Andreas Nilsson
Certezza AB
Stockholm 2010-05-31

A Review of Administrative Tools for DNSSEC – Spring 2010

Kornhamnstorg 61, 2 tr
SE-111 27 Stockholm
Sweden

Telefon: +46 (0)8 791 92 00
Telefon: +46 (0)8 791 95 00

www.certezza.net

Table of Contents

Foreword

This review was performed on commission from .SE (The Internet Infrastructure Foundation), whose influence ends there and Certezza's independence is thereby intact.

The goal of the review is to show the current state of administrative tools for DNSSEC and thereby help customers in finding suitable DNS management products and to encourage providers to continue to refine their products. During the fall of 2009 a first study was conducted. We now follow up on the previous review having added three new vendors and using an updated set of review points based on current DNSSEC developments. The purpose of this product review is to facilitate the deployment of DNSSEC by defining a de facto standard for DNSSEC management tools and providing an assessment of the tools currently available.

Certezza is an independent information and IT security company offering solutions for secure IT infrastructures. Certezza has extensive experience in carrying out analyses, reviews and preliminary studies, combining a structural approach with expertise in the sector of information and IT security.

Abstract

This report is an updated summary of the functionality of some leading DNSSEC management tools. The main focus of the original review was on pure DNSSEC functionality such as signing and key management functionality but this time overall usability has also been considered. Three new products and their corresponding vendors have been included in the review. An important part of the work has been to define an updated set of user review points. The review points now cover most necessary DNSSEC functionality and are fairly generally put in order to be useful for other similar studies.

Generally the reviewed products provide satisfactory DNSSEC functionality and there is a healthy diversion in system packaging, platform support and administration interfaces. Our impression during the previous study was that basic DNSSEC functionality was well-functioning but there were some areas such as NSEC3, usability, key integrity and key migration that needed improvement. Now several of the products have matured and we do not believe that lack of adequate management tools is the main challenge for DNSSEC deployment today.

DNSSEC is a dynamic and emerging technology and so are the management tools. The products changes continuously and it will be interesting to follow the development especially with regards to interoperability, performance and ease of use in larger deployment scenarios. It will be especially interesting to see how the products will cope with the increased DNSSEC use following the signing of the root and continuous signing of top level domains.

1 Introduction

During the fall of 2009 Certezza conducted a first review of administrative tools for DNSSEC [1]. Since the first study was initiated a lot has changed in the DNSSEC area. The root zone is in the process of being signed which will remove one of the major obstacles for DNSSEC deployment. Many of the larger unsigned TLDs (top level domains) now have DNSSEC signing on the road map. The crucial challenge right now is to get momentum in signing second- and third-level DNS zones.

In the study a number of areas that would be interesting to follow up in a future study were identified. The areas included NSEC3 support, usability, key integrity and key migration functionality. Following the rapid development in the area the last six months we now present an updated review including re-testing of previous set of review points, increased focus on usability and inclusion of three new vendors.

1.1 Technical background

DNSSEC is an abbreviation for DNS Security Extensions. DNSSEC allows the recipient to validate the integrity of a DNS answer [2]. The idea is to provide a more secure way to resolve internet addresses to protect against DNS attacks such as cache poisoning [3]. A dependable DNS infrastructure is important for all Internet users. Two examples of use case scenarios where DNSSEC will come in useful are internet banking or communicating new passwords over e-mail.

The integrity of the DNS answers is protected by cryptographically signing the zone's DNS Resource Records (RR) constructing Resource Record Signatures (RRSIG). The public key is then provided to the resolver or application that validates the integrity of the received RR. The integrity is provided by a chain of trust starting with the public key of a TA (Trust Anchor). The TA could be the root of the DNS system or an isolated root published in a DLV (DNSSEC Look-aside Validation) record.

Two pairs of cryptographic keys are used to sign and validate the DNS records in a zone, the ZSK (Zone Signing Key) and the KSK (Key Signing Key). The zone itself is signed by the ZSK. The ZSK is signed by the KSK. The hash of the KSK is published in the parent zone as a DS (Delegation Signer) record. The public key of a parent zone is used to validate the DS record for the child's KSK. The validation process starts at the TA whose public key is obtained independent of the DNSSEC hierarchy, typically directly via the operating system.

1.2 Deployment status and challenges

One of the problems with DNSSEC is that it makes the administration of DNS more complicated. However, this can be partly mitigated by using a management tool which automatically handles the DNSSEC signing and key management. One infrastructural obstacle has been that the root zone and major TLDs has remained unsigned. This is however rapidly changing and the root zone is now in the process of being signed with scheduled finish in the end of June 2010.

In order to achieve a rapid deployment of DNSSEC, it is crucial that the DNS name server operators have access to simple and functional DNSSEC administration tools. The supply of such tools is increasing, but the knowledge among the potential customers is still relatively low. Looking back DNS initially struggled to overcome the simple use of host files. In the same fashion the advantages of DNSSEC will most certainly play out in its favour in the long run.

1.3 Purpose

The primary aim of the initial review was to assist the DNS Name Server operators in finding suitable tools for their DNSSEC administration and thereby facilitate the deployment of DNSSEC. The second goal was to establish a basic set of management features required for practical DNSSEC deployment in order to encourage providers to refine their product. This still holds true with an additional focus on overall usability now that the basic signing functionality has been verified to function properly.

The primary recipients of the project results are DNS name server operators and DNSSEC management tool providers.

1.4 Scope

The scope of the study is limited to management tools used for DNSSEC signing and key management. Equipment and appliances which only provides validation has been left out. It should be noted that many of the evaluated products provide validation functionality even though it was not formally tested in this study.

Performance tests of zone signing have also been left out for two reasons. Firstly due to the fact that several of the reviewed tools only were available as virtual machines. Secondly even with available hardware it is hard to find a fair way of comparing performance. Many of the products in this review are software modules whose performance would depend heavily on the hardware on which they run.

2 Review method

2.1 Product selection

The products and corresponding vendors were chosen based on two main criteria; high deployment rate at customer sites and/or a good reputation as a reliable DNSSEC management tool. After the first review was published we received input about the product selection from vendors and the DNSSEC community. This input together with recent developments have made us include three new management products/vendors, see section 3.2.

2.2 Test setup

The tests were performed in an isolated test lab laid out according to the following figures. The evaluated modules and appliances are marked in bold.

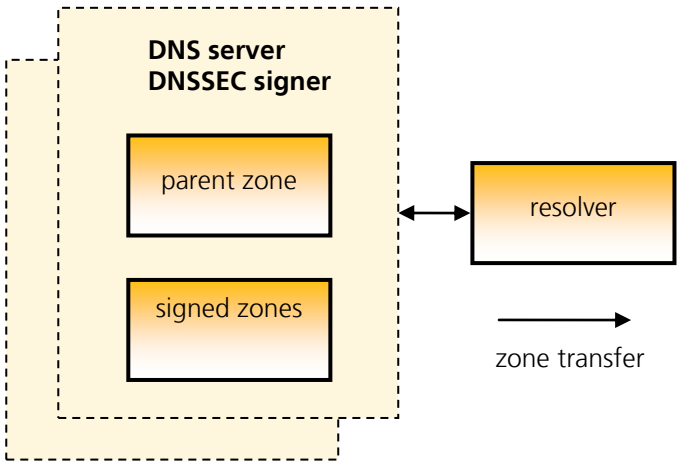

Figure 2.1 Test setup for the IPAM systems and DNS servers.

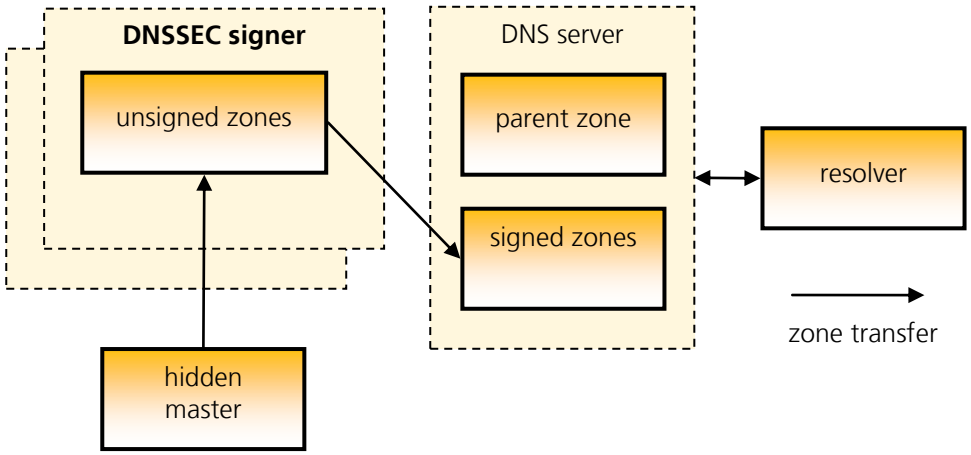

Figure 2.2 Test setup for DNSSEC signers used as a "signer-in-the-middle".

Using these setups we created several signed zones, observe them during the key lifespan and verified SNMP communication between the tested tools and monitoring software. We also experimented with communication between child and parent zone when applicable.

It should be noted that testing the pure DNSSEC signers naturally required third party name servers to handle the incoming and outgoing zone transfers used to communicate the unsigned and signed zones.

2.3 Test execution

The review of the products was performed in Certezza's office according to the test review points listed in chapter 4. Each of the review points was evaluated separately according to the laid out test plan. The claimed functionality for each of the tested products was verified and documented. The results were then sent to the vendors for referral and their comments have been included in the result matrices.

Note that all review points were completely re-tested so that all results are up to date with the latest versions of the reviewed products.

3 Examined products

3.1 Classification

It is important to mention that even though the products perform the same basic functionality (generating keys and signing zone files) they operate in different contexts. Firstly there is a distinction between appliances and software modules. Secondly we have chosen to distinguish between three categories of system packaging; pure DNSSEC signers, DNS servers and complete IPAM systems (basically DNS and DHCP glued together).

A pure DNSSEC signer operates as a "signer-in-the-middle" and sits between a hidden master and the ordinary name server. The zone is imported from the hidden master, signed and then the external name server is notified that the zone is ready to be transferred. IPAM systems and DNS servers integrate this process since they handle the zone files directly.

3.2 Selection

The products were chosen according to the selection criteria in section 2.1 and the products listed in the table below were examined. Input on the first review from vendors and the DNSSEC community together with recent product developments made us include three new management products/vendors, namely ISC BIND, OpenDNSSEC and Xelerance DNSX Secure Signer.

Vendor	Product version reviewed
BlueCat Networks	Proteus 3.0.2.19
Infoblox	Infoblox 5.0
InfoWeapons	SolidDNS 4.0
ISC	BIND 9.7
Microsoft	Windows 2008 R2 (6.1)
OpenDNSSEC	OpenDNSSEC 1.1
Secure64 Software	DNS Signer 3.1
Xelerance	DNSX Secure Signer 1.1

4 Review results

This section lists the test reviews points and the corresponding vendor support. Direct findings by the test team are provided in the middle column and vendor comments are included in the right column.

The original review point selection was based on previous work by Joakim Åhlund and Alexander Lindqvist [4]. As part of this test round the review point set was updated and re-structured based on input from the DNSSEC community and relevant events such as the planned signing of the root zone. For instance a new section about product classification has been added and no testing involving DLV (isolated trust anchors) has been conducted since it is hardly relevant anymore.

We are not recommending one vendor (or setup type for that matter) over another but simply trying to evaluate how well the respective products implement DNSSEC functionality.

4.1 Product classification (A)

Comment: To correctly assess the functionality of the different products it is useful to know their scope and intended environment.

A1.1 – Type of product; hardware appliance or software module?

Product	Findings by the test team	Vendor comments
BlueCat	Hardware appliance	BlueCat provides both hardware and virtual versions of our IPAM and DNS appliances.
Infoblox	Hardware appliance	Purpose built hardware with locked down OS.
InfoWeapons	Hardware appliance	SolidDNS is also available as a Sofpliance (ISO) which can be installed on most standard server hardware platforms, or run as a virtual machine.
ISC (BIND)	Software module (open source)	
Microsoft	Software extension to Microsoft DNS server.	
OpenDNSSEC	Software module (open source)	BSD license
Secure64	Hardware appliance	Our software runs only on the HP Integrity platform.
Xelerance	Hardware appliance	

A1.2 – System packaging; together with an IPAM system, a DNS Server or as a pure DNS Signer?

Product	Findings by the test team	Vendor comments
BlueCat	IPAM system	
Infoblox	IPAM system	
InfoWeapons	DNS server	SolidDNS can be integrated with a third party IPAM system via API.
ISC (BIND)	DNS Server	
Microsoft	DNS Server	
OpenDNSSEC	DNS signer, depends on a third party name server for outgoing zone transfers.	You need a name server in order to load and serve the signed zone file.
Secure64	DNS Signer with accompanying DNS Server (Secure 64 DNS Authority)	
Xelerance	DNS signer	

A1.3 – Supported administration interfaces; GUI, CLI, API

Product	Findings by the test team	Vendor comments
BlueCat	Web GUI, CLI	
Infoblox	Web GUI, Serial CLI, Perl API	
InfoWeapons	Web GUI, CLI, serial console	SolidDNS also has an API for third party systems integration.
ISC (BIND)	CLI, text-based configuration.	
Microsoft	CLI	
OpenDNSSEC	CLI, text-based configuration.	
Secure64	SSH	
Xelerance	Web GUI, SSH	and JSON interface

4.2 Policy management (B)

B1 - Is it possible to select different life spans for different zones and zone records?

Comment: An organisation with domains having different security requirements needs to be able to set different keys and signing policies for zones and zone records depending on the security level.

Product	Findings by the test team	Vendor comments
BlueCat	Different life spans for zones but not for different records.	
Infoblox	Different life spans for zones but not for different records.	
InfoWeapons	Different life spans for zones but not for different records.	
ISC (BIND)	Different life spans for zones and for different records (via partial signing).	
Microsoft	Different life spans for zones but not for different records.*	
OpenDNSSEC	Different life spans for zones but not for different records.	
Secure64	Different life spans for zones but not for different records.	
Xelerance	Different life spans for zones but not for different records.	

*No policy management, the entire key generation process is performed manually.

B2 – Key lifespan

Comment: Can different life spans be selected for the KSK and ZSK?

Product	Findings by the test team	Vendor comments
BlueCat	Yes	
Infoblox	Yes	
InfoWeapons	Yes	
ISC (BIND)	Yes	
Microsoft	Yes	
OpenDNSSEC	Yes	
Secure64	Yes	
Xelerance	Yes	

4.3 Communication and system (C)

4.3.1 General DNS (C1)

C1.1 - Does the DNSSEC implementation support RFC5011?

Comment: The standard protocol used to transfer the public KSK to resolvers is called RFC5011 [5]. If RFC5011 is not supported the public KSK must be distributed manually. This is only a minor issue if the root is signed, but might cause troubles if the TLD is not signed.

Product	Findings by the test team	Vendor comments
BlueCat	No	BlueCat currently uses BIND 9.6.1-P3. This feature is implemented in BIND 9.7 ALPHA. BlueCat will investigate supporting this feature when BIND 9.7 is released publicly by ISC for production use.
Infoblox	No information	The technique used for KSK rollover would allow an RFC5011-compliant resolver to track changes.
InfoWeapons	No information	RFC 5011 will be supported as a software update to SolidDNS 4.1.
ISC (BIND)	Yes	
Microsoft	No	The server does not follow RFC5011.
OpenDNSSEC	No	
Secure64	Yes	Yes we do revoke according to RFC5011.
Xelerance	No	DNSX currently does not set the revoke bit as per RFC 5011.

C1.2 - Which DNS system does the software use?

Product	Findings by the test team	Vendor comments
BlueCat	BIND	
Infoblox	BIND	
InfoWeapons	BIND	BIND 9.7.0p1 (as of SolidDNS 4.1.4)
ISC (BIND)	BIND	
Microsoft	Windows DNS	
OpenDNSSEC	Any third party name server.	
Secure64	Modified version of NSD.	Secure was initially based on NSD, but has been modified significantly since the initial branch.
Xelerance	NSD	DNSX uses NSD and BIND 9.

C1.3 - Is there a backup feature, and if so does the backup include encryption keys?

Comment: Backup features facilitate recovery after a system crash. It is particularly important that copies are made of the ZSK, the KSK and the zone files.

Product	Findings by the test team	Vendor comments
BlueCat	Yes	All keys are stored within the Proteus database and are contained within database backups. Database backups can be scheduled and copied off the system for safe keeping.
Infoblox	Yes	Yes, encrypted as part of the database backup. The Infoblox Grid technique provides several redundancy mechanisms to prevent systems crashes, both at hardware and software level. This provides non-stop management capabilities.
InfoWeapons	Yes	
ISC (BIND)	Manual backup	Backup falls outside the scope of BIND. It may be worth noting that the PKCS#11 HSM support adds some data security by storing keys offline, though.
Microsoft	A key backup can be made from the server's certificate store.	
OpenDNSSEC	Keys are stored in an HSM or SoftHSM. SoftHSM PKCS#11 key tokens can be backed up. Manual backup can be done of the configuration files.	Backup of the keys are done using the routines from the HSM vendor.
Secure64	Yes	Keys are never stored in the clear. During a backup, the private keys are encrypted using the TPM chip in the backup signer, so that only the backup signer can restore the keys.
Xelerance	Backup on file, if backed up encryption keys are protected with GPG.	If using an HSM, there is a backup protected with an HSM master key.

4.3.2 Transfer of DS records (C2)

Comment: The issue of transferring the public key hash DS from child to parent is important for TLDs, registrars or large organisations who handle several zones. Typically updates are transferred manually or using a protocol such as EPP (Extensible Provisioning Protocol).

C2.1 – Is there any notification to the administrator when the DS needs to be transferred due to automatic key rollover?

Product	Findings by the test team	Vendor comments
BlueCat	Yes	Administrators are notified of pending key rollovers through e-mail.
Infoblox	Yes	We notify the administrators when the KSK is about to expire.
InfoWeapons	Yes	An email is sent to the administrator of the zone when a key roll-over happens.
ISC (BIND)	No	
Microsoft	No	
OpenDNSSEC	Yes	You can configure a command that will be

		called whenever the DS RR-set needs to updated. We provide two example programs that will use EPP or e-mail.
Secure64	Yes	Yes, via syslog. We would like to point out that the rollover never finishes until the new DS is published. The chain of trust will not be broken even if the operator misses to upload the new DS.
Xelerance	Yes	Web GUI warning and e-mail notification.

C2.2 – Is it possible to export the public key hash DS or the ZSK for manual transfer?

Product	Findings by the test team	Vendor comments
BlueCat	The ZSK can be manually exported or sent by e-mail in DNSKEY format	
Infoblox	Yes, either a DS hash or the ZSK can be manually exported.	
InfoWeapons	The ZSK can be manually exported in Base64 format.	Yes
ISC (BIND)	Yes, both a DS record and the ZSK can be manually exported.	
Microsoft	Yes the ZSK can be exported from the certificate store.	
OpenDNSSEC	Yes, as a DNSKEY.	DNSKEY or DS
Secure64	The DS records are placed in a special text file.	The DS is generated in four different formats. SHA1, SHA2, DNSKEY, and one large file with SHA1/SHA2 per parent.
Xelerance	Yes, the ZSK can be manually exported.	

C2.3 – Which methods for transferring the public key hash DS are supported?

Product	Findings by the test team	Vendor comments
BlueCat	Manually or by e-mail, see C4.2.	
Infoblox	Manually	It is also possible to automate the transfers trough the API.
InfoWeapons	Manually	Transfer is done manually through out-of-band channels. The child zone can automatically detect if the DS in parent is updated, then resume KSK rollover.
ISC (BIND)	Manually	Usually manual. Automatic in one case: when parent and child zones are both hosted on the same server.
Microsoft	Manually	
OpenDNSSEC	Manual export of the DNSKEY or automatic transfer using for instance EPP.	
Secure64	Manually, see C4.2.	We are currently looking at the work the industry is doing to standardize this transfer.
Xelerance	Manually	

4.3.3 Zone distribution (C3)

C3.1 - Which types of incoming zone transfers/DNS changes are supported?

Comment: Support for incoming zone transfers is necessary to act as a signer-in-the-middle. For IPAM systems it can be useful to import initial zone data from other DNS servers using zone transfers.

Product	File	AXFR	IXFR	Dynamic updates*	Vendor comments
BlueCat	No	Yes	Yes	Yes	Support for dynamic signing is provided in the product for DDNS updates.
Infoblox	No	Yes	Yes	No	Through the Data Import Wizard several file types are supported including CSV, BIND and MS format.
InfoWeapons	Yes	No	No	Yes	
ISC (BIND)	Yes	Yes	Yes	Yes	
Microsoft	Yes	No	No	No	
OpenDNSSEC	Yes	Yes, through a separate module.	No	No	
Secure64	Yes	Yes	Yes	No	
Xelerance	No	Yes	Yes	No	

*Dynamic updates of DNS data to DNSSEC signed zones requires dynamic signing of RRSIGs when the DNS data arrives.

C3.2 - Which types of outgoing zone transfers changes are supported?

Comment: Changes in the DNSSEC zone data must be distributed to for example secondary name servers and slaves.

Product	File	AXFR	IXFR	Vendor comments
BlueCat	Yes, by accessing the appliance via SCP/SFTP.	Yes	Yes	
Infoblox	Yes	Yes	Yes	
InfoWeapons	Yes	Yes	Yes	
ISC (BIND)	Yes	Yes	Yes	
Microsoft	See C5.1.	Yes	Yes	
OpenDNSSEC	Yes	No	No	
Secure64	Yes	Yes	Yes	
Xelerance	Yes, via SCP or UI.	Yes	Yes	

4.3.4 Interoperability support (C4)

Are there any special interoperability features implemented?

Product	Findings by the test team	Vendor comments
BlueCat	Possible to use AD account for authentication. Administration of Windows DNS servers.	No management of DNSSEC enabled Windows servers due to the fact that DNSSEC records in Windows are manually generated.

Infoblox	Possible to use AD account for authentication.	
InfoWeapons	Possible to use AD account or RADIUS server for authentication.	
ISC (BIND)	PKCS#11 support for use of HSM key storage.	
Microsoft	No information	We will interoperate with other vendors that follow the RFCs for the RFCs that we support.
OpenDNSSEC	The system is modular and supports the use of third party tools for several tasks, including PKCS#11 HSMs.	
Secure64	The signer interoperates with major DNS server products and formats.	
Xelerance	No information	DNSX interoperates with any system that correctly implements the DNS/DNSSEC RFCs.

4.4 Key management and signing (D)

4.4.1 Key integrity (D1)

D1.1 - How are the keys stored and does the storage have a security classification?

Comment: To ensure confidentiality and integrity of the private zone keys it is important that they are stored securely, for example in an HSM.

Product	Findings by the test team	Vendor comments
BlueCat	No information	BlueCat is investigating HSMs for inclusion in our appliance line. These cards will be FIPS 140-2 compliant. The current method in which keys are generated is with a FIPS 140-2 compliant version of OpenSSL.
Infoblox	No information	It is stored in the signer's database.
InfoWeapons	No information	The key pairs for DNSSEC are stored securely (behind the firewall and encrypted) in the file system inside the SolidDNS appliance. HSM support is now under development and will be available within Q4 2010.
ISC (BIND)	Keys are stored in a clear-text file by default. The key files should either be stored on an encrypted volume or stored in an HSM.	Note that keys stored in an encrypted volume will not be available for automatic signing. Zones requiring the highest level of key security should use an HSM, or else use offline rather than automatic signing.
Microsoft	The keys are stored as certificates in Windows' certificate store.	The keys can be stored in an HSM. We use standard Windows certificates and CNG so any HSM that is supported by Windows works.
OpenDNSSEC	Hardware HSM with PKCS#11 interface or built in software emulated HSM.	OpenDNSSEC uses PKCS#11. It is thus up to the user to choose its preferred HSM vendor. We do provide a software only HSM, called SoftHSM.
Secure64	The cryptographic software module is FIPS 140-2 certified. Private keys are wrapped using keys on a TPM chip.	The private keys are wrapped using keys that are stored in the onboard TPM chip as the root of these encryption layers.
Xelerance	No information	DNSX supports an HSM which is FIPS 140-2 Level 3 certified. A copy of this certification is available upon request.

4.4.2 Key export (D2)

D2.1 - Can the private keys be exported, if so to which formats?

Comment: Organisations may need to export their private keys for a signed zone. Export is needed for backup reasons as well as for key import during migration to a new DNSSEC management tool.

Product	Findings by the test team	Vendor comments
BlueCat	Only as part of system backup.	Keys cannot be exported by themselves. However, they are part of the database backup, which allows private keys to be backed up for security purposes.
Infoblox	Yes, keys can be exported in a proprietary format using the Perl API.	
InfoWeapons	Only to another SolidDNS appliance through the backup feature.	Schedule for release of DNSSEC key backup has been moved to Q4 2010 due to other higher priority feature requests from existing customers.
ISC (BIND)	Yes for the clear-text file. Private-key-format: v1.3.	Format v1.2 also supported for use by older versions of BIND 9.
Microsoft	Yes, keys can be exported in the same way as certificates.	
OpenDNSSEC	Keys can be exported from the SoftHSM in PKCS#8 format.	
Secure64	Yes, but only to another Secure64 signer.	
Xelerance	Yes, encrypted with GPG in the backup/export feature.	Or encrypted with the HSM Master key when an HSM module is used.

D2.2 - How are the exported private keys protected?

Product	Findings by the test team	Vendor comments
BlueCat	Not applicable, see D2.1.	
Infoblox	No information	The keys are stored in a database which is locked down and cannot be reached directly from the CLI or through database queries. In the backups the keys are encrypted.
InfoWeapons	No information	There is no direct way to gain access to the private keys stored within the system from any of the available management interfaces.
ISC (BIND)	No protection. Should be stored on encrypted device.	
Microsoft	Password protected pfx files.	
OpenDNSSEC	See D2.1.	
Secure64	Ordinary TPM to TPM key backup.	When keys are backed up to another Secure64 DNS Signer server, they are first encrypted using another TPM-protected public key from the backup server and then transmitted over the network.
Xelerance	See D2.1.	For the HSM version, the export format is tied to the HSM to guarantee only authorized HSM cards can read an encrypted export.

4.4.3 Key import (D3)

D3.1 - Can keys be imported from another source, if so which formats are supported?

Comment: There are several reasons why the keys need to be recoverable. Two examples are recovery from backup and during migration from one DNSSEC product to another.

Product	Findings by the test team	Vendor comments
BlueCat	No	Keys are automatically created by the Key Policy manager within the BlueCat product.
Infoblox	No information	Yes, through a Perl API using a proprietary format.
InfoWeapons	Import of individual Base64 encoded keys or from another SolidDNS appliance.	
ISC (BIND)	Yes, in BIND private-key-format v1.3.	Format v1.2 can be imported as well, from older versions of BIND.
Microsoft	It is possible to import keys stored in pfx format.	
OpenDNSSEC	Keys can be imported in PKCS#8 format.	OpenDNSSEC also has a tool which can convert BIND key files into PKCS#8 format.
Secure64	Yes but only from another Secure64 signer.	Keys can be recovered from another Secure64 DNS Signer. If a customer needs to migrate to another DNSSEC product, there is a documented key rollover procedure that can be utilized to accomplish this.
Xelerance	Keys encrypted with GPG can be imported.	For the HSM version, due to certification, only keys that have never been decrypted outside the HSM are allowed to be used while the HSM is in FIPS compliance mode.

4.4.4 Zone signing (D4)

D4.1 - Is it possible to use the same keys to sign several zones?

Comment: For some registrars and TLDs this is an important feature to achieve acceptable performance. Interestingly enough very few of the evaluated products currently support this function even though it is a hot topic when discussing DNSSEC deployment.

Product	Findings by the test team	Vendor comments
BlueCat	No	BlueCat's Key Policy manager handles the creation and rollover of all keys. Individual key pairs are created for each zone.
Infoblox	No	
InfoWeapons	No	
ISC (BIND)	Yes, the keys are pre-generated and chosen when signing the zone.	
Microsoft	Yes	
OpenDNSSEC	Beta support exists but definitive support is scheduled for OpenDNSSEC 1.2.	
Secure64	No	
Xelerance	No	

D4.2 - Can keys be generated for several zones simultaneously?

Comment: In order to save time, it is important for large organisations with many domains that key generation and signing can be done for several zones simultaneously.

Product	Findings by the test team	Vendor comments
BlueCat	Yes	A policy can be linked to a DNS view which can contain any number of zones, this will generate keys for all zones within the view automatically for the administrator
Infoblox	Key creation for one zone at a time; the keys are created when the zones are signed for the first time.	
InfoWeapons	Key creation for one zone at a time; the keys are created when the zones are signed for the first time.	Restarting the DNS service forces simultaneous key generation and zone signing for all zones automatically.
ISC (BIND)	Yes, via scripting.	
Microsoft	Yes, via scripting.	
OpenDNSSEC	Yes, via scripting.	Keys are normally generated on the fly. But you can pre-generate keys using the CLI.
Secure64	Yes, keys can be pre-generated and then used to sign several zones.	The pre-generation of keys along with our optimized crypto engine makes signing very fast.
Xelerance	Yes, keys are generated automatically when zones are imported to the signer.	DNSX automatically generates the keys when required. When zones are added in bulk, keys are generated in bulk.

D4.3 - How can the administrator monitor the zone signing process?

Comment: To assure the accessibility of the zone and increase the awareness by the zone administrator, it is important to be able to monitor the signing process.

Product	Findings by the test team	Vendor comments
BlueCat	Signing occurs automatically when an unsigned zone is deployed.	Bulk signing of zones occurs when a deployment is made to an Adonis which has configured DNSSEC zones. BlueCat is investigating the scheduled signing of zones in a future release.
Infoblox	Signing is done in the background and progress is not presented.	
InfoWeapons	Signing is done in the background and progress is not presented.	The administrator can monitor progress by viewing the system logs.
ISC (BIND)	For manual signing it is up to the administrator to set up monitoring. For automatic signing monitoring can be done via syslog or file.	
Microsoft	The signing process is manual.	
OpenDNSSEC	No live monitoring, signing information is logged to syslog.	
Secure64	No live monitoring, signing status can retrieved through 'show dnssec status'.	
Xelerance	Zones are signed automatically when imported to the signer. No progress is shown.	

D4.4 - Can zone signing be distributed over time?

Comment: When several zones are signed on the same occasion, it is convenient if the signing process can be automatically spread over time in order to reduce the machine/processor load.

Product	Findings by the test team	Vendor comments
BlueCat	See answer in D4.2.	
Infoblox	No information	The zone is signed when the user so requests. It is possible to multi-select zones for signing; these would all be signed sequentially, but without any other attempt to pace the signing.
InfoWeapons	No	The signing is done every time a reload or DNS restart is done.
ISC (BIND)	No	The auto-dnssec/signature maintenance features of named automatically spread the process over time. This can be configured with options in named.conf.
Microsoft	The signing process is started manually.	
OpenDNSSEC	No, zones are signed when they are added to the configuration.	The zone will be rescheduled for signing according to the time when it was finished the previous run. This will create a spreading effect.
Secure64	No, the signing process is done automatically in the background when enabled in the configuration.	
Xelerance	No, see D4.3.	Signing is skipped when load is high, leading to distributed zone signing automatically.

4.4.5 SOA management (D5)

D5.1 - How are the SOA serial numbers updated?

Comment: For zone file changes to take effect, the SOA serial numbers must be updated. There may be reasons to leave the SOA unchanged such as preventing updates from being propagated further.

Product	Findings by the test team	Vendor comments
BlueCat	Optional	
Infoblox	As a counter.	
InfoWeapons	Counter or manual.	The SOA is always incremented every time a signed zone is reloaded.
ISC (BIND)	Optional	
Microsoft	Manual	
OpenDNSSEC	Optional	
Secure64	If the zone is managed by the appliance, the SOA is handled manually. If the appliance acts like a “signer in the middle” the SOA is incremented.	
Xelerance	Optional	

D5.2 - Which of the following serial number formats are supported; counter, Unix time, date and stay unchanged?

Product	Findings by the test team	Vendor comments
BlueCat	Counter, date or manual.	
Infoblox	Only counter.	
InfoWeapons	Only counter.	
ISC (BIND)	Counter, Unix time and stay unchanged.	
Microsoft	Manual	
OpenDNSSEC	Counter, date counter, Unix time and stay unchanged.	
Secure64	Counter or manual.	
Xelerance	Counter or date.	YYYYMMDDXX if that is higher than the serial of the unsigned zone, otherwise counter.

4.4.6 NSEC3 (D6)

D6.1 – Is NSEC3 opt-in and opt-out supported?

Comment: NSEC3 support is important for privacy issues since NSEC enables so called zone enumeration by which external entities can list all names in a zone. If using NSEC3 opt-out, only authoritative data and delegation records are signed.

Product	Findings by the test team	Vendor comments
BlueCat	No, only NSEC3 opt-in	
Infoblox	Yes	
InfoWeapons	Yes	
ISC (BIND)	Yes	
Microsoft	No, only NSEC is supported.	
OpenDNSSEC	Yes	
Secure64	Yes	
Xelerance	Yes	

4.4.7 Signing algorithms (D7)

D7.1 - Is it possible to configure which signing algorithm is used?

Comment: For security and compatibility reasons, it is important to be able to choose the signing and hashing algorithms.

Product	Findings by the test team	Vendor comments
BlueCat	Yes	
Infoblox	Yes	
InfoWeapons	Yes	
ISC (BIND)	Yes	
Microsoft	No	
OpenDNSSEC	Yes	
Secure64	Yes	
Xelerance	Yes	

D7.2 - Which signing algorithms are supported?

Product	Findings by the test team*	Vendor comments
BlueCat	RSAMD5, RSASHA1(NSEC3), DSA(NSEC3)	
Infoblox	RSASHA1(NSEC3), RSAMD5, DSA(NSEC3)	
InfoWeapons	RSASHA1(NSEC3)	DSASHA1NSEC3 is available as a software patch update.
ISC (BIND)	RSAMD5, DSA(NSEC3), RSASHA1/256/512(NSEC3)	
Microsoft	RSASHA1	
OpenDNSSEC	RSASHA1/256/512(NSEC3)	
Secure64	RSASHA1(NSEC3)	
Xelerance	RSASHA1(NSEC3)	RSASHA256 will be supported by Q3 2010. GOST by Q4 2010

*The notion (NSEC3) indicates NSEC3 support for the algorithm.

4.4.8 Key rollover (D8)

D8.1 - Can the administrator monitor key rollovers?

Comment: To assure the accessibility of the zone and increase the awareness by the zone administrator, it is important that the key rollover for ZSK and KSK can be monitored.

Product	Findings by the test team	Vendor comments
BlueCat	ZSK and KSK rollovers are automatic or can be carried out in the GUI.	
Infoblox	The ZSK rollover is automatic. The KSK rollover is performed manually. A notification is sent by e-mail and/or SNMP when a KSK rollover is imminent.	
InfoWeapons	Rollovers for both the ZSK and KSK are performed automatically.	Notification via e-mail is done during key rollover.
ISC (BIND)	The ZSK rollover is automatic. BIND 9.7 currently does not fully support automatic KSK rollovers. Notification via log file or syslog.	Fully automatic KSK rollovers are not recommended. They do work, but because of the lack of automatic DS notification, built-in delays to handle TTL timeouts, etc, it is generally safer to roll KSKs manually. These features are planned for future releases.
Microsoft	It is a manual process.	
OpenDNSSEC	Key rollovers are done automatically and logged using syslog.	The CLI can show the expected key rollovers.
Secure64	'Show dnssec status' lists information about the keys, including the next rollover. Roll info is logged.	'Show dnssec status' gives lists all information about the key including next rollover. All roll info is logged in syslog.
Xelerance	KSK and ZSK rollovers can either be done automatically or manually.	KSK rollovers cannot be fully automated due to the lack of a standard to communicate these to a parent.

D8.2 - Can the keys in the zone file be pre- and post-published?

Comment: Allowing pre- and post-publishing of the keys in zone files facilitates a secure key rollover since it gives the possibility to use several concurrent zone keys.

Product	Findings by the test team	Vendor comments
BlueCat	Pre-publish and the double signing method is supported for the KSK and the ZSK.	
Infoblox	The double signing method is used for both the KSK and the ZSK.	
InfoWeapons	No information	Yes, the zone file will contain pre-published and current ZSKs. During ZSK rollover, once the ZSK reaches its end of life, the zone will be resigned with the KSK and pre-published ZSK.
ISC (BIND)	Pre-publish is supported for the KSK and the ZSK.	
Microsoft	Support for double signing and pre-publish methods.	
OpenDNSSEC	The ZSK is pre-published and the double signature method is used for the KSK.	
Secure64	The ZSK is pre-published and the double signature method is used for the KSK.	
Xelerance	Pre-publish is supported for the KSK and the ZSK.	DNSX always performs pre- and post-publishing of the keys.

D8.3 - Can the key rollover be distributed over time?

Comment: When several key rollovers are performed at the same time, it is useful to know if the rollover process can be automatically distributed over time to reduce the machine/processor load. If automated signing is supported it is always possible to let the life span vary in order to achieve spread out re-signing.

Product	Findings by the test team	Vendor comments
BlueCat	No	
Infoblox	No	
InfoWeapons	No	
ISC (BIND)	No	Key changes occur on schedule; zone resigning will be spread over time. (See comments for question D4.4.)
Microsoft	Manual process	
OpenDNSSEC	No	
Secure64	No	
Xelerance	No	DNSX performs the key rollover based on timer settings that can be configured on a default or per-domain setting. Load distribution will cause further spreading of signing and rollover time

4.5 Status and monitoring (E)

4.5.1 Keys (E1)

Is should be possible to retrieve key attributes such as time of creation and expiry date for the KSK and ZSK conveniently.

Product	Findings by the test team	Vendor comments
BlueCat	Yes, keys can be viewed per zone; active/inactive status and expiry date.	Proteus contains a report which can detail the expiry and signing status of all zones within a view.
Infoblox	The ZSK rollover is automatic. The administrator is notified in the GUI when a KSK rollover is necessary.	
InfoWeapons	No	This feature will be available by Q4 2010. Currently, the key expiry date is included in the following email notifications: - Pre-expiry KSK rollover notification. - Expired KSK notification.
ISC (BIND)	Yes, via the command dnssec-settime.	
Microsoft	Yes, the information is stored in the certificates.	
OpenDNSSEC	It is possible to retrieve key status and next scheduled rollover.	
Secure64	Yes	
Xelerance	Some key attributes such as key age is displayed.	DNSX shows the individual zone's (re)signing statistics in the single domain view through its web interface.

4.5.2 Signing (E2)

Possibility to retrieve zone signing attributes. It is convenient to be able to view the zone's RRSIGs without doing a zone transfer.

Product	Findings by the test team	Vendor comments
BlueCat	Keys can be viewed per zone but the RRSIGs are not available in the GUI.	
Infoblox	It is possible to view the RRSIGs for a zone in the GUI.	
InfoWeapons	RRSIGs can be viewed in the "config file" tab of a zone.	
ISC (BIND)	Only by looking at the zone file.	
Microsoft	No	
OpenDNSSEC	Only by looking at the zone file.	
Secure64	No, it is not possible to view the RRSIGs directly in the GUI.	
Xelerance	It is possible to view the RRSIGs for a zone in the GUI.	

4.5.3 Logging (E3)

What information is logged and how is the log data presented to the administrator?

Comment: Comprehensive and easily accessible logs are important for auditing and troubleshooting. It is also important that an alarm is raised if critical errors occur.

Product	Findings by the test team	Vendor comments
BlueCat	No information	All events are logged to the Audit log within Proteus, this includes key operations, configured signing of zones and all user-initiated changes. Protocol data is logged via syslog.
Infoblox	No information	The following events are logged: Signing/unsigning, key generation, re-generation of expired signatures and key rollovers.
InfoWeapons	No data regarding DNSSEC is logged except that the key rollover daemon runs periodically. The logs can be sent to another machine.	The DNSSEC validation process is logged if DNSSEC debug is enabled. Log data can be viewed as an event in the System Log page.
ISC (BIND)	There are many logging categories, see user manual. Logs can be sent to file or syslog.	
Microsoft	No information	The event viewer will log when signatures in a zone are about to expire. No events related to key generation or zone signing (other than prompting for re-signing) are fired.
OpenDNSSEC	Most of the command line tools log extensively to syslog.	
Secure64	Yes, relevant DNSSEC information is logged in syslog.	
Xelerance	No information	DNSX produced AUDIT logs for each key and sign operation. Logs can be generated locally, or send via syslog. The DNSX logging facility complies with NIST Special Publication 800-92.

4.5.4 Monitoring and alerts (E4)

What actions are taken if key generation, signing, DNS server, or hardware fails? How will this interface with SNMP software?

Product	Findings by the test team	Vendor comments
BlueCat	Errors can be reported via e-mail or SNMP traps.	
Infoblox	SNMP support but not for DNSSEC. Error reporting in the GUI.	Errors reported via GUI, Perl API, or syslog, depending on how the faulting action was initiated.
InfoWeapons	SNMP support for DNSSEC in debug mode.	A notification in the web UI appears if key generation, signing or DNS service fails. An event will also appear in the System log file. CPU, memory and basic DNS queries/failures can be retrieved via SNMP. DNSSEC related info/failures will also appear in the System log file with debug mode enabled.
ISC (BIND)	No SNMP support. Errors reported via log file or syslog.	

Microsoft	No SNMP support.	
OpenDNSSEC	Errors are logged but there is no SNMP support.	
Secure64	None, the administrator have to run manual commands or inspect the syslog.	
Xelerance	No SNMP support.	It is recommended that a central logging facility processes the DNSX syslog messages and uses the existing alert facilities. DNSX can be configured to send out e-mails for alerts.

4.5.5 Overall usability (E5)

Without aspiring to do a completely objective comparison the test team still thought it was meaningful to add some short subjective notes summarizing facts that did not fit into the formal review points. Note that the vendors have not been able to comment on this table.

Product	Findings by the test team
BlueCat	Full-fledged IPAM system. Relatively easy to get started with configuring DNSSEC on existing BlueCat Adonis appliances managed by Proteus. No NSEC3 opt-out support might be negative for TLDs and registrars.
Infoblox	Another appliance based full-fledged IPAM system. All major DNSSEC functionality is there and the UI is modern and intuitive.
InfoWeapons	InfoWeapons is mainly a DNS server but integrates with third party IPAM. The DNSSEC functionality works as expected but the UI was relatively difficult to navigate. The SolidDNS appliance is available as a virtual machine.
ISC (BIND)	All major DNSSEC features are implemented and BIND is actually used as a base in several of the other support products. For administrators already using the BIND CLI for DNS management there is no need to change for DNSSEC reasons. One drawback is that keys are stored in clear-text by default so an HSM is typically required. Plus for ability to use the same key for several zones.
Microsoft	No DNSSEC policy management, the complete key management process is handled manually via CLI. Integration into the DNS Server MMC UI would have been preferable. No algorithm selection and no NSEC3 support. These factors combined make larger deployments impractical. Plus for ability to use the same key for several zones.
OpenDNSSEC	OpenDNSSEC is a CLI-based thin DNSSEC signer and is the most light weight solution reviewed. The SoftHSM feature comes in handy for smaller deployment scenarios. Currently a third party name server is required for outgoing zone transfers. The architecture is Linux like with opportunities to plug in third party tools or own scripts.
Secure64	Appliance based DNSSEC signer which can also work as a DNS server. All major DNSSEC functionality is there. A web UI would have been nice to complement the CLI but a plus for the security focus with a dedicated hardened OS and TPM key storage.
Xelerance	Appliance based DNSSEC signer which implements the major DNSSEC functionality. However the UI is non-intuitive and old fashioned which brings down the overall impression.

5 Key Findings

5.1 Summary

The general standard of the reviewed products is good and there is a healthy diversion in system packaging, platform support and administration interfaces. With a reservation for performance (which we did not test as motivated in section 1.4) the management tools work as expected and we see no apparent obstacles for major deployment. Some desired functionality is still missing from several of the products, notably support for using the same key for several zones and non-proprietary key migration. However crucial functions seem to work well and the products facilitate DNSSEC management in an adequate way.

DNSSEC is a dynamic and emerging technology and so are the management tools. The products changes continuously and it will be interesting to follow the development especially with regards to interoperability, performance and ease of use in larger deployment scenarios.

5.2 Suggested future work

Our impression during the previous testing phase was that basic DNSSEC functionality was well-functioning but there were some areas such as key integrity, NSEC3 and UI that were being continuously improved. Now several of the products have matured somewhat and we do not believe that lack of adequate management tools is the biggest challenge for DNSSEC deployment today.

The upcoming challenge for DNSSEC now is to prove that it works smoothly for large deployments. Several categories of stakeholders have (rightfully) expressed concerns about adding additional complexity to the DNS system. It is important to address these questions and prove the sceptics wrong by carrying out successful DNSSEC deployments at TLDs and other major zones.

As for the development of management tools it will be interesting to see how the products will cope with the increased DNSSEC use following the signing of the root and continuous signing of TLDs. For example one problem we foresee (based on the test results and current DNSSEC deployment strategies) is that registrars for performance reasons might want to use the same key for several zones. This feature is currently only supported in three out of eight reviewed products.

There are other similar deployment issues that might be interesting to revisit when DNSSEC signing and validation has reached a larger install base. We recommend an updated review of DNSSEC management tools in perhaps twelve months time with focus on evaluating the ability to handle larger real life deployment scenarios.

6 Abbreviations

AD – Active Directory
API – Application Programming Interface
BIND – Berkeley Internet Name Domain
CLI – Command Line Interface
DHCP – Dynamic Host Configuration Protocol
DLV – DNSSEC Look-aside Validation
DNS – Domain Name System
DNSSEC – Domain Name System Security Extensions
DS – Delegation Signer
EPP – Extensible Provisioning Protocol
FIPS – Federal Information Processing Standard
GUI – Graphical User Interface
HSM – Hardware Security Module
IETF – Internet Engineering Task Force
IPAM – Internet Protocol Address Management
ISC – Internet Systems Consortium
JSON – JavaScript Object Notation
KSK – Key Signing Key
NSD – Name Server Daemon
NSEC – Next Secure
NSEC3 – Next Secure 3
PKCS – Public Key Cryptography Standard
RFC – Request for Comment
RNG – Random Number Generator
RR – Resource Record
RRSIG – Resource Record Signature
SCP – Secure Copy
SOA – Start of Authority
SSH – Secure Shell
SNMP – Simple Network Management Protocol
TA – Trust Anchor
TLD – Top Level Domain
TPM – Trusted Platform Module
TTL – Time to Live
UI – User Interface
ZSK – Zone Signing Key

7 References

[1] ÅHLUND J. *A Review of Administrative Tools for DNSSEC.* 2009

[2] RFC 3833 - Threat Analysis of the Domain Name System (DNS). 2004. http://tools.ietf.org/html/rfc3833

[3] KLEIN A, *BIND 9 DNS Cache Poisoning.* 2007

[4] LINDQVIST A., ÅHLUND J. 2007. *System för DNSSEC-administration*. KTH

[5] RFC 5011 - Automated Updates of DNS Security (DNSSEC) Trust Anchors. 2007. http://www.ietf.org/rfc/rfc5011.txt