

ccNSO IANA WG: DNSSEC BRIEFING and Root Zone Signing (Part I)

Date: 4th February 2008

Summary

This document is the first part of a briefing from the ccNSO IANA Working Group about DNSSEC, provided in response to the ccNSO demand: <http://ccnso.icann.org/about/minutes/ccnso-minutes-31jul07.pdf>
"the IANA Working Group is asked for help in providing input to the Council on Root Zone signing from a technical perspective."

There were various related discussions in the group, revealing different possible strategies to manage a signed zone, and to deploy DNSSEC. We took the opportunity to briefly report about our discussions in order to provide a better overview of the issue.

This first part provides a general background about about the DNSSEC protocol and operations, as well as a list of references. It also reports about discussions related to the deployment of this technology at a global level, and launch the operational issue of signing the root zone.

A second part, which is not yet completed, will focus on practical cases and scenarios, including the Root Zone Case.

Table of Contents

PART I: General Background

1. Introduction

2. DNSSEC Background

- 2.1. Why DNSSEC ?
- 2.2. What is DNSSEC ?
- 2.3. DNSSEC, ICANN, ccNSO DNSSEC Survey

3. Signing, Publishing

- 3.1. What does 'signing a zone' means
- 3.2. Key dissemination
 - 3.2.1. Principles
 - 3.2.2. Alternatives
 - 3.2.3. Key Time Life and key rollover
 - 3.2.4. Emergency plan
- 3.3. What does serving a signed zone means ?

(PART II : Practical cases (TBW))

A. References (Main Documents, Statements and Portails)

B. Annexes

1. Part II table of content
2. Contacts

PART I: General Background

1. Introduction

DNSSEC is a protocol designed to verify the authenticity and the integrity of DNS responses. As such, it improves the DNS service, and also increases its ability to resist some forms of attack; therefore DNSSEC could improve global DNS security.

DNSSEC implementation in the public DNS tree has been a recurrent topic discussed over the past years within the ICANN community.

The root zone is at the top of the DNS tree; since DNSSEC relies on a chain of trust built in the DNS tree, and traversed over DNS resolutions, the root zone signature is pivotal to global DNSSEC deployment.

The IANA working group was asked to provide input on this subject:

<http://ccnso.icann.org/about/minutes/ccnso-minutes-31jul07.pdf>

"the IANA Working Group is asked for help in providing input to the Council on Root Zone signing from a technical perspective."

This paper intends to fulfill this request.

There are some high level issues related to DNSSEC, such as introducing a zone signing process into operations, managing keys, scaling DNS servers in a DNSSEC context, information exchange with the parent zone, collecting keys, etc. Each were discussed in the IANA WG.

This paper briefly reports those discussions.

In particular, the root zone is considered, including information about IANA's ongoing activities with regard to DNSSEC, especially those related to the IANA DNSSEC testbed [REF 7]:

<https://ns.iana.org/dnssec/status.html>

We also took the opportunity to briefly contemplate general matters that may require attention in the case of ccTLDs.

As such, this paper does not intend to provide a formal position about whether or not DNSSEC should be deployed in the public DNS tree, nor does it intend to indicate if the root zone should be signed or not. In addition, it is not written in order to replace relevant technical or operational documentation (see reference section for relevant documentation, in particular IETF RFC [REF 8 9 10 11]).

However, this paper does seek to examine the different possible scenarios, and to help the reader to better grasp the benefits and risks of DNSSEC, with a special focus on root zone management, as well as identifying some of the main issues to be considered before planning a DNSSEC implementation.

2. DNSSEC Background

2.1. Why DNSSEC ?

The strength, robustness and flexibility of the DNS is as a result of its highly distributed architecture. This can also be seen as its weakness, since a DNS response obtained by a final user may have to pass through unsecure layers and equipment (including local networks, local resolvers, DNS cache, etc.): there are many links over a resolution process that may be vulnerable to malicious activities.

As most internet applications, such as web or mail protocols, rely on DNS responses to permit dialogue between internet users, corrupt DNS data dispatched on the internet could, in the worst case, lead to the mis-directing of web pages or mis-delivery of e-mails.

Knowledge about this kind of DNS vulnerability is not new and was identified many years ago.

DNSSEC is a protocol that improves the ability of the DNS to resist attacks against vulnerable equipment; it protects DNS information from possible corruption, even if the channel used to transport is unsecure.

2.2. What is DNSSEC ?

DNSSEC consist of asymmetric cryptographic signatures included in the DNS, adding security features to the DNS [REF 8].

It allows for the verification of the authenticity and the integrity of a DNS response, by traversing a chain of trust over DNS resolutions, anchored from the authoritative publisher of a specific DNS record, to the user DNS application that asks for it (therefore, it also protects against false denial of existence in responses).

In other words, in a full DNSSEC environment, a user asking to connect to a web site will be able to check that his web browser has received the correct authoritative DNS information about the web site. (that is: that the information he has received is the one that was published by the authoritative DNS server for the site name).

DNS information would be signed before being published and could not be faked anymore: DNSSEC protects against some kinds of DNS abuse and, as such, can be a major DNS security improvement.

However, it would not be appropriate to say that DNSSEC "secures the DNS", since it doesn't solve all DNS security issues. It does not protect against DDos attacks for example, nor against the many misconfigured or outdated DNS software that is present on the net [REF 2].

Moreover, DNSSEC requires the implementation of strict and rigorous general security policies in order to be usefully and effectively deployed [REF 11]; DNSSEC adds security, as long as strict security rules are respected when deploying this technology : DNSSEC may secure the DNS as long as it is operated in secure environment. (Vint Cerf: "Security is a mesh of actions and features and mechanisms. No one thing makes you secure." [REF 1])

Scaling is another issue to consider, since DNSSEC introduces a significant increase of information circulating in the DNS responses [REF 14 15 16].

2.3. DNSSEC, ICANN, ccNSO DNSSEC Survey

Over the past years, discussions about the implementation and deployment of DNSSEC have taken place within the ICANN community.

Notably, the SSAC has facilitated exchanges across the community about DNSSEC during the ICANN public meetings, and encouraged the use of this technology, at least for testing:

<http://gnso.icann.org/meetings/crocker-ssac-kl-18jul04.pdf>

<http://www.icann.org/meetings/saopaulo/presentation-ssac-07dec06.pdf>

<http://www.icann.org/meetings/lisbon/agenda-DNSSEC-28mar07.htm>

<http://ccnso.icann.org/meetings/san-juan/members-report-v2-2.pdf>

<http://losangeles2007.icann.org/node/53>

Indications about discussions between DoC, ICANN and Verisign for a signed DNS root zone implementation are known:

<http://icann.org/topics/vrsn-settlement/revised-root-transition-agreement-clean-29jan06.pdf>

Some ccTLDs have been quite proactive about DNSSEC, and have started to partially implement this technology, by signing their TLD zone such as .se or .pr. The most recent announcements within the ccTLD community indicate that some registration chains have deployed and fully compliant with DNSSEC (.bg).

RIPE has also received the IAB endorsement to deploy this technology for E164.ARPA zone, and has started to do it:

<http://www.iab.org/documents/correspondence/2007-07-24-iab-itu-dnssec-e164.html>

Finally, the RIPE NCC has sent a letter to ICANN requesting the DNS Root be signed:

<http://www.icann.org/correspondence/pawlik-to-cerf-07jun12.pdf>

DNSSEC has also been discussed within the ccNSO, at the San Juan and the Los Angeles meetings:

<http://ccnso.icann.org/meetings/san-juan/presentations.htm>

<http://ccnso.icann.org/meetings/san-juan/amended-ccnso-council-minutes-27jun07.pdf>

<http://ccnso.icann.org/meetings/losangeles/presentations.htm>

also [REF 5 6 7]

DNSSEC was also a subject of debate across the ccTLD community. One of the main inherent issues identified was that this technology provided new possibilities for zone enumeration ("zone walking" issue). NSEC3 is the fix which solve this for DNSSEC, and is now a standard [REF 12]. However, tests and operational reports of this new version of DNSSEC in real world environment are still quite rare.

A survey on the usage and knowledge of DNSSEC was also conducted amongst ccTLDs in September and October 2007, it received 61 replies [REF 5].

The results show that, although only very few respondents have introduced DNSSEC in their registry (7%), almost all of them know what DNSSEC is. Most respondents think that they will introduce it within the next three years:

<http://www.ccnso.icann.org/surveys/dnssec-survey-report-2007.pdf>

3. **Signing, Publishing**

3.1. What does 'signing a zone' means

Before considering the zone signature process, it needs to be repeated that DNSSEC doesn't secure the DNS by itself. DNSSEC could be one of the elements that a zone operator may consider in a more general security plan. Such a plan may be established as a result of a more general risk management approach.

This said, it needs to be highlighted that DNSSEC significantly modifies the usual DNS model since :

- o the [public part of the "authoritative" key that has signed the public part of the "authoritative"] key used to sign a zone is collected and signed by the parent domain operator and published in the parent zone [REF 10];
- o DNSSEC introduces new DNS resource records in the zonefiles (public keys -DNSKEYS-, resource record signatures -RRSIG-, next secure -NSEC- and delegation signer -DS- [REF 9]);
- o A dedicated DNS resolution mechanism is implemented in DNS software resolvers to collect keys. Once collected, a public key will allow the checking of data received at each step of the usual DNS resolution process.

From an operations point of view, DNSSEC introduces changes in procedures for zone management and zone publication. Basically, to manage and announce a signed DNS zone [REF 11]:

1. two keys (KSK and ZSK) need to be generated (and managed)
2. the zone needs to be signed with the Zone Signing Key (ZSK)
3. the ZSK has to be signed with the Key Signing Key (KSK)
4. the signed zone must then be announced by DNSSEC enabled authoritative DNS servers
5. the public part of the KSK needs to be disseminated

Particular attention should be paid to resources that are required to effectively sign a zone (step 2), especially for large zones, since this operation consumes CPU and memory. Some indications are known and provide a good idea about the current scaling (time and hardware used [REF 14 15 16]:

<http://www.ripe.net/docs/ripe-352.html>,

<http://lists.oarci.net/pipermail/dns-operations/2008-January/002193.html>).

It's noted that dynamic updates are possible with DNSSEC, but the time to update a signed record is of course longer than if this record didn't need to be signed. Also, specific considerations for key management may need to be taken into account when implementing dynamic updates, since in that case, the signature process is a step that is performed within the zone update process flow. The new format proposed by NSEC3 can also be an option for large and frequently refreshed zones, since NSEC3 allows the partial signing of a zone: the signature process may therefore be implemented only for certain records that would need it. Dynamic update is also supported with NSEC3.

3.2. Key dissemination

3.2.1. Principles

Since DNSSEC technology is based on asymmetric cryptographic signatures included in the DNS, the public part of the key pair used to sign a zone record needs to be known by security aware resolvers for them to be able to verify responses upon receipt.

To rephrase this, DNSSEC security is effective when a security aware resolver receives a signed response, and when it knows the correct public key that will allow the checking of the signature attached to this response.

From a DNS zone publisher point of view, an issue now raised is : how will security aware resolvers know my public Zone Signing Key (ZSK) ? How should I publish this key ?

The response to this is that a zone operator can simply introduce the public part of its ZSK into the zone (as a DNSKEY record) for security aware resolvers to query it. Therefore, the ZSK is published as any other record in the zone file, except that it is signed by another key (Key Signing Key); KSKs are keys specifically used to sign ZSKs.

So the question is now: how will resolvers know the public part of my KSK for checking my ZSK upon reception ?

Again, the DNS may be naturally used by a zone operator to disseminate its KSK if the parent zone is DNSSEC compliant. In this case then he may securely provide the public part of the KSK to the parent zone operator -exactly as he already provides other data-, and ask him to sign and publish it (as a DS record) along with other information that he already publishes.

3.2.2. Alternatives

If the parent zone is not DNSSEC compliant, then specific channels need to be set up by a zone operator to publish the public part of its KSK : secured web sites, mailing lists, contracts etc. This is the path that some ccTLDs that have signed their zone have adopted, since the root zone is not signed. The -ccTLD- KSK has then to be collected by DNS cache operators, and included manually (or automatically) in resolvers, and declared as the trust anchor for the associated -ccTLD- domain. With DNSSEC popularity, if this solution was spread, it would lead operators to maintain a list of places and a set of specific procedures per DNSSEC compliant domain : where to get the KSK for this domain ? How to collect it ? How to know that a KSK in my list needs to be refreshed ? How to verify it ? etc. and this doesn't scale, unless a limited number of domains are secured.

There is another alternate solution for a zone operator to still use the DNS for public KSK dissemination when the parent zone is not signed. The principle is to introduce [an]other entry point[s] than the parent zone for the domain to be secured, where security aware resolvers could obtain KSKs from. This mechanism is known as DLV (DNSSEC Look-aside Validation) [REF 17].

Although DLV works, this solution for the global DNS tree is widely presented at best as a facilitator that could help to deploy DNSSEC until the root zone is signed, at worst as a bad idea to use, since it would introduce new problems (more complexity, less robustness, synchronisation issues, organisational issues, legal issues, etc.).

While the root zone is not signed, there is no root KSK, and no procedure for key exchanges between IANA and TLD operators, any alternative used to deploy DNSSEC in the public DNS tree dooms DNS cache operator to maintain a list of domain public keys, refreshing with specific each time this is necessary and/or to maintain a list of DLV repository: this would not scale [REF 3 4].

Since the root zone is at the top of the DNS tree, it has no parent zone. Ideally, we see that if the root zone was signed and if appropriate key exchange procedures implemented with TLDs, a resolver would need only to know the root KSK, and would build any chain of trust from this key that could be used as a universal trust anchor [REF 4].

3.2.3. Key Time Life and key rollover

As a general principle in cryptography, keys (therefore signatures) are not valid forever : the higher a key's usage frequency or the longer a key's lifetime, the greater the probability that it could be compromised.

Key Rollover is the process that is periodically performed to renew keys.

A ZSK is used to sign a zone, each time this zone changes. Since the ZSK is used frequently, its lifetime should be relatively short to protect against attacks. At the same time, (once signed by the KSK) the ZSK public part is published as a DNSKEY record within this zone in the same manner as any other record.

A KSK is used to sign the ZSK: it's only used each time a ZSK is renewed, and therefore KSK lifetimes may be much longer than ZSK. On the other hand, the public part of a zone KSK is published both as a DNSKEY in this zone and also elsewhere (normally in the parent zone if it is signed).

A Key rollover is a planned process that follows clear and secured procedures. The frequency for rollover depends on different parameters (size of the signed zone, robustness of procedures, zone update frequency, etc). It's sensible to regularly review procedures and frequency needs to take into account crypto developments or identified new threats [REF 10].

3.2.4. Emergency plan

On the side of the planned key rollover processes, a key may also need to be replaced as soon as possible if it has been compromised. There are different kind of malicious activities that could be performed with a compromised KSK or a compromised ZSK [REF 10]. DNSSEC doesn't currently include any revocation mechanisms (RFC5011 proposes this feature), an emergency plan must be ready to face this kind of situation if it occurs. Since ZSKs are managed, used and published locally, the rollover process is easier than if a KSK is compromised (risks are also less severe).

Due to the necessity to coordinate promptly with the parent zone to replace a compromised KSK, an "authenticated out-of-band and secure notify mechanism to contact a parent" is needed in this case. The emergency plan also needs to be agreed between the two parties to solve such a situation if it occurs. In particular, procedures between IANA and TLD managers need to be secured, to guarantee that a new TLD KSK can be submitted, signed and published promptly in the root zone in the case of an emergency.

Various documentation is available describing how to plan key rollover or implement related operation, such as RFC 4641 [REF 10] or RFC4986 for example.

3.3. What does serving a signed zone means ?

There is also a scaling issue that needs to be considered from a DNS servers point of view since the size of a signed zone does grow significantly, so does the size of signed responses. This may impact bandwidth consumption of authoritative name servers, as well as producing overhead cache servers or impact the behaviour of certain equipments [REF 15 16 18].

There are already indications publicly available on this issue that propose testing methodologies, and that report about concrete cases. Globally, there are many ways for the technology to support the load today, even in extreme cases ([REF 15 16], benefit of anycast, load balancing solutions).

It's however highlighted here that a robust monitoring policy for DNS service (using tools such as DNSMON or DSC) becomes even more necessary when planning to deploy DNSSEC.

A. References (Main documents, statements and Portails)

[REF 1]

Title: A RISK MANAGEMENT PRIMER FOR CEOs AND DIRECTORS

Date: December 2007

Abstract:

A 16 page paper to increase awareness about corporate security approach, and helps to evaluate it. Also helps to review policies and plans implemented to protect an organisation against electronic aggression. Includes an "Information Security Checklist" (page 11).

Href: http://www.acus.org/docs/071212_Cyber_Attack_Report.pdfREF

[REF 2]

Title: DNS Threat Analysis

Abstract:

This paper is a coeffer between NLNET LAB and SE registry (IIF). Assuming DNS is a critical infrastructure component, it lists and describes the various threats surrounding the DNS, and provides indications on measures or to help to fix them. In particular, it recommends the deployment of DNSSEC to fix data integrity issue.

Href: <http://www.nlnetlabs.nl/downloads/se-consult.pdf>

[REF 3]

Title: DNSSEC: Once More, With Feeling!

Abstract:

General discussion about DNSSEC deployment by Geoff Huston, that includes a good overview of different aspects that need consideration. A focus on the root zone case indicates that the root zone signature is pivotal to DNSSEC deployment, and also concludes that the substantive issues for DNSSEC are much further down in the DNS hierarchy than at the root.

Href: http://www.circleid.com/posts/dnssec_once_more_with_feeling/

[REF 4]

Title: DNSSEC Deployment at the Root

Date: May 2006

Abstract:

A discussion by Thierry Moreau on the issue of deploying DNSSEC with a specific focus on the root. Three issues are identified for DNSSEC to be deployed:

- 1/ solving the "zone walking" issue
- 2/ solving the trust anchor key management issue
- 3/ check that DNSSEC is adequate for full-scale deployment.

Href: http://www.circleid.com/posts/dnssec_deployment_at_root/

[REF 5]

Title: DNSSEC Survey Results

Date: October 2007

Abstract: Result of a survey on the usage and knowledge of DNSSEC conducted by Gabriella Schitteck for the ccNSO in September and October 2007 and that received 61 replied. Most respondents think that they would introduce DNSEC by 2011.

Href: <http://losangeles2007.icann.org/files/losangeles/presentation-ccnso-dnssec-survey-results-schitteck-30oct07.pdf>

[REF 6]**Title:** SIGNING THE ROOT ZONE**Date:** October 2007**Abstract:**

Presentation from Olivier Guillard over the ICANN ccNSO members meeting in Los Angeles. Main identified perspectives to consider with regard to signing the root are:

- 1/ Interaction with cache DNS server operators and operations involved
- 2/ Root zone management, root signing process and overhead
- 3/ Interactions with ccs and key exchanges

Href: <http://losangeles2007.icann.org/files/losangeles/SigningRootZoneOlivier.pdf>**[REF 7]:****Title:** DNSSEC @ IANA**Date:** October 2007**Abstract:**

Last IANA update about DNSsec. These slides were presented by Richard Lamb over the ICANN meeting in Los Angeles. It includes useful technical information for TLD, as well as indications about the current operational strategy considered by IANA for DNSsec deployment.

Href: http://losangeles2007.icann.org/files/losangeles/Lamb-DNSSEC_at_IANA.pdf**Href:** (IANA portail on DNSSEC) <https://ns.iana.org/dnssec/status.html>**[REF 8]****Title:** RFC 4033: DNS Security Introduction and Requirements**Date:** March 2005**Abstract:**

The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System. This document introduces these extensions and describes their capabilities and limitations. This document also discusses the services that the DNS security extensions do and do not provide. Last, this document describes the interrelationships between the documents that collectively describe DNSSEC.

Href: <http://www.ietf.org/rfc/rfc4033.txt>**[REF 9]****Title:** RFC 4034: Resource Records for the DNS Security Extensions**Date:** March 2005**Abstract:**

This document defines the 4 new records introduced by DNSSEC: public key (DNSKEY), delegation signer (DS), resource record digital signature (RRSIG), and authenticated denial of existence (NSEC) resource records.

Href: <http://www.ietf.org/rfc/rfc4034.txt>**[REF 10]****Title:** RFC 4035: Protocol Modifications for the DNS Security Extensions**Date:** March 2005**Abstract:**

This document defines the concept of a signed zone, along with the requirements for serving and resolving by using DNSSEC. These techniques allow a security-aware resolver to authenticate both DNS resource records and authoritative DNS error indications.

Href: <http://www.ietf.org/rfc/rfc4035.txt>

[REF 11]**Title:** RFC 4641: DNSSEC Operational Practices**Date:** September 2006**Abstract:**

This document describes a set of practices for operating the DNS with security extensions (DNSSEC). The target audience is zone administrators deploying DNSSEC.

Href: <http://www.ietf.org/rfc/rfc4641.txt>**[REF 12]****Title:** DNSSEC Hashed Authenticated Denial of Existence (NSEC3)**Date:** December 2007**Abstract:**

This draft ietf is on standard track. NSEC3 is a replacement for the NSEC resource record. This new resource record fix the zone enumeration issue ("zone walking") that is possible with NSEC. NSEC3 usage also permit to sign only some of the records in a zonefile, wheither NSEC require whole zones to be signed.

Href: <ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-dnsext-nsec3-13.txt>**[REF 13]****Title:** A Root with a view...**Date:** November 2007**Abstract:**

DNS traffic requires attention when planning to deploy DNSSEC. This is the L root traffic statistics published by ICANN on the ICANN blog. These information, produced by the dsc tool, give a view of the current query types and traffic that one of the root servers receives.

Href: <http://blog.icann.org/?p=240>**Href :** (DSC tool) <http://dns.measurement-factory.com/tools/dsc/>**[REF 14]****Title:** Measuring the resource requirements of DNSSEC**Date:** September 2005**Abstract:**

Laboratory tests: impact of DNSSEC on CPU, memory and bandwidth consumption of authoritative name in the context of ns-pri.ripe.net and k.root-servers.net. It's concluded that "deploying DNSSEC on k.root-servers.net can easily be done with the currently deployed systems."

Href: <http://www.ripe.net/ripe/docs/ripe-352.html>**[REF 15]****Title:** Exploring the Overhead of DNSSEC**Abstract:**

laboratory tests: meausrement of the overhead of DNSSEC on authoritative and caching DNS servers.

Concludes that DNSSEC deployment would increase DNS bandwidth consumption by a

factor between 3,4 and 12,7 in the worst case, and foresse an average overhead factor between 2 and 6,2 in the worst case.

Href: <http://www.net.informatik.tu-muenchen.de/~anja/feldmann/papers/dnssec05.pdf>

[REF 16]

Title: Observation from DNSSEC deployment

Abstract:

SecSpider is a globally distributed polling system that crawls a list of secure zones once every day. This 6 page paper provides an excellent overview of DNSSEC deployment and monitoring issues, it includes metrics and prospective considerations related to DNSSEC. SecSpider is partially supported by BSF.

Href: http://irl.cs.ucla.edu/papers/SecSpider_NPsec07.pdf

Href: (secspider portal) <http://secspider.cs.ucla.edu/>

[REF 17]

Title: ISC's DLV Registry

Abstract:

DLV (DNSSEC Look-aside Validation) is a non-IETF extension that proposes to introduce additional DNS entry points from which resolvers could obtain DNSSEC validation information. This REF is the portal on the ISC's DLV registry which is the most popular one.

Href: <https://secure.isc.org/index.pl?/ops/dlv/>

[REF 18]

Title: SSAC Statement to ICANN and Community on Deployment of DNSSEC

Date: 30 January 2008

Abstract:

Under certain environment, some issues were revealed that may impact DNSSEC deployment. This paper identifies and recommends a set of actions to secure the deployment of this technology at a global level.

Href: <http://www.icann.org/committees/security/sac026.pdf>

B. ANNEXES

B1. **PART II : Practical cases** (proposed table of content)

Table of content

- 4. The root zone case
 - 4.1 Why sign the root ?
 - 4.2 What is signing the root? Key management
 - 4.3 Root servers briefing
 - 4.4 Customer considerations: IANA interface
- 5. Possible worlds
 - 5.1 Root not signed
 - 5.1.1 Implications for ccTLDs which are signed
 - 5.1.2 Implications for ccTLDs which are not signed
 - 5.2 Signed root
 - 5.2.1 Implication for ccTLDs who have signed their zone
 - 5.2.2 Interaction/processes that need to be in place
 - 5.2.3 Implication for ccTLDs who have not signed their zone
- 6. Conclusions ?

B2.. **Contacts**

This briefing was produced by the IANA Working Group:

<http://ccnso.icann.org/workinggroups/ianawg.htm>

Who to contact about this paper:

Olivier.Guillard at nic.fr

Drafting team and reviewers (Thanks!):

Lesley Cowley (.uk), Olivier Guillard (.fr), Richard Lamb (icann), Oscar Moreno (.pr), frederico neves (.br), Shinta Sato (.jp), Gabriella Schitteck (icann) and Roy Arends (.uk), Bart Boswinkel (icann), Ondrej filip (.cz), Jean-Philippe Pick (fr)