

# Survey of Available Tools for DNSSEC

Russ Mundy  
SPARTA, Inc.  
25 June 2008

# Available Resources

- Various categories of resources are available
  - Tools for zone data administration
  - Tools for secure delegation registration
  - Tools for supporting operations at the validating systems including DNSSEC-capable applications
  - Developer resources
  - Operator guidance documentation
- Some of the available tools are catalogued at <http://www.dnssec-deployment.org/tracker>
- Existing tools have broad coverage
- Some gaps remain (currently being addressed within the community)



# Resources for Zone Administration

# Name Servers

BIND	Authoritative, validating, recursive, and caching open source name server implementation	ISC	<a href="http://www.isc.org">www.isc.org</a>
NSD	Authoritative only, open source name server	NLNet Labs	<a href="http://www.nlnetlabs.nl/nsd">http://www.nlnetlabs.nl/nsd</a>
UNBOUND	Validating, recursive and caching open source name server	NLNet Labs, Verisign, Nominet, Kirei	<a href="http://unbound.net/">http://unbound.net/</a>
ANS	Authoritative name server	Nominum, Inc.	<a href="http://www.nominum.com">www.nominum.com</a>
CNS	Recursive name server	Nominum, Inc	<a href="http://www.nominum.com">www.nominum.com</a>



# Key Generation and Zone Signing

dnssec-keygen, dnssec-signzone	Standard tools provided with the BIND distribution	ISC	<a href="http://www.isc.org">http://www.isc.org</a>
nom_keytool, ans_signer	Standard tools provided with the ANS distribution	Nominum	<a href="http://www.nominum.com">www.nominum.com</a>
jdnssec-keygen, jdnssec-signzone	Tools from the jdnssec-tools suite	Verisign Labs	<a href="http://www.verisignlabs.com/dnssec-tools/">http://www.verisignlabs.com/dnssec-tools/</a>
ldns-keygen, ldns-signzone	Tools from the ldns tool suite	NLNet Labs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
pdnssec-keygen, pdnssec-signzone,	Tools from the DNSSEC perltools distribution	Roy Arends	<a href="http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/">http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/</a>
zonesigner	Wrapper around BIND tools, available in the dnssec-tools suite	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Zonesigner">http://www.dnssec-tools.org/wiki/index.php/Zonesigner</a>
dnssec-zkt and dnssec-signer -	Wrapper around BIND tools	HZNET	<a href="http://www.hznet.de/dns/zkt/">http://www.hznet.de/dns/zkt/</a>
ldns-zsplit and ldns-zcat	Tool from the ldns package for enabling parallel signing a large zone	NLNetLabs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
maintkeydb, dnssigner	Tools from the DNSSEC Key Management Tools suite	RIPE NCC	<a href="https://www.ripe.net/projects/dnssec_maint_tool/">https://www.ripe.net/projects/dnssec_maint_tool/</a>

# Key Rollover

Rollerd and rollctl	Tool from the dnssec-tools package for managing different phases of ZSK and KSK rollover	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Rollerd">http://www.dnssec-tools.org/wiki/index.php/Rollerd</a>
Maintkeydb	Command line interface to a database containing DNSSEC Keys	RIPE NCC	<a href="https://www.ripe.net/projects/disi/dnssec_maint_tool/">https://www.ripe.net/projects/disi/dnssec_maint_tool/</a>

# Hardware Interface

DNSSEC Smartcard Utility	Supports operations for storing keys to Any PKCS#15 smartcard supported by OpenSC and exporting them as DNSSEC records	.SE	<a href="http://opensource.iis.se/trac/dnssec/browser/pkcs15-dnssec">http://opensource.iis.se/trac/dnssec/browser/pkcs15-dnssec</a>
pkcs11HSMtools	Modifications to BIND for native PKCS-11 HSM support	IANA	<a href="http://www.xtcn.com/~lamb/pkcs11HSMtools.tar.gz">http://www.xtcn.com/~lamb/pkcs11HSMtools.tar.gz</a>
Software for interfacing with crypto hardware	EVP Perl Implementation	Nominet	<a href="http://www.nominet.com">www.nominet.com</a>
DNSSEC Appliance	A secured appliance that can be used as an automation engine for DNSSEC management tasks	Secure64	<a href="http://www.secure64.com/products.shtml">http://www.secure64.com/products.shtml</a>
dnsX	An appliance containing a secure signer, caching resolver and authoritative name server	Xelerance	<a href="http://www.xelerance.com/">http://www.xelerance.com/</a>

# Zone Troubleshooting

SZIT monitor extension	Tests the zone contents against best common practices and overall security	NIST	<a href="http://snad.ncsl.nist.gov/dnssec/">http://snad.ncsl.nist.gov/dnssec/</a>
donuts and donutsd	A dnslint like application available in the dnssec-tools site, for analyzing zone files.	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Donuts">http://www.dnssec-tools.org/wiki/index.php/Donuts</a>
Mapper	Tool in the dnssec-tools suite that maps DNS realms, color coding the results to allow for easy visual interpretation of the results	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Mapper">http://www.dnssec-tools.org/wiki/index.php/Mapper</a>
jdnssec-verifyzone	Verifies all of the signatures in a zone for cryptographic validity	Verisign Labs	<a href="http://www.verisignlabs.com/dnssec-tools/">http://www.verisignlabs.com/dnssec-tools/</a>
named-checkzone	Standard tool provided with the BIND distribution	ISC, BIND	<a href="http://www.isc.org">www.isc.org</a>





# Resources for Creating Secure Delegations

# DS Record Creation

dnssec-dstool	simple tool for generating DS (or DLV) records from DNSKEY records	Verisign Labs	<a href="http://www.verisignlabs.com/dnssec-tools/">http://www.verisignlabs.com/dnssec-tools/</a>
ldns-key2dns	DNSKEY to DS conversion	NLNet Labs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
Key2ds, Net::DNS::Sec	DNSKEY to DS conversion	Olaf Kolkman	<a href="http://www.net-dns.org/">http://www.net-dns.org/</a>

# Update to Parent

Regsoft	Front-end for updating contents of a registry	Shinkuro, Inc	
CADR	registrar software that can move keys from sub-zones to parent zones	Afilias, Shinkuro, SPARTA, EP.net	<a href="http://cadr.rs.net/">http://cadr.rs.net/</a>
libepp-nicbr	library that partially implements the Extensible Provisioning Protocol (EPP), as described in the Internet Drafts RFC3730bis to RFC3734bis and RFC3735	NIC.br	<a href="http://registro.br/epp/index-EN.html">http://registro.br/epp/index-EN.html</a>



# Resources for Validating Systems

# Fetching SEP Key Information

ISC DLV registry	Trust Anchor Repository constructed through explicit zone owner registration	ISC	<a href="https://secure.isc.org/index.pl?ops/dlv/">https://secure.isc.org/index.pl?ops/dlv/</a>
Secspider	Trust Anchor Repository populated by a crawler program	UCLA, Colorado State	<a href="http://secspider.cs.ucla.edu/">http://secspider.cs.ucla.edu/</a>
IKS Jena Survey	Trust Anchor Repository populated by a crawler program	IKS Jena	<a href="http://www.iks-jena.de/leistungen/dnssec.php">http://www.iks-jena.de/leistungen/dnssec.php</a>
IANA TAR	(Currently) demo Trust Anchor Repository for SEP keys for TLDs	IANA	<a href="https://ns.iana.org/dnssec/status.html">https://ns.iana.org/dnssec/status.html</a>
ldns-keyfetcher	queries and retrieves DNSKEYs for a given domain	NLNet Labs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
getdnskeys	Tool in the dnssec-tools suite for fetching, comparing and remembering a list of DNSKEYs from DNS zones	SPARTA, Inc	<a href="http://www.dnssec-tools.org">www.dnssec-tools.org</a>



# Automated TA Rollover

trustman	Implementation of RFC 5011 for automated rollover of trust anchors in validating resolvers. Tool available in the dnssec-tools distribution	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Trustman">http://www.dnssec-tools.org/wiki/index.php/Trustman</a>
----------	---	-------------	---

# Troubleshooting

dig	Standard tool provided with the BIND software	ISC	<a href="http://www.isc.org">www.isc.org</a>
drill	Debugging/query tool for DNSSEC, similar to dig	NLNet Labs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
validate	A tool that helps determine the validation status for a DNS record and the reasons for validation failure if any	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Validate">http://www.dnssec-tools.org/wiki/index.php/Validate</a>
dnspktflow	This tool, when combined with tethereal and graphviz, can trace tcpdump/tethereal network packet captures to visually diagram dns packet flows	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Dnspktflow">http://www.dnssec-tools.org/wiki/index.php/Dnspktflow</a>
Traffic Monitoring Tool	Tool to capture and analyze DNS traffic to and from a name server	NIST	<a href="http://snad.ncsl.nist.gov/dnssec/">http://snad.ncsl.nist.gov/dnssec/</a>
dnscap	network capture utility designed specifically for DNS traffic	OARCI	<a href="http://public.oarci.net/tools/dnscap">http://public.oarci.net/tools/dnscap</a>
Logwatch	Configuration plugin to have logwatch perform DNSSEC parsing of system logging messages from running BIND name server	Plugin provided by SPARTA, Inc available in the logwatch distribution	<a href="http://www2.logwatch.org:81/">http://www2.logwatch.org:81/</a>
dnstdump	Perl script that captures and displays DNS packets seen on the network	The Measurement Factory	<a href="http://dns.measurement-factory.com/tools/dnstdump/">http://dns.measurement-factory.com/tools/dnstdump/</a>



# DNSSEC Capable Applications



Firefox	patch that enables DNSSEC checking of DNS lookups done with Firefox	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Firefox">http://www.dnssec-tools.org/wiki/index.php/Firefox</a>
Thunderbird	patch that enables DNSSEC validation in the Thunderbird mail app	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Thunderbird">http://www.dnssec-tools.org/wiki/index.php/Thunderbird</a>
SSH	patch that contains support for local DNSSEC validation for all DNS lookups	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/SSH">http://www.dnssec-tools.org/wiki/index.php/SSH</a>
Sendmail	patch for adding DNSSEC validation support during lookups	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Sendmail">http://www.dnssec-tools.org/wiki/index.php/Sendmail</a>
Postfix	patch for adding DNSSEC validation support during lookups	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Postfix">http://www.dnssec-tools.org/wiki/index.php/Postfix</a>
libsF2	patch for adding DNSSEC validation support during lookups and adding a new field in the mail header based on the results of the checks	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/LibSPF">http://www.dnssec-tools.org/wiki/index.php/LibSPF</a>
wget	patch to enable DNSSEC validation in wget	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Wget">http://www.dnssec-tools.org/wiki/index.php/Wget</a>
ncftp	patch to enable DNSSEC validation during lookups	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Ncftp">http://www.dnssec-tools.org/wiki/index.php/Ncftp</a>
proftpd	patch to enable DNSSEC validation during lookups	SPARTA, Inc	<a href="http://www.dnssec-tools.org/wiki/index.php/Proftpd">http://www.dnssec-tools.org/wiki/index.php/Proftpd</a>





# Developer Resources

# Validation Libraries

libval	A C library that provides interfaces for name lookup with DNSSEC validation support.	SPARTA, Inc	<a href="http://www.dnssec-tools.org/docs/tool-description/libval.html">http://www.dnssec-tools.org/docs/tool-description/libval.html</a>
libval_shim	LD_PRELOAD-based approach for transparently adding DNSSEC capability to existing applications	SPARTA, Inc	<a href="http://www.dnssec-tools.org/docs/tool-description/libval_shim.html">http://www.dnssec-tools.org/docs/tool-description/libval_shim.html</a>
ldns library	A C library that provides validation capability	NLNet Labs	<a href="http://www.nlnetlabs.nl/ldns/">http://www.nlnetlabs.nl/ldns/</a>
libunbound	A C library that can be linked against applications to provide validation capability	NLNet Labs, Verisign, Nominet, Kirei	<a href="http://unbound.net/">http://unbound.net/</a>

# Perl SDKs

Net::DNS::SEC	Extension to Net::DNS with DNSSEC functionality	RIPE NCC	<a href="http://www.net-dns.org/">http://www.net-dns.org/</a>
Net::DNS::SEC::Tools	Tools and modules that provide zone signing and key management configuration utilities.	SPARTA Inc	<a href="http://www.dnssec-tools.org/">http://www.dnssec-tools.org/</a>
Net::DNS::ZoneFile::Fast	provides the ability to parse zone files that BIND8 and BIND9 use, fast.	Anton Berezin and SPARTA, Inc	<a href="http://search.cpan.org/dist/Net-DNS-ZoneFile-Fast/Fast.pm">http://search.cpan.org/dist/Net-DNS-ZoneFile-Fast/Fast.pm</a>



# Validator API

DNSSEC Validator API	Proposed API between applications and security aware validating stub resolvers	SPARTA, Inc	<a href="http://tools.ietf.org/id/draft-hayatnagarkar-dnsext-validator-api-06.txt">http://tools.ietf.org/id/draft-hayatnagarkar-dnsext-validator-api-06.txt</a>
libunbound API	API provided by the libunbound library	NLNet Labs, Verisign, Nominet, Kirei	<a href="http://www.unbound.net/documentation/index.html">http://www.unbound.net/documentation/index.html</a>



# Testing Resources

maketestzone	useful for generating test data which DNSSEC aware software can be tested against	SPARTA, Inc	<a href="http://www.dnssec-tools.org">www.dnssec-tools.org</a>
Querysim	A DNS traffic replay tool	NIST	<a href="http://snad.ncsl.nist.gov/dnssec/">http://snad.ncsl.nist.gov/dnssec/</a>
Packet Server	A tool that helps crafting packets with various settings to test the behavior of validating resolvers	Roy Arends	<a href="http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/">http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/</a>



# Deployment Aids



# Operator Guidance Documentation



NIST Special Publication 800-81	Recommendations of the National Institute of Science and Technology, Deployment Guide	NIST	<a href="http://csrc.nist.gov/publications/nistpubs/">http://csrc.nist.gov/publications/nistpubs/</a>
RFC 4641	DNSSEC Operational Practices	IETF	<a href="http://www.ietf.org/rfc/rfc4641.txt">http://www.ietf.org/rfc/rfc4641.txt</a>
Step-by-Step guides	Guides for signed zone operation	SPARTA, Inc	<a href="http://www.dnssec-tools.org/resources/documentation.html">http://www.dnssec-tools.org/resources/documentation.html</a>
DNSSEC Howto	A tutorial in disguise	NLNet Labs	<a href="http://www.nlnetlabs.nl/dnssec/howto/">http://www.nlnetlabs.nl/dnssec/howto/</a>