DNSSEC for Everybody: A Beginner's Guide

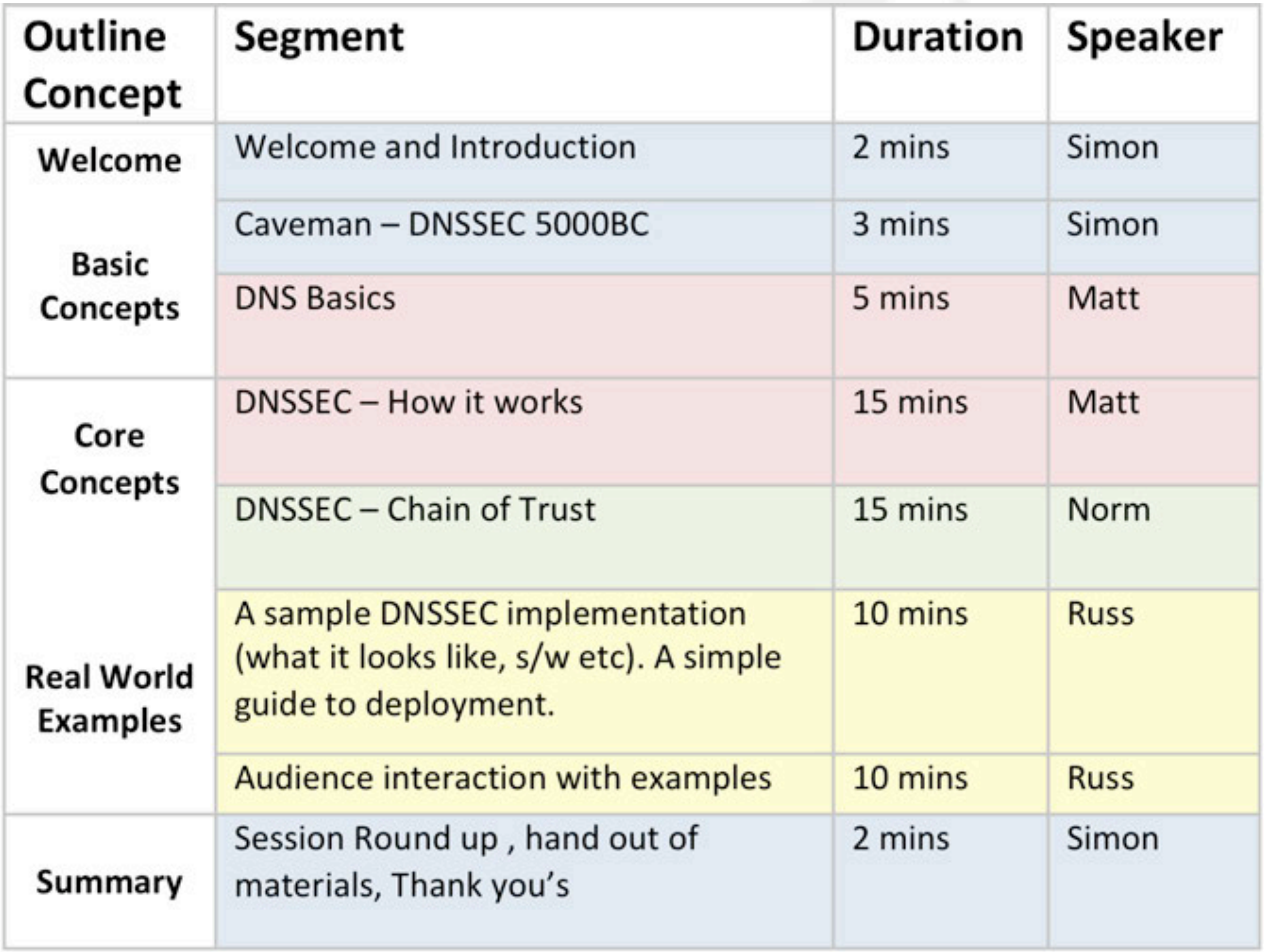
San Francisco, California

14 March 2011

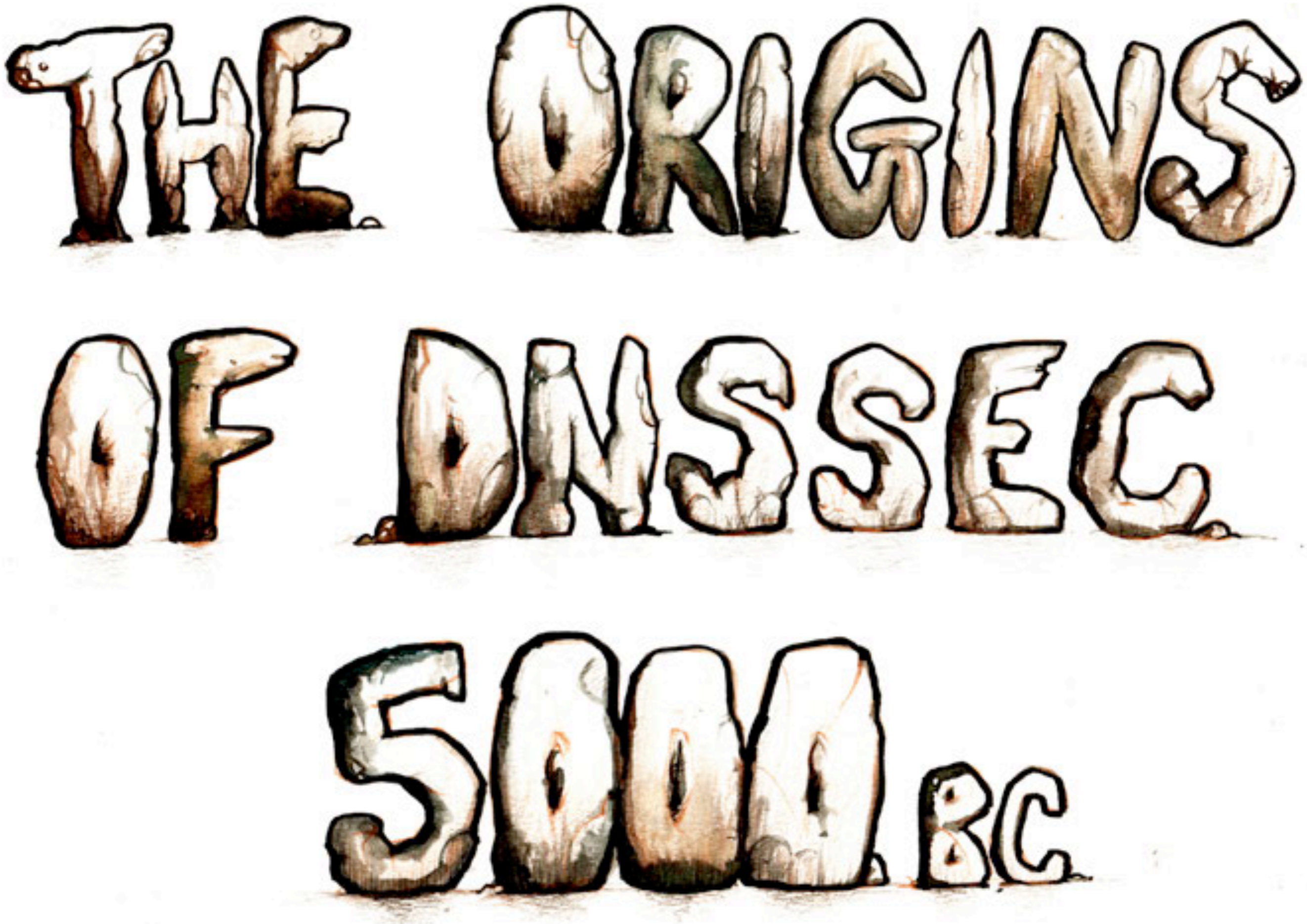
4:00 to 5:00 p.m.

Colonial Room

The Schedule

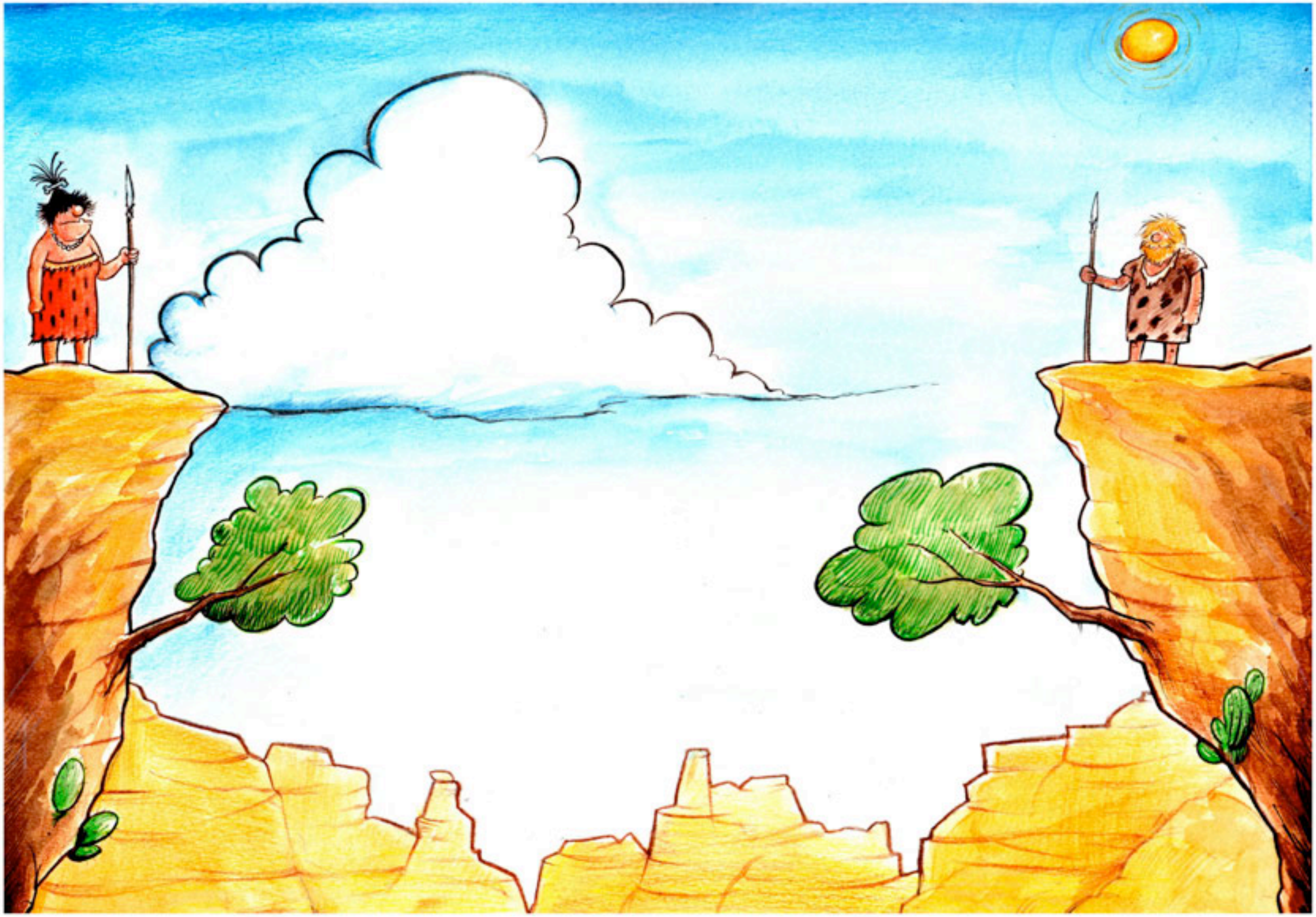


Outline Concept	Segment	Duration	Speaker
Welcome	Welcome and Introduction	2 mins	Simon
Basic Concepts	Caveman – DNSSEC 5000BC	3 mins	Simon
	DNS Basics	5 mins	Matt
Core Concepts	DNSSEC – How it works	15 mins	Matt
	DNSSEC – Chain of Trust	15 mins	Norm
Real World Examples	A sample DNSSEC implementation (what it looks like, s/w etc). A simple guide to deployment.	10 mins	Russ
	Audience interaction with examples	10 mins	Russ
Summary	Session Round up , hand out of materials, Thank you's	2 mins	Simon

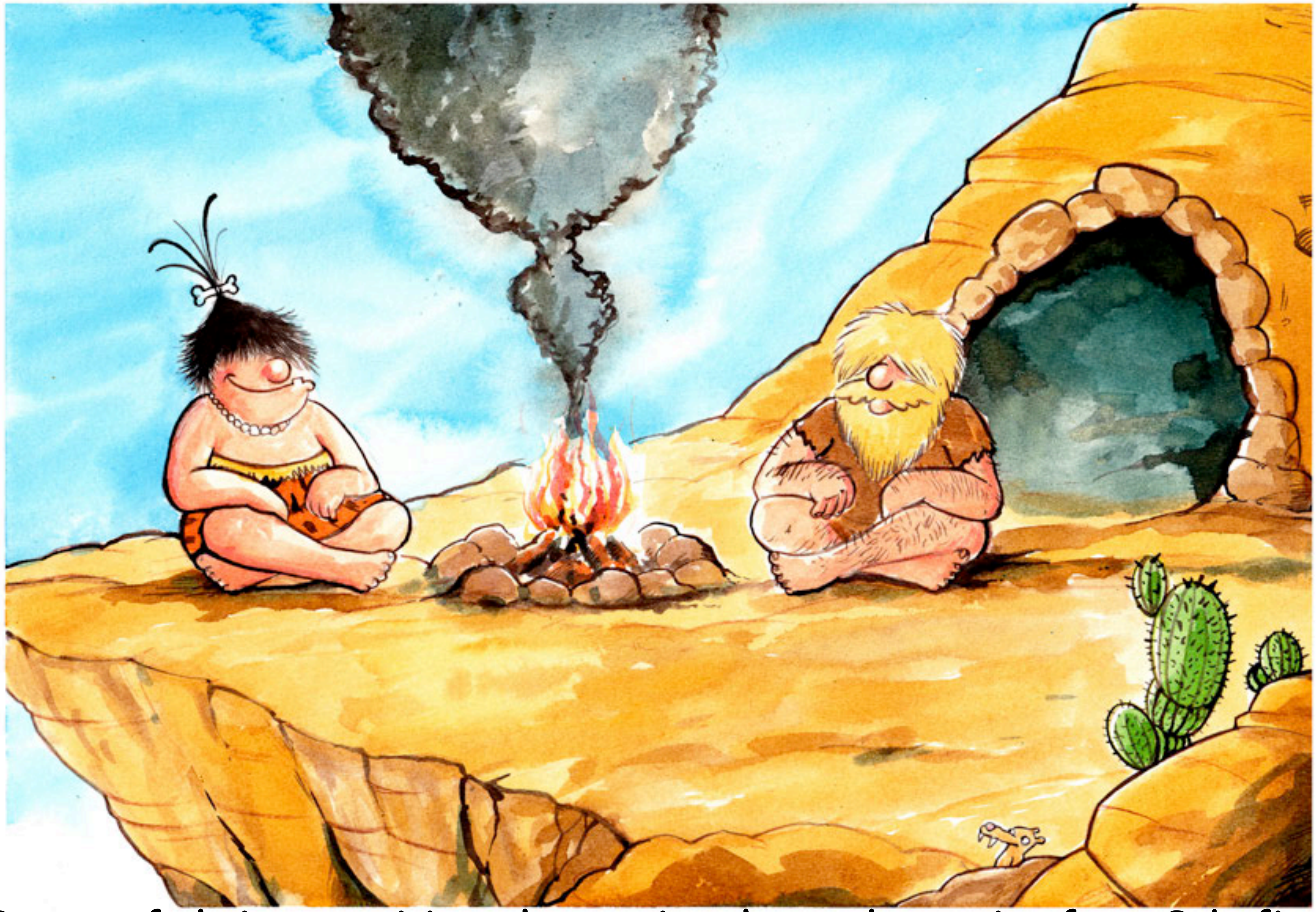

THE ORIGINS
OF DNSSEC
5000 BC

This is Ugwina. She lives in a cave on the edge of the Grand Canyon...

This is Og. He lives in a cave on the other side of the Grand Canyon...



It's a long way down and a long way round. Ugwina and Og don't get to talk much...



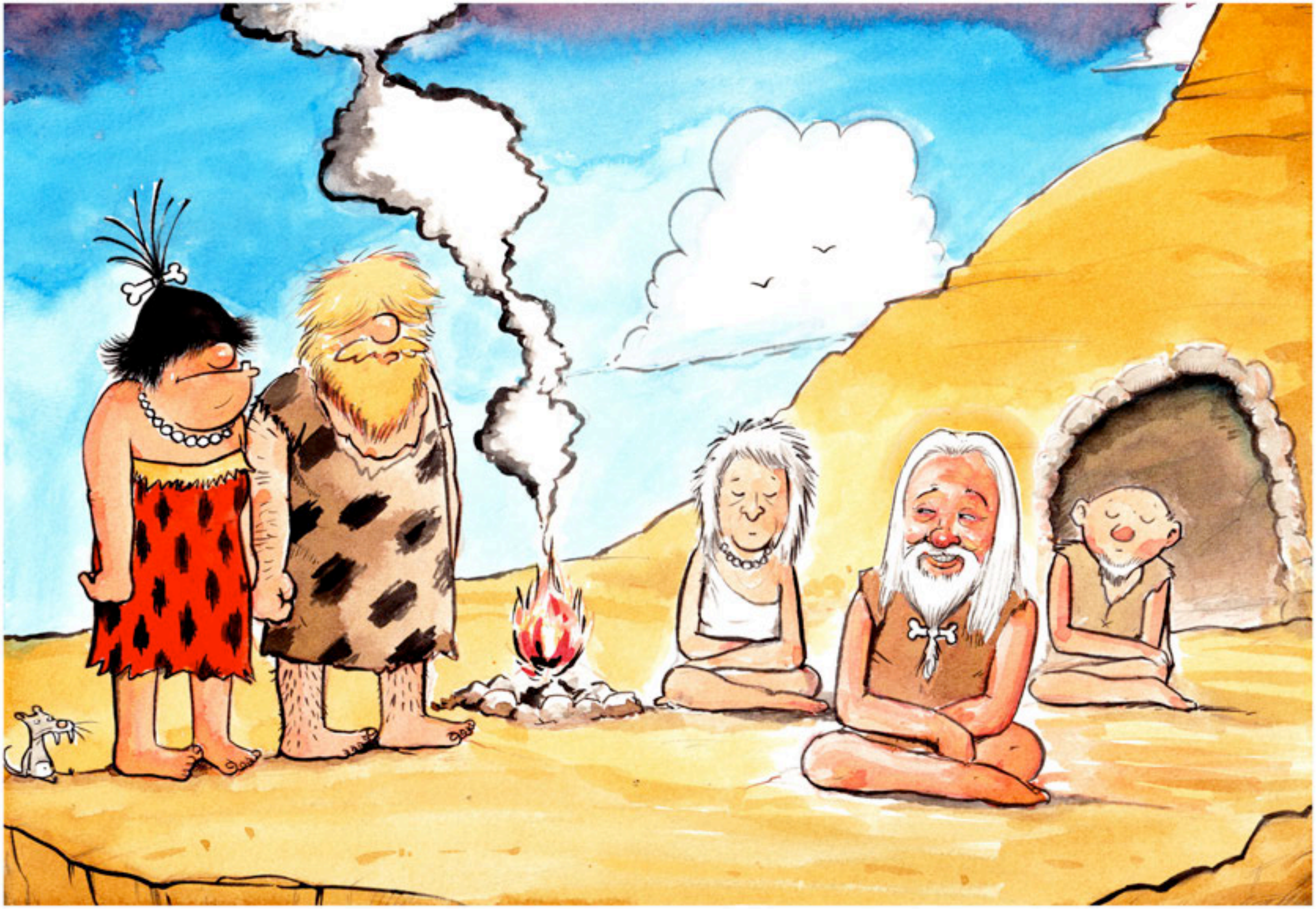
On one of their rare visits, they notice the smoke coming from Og's fire

...and soon they are chatting regularly using smoke signals

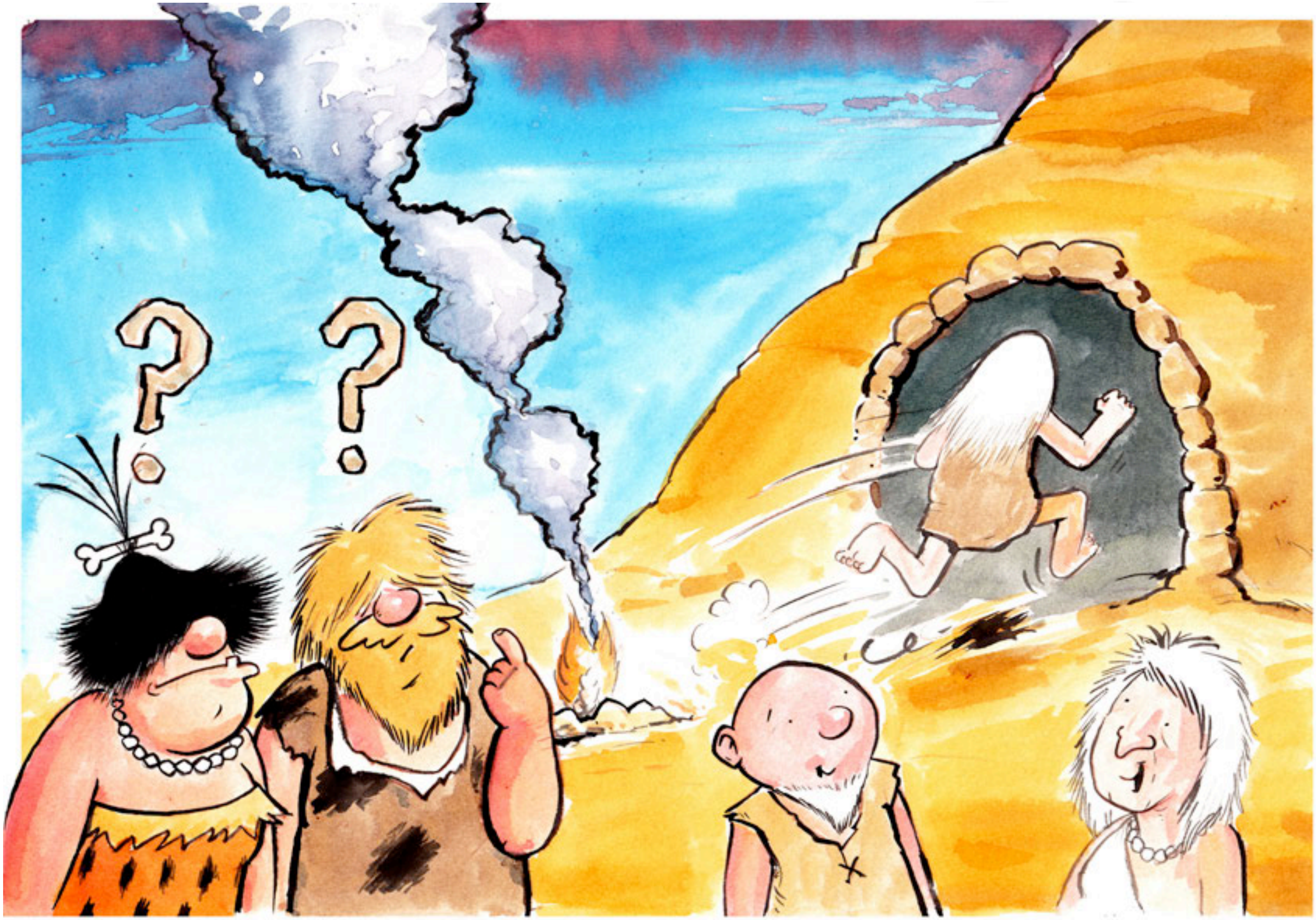
until one day, mischievous caveman Kaminsky moves in next door to Ug and starts sending smoke signals too...

Now Ugwina is really confused. She doesn't know which smoke to believe...

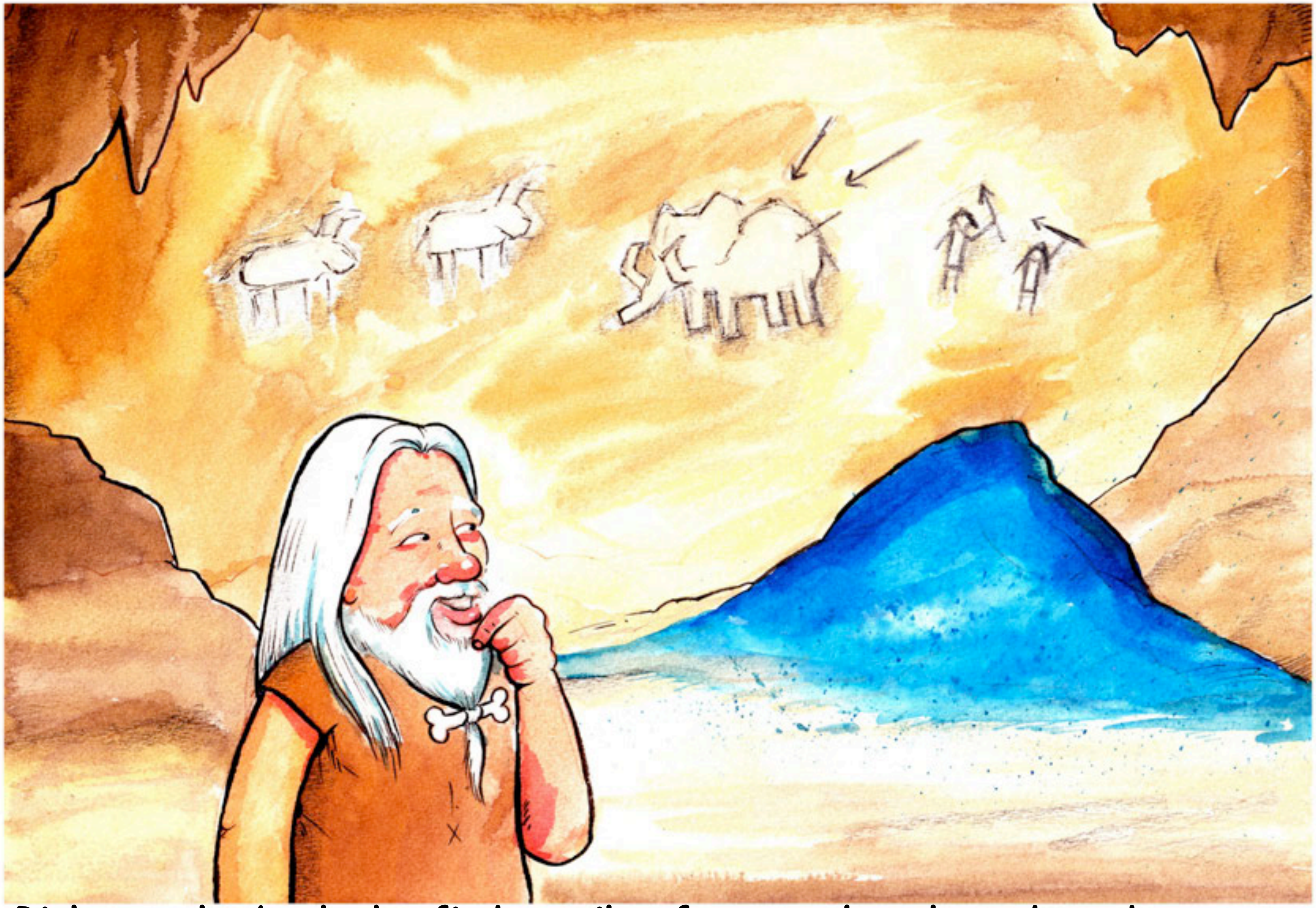
So Ugwina sets off down the canyon to try and sort out the mess...



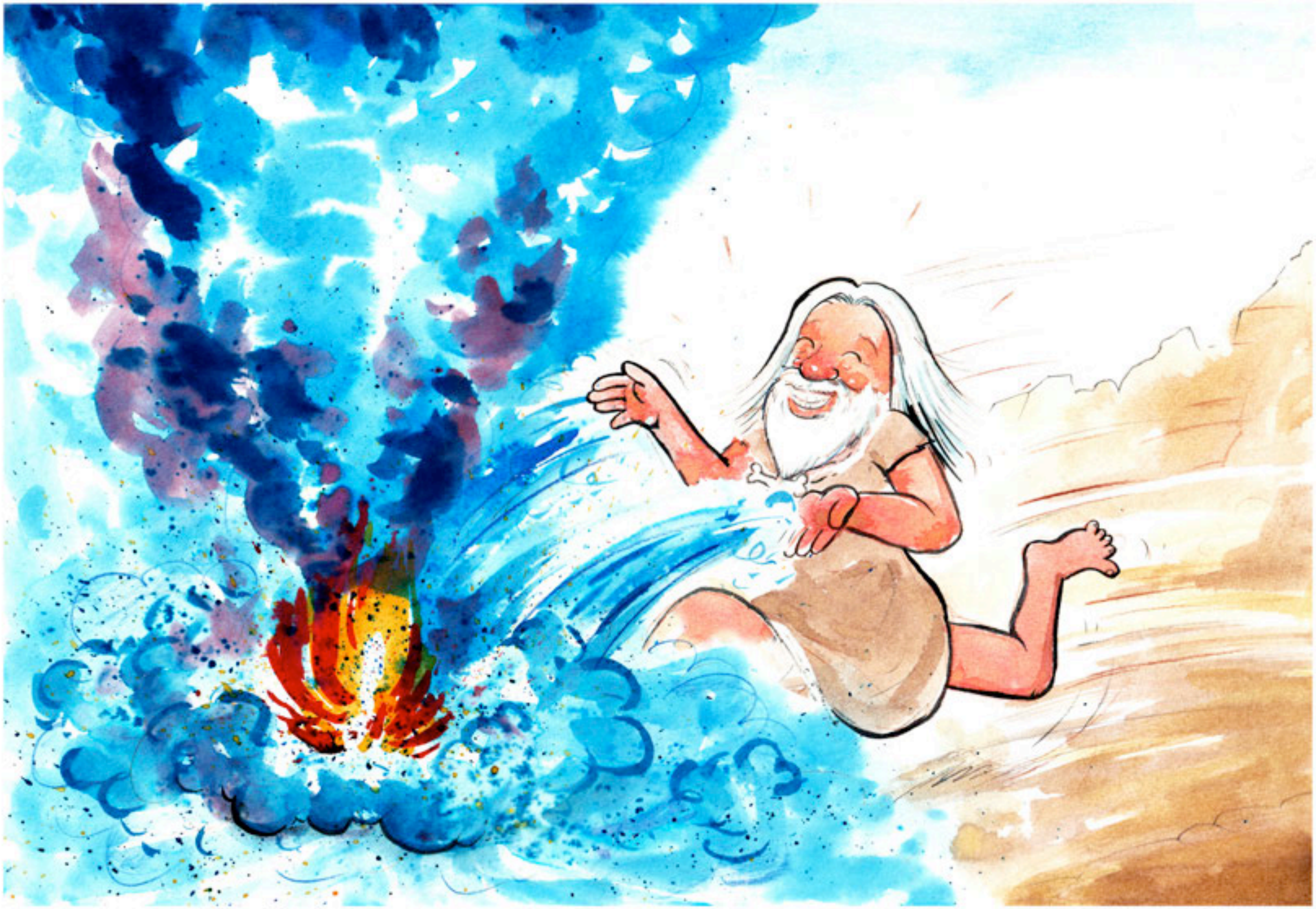
Ugwina and Og consult the wise village elders. Caveman Diffie thinks that he might have a cunning idea...



And in a flash, jumps up and runs into Ug's cave...!



Right at the back, he finds a pile of strangely coloured sand that has only ever been found in Ug's cave...



And with a skip, he rushes out and throws some of the sand onto the fire. The smoke turns a magnificent blue...

Now Ugwina and Og can chat happily again, safe in the knowledge that nobody can interfere with their conversation…

ICANN

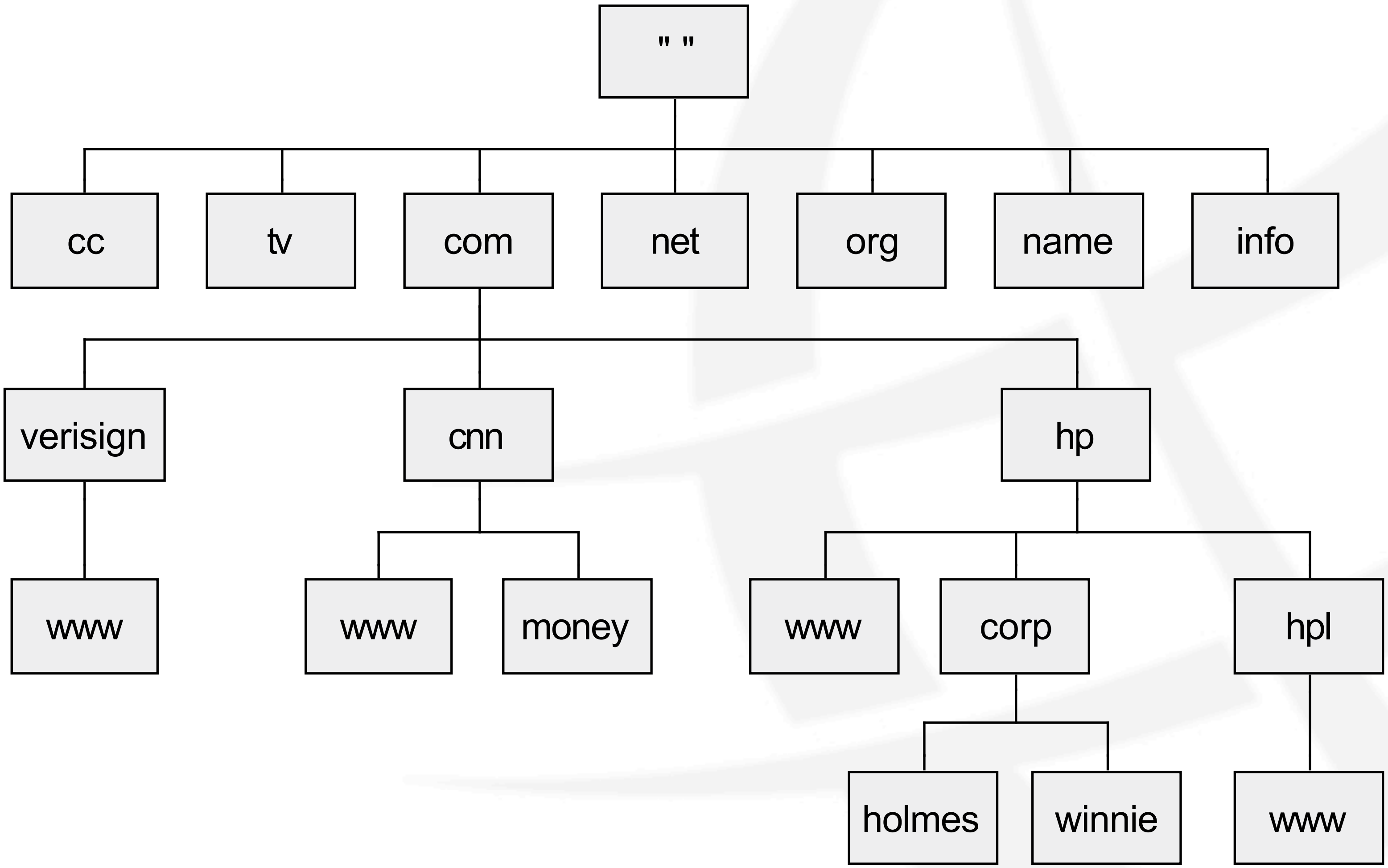
DNSSEC Basics and How it Works

Matt Larson, VeriSign

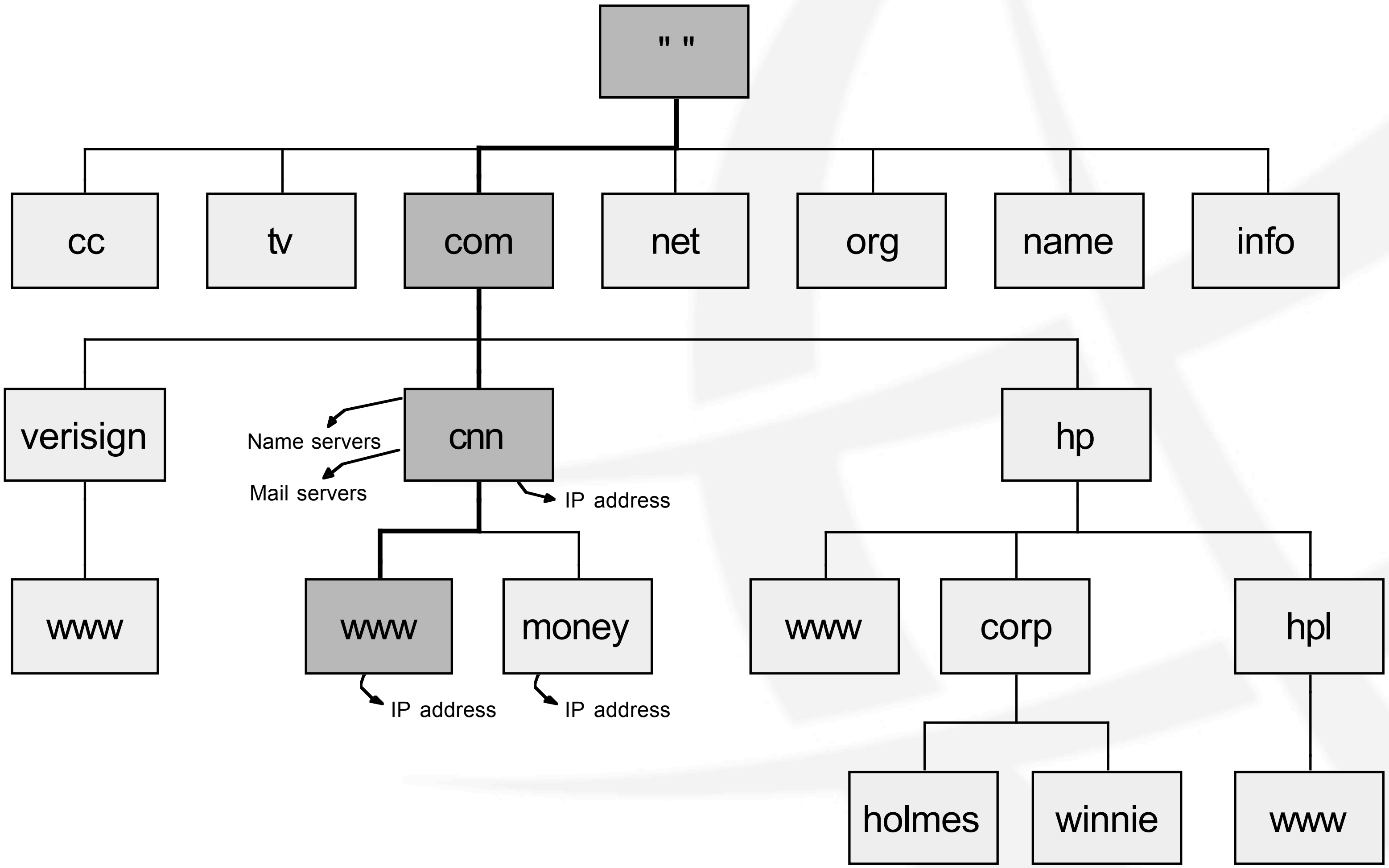
in San Francisco ▪ 13-18 March 2011

ICANN SILICON VALLEY Meeting

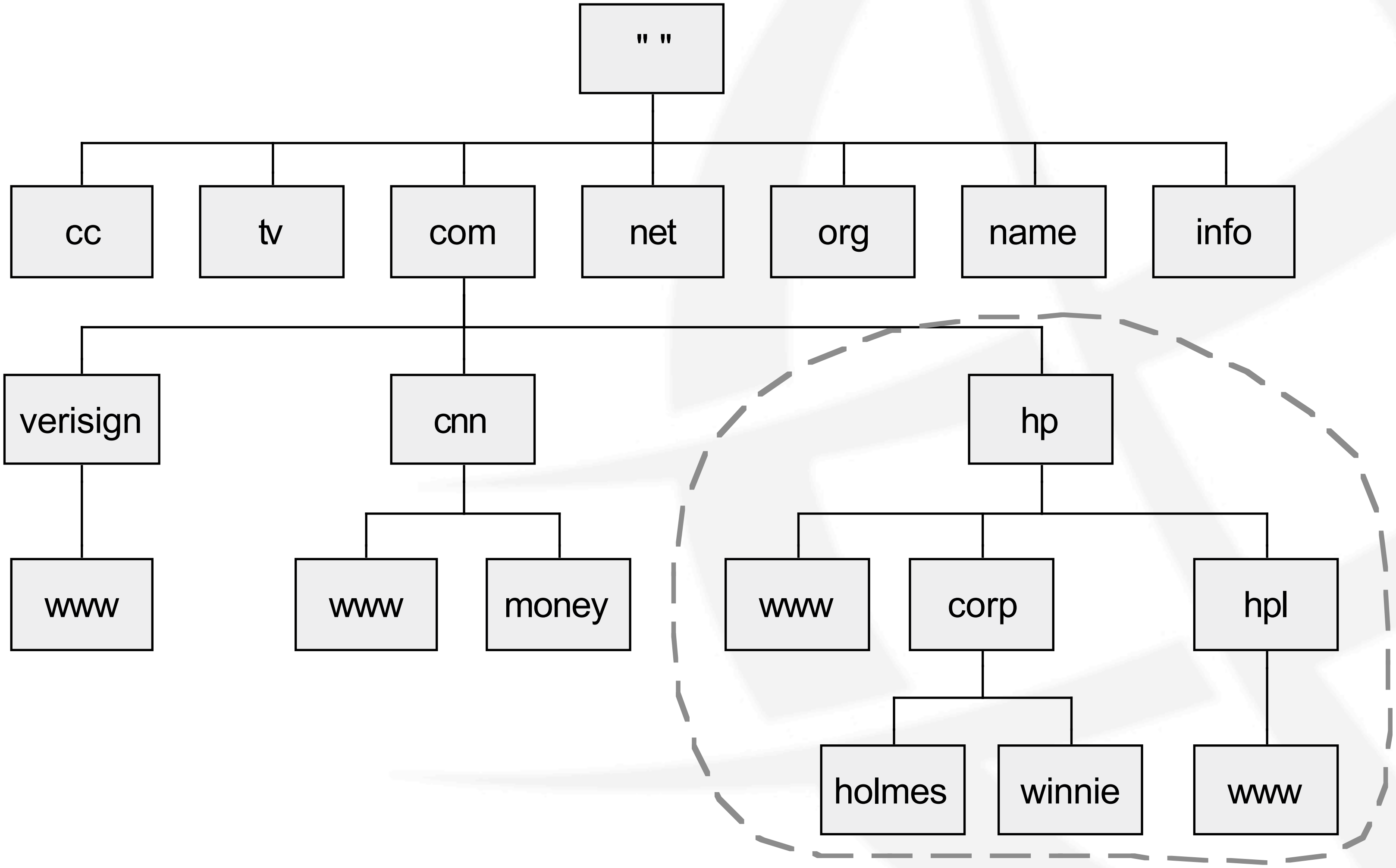
The Name Space



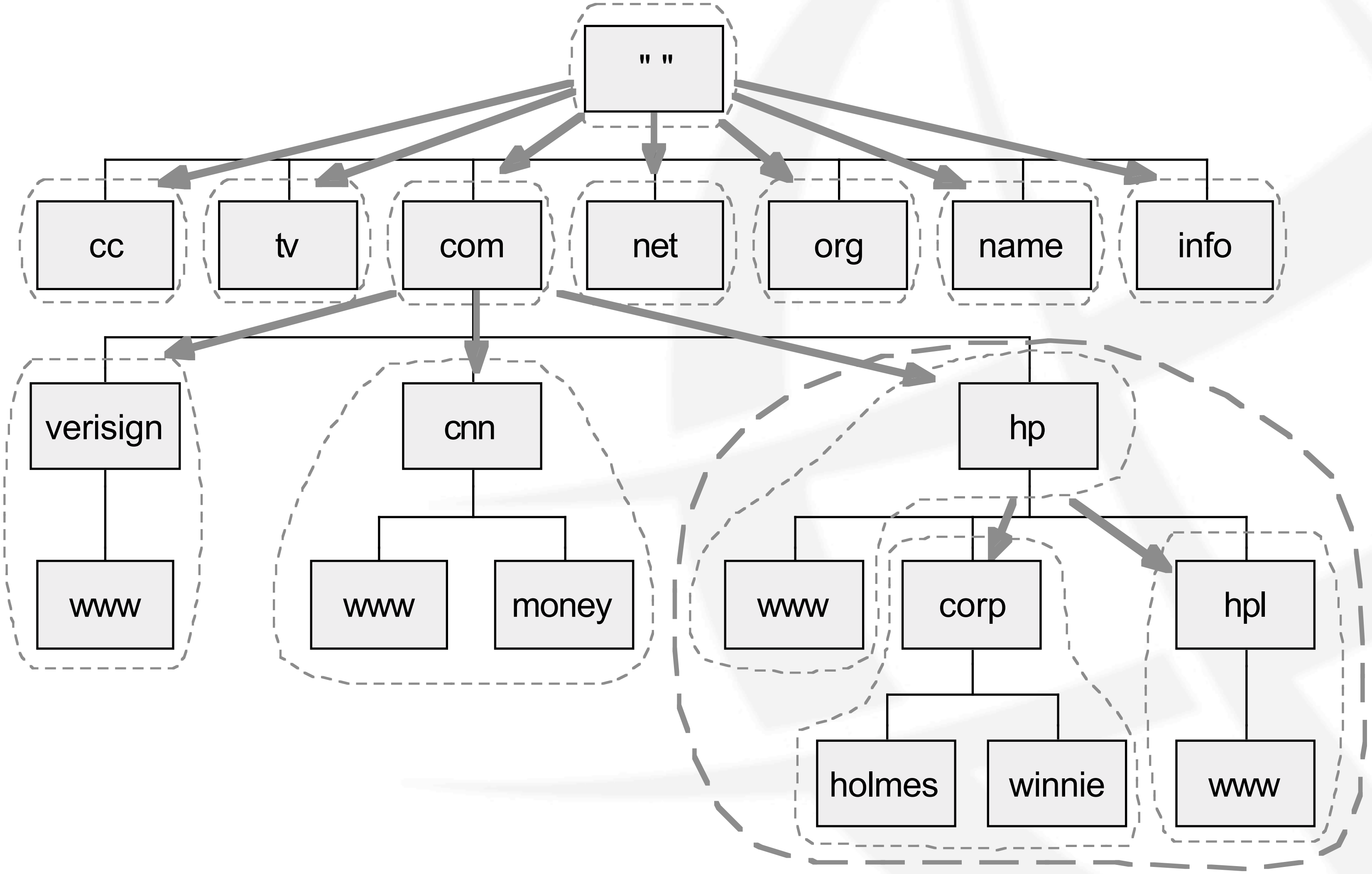
Domain Names: *www.cnn.com*



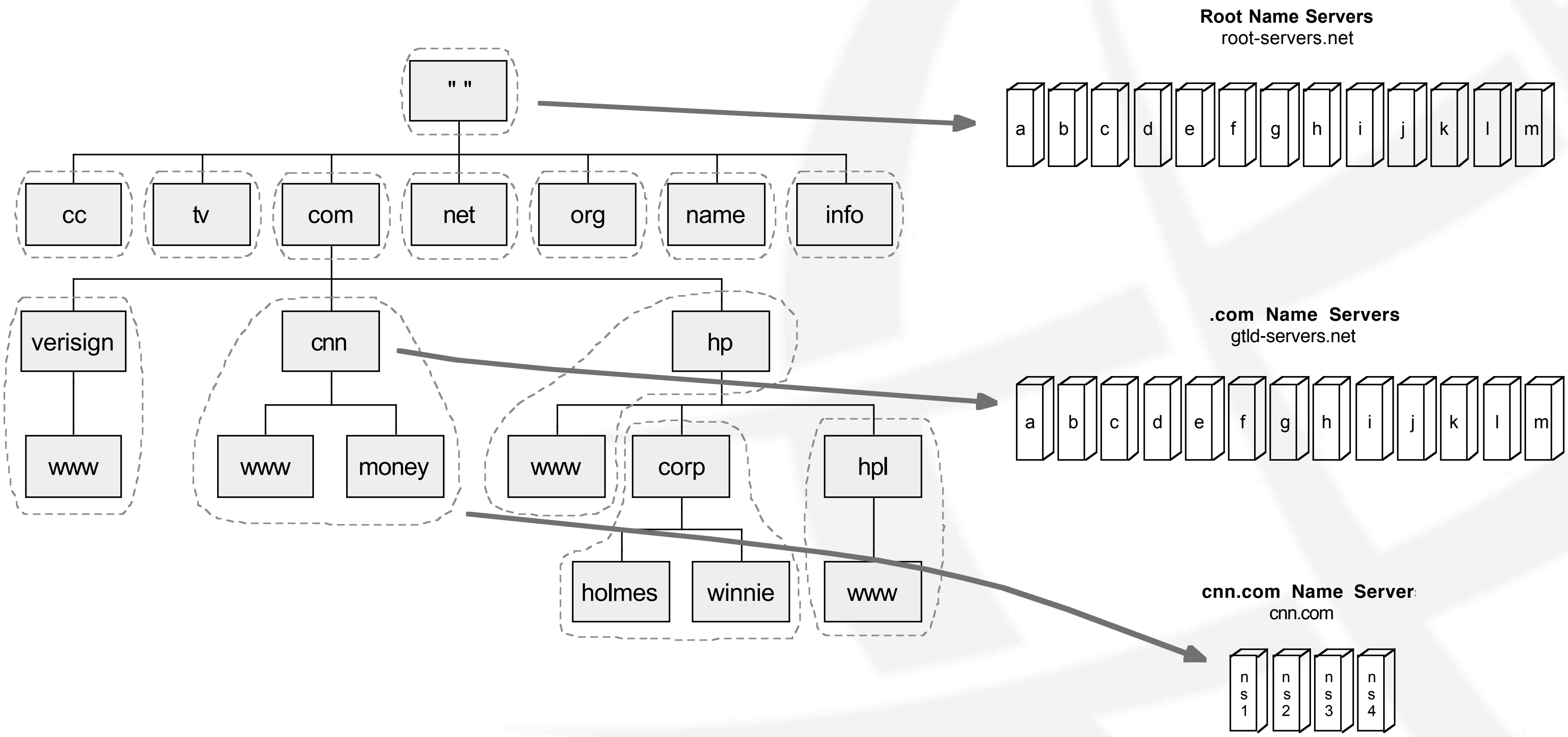
Domains: *hp.com*



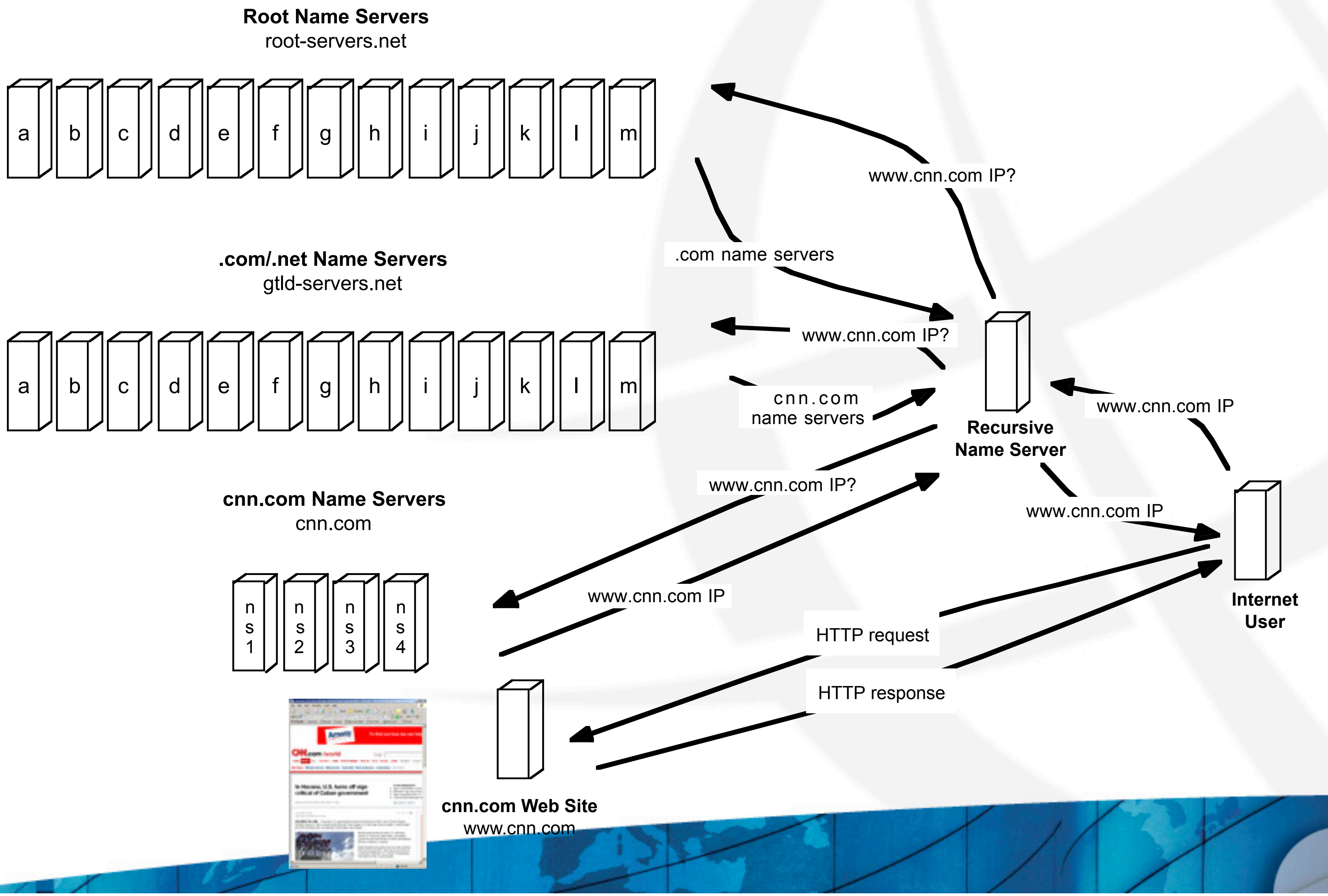
Zones


" "
cc
tv
com
net
org
name
info
verisign
www
cnn
www
money
hp
www
corp
hpl
holmes
winnie
www

Name Servers



Name Resolution



Root Name Servers
root-servers.net

.com/.net Name Servers
gtld-servers.net

cnn.com Name Servers
cnn.com

cnn.com Web Site
www.cnn.com

Recursive Name Server

Internet User

www.cnn.com IP?

.com name servers

www.cnn.com IP?

cnn.com name servers

www.cnn.com IP?

www.cnn.com IP

www.cnn.com IP

www.cnn.com IP

HTTP request

HTTP response

DNS Security

- DNS has no security
- One packet for query, one packet for response
- Must rely on source IP-based authentication
- Easily spoofed
- Clever resolvers help a lot
- But we need something better

What DNSSEC Does

- DNSSEC uses **public key cryptography** and **digital signatures** to provide:
  - Data origin authentication
    - "Did this DNS response really come from the *.com* zone?"
  - Data integrity
    - "Did an attacker (e.g., a man-in-the-middle) modify the data in this response since it was signed?"
- Bottom line: DNSSEC offers protection against spoofing of DNS data

What DNSSEC Doesn’t Do

- DNSSEC does not:
  - Provide any confidentiality for DNS data
    - I.e., no encryption
    - The data in the DNS is public, after all
  - Address attacks against the name server itself
    - Denial of service,
    - Packets of death,
    - etc.

Key Pairs

- In DNSSEC, each zone has a public/ private key pair
- The zone's **public key** is stored in the new **DNSKEY** record
- The zone's **private key** is kept safe
  - Stored offline (ideally)
  - Perhaps held in an HSM (Hardware Security Module)

Digital Signatures

- A zone’s private key signs each piece of DNS data in a zone
- Each digital signature is stored in an **RRSIG** record

Chain of Trust

- There are no certificates in DNSSEC
- The trust model is rigid
- The **chain of trust** flows from parent zone to child zone
- Only a zone's parent can vouch for its keys' identity

Types of Keys

- Signed zone has DNSKEY records at its apex
  - Usually multiple keys
  - One or more **key-signing keys (KSKs)**
  - One or more **zone-signing keys (ZSKs)**
- KSK
  - Signs only the DNSKEY records
- ZSK
  - Signs the rest of the zone

Delegation Signer (DS) Records

- The **Delegation Signer (DS)** record specifies a child zone’s key
- A zone’s DS records only appear in its parent zone
- DS records are signed by the parent zone

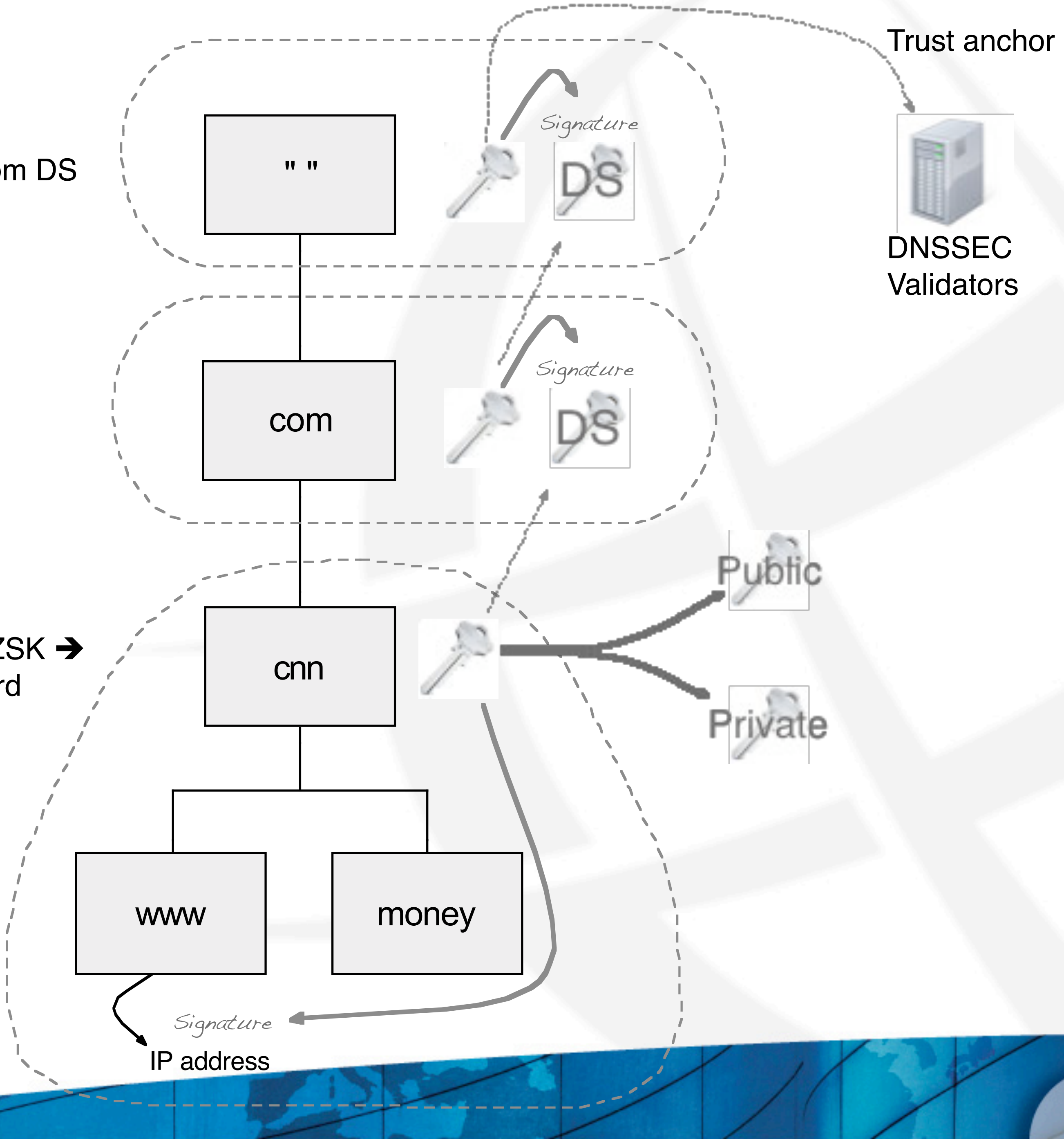
Trust Anchors

- You have to trust somebody
- DNSSEC validators need a list of trust anchors
- A trust anchor is a key that is implicitly trusted
- Analogous to list of certificate authorities (CAs) in web browsers

root KSK ➔ root ZSK ➔ com DS

com KSK ➔ com ZSK ➔
cnn.com DS

cnn.com KSK ➔ cnn.com ZSK ➔
www.cnn.com A record



ICANN

DNSSEC Chain of Trust

Norm Richie, ISC

in San Francisco ▪ 13-18 March 2011

ICANN SILICON VALLEY Meeting

A Sample DNSSEC Implementation & Audience Interaction

Russ Mundy, Cobham Solutions

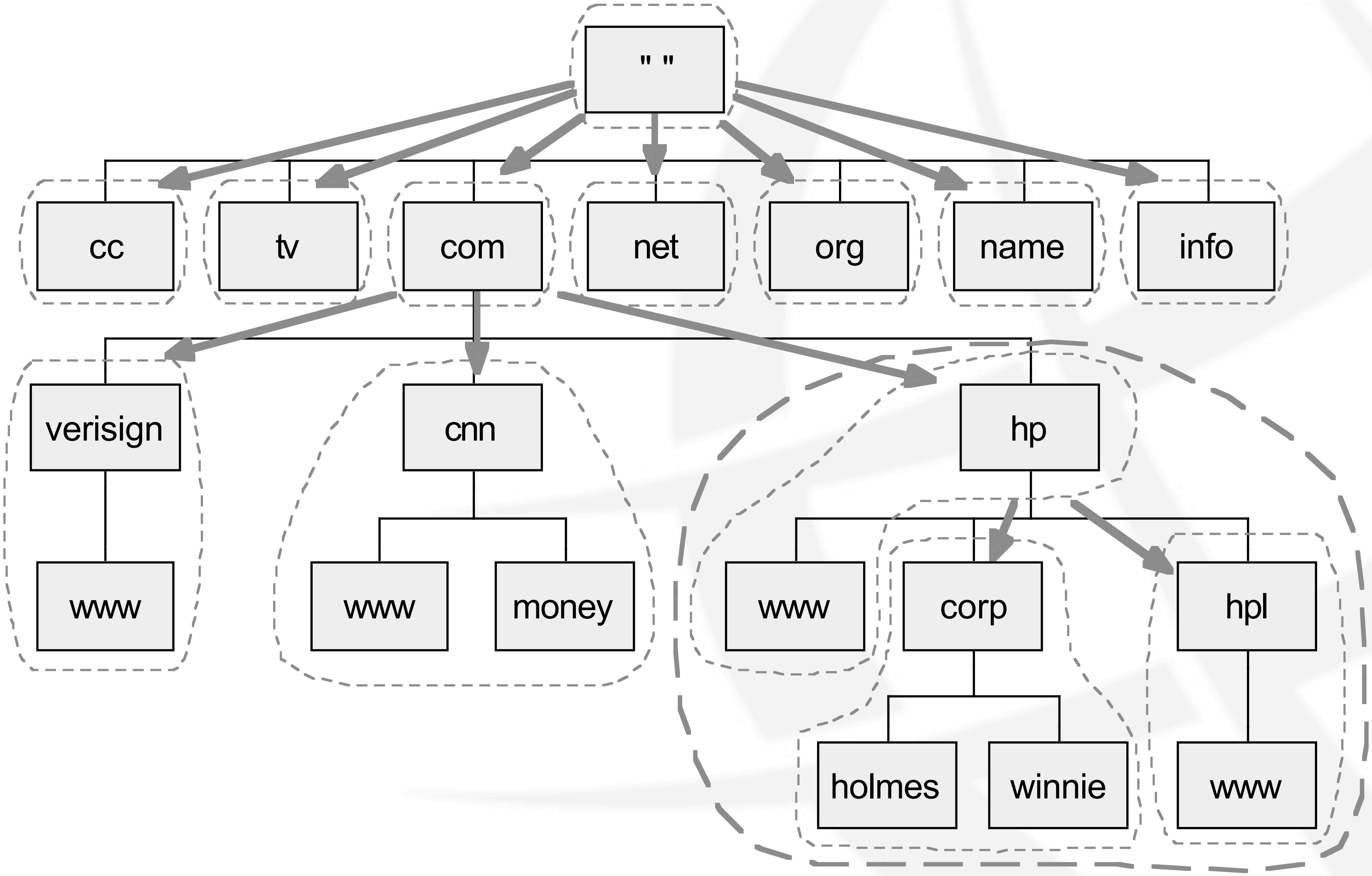
DNSSEC Implementation Samples

- DNSSEC implementation depends upon & is mostly driven by an activity's DNS functions
  - DNS is made up of many parts, e.g., name server operators, applications users, name holders ("owners"), DNS provisioning
  - Activities with large, complex DNS functions are more likely to have more complex DNSSEC implementation activities
    - Also more likely to have 'DNS knowledgeable' staff

DNSSEC Implementation Samples, Continued

- DNS size and complexity examples:
  - Registry responsible for a large TLD operation, e.g., .com
  - Substantial enterprise with many components with many geographic locations, e.g., hp.com
  - Internet-based businesses with a number of business critical zones, e.g., www.verisign.com
  - Activities with non-critical DNS zones, e.g., net-snmp.org
  - Proverbial Internet end users (all of us here)

Zones

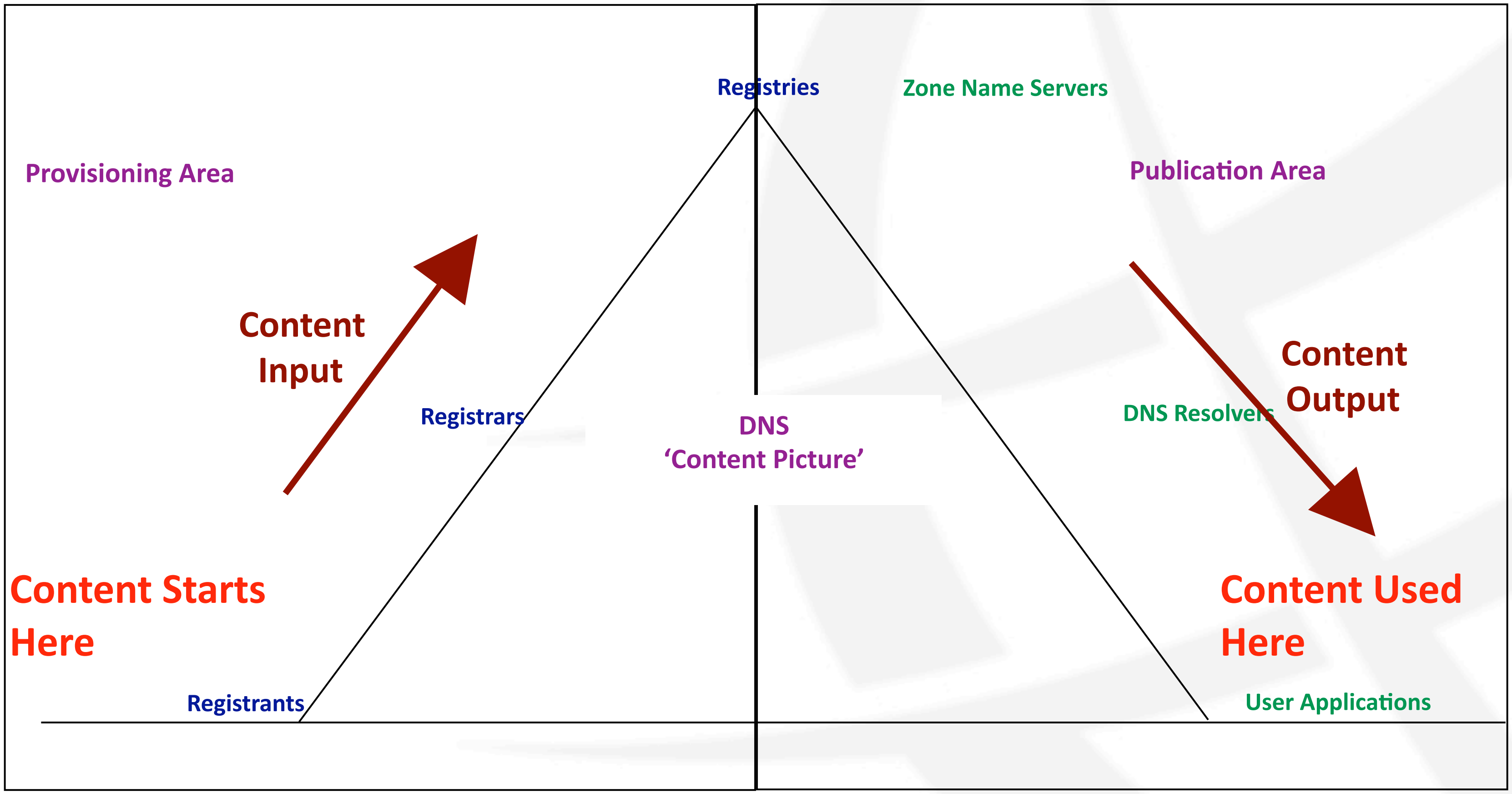

" "
cc
tv
com
net
org
name
info
verisign
www
cnn
www
money
hp
www
corp
hpl
holmes
winnie
www

General Principle:

- If an activity does a lot with their DNS functions and operations then they probably will want to do a lot with the associated DNSSEC pieces;
- If an activity does little or nothing with their DNS functions and operations then they probably will want to do little or nothing with the associated DNSSEC pieces.

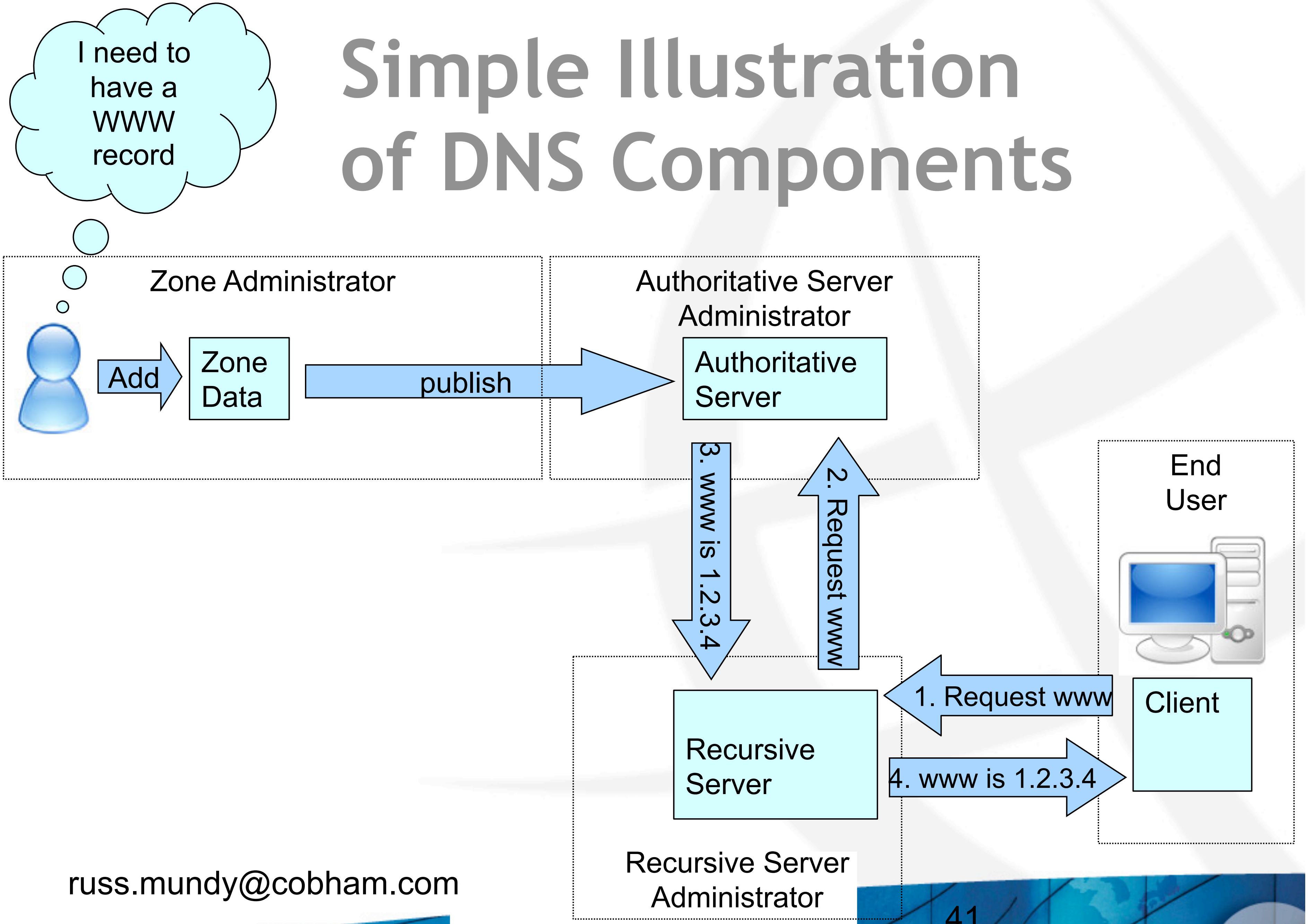
DNS Zone Content Flow

(for example, www.icann.org or www.cnn.com)



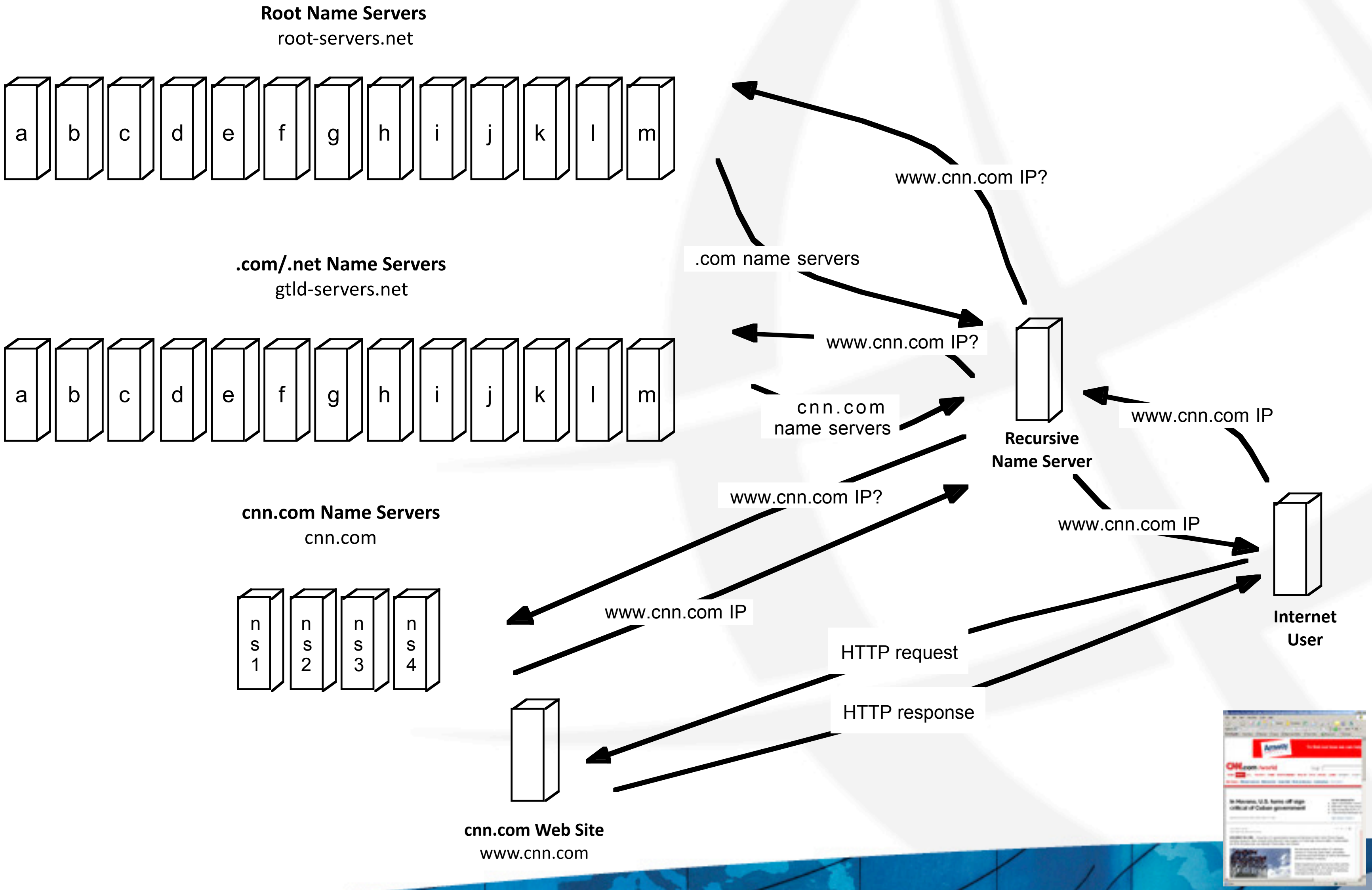
russ.mundy@cobham.com

Simple Illustration of DNS Components



russ.mundy@cobham.com

Name Resolution



Root Name Servers
root-servers.net

.com/.net Name Servers
gtld-servers.net

cnn.com Name Servers
cnn.com

Recursive Name Server

Internet User

cnn.com Web Site
www.cnn.com

www.cnn.com IP?

.com name servers

www.cnn.com IP?

cnn.com name servers

www.cnn.com IP?

www.cnn.com IP

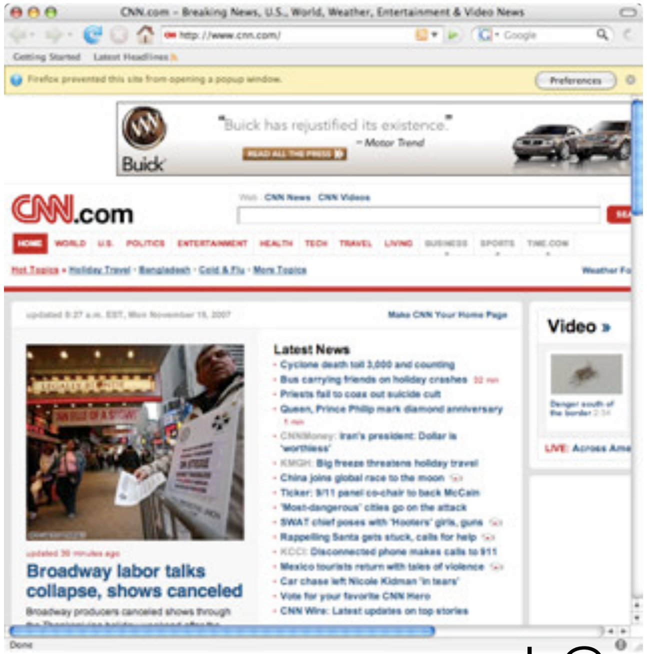
www.cnn.com IP

www.cnn.com IP

HTTP request

HTTP response

1 Webpage = Multiple DNS Name Resolutions



CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News

http://www.cnn.com/

Getting Started Latest Headlines

Firefox prevented this site from opening a popup window. Preferences

"Buick has rejustified its existence."
– Motor Trend
READ ALL THE PRESS
Buick

CNN.com

Web CNN News CNN Videos

HOME WORLD U.S. POLITICS ENTERTAINMENT HEALTH TECH TRAVEL LIVING BUSINESS SPORTS TIME.COM

Hot Topics » Holiday Travel · Bangladesh · Cold & Flu · More Topics Weather Fo

updated 8:27 a.m. EST, Mon November 19, 2007 Make CNN Your Home Page

updated 30 minutes ago

Broadway labor talks collapse, shows canceled

Broadway producers canceled shows through

Latest News

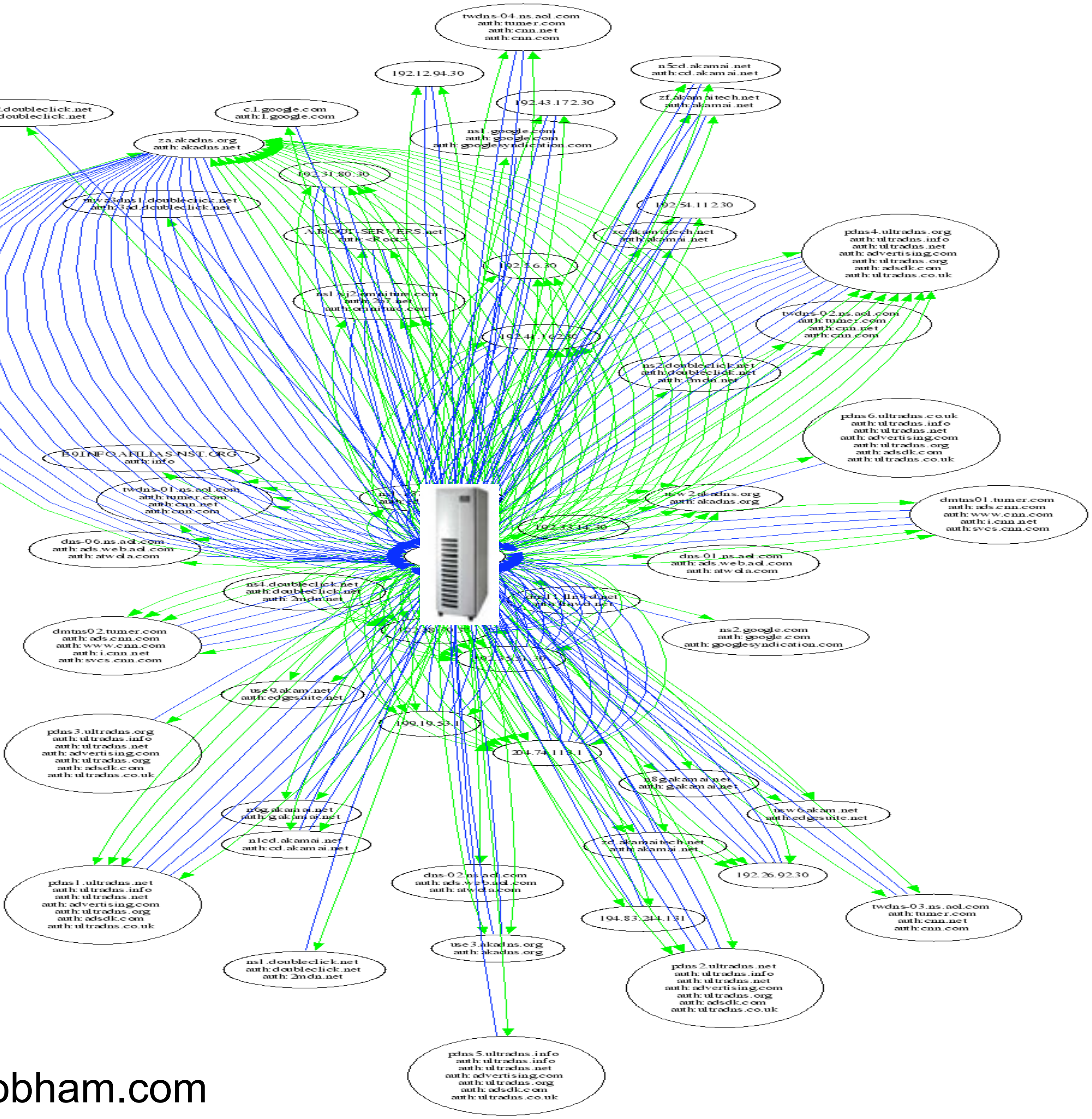
- Cyclone death toll 3,000 and counting
- Bus carrying friends on holiday crashes 32 min
- Priests fail to coax out suicide cult
- Queen, Prince Philip mark diamond anniversary 1 min
- CNNMoney: Iran's president: Dollar is 'worthless'
- KMGH: Big freeze threatens holiday travel
- China joins global race to the moon
- Ticker: 9/11 panel co-chair to back McCain
- 'Most-dangerous' cities go on the attack
- SWAT chief poses with 'Hooters' girls, guns
- Rappelling Santa gets stuck, calls for help
- KCCI: Disconnected phone makes calls to 911
- Mexico tourists return with tales of violence
- Car chase left Nicole Kidman 'in tears'
- Vote for your favorite CNN Hero
- CNN Wire: Latest updates on top stories

Video »

Danger south of the border 2:34

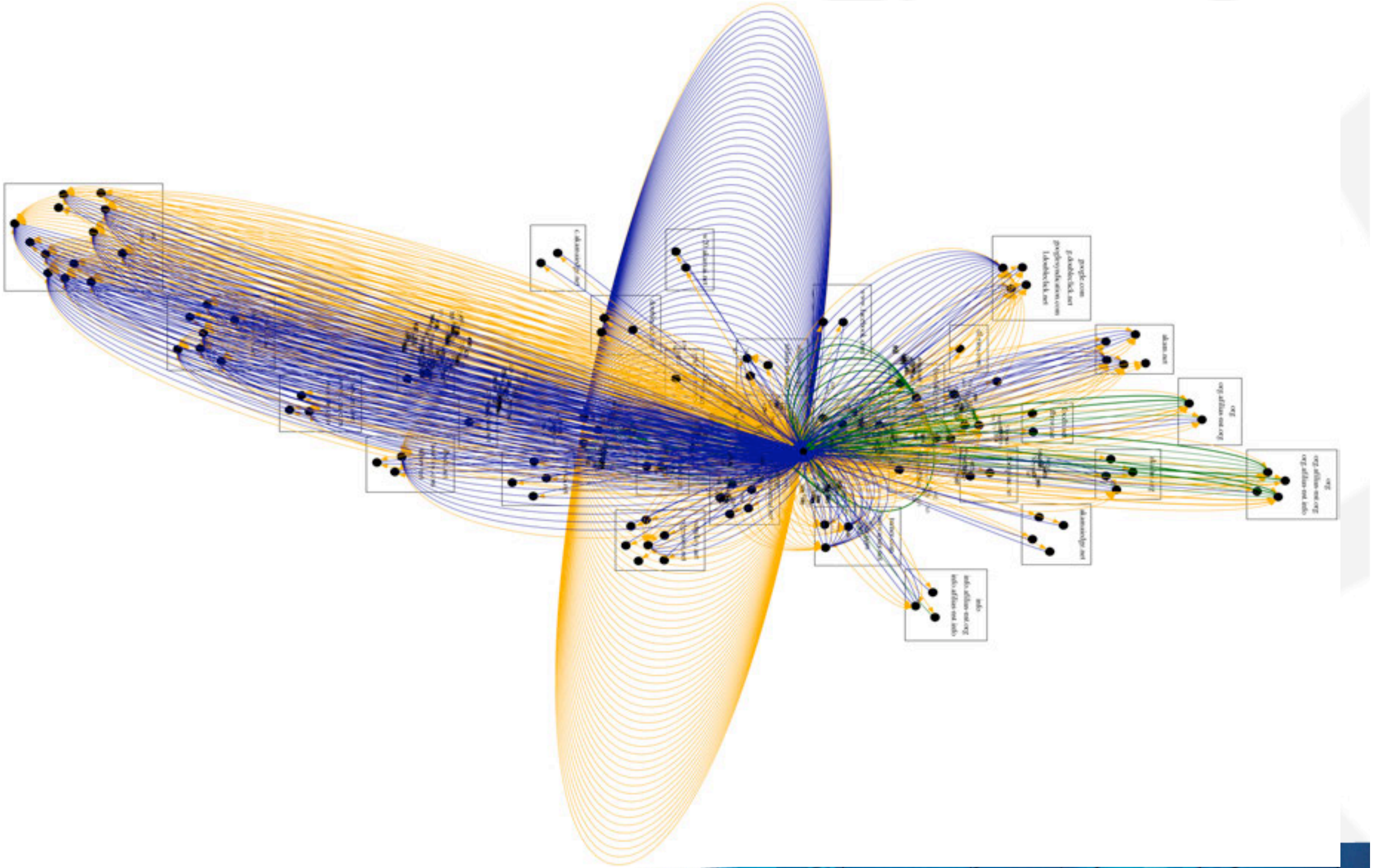
LIVE: Across Ame

Done



russ.mundy@cobham.com

www.cnn.com


google.com
g.doubleclick.net
googlesyndication.com
1.doubleclick.net
akam.net
akamaiedge.net
info
info.afilias-nst.org
info.afilias-nst.info

DNS Basic Functions

- DNS provides the translation from names to network addresses
- Get the right DNS content to Internet users

➢ IT’S **<u>DNS CONTENT</u>** THAT MATTERS!

How Does DNSSEC Fit?

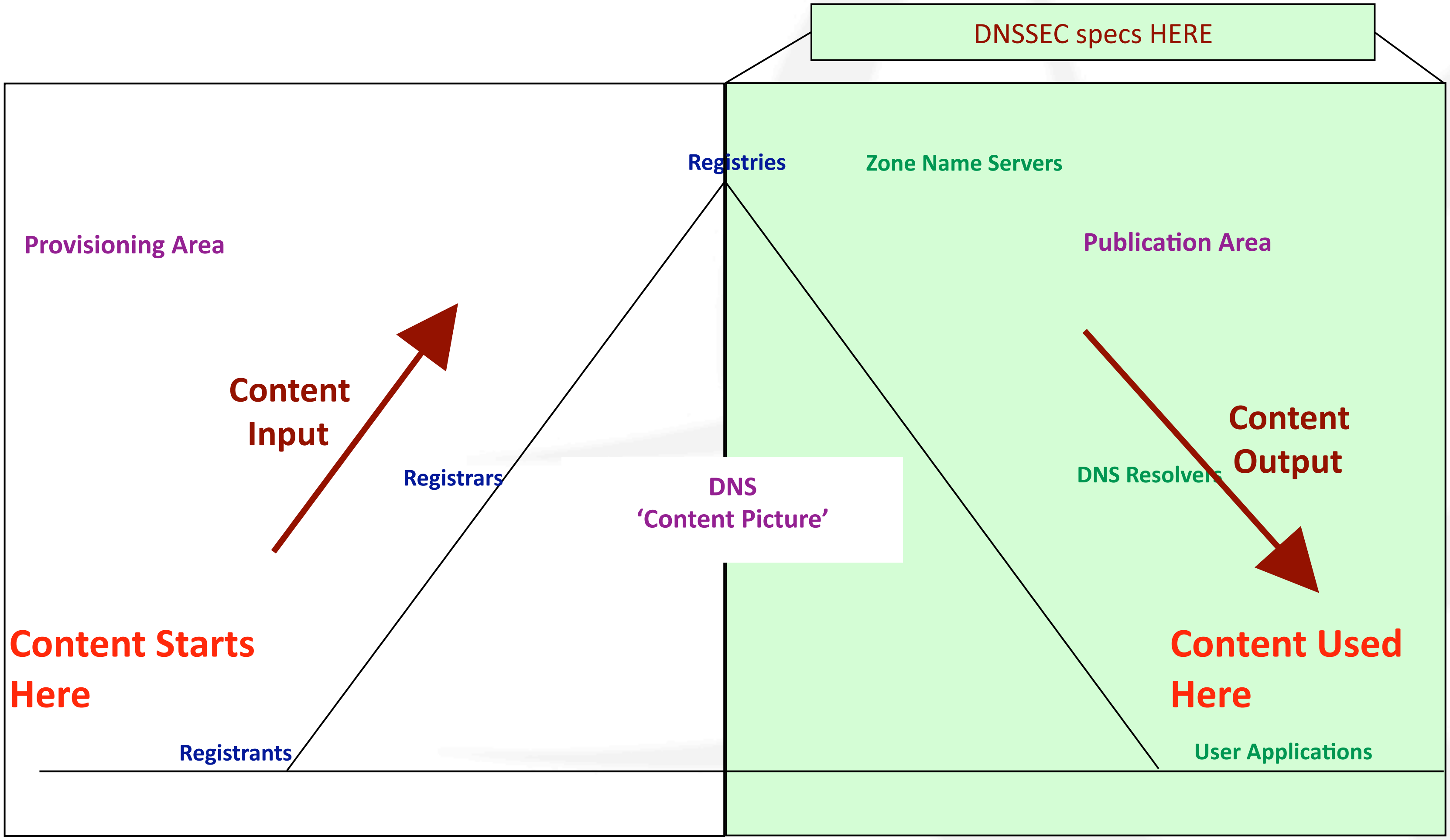
- DNSSEC required to thwart attacks on DNS CONTENT
  - DNS attacks used to attack Internet users applications

➢ Protect **DNS CONTENT** as much as (or more than) any DNSSEC information

  ➢ Including DNSSEC private keys!!

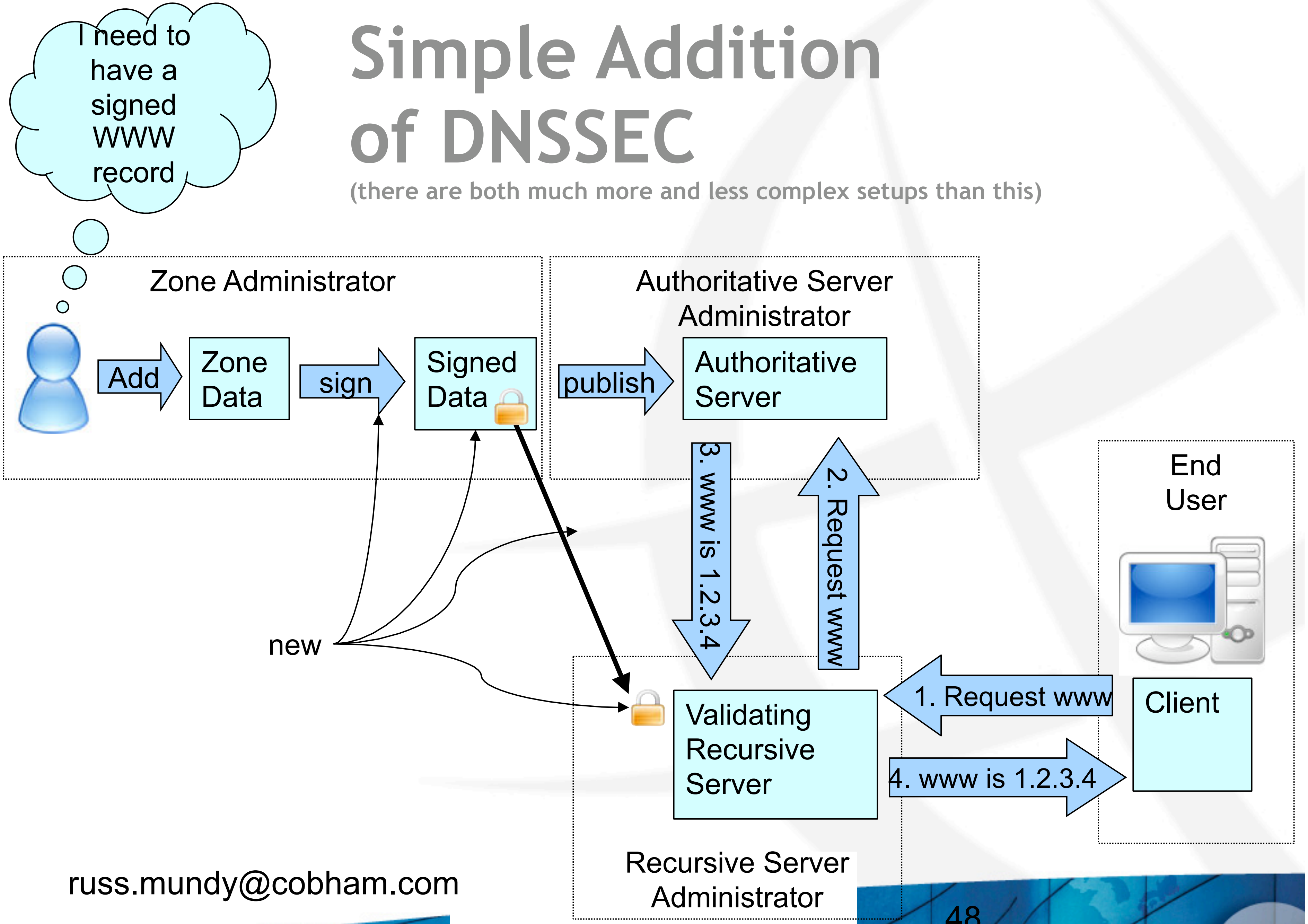
DNS Zone Content Flow

(for example, www.icann.org or www.cnn.com)



Simple Addition of DNSSEC

(there are both much more and less complex setups than this)



russ.mundy@cobham.com

Implementation Samples

- In general, try to do DNSSEC in the same way that you are doing DNS

Implementation Samples

- If you’re running much or all of your DNS functions and operations, DNSSEC implementation could be based on:
  - – Extend DNS operation to incorporate DNSSEC;
  - – Use open source DNSSEC tools (e.g., from www.dnssec-tools.org or opendnssec.org);
  - – Use commercial DNSSEC products;
  - – Mix elements from ‘all of the above’

Implementation Samples

- If DNS functions and operations are being done with one (or several) software & hardware products, find out if the product providers have (or will) incorporate DNSSEC to support your DNS functions and operations.
  - If not, push them for adding DNSSEC to their products; or
  - Examine additional or different products or services that will provide DNSSEC, e.g., emerging DNSSEC signing services.

Implementation Samples

- If you are the holder (‘owner’) of names but “out-source” DNS functions and operations, e.g., to your registrar, then determine if the “out-source” offers DNSSEC capability.
  - If not, push on them to develop and offer DNSSEC capability
  - Consider using a different “out-source” DNS service
  - Consider developing “in-house” DNS (and DNSSEC) capabilities

Audience Interaction and Participation

ICANN

Summary

Simon McCalla, Nominet UK

in San Francisco ▪ 13-18 March 2011

ICANN SILICON VALLEY Meeting

Thank You and Questions