Securing the Root: A Proposal for Distributing Signing Authority

17 May, 2007

Drafters:
Brenden Kuerbis
Milton Mueller

Management of the Domain Name System (DNS) root zone file is a uniquely global policy problem. For the Internet to connect everyone, the root must be coordinated and compatible. While authority over the legacy root zone file has been contentious and divisive at times, everyone agrees that the Internet should be made more secure. A newly standardized protocol, DNS Security Extensions (DNSSEC), would make the Internet's infrastructure more secure. In order to fully implement DNSSEC, the procedures for managing the DNS root must be revised. Therein lies an opportunity. In revising the root zone management procedures, we can develop a new solution that diminishes the impact of the legacy monopoly held by the U.S. government and avoids another contentious debate over unilateral U.S. control. In this paper we describe the outlines of a new system for the management of a DNSSEC-enabled root. Our proposal distributes authority over securing the root, unlike another recently suggested method, while avoiding the risks and pitfalls of an intergovernmental power sharing scheme.

1. What is DNSSEC and How Does it Improve Internet Security?

The functioning of the DNS is dependent on the successful interaction between *resolvers* and *nameservers*. Resolvers *query* nameservers, sending a domain name and receiving a *response* with corresponding resource record information (e.g., an IP address). DNSSEC is a proposed standard which modifies DNS resource records and protocols to provide security for query and response transactions made between name resolvers and nameservers. By introducing public-key cryptographic signed data into the DNS using four new resource records (see Appendix A for an overview of the resource records introduced and how they interact), DNSSEC specifically provides:

- Source authentication: a resolver can determine that a response originated from a zone's authoritative nameserver[1]
- Integrity verification: a resolver can determine that a response has not been tampered with in transit
- Authenticated denial of existence: a resolver can verify that a particular query is unresolvable because no DNS resource record exists on the authoritative nameserver

DNSSEC is intended to protect against some DNS attacks, including spoofing attacks which use "man-in-the-middle" techniques like packet interception, transaction ID guessing and query prediction, and DNS cache poisoning techniques like name chaining and transaction ID prediction.[2] These attacks can be exploited to redirect resolver

[1] A zone is an administratively determined section or "cut" of the domain name space. For example, .com, .edu and .se are three top level domain (TLD) zones; companyA.com is a second level domain zone in the DNS. A zone is served by one or more nameservers, i.e., a host machine which maintains DNS information for zero or more zones. In addition, for each zone, there exists a single authoritative DNS nameserver which hosts the original zone data, although this nameserver is typically mirrored in several locations. For TLD zones, the primary master server which hosts the root (".") zone file is authoritative. It is mirrored by root server operators around the world.

[2] See Atkins, D., Austein, R. (2004), RFC3833: Threat Analysis of the Domain Name System (DNS). Retrieved December 2006, from http://www.ietf.org/rfc/rfc3833.txt for a detailed analysis of threats which DNSSEC addresses; for information on the different types of DNS spoofing attacks see U. Steinhoff , A. Wiesmaier, R. Araújo; The State of the Art in DNS Spoofing; In: 4th International Conference on Applied Cryptography and Network Security (ACNS'06) and

requests to bogus hosts, where other disruptive or criminal acts, like data phishing and malware infections can occur which threaten security.[3] While various types of DNS attacks have increased, there is no public data available that quantifies the risk and associated damage of attacks that could be prevented by DNSSEC, leaving many cost-benefit questions unanswered. Importantly, DNSSEC does not address other well-known DNS vulnerabilities like distributed denial of service (DDoS) attacks. Likewise, DNSSEC provides little defense against basic phishing attacks for which success is largely dependent on end-user behavior.

2. Some Economics and Politics of DNSSEC

Despite widespread belief that remedying security vulnerabilities in the DNS would be beneficial, the development and deployment of the DNSSEC protocol has taken an extraordinary amount of time. The specification was initially developed in the mid 1990s, several years after security vulnerabilities in the DNS became publicly known and discussed within the Internet Engineering Task Force (IETF). It was first published as a RFC in 1997.[4] In 2001, substantial changes were proposed to the specification and it was re-written between 2001 and 2005. Finally, in March 2005, the revised specification was approved by the Internet Engineering Steering Group (IESG) and published in three separate RFCs covering requirements, additional resources, and protocol modifications.[5] The delay in development is partially attributable to the technical and organizational complexity of the protocol, the economics associated with its implementation, and an expanding array of interests in a secure DNS.

By any measure, the DNS has been an incredibly reliable and effective globally distributed lookup directory, resolving billions of queries each day and facilitating substantial worldwide Internet commerce.[6] This success places a heavy burden of proof on any new proposals that add complexity by changing the underlying technology and processes. DNSSEC is not a simple protocol; it requires the development of upgraded or new software and imposes an additional computational burden on the resolver and nameserver infrastructure.[7] For large TLD registries, unless additional protocols are

Ariyapperuma, S., Mitchell, Chris J., Information Security Group, (2007) Security vulnerabilities in DNS and DNSSEC. Retrieved January 2007, from http://www.isg.rhul.ac.uk/cjm/svidad.pdf.

[3] For detail associated with a single episode of DNS poisoning that occurred in March 2005, see http://isc.sans.org/presentations/dnspoisoning.html

[4] See Eastlake III, D. E., & Kaufman, C. (1997). RFC 2065: Domain Name System Security Extensions. Retrieved March 15, 2005, from http://www.ietf.org/rfc/rfc2065.txt. This document became obsolete with the publication of Eastlake, D. (1999). RFC 2535: Domain Name System Security Extensions, from http://www.ietf.org/rfc/rfc2535.txt

[5] See Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *RFC4033: DNS Security Introduction and Requirements*. Retrieved March 15, 2005, from http://www.ietf.org/rfc/rfc4033.txt; Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *RFC4034: Resource Records for the DNS Security Extensions*. Retrieved March 15, 2005, from http://www.ietf.org/rfc/rfc4033.txt; and Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *RFC4035: Protocol Modifications for the DNS Security Extensions*. Retrieved March, 2005, from http://www.ietf.org/rfc/rfc4033.txt.

[6] See National Research Council. (2005). Signposts in Cyberspace: The Domain Name System and Internet Navigation. Washington D.C.: National Academies Press and OECD Key ICT Indicators, available at http://www.oecd.org/document/23/0,2340,en_2649_34449_33987543_1_1_1_1,00.html

[7] See Guillard, A. (2006). DNSSEC Operational Impact and Performance. ICCGI 2006, 63. See also Ager, B., Dreger, H., & Feldmann, A. (2006). Predicting the DNSSEC overhead using DNS traces. 40th Annual Conference on Information

adopted, the deployment of DNSSEC will likely be delayed indefinitely.[8] The use of digital signatures introduces the need for methods and organizational security policies pertaining to key generation (e.g., algorithm, length), distribution, storage, and scheduled or emergency rollovers. These issues are particularly important for zones higher in an authentication chain. Additionally, the type and number of organizations affected by the changes DNSSEC requires have expanded. Originally, enterprises, universities and government agencies were largely responsible for operating their own nameservers. Today a whole industry sector has developed around managed DNS services.

DNSSEC also faces a classic chicken-and-egg adoption conundrum. Without a critical mass of signed zones (and particularly .com and the root), there is no viable demand for the development of DNS security aware applications. On the other hand, without such applications there is no demand for signed zones. In the context of price regulation by ICANN, the gTLD registries have no known pricing model for providing secure DNS services. Despite this, efforts are underway to develop other protocols and systems that could use a security enhanced DNS. For instance, Domain Keys Identified Mail (DKIM) proposes to use secure domains to authenticate the source or intermediary of an email message, as well as the contents of messages, in order to deal with email based spam.[9] And identity management systems like OpenID, in which a user's identity is associated with a particular URL, could also leverage the widespread deployment of DNSSEC.[10] However, both of these are nascent technologies and certainly not “killer apps” which could spark DNSSEC adoption at this point. Faced with this uncertainty, the larger or more critical zones (e.g., .com) are still weighing the costs and benefits of DNSSEC.

Another possible benefit of DNSSEC is its ability to enable widespread encrypted communications, which has long been of concern to law enforcement and surveillance interests.[11] While the protocol itself specifically does not address confidentiality of data or communications, the adoption of DNSSEC could create a globally accessible,

Sciences and Systems, 1484-1489. DNSSEC does not face one classic adoption hurdle, backward compatibility, as it was designed to be interoperable with the existing system.

[8] Specifically, the addition of NSEC RRs (see Appendix) creates the opportunity for “zone walking” or enumeration of DNS data, a significant concern for large zones because of data privacy risks. In response, NSEC3 “opt-out” was proposed. See B. Laurie, Sisson, G., Arends, R., Blacka, D,, *DNSSEC Hashed Authenticated Denial of Existence*, Internet-Draft, January 2007. Available at http://tools.ietf.org/html/draft-ietf-dnsext-nsec3-10. VeriSign has led the effort, hosting an important developer’s workshop and expressing the importance of NSEC3 opt-out for them. The tradeoff is that if a zone adopts this protocol it would diminish the original “authenticated denial of existence” capabilities of DNSSEC within that zone.

[9] See T. Hansen, Crocker, D., Hallam-Baker, P., *DomainKeys Identified Mail (DKIM) Service Overview*, Internet-Draft, October 2006. Available at http://www.ietf.org/internet-drafts/draft-ietf-dkim-overview-03.txt

[10] See D. Recordon and Reed, D., *OpenID 2.0: a platform for user-centric identity management*, Proceedings of the second ACM Workshop on Digital Identity Management, 2006.

[11] In fact, early DNSSEC deployment efforts were tripped up by U.S. export controls, resulting in the temporary removal of BIND (i.e., the market dominant DNS software) prototype source code from the Web. Originally classified in 1996 by the Bureau of Export Administration (BXA) as authentication software and therefore exempt from Export Administration Regulations, the software was reclassified as a controlled item almost a year later by BXA, making it subject to export restrictions. BXA concern centered over the inclusion of RSAREF, a collection of the various cryptographic routines source code which could be modified to provide data confidentiality. However, it was argued that BXA had questionable jurisdiction and its action was based upon an unwritten rule to reclassify the software. Eventually, with liberalization of export controls, the restriction was lifted. See Gilmore (2000) at http://www.chiark.greenend.org.uk/pipermail/ukcrypto/2000-February/047193.html

authenticable infrastructure for the secure distribution of other information. A secure DNS could help resolve long-standing problems associated with secure distribution of public-keys and certificates, facilitating communications privacy using popular encryption systems such as SSH or PGP.[12] In fact, engineers working for the main US government contractor on DNSSEC were cognizant of this benefit early on, viewing it as a potential "big driver behind DNS security."[13]

Given the associated hurdles and potential for DNSSEC, it is no surprise that there has been broad interest in the protocol's development and adoption. Early development came from specialized agencies within the U.S. Department of Defense (DoD) and its contractors, along with technical experts participating within the Security Area of the Internet Engineering Task Force (IETF). Interest in DNSSEC expanded greatly as the Internet developed into a widely used and critical piece of communications infrastructure. Beginning in 2001, development shifted to the IETF's Internet Area, and a range of technical experts from registries, DNS management and software providers, applications developers, U.S. government (USG) agencies and individuals associated with government and industry-supported research centers sought to influence DNSSEC. And recently, as the protocol moved toward the deployment stage, Internet governance institutions like ICANN have become increasingly involved.

The USG's role in DNSSEC's evolution since 2001 has focused on both development and deployment activities. In addition to a general increase in funding of basic research on Internet security coinciding with the 2002 Cyber Security Research and Development Act,[14] the National Science Foundation (NSF) has awarded grants to DNSSEC-specific projects and researchers directly involved in the standard's evolution. The DoD continued its lengthy participation in applied DNSSEC research and the standard's development via private contractors. Individuals with these organizations have actively participated in the IETF process and continue efforts to promote DNSSEC within the Internet's technical community and ICANN.

The Department of Commerce's National Institute for Standards and Technology (NIST) was active in the revised protocol's development, participating extensively in the IETF's DNSEXT Working Group since 2001, and leading IETF editorship of five core DNSSEC specifications. In part, these activities were driven by Title III of the E-Government Act of 2002 (i.e., the Federal Information Security Management Act (FISMA)), which required NIST to "develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems."[15] In addition, the Act required that NIST "consult with other agencies and offices and the

[12] See S. Joesefsson, *Storing Certificates in the Domain Name System (DNS)*, RFC4398, March 2006.
[13] See presentation from Trusted Information Systems Labs at the May 2001 North American Networks Operators Group (NANOG) meeting, available at http://www.nanog.org/mtg-0105/ppt/lewis.ppt#280,13,Result: Value of Key Distribution
[14] See H.R. 3394, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.107
[15] See E-Government Act of 2002, Pub. L. no. 107-347, 116 stat 2899 (2002). Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107

private sector (including the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security)." [16]

Beginning in 2003, the U.S. Department of Homeland Security's Directorate for Science and Technology became active through its Internet Infrastructure Security Program (IISP).[17] DHS involvement was in response to the role given to them as part of the 2002 Homeland Security Act, the *National Strategy to Secure Cyberspace*, and the 2003 Homeland Security Presidential Directive 7, which positioned DHS to become the lead federal point of contact for the information technology and telecommunications industry sector. Working together to support compliance with Federal Information Processing Standards (FIPS) as required by FISMA, NIST drafted several documents pertaining to DNSSEC which were sponsored by DHS.

Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide, was published in May 2006, providing implementation guidelines (e.g., key management policies) for USG organizations running DNSSEC.[18] In October 2006, NIST produced together with two central defense contractors, *Signing the Domain Name System Root Zone: Technical Specification*, making recommendations for changes in root zone file management with respect to the implementation of DNSSEC.[19] And in December 2006, NIST announced the release of the revised *Special Publication 800-53, Recommended Security Controls for Federal Information Systems*, which provided guidance on the use of external information systems (like the DNS) and outlined plans for the staged deployment of DNSSEC technology within medium and high impact federal IT systems.[20] U.S. federal agencies will have one year after the document's final publication to comply with the new standards.

3. The Root of the Problem: Creating a Trust Anchor(s)

DNSSEC implements a hierarchical model of trust. A DNS security-aware resolver's ability to validate nameserver responses is accomplished by establishing an authentication chain from a known trust anchor(s) (i.e., a cryptographic public key[21]) to the zone which has provided the signed response. If a resolver is configured with a trust

[16] The relationship between law enforcement and surveillance interests and technical agencies (like NIST) in the U.S. government, as it pertains to encryption use in communications systems in the United States, has been a source of controversy for two decades. See Diffie and Landau (1998) for the history of the National Security Agency's (NSA) role in encryption related standards and the Computer Security Act of 1987, which moved official development of federal encryption standards (for unclassified material) to NIST from NSA. The importance of creating this separation still resonates with lawmakers; the current administration's proposal to move the NIST's Computer Security Division to the DHS (see Homeland Security Act of 2002 as introduced in House) during its formation was met with strong resistance by Senator Cantwell (WA) and others familiar with the "crypto-wars" of the early 1990s, and ultimately the proposal failed. See Carney, D. (2003). DHS and NIST to Collaborate. Retrieved November 30, 2005, from http://www.techlawjournal.com/topstories/2003/20030522.asp

[17] See http://www.us-cert.gov/press_room/050215cybersec.html

[18] See http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

[19] Available at http://mail.shinkuro.com:8100/Lists/dnssec-deployment/Message/553-02-B/061031RootSignSpec.pdf

[20] Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

[21] This key data is contained in the DNSKEY or a signed DS resource record, see Appendix A.

anchor(s) that exists higher in the DNS tree, e.g., the root's public key,[22] it can theoretically verify any signed responses.[23] This is because a path can always be constructed from the root to lower zones, assuming every zone in the path is signed and carries a Delegation Signer (DS) record for child zones. This architectural design highlights the critical importance of parent nameservers maintaining and signing DS records, if widespread deployment of DNSSEC across the Internet is to be achieved.

However, what happens in a scenario if portions of the DNS tree, and particularly the root, is not signed? A broken authentication hierarchy, where a parent zone does not support DNSSEC, creates the "islands of trust" problem. For instance, the entire country code for Sweden, .se, is signed yet its parent (the root) is not.[24] The .se zone is a secure island isolated from the rest of the DNS tree. Therefore, the .se registry is responsible for the associated key management tasks (e.g., signing, distribution, rollover to new key, etc.) and security aware resolvers must manually configure its trust anchor. Another example might be USG agencies under the .gov or .mil top-level domains, where implementation of DNSSEC is being pushed by the need to be compliant with FISMA. With key government software vendor Microsoft planning to support DNSSEC in their DNS server software in early 2008, it will be possible to deploy DNSSEC in zones the USG is responsible for without securing the root.[25]

Other options[26] for dealing with the absence of signed DS records in the root have been proposed. DNSSEC Look-aside Validation (DLV)[27] was originally put forth as an interim solution until the root was signed. DLV bypasses the normal DNS hierarchy and allows resolvers to validate DNSSEC-signed data from zones whose ancestors either aren't signed (e.g., the root) or refuse to publish DS records for their child zones. The current specification suggests that IANA maintain a DLV registry, although more than one party could maintain a registry of validated entry points to secure zones.[28] While the introduction of multiple DLV registries could be beneficial from a market competition standpoint, its early adoption could also pre-empt efforts to sign the root.

[22] To be precise, the key mentioned above is actually the "key signing key" (KSK) for the root zone. In fact, in most cases each zone will manage two types of key-pairs, KSKs and zone signing keys (ZSKs). The ZSK key-pair is used to sign a particular zone's record sets and will be used frequently by resolvers in queries, while the KSK key-pair is used less frequently because it is used only to sign and authenticate a zone's ZSK.

[23] R. Chandramouli and S. Rose, "Challenges in securing the domain name system," Security & Privacy Magazine, IEEE 4, no. 1 (2006): 84- 87. This point is actually very theoretical if the zones in which the majority of domain names exist (e.g., .com) do not implement DNSSEC.

[24] Sweden's Internet Infrastructure Foundation announced commercial DNSSEC service in February 2006, with secure resolution being offered by Swedish ISP TeliaSonera. See http://www.iis.se/english/nyheter/news/2007-02-16?lang=en%20.

[25] Concerning Microsoft's support see http://www.dnssec-deployment.org/news/2006211-Microsoft-DNSSEC.pdf. See http://www.upi.com/Security_Terrorism/Analysis/2007/04/12/analysis_owning_the_keys_to_the_internet/ for claim that DNSSEC can be deployed within USG zones without the root being signed.

[26] This is not exhaustive list of alternatives dealing with an unsigned root. Other non-hierarchical solutions have been suggested. E.g., one proposes out of band "web-of-trust" trust anchor distribution, another suggests islands cross-sign KSKs. Furthermore, it does not include trust anchor update alternatives the Working Group has considered, e.g. trustupdate-threshold, trustupdate-timers, and TAKREM.

[27] One implementation is currently run by ISC, makers of the market dominant BIND name serving software.

[28] See S. Weiler, *DNSSEC Lookaside Validation (DLV)*, Internet-Draft, March 2007. Available at http://tools.ietf.org/html/draft-weiler-dnssec-dlv-02.

Either of the scenarios above, manual configuration or DLV, would enable the incremental deployment of DNSSEC since the protocol allows resolvers to store and use multiple trust anchors. However, while these alternatives remove the difficult hurdle associated with signing the root zone file, it also changes who absorbs the deployment and ongoing costs of DNSSEC. Such an approach risks eliminating the efficiencies gained by maintaining relatively few trust anchors for the secure, global DNS. Multiple organizations would have to deal with the same operational questions and expenses, namely key management and liability surrounding holding such a critical position in an authentication hierarchy. More importantly, having numerous trust anchors would increase the burden of security policy evaluation and key updating for resolver operators (i.e., to ISPs running caching resolvers, and perhaps ultimately, to security-aware stub resolvers used by end-user applications). Arguably, it presents a situation that is simply not scalable across the entire Internet.

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

4. A Proposal for Distributing Root Signing Authority

It is evident that the best way to secure the DNS effectively, efficiently, and globally is to implement DNSSEC at the root. But how?

A report prepared in late 2006 for the U.S. Department of Homeland Security proposed that a single organization assume the role of Root Key Operator (RKO), and be responsible for the Key Signing Key (KSK) and Zone Signing Key (ZSK) for the Internet's root zone.[29] Although the report did not explicitly say that the control of the keys would be held by DHS itself or even a U.S. government agency, the politically sensitive association between a U.S. national security organization and the root signing process triggered international concern.[30] This concern was first publicly expressed at the recent ICANN meeting in Lisbon by the president of the Canadian Internet Registration Authority (CIRA). It was followed by a flurry of stories questioning the motives of the U.S. government, and a public response by DHS over a month later where the responsible Program Manager indicated a new specification would be released for public comment by late summer 2007.[31]

This paper proposes an alternative to the DHS proposal that is technically feasible and takes into account the political, economic, and operational issues. The development of a procedure to sign the DNS root zone file provides an opportunity to achieve shared responsibility for the secure and stable operation of the Internet's root zone. It is

[29] See *Signing the Domain Name System Root Zone: Technical Specification*, available at http://mail.shinkuro.com:8100/Lists/dnssec-deployment/Message/553-02-B/061031RootSignSpec.pdf

[30] See http://www.heise.de/english/newsticker/news/87655/from/rss09.

[31] See http://www.upi.com/Security_Terrorism/Analysis/2007/04/12/analysis_owning_the_keys_to_the_internet/. The strong public reaction was perhaps reflective of the way in which the DHS report was handled. The document was reviewed initially by other USG agencies and then distributed for comment in November 2006 to a limited group of technical experts in government, academia, and key Internet governance and infrastructure organizations from eight countries the USG has traditionally dealt with concerning Internet governance issues. Surprisingly, the document was marked "not for further distribution" yet posted to a publicly available listserv. An unknown number of comments on the report were received, but were not made available to the public. The exception was one comment posted independently to the listserv by a DNSEXT Working Group participant, see http://mail.shinkuro.com:8100/Lists/dnssec-deployment/Message/559-02-B/closing_the_gap_rko_tak_rollover.pdf

possible for **multiple (but limited in number) non-governmental Root Key Operators (RKOs) to take responsibility for generating, using and distributing root zone key-signing keys (KSKs) and zone signing keys (ZSKs).** In practice, this will require close coordination between Root Key Operators and Root Zone Maintaining organizations in executing contractually agreed upon roles.

To clearly understand how this proposal will impact modifying and publishing the Root Zone File (RZF), it is best to briefly outline the current process and actors involved. Currently, change requests from registries are sent to ICANN (specifically IANA) for processing. Once it is determined that the changes meet IANA's narrow technical requirements and they are approved by the ICANN Board, the request is forwarded to the U.S. Department of Commerce for review and approval. If the Commerce Department approves, the Root Zone Maintainer (RZM), currently VeriSign, edits and generates the revised RZF. The RZF is then loaded by the Root Zone Distributor (RZD) (also VeriSign at this time) to the Distribution Master Name Server. Once there, it can be retrieved by the other root server operators located around the world.

Implementing DNSSEC will require modifications of hardware, software and operational procedures within most of the aforementioned organizations. The notable exception to these change requirements is the authorization role played by the Department of Commerce, which has no impact on the technical operation of the DNS or the deployment of DNSSEC.

Instead of a single RKO, we propose that multiple, independent, nongovernmental RKOs be responsible for generating KSKs and ZSKs and transmitting the public portions of these keys to the Root Zone Maintainer for construction of a Root Keyset (see Figure 1 below). RKOs would be also responsible for distribution of the public portion of their KSK (i.e., the "trust anchor") globally. Once constructed, the Root Keyset would be distributed to the RKOs for signature over the complete set of keys. The signed Root Keyset is then returned to the RZM for inclusion in the RZF. Each RKO will then sign a copy of the root zone file using the private portion of their respective ZSKs and transmit it to the RZM who will merge the files. All of the exchange of data between RKOs and the RZM would occur on secure out-of-band channels. The merged RZF would then be distributed according to existing procedures. A resolver could utilize any one of the available KSKs to authenticate the RZF contents.

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

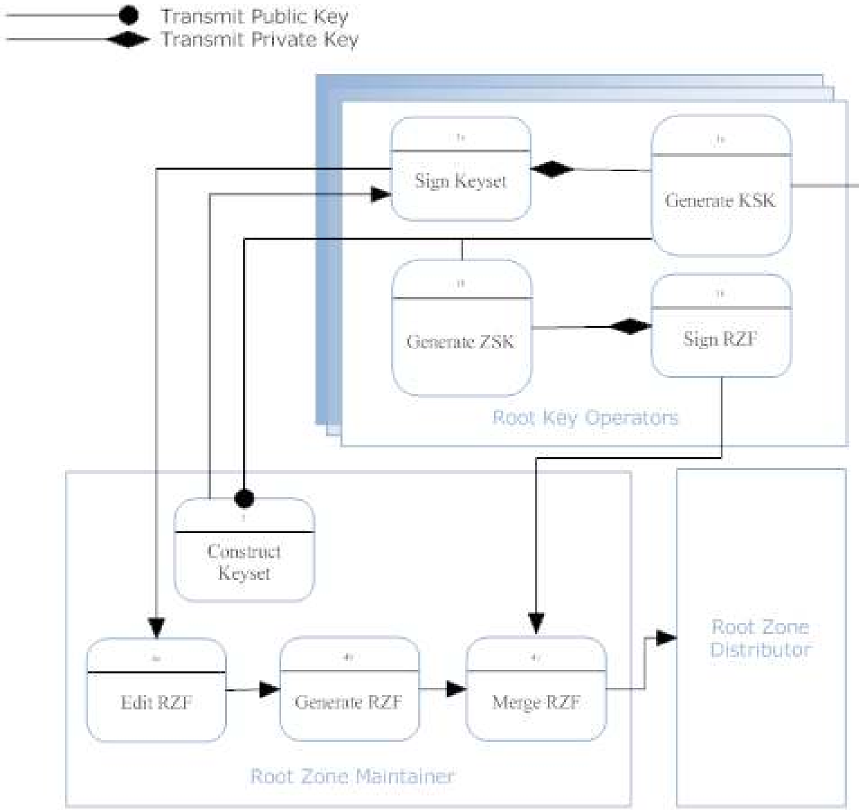

Figure 1: Root Signing Process with Multiple RKOs

Like any procedural recommendation, there are benefits, risks and unknowns. Some of these are identified below:

Eliminate threats of political interference

A prominent feature of this proposal is the elimination of governmental organizations from the root zone management process. While the majority of domain names are currently registered in gTLD namespaces, the majority of TLDs in the root are ccTLDs and it is these namespaces which are experiencing strong growth.[32] The issue of who controls delegation and redelegation of ccTLDs has always been sensitive,[33] and the addition of Delegation Signer (DS) records to the root will only serve to amplify these concerns. Because of this, the direct involvement in root signing, or additional oversight of data flows between RKOs and the RZM, by any government is ill advised. It only serves to introduce risk, raise uncertainty among contracted parties, and undermine the credibility of the system. Moreover, it is unnecessary from an operations perspective.

[32] See http://www.verisign.com/static/040767.pdf

[33] See pg. 254, National Research Council. (2005). Signposts in Cyberspace: The Domain Name System and Internet Navigation. Washington D.C.: National Academies Press. Available at http://books.nap.edu/openbook.php?isbn=0309096405&page=254

Cases of incorrect data being sent to another party can be remedied using operational quality control techniques like standards certification. Furthermore, given the openness of the DNS, any verification that an outside party would perform can be done by anyone if the process is done with minimum standards of transparency. The deployment of DNSSEC at the root is best left to the organizations that are contractually obligated for maintaining the RZF contents and should be let alone from potentially destabilizing interference created by government oversight.

Mitigate threats of an uncoordinated root

The proposal outlined above introduces certain risks. However, these risks exist in the root signing process irrespective of the number of RKOs chosen. First, there is the risk of a party introducing unapproved changes (i.e., adding, deleting, altering resource records) in the RZF. For example, an RKO could alter the contents of the root zone file it signs and return it to the RZM for inclusion in the merged RZF. Second, there is the risk of a party not receiving the RZF it expects. For example, the RZF could be modified by IANA/ICANN (or the RZM) and the RKO receives a copy of the RZF for signature which does not meet their expectations. Ultimately, the process of digitally signing the root does not address the fundamental issue of who has the power to decide the contents of the root zone file. But by developing the right organizational and legal framework, undesirable actions can be constrained to acceptable levels, and a single, authoritative RZF with multiple signatures can be achieved, thereby increasing stability and security at the root.

First, TLD registries must have contractual agreements in place with IANA/ICANN for delegation services, stipulating what resource records for their zone are to be included in the RZF. This also requires conditions that avoid leading IANA/ICANN and registries to violate their agreements. For instance, IANA/ICANN must be an institution that is not subject to outside influence. It should simply make the technical determination for resource record additions to the root based on documented policies and transparent processes. And it should be held legally accountable if it deviates from these policies and processes.

Second, TLD registries interested in offering secure DNS services must have contractual arrangements with an RKO for signature services over the same resource records. In addition to digitally signing those records, part of an RKO's obligations should be monitoring and information sharing. If any one of the RKOs receive a RZF for signature with unexpected contents, the contracted RKO would obviously not sign (nor should the others if their root signing services provide any level of assurance), and then the affected registry can take action against IANA/ICANN. Given these arrangements, a RKO should always receive what it expects to receive, and if it doesn't, the affected party (the TLD registry) has recourse.

Third, assuming the services performed by the RZM continue to be maintained by an organization separate from IANA/ICANN,[34] its role should be contractually limited to distributing the RZF to RKOs for signatures and ensuring that the RZF contents which were sent to the RKOs are, in fact, the contents which are signed. An RKO could always introduce a change, but the use of audits by the RZM would catch this prior to its merging and subsequent distribution of the RZF to root server operators. Processing audits will add additional steps; however, it is not likely to pose a significant operational hurdle. Even with the addition of DNSSEC resource records, the root zone will not be not a large data file. The current management of the RZF already incorporates digital signatures, error checking, and correction processes, so the existing parties are familiar with the techniques. Nonetheless, any process that involves coordinating multiple parties and which may need to occur on an unscheduled basis will need to be well documented, tested, and transparent.

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

Inevitably, scenarios can be imagined where the proposal herein could falter. A registry could become insolvent raising issues of TLD redelegation; a RKO could sign a RZF which includes a TLD that knowingly hosts DS records for malicious websites; IANA/ICANN, a RKO or the RZM could be pressured by external actors to remove a DS record. However, it is important to realize that *any root signing arrangement* will have risks. And many of these risks already exist today in some form; we have simply managed to avoid them. The important questions are, how can these risks be mitigated, and are they greater than the possible benefits of signing the root? It is more likely the case that if the root signing process is grounded in contractual obligations with clear responsibilities and incentives, documented policy and transparent processes, and independent institutions, any conflict which arises can be resolved.

[34] The transition of this role to ICANN was agreed upon in the 2006 Settlement Agreement with VeriSign, see http://icann.org/topics/vrsn-settlement/revised-root-transition-agreement-redline-29jan06.pdf. Details on progress toward transition are available at http://www.wwtld.org/eiana/. Completion could simplify the process of deploying DNSSEC at the root by reducing the number of parties involved.

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

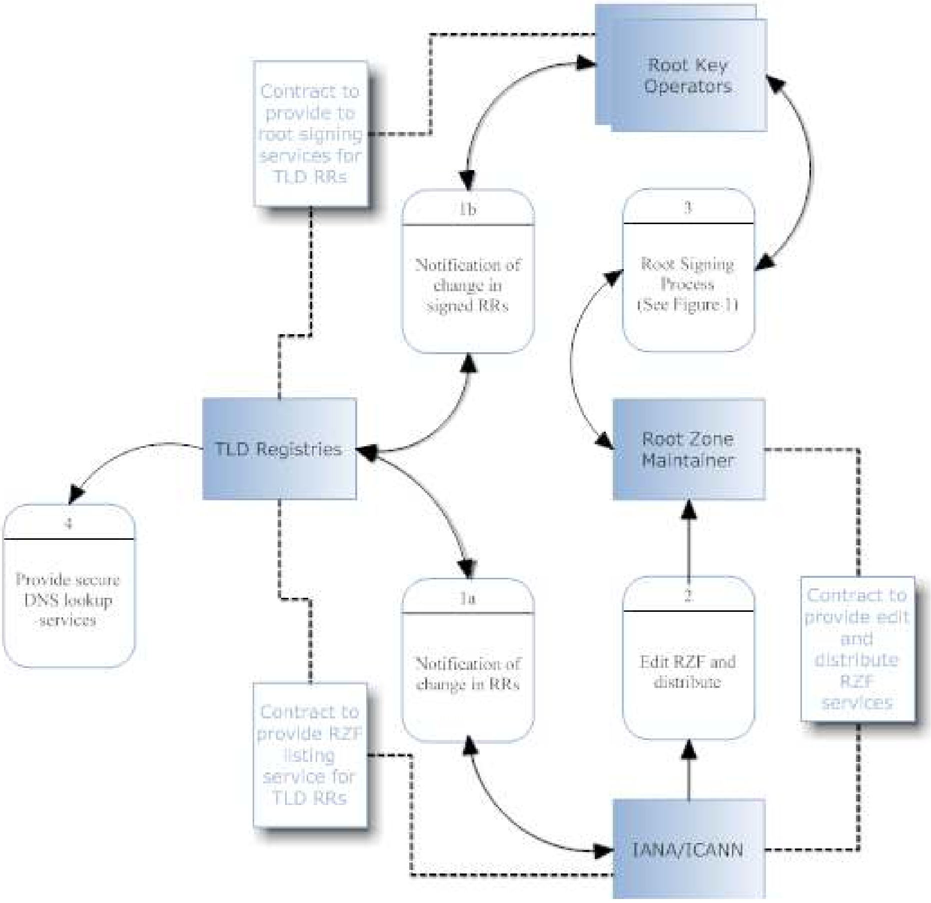
Root Key Operators
Contract to provide to root signing services for TLD RRs
1b
Notification of change in signed RRs
3
Root Signing Process (See Figure 1)
TLD Registries
Root Zone Maintainer
4
Provide secure DNS lookup services
1a
Notification of change in RRs
2
Edit RZF and distribute
Contract to provide edit and distribute RZF services
Contract to provide RZF listing service for TLD RRs
IANA/ICANN

Figure 2: Root Zone File Management Organizational Responsibilities

Distribute authority to increase resilience, diffuse liability

A key feature of the Internet's architecture and the DNS is decentralization. For instance, the DNS is distributed among many nameservers. Another example is the anycasting of root servers. Decentralization of critical Internet resources increases robustness of the entire system, protecting it from intentional and unintentional attacks. Having multiple, coequal RKOs makes the DNSSEC architecture more resilient against temporary outages that might be suffered by a single RKO. Resolver operators could use any number of available RKO trust anchors to validate RZF contents depending on their desired level of assurance. Distribution of control over the RZF KSK among multiple entities is desirable from the viewpoint of a decentralized Internet.

Liability is a powerful negative incentive which might discourage organizations from signing the root.[35] By involving multiple RKOs in the root signing process, potential liability associated with providing a signed RZF could be diffused. It could increase the variety of contracting arrangements between actors involved in root zone management and those relying on stable operation of a secure root. It is still unknown, however, what legal relationships may develop between RKOs, nameserver and resolver operators in the proposed system and under what jurisdiction these relationship may fall. This is a topic for future research.

Given the unique position held by RKOs as global "root authorities," some might suggest that it is necessary for them to gain international status to limit their liability. Just as common carriers in the US have limited liability, other governments and transnational organizations (e.g., the ITU) have also placed limitations of liability on certain telecommunications services.[36] Another approach to consider may be the development of a safe harbor for RKOs. Safe harbors have been used in other Internet governance issues (e.g., EU-US data protection and the Communications Decency Act), where an actors liability is made conditional only upon the non-compliance with some private rule regime.[37] In either case, the risk of these approaches is that RKOs are absolved of liability to the point that using “secure DNS” lookups becomes meaningless for applications which seek to rely on them. A compromise solution might involve limited liability for RKOs as DNSSEC is first deployed, but which sunsets after a certain period of time after the technology is shown to perform adequately. Such a scenario could also help create a market for DNS security aware applications.

Determination of Root Key Operators

A central question is determining how many and what organizations could be a RKO. The answer will be determined partly by technical constraints, partly by prior experience with other root authorities, and by market mechanisms. Technical constraints may include the number of keys in the Root Keyset, the number of keys used to generate signatures for the root zone data, properties of the keys such as size and algorithm used, response message size constraints, and the need to roll over keys periodically. Some of these constraints will lessen as technology evolves; others have policy dimensions as well, for instance, the choice of key size and algorithm used.

A secured DNS is not unlike a public PKI (Public Key Infrastructure). It combines limited digital signature services, facilities, policies, procedures, agreements, organizations and

KSK	Key Signing Key
RKO	Root Key Operator
RZD	Root Zone Distributor
RZF	Root Zone File
RZM	Root Zone Maintainer
ZSK	Zone Signing Key

[35] This assertion is evident in comments heard on various DNSSEC lists. E.g., in a conversation about IANA implementing a DLV registry, an employee of ICANN noted that “the holder of the root KSK is setting itself up to be a teensy bit of a target. Compromise of the root KSK would have … significant implications and likely astounding liabilities. Who wants that?”

[36] See Baum, M. (1994) *Federal Certificate Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures*, (Report NIST-GCR-94-654) Washington D.C.: U.S. Department of Commerce. 311-313. Available at https://www.verisign.com/repository/pubs/fca_liability.pdf

[37] See pgs. 115, 148-156, National Research Council. (1996).Global Networks and Local Values: A Comparative Look at Germany and the United States. Washington D.C.: National Academies Press as cited on pg. 210, Engel, C. (2006). The Role of Law in the Governance of the Internet, *International Review of Law, Computers & Technology*, 20(1&2), 201-216.

people to supply secure DNS queries and resolutions. The critical role of Certificate Authorities in PKIs is similar to the role RKOs will play. Experience with assessment and accreditation regimes, standards, and best practices for PKIs could provide guidance in determining actors suitable for providing RKO services. Assessment and accreditation regimes are useful in that they can ensure objective oversight, promote trustworthiness, and provide organizations with risk management tools that "can demonstrate due diligence, satisfy insurance requirements and reduce legal exposure."[38] A broad array of PKI assessment and accreditation schemes exist at the national, regional and sectoral levels, e.g., the *Common Criteria for Information Technology Security Evaluation*. Similarly, NIST has documented standards and best practices for key management organizations which could serve as guidelines. Similar efforts from other countries should be examined as well. At a global level, the UNCITRAL Model Law on Electronic Signatures offers general remarks for characteristics that organizations within a PKI, including root authorities, should posses.

To date the development of broadly available public PKIs has been slow, with a mix of widely available Certificate Authorities offering services with minimal liability protection (if any), while more purpose-specific "private" Certificate Authorities (e.g, the USG Federal Bridge Certificate Authority, or corporate PKIs) have emerged for higher-risk scenarios. The level of assurance provided by the digital signatures in each case varies according to the economic incentives of the parties.[39] Until and unless the economic incentives for signing the root are more clearly understood, and we are able to create an organizational and legal framework that appropriately balances risk and the potential for reward, the deployment of DNSSEC will most likely approximate the first scenario.

5. Is Multilateral Government Control of the Root Zone File an Option?

Two important ICANN insiders, AT&T lobbyist Marilyn Cade and former Commerce Department official Becky Burr, have developed a proposal to end unilateral U.S. oversight of the root. Under the Burr-Cade proposal, a 15-member Working Group of governmental representatives would be formed. This group would be authorized to place a "time-limited hold" on changes in the root zone recommended by IANA. According to Burr-Cade, such a hold could be placed "solely on the grounds that such change creates an unreasonable risk to the technical stability or security of the DNS and/or the Internet." The purpose of the Burr-Cade proposal is to "multi-lateralize" U.S. oversight authority. Aside from that, it is based on the same principle as the current system, which is that governmental oversight and direct intervention in the zone file modification process are needed to ensure that the Internet is not "de-stabilized". It takes existing U.S. authority and distributes it among a larger pool of governments.

KSK – Key Signing Key

RKO - Root Key Operator

RZD – Root Zone Distributor

RZF – Root Zone File

RZM – Root Zone Maintainer

ZSK – Zone Signing Key

[38] See Chapter 11, Ford, W., & Baum, M.S. (1997). *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. Prentice-Hall, Inc. Upper Saddle River, NJ, USA.

[39] The need to align economic incentives has been increasingly recognized as instrumental in deploying information security technology; see e.g., Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science, 314*(5799), 610.

In our view, the Burr-Cade proposal adds nothing to the technical security of DNS management, but compounds the political problem by thrusting more governments into a process where governments add no value in the first place.

Let us assume for a moment that all governments involved have the right incentives and would completely restrict their attention to technical matters. It is still hard to see how governmental review of zone file maintenance helps. A DNS zone file is composed of several hundred lines of domain names, IP addresses and software commands. It is implausible on its face to assert that the technicians who perform the IANA function, and the root server operators who implement the changes, would fail to spot a modification that would cause technical problems, but a committee of governmental policy people would recognize it. It would make more sense to develop robust automated procedures, and allow autonomous technical experts, not political representatives of nations, to review the changes for their impact on technical stability.

But of course we cannot assume that governments have the right incentives. While the proposal nominally restricts “time-limited holds” to changes that pose a risk to “technical stability and security,” there is no way to prevent this authority from being used for political purposes. And in fact, that is what governments are really interested in. Governments are intrinsically political institutions. All of our past experience suggests that they are interested in the DNS root because of its political, strategic and economic importance, not for any technical reason. There is no way to automatically restrict the challenges governments make to ones that are actually “technical” in nature; the status of any challenge would have to be debated and approved or overruled after it was made. We see a major risk that this authority might be abused. The risk increases as the Working Group becomes more broadly representative. As more autonomous and diverse governments are involved, the greater the likelihood that the group will reflect the intense political conflicts in the world as a whole. (Not coincidentally, Burr-Cade’s selection criteria for the European and Asia-Pacific region members Working Group have been defined in a way that seems deliberately designed to exclude Russia and China. While this is understandable, it only reinforces our view that as long as governments are involved there is no escape from the insertion of geopolitical conflicts into Internet management.)

Throughout ICANN’s history, we have been subjected to countless claims that one thing or another “threatens the stability of the Internet” when in fact the objection was based on economic or political motives. And we already have one instance (the .xxx incident) in which purely political factors motivated a sudden governmental interest in the addition of a TLD to the root. In this respect, the Burr-Cade proposal might worsen the situation by institutionalizing governmental opportunities to exploit their veto power for political purposes and multiplying the number of governments involved. The invocation of “technical stability” is likely to function as a fig leaf that gives politicians an opening to interfere with Internet management for political or economic reasons.

The Burr-Cade proposal focuses attention on the wrong problem. There is no need for governmental oversight of root zone management *per se*; rather, there is a need for governments to ensure that whoever controls the root is responsible and accountable, and that the procedures followed are well-defined, clear and auditable. In order to ensure that, governments do not need to insert themselves directly into the root zone file management process, nor assert some kind of veto over changes. The most direct and effective answer to the real security and stability threats faced in RZF management is to make the organizations that manage the root zone directly responsible for damages caused by negligence or willful manipulation of the zone file. In that respect it is better to have private actors, who are more easily subject to lawsuits, in charge of the process. Governmental bodies have various kinds of immunity, and thus would be less accountable.

6. Conclusion

The widespread deployment of DNSSEC could make the Internet more secure, increasing the integrity and source authentication of DNS queries and responses, and preventing some disruptive or criminal acts. A critical aspect of deploying DNSSEC is the addition of resource records for each TLD and digitally signing the root zone file. To accomplish this, changes in root zone file management must be made if there is to be a manageable number of trust anchors for DNSSEC. A root signing procedure which includes multiple, but limited number of Root Key Operators provides an opportunity to distribute authority without the risks of multi-lateralization. This redesign provides an opportunity to phase out increasingly controversial national government oversight in favor of trusted nongovernmental actors.

The Internet Governance Project (IGP) is an interdisciplinary consortium of academics with scholarly and practical expertise in international governance, Internet policy, and information and communication technology.

To download its papers or to learn more about IGP, go to
http://internetgovernance.org

Appendix A: How Does DNSSEC Work?

A DNSSEC-enabled nameserver for a particular zone will store a **Signature Resource Record (RRSIG)** for the various sets of records it hosts. For example, it will contain the signed set of A records (RRSIG(A)), which point domain names to unique IP addresses. The RRSIG is a digital signature created by taking a hash of a zone's particular resource record set which is then encrypted using the private portion of a zone administrator's cryptographic key set. The corresponding public portion of this key set is stored in the **DNSKEY Resource Record.** When receiving a signed DNS response from a nameserver, a DNSSEC-aware resolver will decipher the appropriate RRSIG set using the zone's DNSKEY. It compares the now exposed resource record set hash against a generated hash of the nameservers unsigned resource record set, and is able to confirm or deny the integrity and origin authenticity of various information types.

How does a resolver know the authentic DNSKEY for a particular zone? The **Delegation Signer (DS) Resource Record** is served by the parent zone and creates an authenticable delegation point between parent and child zones. To validate a child zone's DNSKEY, a resolver retrieves the associated DS, RRSIG(DS) and DNSKEY of the parent zone. The DS is validated against the deciphered RRSIG(DS), and then the DS data is used to authenticate the DNSKEY of the child zone. In a sense, the signed DS acts like a “certificate” that is authoritatively served from the parent zone and binds a child zone to its DNSKEY. The parent zone nameserver becomes in effect a “trusted third party,” facilitating the exchange of DNS information between resolver and child zone. A series of these delegation relationships forms an authentication chain, which form a path a resolver can follow from the DNS root's public key (aka a “trust anchor”). Finally, the **Next Secure (NSEC) Resource Record** chains signed records together, allowing a resolver to traverse a zone file and determine if a particular host name does not exist in the DNS.

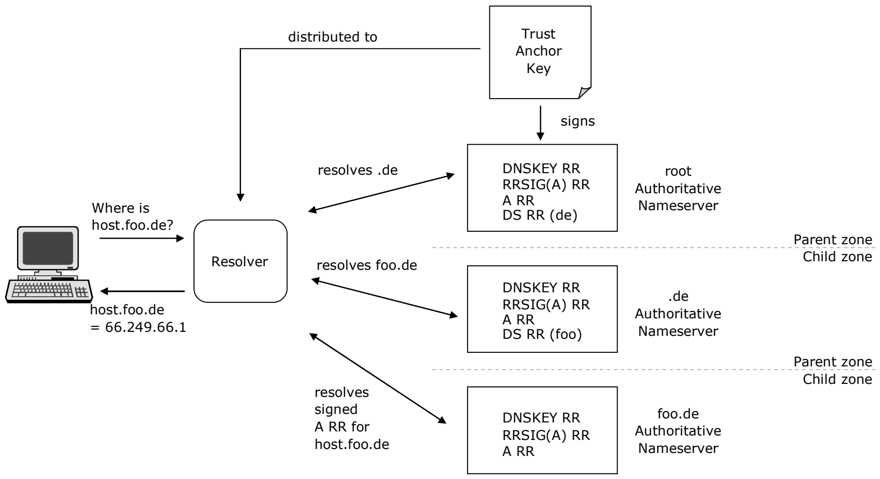

Figure 3: Simple DNSSEC Query and Response