## The Schedule

<table>
<thead>
<tr>
<th>Outline Concept</th>
<th>Segment</th>
<th>Duration</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Welcome and Introduction</td>
<td>2 mins</td>
<td>Simon</td>
</tr>
<tr>
<td></td>
<td>Caveman – DNSSEC 5000BC</td>
<td>3 mins</td>
<td>Simon</td>
</tr>
<tr>
<td>Basic Concepts</td>
<td>DNS Basics</td>
<td>5 mins</td>
<td>Roy/Matt</td>
</tr>
<tr>
<td></td>
<td>DNS Chain of Trust - Live</td>
<td>5 mins</td>
<td>Norm</td>
</tr>
<tr>
<td>Core Concepts</td>
<td>DNSSEC – How it works</td>
<td>10 mins</td>
<td>Roy/Matt</td>
</tr>
<tr>
<td></td>
<td>DNSSEC – Chain of Trust Live</td>
<td>5 mins</td>
<td>Norm</td>
</tr>
<tr>
<td>Real World Examples</td>
<td>A sample DNSSEC implementation (what it looks like, s/w etc). A simple guide to deployment.</td>
<td>10 mins</td>
<td>Russ</td>
</tr>
<tr>
<td></td>
<td>A guide to DNSSEC Deployment options: Technologies and vendors.</td>
<td>10 mins</td>
<td>Russ</td>
</tr>
<tr>
<td>Summary</td>
<td>Session Round up, hand out of materials, Thank you’s</td>
<td>2 mins</td>
<td>Simon</td>
</tr>
</tbody>
</table>
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
So Ugwina sets off down the canyon to try and sort out the mess...
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...
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
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

root

uk

com

cr

bigbank.com (www)
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

- root
- uk
- com
- cr
- bigbank.com (www)
- ✗ bigbank.com (www)
A Sample DNSSEC Implementation & Guide to Deployment Options

Russ Mundy, Cobham
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)
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)

Content Starts Here

Content Input

Provisioning Area

Content ‘Content Picture’

Registries

Zone Name Servers

Publication Area

Content Used Here

Content Output

User Applications
Simple Illustration of DNS Components

I need to have a WWW record

1. Request www
2. Request www
3. www is 1.2.3.4
4. www is 1.2.3.4

Add Zone Data

publish

Authoritative Server

Recursive Server

End User

Client

russ.mundy@cobham.com
Name Resolution

Root Name Servers
root-servers.net

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

www.cnn.com IP?

Recursive Name Server
cnn.com name servers

www.cnn.com IP?

Internet User

HTTP request
HTTP response

www.cnn.com IP

www.cnn.com IP

www.cnn.com IP

www.cnn.com IP
1 Webpage = Multiple DNS Name Resolutions
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@cobham.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!!
DNS Zone Content Flow
(for example, www.icann.org or www.cnn.com)

Provisioning Area

Content Starts Here

Registries

Zone Name Servers

Publication Area

DNS Resolvers

Content Used Here

Content Output

DNS ‘Content Picture’

DNS Resolvers

User Applications

russ.mundy@cobham.com
Simple Addition of DNSSEC
(there are both much more and less complex setups than this)

I need to have a signed WWW record

Add Zone Data Sign Published

Authoritative Server

Validating Recursive Server

End User

1. Request www
2. Request www
3. www is 1.2.3.4
4. www is 1.2.3.4

russ.mundy@sparta.com
Implementation Samples

• In general, try to do DNSSEC in the same way that you are doing DNS
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
Thank You and Questions