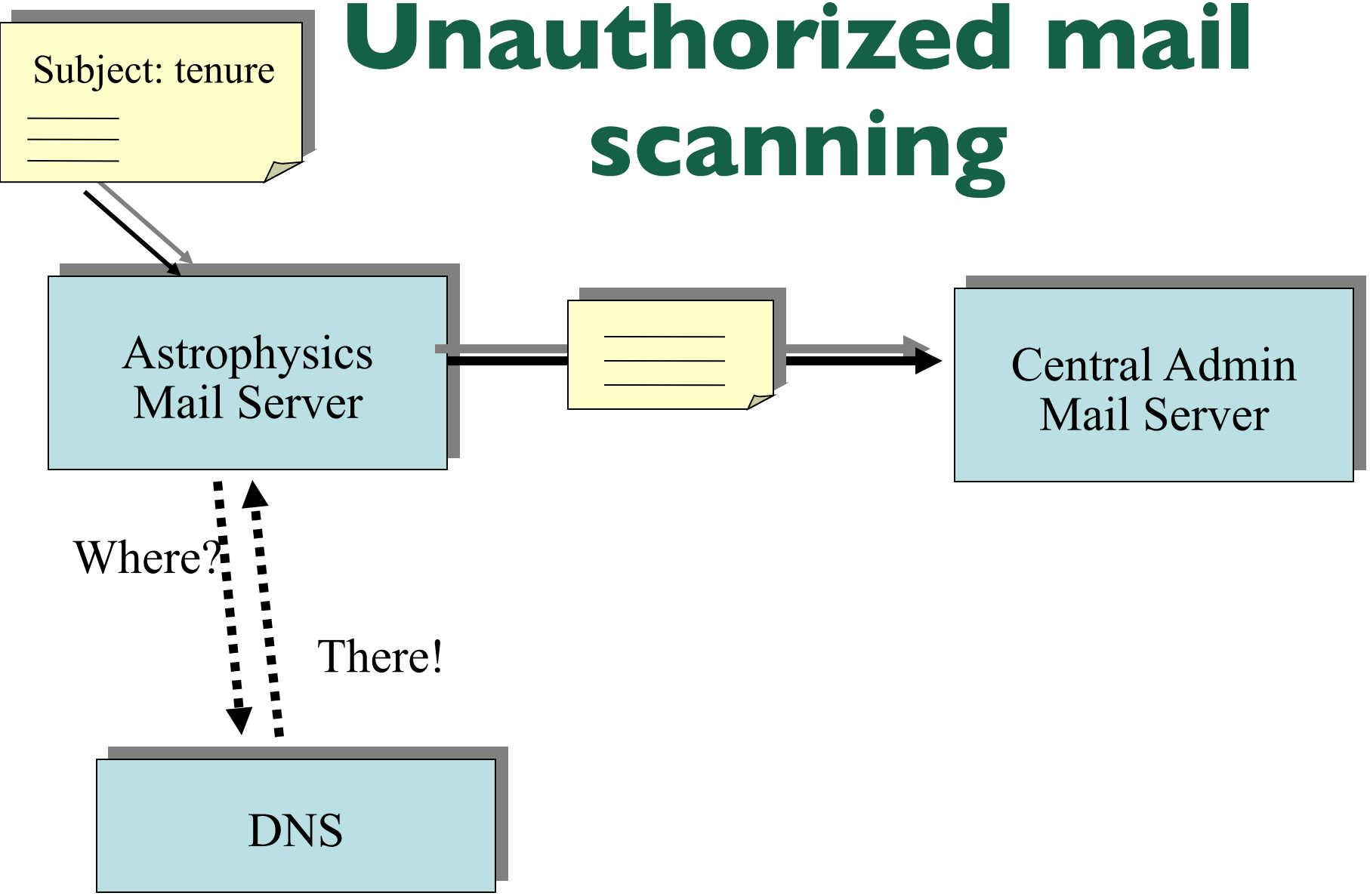
DNS Vulnerabilities



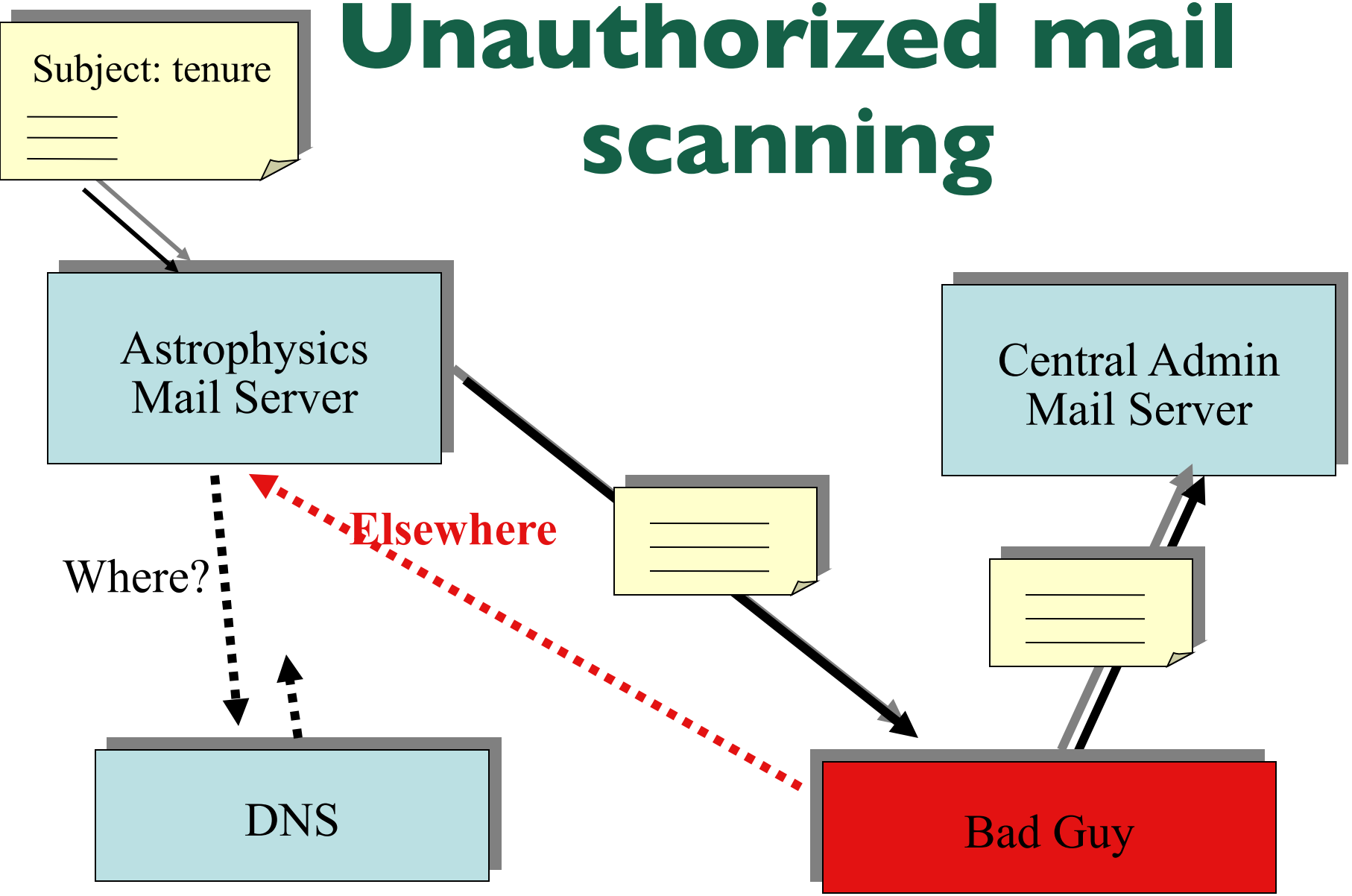
Provisioning

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.

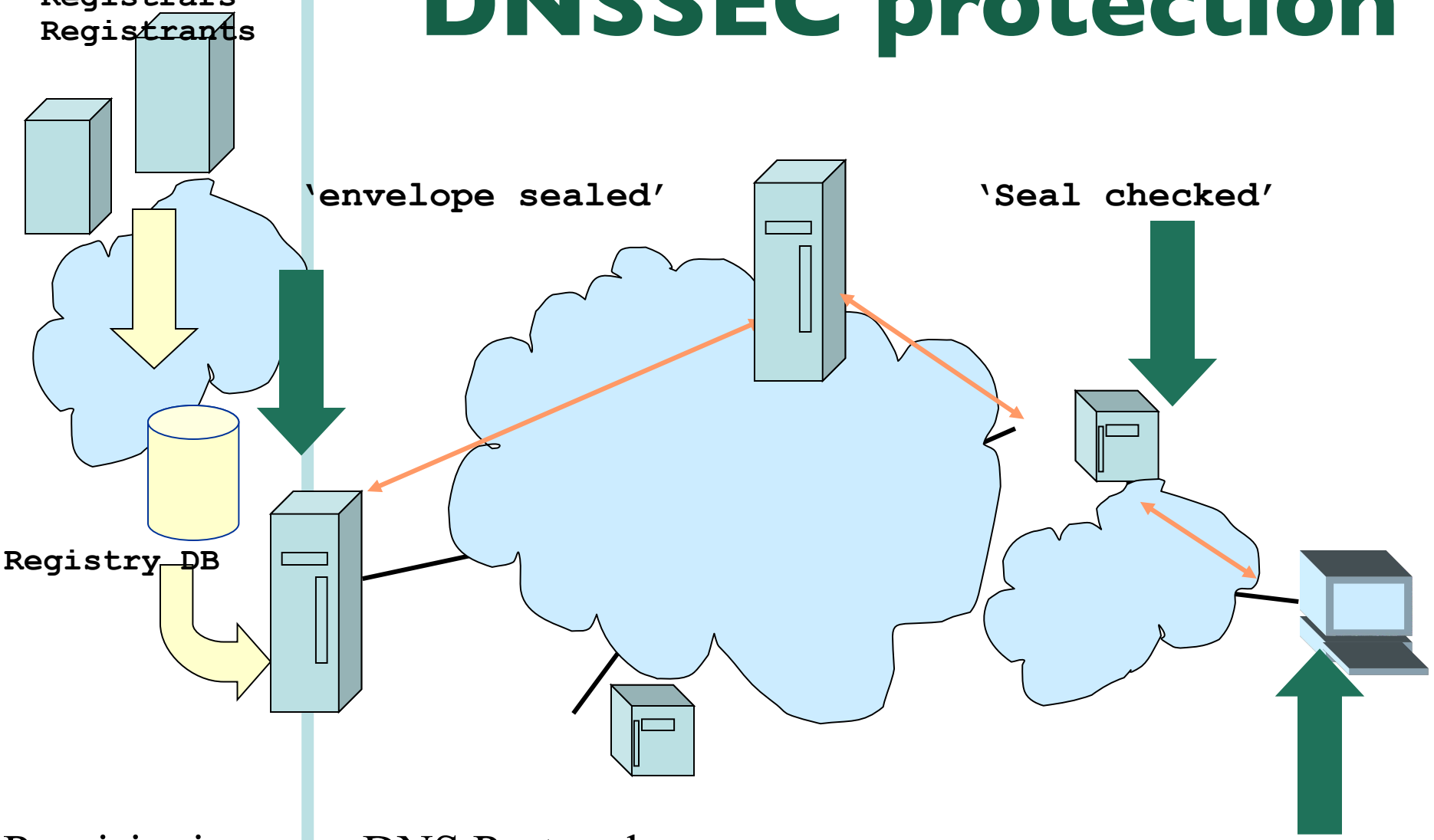
Authenticity and Integrity

- 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



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.PVLZIETR5B3RJBR86RHTDGRJVEKL9QFHOUOR3MEPL5WGLH8LEJPEZQNJQPZMXAMZCETTDMII2RXVPYLXTDBPDG
==)

[....]

TRSTECH.NET. 86400 **DNSKEY** 257 3 5
(AWEAAZRWNEVGBMAT+YW9K+XLLK6WQN3F1HEKS/TFUCJAVWLKYHKTB5+2GDCC7QW4MA3DWAKBPQV+4NSG/6YLWQZ
BNF6GSRW3PHZIR53U8FDGF3YUYZTOD8HSLO4OTKZFMXAWNDSJFLYOWKZYYCXB+TMWUWQEYWMHC5AZUTL7KHJNDIZ
3) ; KEY ID = 36472

[.....]

TRSTECH.NET. 86400 **RRSIG** DNSKEY 5 2 86400 20061227191027 (20061127191027 33888 TRSTECH.NET.
J82IBTIEZOOHEOMIGH52SLTTIXHIJ9JT12RIEPZR9+EAEW/24WJQVKICWLRN1DFYXTBK1V24F9NZKUH5TFEFW==)

[...]

TRSTECH.NET. 3600 **NSEC** AALAIN.TRSTECH.NET. NS SOA MX RRSIG NSEC DNSKEY

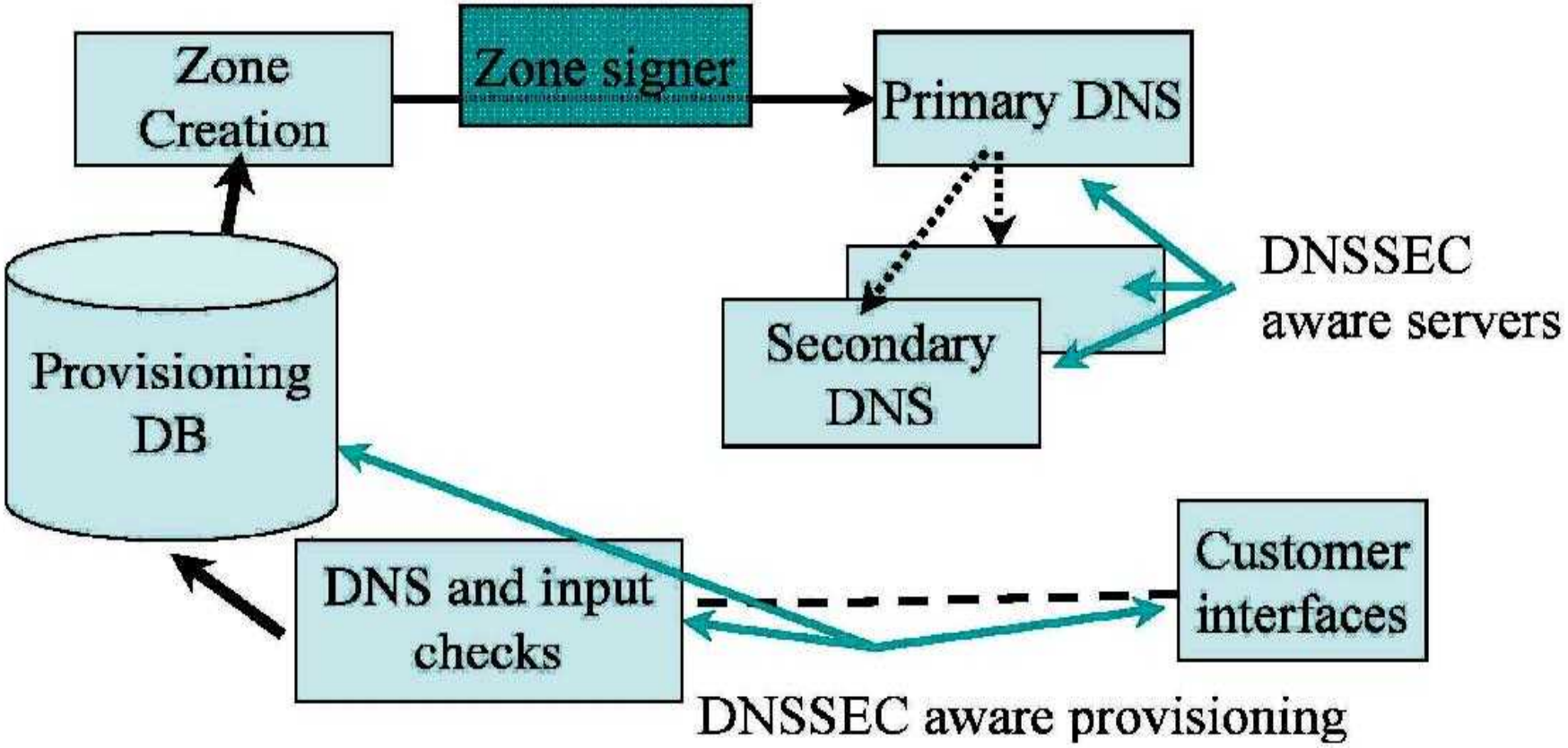
TRSTECH.NET. 3600 **RRSIG** NSEC 5 2 3600 20061227191027 (20061127191027 33888 TRSTECH.NET.
TE9+FGO2YR5FWOU3/UXYW/UB4M6YOBJNKHHTWW835FF2QMZRPRAFLP5ZNAK200M901UY7XI200O8NVRDV8XXB9Q==)

[...]

DNSSEC Deployment Tasks

- **Key maintenance policies and tools**
- Private key use and protection
- Public key distribution
- **Zone signing and integration into the provisioning chain**
- **DNS server infrastructure**
- **Secure delegation registry changes**
- **Interfacing with customers**

DNSSEC Architecture modification



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

- Works ongoing to sign the root
  - 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 and ITAR

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... DLV and ITAR

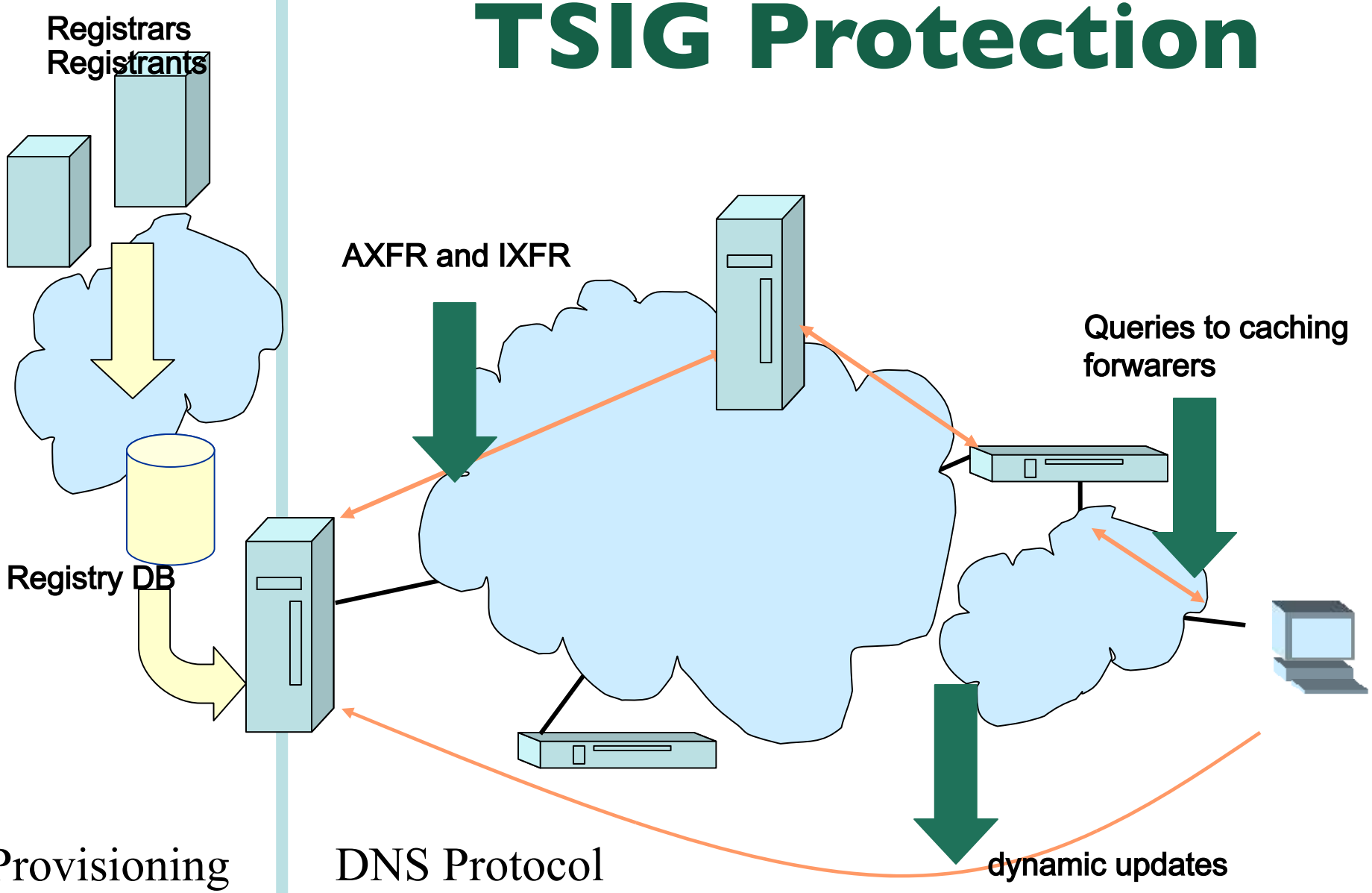
ITAR: Interim Trust Anchor Repositories

- 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



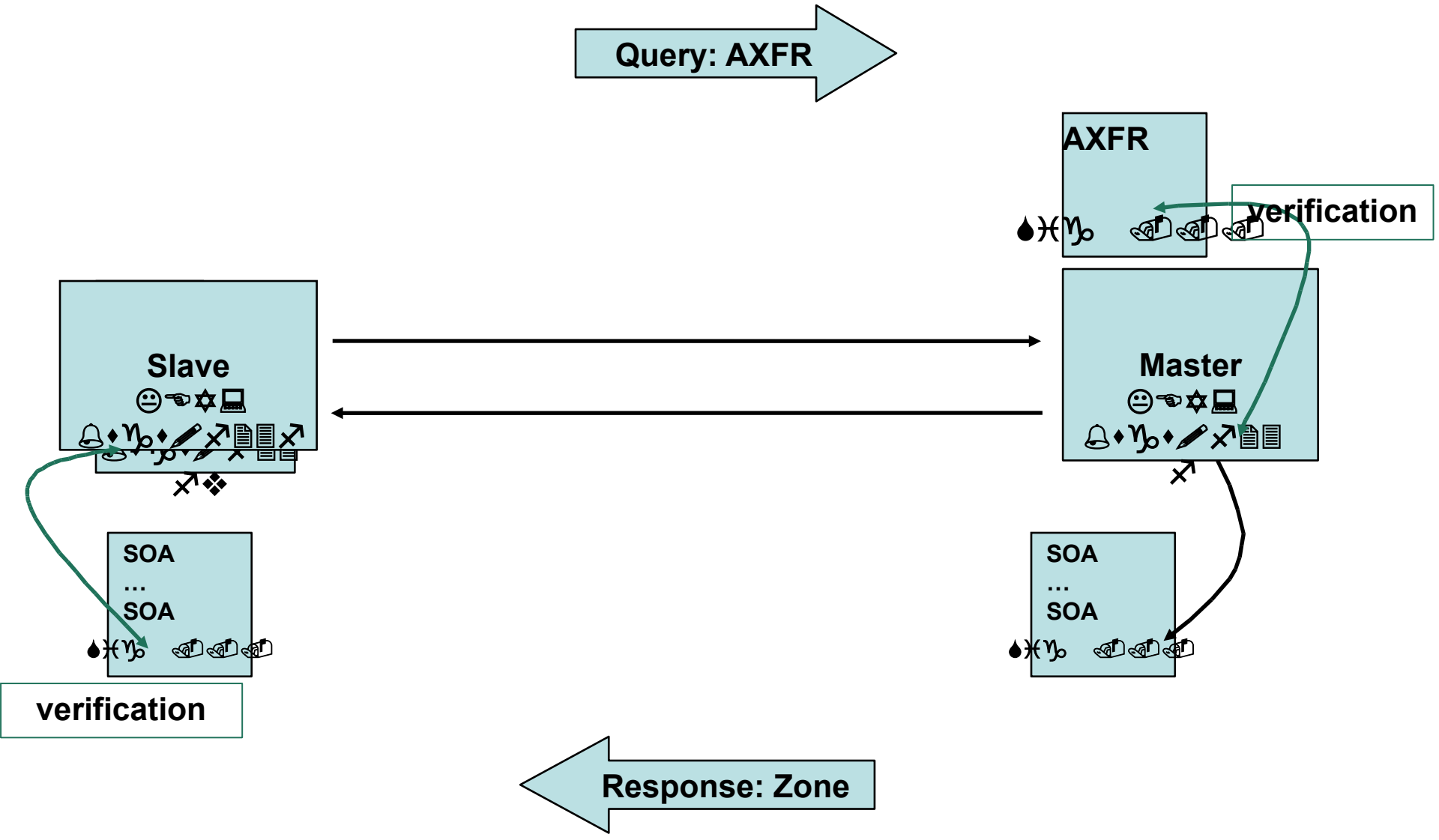
Provisioning

DNS Protocol

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 Example



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

DNSSEC Adoption

http://www.xelerance.com/dnssec

Categories of Tools

Taking full advantage of DNSSEC capabilities will occur gradually over time

Adding DNSSEC capabilities to various DNS related functions will occur gradually

Large number of open source tools available

- Existing tools continue to evolve
- New tools and capabilities continue to appear

Available Resources

- Various categories of resources are available

Resources for Zone Administration

Resources for Creating Secure Delegations

Resources for Validating

Applications Related Capabilities

Developer and Usage Guides

- Some of the available tools are catalogued at https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources

Existing tools have broad coverage

Some gaps remain

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?

DNSSEC in detail

Stay with us if you want to learn about how it works

What we just had is a summary of what it is