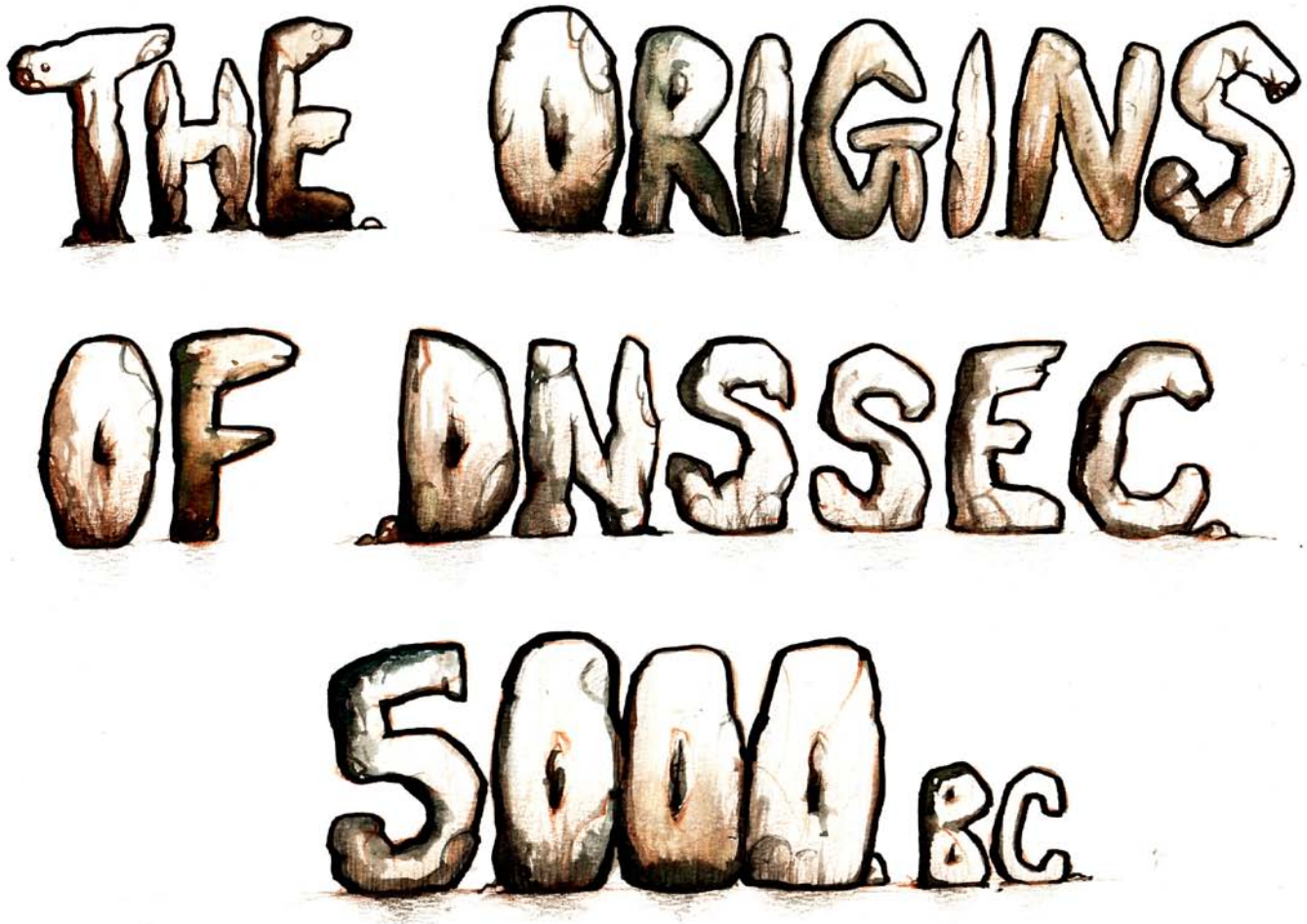
DNSSEC for Everybody: A Beginner's Guide

Prague, Czech Republic

25 June 2012

The Schedule

Outline Concept	Segment	Duration	Speaker
Welcome	Welcome and	2 mins	Simon
Basic Concepts	Caveman – DNSSEC	3 mins	Simon
	DNS Basics	5 mins	Roy
	DNS Chain of Trust - Live	5 mins	Norm
Core Concepts	DNSSEC – How it works	10 mins	Roy
	DNSSEC – Chain of Trust	5 mins	Norm
Real World Examples	A sample DNSSEC implementation (what it looks like, s/w etc). A simple guide to deployment.	10 mins	Russ
	A guide to DNSSEC Deployment options: Technologies and vendors.	10 mins	Russ
Summary	Session Round up, hand out of materials, Thank you's	2 mins	Simon

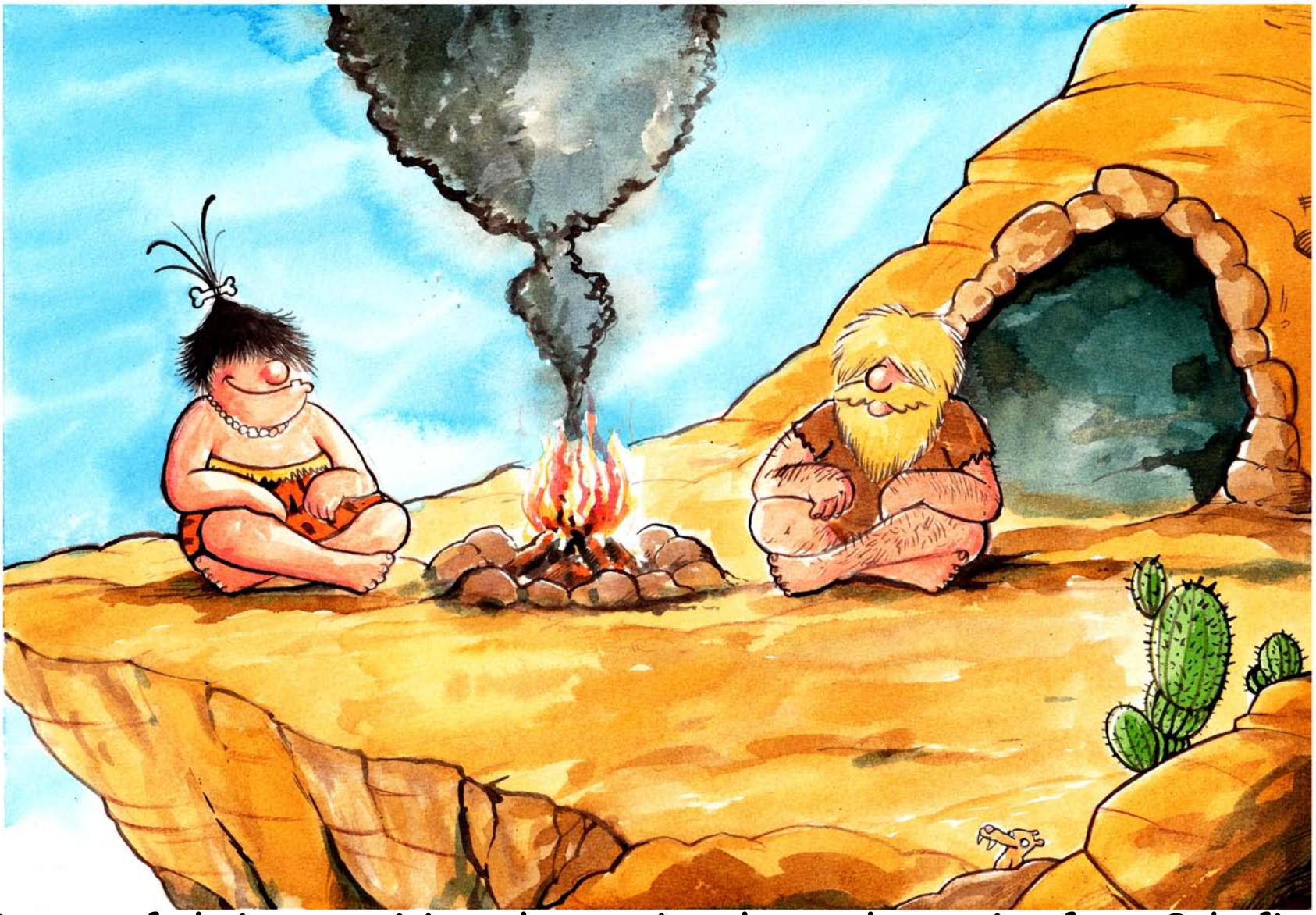


nominet®

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

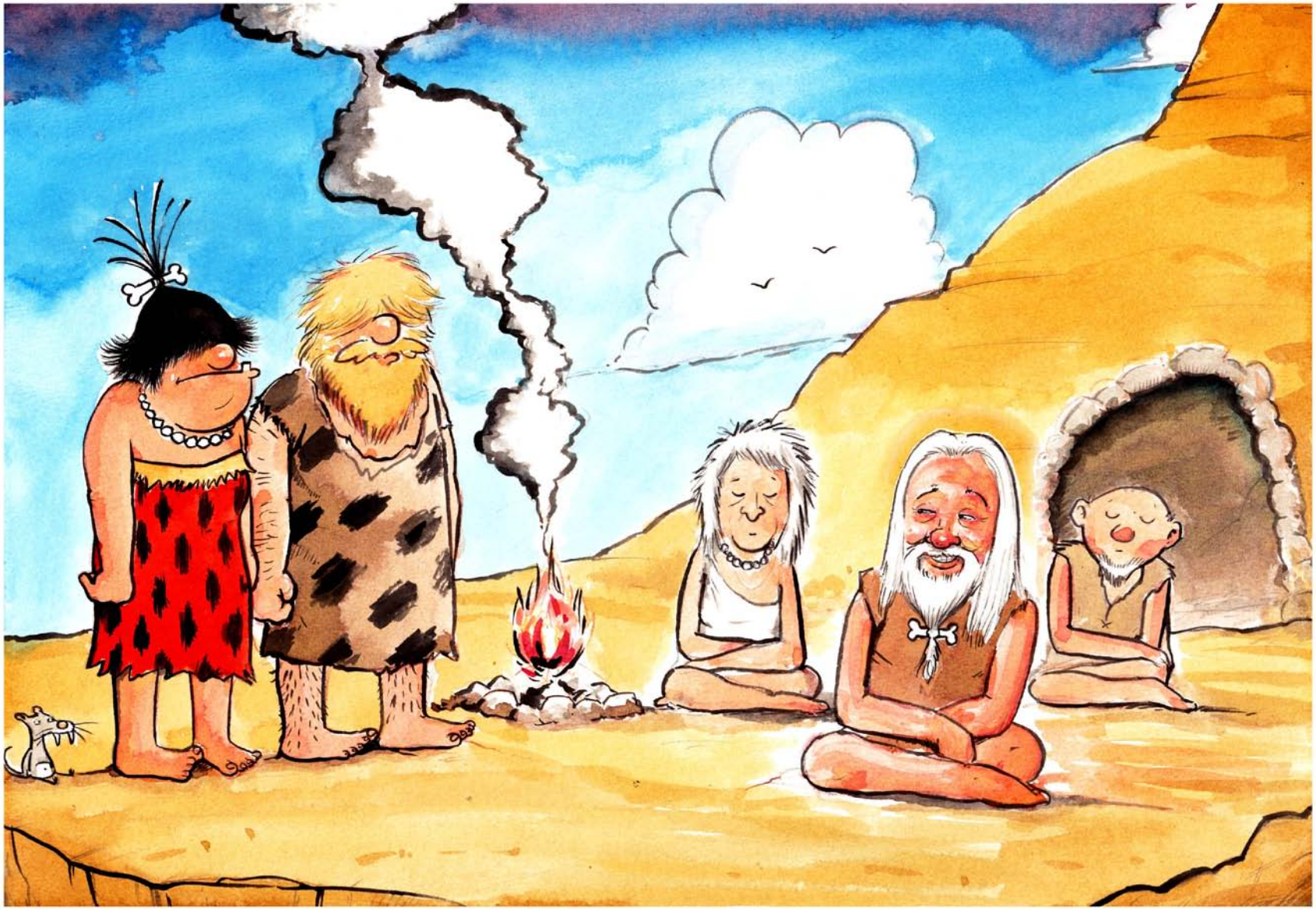
nominet®

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

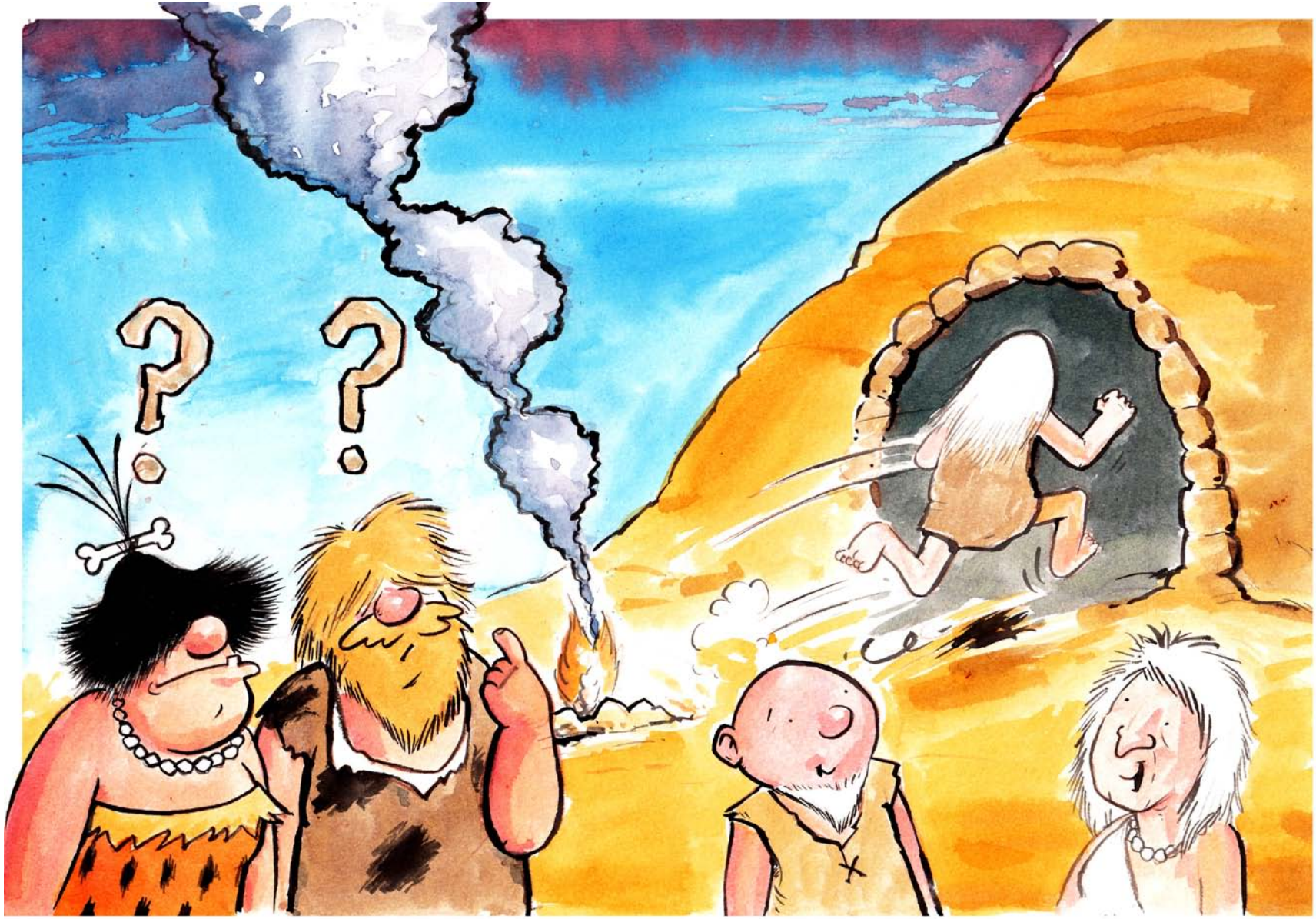
Now Ugwina is really confused. She doesn't know which smoke to believe...

nominet®

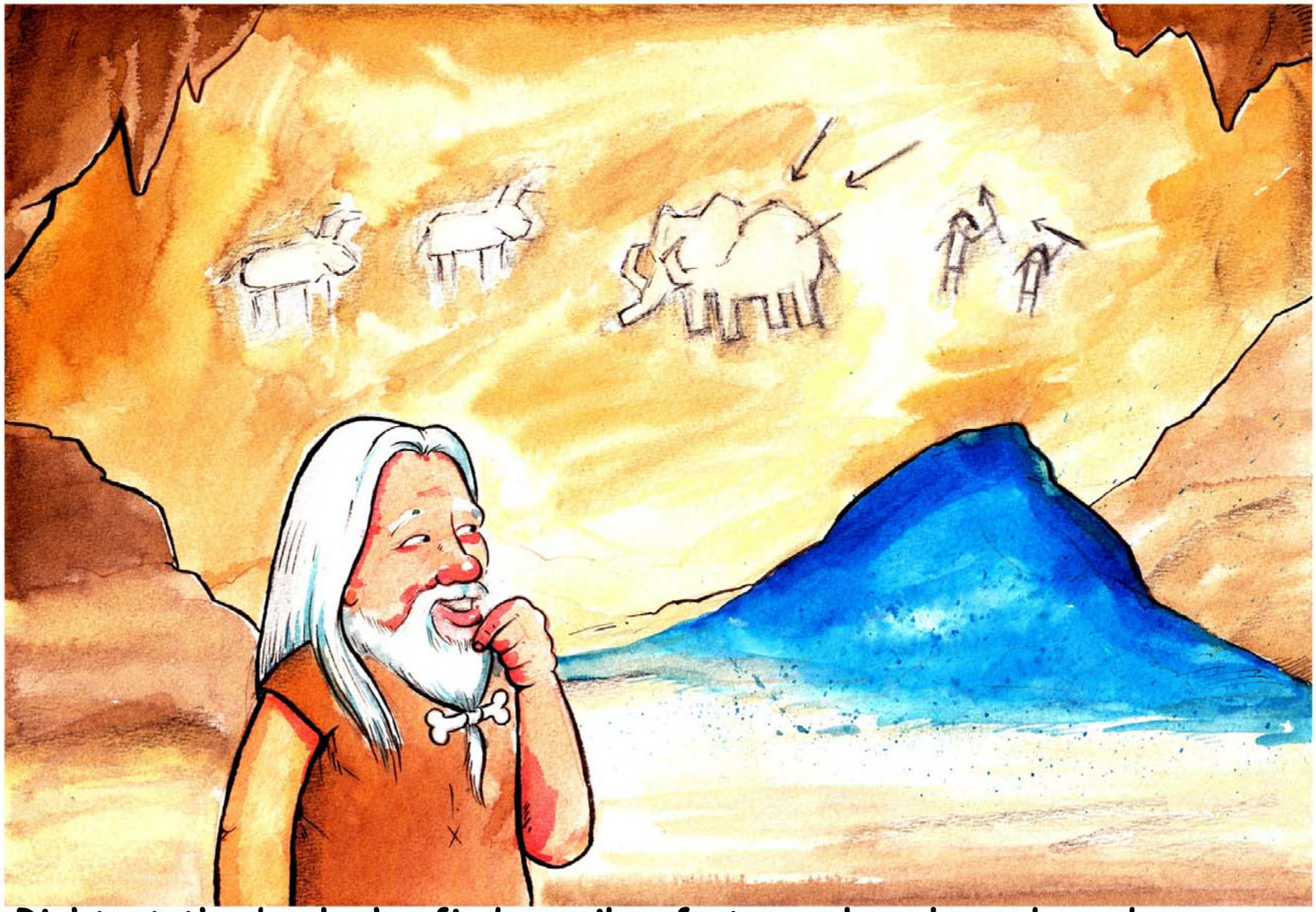
So Ugwina sets off down the canyon to try and sort out the mess...



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…

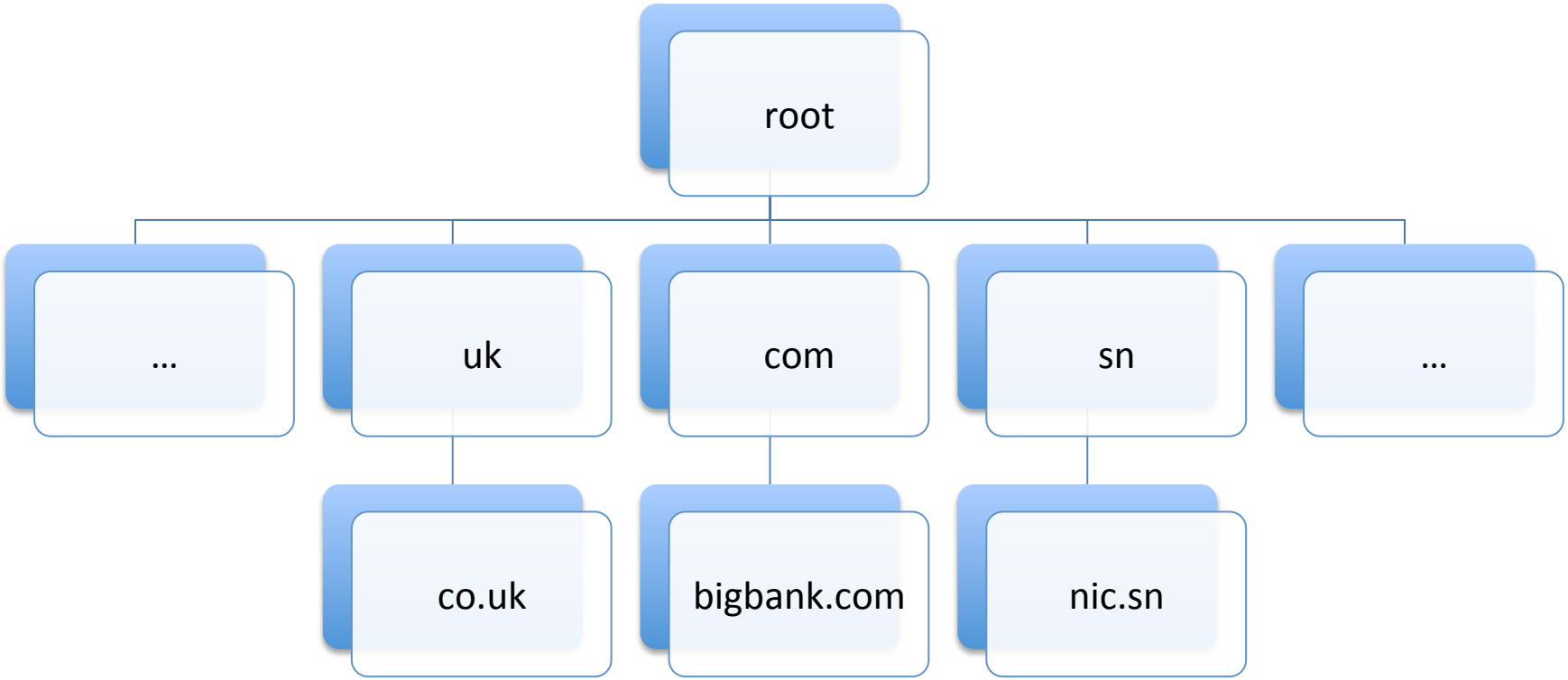
Introduction to DNSSEC

Roy Arends, Nominet UK

ICANN

Dakar
SÉNÉGAL
N°42 23 - 28 October 2011

High level concept of DNS

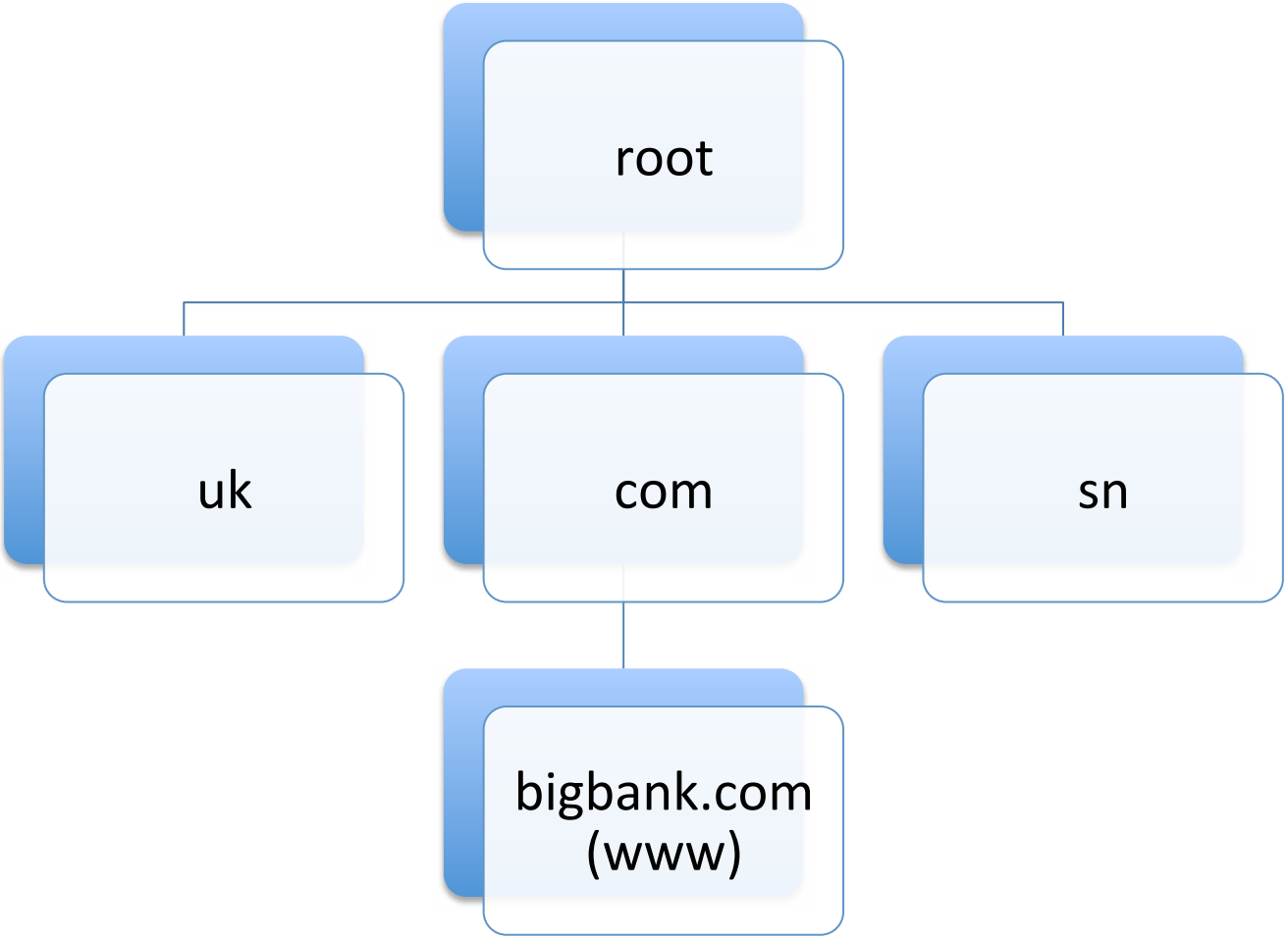


High level concept of DNS

- A resolver knows where the root-zone is
- Traverses the DNS hierarchy
- Each level refers the resolver to the next level
- Until the question has been answered
- The resolver caches all that information for future use.

…Ugwina, the resolver, chatting with Og, the server…

High level concept of DNS

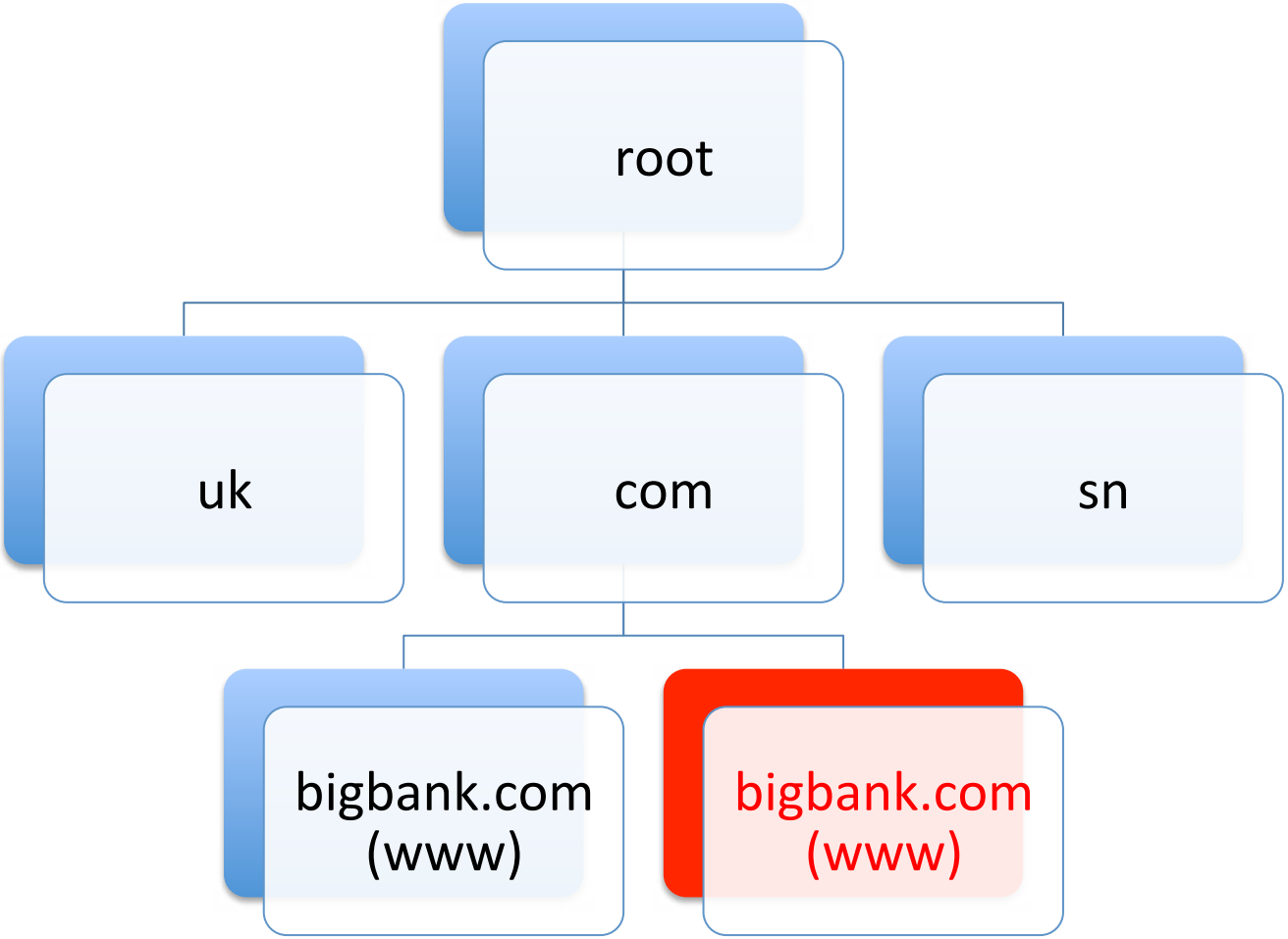


High level concept of DNS

- There is no security
- Names are easily spoofed
- Caches are easily poisoned

…Ugwina, the resolver is confused. She doesn't know who the real Og is…

High level concept of DNS



DNSSEC is the solution

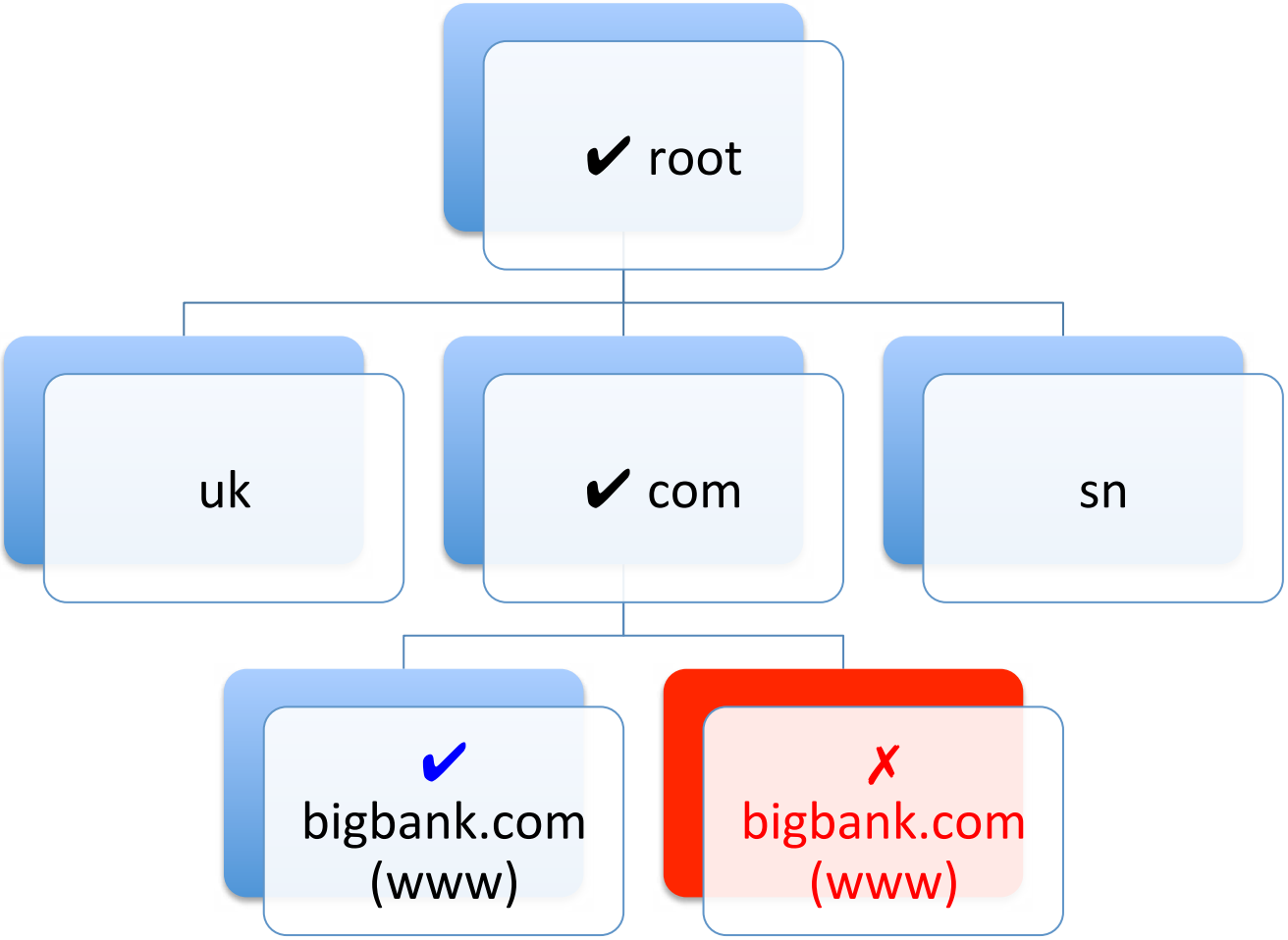
- DNSSEC uses **digital signatures** to assure that information is correct and came from the right place.
- The keys and signatures to verify the information, is stored in the DNS as well
- Since DNS is a lookup system, keys can simply be looked up, like any data.

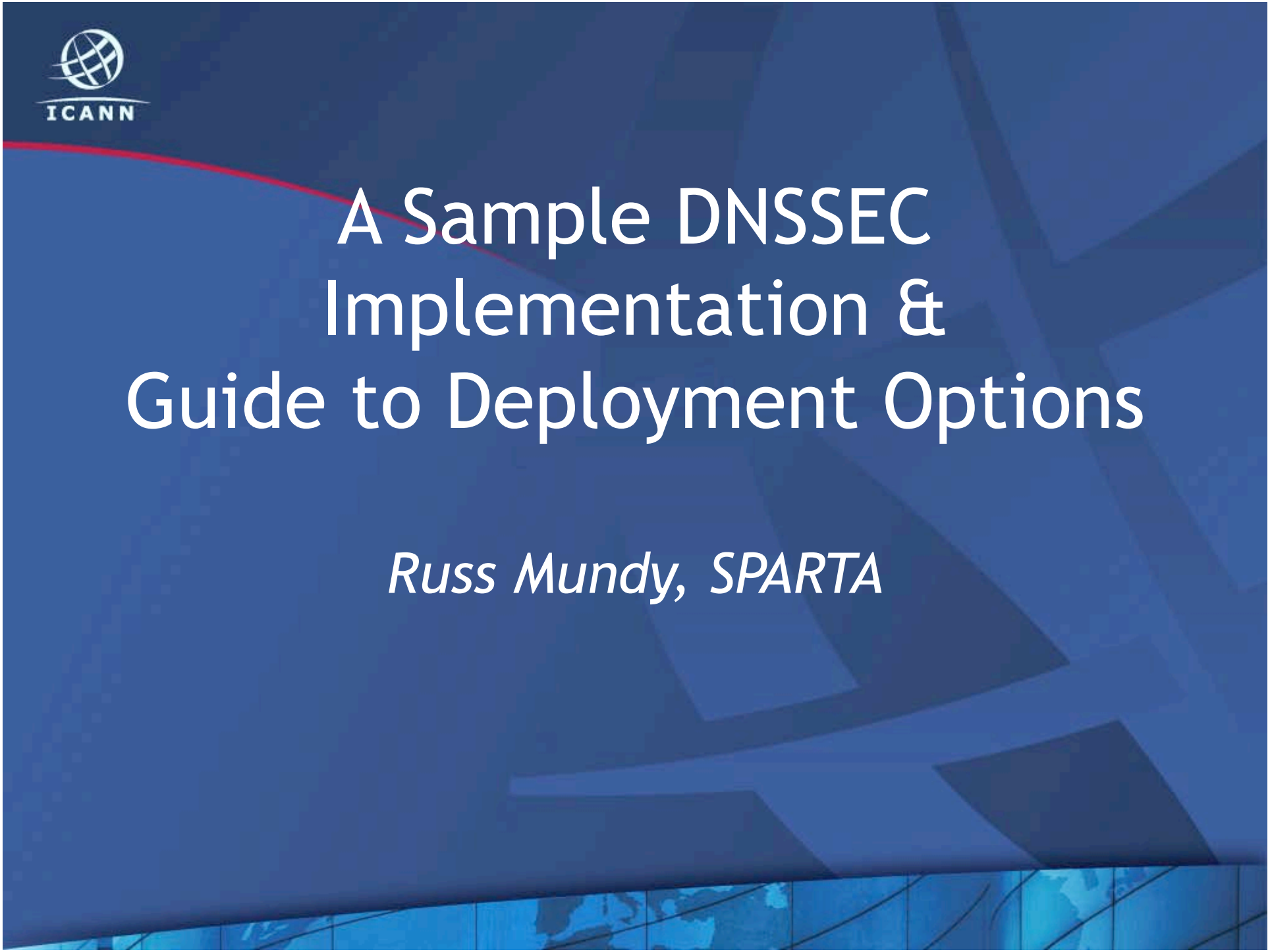
…Ugwina, the resolver, can verify that the real Og sends the message…

High level concept of DNSSEC

- A resolver knows what the root-key is
- It builds a Chain of Trust:
  - Each level signs the key of the next level
  - Until the chain is complete

High level concept of DNSSEC





A Sample DNSSEC Implementation & Guide to Deployment Options

Russ Mundy, SPARTA

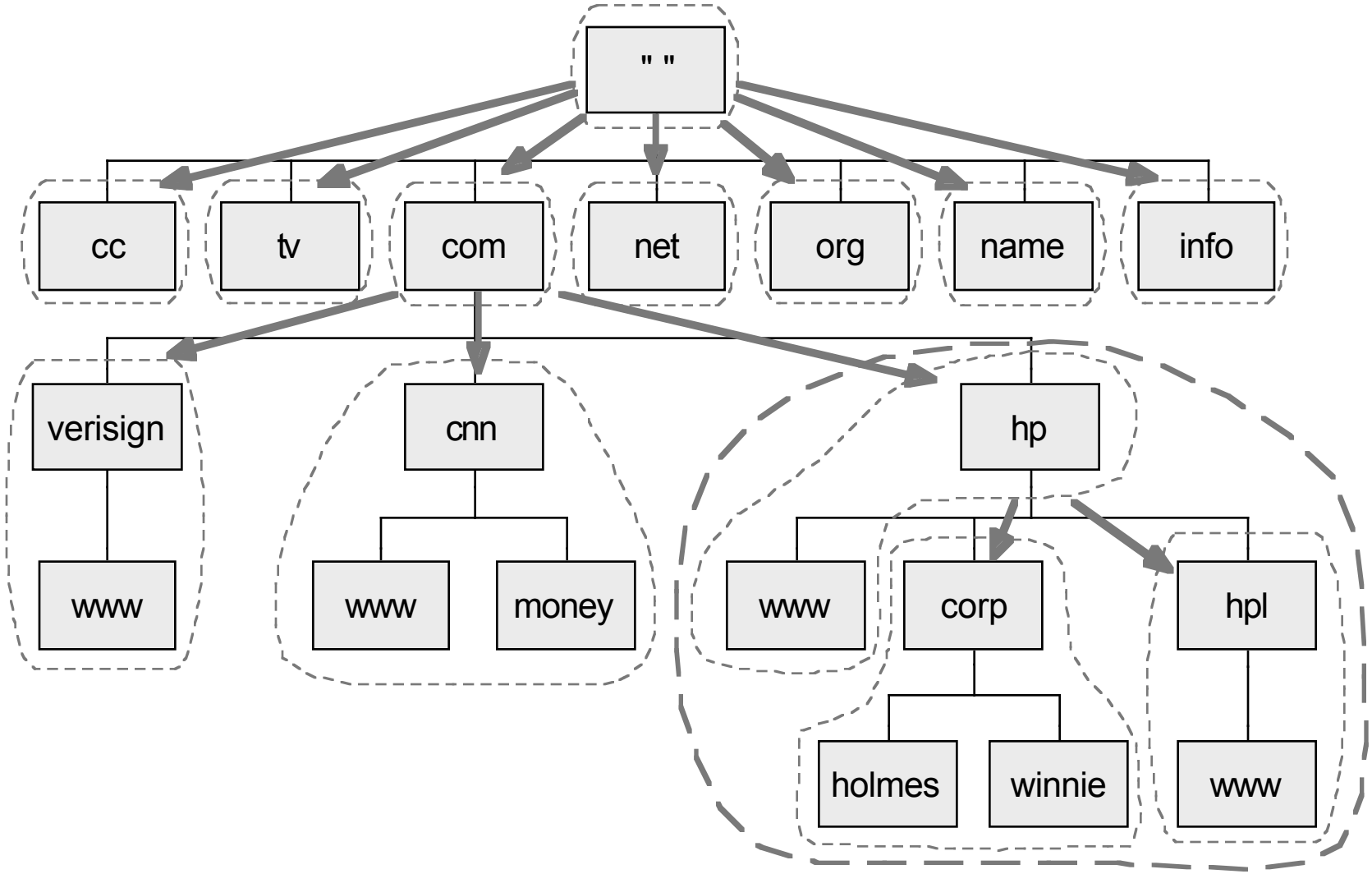
DNSSEC Implementation Samples

- 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

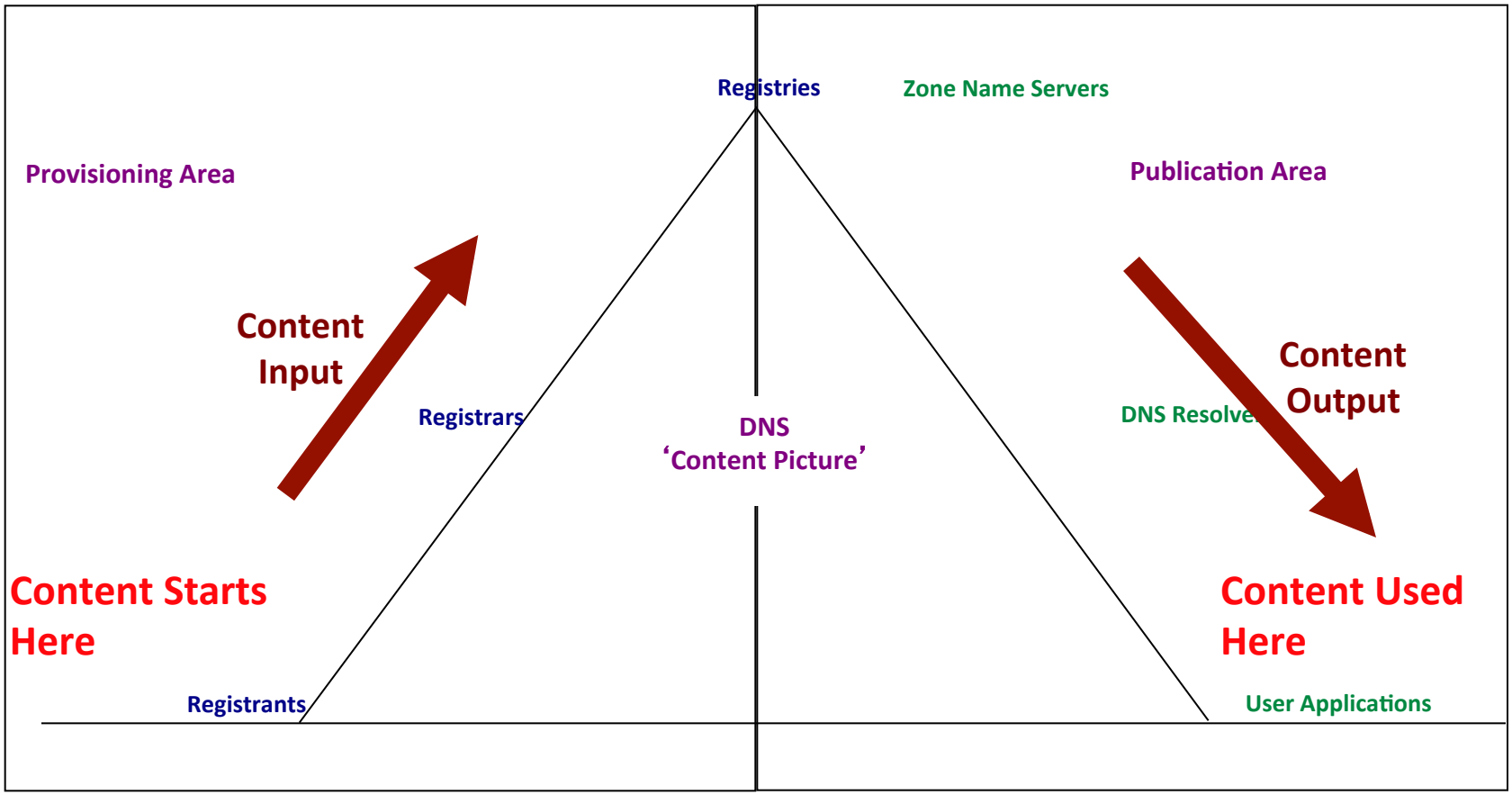

" "
cc
tv
com
net
org
name
info
verisign
cnn
hp
www
www
money
www
corp
hpl
holmes
winnie
www

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)

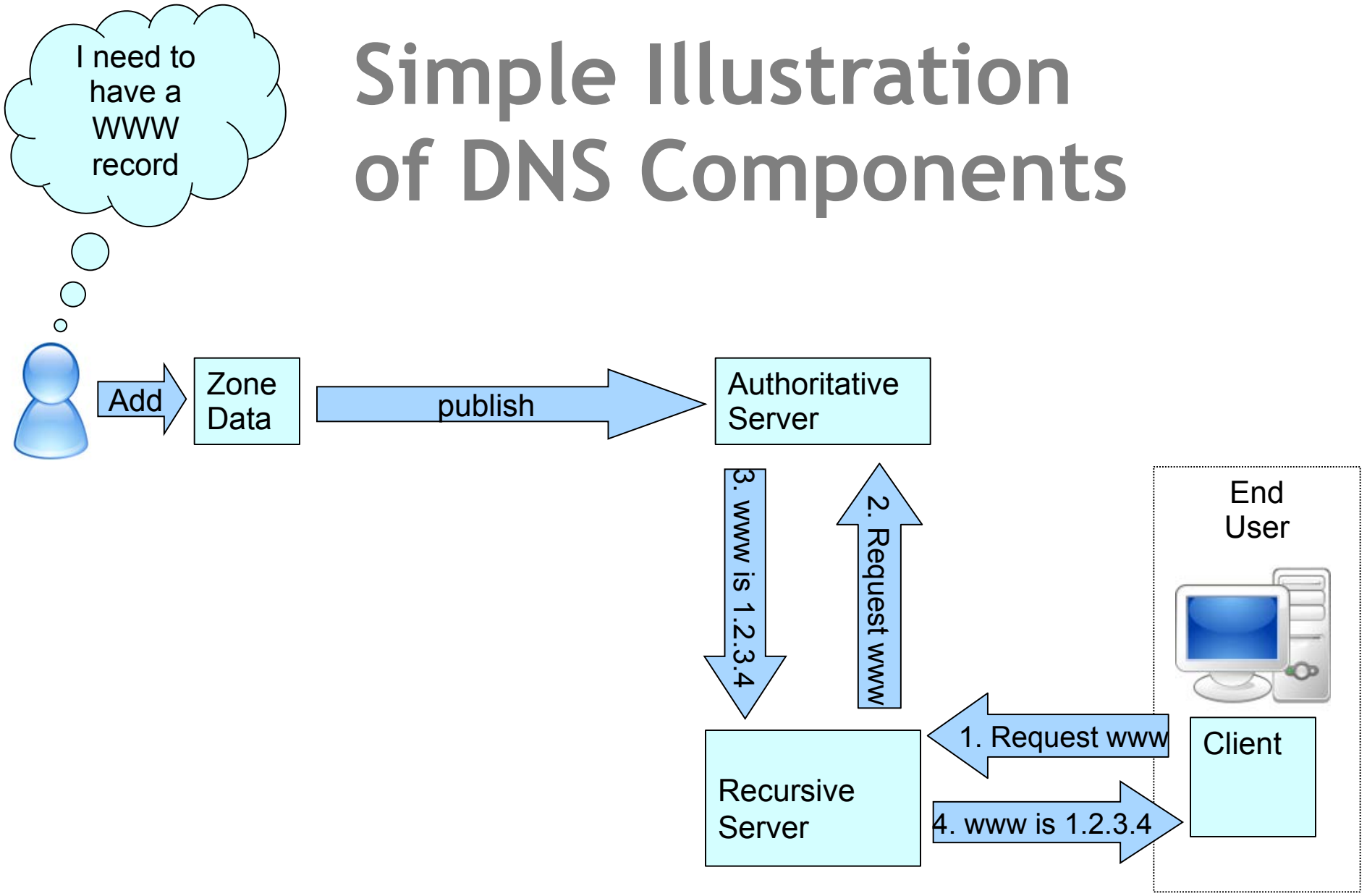


russ.mundy@sparta.com

Questions for Everyone …

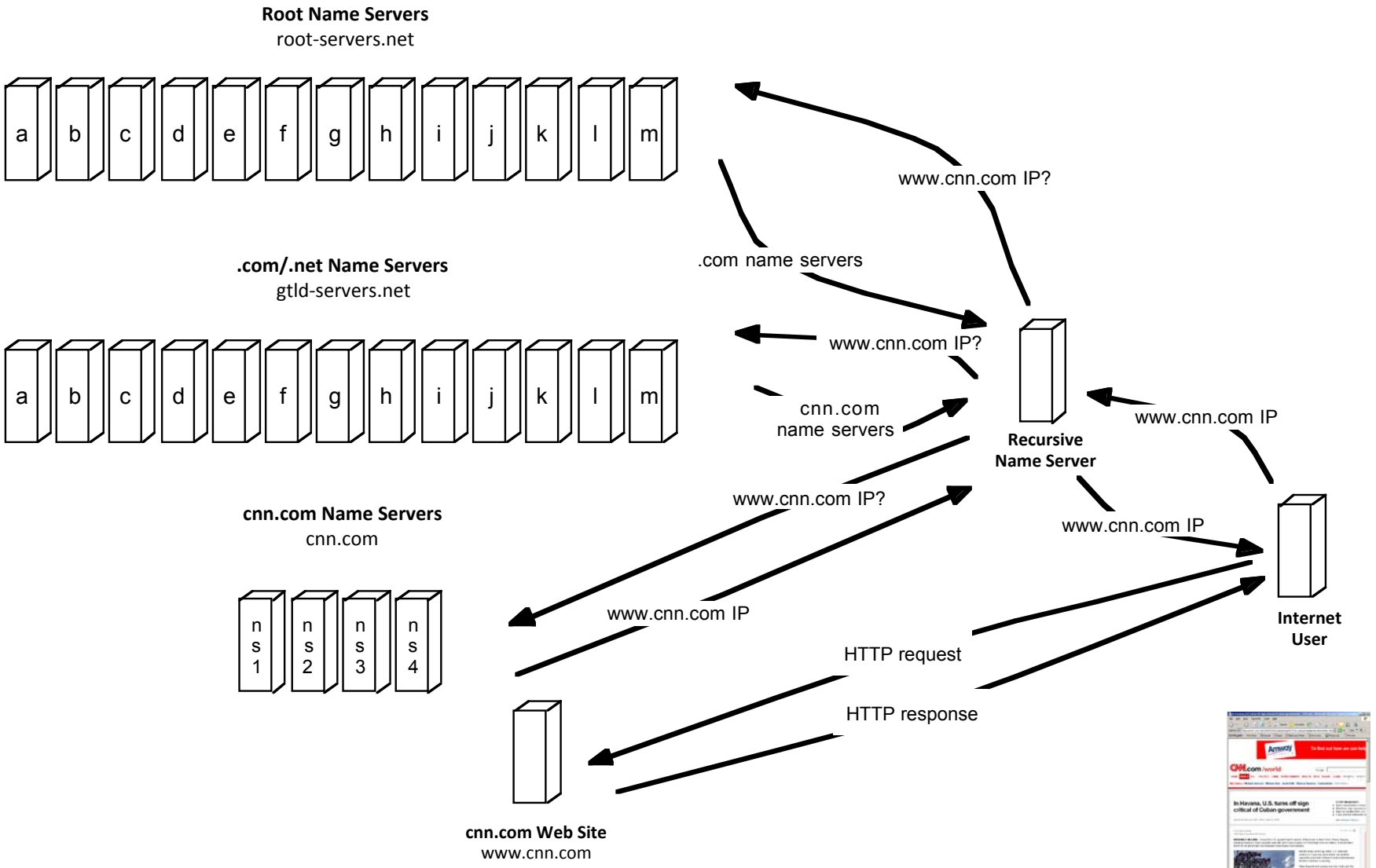
- Do you know WHERE you get your DNS name(s) from?
- Do you know WHO operates the DNS name servers for your name(s)?

Simple Illustration of DNS Components

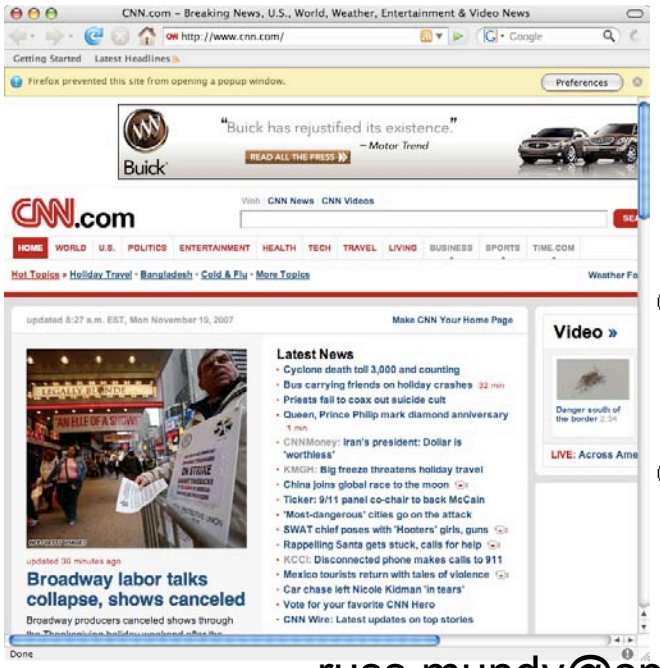


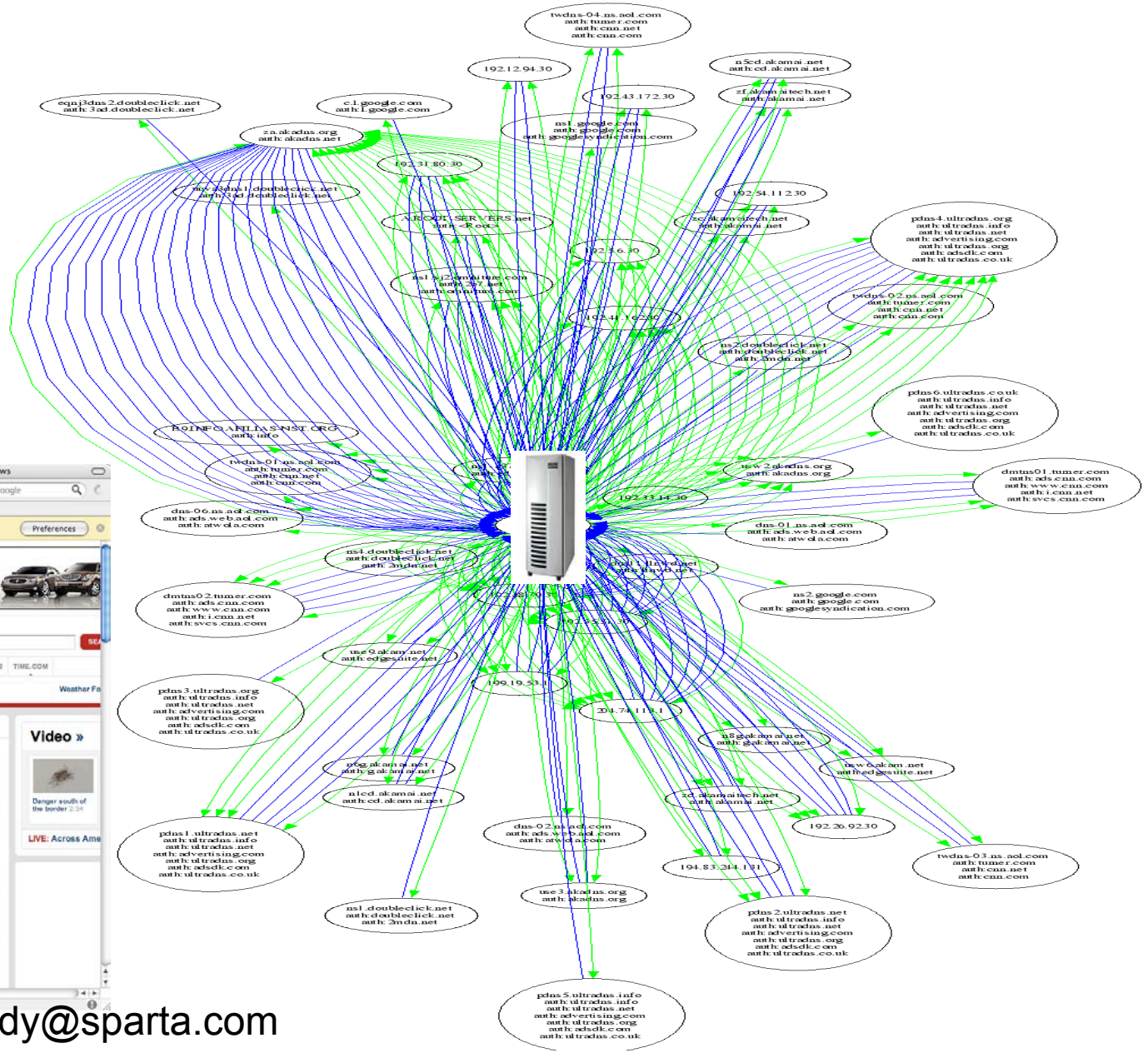
russ.mundy@sparta.com

Name Resolution



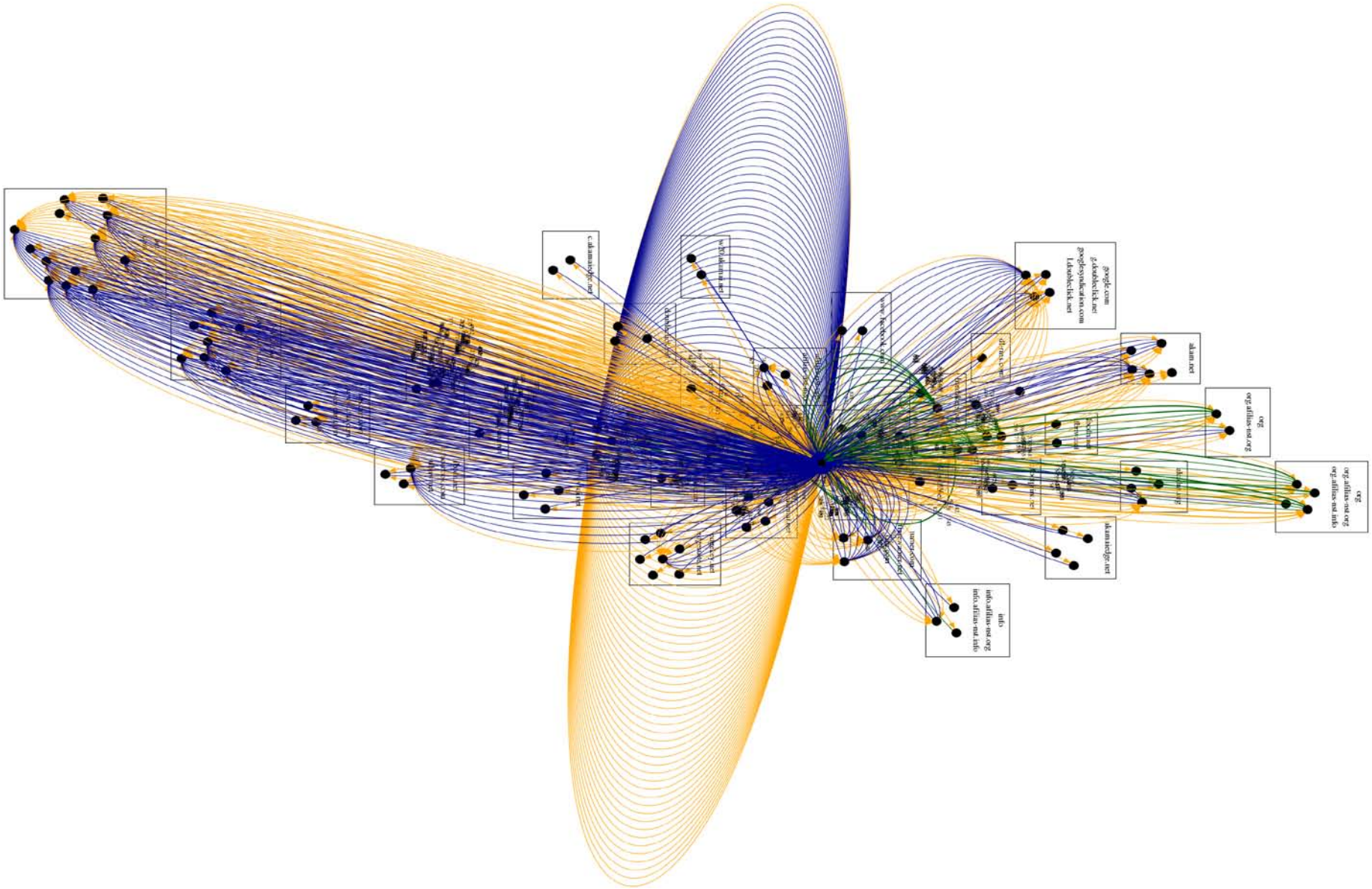
1 Webpage = Multiple DNS Name Resolutions





russ.mundy@sparta.com

www.cnn.com



DNS Basic Functions

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

➢ IT'S **DNS ZONE DATA** THAT MATTERS!

russ.mundy@sparta.com

How Does DNSSEC Fit?

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

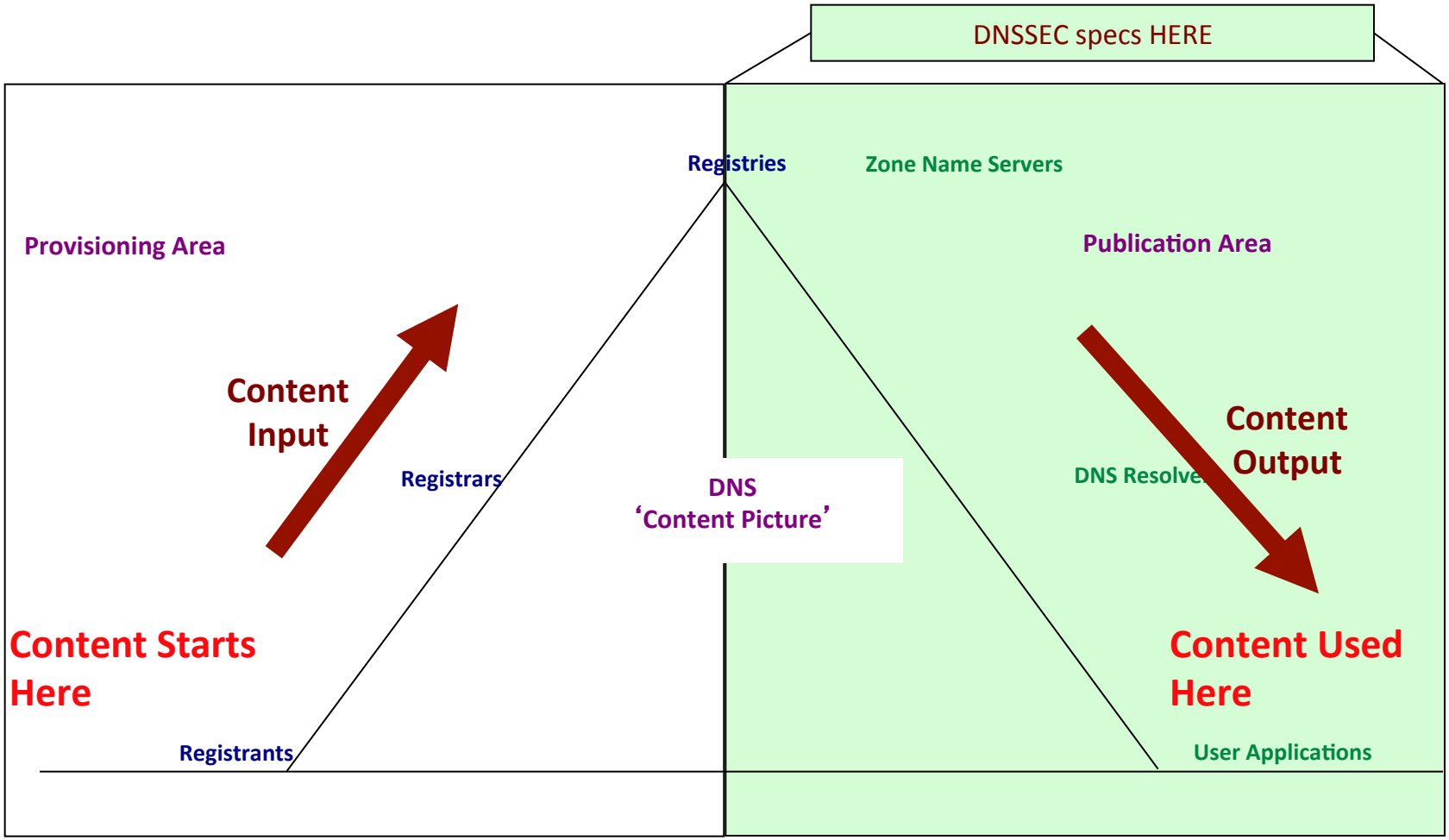
➢ Protect **DNS ZONE DATA** as much as (or more than) any DNSSEC information

  ➢ Including DNSSEC private keys!!

russ.mundy@sparta.com

DNS Zone Content Flow

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



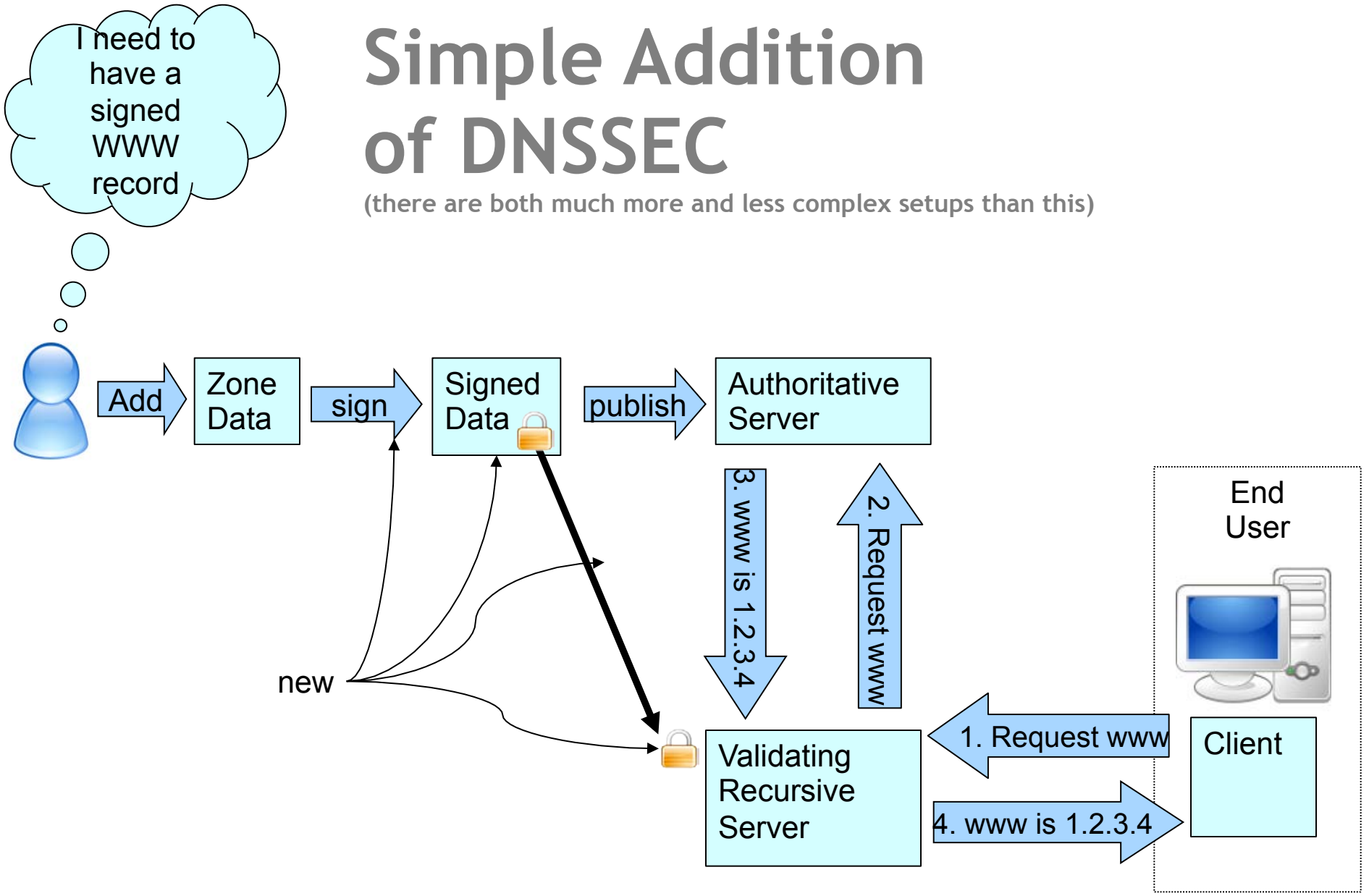
russ.mundy@sparta.com

Implementation Samples

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

Simple Addition of DNSSEC

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



russ.mundy@sparta.com

Implementation Samples

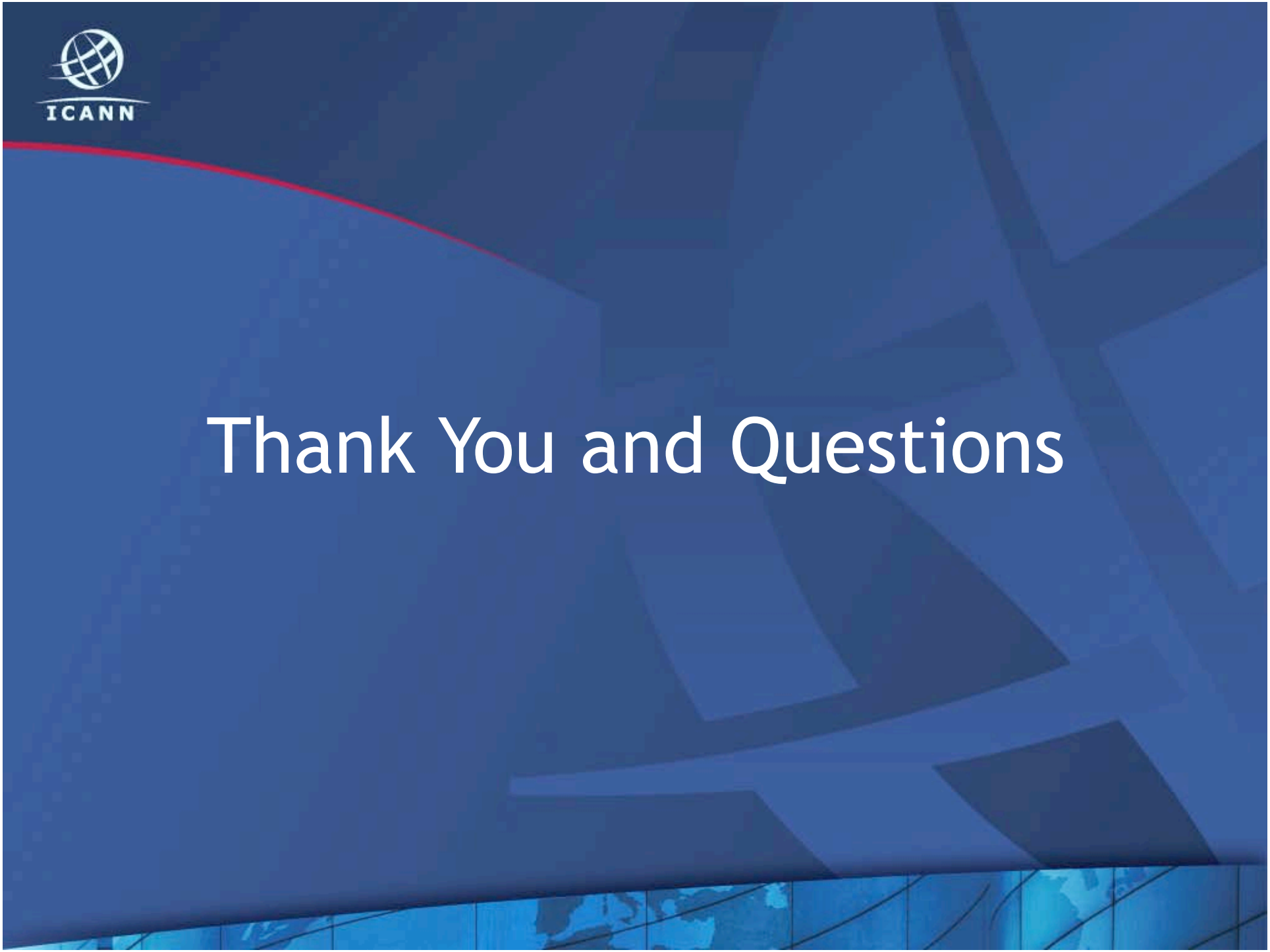
- If you're running much or all of your DNS functions and operations, DNSSEC implementation could be based on:
  - Extend DNS operation to incorporate DNSSEC;
  - Use open source DNSSEC tools (e.g., from www.dnssec-tools.org or opendnssec.org);
  - Use commercial DNSSEC products;
  - Use DNSSEC signing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


ICANN
Thank You and Questions