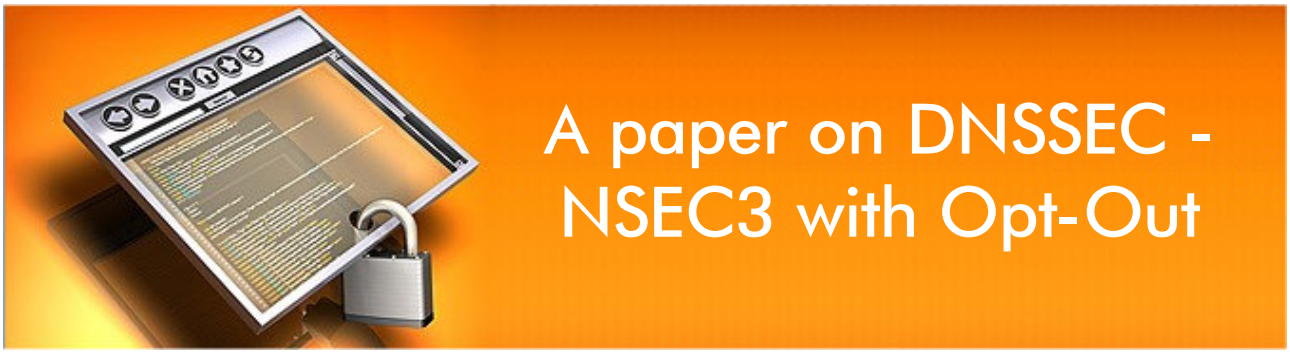

DNSSEC – A Way Forward for TLD Registries

Method for faster adoption of DNSSEC

Providing greater security with minimal impact on customers, registries and Zone Management

A white paper by

CommunityDNS

September 2009

Table of Contents

Executive Summary

DNSSEC is an emerging standard helping Net users with domain name verification through authentication.

Challenges include:

- Domain owners submitting keys to Registry
- Impactful due to larger data requirements
- Vulnerabilities introduced with current design
- Slow adoption due to all-or-nothing approach

NSEC3+OptOut is designed to speed adoption of DNSSEC through:

- Manageable implementation increments
- Provides options for better end-user experience
- Less impact to the unsigned user.

This paper explores how DNSSEC may be adopted quicker while at the same time providing users with an opportunity to by-pass some of DNSSEC's current vulnerabilities. In addition, this paper also explores how Registries can more easily tackle the process of implementing DNSSEC.

DNSSEC (DNS SECurity), an emerging standard developed to assist users gain assurance that the remote DNS server they are seeking to communicate with has been independently verified and are genuine.

One challenge for DNSSEC deployment faced by Registry operators is empowering the domain name owner with mechanisms to submit their unique domain name authentication key to the Registry. This process requires the key provider for a specific domain name to be authenticated, usually by the Registrar. Then the Registrar needs to have mechanisms in place to accept keys from these providers, who in turn submit the key data to the Registry for inclusion in the TLD zone file on behalf of their customer.

From an operator perspective, another challenge deals with the additional data elements required in the Zone File to accommodate DNSSEC; making the size and management of the Zone Data increasingly complex. For example, when becoming DNSSEC compliant the zone size alone can increase by as much as eight times.

From the users perspective, the challenge associated with DNSSEC is keeping the user informed as to occasions when DNSSEC is enabled and also when verification fails. As a consequence Application Level providers needs to ensure their products are optimised for DNSSEC compliance. Such issues can taint the benefits of and dampen adoption of DNSSEC by the user, and critical mass may only occur once DNSSEC is considered mature.

Regarding today's Root Server structure, four factors have been determined to have an impact on the scaling of the Root; those being DNSSEC, IPv6, IDNs and new TLDs. DNSSEC has been determined to have the largest impact on the scaling of the Root by having the largest increase in size to the currently small Root file. DNSSEC will:

- Increase the amount of data required for each TLD.

- Increase the number of variables per TLD
- Increase the number of changes per TLD per year.

DNSSEC is currently available in two different forms; NSEC and NSEC3. This paper explores the using by TLD Registry operators of a variation of DNSSEC with an Opt-Out option; an option achievable through NSEC3+OptOut. NSEC3+OptOut allows:

- Users to become compliant on either a specified time frame or on a schedule that better aligns with organizational objectives.
- Allows TLDs the opportunity to tackle DNSSEC compliance in more manageable increments by allowing TLDs to move forward without the requirement of having ALL associated names compliant before moving forward.
- Mitigates existing design vulnerabilities.
- NSEC3 with opt-out requires customers to explicitly state they want to use DNSSEC and thus impact on Zone sized is small. Standard NSEC or NSEC3 requires all records are signed.
- Less "impact" on "non-signed" users at all levels in the DNS tree.

This Paper does not address vulnerabilities current is all forms of DNSSEC namely:

- Use of ITAR(s) either with or without a Signed ROOT.
- Key Management issues in general and Key Roll-Over in particular.

Problems with transferring a domain from one name server provider (Registrar) to another without down-time.

What Is DNSSEC

DNSSEC is a verification mechanism for DNS data allowing end users the ability to verify intended destination's domain name.

The added benefit of DNSSEC is the establishment of a "chain-of-authentication".

DNSSEC:

- Is not a data encryption mechanism
- Does not provide error correction
- Does have an error recovery mechanism
- Currently introduces additional vulnerabilities

DNSSEC is a verification mechanism for DNS data. It allows an end-user to verify that the zone data they have been presented with was published by the person who holds the private key for that domain. If TLD operators obtain a referencing tag called a "finger print" of their customer's public key and include it in their zone, end users will be able to use this to verify the customer's zone data. By signing these finger prints (DS Records) with TLD's own keys, an end user can use the TLD operators keys to verify the customer's key and hence verify they have the right keys for the customer's zone. This is called the "chain of authentication".

DNSSEC is not an encryption mechanism and provides no security to prevent snooping on what queries are being done by which users.

DNSSEC does not have an error correction mechanism

DNSSEC Application providers have introduced with different levels of success, an error recovery mechanism, designed to clear out all data that had failed verification to the highest point where verification succeeded.

In this way, DNSSEC provides additional mechanisms by which DNS resolution may fail. Therefore, some customers may prefer to take their chances with their existing zone data – and keep the status-quo by not signing their zone.

For these users we must try and retain the existing stability, reliability and speed that has historically been a key feature of DNS resolution.

However, for domain holders customers, for example those dealing with financial transactions, may feel that it would be better that the end user is not presented with a web site at all than run the risk of having the users sent to the wrong site.

For these users we must provide the ability for them to sign their zones and provide them with the chain of authentication they need in order for their zone data to be publicly verifiable.

Benefits of DNSSEC

The key benefit of DNSSEC is in providing a mechanism where Internet users are confident about reaching their intended sites/ servers.

DNSSEC provides a mechanism by which an end user can guarantee that the DNS data they have is the same as that which was published by the holder of the zone's private key.

Currently when an end-user visits a web site they can not be sure that the site they are visiting is the one the zone owner published. With a completely DNSSEC signed DNS tree, the end user can be sure (and prove cryptographically) that the DNS data they have in their hand is correct.

The side benefit of DNSSEC is establishment of a "Chain-of-Authentication" between the Root and the destined site.

This is of great benefit in itself, however, it is undoubtedly in between the end user and the destined site. The new application this will unlock that the true benefit of DNSSEC will become apparent.

Once a full chain of authentication can be established all the way to the ROOT zone, the flexible, reliable and fast distributed database that is DNS will become the backbone for a whole range of new applications that will be opened up by the benefit that verifiable DNS provides.

Specifically, there are a wide range of existing applications that require verifiable public keys in order to provide secure and guaranteed communication. A DNSSEC signed zone can provide this mechanism.

DNSSEC comes in two basic flavours:
- NSEC
- NSEC3

NSEC allows the vulnerability of "zone walking" which can limit the range of new applications for which DNSSEC would be appropriate.

NSEC3 solves the "zone walking" vulnerability through the use of an irreversible hash.

NSEC3+OptOut adds flexibility and scalablility for DNSSEC implementation through the Opt-Out option benefitting the registry, customer's zone file and the end user.

NSEC3+OptOut will result in the increase on zone size being kept significantly smaller.

Different Flavours

DNSEC comes in two different flavours, "NSEC" (represented and expanded on in RFC 4034, 4035 and 4036) and "NSEC3" (represented in RFC5155).

DNSSEC provides a mechanism by which all the zone date can be verified. For every set of resource records a signature is created. With this signature the client is able to verify the resource record data. To proof the non-existents of a records 2 techniques can be used:

NSEC

"NSEC" works in two main ways – Firstly it creates a chain from one record to the next so that it can be proved where a name does not exist, and finally, it creates a list of which resource records exist for any particular name, so it can be proved where there is no data for any particular record type.

NSEC3

NSEC3 is a variation on NSEC that essentially provides exactly the same capability by a slightly different mechanism.

With "NSEC" the chain of records chains the actual record names in the zone file. This means all you have to do is obtain one name that exists in the zone file and you can follow the chain to obtain a copy of the entire zone – this is termed "zone walking". There are some circumstances where this was considered undesirable. If, for example, the zone file was a published list of e-mail keys allowing for the verification of encrypted e-mail, then by "walking the zone" an unauthorised third party could obtain a list of all the e-mail addresses (or domain names) in that zone.

It was therefore clear that the ability to "walk the zone" would limit the range of new applications that DNSSEC would be appropriate for.

"NSEC3" solved this by creating an irreversible hash (checksum) of each name in the zone and then creating the chain on these "hashed" names. Queries directed at these "hashed" names will always return NXDOMAIN (Name does not exist) – thus it is impossible to walk the list of hashed names. But even if it were possible, it would not be possible to use this to re-create the list of real names.

However, if a query comes in for a name that does not exist we

can still prove it does not exist because we can provide enough information to prove there is no hash record of the name requested. The client can calculate the hash value of his query and evaluate if it is between the received hashes from the DNS server.

NSEC3+OptOut

"NSEC3" provides an additional feature aimed specifically at TLD operators to make it easier for them to implement DNSSEC. This feature is called "opt-out".

With standard "NSEC" and "NSEC3" all records in a zone are signed. However, with "Opt-Out" only the authoritative data in the zone file (e.g. the zone's SOA record) and those delegated zone that are themselves signed will be signed by the TLD operator.

So if a TLD operator has 50,000 names in their zone of which 1% have signed their own zone, under the opt-out scheme, the TLD zone will contain about 500 signed names instead of 50,000. With an average size of around 350 bytes per set of signed records (NSEC3+RRSIG) using Opt-Out will result in the increase on zone size being kept very significantly smaller.

If all delegated zones in a TLD are themselves signed then the only difference between using Opt-Out and not would be a flag to say it had been used. However, if no delegated sub-domains are signed the zone file will be only a little different from an unsigned zone file.

Advantages and Disadvantages of These Three Options

Changes in a non-OptOut zone means approximately 85% to 95% of the zone file changes regularly.

Changes in an NSEC3+OptOut means less of the zone file changes regularly as changes will only apply to the names that have opted to be signed.

The zone size with basic NSEC or NSEC3 will increase by as much as 8 times.

With standard NSEC an end user can verify :-

1. The data they have been given is correct
2. Where the name exists, but there is no data
3. Where the name does not exist
4. Obtain and verify data they need in order to verify a delegated zone

NSEC3 provides exactly the same ability. However, the price to be paid is that an NSEC (or NSEC3 without use of opt-out) record must be created for every name in the zone and an RRSIG record must be created for every set of records in the zone.

Typically this increases the zone size by up to 8 times. This will therefore increase the time it takes to transfer the zone and the time it takes for the newly transferred zone to be loaded for serving.

All replies sent out (when the client has set the special "I want DNSSEC" flag in the query) must contain at least one RRSIG record and may contain up to three NSEC/NSEC3 records, plus their corresponding RRSIG records. For an NXDOMAIN reply this means a reply will increase from about 100 bytes to about 1,000 bytes for NSEC or 1,500 bytes for NSEC3.

For a delegated sub-domain that is not signed the reply will go from about 150 bytes to 500 for NSEC or 1,000 for NSEC3. For a delegated sub-domain that is signed the reply will go from about 150 bytes to 500 for both NSEC and NSEC3.

For NSEC3 with Opt-Out the size of replies are comparable with standard NSEC3, however, the proof provided and the work required to achieve the answer will be different.

The corresponding proofs for NSEC3 with Opt-Out are :-

1. The data on authoritative records or delegated sub-domains that are signed can be verified, but records provided on unsigned sub-domains cannot be verified.
2. For an authoritative record or a signed delegated sub-domain it can be proved whether resource record of a particular type exist or not.
3. It can be proved that an authoritative record or a signed delegated sub-domains does not exist by a particular

NSEC and NSEC3 require additional server load due to signing large amounts of data.

NSEC and NSEC3 require increased bandwidth to handle larger zone transfers.

NSEC3 with OptOut does *not* require added server load due to smaller amounts of data being signed, nor does it require increased bandwidth due to marginal increase in zone file size.

name – however, it cannot be proved whether an unsigned sub-domain exists or if the name simply does not exist at all.

4. For zones signed with NSEC3+OptOut the security provided for users who have signed their zones is exactly the same as for an NSEC3 zone that does not use OptOut. For unsigned zones under the signed TLD the security level doesn't change. A signed TLD doesn't increase the security of an unsigned zone under this TLD.

Further more, a requirement of DNSSEC is that the keys used to sign the data (the K-KEY) are changed regularly in order to mitigate against replay attacks. When this is done every single RRSIG record will change. For a non-OptOut zone this will typically mean in the region of (by volume) 85% to 95% of the zone file changing.

In fact, even if the zone file is re-signed using the same key but to cover a different time period, all RRSIG records will change.

Summary:

With NSEC and NSEC3:

The zone file will be considerably larger, but the existence or non-existence of any resource record or name can be conclusively proved.

The CPU load will increase considerably in both the time it takes to load the zone and time it takes to generate answers and the memory requirement will increase in line with the zone size anywhere by as much as 8 times.

The load on the server that generates the zone will also increase because of the additional workload in signing all the data.

The increase in bandwidth required for zone transfer (and therefore the time taken in the transfer) will increase in line with the zone size – i.e. up to 8 times.

With NSEC3+OptOut:

The zone will only be marginally larger (depending on the number of signed sub-zones) and the proofs that can be provided for authoritative data or a signed delegated sub-domain are exactly the same as with standard NSEC3. But the ability to provide proof on non-existent or unsigned delegated sub-domains will be lost – in lay terms, if the user doesn't care

about securing his domain, why should you?

This means that, as is the case with a totally unsigned domain (i.e. now, for most TLDs), it could be possible for an attacker to convince a resolver that an unsigned sub-domain exists where really it does not or to re-direct an unsigned sub-domain to different set of name servers.

It is likely that an increase in CPU load and memory usage will be marginal – although this will be implementation specific. Any increase in bandwidth required for zone transfer will be marginal.

It allows for quicker adoption of DNSSEC by providing signed services for those who wish to be signed instead of having for all parties involved to provide the resources to sign every zone and subzone for a respective TLD. Users will have the option to sign and opt-in on their schedule, thus increasing their confidence in the signing process.

In all cases replies to queries (and therefore outbound bandwidth) on zones that are DNSSEC signed will be considerably larger.

Software that Supports DNSSEC

DNSSEC supported platforms include:

- BIND
- NSD
- Unbound
- CommunityDNS
- Nominum

ISC's Bind 9.6.1-P1 is ISC's current recommended distribution for DNSSEC and is fully compliant with all relevant RFCs for NSEC, NSEC3 and NSEC3+OptOut. As of writing 9.7.x is still in beta. It can act as both an authoritative master / slave or recursive resolver. "Bind" is open source.

NL-Labs' NSD 3.2.3 and above is fully DNSSEC compliant. It can act as both an authoritative master / slave or recursive resolver. "NSD" is open source.

Unbound v1.3.3 or above is a caching recursive resolver that supports DNSSEC and DNSSEC verification. "Unbound" is open source.

CommunityDNS provides world class Anycast DNS Slave services using a custom-written DNS server designed specifically for high performance name resolution Anycast services. CommunityDNS service is DNSEC compliant providing very high speed service tuned specifically for NSEC3 and NSEC3+OptOut.

Nominum provides a DNS slave service that is fully DNSSEC compliant.

Recommendations

TLDs should embrace DNSSEC by signing their zones with NSEC3+OptOut as it will be less impactful and make for quicker adoption

Based on our testing, we recommend that TLDs proceed with signing their zones on the basis of NSEC3 with OptOut. This will:-

1. Provide Security for customers who need it
2. Minimise the immediate impact on existing systems in terms of memory, CPU load, bandwidth and storage.
3. Allow them to move to a fully signed zone in the future, if and when they feel this is necessary.
4. Avoids the potential exposures within the design of DNSSEC, NSEC and NSEC3.

Additional Considerations

Registry operators will need to accept DS records from customers for the zone file.

In order to provide the full chain of authentication, registry operators will have to ensure that they are able to accept the finger print (DS) records from their customers (often via a Registrar) and include them in the zone file.

If the Registry uses EPP they will need to refer to RFC4310 for the DNSSEC extensions to EPP.

Note: even if a registry does not sign its zone they could include their customer's DS records. However, they would not be verifiable until the TLD zone is itself signed. Therefore there would be no chain of authentication.

Two DS records for each signed zone. Each DS record represents the customer's public key using SHA1 and SHA256.

Under the current scheme there will typically be two DS records for each customer's signed zone. These are a hash of the customer's public key using SHA1 and SHA256. In text form in the zone file these will be 50 and 75 bytes respectively plus the "<name> IN DS" prefix and optional TTL.

DS records need to be correct else the unverifiable zone will be rejected.

As these DS records are used to verify the customer's DNS data, it is vital that they are correct otherwise the customers zone will become unverifiable and therefore be rejected by a verifying resolver.

"orphaned" or "prompted" GLUE records – Explained

A Registry should include "glue" address records in the parent zone

If the name servers for a zone are within the same zone, there will be a problem resolving that zone. The solution is to include "glue" address records in the parent zone, giving the resolvers a non-authoritative "hint".

I.e. If the zone "example.com" has name servers :-

```
example.com. in ns ns1.example.com.
example.com. in ns ns2.example.com.
```

In order to resolve the domain, we will need "glue" records :-

```
ns1.example.com. in a 1.2.3.4
ns2.example.com. in a 5.6.7.8
```

For a zone signed with NSEC3+OptOut, the existence of glue records is irrelevant. As before, if "example.com" is unsigned, then none of these records will be signed. If "example.com" is signed then, as before, only the DS records will be signed.

The owner of "example.com" may also own other zones that use these names servers. This has no implications to signing the zone.

However, if "example.com" expires and the owner chooses not to renew it. The registry has three choices.

1. If "ns1.example.com" and "ns2.example.com" are not used by any other domain they could simply and safely drop the glue records and there is no implications to the signing of the zone.
2. If these name servers are used by other names within the zone, the registry could still choose to drop these glue records. This would stop all zones that used these names servers from resolving, but it would have no implications to the signing of the zone.
3. The registry could choose to keep these address records in the zone – maybe because they are used by another domain name, or simply because it is too time consuming to decide whether they are required or not.

If the registry chooses option 3 and leave the address records in the zone file, then they create an "orphaned" or "promoted" glue record.

In fact, these address records are no longer "glue" entries as "example.com" is no longer a delegated sub-domain. These entries are now simply authoritative address records within the parent zone (in our example the dot-COM zone).

"orphaned" or "prompted" GLUE records – Implications

Registries should remove all "orphaned" or "promoted" glue records before signing the zone.

As explained, "orphaned" or "promoted" glue entries are authoritative records. If the parent zone is signed, these authoritative records **must** also be signed. In this scenario, signing the zone with or without "opt-out" is irrelevant.

Hash records for both the promoted glue records and the extinct parent (in our case "example.com") must also be created. This proves that there is no data available for the extinct parent as this is now the Closest Encloser for the promoted glue records.

Why is this important?

A registry signing their zone using NSEC3+OptOut could generate possibly thousands of "orphaned" or "promoted" glue records unless they has taken steps to eliminate them.

A registry would normally only expect to generate a few NSEC3 and RRSIG records (one for every signed sub-zone). However with NSEC3+OptOut, they may in fact end up with many thousands of NSEC3 & RRSIG records.

Recommendation

We recommend that registries takes steps to eliminate these "orphaned" or "promoted" glue records before going ahead with signing the zone.

DNSSEC using NSEC and NSEC3 will see an incremental increased zone file size by as much as 8% whereas an increase of as much as 5% will be seen when using NSEC3+OptOUT.

The time taken to sign and load the zones will be significantly less due to smaller numbers of signed names.

"Zone Walking" is no longer an issue.

Using NSEC3+OptOut results in:

- Quicker adoption of DNSSEC
- Less impact on Root scalability
- Flexibility for TLDs through incremental adoption
- Provides users with less exposure to current vulnerabilities
- Provides non-DNSSEC-aware users with a better user experience
- Allows organizational adoption based upon established objectives

Summary

	NSEC	NSEC3	NSEC3+OptOut
Provide security for customers who sign	Yes	Yes	Yes – exactly the same as NSEC3
Provide security for authoritative data in the zone file	Yes	Yes	Yes – exactly the same as NSEC3
Prove NXDOMAIN	Yes	Yes	No – but can prove there is no signed sub-domain by that name
Prove NO-DATA	Yes	Yes	Yes (for authoritative data in the zone)
Prove Unsigned sub-domain	Yes	Yes	No – but can prove there is no signed sub-domain by that name
Prove Wild card match	Yes	Yes	No – but can prove there is no signed sub-domain by that name
Increase zone size	Up to 8 times	Up to 8 times	< 5% (depending on the numbers of signed subdomains)
Time to sign zone	Long	Long	Not much longer than creating zone (depending on the numbers of signed sub-domains)
Time to load	Long	Long	Not much longer than unsigned zone (depending on the numbers of signed sub-domains)
Guaranteed un-Walkable	No	Yes	Yes
For TLDs ONLY	No	No	Yes

If a TLD signs with NSEC3+OptOut it is important to note that their customers can use either NSEC or NSEC3 – it is NOT recommended that customers should use the OptOut as there is a need to positively confirm a name does not exist.
With a fully signed NSEC3 zone, in theory attackers can convince a resolver that an unsigned sub-domain exists that hashes to the same result as an unsigned sub-domain that does exist.

However, with 2^160 (~1, 460, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000) different possibilities it will be hard to find one and it is likely that the name itself will not be useful (e.g. it will appear to be made of random characters). It will almost certainly be cheaper to simply buy a name!

About CommunityDNS

With offices in the US, the UK and Japan, CommunityDNS is the global Anycast provider successfully supporting over 120 million domain names from over 97 TLDs, processing over 18 billion queries per day.

With security integral in the network's initial design, CommunityDNS was chosen to work as a contributing partner in a Project of the European Commission Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme, administered by the European Commission - Directorate-General Justice, Freedom and Security.

CommunityDNS provides global DNS Anycast services, fully managed DNS platform services and DNS white-labelling supporting DNSSEC, IPv4 and IPv6 queries.

More information regarding CommunityDNS may be found at: http://communitydns.net/facts.html

Contact Us

CommunityDNS.net
Carpenter House
Broad Quay
Bath
BA1 1UD
UK

feedback@CommunityDNS.net