The Internet Corporation for Assigned Names and Numbers

ICANN

2 September 2008

Ms Meredith A. Baker
Acting Assistant Secretary for Communications and Information
United States Department of Commerce
National Telecommunications and Information Administration
WASHINGTON, DC 20230

Dear Hon. Assistant Secretary Baker,

Attached, please find ICANN's proposal to sign the root zone file with DNSSEC technology. This proposal has been written by ICANN staff, as authorized by ICANN's Board, with the goal to proceed with appropriate speed and deploy DNSSEC at the root level as a step towards improving the overall security of the DNS.

As mentioned to you in my letter of 16 August 2008, to ensure a technically sound proposal, this document has already been reviewed by a group of DNSSEC experts. These include members and liaisons ofICANN's Board (including Steve Crocker, Suzanne Wolf, Harlad Alvestrand, and Thomas Narten), and externally include Vint Cerf, Olaf Kolkman, Russ Housley, Patrik Falstrom and Steve Bellovin. The feedback ICANN received from this group indicates that the proposal is technically sound, and appropriate.

The proposal envisions that ICANN, VeriSign and the NTIA all have an ongoing role in producing and distributing the signed root zone. Based on the chain of trust notion at the core of DNSSEC, the proposal suggests modifications to the current roles.

While this proposal strives to be clear and direct, inevitably there will be some items that require clarification and discussion. It may well be useful to have an early teleconference or in-person meeting with NTIA (and its designees) and ICANN representatives to provide this clarification; if helpful, I will make ICANN staff available at your earliest convenience.

As you will see from the attached proposal, ICANN's community has also called for ICANN to take action with respect to DNSSEC-signing the root zone file. At the core of ICANN's processes is the notion of community consultation. In some weeks, ICANN will, of necessity, seek community feedback on this proposal, as evolved in consultation with NTIA.

ICANN

This is a moment of challenge and opportunity in addressing the overall stability and security of the DNS system; the mission around which ICANN was formed. Working with the NTIA, ICANN looks forward to take action that will fulfill on that promise for all those around the world who depend daily on the Internet.

Sincerely,

Paul Twomey
President and CEO

cc: Fiona Alexander
Suzanne Senne
Vernita Harris
ICANN Board
Vint Cerf
Doug Brent
Paul Levins

**ICANN Proposal to DNSSEC-Sign the Root Zone**

## Executive Summary

This document asks and proposes answers to three questions related to DNSSEC signing of the root zone:

1. Why should the root zone be DNSSEC-signed?
2. Why does ICANN propose to sign the root zone?
3. How and when should the root zone be signed?

In summary:

1. DNS Security Extensions protocol (DNSSEC)[1] provides for the validation of data returned by domain name lookups by incorporating a chain of trust into the DNS hierarchy. The introduction of DNSSEC improves confidence that the DNS data that is being delivered is not being modified in transit. Still, signing a zone does not add any new controls over the content or distribution of the zone and does not encrypt the zone data

   The root zone should be DNSSEC-signed to allow for validation of top-level domain data in the root zone; to enable an authoritative, hierarchical, scalable and maintainable repository for top-level domain trust anchors; and to provide leadership so that DNSSEC can ultimately be fully deployed to all Internet users. DNSSEC offers strong protection against a class of attacks that have recently been deemed increasingly likely and quite dangerous. Importantly, full deployment of DNSSEC can address security flaws in the DNS protocol that will be exacerbated over time as bad actors have more resources and time to mount attacks. Announcing that the root zone will be DNSSEC signed in the near future will provide confidence to TLD operators and software vendors considering their DNSSEC implementation plans.

2. ICANN is the appropriate entity to perform the key management and DNSSEC signing functions for the root zone. The DNSSEC signer of the root zone must be a trusted actor whose root zone related activities are open, transparent, and accountable. ICANN has worked with the international community and through its partnership with the U.S. Government to build credibility within the DNS community. It uses open and transparent processes for validating root zone changes along with other necessary zone maintenance processes and policies. Technical coordination of the DNS is a core pillar of ICANN. As an internationally organized not-for-profit corporation that is not subject to market-based profit and loss considerations, commercial change or acquisition, ICANN can provide a long-term constancy to root zone signing in the interest of all Internet users.

   Given concerns about potential data corruption in transmission, it is logical from operational, technical and security perspectives that the validator of root zone changes also authenticates the validity of the final product. ICANN has the experience of producing a publicly available

[1] See RFCs 4033, 4034, and 4035

signed root zone through a testbed[2] established in June 2007 that has been widely tested by DNS software vendors and the interested DNSSEC community. In becoming the root zone DNSSEC operator and key custodian, ICANN will use its competency in technical operations to act as an accountable entity that the global community accepts as valid to do this work. ICANN's open, transparent and international participatory policy process will allow for root zone management to adapt to changing needs over time as this technology is operationally deployed throughout the Internet and as new lessons are learned.

3. Today, ICANN's role is to validate root zone changes. As part of the DNSSEC effort, ICANN proposes to edit and compile the root zone file, and sign it. However, the present tripartite arrangement of root zone partnership should continue; VeriSign distributing the root zone file after audit and authorization by the U.S. Department of Commerce and ICANN performing its proposed role. This DNSSEC signing infrastructure is modeled on best current practices of TLD operators providing DNSSEC-signed zones, and more than a year of ICANN operational experience with the testbed. ICANN will provide an open and transparent process regarding both the final decisions of technical infrastructure, and regarding signing oversight functions. While technical preparatory work will be ongoing, ICANN envisions a process that initiates a public consultation period in October 2008 and that will yield full test mode operation in six months and a production signed root zone in nine months – by June, 2009.

The proposal outlined in this document is subject to U.S. Department of Commerce (DoC), National Telecommunications and Information Administration (NTIA) approval. While broadly in accordance with ICANN's existing contract with the U.S. Department of Commerce to perform the functions of the Internet Assigned Numbers Authority (IANA), ICANN and NTIA should review the contract to determine if amendments are required.

**1. Why Should the Root Zone be DNSSEC-Signed?**

DNS Security Extensions protocol (DNSSEC)[3], a series of protocol extensions defined in RFCs 4033, 4034, and 4035, provides for the validation of data returned by domain name lookups by incorporating a chain of trust into the DNS hierarchy. The chain is built using public key cryptography, with each link in the chain representing a public-private key pair. Once deployed, validating software can verify that the signed DNS data received is the same as that contained in the originating DNS server using a "trust anchor" or public key for the signed zone and its signed children zones. DNSSEC is backward compatible with existing DNS, leaving records as they are — unencrypted — but ensuring that their integrity can be validated, if explicitly requested, through the use of digital signatures. Users of the DNS who choose not to adopt DNSSEC will be able to access the root zone just as they do today with no changes on their part; however, those wishing to validate the DNS data received will be able to do so. Essentially, the chain of trust becomes one of increasing confidence that the data being received through the DNS has not been tampered with during its path through the Internet. Providing this trust chain from the root zone to the caching resolver, and ultimately to the user, will enhance DNS security.

[2] See https://ns.iana.org/dnssec/root.zone.signed and https://ns.iana.org/dnssec/status.html
[3] See RFCs 4033, 4034, and 4035

Once DNSSEC is fully deployed, a foundational trust anchor for the root of the DNS would protect users from attacks such as cache poisoning[4], where an attacker would reply to DNS queries with a bogus DNS response that could, for example, send subsequent users to the attacker's web pages for account/password collection. Recent exploits of inherent DNS protocol deficiencies make such man-in-the-middle and cache poising attacks significantly easier for the would-be attacker to implement. Being able to protect against this is among the primary motivations for deployment of DNSSEC. After many years of discussion about cost vs. benefit, there is now a growing consensus that the values of deploying DNSSEC outweigh the potential costs.

Currently, DNSSEC is being deployed by only a few top-level and second-level domain operators. These early adopters are necessarily creating "islands of trust" for their signed zones, as there is no established chain of trust above them. As a result, the trust anchors for their zones must be authenticated externally.[5] Signing the root zone will establish a trust anchor that will initiate the chain of trust from the root to the signed TLDs to the signed second-level domains of the signed TLDs, eventually absorbing the islands of trust. While the voluntary nature of DNSSEC adoption makes islands of trust inevitable in early adoption, the sooner the root is signed, the earlier the islands of trust can be connected in a chain of trust establishing greater confidence in DNS data.

A secondary problem introduced by delaying signing the root is that as long as the root remains unsigned, alternate trust anchor repositories for root-level data will be created in order to fill a real need for out-of-band authentication. This will lead to situations where those wanting to configure trust anchors as validation in their name servers may need to consult more than one trust anchor repository to fully capture all the available trust anchors. These multiple sources of trust data will inevitably diverge, leading to non-synchronous updates of trust anchors, or even conflicting data on current trust anchors. Such a situation can cause confusion and distrust of the DNSSEC signing process and delay deployment until authoritative DS records can be obtained from a single source. The root zone should be that authoritative source for the top-level domains, and announcing plans for signing the root zone will forestall some of these issues.

**2. Why does ICANN propose to sign the root zone?**

The chief concept behind this proposal is trust – of users who exist in an international community. DNSSEC is a technology, and does not by itself offer a solution to a trusted DNS. Trust comes from a process that offers secure, stable, and accountable operations of the root zone signer, integration with existing root zone management processes, and global Internet community endorsement. ICANN is the organization best positioned to ensure all of these elements.

---

[4] To perform a cache poisoning attack, the attacker exploits a flaw in the DNS (Domain Name Server) software that can make it accept incorrect information. If the server does not correctly validate DNS responses to ensure that they have come from an authoritative source, the server will end up caching the incorrect entries locally and serve them to users that make the same request. This technique can be used to replace arbitrary content for a set of victims with content of an attacker's choosing. For example, an attacker poisons the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he controls. He then creates false entries for files on a server with names matching those on the target server. These files could contain malicious content, such as a worm or a virus. A user whose computer has referenced the poisoned DNS server would be tricked into thinking that the content comes from the target server and unknowingly download malicious content

[5] At the behest of leaders in the DNS community and as directed by ICANN's Board, ICANN is in the process of establishing an Interim Trust Anchor Repository (Interim-TAR) for Top Level Domains that are implementing DNSSEC.

2.1 Secure and Stable Operations

DNSSEC operational experience at the TLD level has made it clear that in order to avoid service failures and errors, as much of the signing architecture as possible must be automated and that an unbroken chain of custody for TLD trust anchor material be maintained. For the root zone, this chain of custody begins with the requests for changes that TLD operators initiate with the IANA function and with the zone information maintained by the IANA function.

Recent reviews of existing DNSSEC implementations, considering new methods of cache poisoning and other security issues, highlight the added value in bringing together the data validation, editing, and compilation elements of the root zone maintainer functions as well as placing them in close physical proximity to the DNSSEC signing equipment. Experience has led to the view among DNSSEC experts that signing operations should be fully automated[6] to eliminate the costly risk of signing failure and to reduce the time required to recover from compromises[7]. Automating the process involves keeping signing and zone database hardware physically together and connected to facilitate a direct, secure connection.

ICANN will put in place a signing infrastructure that meets these security and stability criteria, and an automated approach has been at the core of ICANN's year-old DNSSEC signing testbed. All zone processing changes start in the IANA function, and the signing infrastructure and processes can offer automation from the point at which change requests are validated through to the production of the signed zone. Having one entity manage the editing of the zone maintains physical proximity of relevant functions and maximal control of the data.

2.2 Integration with Existing Root Zone Management Processes

The current root zone management process has three parties, not counting the TLD managers: ICANN, managing the IANA functions including validating requests and verifying technical conformity; NTIA, managing the authorization function; and VeriSign, managing the editing, compilation, and distribution functions. Root zone signing must take into account these various roles, while also fulfilling the technical security criteria outlined in the previous section.[8]

Top-level domains in the root zone are defined by name server (NS) resource records (RRs) and associated address (A for IPv4 or AAAA for IPv6) RRs. When a TLD signs its zone, it will create a delegation signer (DS) resource record that provides for the chain of trust between the child zone (the TLD) and the parent (the root). Absent having the root signed, these records are as liable to cache poisoning as the NS records currently are (through the attack methods mentioned previously) and thus cannot be trusted without some sort of out-of-band validation mechanism.

---

[6] .SE and .UK have developed plans for such automation in their TLD DNSSEC operations.

[7] By being able to reduce the keyset signature validity period by automating its generation.

[8] While not specifically related to DNSSEC signing, the potential expansion of the root zone with new TLDs in 2009 will potentially also have an important impact on root zone management processes. Any changes to process should accommodate the notions of a more scalable and nimble process that avoids error-prone manual processing and hand-offs. ICANN's proposed zone compilation and signing process can address this scalability concern and have zone signing available concurrently or in close proximity to the introduction of new TLDs into the root zone.

The introduction of DS RRs into the root zone would be the first significant addition of an informational record to the root zone since the introduction of IPv6 AAAA records in 2004. Developing appropriate verification and validation processes for the DS RR inclusions in the zone is an essential step in the process of DNSSEC signing the root. Without having these records in the root zone, as noted above, trust anchor repositories will be deployed to provide the out-of-band verification required for authenticating signed TLD zones. Aside from the questions raised in including these specific data elements, there are concerns about the best method for ensuring the validity of the signed data. The conclusion of the DNS technical community to date is that there are distinct and valuable benefits in securely managing the data from initial entry into the system to eventual compilation of a signed root zone. Other models that distribute responsibility for validating and compiling the data as a part of root zone signing within the current framework create avenues for potential corruption or error during transmission of data from one root zone management participant to another.

For this reason, ICANN proposes changes in the current root zone management roles:

ICANN: Today, ICANN validates root zone changes, working as a trusted partner with TLD managers to ensure changes are made correctly for their zones. ICANN proposes to extend this trust further to compiling these changes into the authoritative root zone file and signing it. ICANN is now concluding the development of software (EIANA) that accepts changes from TLD operators to create a set of zone edits (deployment of EIANA is subject to DoC approval per the contract for the IANA functions). A logical extension of this EIANA work is to directly create as output a root zone file (this functionality is demonstrable today). Further, this software will be extended to accommodate the process for entering DS RR records, and transferring all of this information to the automated signing infrastructure thus producing the signed root zone. As discussed later in the document, the schedule to complete and test this functionality is three months.

VeriSign: Today, after authorization by the Department of Commerce, VeriSign accepts changes from ICANN's IANA function, compiles these changes into the authoritative root zone file, then distributes that zone to root server operators. This proposal envisions transferring the compilation function to ICANN, and maintaining VeriSign's important role in trusted, secure root zone distribution.

U.S. Department of Commerce: Today, the U.S. Department of Commerce through the NTIA authorizes changes one-by-one in the root zone file. This proposal envisions a generalized authorization and audit role such that changes can be authorized without having to pass unsigned data among parties. Just as a financial audit validates organizational adherence to defined process, and ensures that the financial records are an accurate reflection of those processes, NTIA's review could be expanded to include all elements of root zone production from validation of requests through root zone signing. Periodically (on a basis to be determined by them), NTIA could review root zone validation processes and confirm that zone changes are accurately reflected in the produced root zone. This process is critical to preserving oversight of the fact that validated changes and the root zone itself are handled according to policy.

ICANN proposes that the data – from the time of submission by the TLD operator to the time of compilation and signing of the root zone – be part of an overall secure process operated by ICANN.[9] To avoid the introduction of error, there should be no transfers of data between parties for each of the steps of verification, authorization, editing, compiling, and signing of the zone.

With the increased confidence in the security of DNS that DNSSEC will bring, it becomes ever more important that the trust achieved from ICANN's validation and authentication of TLD trust anchor material[10] be maintained through to a signed root zone file. Given the conclusion from DNSSEC experts that whoever compiles the zone should sign the zone, in order to guarantee the integrity of TLD trust anchor material, the Root Zone Validation and Root Zone Maintainer functions should be combined. Of course, the resulting published zone file remains accessible to all.

2.3 Global Internet Community Endorsement of Signing Process

To fully exploit the value of a DNSSEC-signed root zone, the process for signing the root zone must have the acceptance and endorsement of the global Internet community. Beyond essential technical considerations, the decisions involved in initiating a signed root are also social, embedded in many of the same concerns that influence Internet policy issues in international forums. However, the trust model inherent in DNSSEC signing of the root and full deployment throughout the DNS hierarchy gain significantly when the participants trust the root zone signer. Without this trust, DNSSEC deployment could actually lead to fragmentation of purported trust points contributing to the potential disruption of a single, global, interoperable Internet.

The root zone will be signed with a Zone Signing Key (ZSK). The ZSK holder signs the records in the root, which provides integrity and authentication of DNS information. This does not confer any greater control or privilege than exists today with an unsigned root. **Signing a zone does not add any new controls over the content or distribution of the zone. DNSSEC does not encrypt the zone data, but merely adds an authentication record that can be verified by a name server set to receive that data. Any name server operator can choose to ignore the signing information and still receive all the zone data as if the zone had not been signed.**

2.4 ICANN best fills these requirements

ICANN meets the requirements outlined above; ICANN will provide secure and stable operations, can integrate root signing with a process that begins at the inception point (validating root zone changes), and will seek, and expect to receive global community endorsement for this role.

ICANN has as its core mission "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." This is the first sentence of ICANN's bylaws, and it is the directive that guides its activities as an organization and as a community. The primary core value is "preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet." Fulfilling this mission and goal is the reason for ICANN's existence.

---

[9] This proposal assumes that the approval process for handling TLD delegations and redelegations will remain as it is today.
[10] In the form of DS records

Further, ICANN is financially stable, able to support changing policies based on dynamic technical/protocol requirements, open to public consultation on changes to policy that affect a significant portion of the DNS community and able to resist capture by parties unwilling to support these open, transparent, and accountable qualities. ICANN is a trusted participant in the global Internet community, particularly having a strong, positive reputation in the DNS community. ICANN has been contracted by the Department of Commerce for almost ten years to perform the IANA function. Indeed, the current IANA contract acknowledges that "In connection with its work under these agreements, ICANN has developed and maintained close, constructive working relationships with a variety of interested parties, including Internet standards development organizations and technical bodies." (Section C.1.2)

A growing number of international stakeholders have been calling for ICANN to take action towards signing the root zone. In June 2007, the RIPE community[11] sent a letter requesting ICANN to get the root zone signed "as soon as realistically possible"[12]. This was followed by requests in October 2007 from major Swedish (.SE) stakeholders interested in DNSSEC[13] and Nominet (the .UK registry) asking ICANN to instruct staff to "take the necessary steps" to sign the root zone[14]. And most recently, on 28 August 2008, the APNIC community expressed unanimous support for ICANN's stated proposals for signing the root zone[15]. Currently DNSSEC is deployed by four (4) TLD operators (.SE, .BR, .BG, .PR) with others preparing for deployment (.ORG[16], .UK. .CZ, and even by the US Government .GOV[17]). Finally, a recent survey of ccTLD operators also indicates a clear expectation of DNSSEC adoption and root zone signing by ICANN/IANA[18].

Open and public consultations on the best methods of developing and testing ICANN's DNSSEC-signed root zone demonstrate willingness to engage the community on the key issues of best practices for security and stability.

---

11 RIPE, Réseaux IP Européens is "a collaborative forum open to all parties interested in wide area IP networks in Europe and beyond". See http://www.ripe.net/ripe/index.html.

12 http://www.ripe.net/ripe/wg/dns/icann-root-signing.pdf

13 http://www.iis.se/docs/brev_iana_pdf.pdf

14 http://www.nominet.org.uk/digitalAssets/25692_Signing_the_Root.pdf

15 http://www.apnic.net/meetings/26/icann-letter.pdf

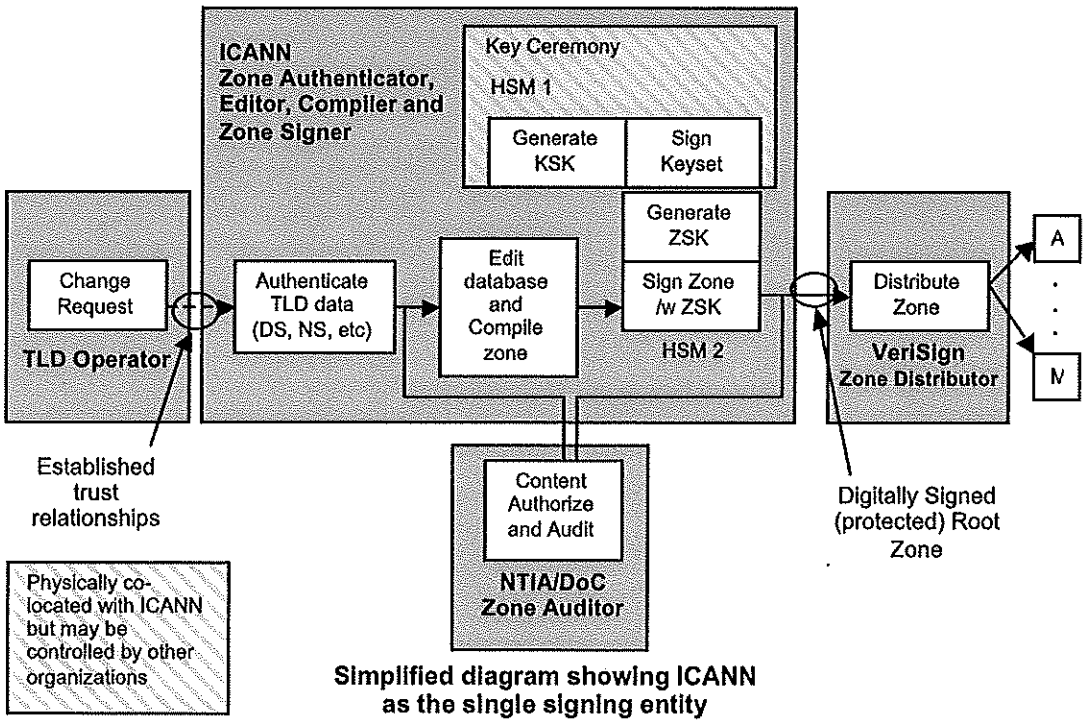
16 https://par.icann.org/files/paris/RaadDNSSEC.pdf and http://www.icann.org/correspondence/viltz-to-dam-02aug06.pdf

17 http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

18 http://ccnso.icann.org/surveys/dnssec-survey-report-2007.pdf

### 3. How and when should the root zone be signed?

### 3.1 System Block Diagram




**Simplified diagram showing ICANN as the single signing entity**

This diagram shows the primary functions and roles in the proposed signing model.

TLD Operator: A TLD Operator submits requests to ICANN based on an existing trust relationship through the IANA function of ICANN.

Zone Authenticator: Changes are validated through the processes run by the existing IANA function.

Zone Editor and Compiler: Validated changes are entered into a database using the ICANN and community-developed EIANA tool; a zone file is automatically created.

Zone Signer: ICANN automatically signs the zone using the Zone Signing Key, which it directly manages.

Key Signing Key Custodian(s): A party, to be defined by community input, will periodically create a new Key Signing Key (KSK) that with the ZSK signs the zone file. The hardware to perform this task is controlled by ICANN, but the KSK owner(s) has credentials that are necessary for a new KSK to be created. KSK creation occurs in a key signing ceremony (more on this below).

Zone Auditor: The U.S. Department of Commerce NTIA will periodically audit the signed zone file to ensure that IANA processes to validate changes are being followed correctly, and that the aggregate of these changes appear correctly in the zone file.

Zone Distributor: The zone distributor, proposed to be VeriSign, takes the signed zone and distributes it to the root server operators.

The important characteristics of this system include:

- A robust and secure signing system
- A mutually trusted process between TLD operator and signer for accepting and validating DS key RR data
- An open, transparent, flexible and secure process for key generation, publication and control that is acceptable to all stakeholders
- Clearly documented and secure audit procedures
- A flexible and open process for incorporating ongoing improvements and changes in requirements

Drawing on the deployment experience of DNSSEC experts[19] and experience from ICANN's signed root testbed, ICANN's proposed implementation includes specific elements, such as:

- Reliability through extensive automation and redundancy at multiple remote backup sites
- Highest level NIST certified crypto devices[20] employed for key generation, storage and use
- Use of 24 hour manned, secured facilities which include, among other mechanisms, multiple biometric access controls
- Building on ICANN's current process for vetting and collecting zone change data and based on established relationships with TLD operators, collect and validate critical TLD key data, and update the signed zone as necessary
- A documented and public key generation ceremony
- Implement and publish secure and stable audit procedures.
- Continuing to employ ICANN's public consultation processes to evolve the signing system to meet the needs of the community

In this system design, data authentication, editing and signing of the zone happen within the ICANN entity, eliminating cross-organizational hand-offs and reducing potential sources of error. As stressed elsewhere in the document, it provides for a level of integration and building off of the original point

19 Including Roy Arends, Jakob Schlyter, Patrik Fältström, Olaf Kolkman, Jaap Akkerhuis

20 NIST FIPS 140-2 Level 4

of trust, i.e. the hand-off of information between a TLD operator and the IANA function within ICANN.

In order to facilitate automation as well as future flexibility, the key devices (hardware security modules (HSMs) in the figure) are all co-located to allow for direct connection to signing equipment. This eliminates the costly risk of a signature expiration on either keyset or DNS record (that would cause the zone or record to go dark) by completely eliminating the need to regularly exchange sensitive signing key material between disparate entities. Such automation also allows for a significant reduction in the time required to recover from a key compromise.

Note that merely holding the key devices confers no control over the keys since any use must be authenticated with cards, PINs or both and any tamper attempt automatically destroys all keys. Keys may therefore be under stewardship by entities other than ICANN (see key signing ceremony below).

### 3.2 Important Operational Considerations

The technology behind DNSSEC is not new and has been developed for at least a decade (and the underlying PKI technology is older). However, DNSSEC deployment is relatively new and there is only limited operational experience from a few DNSSEC operators.

ICANN's proposed system was developed in close consultation with those in the forefront of DNSSEC deployment and following documented best practices. It was also designed with the understanding that operational experience in this area is evolving and that the system must be flexible enough to seamlessly incorporate updates and changes without negatively impacting the Internet. This acknowledges both the realities of changing technology but also changing views of governance and policy. As noted in ICANN core value 9, "Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most affected."

Some important operational considerations include transparency through the key ceremony and establishing operations and implementation parameters.

#### 3.2.1 Transparency through the Key Ceremony

Just as the process for arriving at a root signing system requires openness to maintain the trust of the community, the ongoing operation of that system must be open and transparent. In order to ensure the participation of the widest range of stakeholders in the community, ICANN's proposed system incorporates what is called a Key Ceremony. Keys for the root are generated, witnessed, and published at this public ceremony in advance of their use. Auditors and experts, who may also be stakeholders, are present to ensure the integrity of the process. The ceremony is also filmed and broadcast.

DNSSEC keys have a public and private component. Keys are generated in certified tamper proof hardware with the private component never known to anyone. The public half (of the KSK – the ICANN design uses two (2) to simplify rollover and aid in recovery) however effectively becomes the

"trust anchor" for the root and is witnessed by all participants in the ceremony. Any attempt by a would-be hacker to use any other key to fool DNSSEC will be met with failure. No one ever knows the private half required to sign the zone and it is computationally infeasible to guess the private key from the public one before a new one is generated. ICANN's proposed system continues to involve security engineering expertise to ensure the Key Ceremony procedures and associated equipment (multiple class 5 safes, safe deposit boxes, biometric access, etc.) do not inadvertently introduce vulnerabilities.

3.2.2 Operations and Implementation Parameters

There are a number of operational and implementation parameters that are best determined through consultation with experts, and ICANN's decision-making mechanisms and operational practices, are well suited to this kind of consultation.

3.2.2.1 Key Ceremony implementation
A set of implementation choices for the key ceremony is required, with the goal of maximizing the transparency and trust in the overall zone signing processes:

- *Roles*
  Who should perform which tasks in the ceremony and how should they be selected? Basic security engineering principles make it clear that the access to facilities, biometric credentials, combinations, key generation equipment, smart cards, PINs, physical keys should be distributed to different individuals. How are these individuals selected, and from which entities?

- *Frequency*
  How frequently should the Key Ceremony be performed?

- *Audit*
  What is the process for selection of an entity to perform regular on-going audits?

- *Reporting*
  What is the format and frequency of reporting to the community?

3.2.2.2 Disaster recovery and remote site locations

ICANN's proposed system was designed with distributed remote backup sites as an integral requirement. ICANN, as L-root operator and more recently in the creation of comprehensive community developed gTLD Registry Failover Plans, has developed experience in disaster recovery and will continue to consult with industry experts specializing in this aspect of security to ensure the ICANN's proposed system is protected by facilities that meet the industry's highest standards. However, discussions regarding the locations for and operators of such globally relevant operations, whether existing or commissioned, should be carried out with the community.

3.2.2.3 Security – System Parameters

ICANN's proposed system has been designed to be flexible when it comes to the selection of the various DNSSEC operational parameters. Since the value of many of these parameters represent trade-offs between stability and security, selection will follow public review by specialists and the technical community. Some of these parameters include:

- Keys
  - *Key rollover times*

    Based on documents outlining best current practices and drawing on current DNSSEC deployments, KSK rollover times of a year seem reasonable. However, recent discussions at the IETF indicate that much longer periods may provide sufficient protection from key compromise. The advantage of a longer-lived key is that it offers greater stability.

  - *Key lengths*

    Best current practice suggests that a key length of 1024-2048 bits provides sufficient protection from compromise. However, some suggest that greater key lengths might make sense for the root, while other discussions indicate shorter key lengths would provide just as much protection given key rollover times.

  - *Key backup*

    ICANN's proposed system circumvents many of the security and reliability problems inherent in backing up key material amongst remote sites by pre-generating at least the next year's worth of necessary keys, KSK and ZSK, in advance. The keys never leave the storage devices – ever. How far in advance keys should be generated is a question for consultation with the experts in the community.

- Selection of signature validity periods

  - *...on DNS data*

    Drawing on the operational experience of DNSSEC deployments such as .SE (doing so since Feb 2007), the length of time a signature on any particular record in the zone file is valid might be a week. The selection of this parameter is a delicate balance between security and stability. For example, the shorter the duration of signature validity, the more control over a replay attack, but this decision drives more stringent requirements on the distribution of fresh data, i.e., the data received at a DNSSEC validating resolver could never be older than a week.

  - *...on keyset*

    Best current practices suggest ZSK rollover times be on the order of a month. However a compromised ZSK would allow the attacker to then take control of the entire zone for a month before the compromised key would expire from an existing keyset. ICANN's proposed system embraces automation to not only greatly increase reliability but to also allow for the flexibility to greatly reduce the keyset validity period and therefore compromise recovery time. The reduction of recovery time however does decrease stability. ICANN looks to the experts in the community to continually advise on the selection of such parameters in the interest of balanced security and stability.

Establishing appropriate answers for parameters relating to the Key Ceremony, remote sites/disaster recovery, and key handling is critical. As noted above, decisions are best established through expert consultation. As described below, it is anticipated that this expert review will go on in parallel with overall system implementation.

### 3.4 Timelines Milestones and Proposed Implementation Plan

The attached diagram shows some of the key milestones in preparing for signing the root on a daily production basis. The milestones are broken into three broad categories of work: Decisions/Consultations, Operational Readiness and Environmental Readiness.

Historical milestones

Several actions and milestones have already occurred that make the production signing of the root possible. These include analysis and information dissemination by ICANN's SSAC, early TLD deployment at .se, .br, .pr, .bg and plans by others, ICANN's proof-of-concept signed zone available since June 2007, and the imminent ICANN trust anchor repository. All of this work was given greater urgency with the DNS vulnerability announced by Dan Kaminsky on 6 August 2008.

Decisions/Consultations

ICANN will initiate a public consultation process on this proposal beginning in October, 2008. At the same time, ICANN will create a DNSSEC-Signing Implementation Task Force comprised of the current parties to the root zone management process, as well as DNS and security experts. Experts from DoC and VeriSign will be specifically invited. Starting with the operational guidelines ICANN has already implemented in its testbed root zone signing, this Task Force would define a best practices process for ICANN to follow, and would identify "best of breed" architecture, equipment and security elements for the signing process. ICANN envisions the work of this Task Force to include public consultations and expert consultations on certain central issues, such as the appropriate controllers of the KSK, the options for failsafe key management, disaster recovery, service level commitments for ICANN's management of the signing process, and roles in the Key Signing Ceremony. The public consultations would continue through the work of the Task Force, a three-month period closing with the issuance of a final report to the ICANN Board recommending a specific implementation scenario.

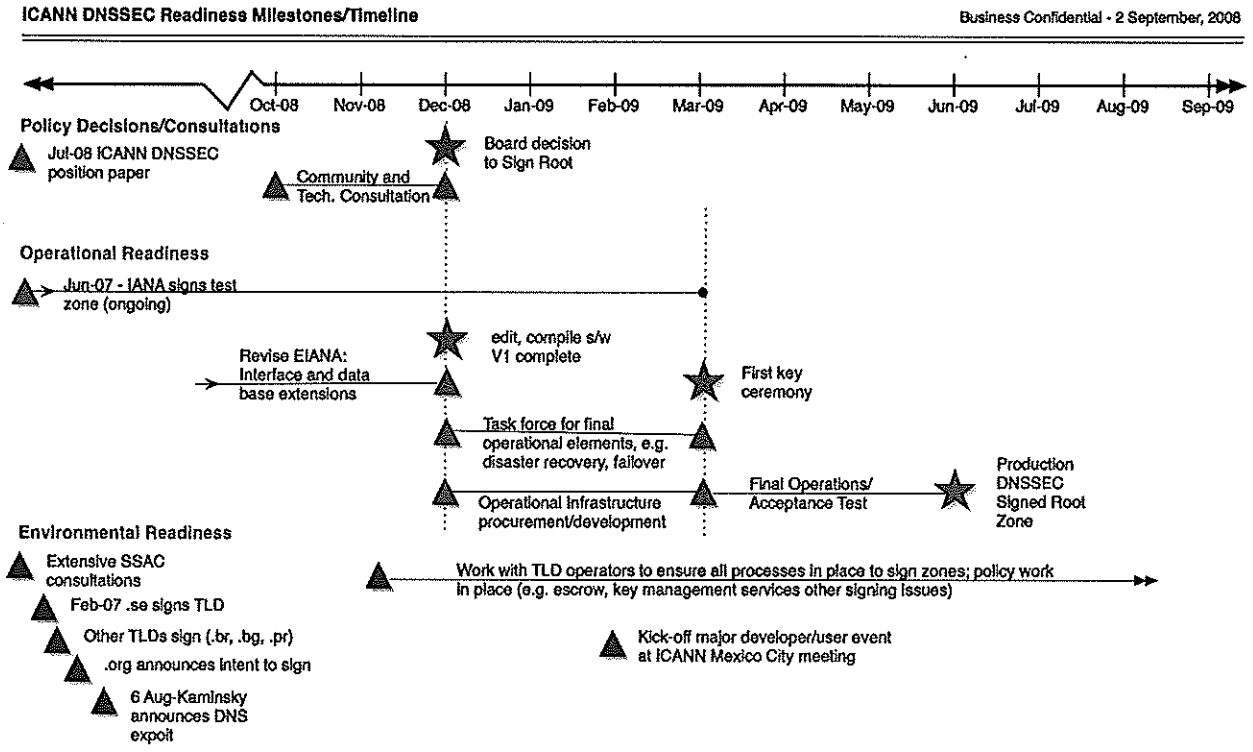
Operational Readiness

Beginning prior to, but continuing simultaneously with the work of the DNSSEC-Signing Implementation Task Force, the existing RZM/EIANA software will be enhanced with necessary processes for adding TLD DS records, modifying them as needed, and integrating with the root zone signer for actually creating a signed zone. Along with modifications to the authorization/audit communications process, the necessary development and testing of the revised software would be completed in 90 days. With the capability to directly produce a signed zone, and with the signing implementation scenario agreed, ICANN would produce a test signed zone using these tools, declaring readiness when the process is flawless for 90 consecutive days. Deploying the signing equipment, backup sites, and testing the installations could be completed in 90 days.

Altogether, from the initial decision that ICANN should DNSSEC sign the root zone, implementation could be accomplished in 9 months, with a successful signing process implemented at 180 days, and an additional 90 days of ongoing testing to ensure stability and security of the systems.

Environmental Readiness

There is another set of work related to energizing and leading the broad community of actors in the deployment of DNSSEC. This community includes TLD operators, software and service vendors and custom software developers. There will also be a significant amount of end-user education to make this new capability useful for users in all environments, including educational, personal, and business use.



**Conclusion**

ICANN proposes that the root zone be signed, and that ICANN be the entity that signs the root zone. Further, ICANN proposes that there should be a single process for editing, compiling and signing the root to minimize intra-organization data transfer, and minimize the possibility for error. The authenticity of the zone file begins with the authentication and validation of the changes themselves by the IANA function of ICANN; creation of a signed zone should be a single process deriving from that initial validation.

ICANN is a not-for-profit, public benefit corporation that represents a global, multi-stakeholder community with a central focus on the security and stability of the DNS. ICANN is most likely to have global support to fulfill the signing role, and will undertake a consultation to determine this. Evidence of this support is demonstrated by the growing call from concerned TLD, RIR and other technical communities for ICANN to move forward with signing the root zone. Evolving policy issues, concerns of global oversight, interactions with parties in the DNS environment (such as registries and registrars), make ICANN the logical entity to perform this function.

ICANN has more than a year of experience in producing a signed root zone that has already been widely tested. ICANN has "built-in" the participation of a group of world-class DNS experts. ICANN also recognizes that there are outstanding deployment choices that no entity has fully answered, and that ICANN has and will continue to engage in an open process to seek advice and answers. While no outstanding question represents a technical roadblock, important decisions have to be made, and they are best made in an open manner.

ICANN's transparent, international and community-based processes are ideally suited to support the key stakeholder consultation required to finalize operational parameters and enable ongoing monitoring of these parameters.

Through a well-documented key ceremony with appropriate participants, the proposed U.S. Department of Commerce NTIA authorization and audit function, and appropriate third-party control of key-signing keys, there can be adequate oversight to assure successful longevity of the trust model of a signed root.

Beginning with the proposed consultation in October, ICANN looks forward to working with DoC and interested parties to refine this proposal, and then bring it to rapid fruition for the benefit of all Internet users.