

**INTERCONNECT  
COMMUNICATIONS**



## **MC / 080:DNSSEC Deployment Study**

**Final Report**

**Merlin House  
Chepstow  
NP16 5PB  
United Kingdom**

**Telephone: +44 1291 638400  
Facsimile: +44 1291 638401  
Email: [info@icc-uk.com](mailto:info@icc-uk.com)  
Internet: [www.icc-uk.com](http://www.icc-uk.com)**



**INTERCONNECT COMMUNICATIONS**  
A Telcordia Technologies Company

## Notice

This document is provided in good faith and is based on InterConnect's understanding of the recipient's requirements. InterConnect would be pleased to discuss the contents of this document particularly if the recipient's requirements have in any way changed.

InterConnect is a wholly owned subsidiary of Telcordia Technologies Inc.

All rights reserved.

Copyright © InterConnect Communications Ltd, 2011

InterConnect Communications Ltd  
Merlin House  
Station Road  
Chepstow  
NP16 5PB  
United Kingdom

Telephone: +44 1291 638400

Facsimile: +44 1291 638401

[www.icc-uk.com](http://www.icc-uk.com)

Persons to contact in relation to this document:

Brian Aitken  
Business Development Executive  
DDI: +44 (0) 1291 638426  
Fax: +44 (0) 1291 638401  
Email: [brianaitken@icc-uk.com](mailto:brianaitken@icc-uk.com)

## Contents

<b>1. EXECUTIVE SUMMARY</b> .....	<b>5</b>
<b>2. SECURING THE DNS</b> .....	<b>6</b>
2.1 SECURING THE INFRASTRUCTURE OF THE INTERNET .....	6
2.1.1 <i>Technical implications</i> .....	6
2.1.2 <i>Public Policy implications</i> .....	7
2.2 THREATS TO THE DNS.....	7
2.2.1 <i>Threats to the Platform</i> .....	8
2.2.2 <i>Threats in the DNS Hosting Context</i> .....	8
2.2.3 <i>Threats related to DNS Queries and Transactions</i> .....	8
<b>3. DNSSEC – AN OVERVIEW</b> .....	<b>10</b>
3.1 WHAT DOES DNSSEC DO?.....	10
3.2 WHAT DOES DNSSEC NOT DO? .....	10
3.3 HOW DOES DNSSEC WORK?.....	10
3.3.1 <i>Public Key Cryptography</i> .....	11
3.3.2 <i>Digital Signatures</i> .....	11
3.3.3 <i>Extending the DNS</i> .....	12
3.3.4 <i>The DNSSEC Chain of Trust and the DS Record</i> .....	14
3.4 DEPLOYMENT ALTERNATIVES.....	15
<b>4. BARRIERS TO DNSSEC DEPLOYMENT</b> .....	<b>17</b>
4.1 BARRIERS TO DNSSEC DEPLOYMENT .....	17
4.2 DEPLOYMENT BARRIERS AT HOSTING COMPANIES AND ISPS.....	17
4.2.1 <i>Real versus perceived barriers</i> .....	17
4.2.2 <i>Technical barriers</i> .....	18
4.2.3 <i>Economic Barriers</i> .....	18
4.2.4 <i>DNSSEC CAPEX and OPEX</i> .....	20
4.3 DEPLOYMENT BARRIERS AT END USER SITES .....	20
4.4 DEPLOYMENT BARRIERS IN CONSUMER BROADBAND NETWORKS .....	21
4.5 THE “BOOTSTRAP PROBLEM” FOR DNSSEC .....	21
<b>5. DNSSEC DEPLOYMENT – A GLOBAL PERSPECTIVE</b> .....	<b>23</b>
5.1 STATISTICS AND HISTORY.....	23
5.2 STATISTICAL PATTERNS OF DNSSEC ADOPTION IN THE ROOT.....	23
<b>6. DNSSEC DEPLOYMENT – A G20 PERSPECTIVE</b> .....	<b>26</b>
6.1 REVIEW OF DNSSEC ADOPTION OF LEADING COMMERCIAL SITES .....	27
6.2 COMPARISON OF DNSSEC ADOPTION AMONGST CCTLDS VERSUS GTLDS.....	28
<b>7. DNSSEC DEPLOYMENT – A EUROPEAN PERSPECTIVE</b> .....	<b>30</b>
7.1 EARLY ADOPTIONS .....	30
7.2 DNSSEC ADOPTION IN EUROPE IN MID-2011 .....	33
7.3 NSEC AND NSEC 3 IN EUROPE .....	33
7.4 BEYOND SIGNING CCTLDS -- DEPLOYMENT WITHIN CCTLDS.....	35
7.5 DO EUROPEAN DNS CLIENTS REQUEST SECURITY INFORMATION?.....	35

<b>8.</b>	<b>DNSSEC DEPLOYMENT – THE UK PERSPECTIVE .....</b>	<b>37</b>
8.1	IMPLICATIONS OF A STRUCTURE SECOND-LEVEL NAMESPACE .....	37
8.2	HISTORY AND CONTEXT FOR SIGNING .UK .....	37
8.2.1	<i>NSEC3 and Zone Walking in ccTLDs .....</i>	<i>37</i>
8.2.2	<i>Legal and policy issues related to .UK zone enumeration.....</i>	<i>37</i>
8.2.3	<i>Nominet’s Advocacy of DNSSEC.....</i>	<i>38</i>
8.3	RELATIONSHIP BETWEEN UK REGISTRY AND REGISTRARS .....	38
8.4	HISTORY AND CONTEXT FOR SIGNING THE SECOND-LEVEL UNDER .UK .....	39
8.5	CORPORATE ADOPTION OF DNSSEC IN THE UK .....	40
8.5.1	<i>Previous Approaches to DNSSEC in the UK .....</i>	<i>40</i>
8.5.2	<i>Corporate adoption of DNSSEC in public facing DNS .....</i>	<i>42</i>
8.5.3	<i>Support for DNSSEC Adoption by UK Registrars.....</i>	<i>42</i>
<b>9.</b>	<b>ISSUES FOR CONSIDERATION – WHAT CONSTITUTES SUCCESS? .....</b>	<b>43</b>
<b>10.</b>	<b>ISSUES FOR CONSIDERATION – ARE INCENTIVES REQUIRED FOR GREATER DEPLOYMENT?.....</b>	<b>43</b>
<b>11.</b>	<b>APPENDIX A: REVIEW OF THE STATE OF DNSSEC STANDARDS AT THE IETF .....</b>	<b>45</b>
11.1	ESTABLISHED STANDARDS .....	45
11.1.1	<i>Domain Name System Security Extensions (RFC 2535) .....</i>	<i>45</i>
11.1.2	<i>Domain Name System Security Signing Authority (RFC 3008).....</i>	<i>45</i>
11.1.3	<i>Indicating Resolver Support for DNSSEC (RFC 3225) .....</i>	<i>45</i>
11.1.4	<i>DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format (RFC 3845) .....</i>	<i>45</i>
11.1.5	<i>Resource Records for the DNS Security Extensions (RFC 4034) .....</i>	<i>46</i>
11.1.6	<i>Protocol Modifications for the DNS Security Extensions (RFC 4035) .....</i>	<i>46</i>
11.1.7	<i>Minimally Covering NSEC Records and DNSSEC On-line Signing (RFC 4470).....</i>	<i>46</i>
11.1.8	<i>Use of SHA-256 in DNSSEC Delegation Signer (DS) Records (RFC 4509).....</i>	<i>46</i>
11.1.9	<i>DNS Security (DNSSEC) Opt-In (RFC 4956).....</i>	<i>47</i>
11.1.10	<i>DNSSEC Hashed Authenticated Denial of Existence (RFC 5155) .....</i>	<i>47</i>
11.1.11	<i>Use of SHA-21 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC (RFC 5702)</i>	<i>48</i>
11.2	INTRODUCTIONS, OPERATIONAL ADVICE AND OTHER DOCUMENTS.....	48
11.2.1	<i>DNS Security Operational Considerations (RFC 2541) .....</i>	<i>48</i>
11.2.2	<i>A Threat Analysis of the Domain Name System (RFC 3833) .....</i>	<i>48</i>
11.2.3	<i>DNS Security Introduction and Requirements (RFC 4033) .....</i>	<i>48</i>
11.2.4	<i>DNSSEC Operational Practices (RFC 4641) .....</i>	<i>49</i>
11.2.5	<i>DNS Security (DNSSEC) Experiments (RFC 4955) .....</i>	<i>49</i>
11.3	EMERGING CHANGES TO DNSSEC .....	49
11.3.1	<i>Client Signalling of Encryption Capabilities .....</i>	<i>49</i>
11.3.2	<i>DNSSEC Policy and Practice Statement Framework .....</i>	<i>49</i>
11.3.3	<i>Revision of DNSSEC Operational Practices .....</i>	<i>49</i>
<b>12.</b>	<b>APPENDIX B: GLOSSARY OF TERMS AND ACRONYMS.....</b>	<b>50</b>

## 1. Executive Summary

This report, in response to Ofcom's MC/080 DNSSEC Deployment Study, was asked to address four major issues.

- 1. Provide a comparison of the UK's progress and extent deployment of DNSSEC against other EU member states and G20 nations.** In May of 2011, during work on this report, Nominet signed the second-level namespace for .UK. This important development makes it possible for any .UK domain name holder to establish a Chain of Trust that authenticates and protects answers to queries on the DNS. The UK is the second largest Country Code Top Level Domain (ccTLD) in Europe and is now ready for wide-scale production deployment of DNSSEC for .UK domain holders. Amongst G20 nations, the UK is also the second largest of the signed zones ready for production and is one of only seven of the G20 ccTLDs to have a production-ready, signed zone.
- 2. Examine Nominet's progress against that of other national registries in the deployment of DNSSEC.** Nominet has been a leader in supporting the specification and deployment of DNSSEC. The registry has made investments in staff and other resources to aid in the general deployment of DNSSEC. Other national registries have done earlier deployments of DNSSEC, but given the size (second largest ccTLD in the world) and complexity (a structured second-level domain space), Nominet wisely adopted a cautious approach in their deployment. While .UK and its second level are now signed and in production, the true test of Nominet's progress will be in how well registrars' and end users' DNSSEC needs – including services, education and outreach – are met in the future. Nominet also wisely adopted a DNSSEC technology that was sensitive to privacy issues – avoiding a public policy issue that remains a concern in other national contexts.
- 3. Establish if any barriers to DNSSEC deployment exist (e.g. technical or economic)** DNSSEC is a complex protocol to deploy and support. It involves far more than taking an existing DNS Server and “adding a feature.” The complexity and potential side-effects on network engineering and performance have made some organizations reluctant to invest in or deploy DNSSEC. However, many perceived technical barriers have been overcome through better education. The crucial barrier to DNSSEC deployment in the UK is an economic and commercial one: lack of concrete demand in commercial settings. The UK is now in a position to see if a small set of early adopters will lead to the critical mass necessary for ISPs, hosting companies and registrars to begin offering DNSSEC related services and products.
- 4. Identify barriers or issues preventing adoption and deployment by UK hosting providers, Internet Service Providers and businesses** The biggest barrier to DNSSEC deployment is the inability to quantify the benefit gained by its deployment. In interviews, ISPs and other hosting companies all say that there is no customer demand for DNSSEC. While they understand the benefit for authenticating DNS queries, they have no economic justification for its development or deployment. With the signing of the second-level domain for .UK one of the biggest barriers to deployment has been removed. What should emerge next in the UK are a series of services and offerings that remove the remaining technical and administrative barriers to the use of DNSSEC. The UK does not suffer from a problem that other nation states experience: catastrophically outdated equipment and software versions.

## 2. Securing the DNS

### 2.1 Securing the Infrastructure of the Internet

Today's Internet is on a scale and scope unimaginable to those who framed it.

The Internet originated within the US Defence Advanced Research Projects Agency in the 1960s. It was brought from concept into operation through a loose collaboration of researchers and engineers within academia, government research units, and telecommunications companies. In an environment where the early actors knew and trusted each other, where there was no commercial use, and therefore no incentive to do harm on a large scale, the Internet evolved without built-in security.

The ground rules upon which the early Internet protocols were based help to explain why. The idea was that networks could be of arbitrary design, and would not require internal changes in order to connect to the network; communications would be on a best-effort basis; and there would be no global control at the operations level<sup>1</sup>.

There was no business plan and no driving intention to make money from the network. Instead “those individuals thinking about the Internet in the 1960s and ‘70s planned a network that would cobble together existing research and government networks and then wring as much use as possible from them.”<sup>2</sup>

This is in contrast to proprietary early networks, such as AOL and CompuServe, which needed to identify their users in order to bill them. With user identification, came accountability – if someone misused the proprietary network, they could be thrown off it. However, those proprietary networks declined, as the market preferred the utility, flexibility and freedom afforded by the Internet.

The success of networking was not guaranteed. As late as 1992, IBM was famously quoted as saying “you cannot build a corporate network on TCP/IP” [the underlying Internet protocol].

#### 2.1.1 Technical implications

A fundamental assumption underlying the Internet's evolution is trust. Its early users were also its creators, who knew each other, and the vulnerabilities were seen as technical rather than malfeasance: “the most serious problems in the Internet have been caused by unenvisaged mechanisms triggered by low probability events; mere human malice would never have taken so devious a course.”<sup>3</sup>

---

<sup>1</sup>Leiner, B., et al, A Brief History of the Internet <http://www.isoc.org/internet/history/brief.shtml>.

<sup>2</sup>Zittrain, J., The Future of the Internet and How to Stop it, 2008.

<sup>3</sup>RFC 1122, Braden, R., 1989, IETF.

The Domain Name System (DNS) is not alone in having no built-in security, or user authentication: “the assumption that network participants can be trusted...infuses the Internet’s design at nearly every level.”<sup>4</sup>

### 2.1.2 Public Policy implications

The Internet does not conform to classic regulatory norms. In contrast to broadcast or telecommunications, there is no concept of a licensed operator in most countries, including the UK, and more significantly (absent national legislation) there was no legal or legislative basis (at that time) for any would-be licensor or regulator. For this reason, the UK Government in 2004 chose not to run a public auction for the UK ENUM Tier 1 operator, because “the concept of ownership or rights of use [in relation to ENUM or the domain name system] is not sufficiently clearly established as belonging to the national government.”<sup>5</sup>

The relevance of this to the security protocol for the Domain Name System, DNSSEC, is the legitimacy of the “trust anchor”. In order for an individual domain name to be “signed” or trusted, there needs to be an unbroken chain of trust from the domain name, through the Top Level Domain (TLD) registry (eg .uk or .com) up to the root database, or IANA, operated by ICANN under contract with the US Government.

For many years, the root remained unsigned, partly because it was unclear *who should sign it*. Potential candidates were the root operator, VeriSign (a US for-profit corporation), ICANN (the non-profit, private sector organisation which coordinates Internet naming and numbering) and the United States Government, which reviews and authorizes every change to the DNS root zone. Politically, any of the options, especially the latter, would have been unacceptable to a wide range of stakeholders.<sup>6</sup>

This was resolved in 2009, by a quiet, salami-slice approach which avoided the overt involvement of the US Government. The root zone was signed for internal use by VeriSign (the “A” root operator) and ICANN. ICANN published the root zone trust anchor in June 2010<sup>7</sup>. This paved the way for the rollout of DNSSEC.

## 2.2 Threats to the DNS

The DNS is a critical piece of the Internet’s infrastructure and makes a natural target for people and organizations attempting to abuse the Internet. Threats to the DNS take many forms. Some threats are attacks on the zone files and servers that make up the infrastructure of the DNS. Others are attacks on the information that moves between resolvers and servers in the

---

<sup>4</sup>Zittrain (2008)

<sup>5</sup> DTI, “ENUM, Consultation on the Proposed Arrangements” August 2004, para 4.8, p 17, [www.bis.gov.uk/files/file29328.pdf](http://www.bis.gov.uk/files/file29328.pdf)

<sup>6</sup> The United Nations’ World Summit on the Information Society, 2003-2005 brought to the fore international tensions relating to the role of the US Government in overseeing (or managing) the root zone of the Domain Name System. See Carl Bildt, 2005 <http://bildt.blogspot.com/2005/10/european-union-iran-saudi-arabia-cuba.html>

<sup>7</sup> See High Level timeline at <http://www.root-dnssec.org/>

DNS. To understand DNSSEC – and what it can and cannot provide – a basic understanding of the threats to the DNS is important.

The DNS is subject to security problems in three key areas: confidentiality, integrity and availability. For the purposes of this work a loss of confidentiality is the unauthorized disclosure of or access to information. A loss of integrity is the unauthorized modification or destruction of information. And a loss of availability is the disruption of access to the underlying service. DNSSEC is not an extension that provides tools for ensuring confidentiality or availability. Instead, its goal is to ensure integrity.

### **2.2.1 Threats to the Platform**

Modern DNS service provision is much different than the ancient, one-server, one-IP address, unicast service of ten years ago. Today's DNS services are provided in a geographically dispersed, topologically complex anycast environment. Despite this, the underlying platforms remain vulnerable to problems associated with the underlying operating system, the network stack supporting the servers, the DNS software itself and problems with the repository of data that serves either as the configuration tool or the zone files themselves.

For the purposes of a discussion of DNSSEC, threats to the actual server platform are out of scope. Most of these threats are not specific to the DNS, but instead are common to all hosts on the Internet.

The two main platform threats that are specific to the DNS are attacks on the DNS software itself and on the repositories that the DNS uses to provide its services.

Operators of DNS services are careful to ensure that the DNS software they use run on platforms that can be made secure from unauthorized access. The platforms must be hardened against brute force Denial of Service Attacks while remaining robustly available.

### **2.2.2 Threats in the DNS Hosting Context**

#### **Inherent weaknesses in DNS Server Software**

All software suffers from potential problems with its configuration and operation. DNS server software has historically fought against problems such as buffer overflows that result in either denial of server or access to privileged control of the DNS Server itself.

#### **Denial of Service Attacks**

Among the most famous of the attacks on the DNS, these attacks attempt to make a DNS Server, group of servers, or authoritative server unavailable. The result can be that all the services, for which the DNS server is authoritative for are no longer available. Most modern DNS servers and their host platforms are hardened against these types of attacks.

### **2.2.3 Threats related to DNS Queries and Transactions**

#### **DNS Cache Poisoning**

Long a well-known threat to the DNS, DNSSEC is built to expressly forbid Cache Poisoning. The DNS is built to “remember,” or cache, responses to queries in order to improve

performance. If the cache is attacked in a way that allows the cache to be corrupted with malicious but otherwise well-formed data then the compromised cache will be used until the bad entries time out. If an attacker puts an unusually large value on the Resource Record's Time to Live parameter, the compromised information will remain in the cache waiting to be served to unwitting victims for a significant period of time.

### **Packet Interception**

If a malicious server is able to insert itself in the data path between client and server, it has the potential to eavesdrop on requests from the client and send malicious responses by pretending to be an authoritative name server before the legitimate server can respond.

### **Resource Record Removal**

An attacker may also be able to put itself in the data path between client and server and rather than injecting forged responses, simply remove Resource Records which form the response. The result could be DNS query resolution failure and a possible denial of service on the resources being queried for.

### **Spoofing of DNS responses**

The DNS has a built-in mechanism that allows servers to make multiple upstream queries in order to resolve a DNS query. If the DNS server is fooled into believing that it is receiving a response from a trusted DNS server when, in fact, it is being attacked, we refer to that attack as a spoofing attack. The strategy is to have the malicious server listen for DNS queries and then attempt to guess the parameters needed to insert a reply of its own choosing. In older versions of DNS Server software the guessing was made easier by having the software choose sequential numbers for the identification numbers of the queries. Modern software randomizes the port number and sequence number to avoid this attack.

### **Kaminsky Attack**

A very famous recent attack that takes advantage of the fact that the DNS only uses 65,536 possible transactions IDs, a trivial amount to inject toward a valid DNS Server. Kaminsky was not the first to exploit or identify the attack strategy, but was the first to describe an attack that bypassed all, then, current defences. Most defences used by DNS Servers today against the Kaminsky are fairly fragile. Kaminsky himself supports the use of DNSSEC as a defend against this sophisticated attack.

### **3. DNSSEC – An Overview**

#### **3.1 What does DNSSEC do?**

Fundamentally, DNSSEC solves two crucial problems related to the DNS. The original design of the DNS was almost completely focused on data availability – as we have seen, there was no security component at all in the original design.

DNSSEC is focused on two things:

1. Authentication of the data provided by the DNS; and,
2. The ability to check the validity of the data provided by the DNS.

DNSSEC is a backward compatible technology that extends the DNS by providing origin authentication of DNS data, data integrity and, where needed, authenticated denial of existence of domain name and resource records.

#### **3.2 What does DNSSEC not do?**

It is important to understand that DNSSEC does not solve all of the security problems related to the DNS.

DNSSEC does not provide confidentiality of DNS responses or communications between DNS clients and servers. It also does not prevent attacks on DNS servers using other parts of the network stack – for instance, implementation of DNSSEC does not protect against distributed denial of service attacks or IP spoofing.

DNSSEC does not provide authorization or control over who can use services.

Importantly, DNSSEC does not address privacy issues related to the DNS.

#### **3.3 How does DNSSEC work?**

In essence, DNSSEC uses cryptography to provide authentication and integrity information about DNS data.

The Internet relies on the ability of people and computers interacting at a distance. A customer may not have ever seen or met the principals of an Internet business but they still have to be able to exchange information. How does that customer know for sure that the information sent from the business was really sent from that business and not an imposter? In the real world we have many physical clues and cues that guide our application of trust to transactions. Most of these physical clues are simply not available on the Internet.

One of the keys to building private and reliable communications between people, businesses and organizations on the Internet is to use cryptography. Many types of cryptography are in use in the public Internet, but DNSSEC uses a very specific type: public key cryptography.

### 3.3.1 Public Key Cryptography

Essentially, public key cryptography was intended to be a secure, easy-to-deploy method for ensuring that messages and transactions can be changed into a form that can only be read by the intended recipient.

Each person, business or organization gets two "keys." One, the "public key" is given to all possible recipients and made public. The other, the "private key," is kept secret and in the hands of the sender. Messages encrypted with the "public" key can only be decrypted with the matching private key. So, when I want to send a secret message to you I simply encrypt the message using your public key. Because the only person who can decrypt the message is the person who has the matching private key, it doesn't matter who intercepts the message. Even if someone could get a copy of the encrypted message, they couldn't decode it because they wouldn't have the matching private key.

This strategy for protecting messages on the Internet has wide use in technologies such as SSL, TLS, PGP and VPNs. But it also has two other features that are of special importance to DNSSEC.

### 3.3.2 Digital Signatures

One of the features of Public Key Cryptography that is of special importance is Digital Signatures. Simply put, if I use my private key to generate a signature of a document or encrypt a message, you can verify that it was truly me by verifying the signature against my public key. As with protecting the confidentiality of messages, the digital signature relies on the essential property of the key pair: messages signed with the private key can only be verified using the matching public key.

The signature that is created using the digital signing algorithm verifies the authenticity of that message. Put more simply, the digital signature guarantees that the sender of the message is who they say they are.

Digital signatures have three important properties:

- **AUTHENTICATION**--digital signatures are regularly used to authenticate the true source of messages. When a private key is used to sign a message, a valid signature indicates that the message was sent by the holder of the private key. This ensures sender authenticity.
- **INTEGRITY**-- besides being confident that the message came from who purported to send it, it is also important to ensure that the message has not been altered in any way during transmission. We often refer to this as "data integrity." A digital signature can ensure that the message was received just as it was sent: if a message is digitally signed, any change in the message after it was signed would invalidate the signature.
- **NON-REPUDIATION**-- if a sender has signed some information, they cannot, at a later time, deny having signed it. In the same way, just because a person has access to a public key of some user, there is no way to use that public key to forge a valid signature.

DNSSEC makes essential use of the first two of these properties of digital signatures. The fundamental feature that DNSSEC provides is ***to guarantee that the answer received as a result of a DNS query is exactly the answer that corresponds to the authoritative state of the DNS records related to that query.***

### 3.3.3 Extending the DNS

DNSSEC is an extension to the DNS. Fundamentally, it adds records to the DNS that can be used by DNS clients to validate the authenticity and integrity of an answer to a DNS query. Where a DNS server must indicate that it has no records with which to respond to a query, DNSSEC provides a way for this "negative answer" to be authenticated as well.

To accomplish this DNSSEC adds a set of new DNS resource records:

- DNSKEY
- RRSIG
- NSEC
- DS

#### The DNSKEY Resource Record

Every zone file that is secured by DNSSEC has a public and private key pair. The administrator of the zone is responsible for keeping the private key secret. However, in order to check the signature on the zone data, DNS clients must be able to get a copy of the matching public key. As a result, the public key is published in the DNS using DNSSEC's DNSKEY resource record. Here is an example taken from the documents that defined DNSSEC

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
    Cbl+BBZH4b/0PY1kxkmvHjcZc8no
    kfzj31GajIQKY+5CptLr3buXA10h
    WqTkF7H6RfoRqXQeogmMHfpftf6z
    Mv1LyBUgia7za6ZEzOJB0ztyvhjL
742iU/TpPSEDhm2SNKLi jFUpn1U
    aNvv4w== )
```

The Time to Live value is 1 day (86400 seconds). Time to Live is a value that controls how long any nameserver is allowed to cache the information that it may acquire in a query. The Flags value is 256, indicating that this is a Zone Key. The protocol value is a constant number: 3. The following field is the identifier for the public key algorithm, and the value 5 indicates RSA/SHA1. The RR value is simply the encoding of the public key that the client will use to validate the signed zone.

#### The RRSIG Resource Record

A Resource Record Set is a collection of resource records in a DNS Zone file that have a common name, class and type. In practice this means that there would be a resource record set associated with each part of a DNS query response. Another way to say this is that the RRSIG is the Zone Administrator's private key applied to the part of the zone requested by the client: a digital signature for the Resource Record Set. In a typical zone with SOA, NS, A MX and

## MC/080 DNSSEC Deployment Study

DNSKEY resource records there would be five separate resource record sets, each with a separate RRSIG record. Here is an example of a RRSIG from the documents that defined DNSSEC

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
20030220173103 2642 example.com.
  oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
  PYGv07h108dUKGMeDPKi jVCHX3DDKdfb+v6o
  B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rzn1803t
  GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
  J5D6fwFm8nN+6pBzedQfsS3Ap3o= )
```

The zone name is followed by the Time to Live value and the Class field. RRSIG indicates the resource record type. These four fields are followed by a "Type Covered" field which indicates that this is a signing of the A resource records in "host.example.com". The next field indicates the name of the algorithm used to sign the resource record set. The number "3" indicates that there are three labels in the original zone name (in this case, "host," "example," and "com."). The next field (86400) indicates the original Time to Live value for the covered A resource record set. Following that are date stamps indicating when the resource record set was signed and when the signature expires. The key tag is 2642 and the signer's name is "example.com". The rest of the RR value is the digital signature of the resource record set.

The DNSKEY and the RRSIG can be used to check the authenticity and the integrity of a DNS response. But only when there is a response! What happens when there is no data to return?

### The NSEC Resource Record

The NSEC record was created so that something could be returned in the event the resource requested does not exist. When a client makes a DNS query and either the name does not exist, or if the resource record type requested does not exist, the NSEC record is returned as a negative answer: a digitally signed indication that the name or resource record was not found.

Effectively the NSEC record is a way for the DNS server to bridge the gap between names in a secured zone. The strings in a zone file are sorted and then NSEC records are put in place to cover the gaps between the strings in the zone. If the zone contained the names "here" and "there" then there would be a NSEC record for "here" and its value would be "there" indicating that there are no defined names in the list of possible names between "here" and "there". Here is an example of a NSEC record from the RFC that created DNSSEC

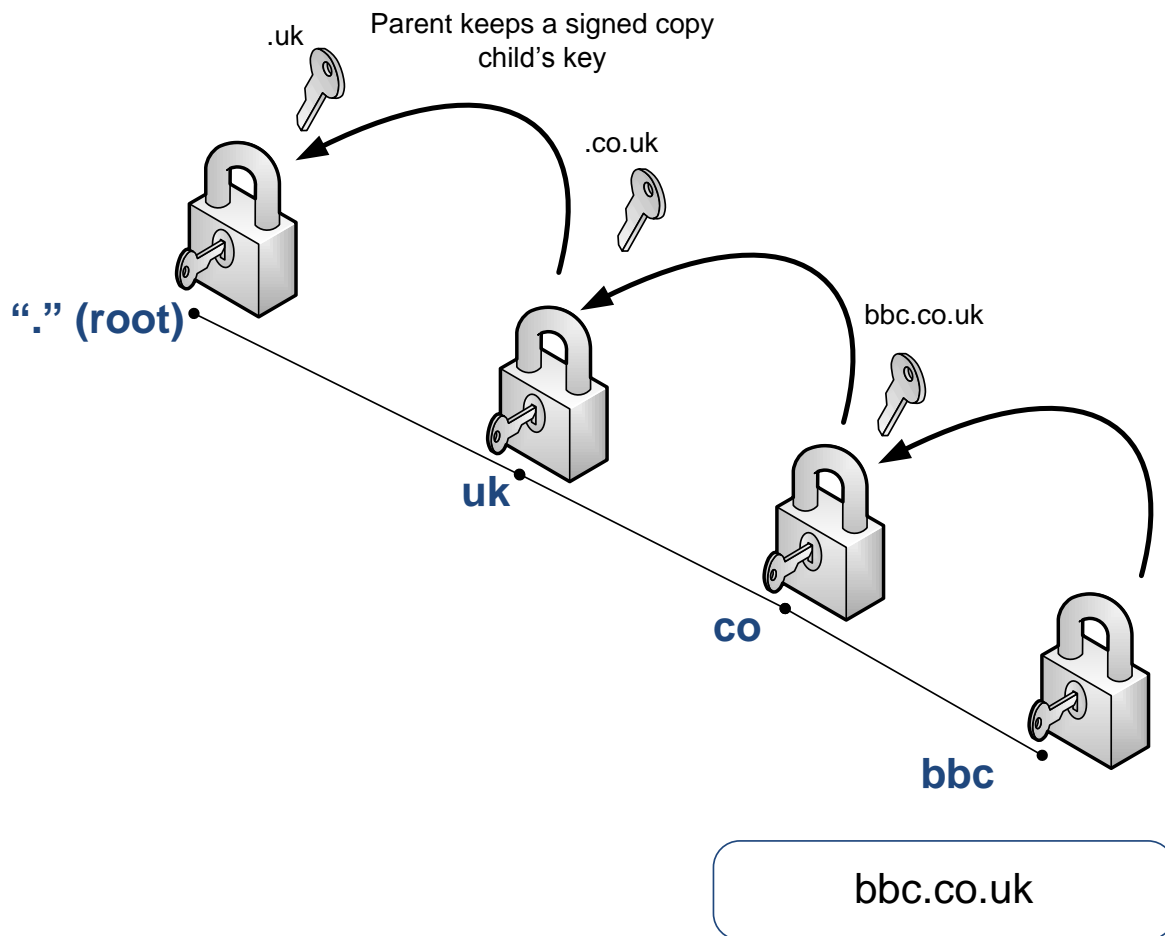
```
alfa.example.com. 86400 IN NSEC host.example.com. (
  A MX RRSIG NSEC TYPE1234 )
```

As before, the first four fields specify the name, Time to Live, Class and Resource Record type (this time, NSEC). This record then indicates that the next name, in sorted order, after "alfa.example.com" in the zone is "host.example.com". The codes "A" "MX" "RRSIG" "NSEC" and "TYPE1234" indicate that there are "A" "MX" "RRSIG" "NSEC" and "TYPE1234" resource records associated with the name alfa.example.com. One implication of this is that, by collecting the information from the NSEC records, we can enumerate the entire contents of a DNS zone. We'll come back to this important implication when we discuss the NSEC3 record in Section 7.3 of this report.

### 3.3.4 The DNSSEC Chain of Trust and the DS Record

There needs to be a way to validate the public key held in the DNSKEY record. Otherwise, an attacker could simply intercept the DNS query responses, sign the records with their own private key and substitute their public key to make the DNS query look authentic (even though it had now been corrupted by the attacker). So the question is: how can a DNS client ensure that the DNSKEY record it retrieved is valid? DNSSEC solves this problem through a "chain of trust" in the DNS.

Except for the root zone, every zone has a parent. For instance, ".co.uk" is the parent zone of ".bbc.co.uk" and ".uk" is the parent zone of ".co.uk"



To solve the problem, the parent zone keeps a signed copy of the child zone's public key. The parent zone signs this copy with its own private key and then publishes both the copy and a matching RRSIG record resource record. In essence, the public key of a zone is signed by a "higher authority" – the parent.

### The DS Resource Record

To prove that a zone file's DNSKEY is truly authentic, the client first verifies that the parent's copy is authentic. It does this by calculating the signature of the key inside the DS record using the parent's public key. If it matches the RRSIG associated with the DS record, then the parent copy is authentic. Next, the parent copy is compared against the child's copy – if they are the same, the parent has authenticated the child's DNSKEY.

Of course, it might be suspected that the parent zone's public key has been compromised. But the chain of trust means that the parent zone's public key can be checked against the copy of the parent's zone held by the parent of the parent. The same process can be used until the DNSSEC client encounters a "trusted" DNSKEY. The ideal "trusted" DNSKEY is that of the root zone -- and the good news is that the root zone has been signed since June of 2010.

Here is an example of a DS record for the zone example.com

```
dskey.example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A  
98631FAD1A292118 )
```

As always, the first four fields are the name, Time to Live, Class, and resource record type (this time, the DS record). 60485 is the key tag for the corresponding "dnskey.example.com" DNSKEY resource record. The number "5" indicates the algorithm used by "dnskey.example.com" to construct the DNSKEY resource record. The value "1" indicates the algorithm used to construct the digest and the remainder of the record is the digest of the DNSKEY in hexadecimal format.

Stripped to its essentials, DNSSEC simply adds additional data to the responses that allow the DNS client to authenticate the resource records returned by the server.

If the client requests the security information

- if the string and resource record type being queried exist, the authoritative name server simply adds the RRSIG to the response;
- if the string or the resource record being queried are not in the zone, the authoritative name server instead returns the NSEC record and its accompanying RRSIG record to indicate the negative response.

The DNS client can always take the returned RRSIG data and calculate its own copy of the signature to see if they match. The DNSKEY is needed to do this and if the client has not validated the DNSKEY within some set time period, the client needs to also validate the DNSKEY using the DS record stored at the parent zone. Each parent zone public key, in turn, must also be validated. Once the chain of trust is built and the signatures match, the DNS response can be considered to be validated and authentic.

## **3.4 Deployment Alternatives**

DNSSEC in .UK zones relies on a process that generates the appropriate DNSSEC records, along with the DS resource record, and then effective publication in the appropriate zones.

There are a series of deployment alternatives that can be either used by themselves, or are sometimes combined.

- Self-signing by DNS Servers -- Several major software vendors that produce enterprise class DNS Servers now have integrated tools for signing, resigning, and deploying zones. For some enterprise users there is an enormous advantage in terms of support and license cost to use the same software for DNSSEC that is used for DNS operations. The risk is in larger zones where performance may be an issue because of very dynamic zones requiring frequent, incremental zone signing or, full resigning. Examples of DNS Servers that do self-signing include BIND (the most popular of the DNS name servers), ANS (a commercial product from Nominum), and Unbound (an example of open source DNS Name Server that is intended, in part, as an alternative to BIND).
- Self-signing by assistive software – for many of the Open Source DNS servers, assistive software has emerged that effectively off-loads the signing, resigning and deploying activity away from the DNS zone provisioning system or the DNS master. The advantage of this is to separate the performance and reliability of the DNS infrastructure system from the DNSSEC signing and publishing activity. An example of this would be the `ldns-keygen` and `ldns-signzone` suites of tools from NLNet labs for unbound. For BIND and ANS similar sets of tools are distributed (`dnssec-keygen` and `nom_keytool`, respectively).
- Packaged solutions for signing – Many vendors now provide enterprise class utility packages (usually a combination of hardware and software, a classic, special purpose network appliance), that act as an intermediary between the provisioning system and the underlying DNS Server (such as BIND). The idea here is to have a tool that monitors the provisioning system or DNS master and then takes the unsigned data and turns into a signed zone for deployment by the existing DNS infrastructure. One example of this is the toolset for interfacing with cryptographic hardware provided by Nominet. Another commercial example is the Secure64 DNS Signer at (<http://www.secure64.com>).
- Outsourcing signing – it is also possible to turn the signing of a zone over to a third party. Several ccTLDs already offer this service and we see more registrars offering this service to their customers.

## **4. Barriers to DNSSEC Deployment**

### **4.1 Barriers to DNSSEC deployment**

Whenever changes are made to major infrastructure there will always be a level of concern, which if not well understood, can result in inertia. Prior to the root name servers being signed in June 2010 there were legitimate concerns over how the existing infrastructure would handle the increase in response length and the number of queries over TCP. As we have seen, DNSSEC requires significant, additional data to be transferred in the DNS packets (for example, the RRSIG and DNSKEY resource records). However, once the root name servers were signed and commenced sending verifiable responses, that initial fear was soon allayed. This meant the focus changed towards setting in place a complete chain of trust from the root, via the TLD operator's domain, right through to their customers. This is needed so end users can take full advantage of the benefits that DNSSEC brings.

Each step along the way requires an education process, resulting in a clear understanding of what DNSSEC can and cannot provide. Education is also crucial in overcoming both real and perceived barriers to DNSSEC deployment.

### **4.2 Deployment barriers at hosting companies and ISPs**

The potential benefits that DNSSEC can deliver will only become fully effective when all parties involved play their part. Having seen DNSSEC deployed at the root and also by a slowly growing number of TLD operators, it's imperative that hosting companies and ISPs look to play their part. Trust has become established at the very highest levels of the Trust Chain in the DNS. Now those responsible for the lower parts of the Trust Chain have to begin DNSSEC implementation for its promise to be realized.

#### **4.2.1 Real versus perceived barriers**

Historically most Internet security initiatives have never been adopted quickly -- something that is difficult to understand when a secure Internet is the cornerstone of its rapid acceptance as a critical infrastructure that supports global commerce and social development. Invariably there will be scepticism that take-up will be slow, that network overheads could yet prove to be a major stumbling block and that costs will prove prohibitive. With DNSSEC there is also a view that the real benefits are difficult to quantify, particularly when required to drive forward a corporate business case for early adoption. Despite the improvements it can bring, it is not the panacea that will facilitate a totally secure Internet and being clear and honest with that message makes the task more challenging.

In order to understand the real barriers to DNSSEC adoption, it is necessary to consider each potential barrier in more detail and to assess the impact each is likely to have on the take up of DNSSEC.

## 4.2.2 Technical barriers

### Protocol related barriers

Technical work on the DNS protocol needed to facilitate the introduction of DNSSEC has long been completed. We have seen that additional resource records types were added; the Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), and Next Secure (NSEC),<sup>8</sup> as well as the addition of two new DNS header flags. Changes were also made to the Extension Mechanisms for the DNS in order to support the larger message sizes<sup>9</sup> responses including DNSKEY and RRSIG. Additional support functions for security aware resolvers were also introduced.<sup>10</sup>

As a result of these protocol changes, and addition of the signature records, there is an increase in the message size: additional data being added to each answer whenever a server responds. Some existing software and hardware will struggle to handle the increased packet size and the larger UDP packets. Whenever the maximum size of a UDP packet is surpassed it sets a truncated response flag which results in that query being repeated using TCP. The overheads associated with TCP mean that it's a less efficient network mechanism than UDP. That fact requires additional memory and computation capacity within clients and servers. The amount of additional capacity is dependent upon the key size but it has been estimated by ISC<sup>11</sup> that a DNSSEC signed zone can vary between 4 to 14 times the size of the original zone, a significant increase. Recent research indicates that the capacity required to handle the additional workload is proportional to the size of the signing key for each unit of DNSSEC activity.

Another feature of the DNS is the ability to synthesize responses on the fly rather than taking the responses from the authoritative zone file. Such synthesized responses are popular attempts to "hide" errors from end users of the Internet. In one such case, a zone's non-existent domains are hidden from view by returning the IP address for a special purpose search engine. This approach, called "wildcarding" is built into the standard for the DNS. However, since the records returned to the client are synthesised on the fly, they can't be signed. DNSSEC does not work in zones where a server is being used to synthesize responses to DNS queries.

## 4.2.3 Economic Barriers

The fact that DNSSEC can provide additional security in the event that certain types of attacks are made on the network makes it difficult to quantify its value so that a definitive cost versus benefits assessment can be made. The likelihood of an attack that results in DNS cache poisoning and the subsequent damage caused is a subjective question. Evidence suggests it is not that prevalent but when it does occur its impact can be substantial.

Without doubt implementing DNSSEC imposes additional costs and demands on a number of players ranging from software developers and infrastructure providers, to zone administrators and those who run DNS servers, clients and applications.

---

<sup>8</sup> See RFC 4034:

<sup>9</sup> See RFC 2672:

<sup>10</sup> See RFC 3225

<sup>11</sup> Internet Systems Consortium

For software developers the issue is simpler than most, the initial standardization work has been completed and they will look to meet the demand, whether that be in terms of DNS server software upgrades, resolvers or key management functions. The inclusion of DNSSEC capabilities within future software packages will be determined by the perceived demand that emanates from the provider and user communities.

Zone implementers face two sets of costs with DNSSEC. Implementing DNSSEC in a zone has an initial cost of deployment in hardware, software, network resources and manpower. But once the initial deployment is complete, there are on-going overheads from DNSSEC -- it is not just an upfront cost that needs to be considered. For instance, it's imperative that zone signatures are maintained. Decisions have to be made over the length of the keys used and 'time to live' values associated with them -- both are critical elements of a successful DNSSEC implementation. Once the time limit of the signed keys expire, unless they are 'refreshed' (re-signed), message failures will occur at the client or resolver level. New procedures will also need to be put in place to deal with unforeseen emergencies such as the urgent regeneration of keys or other required support activities.

Similar to the benefits gained from DNSSEC's introduction -- where it is users who benefit from the assurance that responses to their requests are authoritative -- the tangible benefits of additional and on-going support activities undertaken by zone administrators are again primarily realized by the end user. This situation does not provide an overwhelming incentive for zone administrators to take on the additional administrative load and expense without user demand and a willingness to pay.

The corporate sector is likely to deploy DNSSEC earlier, particularly those organizations whose business operations and networks would clearly benefit from enhanced security as here there is an immediate return. For instance, some parts of the financial services sector have already indicated they are very likely to be early adopters. However, the financial services sector is also awaiting clear guidance from registrars and network providers on the timing for implementation of DNSSEC. As an example, we will see later in the report that Swedish financial companies have been slow to implement DNSSEC despite having .se signed for several years. In this case the problem is not technical in nature -- instead, the relationship between the .se registry and the registrars has contributed to slow uptake in DNSSEC deployment.

There are also benefits from being able to authenticate individuals within an organization and DNSSEC can facilitate this. Some organizations will benefit from deploying DNSSEC within their own, private environment, ensuring their internal communications remained secure and authenticated. It seems likely that some enterprises will be able to leverage DNSSEC -- in private settings -- in ways that go beyond simple authentication of the results of a resource record query.

By enhancing security, DNSSEC clearly delivers a set of desirable features that can justify additional expenditure for certain sectors of the community. For others, economic constraints, not helped by the current economic climate, are likely to result in a staggered evolution. In situations where the level and value of threats to business remain difficult to quantify, the move towards DNSSEC is likely to be dependent upon the DNS provider's software upgrade program and the likelihood of its being bundled with other system improvements.

#### 4.2.4 DNSSEC CAPEX and OPEX

Capital Expenditures (CAPEX) related to DNSSEC are related to investment for future benefit – usually they are funds spent to buy assets or add to an existing inventory of assets. For registrars who want to provide DNSSEC to their customers, the service is often simply an additional service – added-on to a client’s purchase. Including this feature in a registrar’s portfolio is the only action a typical registrar needs to commit to in order to offer DNSSEC. The low CAPEX for registrars (in our survey, less than £5,000) reflects the relatively low technical and operational requirements for registrars.

However, the situation is different for registries. In a study<sup>12</sup> by the European Network and Information Security Agency, registries divided into two categories: those who had large sustained query rates and required large amounts of investment to support the additional DNSSEC workload and those smaller registries that did not require significant additional capacity to support DNSSEC. Our follow-up research shows that the most recent deployments of DNSSEC in Europe for large scale ccTLDs (including .uk and .de) have required CAPEX between £300,000 and £750,000. Most of the costs related to this investment are related to investments in infrastructure components supporting the additional computational and bandwidth requirements associated with DNSSEC. In our survey, almost every CCTLD that has implemented DNSSEC has done so by in-house customization of existing software rather than purchasing commercial-off-the-shelf products (COTS).

In contrast to CAPEX, operational expense (OPEX) is the on-going costs for running a service or business. In our survey, the main OPEX related to DNSSEC was in bandwidth cost. While there is not sufficient operational experience in .uk to quantify OPEX related to running the .uk registry, in other registries (for example .se and .us) the size of the OPEX increase related to bandwidth is roughly 50%. Put another way, the cost of ongoing deployment of DNSSEC related to bandwidth at the registry is roughly one-half of the existing cost of bandwidth prior to deployment. The apparent cause of this increase is the increase in the size (and thus, bandwidth requirements) of DNS responses when signed DNS records are sent by the DNS name servers.

#### 4.3 Deployment barriers at end user sites

For end users to benefit from DNSSEC they will need to utilize client software that is DNSSEC aware. This will inevitably impose additional costs for early adopters. The majority of end users themselves are unlikely to demand DNSSEC enabled software and, unless technically astute, most will remain blissfully unaware of the benefits it can bring and the potential threats that have led to its development. They are only likely to adopt DNSSEC when this capability is included as an additional feature during a software upgrade.

For those who run recursive servers for customers (for instance hosting companies or broadband providers), DNSSEC also poses new problems. As an example, they will need to deal with situations where they may currently provide automatic searches when their users types an invalid address in a browser, this arrangement will not facilitate key validation and

---

<sup>12</sup> See [http://www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts/at\\_download/fullReport](http://www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts/at_download/fullReport)

DNSSEC will not work. They will need to know how to respond to signature failures, whatever the reason.

#### 4.4 Deployment barriers in consumer broadband networks

Many of the deployment barriers in consumer networks echo the issues already raised in other settings (e.g. by the DNS providers and administrators, client, software, and network providers). All will have an impact on how DNSSEC is delivered to the broadband user. In this case, however, the broadband user is often remote from the other parties. Human behaviour may play a more prominent part in this context as the level of understanding is often less. It is more likely that consumers with less understanding of the Internet would ignore any warning messages that certificates or signatures are not valid or have expired. Explaining the potential benefits would prove more difficult, particularly if the majority of sites they accessed did not utilize DNSSEC.

A clear result of our survey work is that DNSSEC may suffer from a problem that crops up with secure Web sessions. In modern browsers, the software checks to make sure that the Digital Certificate of the Web Server is valid. When it isn't, the browser displays an error message which the user must acknowledge. Many users simply click on whatever they need to in order to see the content they requested originally. DNSSEC may be the same for consumers: depending on how the user interface is constructed, the protections that DNSSEC provide might be circumvented by user behaviour.

#### 4.5 The “bootstrap problem” for DNSSEC

Widespread adoption of DNSSEC is unlikely to happen overnight. The Internet in particular has a history of resisting change, but that is not surprising for a network that is truly global. With any network of this size, reaching critical mass is a major challenge.

When discussing economic barriers it was noted that it will often be difficult to substantiate a positive business case for the deployment of DNSSEC. It is not a universal panacea for all types of attack on the Internet, but it does deal effectively with a specific set of threats to the security and integrity of the Internet. What's more: the costs for most parties in the chain of trust are not a one-time expense. Instead, this is an on-going expense with the main benefit going to the client or end user. That is not a good starting point for large-scale, commercial deployment.

Difficulties in substantiating a business case for DNSSEC will therefore result in piecemeal implementation. Unfortunately the benefits from DNSSEC will be far greater if it were widely deployed.

In some situations DNSSEC key registration is already viewed as an additional function that could become a revenue stream. That approach is unlikely to assist in achieving widespread DNSSEC adoption. Similarly if registries increase fees for handling DNSSEC secure domains, that would also likely limit demand. In most cases the least expensive option would prevail. That said, if cache poisoning were to become the focal point for large scale attacks on the Internet, or even if the likelihood of that occurring were to substantially increase, then the call for DNSSEC would immediately increase and the increased cost would not prove to be an insurmountable barrier.

One event that could help encourage the take-up of new gTLDs is the introduction of new generic Top Level Domains. These seem likely to be introduced into the root towards the end of 2012 following extensive consultations within ICANN. Some potential applicants for new Top Level Domains have already indicated they will provide DNSSEC at the top level. More competition within the namespace may see DNSSEC become a differentiator. A competitive marketplace may induce TLDs, who are otherwise indifferent or reluctant to deploy DNSSEC, to move forward with adoption as a competitive imperative.

The need for a secure and trusted Internet is a key requirement that is increasingly accepted. Responsibility for that must be shared between those involved in providing Internet services and those who use it. In order to achieve that goal, education and awareness will always be required. In the Internet environment it is particularly difficult to enforce change, but history tells us as problems arise, innovation, technical expertise and community responsibility come to the fore and the required changes happen. Attempts to force things rarely work. A clear example of this is the move from IPv4 to IPv6 addressing: a clear analogy with DNSSEC. With IPv6 deployment it was always difficult to substantiate a positive business case until the IPv4 address pool was depleted. Now that has happened, the momentum required to support the widespread introduction of IPv6 is rapidly building.

The bootstrap problem for DNSSEC will only be fully resolved when the industry fully accepts the need for its adoption. To assist with that goal there must be both education and coordination. Education so that providers and users fully appreciate the threats that can be mitigated through the deployment of DNSSEC and are able to assess what its deployment would mean for them. Coordination, so that those who share the responsibility for delivering and maintaining the integrity of the Internet work together with early adopters, thereby promoting the benefits that can be derived. For this coordination to achieve its maximum effectiveness at the bootstrap stage it should be built on a multi-stakeholder approach (for instance, see include the that includes the technical community (including the IETF), ICANN, governments, those organizations charged with regulatory oversight, industry and end users.

## 5. DNSSEC Deployment – A Global Perspective

### 5.1 Statistics and history

As a protocol DNSSEC is relatively old. RFC 2535 was published in 1999 and it would have appeared that DNSSEC implementation could have started almost immediately thereafter.

However, the early specification of DNSSEC was marred by a basic problem: deployment was impossible. By 2001, the DS record (see above) was specified, but the Internet specifications for describing the new features of DNSSEC weren't published until March of 2005. Later, in October of 2005, Sweden became the first ccTLD to deploy DNSSEC.

As we have seen, it was soon discovered that the original NSEC record required that zones could be enumerated. While the IETF originally thought this was not a significant problem, registrars and users of the Internet told the IETF that, as currently designed, the NSEC record was not deployable – and in some countries possibly illegal.

In March 2008, the IETF responded with a specification of NSEC3, a replacement for the NSEC approach. Instead of using the names directly, as in NSEC, NSEC3 put a hashed value that represented the name. This made it mathematically far more difficult to collect all the names in a zone by simply doing methodical queries against successive NSEC records.

However, the chain of trust requires that the root be signed as well. Finally, in July of 2010, the IANA signed the root zone of the DNS. This made it possible to trace the chain of trust back to a trusted root – thus, results of queries could be validated against all the zones in the chain of trust.

### 5.2 Statistical Patterns of DNSSEC Adoption in the Root

The root of the public DNS was signed in July of 2010. Prior to that, there existed islands of DNSSEC implementations with a variety of strategies enabled to allow a client to establish that a DNS response was authentic and correct in the absence of a full chain of trust. Once the root was signed, there was a dramatic upsurge in the number of DNSSEC zones available on the public Internet.

Looking globally since July of 2010, the distribution of TLDs that have DS records in the root zone shows that:

- Of the 19 gTLDs in the root zone, 8 have DS records as trust anchors in the root zone ( 42.1% ) These include .arpa, .biz, .com, .edu, .gov, .info, .museum, and .org.
- There are currently 41 Internationalized TLDs (in scripts other than ASCII) in the root zone. Of these, 12 have DS records in the root zone ( 29.2 % )
- There are two regional/cultural TLDs in the root -- .asia and .cat – and both of these have DS records in the root zone.
- Of the 241 active ccTLDs 47 have DS records in the zone ( 19.5 % )

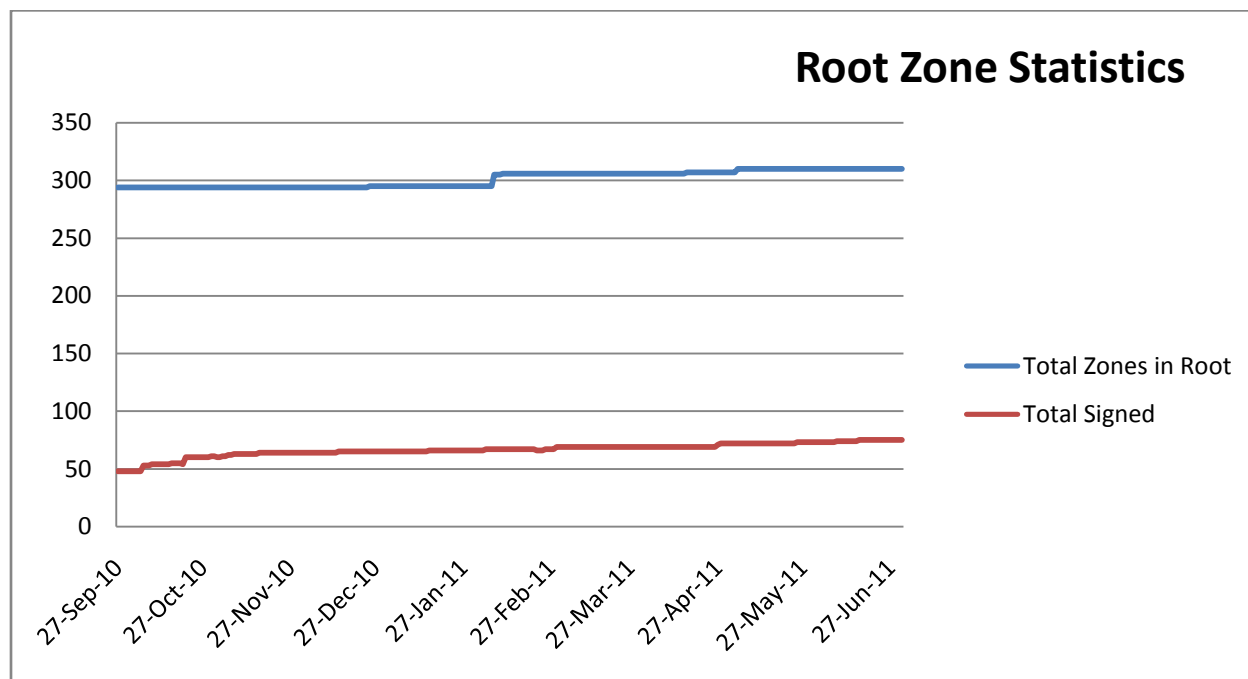
Looking at the global distribution of the active 240 ccTLDs, it is possible to detect another set of trends:

- DNSSEC in the African region is small, 4 out of 53 ccTLDs ( 7.5 % )
- DNSSEC deployment in the North American region is large by percentage because there are so few ccTLDs there, 2 out of 5 zones with DS records in the root ( 40 % )
- DNSSEC in the Latin American/South American and Caribbean region is promising with 10 out of 43 ccTLDs with DS records in the root ( 23.2 % )
- DNSSEC in the Asian/Australian/Pacific region is difficult to assess because of the existence of so many tiny ccTLDs – there are 12 out of a possible 88 DS records in the root for this region ( 13.6% ); and,
- DNSSEC in Europe, as we will see in detail, is very encouraging: 18 out of 51 possible DS records in the root ( 35.3% ).

If you avoid the statistically skewed North American zone (where Canada and Mexico have not signed their zones), Europe emerges as the clear leader regionally in DNSSEC implementation in terms of the number of ccTLDs who have moved DNSSEC into production.

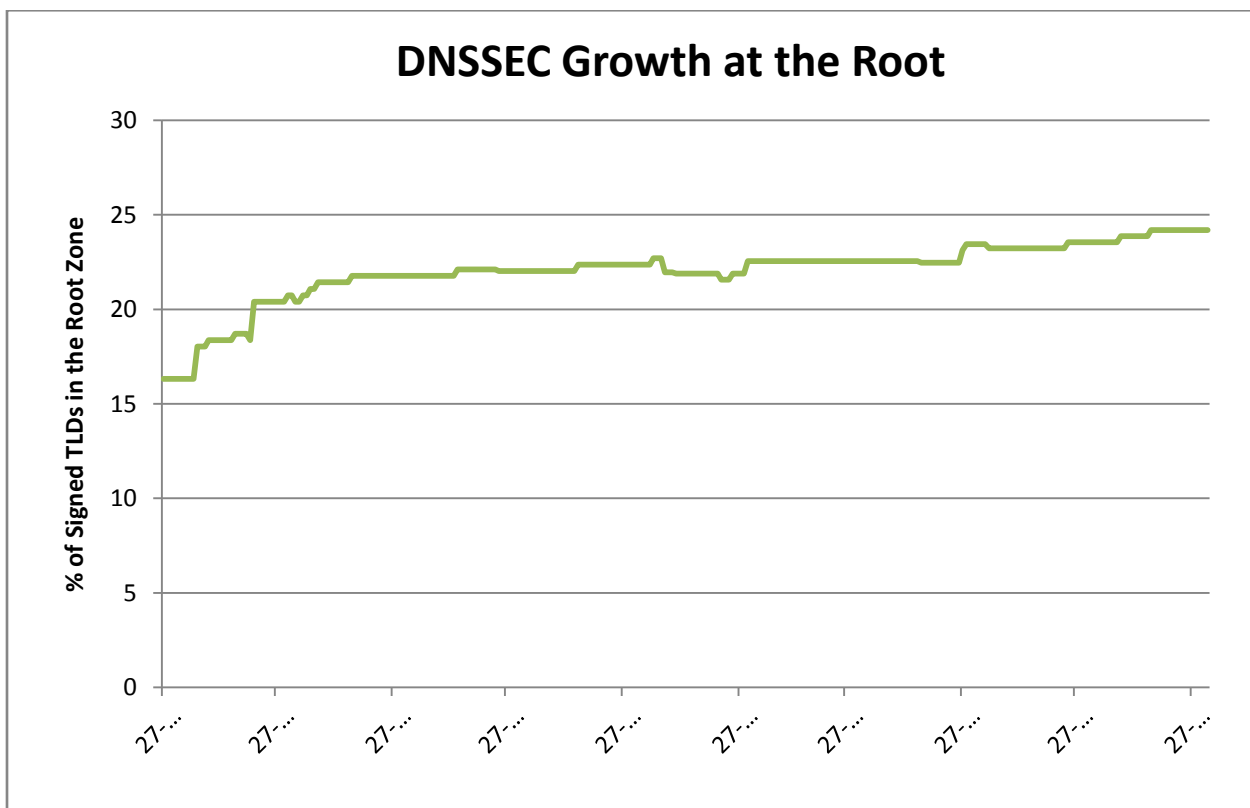
Looking at the root zone statistics since the root zone was signed there are two clear trends. The root zone itself is getting larger (this will become an even more pronounced trend with the introduction of new gTLDs starting in 2012). However, contrary to expectations, the number of zones with DS records in the root is not growing in any substantial way. Globally, the number of zones signed has grown only slightly in the last nine months.

While the number of zones signed is growing slowly, the size of the zones has grown enormously. This is due to the signing of the largest zone in the public Internet- .com with more than 90 million names. A look at the number of DS records in the root shows the following.



If we examine the rate at which new zones are being signed, we see that when the root was signed in July of 2010 there was a period of great growth in the percentage of TLDs signed in the root. In the last nine months the rate has stayed nearly the same: about 23 – 24% of the total number of zones in the root are signed. Below, the graph shows the daily ratio of zones signed versus total number of zones.

It is worth commenting that the great majority of zones remaining – even though it is nearly 75% of the zones in the root -- are relatively small and will contribute a small proportion of total domain names to be signed. The signing of very large zones such as .COM, .NET, .ORG, .UK and .DE will do more for public security on the Internet than the future signing of the remaining zones combined.



A large number of countries who have signed their zones are very small in geographic and economic size. For instance the global DNSSEC deployment experience includes Ascension Island, Antigua, Gibraltar, The British Indian Ocean Territory, Kyrgyzstan, Montenegro, Niue, and Saint Helena as countries who contribute the global statistics above.

Also, even though the root zone was signed in June 2010, collection of statistics for root zone activity commenced in September of that year.

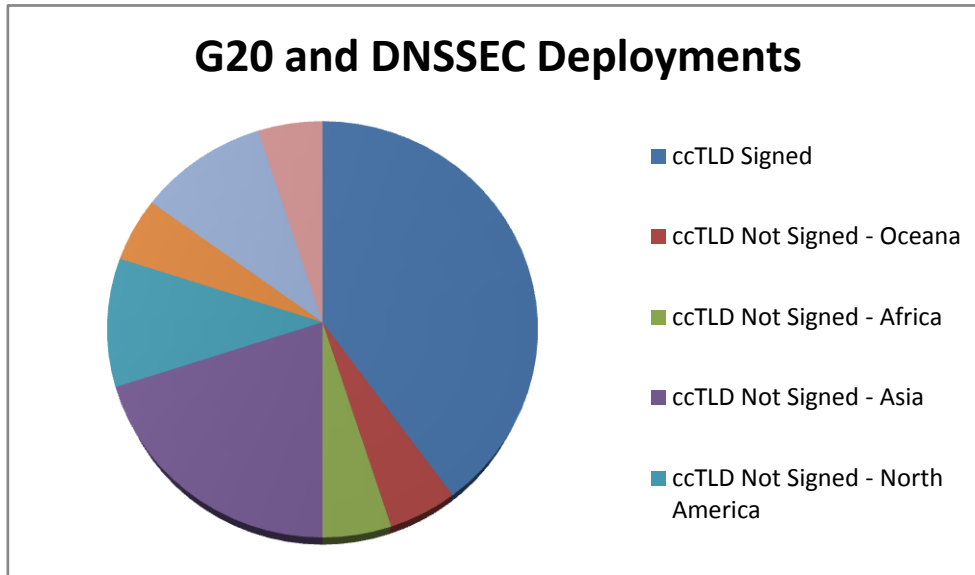
What would happen if we restrict the investigation to the G20 major economies?

## 6. DNSSEC Deployment – A G20 Perspective

Narrowing the focus, we examine the deployment of DNSSEC by restricting the list of countries to the Group of Twenty Finance Ministers and Central Bank Governors. This list includes:

Region	Member
Africa	South Africa
North America	Canada
	Mexico
	United States
South America	Argentina
	Brazil
East Asia	China
	Japan
	South Korea
South Asia	India
Southeast Asia	Indonesia
Western Asia	Saudi Arabia
Eurasia	Russia
	Turkey
Europe	European Union
	France
	Germany
	Italy
Oceania	United Kingdom
	Australia

Allowing the European Union to be represented by .EU for this analysis, we find that 8 of the G20 zones are signed. Of the 12 remaining four are in Asia (China, South Korea, Indonesia and Saudi Arabia). In North America, neither Canada nor Mexico have signed their zones. With the signing of .UK and .DE very recently, Italy remains the only G20 zone in Europe that is unsigned. Australia, Russia, Turkey, South Africa, and Argentina are the other unsigned G20 economy unsigned zones.



If each of the G20 economies' ccTLD were signed it would contribute the following number of potential zones for signing.

Country	Zone Size in Registrations	DNSSEC Status
Germany	14,351,217	Signed
United Kingdom	9,373,754	Signed
China	3,379,441	Not Signed
European Union	3,326,388	Signed
Russia	2,890,071	Not Signed
Brazil	2,459,910	Signed
Italy	2,166,324	Not Signed
Australia	2,059,304	Not Signed
France	2,010,374	Signed
United States	1,682,093	Signed
Canada	1,673,671	Not Signed
Japan	1,214,101	Signed
South Korea	1,085,377	Not Signed
South Africa	642,864	Not Signed
Mexico	482,121	Not Signed
Turkey	240,784	Not Signed

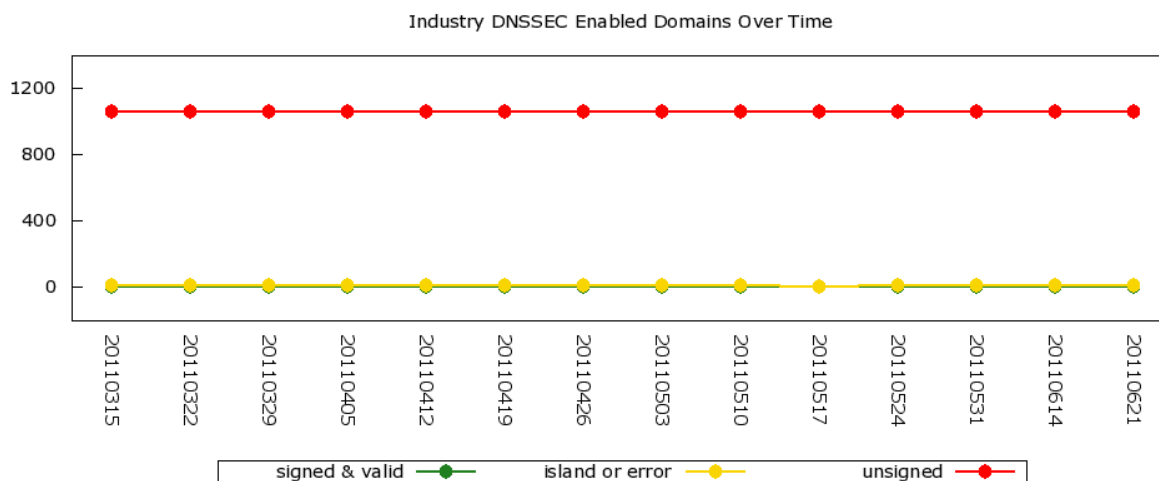
Data is unavailable for Argentina, India, Indonesia and Saudi Arabia.

## 6.1 Review of DNSSEC Adoption of Leading Commercial Sites

In the case of G20 adoption, it is also possible to analyse the DNSSEC at large national and international domains. The strategy is to pick high-value, high-traffic domains and examine

whether or not these domains have DNSSEC implemented. This takes the analysis beyond the realm of just ccTLDs. Since most high-value, high-traffic domains are global in nature, they are often registered in .COM or another generic top-level domain.

The US Government has done a remarkable experiment over a group of 1,076 domains that shows the following



This shows that, since March of this year, when the experiment began, there has been no growth in commercial utilization of DNSSEC when you restrict the monitoring to high-value domains. While the experiment is a US-based one, many of the brands being surveyed are global in nature and many seem to be clear candidates for DNSSEC deployment. Still, less than one-half of one per cent of the surveyed commercial industry was deploying DNSSEC. The rare cases where DNSSEC was being deployed were almost all from Information Technology or Telecommunications sector companies who were likely to have heard about DNSSEC in other channels.

A one-time experiment in mid-May 2011 examining the ten largest constituents of the FTSE 100 companies revealed that none of the ten had deployed DNSSEC in any of the zones they operated for public consumption.

We will examine a UK-specific experiment using the same strategy later in this report.

## 6.2 Comparison of DNSSEC Adoption Amongst ccTLDs versus gTLDs

Previously, we have observed that the G20 economies tend to have large, global businesses that tend to register domain names in generic TLDs (generic top-level domains) rather than ccTLDs. If we examine the gTLDs, it's worth noting that the contribution of these gTLDs is very large by comparison to ccTLDs.

- .com has 95,000,000+ registrations and is signed;
- .net has 13,950,000+ registrations and is signed;
- .org has 9,250,000+ registrations and is signed;

**MC/080 DNSSEC Deployment Study**

- .info has 7,870,000+ registrations and is signed; and
- .biz has 2,100,000+ registrations and is signed.

By comparison,

- .de has 14,350,000+ registrations and has just been signed;
- .uk has 9,370,000+ registrations and has just been signed;
- .nl has 4,420,000+ registrations and is signed;
- .eu has 3,320,000+ registrations and is signed;
- .pl has 2,080,000+ registrations but is not yet signed, and,
- .fr has 2,000,000+ registrations and is signed.

In any single developed economy, the impact of DNSSEC deployment is going to be seen in both the respective ccTLD and in the gTLDs that represent commercial branding and intellectual property. The recent deployment of DNSSEC in .UK and .DE – joining with the slightly more established deployments at .NL, .EU and .FR – will make the European region a leader in DNSSEC deployment amongst ccTLDs.

## 7. DNSSEC Deployment – A European Perspective

### 7.1 Early Adoptions

The extent of adoption of DNSSEC in the European Community is as diverse as the countries themselves. There are countries that have been early adopters and have widespread support – not just at the registry – but through the entire ccTLD economic and technical support chain. There are also countries that have yet to start planning for DNSSEC in their ccTLD. In this report we characterize four groups of DNSSEC implementers in Europe:

- **Successful Adopters** – Those countries that already have a successful, deployed DNSSEC program which is available through registrars.
- **Poised for Success** – Those countries who have finished or nearly finished testbed or other programs that have got them ready for a rollout of DNSSEC services.
- **Pre-implementers** – Those countries who have begun testbed or other pre-implementation planning projects but are unlikely to deliver viable, widespread DNSSEC services to consumers in 2011.
- **Trailing** – Those countries without substantial planning or testing efforts for DNSSEC underway.

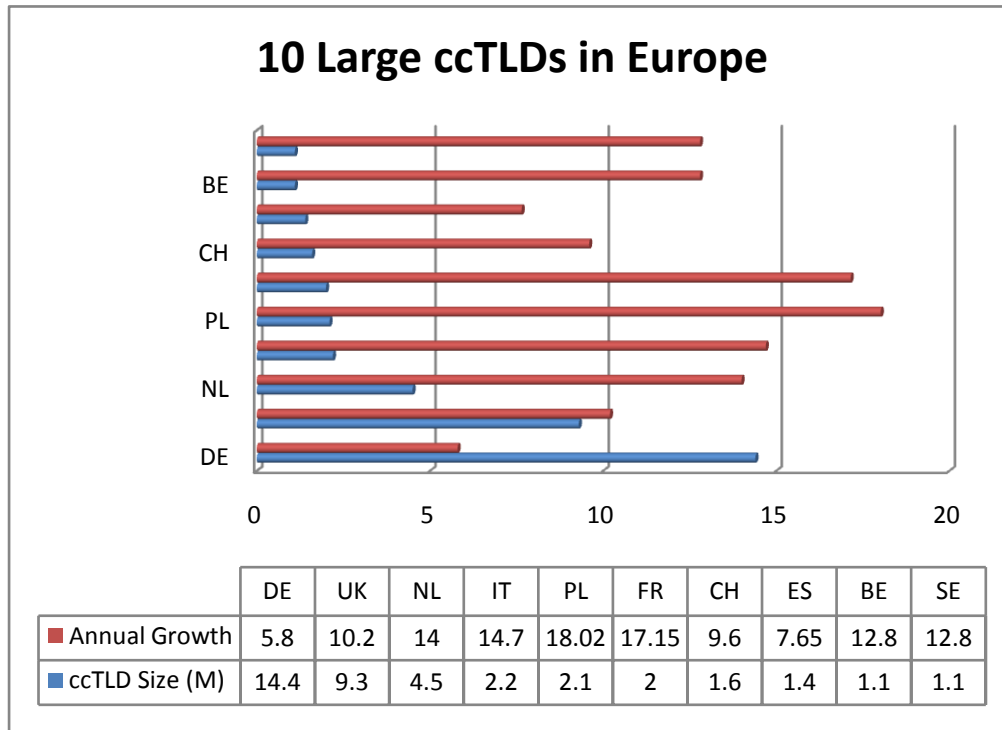
Intuition might lead you to believe that those countries who have the longest experience in ccTLD activities might be the first ones in the Successful Adopters group. However, this appears to not be the case for a variety of reasons, some technical, some economic. Here is a view of the largest ccTLDs by number of domains registered.

On the map on the following page

- The countries **shaded in red** have total registrations greater than 5,000,000;
- The countries **shaded in orange** have total registrations between 1,000,000 and 5,000,000;
- The countries **shaded in green** have total registration between 500,000 and 1,000,000;
- The countries **shaded in blue** have total registrations between 250,000 and 500,000; and,
- The countries shaded in grey have total registrations less than 250,000.

This map makes it evident that the number of registrations in a ccTLD in Europe is directly affected by the amount of time the Internet has been present. Western and Northern Europe have had access to the public Internet nearly since the beginning of the commercial, public Internet. The ccTLDs in these parts of Europe show the impact that experience has had by being the countries with some of the largest numbers of registrations.

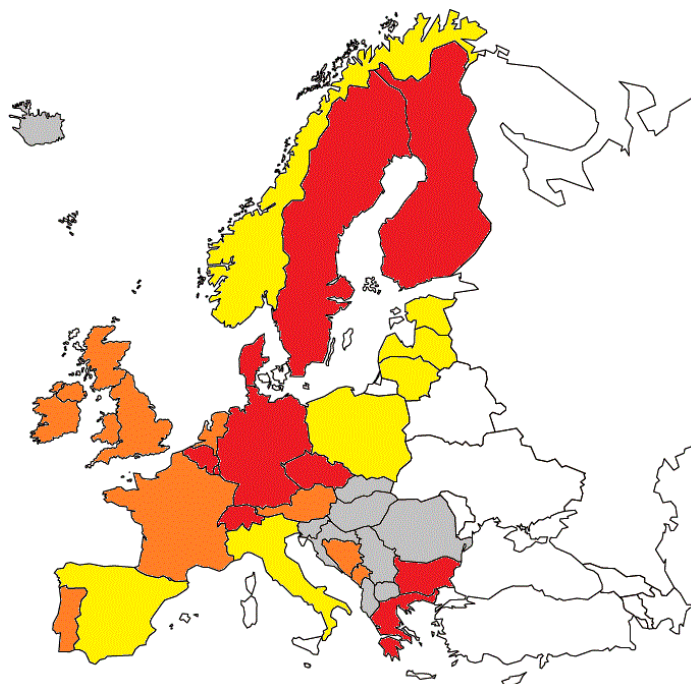




In fact, the early adopters in Europe -- Sweden, Portugal, Czech Republic, Denmark, and Bulgaria – are not the countries with the fastest growing or largest registration base. The motivation for early adoption came from sources other than the consumers of DNS services. While we have noted that the reasons for escalation of registration growth differs from country to country, most often the core explanation is the result of a change of registry policy (for instance, allowing a certain kind of registration that wasn't available before, or relaxation of the rules on who can register). It's worth noting that the overall growth rate for all ccTLDs globally is 9.2 percent annually.

## 7.2 DNSSEC Adoption in Europe in mid-2011

If you were to look at a map and categorize the level of adoption of DNSSEC in Europe, you would see the following:



*Figure 2: European ccTLD Registrations by Country*

The countries shaded in red are successful adopters;  
The countries shaded in orange are poised for success;  
The countries shaded in yellow are pre-implementers;  
The countries shaded in grey will be trailing, late-adopters.

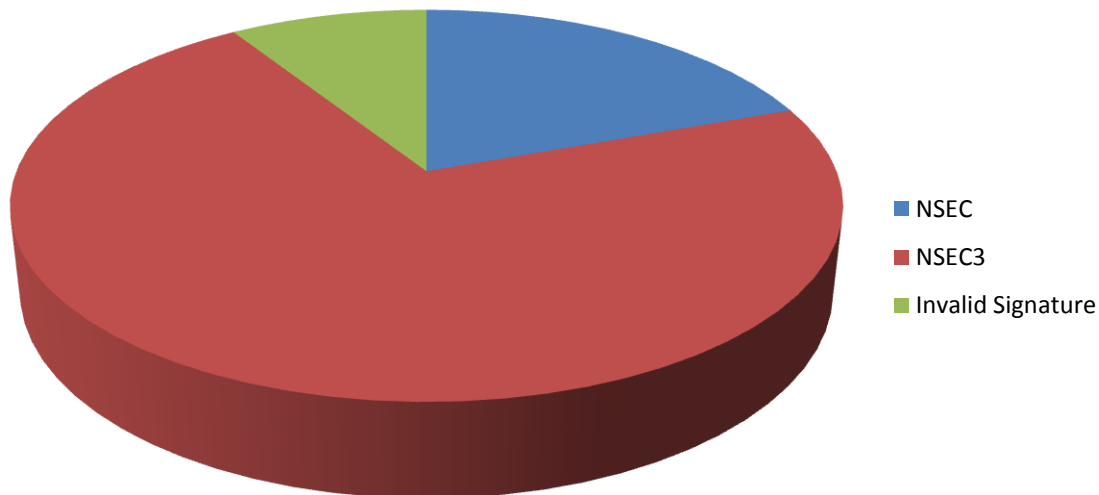
Some smaller countries in Europe have implemented DNSSEC. The reason this happens is a combination of the zone being very small and, almost always, the presence of a core group of networking engineers (in some cases, just one) that have an early adopter interest in implementing DNSSEC. Just as we have seen when we looked at global implementations of DNSSEC, if we remove the impact of very small zones, the implementation of DNSSEC in Europe has been methodical, evolutionary and relatively slow.

## 7.3 NSEC and NSEC 3 in Europe

Another issue, unrelated to technology, appears to have affected DNSSEC implementation in Europe. Many ccTLDs in Europe, when surveyed, indicate that they believe that the contents of the zone they administer is both private and the crucial economic asset for the organization. Without the benefit of the relatively new NSEC3 resource record type, many European ccTLDs were reluctant to implement DNSSEC. The reason for this was the peculiar “zone-gapping”

properties of the NSEC resource record. With a methodical and automated approach, anyone who wanted to acquire the contents of a zone with NSEC records, could simply “walk the zone” and acquire, piece-by-piece almost the entire signed zone. An NSEC record lists the next name in its zone (thus proving that no names exist in the “span” between the NSEC’s owner name and the name in the “next name” field). In the technical literature it is sometimes said that the NSEC record “covers” the names between its owner name and next name. Through repeated

## NSEC and NSEC3 Adoption



queries that return NSEC records, it is possible to retrieve all of the names in the zone, thus “walking” the zone. In the face of this threat to both their business and to their customers’ privacy, many ccTLDs decided to wait until the NSEC3 standard – and supporting, compatible software – was available.

Examining fifteen of the DNSSEC-enabled ccTLD zones in the European community in mid-May 2011 we found the data you see above.

As recently as September 2010 the percentage of ccTLDs that had adopted NSEC3 as the Next SECure resource record type at 65%. Today, in Europe the percentage is past 75%. In addition, looking at this statistic over time, as new ccTLDs adopt DNSSEC, they overwhelmingly use the new standard. In Europe, as new ccTLDs move to support DNSSEC in their zones, it looks increasingly likely that NSEC3 will be the dominant approach to providing authenticated assertion of non-existence of domains.

The availability of the NSEC3 standard is also a factor. Many ccTLDs in Europe were very nervous about the mechanism for authentication of negative responses. In fact, for many ccTLDs the NSEC approach was an inhibitor for the deployment of DNSSEC. The NSEC3 standard wasn’t published until February 2008. Given the development cycle for supporting software and the timing of the signing of the root, it is understandable that technical factors have converged to make DNSSEC deployments more common in 2011.

## 7.4 Beyond Signing ccTLDs -- Deployment Within ccTLDs

What about deployment inside individual countries that had been early adopters of DNSSEC in Europe. Sweden was a very early success story in Europe for adoption of DNSSEC. To examine how well DNSSEC had been adopted by the commercial community, we conducted a simple experiment. Hypothesizing that the banking and financial community might be among the organizations most interested in emphasizing trust and building more secure models for the consumer/provider relationship, we attempted to gauge how much this important industry had adopted DNSSEC in public settings.

To conduct this test we used twenty banks and financial institution at random from the list provided by the Finansinspektionen, the Swedish government agency responsible for financial regulation in Sweden. In mid-May of 2011, none of the twenty banks surveyed had signed the zone that represented the public face of the organization.

We expanded this test to then include ten newspapers, ten traditional retail companies, and finally five ISPs operating in Sweden. Still, none of the 45 companies had DS records in their parent's zone despite the early adoption of DNSSEC by the .se ccTLD.

Sweden's history of technical success with DNSSEC at the root of .se – and its pioneering deployment – has not translated into wide-scale, public, commercial deployment of DNSSEC. Sweden is an example of a common theme throughout early European implementation: deployment of DNSSEC at a ccTLD is a necessary step to bringing secure DNS infrastructure to businesses and consumers. But it not the only necessary step. Also needed is deployment below the country code.

While getting ccTLD zones signed in Europe has been a challenge, deploying DNSSEC beyond the ccTLD into the community is proving to be significantly difficult.

## 7.5 Do European DNS Clients Request Security Information?

There is little European deployment in commercial zones at this time. Still, one can watch to see if clients are trying to retrieve DNSSEC data. Put simply, are clients that are making requests in the DNS requesting DNSSEC data as part of those requests?

Late in 2010, RIPE Labs did an experiment<sup>13</sup> and looked at the quantity of DNSSEC queries coming to one of their servers that serves up DNSSEC data. Remarkably, they found that more than 50% of the queries that came to their instance of ccTLD servers were asking for DNSSEC data.

The RIPE Labs experiment is unable to shed any light on what, if anything, the clients do with the security data they gather. For instance, there is no data on how many clients are actually

---

<sup>13</sup> See <http://labs.ripe.net/Members/dfk/dns-clients-do-request-dnssec-today> This survey looked at 5000 queries per second for a full month at a single root server instance.

**MC/080 DNSSEC Deployment Study**

validating signatures and checking the integrity of DNS query responses. This is clearly an area which requires further research.

A recent study<sup>14</sup> by the Japanese registry indicates that the number of validators (those DNS Clients requesting DNSSEC information) is closer to 25% in other parts of the world. A methodology<sup>15</sup> (also by researchers in Japan) for counting DNSSEC validators was presented at the DNS-OARC workshop in March 2011.

---

<sup>14</sup> See <http://singapore41.icann.org/meetings/singapore2011/presentation-dnssec-validators-jp-22jun11-en.pdf>

<sup>15</sup> See <http://bit.ly/jprs-validators>

## 8. DNSSEC Deployment – The UK Perspective

### 8.1 Implications of a structure second-level namespace

Unlike the majority of Top Level Domains (such as .com and most European ccTLDs), .uk does not offer registrations at the second level. The .uk zone is partitioned into 14 second level domains<sup>16</sup>, 8 of which are managed by Nominet, and the remainder (such as .gov.uk, nhs.uk, and mod.uk) are managed within the public sector. In spite of the high level of second level domains, .co.uk is by far the largest of the zones managed by Nominet, accounting for between 92-95% of monthly registrations over the past five years<sup>17</sup>.

For a TLD structured into second level domains, like .uk, implementing DNSSEC is more complex than with other TLDs. Nominet signed .uk on 1 March 2010<sup>18</sup>, but in reality, this did not introduce DNSSEC to .uk domain name registrants, until the second levels managed by Nominet were signed in May 2011<sup>19</sup>. Only then was it possible for .uk registrars to complete the chain of trust through to individual domains.

### 8.2 History and context for signing .UK

#### 8.2.1 NSEC3 and Zone Walking in ccTLDs

The first Internet standards describing DNSSEC (RFC 4033, 4034, and 4035) were published in 2005. One of the features of the DNSSEC standard was “NSEC”, an authenticated denial of existence resource records. The purpose of NSEC was to give assurance that no phantom domain name had been inserted in the zone, by returning the domains on either side of the signed domain name in the canonical record.

As we saw in Section 7.3, this security feature had an unintended consequence, called “zone walking” or “zone file enumeration”. Once DNSSEC had been implemented in a zone, then a query on a single domain would return also the next name in the zone. By querying the next name, the one after that would be returned, and so on. Therefore, DNSSEC provided a convenient means of taking a copy of an entire zone file, a means which was also susceptible to automation.

#### 8.2.2 Legal and policy issues related to .UK zone enumeration

As we have seen, some TLDs, for instance .se (Sweden), took the view that their zone file was public domain in any event, and became early implementers of DNSSEC.

Others, including Nominet, were not prepared to risk implementing a security protocol which allowed zone file enumeration, for both legal and policy reasons including the following:

<sup>16</sup> See <http://en.wikipedia.org/wiki/.uk>

<sup>17</sup> Source: <http://www.nominet.org.uk/intelligence/statistics/registration/registrationsarchive/> and <http://www.nominet.org.uk/intelligence/statistics/registration/> (for 2011)

<sup>18</sup> <http://www.nominet.org.uk/news/latest/2010/?contentId=7075>

<sup>19</sup> <http://www.nominet.org.uk/registrars/DNSSEC/dnssecdeployment/>

- The registry's legal rights. The TLD register database is a key business asset, of commercial value. The compilation is protected in law under Database Rights in the UK and copyright in other countries. Placing an easy tool for copying the database into third party hands would devalue those rights.
- Consumer protection. It was foreseeable that some of those who would enumerate the zone would use the data for spam, invoice scams or other unlawful conduct, aimed at registrants of the TLD. Nominet has successfully taken legal action to prevent such action and protect UK registrants<sup>20</sup>. To implement DNSSEC in its original form would have run counter to Nominet's attitude towards consumer protection.
- Data protection. A zone file itself contains no personal data, as it contains only the domain name and nameserver records. However, with a copy of the zone file, it is straightforward to populate the records with personal data by running WHOIS queries against each domain name. Therefore, implementing DNSSEC would potentially risk breaches of Data Protection law.

### 8.2.3 Nominet's Advocacy of DNSSEC

For many years, Nominet has publicly advocated a more secure UK Internet<sup>21</sup> and the implementation of DNSSEC<sup>22</sup>. In February 2006, it employed Roy Arends, one of the authors of the first DNSSEC standards, as a researcher. In 2008, RFC 5155 (of which Arends was an author) proposed NSEC3 as a solution to prevent zone file enumeration. Therefore, Nominet invested in research to overcome a key obstacle, in order to pave the way for its implementation of DNSSEC.

### 8.3 Relationship between UK registry and registrars

The .uk domain does not operate any accreditation system for its registrars. It requires no professional standards, technical or operational competence to become a registrar. It is only necessary to fill in an application form and obtain a "tag" (access to Nominet's registry systems)<sup>23</sup>. To benefit for a trade discount (£5 per domain rather than £80), it makes sense for a registrar also to become a member<sup>24</sup>. Nominet has 2,800 active members, and 4,400 active tags<sup>25</sup>.

Nominet has the right to terminate or suspend a registrar's account for breach of the registrar contract, including failure to keep registrant information correct, and failure of good practice

---

<sup>20</sup> See <http://www.nominet.org.uk/disputes/courtcases/>

<sup>21</sup> eg <http://www.nominet.org.uk/news/releases/2007/?contentId=4286>

<sup>22</sup> eg [www.nominet.org.uk/digitalAssets/27762\\_Signing\\_the\\_Root.pdf](http://www.nominet.org.uk/digitalAssets/27762_Signing_the_Root.pdf) (2007)

<sup>23</sup> [https://secure.nominet.org.uk/flows/domain-tag-application.html?\\_flowExecutionKey=\\_c0EF4413E-1119-7D52-9091-D4BE0BEAA455\\_k9548206A-7285-6DC2-05D8-8BF97593FDF7](https://secure.nominet.org.uk/flows/domain-tag-application.html?_flowExecutionKey=_c0EF4413E-1119-7D52-9091-D4BE0BEAA455_k9548206A-7285-6DC2-05D8-8BF97593FDF7)

<sup>24</sup> <http://www.nominet.org.uk/governance/members/becomemember/>

<sup>25</sup> April 2011 Board Communique <http://www.nominet.org.uk/news/latest/?contentId=8395>

terms<sup>26</sup>. However, the good practice terms are fairly weak, and do not require any standards of behaviour or ethics (or even technical training) on the part of a registrar.

Moreover, Nominet has no effective power to expel a member, as expulsion requires a 90% vote of the membership<sup>27</sup>.

While the current arrangement has allowed the registrar marketplace to flourish, in the context of offering a trust service such as DNSSEC, Nominet is at a disadvantage compared to other TLD registries, who undertake some form of registrar accreditation. It has only loose control over the conduct of its registrars, and would not be able to guarantee any quality of service to .uk domain registrants.

#### **8.4 History and context for signing the second-level under .UK**

As we have seen, Nominet has been a leader in standards setting for DNSSEC. In a largely symbolic act, Nominet signed .UK in March of 2010. By signing .UK Nominet indicated its support for DNSSEC and broader deployment in the public Internet. But the structure of .UK prevented this from being much more than an act of support and a call to arms. In fact, at the time, Nominet made no attempt to put its new keys into any of the existing, alternative DNSSEC key stores. Their judgement was that, since the root zone was so close to being signed, there was no reason to complicate operations by switching authoritative trust anchors in a matter of month.

As we have discussed elsewhere, the .UK zone is a structured zone with a set of 14 second level domains. Eight of these second-level domains, including the statistically very important .CO.UK, are managed by Nominet. There is, in addition, a process for proposing future second-level domains. Since all of the .UK registrations take place in these second-level domains, Nominet's signing of them is an important step forward to future deployment of DNSSEC in the UK.

Starting in April and ending on May 18<sup>th</sup>, 2011, Nominet signed its second-level zones and arranged for the appropriate DS record to be in the root. This means that the mechanism is in place for a Chain of Trust to be built from the root zone of the DNS, through the .UK domains, down to the owner of a .UK domain. This is a significant step and it comes at the same time as the German ccTLD operator signing its zone.

Along with signing the zone, Nominet is aware that there needs to be a way for registrars who sell and maintain .UK domain names to build a full Chain of Trust for registrar customers. In the same timeframe, Nominet deployed a service that allows its registry systems to accept DS records from registrars. Along with a production service that allows a .UK registrar to upload, modify and view DS records, Nominet has provided a testbed that allows registrars to test their DNSSEC implementation.

The implication of this development is that .UK customers can now sign their zones (or, have a registrar perform this service on their behalf) and have the correct DNSSEC resource records

---

<sup>26</sup><http://www.nominet.org.uk/registrars/ra/racontract/>

<sup>27</sup> See article 3.6 at <http://www.nominet.org.uk/governance/articles/>

put into the correct places in the DNS. Beginning in May 2011, global Internet users could, if their resolvers were correctly configured, authenticate .UK DNS information where the domain name holder had decided to implement DNSSEC for the chosen zone.

With this development, the UK joins Germany and seven other nations with fully operational DNSSEC deployments at their ccTLD.

## 8.5 Corporate adoption of DNSSEC in the UK

As we have noted several times in this report, it is necessary but not sufficient for the second-level of .UK to be signed. Next, there needs to be adoption of DNSSEC by domain name owners and for DNSSEC services to be provided by registrars.

### 8.5.1 Previous Approaches to DNSSEC in the UK

There is some evidence of a base level of interest in DNSSEC in the UK. Even prior to Nominet's signing of the second-level of .UK, some owners of domain names in .UK were using alternative approaches for trust anchors. This meant that they could deploy DNSSEC in the absence of the root being signed and in the absence of a full Chain of Trust. In a survey of DNSSEC related traffic we have seen some of these domains appear in the public Internet.

The existence of these domains is good news for those who would advocate continued progress on deployment of DNSSEC. The owners of these domains are largely smaller organizations who have some interest in providing a level of trust through the DNS to their users, customers and members. This shows that there is a baseline of early adopter interest in the UK. That early adopter interest is one of the requirements for successful evolution of DNSSEC implementation.

What follows is a sample list of URLs where the underlying domain name is both a .UK domain and also used alternative approaches to providing trust anchors.

- Assoc.org.uk
- Bluechip.co.uk
- Exponent.co.uk
- Papaya.me.uk
- Emspublishing.co.uk
- Volatilepaintball.co.uk
- Ctha.assoc.org.uk
- Dataswift.co.uk
- Creativeparties.co.uk
- Vadt.co.uk
- Cromwellstudios.co.uk
- Geoff.co.uk
- Holisticinsurance.co.uk
- Romansoneeventrust.org.uk
- Ans.org.uk
- Seaviewpembrokeshire.co.uk
- Qaotiq.co.uk
- lwmc.org.uk
- Chromos.org.uk
- Wightmusic.co.uk
- Holistic-books.co.uk
- Gpregistrar.co.uk
- Datsec.co.uk
- Gantspeed.co.uk
- Rowlescourt.co.uk
- Thecastlepractice.co.uk
- Gptrainers.co.uk
- Skyblue.me.uk
- Emsv.co.uk
- lp-home.co.uk

**MC/080 DNSSEC Deployment Study**

- Freedeal.co.uk
- Anwickforge.co.uk
- Cord-it.co.uk
- Medinfo.co.uk
- Whitesfinefoods.co.uk
- Topcatnails.co.uk
- Motobins.co.uk
- Transcendenz.co.uk
- Alanbuxley.co.uk
- Checkmylists.co.uk
- Infracaninophile.co.uk
- Susanna-pearl.org.uk
- Itecworld.co.uk
- Datsec.org.uk
- Steve-c.co.uk
- Filebase.org.uk
- Pylon.org.uk
- Faelix.co.uk
- Waterloroadchurch.org.uk
- Dsns.co.uk
- Aleecat.co.uk
- Tala11.co.uk
- Hawaga.org.uk
- lwso.org.uk
- Krowdrah.co.uk
- Hodgkinsons.co.uk
- Datsec.me.uk
- Moorfarmbuilding.co.uk
- Alarmline.co.uk
- Kingswoodsurgery.co.uk
- Imperial.ac.uk
- Arboris.co.uk
- Costa-action.co.uk
- Fitness.assoc.org.uk
- Igpp.co.uk
- Stickylabels.co.uk
- Jamesweb.org.uk
- Oakridgehotels.co.uk
- Gnomon.org.uk
- Swanfieldchapel.org.uk
- Creativefancydress.co.uk
- Gpfovant.co.uk
- Flightcomparison.co.uk
- Eyeconomy.co.uk
- Unidos.org.uk
- Brackenborough.co.uk
- Edworthy.me.uk
- Complimentary.assoc.org.uk
- Irvineflyers.co.uk
- Jubileegroup.co.uk

### 8.5.2 Corporate adoption of DNSSEC in public facing DNS

As we discussed in the “Barriers” section of this report, one of the significant barriers to deployment is customer demand. Of all the ISPs interviewed in this project each mentioned that the lack of corporate demand for DNSSEC as an offering resulting in no work being done to provide it as a service. Where ISPs provide DNS services for their customers this is an unfortunate development.

ISPs, during interviews, almost unanimously suggested that, since DNSSEC has both start-up and ongoing costs, and since there was no customer demand to defray those costs, they were very unlikely to offer DNSSEC as anything but a custom service in the current economic environment. Two major ISPs in the UK accounting for a very large number of the UK’s customers indicated that they did not have organized testbed programs in place for DNSSEC.

We followed up this discovery with an experiment much like the one conducted on Swedish companies. Our question was: if you looked at the 100 highest-value, highest traffic sites in the .UK domain, would you find any evidence that .UK companies had at least experimented with DNSSEC (for instance, by signing a public facing zone and using an alternative trust anchor)? We used Alexa as the authority for which domain names had the largest amount of traffic and then picked the top 100 .UK sites.

For each of these 100 sites we used a DNSSEC profiler (a tool for examining the state of DNSSEC in a particular zone) to request and examine the DNSSEC related records from the zone.

In none of the top 100 sites in the .UK was there any evidence that the owners of the zone had experimented with DNSSEC prior to Nominet signing the second level domains in .UK.

### 8.5.3 Support for DNSSEC Adoption by UK Registrars

The survey, mentioned in the section above, may be an indication that many companies in the UK made a conscious decision not to experiment with DNSSEC until Nominet signed the second-level of .UK. We have no data to support this hypothesis.

On the other hand, it is clear that registrars and ISPs need tools that will help them market and deploy DNSSEC to their customers. In the absence of this part of the infrastructure, it is clearly more difficult for registrars (as an example) to invest in DNSSEC and attempt to market and deploy the technology.

Nominet has made a decision to deploy a DNSSEC signing service to attempt to address this requirement. While this doesn’t eliminate the need for a registrar to make both initial and on-going investments in infrastructure, it will simplify the signing of zones and significantly reduce the initial outlay that registrars would have to make to offer DNSSEC to their customers. With this service Nominet would sign customers’ zones and create the appropriate DNSSEC keys for the zone and the DS records for the parent.

This is a planned service – with initial beta deployment in July of 2011. It is evidence that Nominet understands that the barriers to deployment must be removed, where possible.

## **9. Issues for Consideration – What Constitutes Success?**

A successful implementation of DNSSEC does require that it's implemented across the complete namespace. In order for that to happen it would be necessary to sign the root (done) and then establish an unbroken chain of authentication through all Top Level Domains, right down to individual registrants. From technical, operational and political standpoints that is not achievable. Neither is it necessary in order to bring substantial benefit to large numbers of consumers. There is evidence that following the signing of the root a number of major registries have now signed their major top level domains with verifiable keys. The challenge is to both encourage others TLD registries and also those further down the chain of trust to play their part, but it will take time.

Other sections of this report set out many of the issues and challenges that need to be faced, the majority of which have no quick fix. Early indications do show there is already considerable momentum building which could lead to widespread adoption. This has not been the case before when various security fixes for the Internet have been developed and constitutes a positive sign that initial efforts to underpin DNSSEC deployment are succeeding. For DNSSEC to be successful that impetus must be maintained and nurtured. Regular reviews of its status and deployment on a global basis will be necessary to ensure that is happening. To set in place firm targets as a measure of success at such an early stage of deployment would be meaningless, it is far more appropriate to focus efforts on education, awareness and coordination with those parties who need to participate to make DNSSEC a success.

## **10. Issues for Consideration – Are Incentives Required for Greater Deployment?**

The Internet continues to grow at a phenomenal pace and over the next few years many changes will occur that will continue to fuel demand such as the widespread introduction of high speed broadband, the explosive growth of new devices, expansion of the namespace and extensive efforts to get underdeveloped countries on-line. That growth will further enhance the need for a more secure Internet as users become more sophisticated and aware. There is clearly a role for DNSSEC to play its part.

The very nature of DNSSEC makes incentives for deployment challenging. The strength of the system stems from the chain of trust that validates the authenticity of a DNS response. To be fully effective each party within that chain, which starts at the authoritative zone file, have to play their part. All have a different focus and role, yet the maximum benefit is derived by the end user, who often is unaware that DNSSEC exists or what role it fulfills. To date only technology savvy users are likely to have any understanding.

The real incentives for deployment are most likely to be self-generating as the Internet eco-system changes. Its unrivalled growth and world-wide acceptance as a critical infrastructure that supports the global economy will continue to fuel competition, also at the global level. Security

**MC/080 DNSSEC Deployment Study**

transactions, secure data and a high degree of trust will become increasingly important. The parties who pay due attention to those aspects will be the ones who succeed. That does not mean the initial bootstrap phase for deployment will be easy, but the nature and history of the Internet shows that when something is needed it happens and when that isn't the case no attempt to force the pace is successful.

## **11. Appendix A: Review of the State of DNSSEC Standards at the IETF**

The Internet Engineering Task Force is the standards organization responsible for DNS and DNSSEC. As we have seen, DNSSEC is an evolving standard – the evolution of the NSEC record is just one example of how things change as operational experience is gained. DNSSEC is a relatively mature technology, but the standards group routinely responds to operational, security and other requirements.

Internet Standards are historically called Requests For Comments (or, more simply, RFCs). The RFCs represent open, public standards that help guarantee interoperability for Internet technologies. The RFC series also provides guidance and experience documents related to Internet Technologies. DNSSEC is a part of the RFC Series.

### **11.1 Established Standards**

#### **11.1.1 Domain Name System Security Extensions (RFC 2535)**

This is the foundation document that established DNSSEC as an Internet technology. It describes the general operation of DNSSEC, the message flows and the resource records needed to make DNSSEC work. This document eventually became obsolete as DNSSEC was redefined in response to operational and deployment problems associated with RFC 2535).

Available at: <http://www.rfc-editor.org/rfc/rfc2065.txt>

#### **11.1.2 Domain Name System Security Signing Authority (RFC 3008)**

This document was an update to RFC 2535. It attempted to improve on that document by requiring that, in a secure zone, zone data must be signed by the zone key. This eliminated the ability to establish local policy for zone signing in DNSSEC. It marks the first attempt to address some of the operational concerns associated with RFC 2535.

Available at: <http://www.rfc-editor.org/rfc/rfc3008.txt>

#### **11.1.3 Indicating Resolver Support for DNSSEC (RFC 3225)**

This document established the bit in the eDNS header that tells DNS Servers that a DNS Client (Resolver) would like to have the security information included in the response to a DNS query. The original specification had mandatory transmission of DNSSEC resource records and was an operational problem as a result. Like RFC 3008, this was an attempt to improve the original specification without having to revise it completely.

Available at: <http://www.rfc-editor.org/rfc/rfc3225.txt>

#### **11.1.4 DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format (RFC 3845)**

This document is another modification of the original standard. This time the NSEC record is changed slightly so that it is able to communicate more than 127 domain names or resource

record types. This was another adjustment for the original DNSSEC protocol based on operational experience.

Available at: <http://www.rfc-editor.org/rfc/rfc3845.txt>

#### **11.1.5 Resource Records for the DNS Security Extensions (RFC 4034)**

By 2004 it had become clear that the original specification for DNSSEC would never receive large-scale deployment on the public Internet. A combination of protocol, security and operational problems led the IETF to reconsider the approach of incremental updates to the standard. Instead, the IETF decided to completely rewrite the standards for DNSSEC – incorporating the operational experience that had been gained in the preceding five years.

The new standard for DNSSEC was codified in a family of documents. This one, RFC 4034, documents the resource records to be used in DNSSEC. In particular, it defines DNSKEY, RRSIG, NSEC, and DS records.

Available at: <http://www.rfc-editor.org/rfc/rfc4034.txt>

#### **11.1.6 Protocol Modifications for the DNS Security Extensions (RFC 4035)**

This is another of the family of documents that replaced the foundation DNSSEC specification in 2005. In this document the protocol changes to the DNS that are needed to support DNSSEC are documented. This effectively obsoleted the older RFCs that provided the original specification for DNSSEC. It also collected and improved upon the “revision” RFCs that came before the new “family” of standards documents.

Available at: <http://www.rfc-editor.org/rfc/rfc4035.txt>

#### **11.1.7 Minimally Covering NSEC Records and DNSSEC On-line Signing (RFC 4470)**

Soon after the publication of the new “family” of standards for DNSSEC, operators discovered that it was simple to walk the zones covered by DNSSEC. The result would be that any implementation of the NSEC record in RFC 4034 would result in a zone that could be fully disclosed by incremental retrieval of domain names in NSEC records. This RFC was the first attempt to address the problem. It was eventually superseded by the definition of the NSEC 3 record.

Available at: <http://www.rfc-editor.org/rfc/rfc4470.txt>

#### **11.1.8 Use of SHA-256 in DNSSEC Delegation Signer (DS) Records (RFC 4509)**

This document specifies how to use the SHA-256 encryption digest type in DNS Delegation Signer (DS) Resource Records (RRs). DS records, when stored in a parent zone, point to DNSKEYs in a child zone.

Available at: <http://www.rfc-editor.org/rfc/rfc4509.txt>

### 11.1.9 DNS Security (DNSSEC) Opt-In (RFC 4956)

This document is an experimental standard that addresses the problem of the cost of secure delegations to unsigned zones for large, delegation-centric zones or zones where insecure delegations are updated rapidly. An example of this kind of zone is .com. In these types of zones the cost of maintaining the NSEC record chain may be extremely high and possibly not of value.

The experimental standard describes an opt-in approach. This approach allows a zone administrator the opportunity to remove insecure delegations from the full NSEC chain.

Available at: <http://www.rfc-editor.org/rfc/rfc4509.txt>

### 11.1.10 DNSSEC Hashed Authenticated Denial of Existence (RFC 5155)

In March of 2008, the standard that effectively made DNSSEC deployable was published. From the standard text:

*“The DNS Security Extensions included the NSEC RR to provide authenticated denial of existence. Though the NSEC RR meets the requirements for authenticated denial of existence, it introduces a side-effect in that the contents of a zone can be enumerated. This property introduces undesired policy issues.*

*The enumeration is enabled by the set of NSEC records that exists inside a signed zone. An NSEC record lists two names that are ordered canonically, in order to show that nothing exists between the two names. The complete set of NSEC records lists all the names in a zone. It is trivial to enumerate the content of a zone by querying for names that do not exist.*

*An enumerated zone can be used, for example, as a source of probable e-mail addresses for spam, or as a key for multiple WHOIS queries to reveal registrant data that many registries may have legal obligations to protect. Many registries therefore prohibit the copying of their zone data; however, the use of NSEC RRs renders these policies unenforceable.”*

This document, co-written by Nominet engineers, describes the NSEC3 document which would eventually be the tool that makes it possible to deploy DNSSEC in a situation where you do not want to prevent zone walking.

Available at: <http://www.rfc-editor.org/rfc/rfc5155.txt>

### **11.1.11 Use of SHA-21 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC (RFC 5702)**

The RFCs that provided the specification for DNSSEC provided a list of cryptographic algorithms to be used in DNSSEC. As cryptographic methods improve, there is a need to extend the list of algorithms that can be used in DNSKEY and RRSIG records. This standard is an example of one of those extensions.

Available at: <http://www.rfc-editor.org/rfc/rfc5702.txt>

## **11.2 Introductions, Operational Advice and Other Documents**

### **11.2.1 DNS Security Operational Considerations (RFC 2541)**

In this legacy document from March of 1999, the authors discuss operational aspects of key and signature generation, lifetime, size, and storage. They also discuss the security of the high level zones and make recommendations about the root zone (which would not be signed until 11 years later). Finally, the authors discuss operational issues for keys and signatures used in connection with the KEY and the legacy SIG DNS resource records.

Available at: <http://www.rfc-editor.org/rfc/rfc2541.txt>

### **11.2.2 A Threat Analysis of the Domain Name System (RFC 3833)**

In August of 2004, two authors critiqued the original specification for DNSSEC by attempting to figure out what threats DNSSEC was designed to protect against. The authors begin by saying:

*“Although the DNS Security Extensions (DNSSEC) have been underdevelopment for most of the last decade, the IETF has never written down the specific set of threats against which DNSSEC is designed to protect. Among other drawbacks, this cart-before-the-horse situation has made it difficult to determine whether DNSSEC meets its design goals, since its design goals are not well specified. This note attempts to document some of the known threats to the DNS, and, in doing so, attempts to measure to what extent (if any) DNSSEC is a useful tool in defending against these threats.”*

Available at: <http://www.rfc-editor.org/rfc/rfc3833.txt>

### **11.2.3 DNS Security Introduction and Requirements (RFC 4033)**

One of the three “family” documents that redefined DNSSEC in March of 2005. This is a general description of how DNSSEC works, what it can and cannot do, and how the family of documents fits together to completely describe DNSSEC.

Available at: <http://www.rfc-editor.org/rfc/rfc4033.txt>

#### **11.2.4 DNSSEC Operational Practices (RFC 4641)**

This document is intended to be a zone administrator's guidebook for using DNSSEC. The document discusses operational aspects of using keys and signatures in the DNS. It also discusses issues of key generation, key storage, signature generation, key rollover, and related policies.

Available at: <http://www.rfc-editor.org/rfc/rfc4641.txt>

#### **11.2.5 DNS Security (DNSSEC) Experiments (RFC 4955)**

To experiment with new DNSSEC technology in the public Internet causes problems for anyone using standard tools. As a result, it is difficult to experiment with new, non-backward compatible DNSSEC technologies. This document defines a way to conduct DNSSEC experiments without affecting the services available to those using public, current DNSSEC technologies.

Available at: <http://www.rfc-editor.org/rfc/rfc4641.txt>

### **11.3 Emerging Changes to DNSSEC**

#### **11.3.1 Client Signalling of Encryption Capabilities**

Digital Signatures are a key part of DNSSEC, but the current standard provides the clients, the resolvers, no way to signal which cryptographic algorithms they support. An emerging piece of work at the IETF provides this functionality as an extension to the capabilities the DNS clients already have. The primary goal of this idea is to measure the uptake of new cryptographic techniques in DNS clients that do validation.

Available at: <http://www.ietf.org/id/draft-ietf-dnsext-dnssec-algo-signal-01.txt>

#### **11.3.2 DNSSEC Policy and Practice Statement Framework**

The IETF is providing an advisory document for operators of DNSSEC zones that help them develop a policy and practice statement. This is intended as a checklist of things that should be in a DNSSEC zone operator's policy and practice documentation – and has, as another feature, the ability to be a partial guide to planning for DNSSEC implementation.

Available at: <http://www.ietf.org/id/draft-ietf-dnsop-dnssec-dps-framework-04.txt>

#### **11.3.3 Revision of DNSSEC Operational Practices**

The IETF provided (see above, RFC 4641) an operational handbook for zone administrators who are deploying DNSSEC. In the time since that was written there has been significantly more experience with deployment and operations. The best practices, from the most recent experience, is being used to revise the IETF's operational practices document for DNSSEC.

Available at: <http://www.ietf.org/id/draft-ietf-dnsop-rfc4641bis-06.txt>

## 12. Appendix B: Glossary of Terms and Acronyms

A Record	An Address Resource Record. The DNS uses this to provide a 32-bit IPv4 address in response to a query about a domain name.
Anycast	The communication between a single sender and the nearest of several receivers in a group. A technique to make DNS servers more widely available and globally distributed.
Authoritative Name Server	The DNS server that publishes information about a specific domain and the name servers of any domains subordinate to it.
BIND	BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.
Cache poisoning	The corruption of an Internet server's Domain Name System table by replacing an Internet address with that of another, rogue address. This can facilitate Web browser hijacking, the insertion of spyware or other malicious actions.
ccTLD	Country Code Top Level Domain (e.g. .uk .fr .us). Top level domain names associated with a specific sovereign nation.
DNS	Domain Name System. The hierarchical naming system built on a public, global database. Primarily used to translate names (for instance, <a href="http://www.bbc.co.uk">www.bbc.co.uk</a> ) into IP addresses (for instance, 190.23.102.17).
DNSKEY Record	A Resource Record that authenticates DNS Resource Record Sets.
DNSSEC	Domain Name System Security Extensions.
DS Resource Record	The Delegation Signer Resource Record. The DS resource record indicates the delegated zone is digitally signed and that the delegated zone recognizes a valid zone key for the delegated zone.
DNS Zone	A Domain Name System zone is a portion of the global DNS namespace for which administrative responsibility has been delegated.
ENUM	Refers to the Internet Engineering Task Force - RFC 6116 (standard) which deals with the use of the Domain Name System for storage of data associated with E.164 (telephone) numbers.
gTLD	Generic Top-Level Domain (e.g. .com, .net, .travel, .coop, .org). Top level domains not associated with a sovereign country.
IANA	Internet Assigned Numbers Authority. The organization responsible, among other things, for managing the root zone of the DNS.
ICANN	Internet Corporation for Assigned Names and Numbers.
IETF	Internet Engineering Task Force. The IETF is an open standards organization that develops and promotes Internet standards dealing in particular with standards of the TCP/IP and the Internet protocol suite.
IP address	A numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
IPv4	The 32-bit Internet Protocol addressing scheme
IPv6	The 128-bit Internet Protocol addressing scheme
ISC	Internet Systems Consortium. The makers of one of the most widely used DNS Servers – BIND.
ISP	Internet Service Provider – an organization that connects individuals, households, businesses and enterprises to the public Internet.
MX record	The Mail Exchanger record. This is a type of resource record in the DNS that specifies a mail server responsible for accepting email messages on behalf of a recipient. The set of MX records of a domain name specifies how email should be routed.

Name Servers	The Domain Name System is maintained by a Distributed Database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root name-servers, the servers to query when looking up (resolving) a TLD.
NSEC Record	Next Secure Record. Part of DNSSEC, used to prove a name does not exist.
NSEC3 Record	A follow-up to the NSEC Record – the major change was a technology that prevented finding all the records in a DNS zone – a privacy and security issue. Being able to recover all the records in a DNS Zone by simply retrieving all the NSEC records is called “walking the zone.” NSEC3 prevents this
PGP	Pretty Good Privacy. A public key encryption technology for ensuring that messages, files and other objects stored or sent by a computer cannot be read by anyone other than those intended.
Resolver	The client-side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought e.g. translation of a domain name into an IP address.
RFC	Request For Comments. A document published by the Internet Engineering Task Force describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.
Root	Refers to the top level of the DNS hierarchical namespace. The “root” is the highest level “Zone” of the Internet and currently has about 320 domains in it (e.g. .com, .uk, .net, .org, .fr and so forth)
RRSIG Record	DNSSEC Signature Record. The Signature for a DNSSEC-secured record set.
TCP/IP	Transmission Control Protocol/Internet Protocol. One of the core parts of the network protocols for the Internet. Compared to UDP it ensures that packets arrive in the right order, are not lost in transit and are not duplicated. It has more overhead than UDP but provides more consistent communication.
TLD	Top Level Domain. A domain at the highest level of the naming hierarchy of the DNS. These names are installed at the “root zone” of the DNS. In <a href="http://www.bbc.co.uk">www.bbc.co.uk</a> the TLD is “.uk” In <a href="http://www.google.com">www.google.com</a> the TLD is “.com”
Trust Anchor	The top level point in the chain of trust where a domain is signed, normally the Top Level Domain Registry (e.g. .uk or .com) or, since July 2010, the root zone of the DNS.
SSL	Secure Socket layer. A tool to provide secure communications over the Internet – widely used by web browsers. An older technology it is now superseded by TLS.
TLS	Transport Layer Security. The most commonly used tool for securing communications over the Internet – especially between web browsers and web servers.
UDP	User Datagram Protocol. One of the core parts of the network protocols for the Internet. Compared to TPC/IP it is much simpler and has less overhead. However, packets may be lost, arrive out of order or appear to be duplicated. The application using UDP must cope with these features.
Unicast	The communication between a single sender and a single receiver over a network.

**MC/080 DNSSEC Deployment Study**

VPN	Virtual Private network. A mechanism that allows one to attach a Local Area Network or single computer to a remote network securely. The VPN uses encryption to support secure remote access to share private data and other network resources
Zone Files	A DNS zone is a single part, often an individual domain, of the name structure of the DNS. The zone file almost always contains mappings between domain names and IP addresses. These mappings are stored as resource records (RRs).