

**DOMAIN NAME SYSTEM SECURITY
(DNSSEC)
DEPLOYMENT INITIATIVE

A ROAD MAP**

February 2005

Table of Contents

Table of Contents	i
Executive Summary	ii
I: Background: Introduction, Definitions and Work to Date	1
1.0 Introduction.....	1
1.1 Goal.....	1
1.2 Background.....	1
1.3 Organizations engaged in deployment activities	2
1.4 Participants in deployment: Roles and responsibilities	3
1.5 Contributing to development of this document	4
2.0 Definitions.....	5
2.1 Signed zones	5
2.2 Present and future DNSSEC-aware applications.....	6
3.0 Sequencing and Dependencies.....	7
3.1 Progress.....	7
3.2 Road maps.....	8
4.0 Outstanding Issues	9
5.0 Measurement, Evaluation and Progress.....	12
References Cited	14
Acknowledgements.....	15
Part II: Road Maps	16
Introduction to the Diagrams	16

Executive Summary

The DNS Security Extensions (DNSSEC) enhance the security of a fundamental element of the Internet infrastructure. DNS is a hierarchical naming system that maps IP (Internet Protocol) addresses to more user-friendly but structured names; the extensions to the original protocol consist of a hierarchy of cryptographic signatures that assure the integrity of the DNS queries by providing origin authentication of DNS data, data integrity and authenticated denial of existence. These measures protect against tampering in caches and transmission and enhance the infrastructure's security, thus contributing to increased trust in the Internet and systems, services and markets that rely upon its secure operation. The DNSSEC protocol has been under development for more than 10 years and was approved by the IESG in October 2004; it is awaiting final publication.

This road map describes the basic goal for deployment; the current state of practice, gaps and barriers; a set of sequences and dependencies; and next steps. Its primary audience consists of operators and administrators of the domain name system (DNS), their vendors and suppliers, and their customers.

The road map is divided into four major tracks: operations, software, issues and measurement of adoption and progress. The document is understood to be a "living" document and will be subject to periodic revision. At this point, its focus is on operations at the zone level: root, registry and registrants (or operators), describing the major phases of deployment – sign, serve, distribute public key and register – while recognizing that each entity that adopts the new protocol will undertake a planning step to analyze its context and requirements. Later versions will focus on the role of the registrants, software and other elements of the road map.

Progress has been observed in the following areas: implementation, testing and product development, including two pilot projects at two major registry operators; education and training, including materials, curriculum and workshops at major meetings; and committed operation in a few small experimental zones that are known to be operating with DNSSEC.

I: Background: Introduction, Definitions and Work to Date

1.0 Introduction

The DNS Security Extensions (DNSSEC) consist of a hierarchy of cryptographic signatures that assure the integrity of the DNS queries by providing origin authentication of DNS data, data integrity and authenticated denial of existence. These measures protect against tampering in caches and transmission and enhance the infrastructure's security, thus contributing to increased trust in the Internet and systems, services and markets that rely upon its secure operation. This road map seeks to build on initial efforts and experiments and to coordinate deployment of the DNSSEC protocol.

This document, itself a work in progress, sets forth the basic goal; the current state of practice, gaps and barriers; a set of sequences and dependencies; and next steps. Its primary audience consists of operators and administrators of the domain name system (DNS), their vendors and suppliers, and their customers.

1.1 Goal

The goal of this effort is to enable DNS all traffic on the Internet to be DNSSEC compliant. In operational terms, this goal translates into the following ideal: Every lookup request requires and receives only DNSSEC-validated answers. It will take a long time to reach a point where all lookup requests are validated. Nonetheless, this is the right goal to put forth.

Achieving this operational goal occurs within the framework of four principal and inter-related tracks: technical, organizational, education and outreach, and public policy. Our primary focus is on the technical issues and process of adoption and the organizational and outreach/ educational activities required to achieve resolution of the technical objectives and activities. Deployment is a fluid process with multiple contingent and dependent relationships requiring broad acceptance in a series of discrete communities as well as enhanced awareness of security issues in among consumers and policy makers. Thus, goals and objectives will necessarily change and monitoring that evolution is itself a programmatic activity.

1.2 Background

The protocol has been under development for more than 10 years. Core ideas were set forth in RFC 2535 [1]. More recent work by Arends, Austein, Massey, Larson, and Rose [2] [3] [4] set forth the DNSSEC specifications, which have been approved by the IESG and are awaiting final publication [5]. Gieben [6] offers a basic description and explanation of key concepts and developments, and Tunnissen [7] provides a

comprehensive guide to important resources including technical documents, public presentations, and pointers to related sites and pilot projects.

Pilot projects have been undertaken in the Netherlands [8] and in Sweden [9], where a signed version of the official .SE zone is currently maintained [10]. The early pilot projects have resulted in hands-on experience with deployment, preparation of training materials, and a fuller understanding of some of the limitations of the specification and clarification of open issues (see, for example, Gieben [11]). Work continues on a global basis. Some current projects and testbeds are summarized in Table 1.

Table 1: Projects and Testbeds Testing the DNSSEC Standard

Name	URL
DNSSEC(.se)	http://dnssec.nic-se.se/
Infrastructure DNSsec et Applications	http://www.idsa.prd.fr/index.php?lang=en
NeuStar Pilot in .US	http://www.potaroo.net/iepg/november2004/DNSSECTrial-in-us.pdf
NIST Advanced Network Technologies Division, Internet Infrastructure Protection	http://www.antd.nist.gov/iipp.shtml
NL Net Labs	http://www.nlnetlabs.nl/dnssec/
	http://www.nlnetlabs.nl/ipv6/publications/v6rootglue.pdf
RIPE NCC – DISI	http://www.ripe.net/disi/
RIPE NCC DNSSEC HOWTO	http://www.ripe.net/projects/disi/dnssec_howto/
Root Server Testbed Network	http://www.rs.net/
VeriSign DLV Registry Pilot	http://www.dlv.verisignlabs.com/
VeriSign.net DNSSEC Pilot	http://www.dnssec-net.verisignlabs.net/

1.3 Organizations engaged in deployment activities

As the work to date shows, DNSSEC deployment engages a range of participants in public, private, for-profit and not-for-profit organizations, some with transnational scope (for example, ICANN, IETF and others). The organizational structure of this coordination effort seeks to mobilize and leverage existing efforts within a coherent framework that enables communication, cross-fertilization of ideas, coordinated approaches to solving common problems, and measurement of progress. Two working groups in the IETF have been critical to the development of the specification: DNSEXT and DNSOPS. The standards work conducted by members of DNSEXT is complete; members of DNSOPS are focused on operational issues. Following kick-off meetings in the spring of 2004, the DNSSEC-Deployment Working Group was organized to provide a forum for those who are actively engaged in DNSSEC deployment activities. Many of the members are also members of IETF working groups allowing for cross-fertilization of ideas and experience. The DNSSEC Deployment Working Group meets by telephone on a weekly basis.

DNSSEC deployment is understood as a set of functions and activities undertaken by a range of organizations to encourage DNSSEC deployment to move in a broad front, engaging entities at all levels. Although some steps are interdependent, others may be undertaken independently by organizations. For purposes of this road map, activities have been divided into four tracks: operations, software, issues and management recognizing that some organizations may engage in activities more than one band. Each of these bands is further subdivided (for example, software is sub-divided into servers, resolvers, operational applications and DNSSEC-aware applications).

This road map offers a framework but remains a work in progress. The following sections lay out key assumptions and terms; the generic process by which DNS functions and the basic changes that DNSSEC introduces; sequencing and dependencies, and the status of development of key pieces as of late summer/fall of 2004.

1.4 Participants in deployment: Roles and responsibilities

Successful deployment of DNSSEC engages five principal classes of participants:

- (i) Zone operators, who make the series of decisions concerning deployment, which affect technical and business practices;
- (ii) Consumers of the services provided through the DNS. These are the end users that use the DNS to locate services such as e-mail, Voip, browsers etc.
- (iii) Providers of services for the DNS. These are the registrars that provide an intermediary function between registry and registrant or suppliers of managed DNS services.
- (iv) Software and equipment suppliers who provide the DNSSEC aware tools for the users mentioned in (i), (ii) and (iii).
- (v) Providers of education and training for those who operate DNSSEC compliant zones. This includes a deeper understanding of practices and procedures as well as manuals that explain how the software works.

Work to date has been primarily focused on the sequence of activities associated with administering zones at the root, registry (gTLD, ccTLD) and registrant (operator) levels with the understanding that each entity will consider its own needs and context carefully. Thus, the first step for both registries and registrants is to undertake a planning analysis. More detail on the road map process is provided in the introduction to Part II, Road Maps.

In subsequent versions of this document, a more complete description will be articulated for the attributes of and requirements for other elements in the process, in particular the role of the registrars and the software (for example, the specialized requirements for

DNSSEC aware browsers). Concerned entities are invited to participate in formulating a strategy to move forward.

1.5 Contributing to development of this document

Much of the work supporting this document is based on the experience of early adopters of DNSSEC. As the work progresses, the Working Group expects the road map to be evolved accordingly. Comments on this document are therefore welcomed and encouraged; please send them to <mailto:dnssec-roadmap@shinkuro.com>.

2.0 Definitions

In this section, several fundamental concepts are described that either are used to characterize how DNSSEC works or will be used to measure progress.

2.1 Signed zones

As set forth in RFCs 1034, 1035 and 1036, DNS is a hierarchical naming system that maps IP addresses to more user-friendly but structured names. DNS has three major components: the domain name space and resource records (RR), which are stored in a tree structure; name servers, which have information about the domain's tree structure; and resolvers, which obtain information from name servers in responses to a query from a client [12].

DNS employs the familiar parent-child metaphor. There is only one root, which is the parent for TLDs. There are currently over 250 top-level domains (TLDs), which fall into one of two primary categories:¹

- ccTLD (country-code TLD). Information may be found at <http://www.iana.org/cctld/cctld-whois.htm>.
- gTLD (generic TLD), further refined into sponsored, which represent a community of interest, and unsponsored (see Table 2).

A TLD is the parent of the second-level domain (or the second-level domain is the child of a TLD); the second level domain is the parent of the third-level domain and so on. As of September 2004, there are over 60 million registered domain names, and several million enterprise-level (or second or third level) domains.

The critical construct is the *signed zone*. As defined in the specification [2], a zone is considered signed when it contains signed Resource Record sets (RRsets), a properly constructed DNSKEY, and Resource Record Signature (RRSIG), Next Secure (NSEC) and (optionally) DS records. A name server that is able to include signatures and other security material along with the requested resource records is called a “security-aware” name server. A “security-aware resolver” uses those signatures to verify the authenticity of records it receives.

¹ A third TLD category is .ARPA, which is only used for infrastructure purposes. (See ICANN, Top Level Domains (gTLDs), 16 December 2003, <http://www.icann.org/tlds/>).

Table 2: gTLD Summary Information

Source: IANA/Generic Top Level Domains, <http://www.iana.org/gtld/gtld.htm>, updated 17 December 2003

Top Level Domain	Operator	For More Information
.AERO	Société Internationale de Télécommunications Aéronautiques (SITA)	http://www.nic.aero/
.BIZ	NeuLevel, Inc.	http://www.neulevel.biz/
.COM	VeriSign Global Registry Services	http://www.verisign.com/products-services/naming-and-directory-services/index.html
.COOP	Dot Cooperation LLC	http://www.cooperative.org/
.EDU	Educause	http://www.educause.edu/edudomain/
.GOV	US General Services Administration	http://www.dotgov.gov/
.INFO	Afilias Limited	http://www.afilias.info/gateway/index.html
.INT	IANA .int Domain Registry	http://www.iana.org/int-dom/
.MIL	US DoD Network Information Center	http://www.nic.mil/
.MUSEUM	Museum Domain Management Association	http://musedoma.museum/
.NAME	Global Name Registry	http://www.gnr.name/
.NET	VeriSign Global Registry Services	http://www.verisign.com/products-services/naming-and-directory-services/index.html
.ORG	Public Interest Registry	http://www.pir.org/
.PRO	RegistryPro	http://www.nic.pro/

2.2 Present and future DNSSEC-aware applications

An important distinction exists between improving current practice and rendering it more security aware and the long term implications as a platform for innovation. DNSSEC protects the transmission of DNS data and therefore addresses a subset of the threats to the Internet infrastructure by ensuring that the zone data received was, indeed, received from the expected source (origin authentication) and that the zone data has not been altered in transmission (data integrity) [6] [13]. It thus counters two types of attacks: spoofing and cache poisoning. In the near term, deployment promises to improve current uses and enhance overall trust in the system.

Potentially more interesting are future applications that will take advantage of the new protocol. Activity in browser development suggests that DNSSEC-aware browsers may be among the earlier new applications. Email is another area in which innovation may be anticipated. For example, the use of the domain and user authentication records, such as SPF (Sender Policy Framework), is strongly benefited by DNSSEC.

3.0 Sequencing and Dependencies

In an effort as complex as adding security the domain name infrastructure, a simple timeline and listing of events and dependencies for the audience of this document would hardly be possible. This section briefly summarizes progress on each major front and then describes the road map approach used for facing forward. These road maps form Part II of the document.

3.1 Progress

We expect deployment to occur along many fronts, that is, roughly simultaneously in zones from the root through enterprises and to engage registries, registrars and registrants. Progress is observed in the following areas:

Design and specification. The protocol is fully specified and as previously noted has been approved by the IESG and is awaiting publication.

Implementation, testing and product development. Considerable implementation and testing work has been undertaken to develop DNSSEC compliant software. BIND 9.3 (<http://www.isc.org/>) is available; earlier versions of BIND with DNSSEC capability are also in use. Also available are NSD (<http://www.nlnetlabs.nl/nsd/>), Nominum Foundation™ Authoritative Name Server and Nominum Foundation™ Caching Name Server (http://www.nominum.com/products_technology.php?id=85). Several prototype systems exist, and tools have been written, for example, Net::DNS::SEC (<http://www.ripe.net/projects/disi/code.html>). A list of available software, utilities and tools is provided by Tunissen [14].

Pilot projects are underway at two major registry operators, VeriSign, Inc. and NeuStar, as previously mentioned (see Table 1). Trials of DNSSEC-aware applications are also expected, depending on the outcomes and experiences of early adopters and the shape and form of the emerging markets. However, it is clear that there are significant gaps in both availability of software products and even in the extent to which the need for such products can be defined. It is expected that early experiments and trials will allow developers to establish clearer product requirements.

More detailed treatment of software is planned for the next version of this document.

Education and training. Training has been underway for several years and continues at major meetings. Major educational and information resources are identified in Table 3.

Committed Operation. A few small experimental zones are known to be operating with DNSSEC.

Table 3: Selected Educational and Training Resources

Title	Agency/URL
axfr.net; private company offering DNS training through multiple venues	axfr.net ; http://www.axfr.net/
DNSSEC Training Course	RIPE Network Coordination Centre http://www.ripe.net/training/dnssec/index.html
DNSSEC Howto	RIPE Network Coordination Center http://www.ripe.net/projects/dns/dnssec_howto/
Secure Domain Name System (DNS) Deployment Guide	Under development; not yet publicly available NIST
Step-By-Step DNS Security Operator Guidance Document, v0.4 (Draft)	Sparta, Inc. http://dnssec-tools.sourceforge.net/docs/step-by-step-guide-draft-v0.4.doc

3.2 Road maps

Part II contains the road maps, which set forth a series of tracks: Operations; Software; Issues; Measurement and Evaluation. These are, in turn, subdivided into bands of activities. For example, the Software track embraces bands of activities grouped by server, resolver, operational applications and DNSSEC-aware applications. The Operations track has been the focus of activity to date with emphasis on the zone. As mentioned in section 1.4, the Operations track will be expanded in the next iteration to provide additional material about registrar activities and administration. The remaining tracks (Software; Issues; Measurement, Evaluation and Progress) remain to be fully fleshed out in cooperation with members of the DNSSEC Deployment Working Group.

The tree diagrams in Part II set forth the high level sequencing and dependencies. An introduction to Part II provides some expansion of the schematic relationships depicted in the diagrams. The four zone view diagrams (root, .arpa, registry and registrants (operators)), in particular, provide templates for deploying DNNSEC and should be consulted to as part of the planning and implementation process and to assist in evaluating progress in broad deployment of the protocol.

4.0 Outstanding Issues

The membership of the DNSSEC Deployment Working Group is actively engaged in deployment activities. Among the tasks that the Working Group has identified is identifying, articulating, and solving outstanding issues. Problem-solving groups are formed as needed to address outstanding issues as these become apparent. At present, five such problem-solving groups have formed: (1) signing the root key, (2) root ops, (3) registries, (4) registrars and (5) software. Unlike the DNSSEC Deployment Working Group, the problem-solving groups are considered impermanent, expected to dissolve as the members achieve solutions to the problems that motivated the team's formation.

Issues that surfaced during work to date have been subjected to a sieve analysis to determine whether work in progress in other venues (for example the IETF) is already addressing the topic and whether topics might be usefully consolidated or re-parsed. A current list of issues identified is summarized in Table 4.

Although this list of issues is included in the road map document as a separate branch, some of the issues in this list have been linked to steps in the deployment process. These interdependencies are indicated by a triangle, which signifies a block or an obstacle.

Table 4: Summary of Issues

Issue	Characterization	Status
1. Root key generation and use	Concerns public-private key pair for the root, including hardware, software, system architecture, procedures, clear allocation of authority and responsibility, and publication and approval of procedures.	Discussions are underway to establish procedures for generating the root key and managing rollover.
2. Timing of signing the root zone and/or management of islands of trust	A DNSSEC signed zone operating without a signed delegation from their parent zone is commonly called an 'island of trust'; this issue deals with questions that arise when zones are signed but the root is not.	Maps to work in progress in DNSOP.
3. Root key rollover and distribution	Procedures for initial distribution of the root public key, periodic rollover of the public key, and its distribution	Under active discussion by the DNSSEC Deployment Working Group
4. Trust anchor key rollover and distribution	Procedures for initial distribution of the trust anchor public key, periodic rollover of the public key, and its distribution; needed in Isolated, Sparse or Dense deployment (below, Table 5) or for some applications.	Maps to work in progress in the IETF Working Group DNSEXT.
5. Zone walking	Refers to authenticated denial of existence, which is accomplished through providing records that indicate the intervals in which no data are available. For some TLDs, the enumerability of zone content is a problem that is prohibitive for DNSSEC deployment.	Maps to work in progress in the IETF Working Group DNSEXT.
6. Last hop	The communication between a stub resolver and a caching name server (both security aware) and the related policies.	Some work has been done on an API for applications to get more detailed DNSSEC information from a response, but that requires a full validating resolver on the same host. No other work has been done on "on-the-wire" solutions other than securing the last hop via transaction security (TSIG, SIG(0)) and trusting the AD bit in the header.
7. End user applications	Addresses end system applications and policies.	Current work has focused on zone and server policy and not the end user policy. Some work has been done on trust anchor management for validators, with a number of proposed solutions.

Issue	Characterization	Status
8. Computational and communication resources required	Considers operational requirements for additional storage, CPU time and communication bandwidth and evaluates the affect these additional requirements may have on adoption and use.	There has been some work measuring the effects, but there is additional work needed. The pieces have to be pulled together and organized.
9. Additional zone operator resource requirements	Additional staff functions required by operation of DNSSEC signed zones Some portions of these additional functions can be effectively done thru automation but this will often vary significantly between various operations.	No specific work is underway to address this issue; some of the automation may be supported by future software tools.
10. Business/usage cases	Analyze, model and quantify the costs and benefits of deployment for different sectors. Different sectors will find different costs and drivers or incentives.	DNSSEC Deployment Working Group plans to gather business cases.

5.0 Measurement, Evaluation and Progress

To describe phases of adoption, the terms empty, isolated, sparse, dense, and complete are defined as follows:

- Empty means that no zones have been signed.
- Isolated means that only a few zones are signed and there is not yet an orderly pattern among the zones which are signed.
- Sparse means there are lots of signed zones, often in coordinated groups, but they're still a minority of the total population. ("Minority" can be measured any of several ways -- number of entries, number of lookups, "importance," etc. This isn't intended to be a precise measure.)
- Dense means most of the zones are signed and it has become the norm.
- Complete means that essentially all zones are signed. Unsigned zones are considered obsolete and inappropriate.

These terms can be used both globally and locally. Globally they describe the broad state of the DNS. These terms also apply locally in the sense that each site has a view of the overall status of DNSSEC deployment, and that view can be used to determine local policies and behavior. These local views may not be the same from all sites. Each site determines whether it views DNSSEC as being deployed only in isolated cases, somewhat sparsely, fairly densely, or ubiquitously. Table 5 sets forth a candidate set of behaviors a site might adopt as DNSSEC deployment increases.

Table 5 summarizes one (but not the only) possible set of behaviors a site might adopt and provides a sense of how a zone's treatment of unsigned responses might change over time as DNSSEC deployment increases. Most importantly, sites control treatment of unsigned responses. There is no global switch that changes each site's behavior in tandem. That said, most sites will find it helpful to know how DNSSEC is progressing and will look for information from authoritative sources.

Table 5: Candidate Local Policies for Treating Unsigned DNS Responses

Local View of Global Deployment Status	Candidate Local Policy for Handling Unsigned Responses
Empty	No signed zones (or not enough to merit notice.)
Isolated	Unsigned responses are expected as the norm. The resolver may have a list of a few zones from which it expects signed responses.
Sparse	Unsigned responses are still expected as the norm although a substantial number of them are, in fact, signed. The resolver has a growing list of SEPs.
Dense	The site expects most zones to be signed will either block unsigned zones or, perhaps, require a list of acceptable unsigned zones.
Complete	The site expects all DNS queries to be signed. An unsigned return response is either treated as an error or treated as an intrusion attempt.

References Cited

- [1] D. Eastlake. RFC 2535. Domain Name System Security Extensions. March 1999. <http://www.ietf.org/rfc/rfc2535.txt?number=2535>
- [2] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. DNS Security Introduction and Requirements. October 10, 2004. <http://www.ietf.org/internet-drafts/draft-ietf-dnssec-dnssec-intro-13.txt>
- [3] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. Protocol Modifications for the DNS Security Extensions. October 10, 2004. <http://www.ietf.org/internet-drafts/draft-ietf-dnssec-protocol-09.txt>
- [4] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. Resource Records for the DNS Security Extensions. October 10, 2004. <http://www.ietf.org/internet-drafts/draft-ietf-dnssec-records-11.txt>
- [5] The status of the Internet drafts is reported in the IETF Draft Tracker (<https://datatracker.ietf.org/public/pidtracker.cgi>) and at the RFC Editor Webpage, <http://www.rfc-editor.org/queue.html>, last updated, 22 October 2004.
- [6] M. Gieben, DNSSEC, The Internet Protocol Journal 7, 2 (June 2004), http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-2/dnssec.html
- [7] DNSSEC – DNS Security Extensions, <http://www.dnssec.org/>
- [8] DNSSEC in NL, 6 January 2004, <http://www.miek.nl/publications/dnssecnl/segreg-report.pdf>.
- [9] DNSSEC(.se), <http://dnssec.nic-se.se/>
- [10] Information about DNSSEC(.se), <http://dnssec.nic-se.se/about.html>
- [11] R. Gieben, DNSSEC in NL, 6 January 2004, <http://www.miek.nl/publications/dnssecnl/segreg-report.pdf>
- [12] P. Mockapetris, RFC 1034: Domain Names – Concepts and Facilities , November 1987, <http://www.ietf.org/rfc/rfc1034.txt?number=1034>.
- [13] D. Atkins, R. Austein, Threat Analysis of the Domain Name System (DNS), RFC 3833, <http://www.ietf.org/rfc/rfc3833.txt?number=3833>.
- [14] DNSSEC – DNS Security Extensions: “DNSEC Software, Tools, Utilities”. January 1, 2005. <http://www.dnssec.net/software.php>

Acknowledgements

This document has been prepared with support from the U.S. Department of Homeland Security under Contract No. FA 8750-04-C-0269. It has been written by Allison Mankin, Amy Friedlander and Steve Crocker but reflects substantial extensive collaboration and consultation with the technical community and contributions by members of the DNSSEC Working Group and the staffs of the U.S. National Institute of Standards and Sparta, Inc.

Part II: Road Maps

Introduction to the Diagrams

The following diagrams represent progressively more detailed views of the Road Map process, beginning with the overall view, encompassing the four tracks as set forth earlier in this document. In keeping with the focus of the work to date, attention is directed to activities within the zone. The zone diagrams can be used in different ways. People actively engaged in deployment may wish to use them as a checklist. The diagrams can also be used to chart progress.

Each branch of the zone – root, .ARPA, registry and registrants (operators) – follows essentially the same four steps: sign, serve, distribute public key, and register although there are significant variations at each level.

- Sign. Creating the signed zone for the level shown, prior to publication.
- Serve. Publishing the signed zone whether or not child zones have been incorporated.
- Distribute Public Key. Making universally available the public key for that zone. This step is required for root; zones below root require it if they do not have a complete signed tree above them up to root. SEP (Secure Entry Point) is the term for the top of an incomplete DNSSEC tree; it applies only below root. The desired goal is the child's placement of public key for signing and publication by parent.
- Register. Accepting and publishing the records of signed child zones.

Although these steps appear separately, this does not imply that they are necessarily independent. They may be tightly integrated (e.g., even in the same piece of software) or they may occur in wholly separate administrations (this is indicated in the diagrams by identifying responsible entities in parentheses.).

It is assumed that zone operators will identify and obtain hardware and DNSSEC compliant software and will undertake basic testing. In the templates, the diagrams call out *community-visible* testing. Specifically, testing is itemized only at the step just prior to the introduction of the signed zone to the infrastructure.

A few additional notes for specific branches follow. These notes explain specific lines in individual diagrams; the line or phrase to which the note applies is indicated in quotation marks.

Root

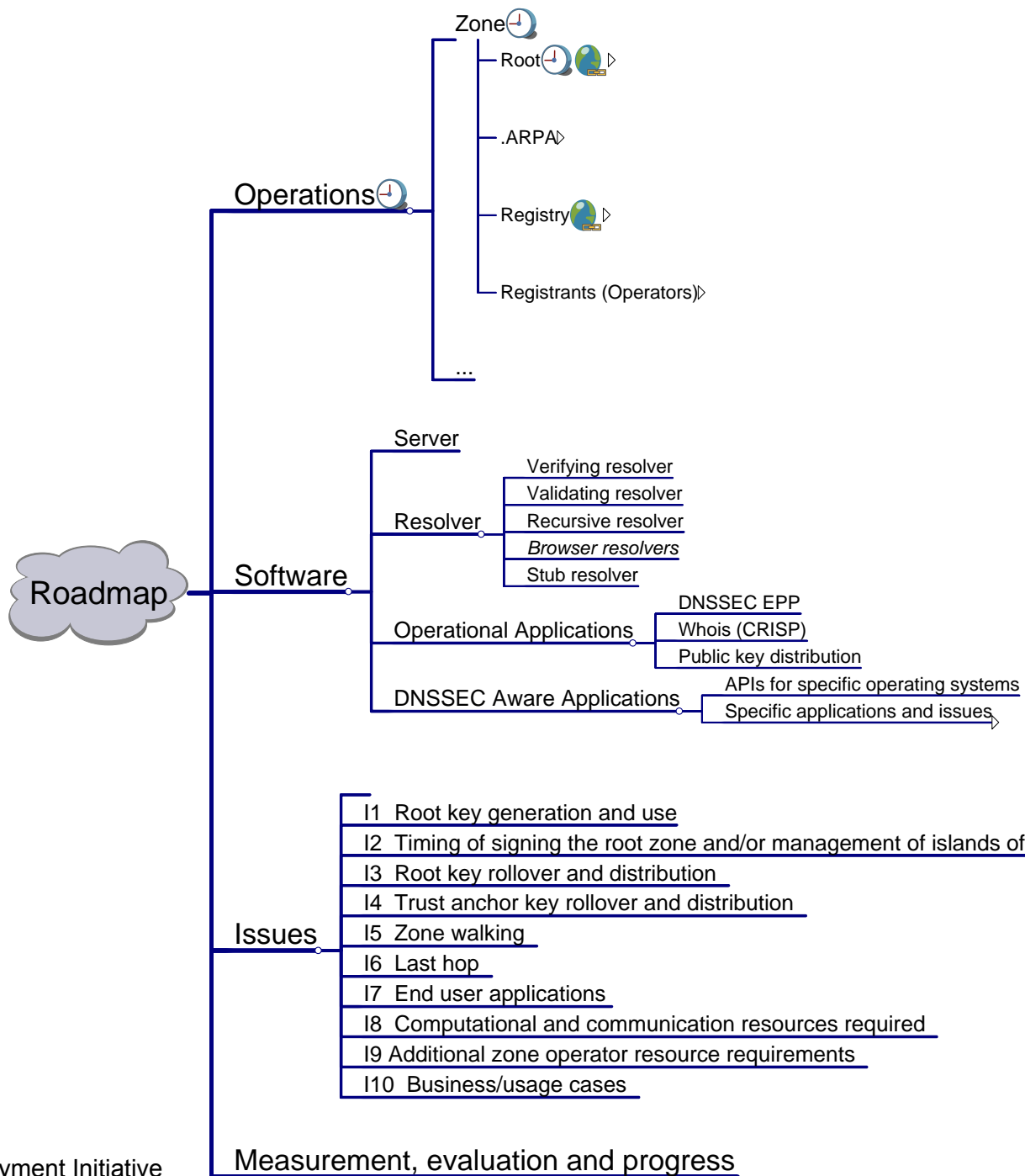
- “All [13 root servers] get DNSSEC compliant software”. Once the root is signed, all 13 of the root servers must be ready to serve the root zone simultaneously. Since the individual root servers vary in the software and other configurations used, this step of all of them being ready with DNSSEC-compliant software has been called out.
- “.ARPA”. This is a special zone which is part of the infrastructure. Once procedures are in place, this subordinate zone will be signed and published before the process is opened up for the other TLDs.

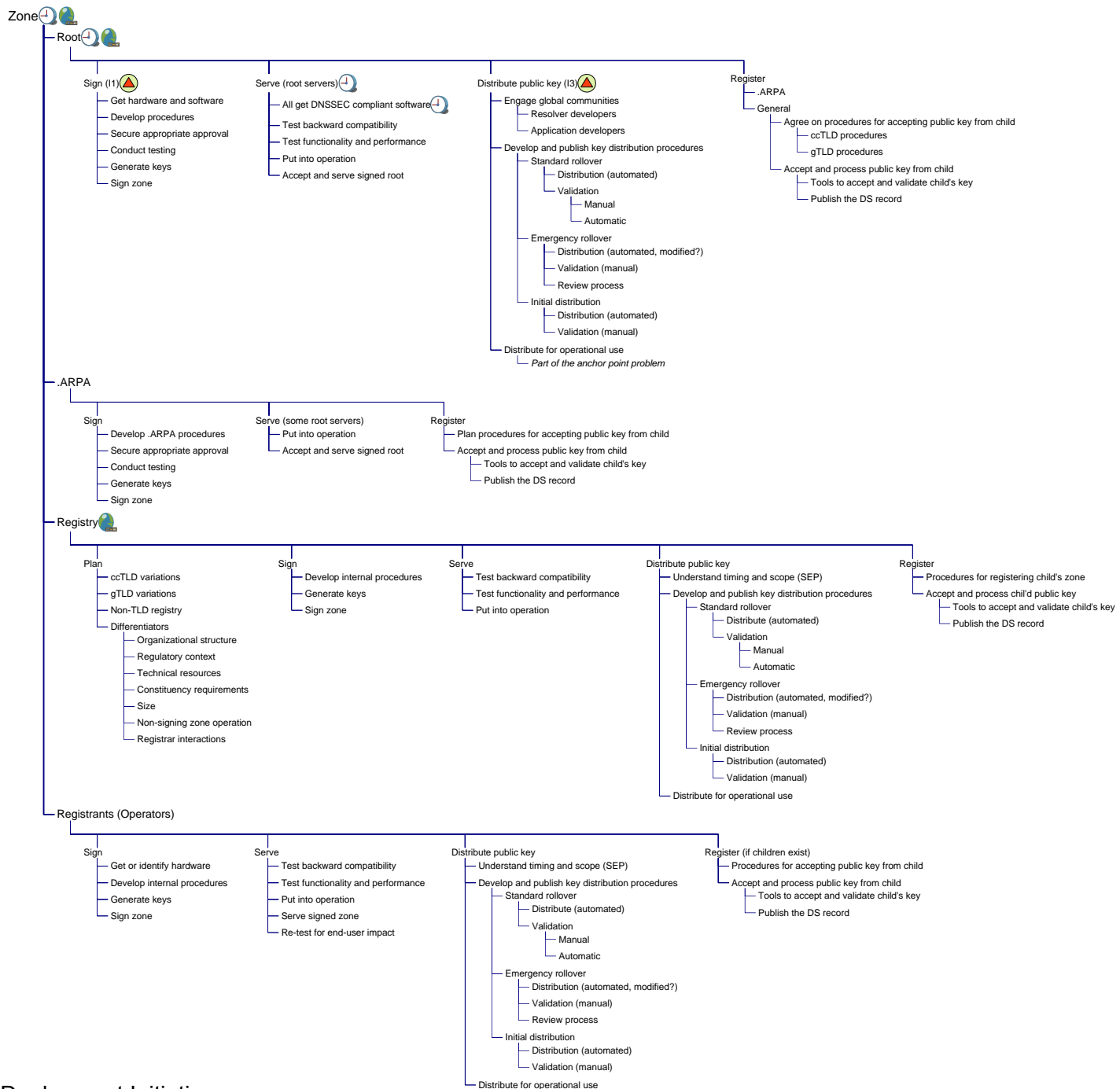
Registry

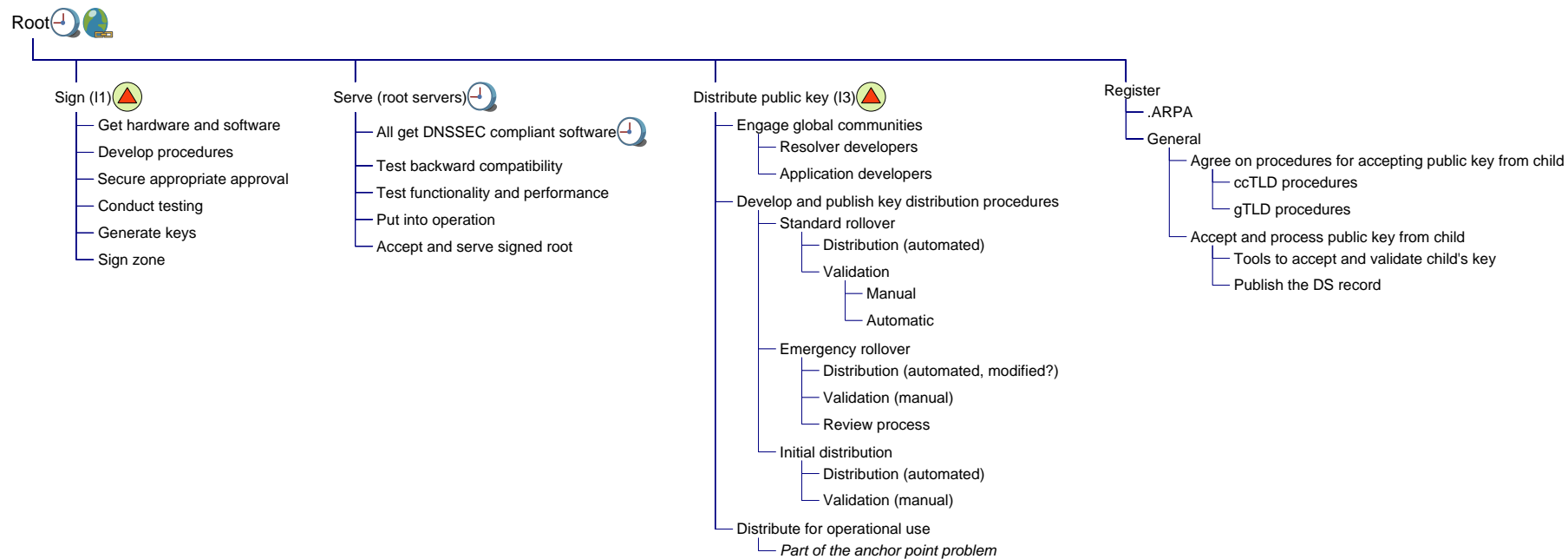
- “Plan”. Registries have many different situations, starting with ccTLDs and gTLDs, which vary among themselves. The planning step and list of differentiators call attention to many of the criteria by which registries may be differentiated and the considerations that may affect their immediate circumstances. These considerations should apply across the template as they may affect execution of the individual steps.
- “Registrar interactions”. One set of differentiators concern registrar relationships. Under the Register step, the expansion of the zone to include children often includes interactions with registrars, so the language in this branch is different from the others. This version of the road map has no further detail about registrar interactions.

Registrants (Operators)

- “Get or identify hardware”. Smaller operators may be able to add DNSSEC to the hardware already in operation so this step is called out.
- “Re-test for end-user impact”. This class of zone operators may be maintaining the zone files containing large sites’ host information, and errors or problems may interact in a more direct or complex way for end-users than in other zone environments.







.ARPA 

Sign


- Develop .ARPA procedures
- Secure appropriate approval
- Conduct testing
- Generate keys
- Sign zone

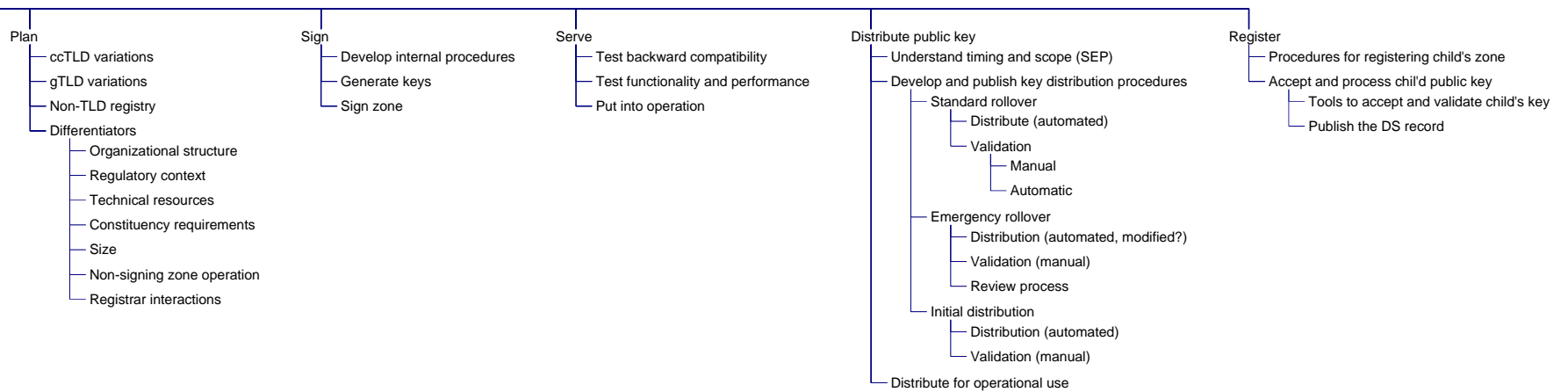
Serve (some root servers)

- Put into operation
- Accept and serve signed root

Register

- Plan procedures for accepting public key from child
- Accept and process public key from child
 - Tools to accept and validate child's key
 - Publish the DS record

Registry 



Registrants (Operators) 