Authentic Web

Empowering Teams for DNS Security, Compliance and Performance

How to Implement and Manage DNSSEC

Protect against Man-In-The-Middle and DNS Hijacking

A Discussion Paper on DNSSEC

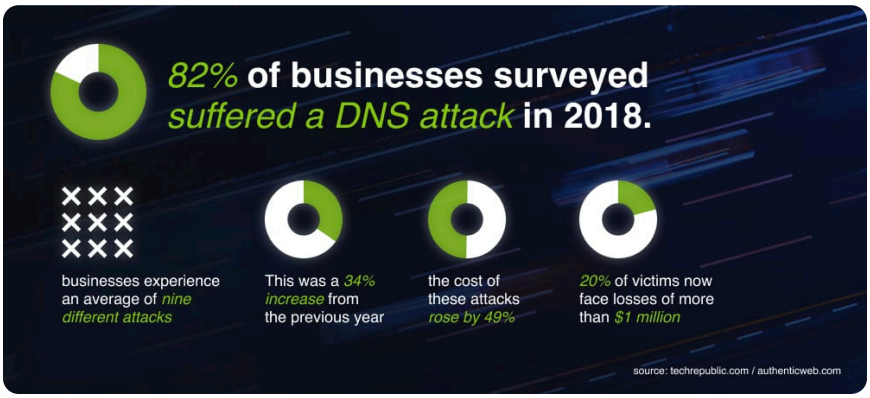
"The Domain Name System (DNS) underpins every digital service. Yet, domain and DNS audits reveal major compliance gaps in security policy enforcement. Manual change management processes do not work in the digitally transformed enterprise."

Peter LaMantia, CEO, Authentic Web Inc.

The Need for Comprehensive DNS Security

In a digital world, organizations and individuals rely on the internet daily for a limitless number of essential tasks. Internet users count on organizations to maintain online service availability and to protect their data privacy. Users need to be able to trust that digital brands are authentic i.e., that a brand web presence is who they say they are. Unfortunately, digital brand trust is increasingly threatened by vulnerabilities in the internet's very foundation: The Domain Name System, or DNS.

Every single online action starts with the DNS. Whether for shopping, banking, paying a tax bill, or connecting with an enterprise service delivery system — any browsing purpose at all — the DNS directs requests to the online destinations, content and applications sought by users. The DNS is central to the internet and how it operates. It is this very criticality that has made the DNS vulnerable to abuse. Hijacking, spoofing, Man-in-the Middle attacks, and other threats can disrupt an organization's online operations with disastrous consequences for brand reputations and user security.



There are many best practice defences that infrastructure leaders need to ensure are covered when they define and implement DNS security policies to keep their networks fully operational, secure and customers safe. Those measures include Domain Name System Security Extensions (DNSSEC), Sending Policy Framework (SPF), Domain-based Reporting and Conformance (DMARC), a secondary DNS network, and a security policy of HTTPS Everywhere. Security policies and measures then need to be enforced with robust change management controls.

Learn the business process improvement best practices to protect your online presence.

The Complete Business Process Guide for DNS Management →

In this paper, we are taking a deeper dive into DNSSEC.

Domain Name System Security Extensions, or DNSSEC, helps defend against DNS security threats, specifically related to Man-In-The-Middle (MITM) and DNS Hijacks. While DNSSEC is extremely effective, many organizations have not yet adopted it simply because it is challenging to set up and manage over the lifecycle of a domain and the larger portfolio of domains.

Traditional, manual practices for DNS management and the common practice of using multiple DNS services have made DNSSEC deployment cumbersome, inefficient, and costly. There is a solution: consolidating all domains and DNS services under a unified, automated environment can simplify and secure organizations' at-risk internet operations.

In this guide to DNSSEC, we will explain what DNSSEC is, how it works, and why it's important. We will also identify the obstacles to implementing DNSSEC and show how a simplified approach to DNS management makes effective deployment possible.

© 2021 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

What is DNSSEC?

DNSSEC is a security protocol that validates DNS query responses. It protects internet users (clients) from forged DNS data in recursive servers, often referred to as DNS cache poisoning. DNSSEC uses tamper-proof, digitally signed keys to verify the authenticity of a domain's zone files and sends internet users to the intended brand authentic destination.

Understanding what DNSSEC is requires looking at the DNS itself. The domain name system was developed in the 1980s to make the internet easier to use. It's often described as a directory that translates the words we type into a browser into an IP address where content is served. For example, apple.com is an easily remembered domain. The DNS translates the domain (URL) to an internet protocol (IP) address on the server(s) where Apple's website is found – in this case (at the time of writing), 17.253.134.10. The DNS makes browser-based address queries significantly easier than an unwieldy list of millions of numeric IP addresses.

Ease of use and ubiquity are contributing factors to the evolving risks associated with the DNS. As the internet matured, it became apparent that there were many ways to abuse and misuse the DNS for malicious purposes. The DNS is not by design, very secure. It is a global list of web servers that make the internet available to all of us. For years, malicious parties have become inventively adept at compromising the DNS by intercepting, forging and/or manipulating DNS query responses. As a result, internet users and organizations cannot always be sure that online content requested is in fact from a legitimate, authenticated source.

DNSSEC was the industry response to the authentication vulnerabilities inherent to the DNS. It was developed by the Internet Engineering Task Force (IETF) to counter the "impersonation" problems associated with the DNS. DNSSEC's dual-encrypted signature keys ensure that the online content internet users request through their browsers returns legitimate, authenticated results from the Domain Name System. Without DNSSEC, organizations are vulnerable to their DNS systems (and customers) being compromised by way of MITM or DNS Hijacking.

© 2021 Authentic Web Inc. All rights reserved.

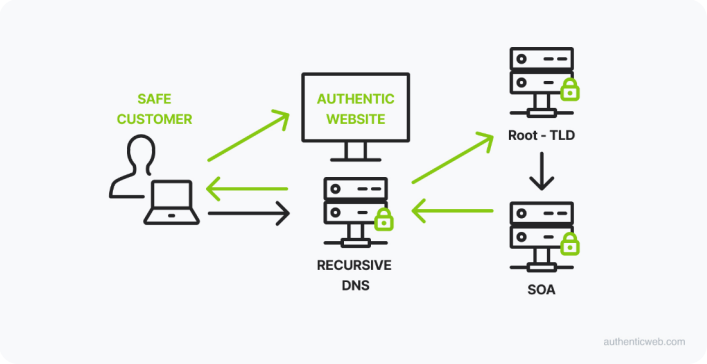
1.855.436.8853 | info@authenticweb.com

How does DNSSEC work?

The DNS is organized into zones and uses resolvers to direct browser-based queries. To protect DNS zones, DNSSEC matches two digital keys, one public and one private. Together, digital signing (DS) keys validate the authenticity of DNS data. Cryptographic signatures ensure that DNS resolvers are locating legitimate IP destinations preventing hijacking of recursive server DNS zone files due to cache poisoning. Keys themselves are signed as part of a digital chain of trust.

The private key is known only to the domain owner. When DNS data is requested a DSKEY is used to "sign" the data. The recursive DNS server compares the signature to the public key in the TLD registry records. If the keys match, the internet user receives the records that point to a host and gains access to the brand authentic website. If they are different, the records are assumed to be a forgery and the DNS data is dumped without being returned to the end user.

DNSSEC offers brand protection by ensuring internet users will not be misdirected to fraudulent content destinations. Online shoppers visiting www.Gucci.com have every expectation of being at the real Gucci website. Likewise, banking customers certainly want assurances that their online transactions are taking place at the authoritative bank website rather than a fraudulent imposter site designed to intercept and steal their vital information. DNSSEC assures internet users that requested online destinations are brand authentic.



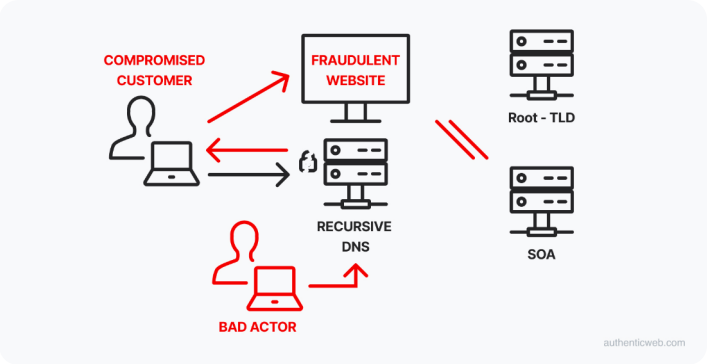
What can happen without DNSSEC?

Without DNSSEC, organizations are exposed to the risk of DNS hijacking, or "spoofing" largely by DNS cache poisoning. DNS recursive servers operate more efficiently when they store DNS query data for repeated or similar DNS queries. DNS cached data can be compromised and modified to return a falsified response.

Once a user is misdirected to a fraudulent website (IP address), their computer is open to malicious content like malware and viruses. It's particularly insidious when hackers can impersonate a legitimate website, complete with SSL certificate encryption to dupe a user into logging in, believing the website or application to be legitimate. DNS hijacking can and has resulted in stolen data and credentials.

A company's online presence is crucial to its financial performance. DNS attacks can disable websites, interrupt sales, and trigger the loss of loyal customers. Brand reputation can suffer, exacerbated by lawsuits and regulatory penalties. Organizations that ignore DNS defences like DNSSEC place themselves and their users at significant risk.

Every sector is vulnerable to DNS compromise, but malicious parties go where the money is, making some industries particularly exposed. Financial data such as banking information, credentials or credit card records are lucrative spoils to hackers. Organizations that store payment data in industries like finance, banking, healthcare, and online payment services are at high risk. Government and membership-related services such as hotel loyalty programs are frequently targeted by DNS attackers.



© 2021 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

Why DNSSEC is only now being adopted?

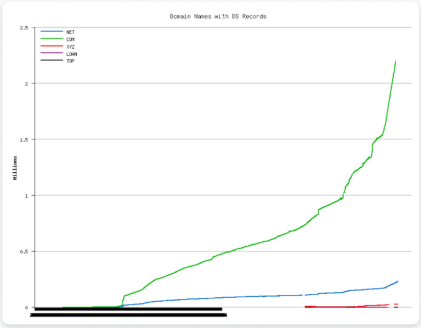
DNSSEC is proven to be a reliable defence against DNS hijacking, yet many organizations have not deployed it. Two factors influencing the lack of broad adoption are the perceived complexity and cost of effectively implementing DNSSEC.

1. DNSSEC adoption is complicated and costly because of the way companies manage their external DNS. Most enterprise-level organizations use multiple registrars and often many more managed DNS services due to legacy decisions or corporate acquisitions over many years. Because not all DNS providers support DNSSEC, and rarely integrate with registrar systems, deployment can be inconsistent or unfeasible for large parts of a company's domain portfolio.
2. DNSSEC requires a coordinated chain of trust for each domain query. Domain registrars, DNS providers, and TLD registries each contribute to the chain of trust supporting DNSSEC. With so many parties in the mix, consistent, low-effort administration of DNSSEC across a domain portfolio becomes challenging.

Those are the external challenges. Internally, organizations lack sufficient expertise to correctly implement and maintain DNSSEC. The steps to setting up DS keys and RRSIGs at your DNS service and ensuring they are in sync with domain registrars and registries are typically manual, involving staff work effort. Additionally, the DS keys roll over each year, adding complexity that must be maintained over the lifecycle of every domain.

In this manual operation scenario, to validate correct operation of DNSSEC, it's necessary to constantly check that digital signing keys are present and valid. In a domain portfolio of hundreds or thousands of domains, it's a formidable task and unreasonable to expect compliance. It requires checking the domain zone file to verify that the RRSIG and DS records are present and correct. Further complicating the process, a lookup tool may confirm that digital signing keys are present even when the DS key may have expired or the RRSIG has been changed. To maintain DNSSEC integrity, all keys must be tracked and rolled across multiple systems.

Demonstrating the importance of DNSSEC, despite the complexities, research from Verisign Labs shows an explosion in DNSSEC over recent years both because the incident rate of compromised customers is increasing and secondly because new automation tools are being built to help teams manage DNSSEC through automation over the domain lifecycle. This is a good thing.



Source: Verisign Labs

How to ensure your DNSSEC is working

Given all the moving parts, it's easy for organizations to assume DNSSEC is actively working when, in fact, a broken link in the DNS chain of trust has invalidated the authentication. The most important test to ensure that DNSSEC is active is to confirm the presence and validity of the digital signing keys, specifically the resource record signature (RRSIG) and the delegation signer (DS key.) An invalid RRSIG will prevent the DNS from returning a query result. While your DNS security will remain intact in this scenario, users will be blocked from content.

© 2021 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

A missing or expired DS key at the top-level domain registry will continue to return DNS query results, however, they will be non-authenticated and therefore open to exploitation and misuse.

Testing DNSSEC validity on all domains is a tedious, manual process requiring verification of signature keys, potentially on multiple registries. While there are tools to make this task easier, e.g., Verisign Lab's DNSSEC Analyzer, most of them test a single domain at a time. This is impractical for large domain portfolios, moreover, it does not monitor DNSSEC in real time.

The most effective way to monitor and manage DNSSEC is within an integrated, end-to-end, domain/DNS change management system. Otherwise, enterprise DNSSEC can be misconfigured or operating with expired keys that offer no protection at all.

How to implement DNSSEC

The biggest problem with DNSSEC isn't the protocol itself although continuous improvements are underway. The real problem underlying its cost and complexity is inefficient DNS management due to manual, legacy processes. Four basic steps are best practice essentials to prepare any organization's domain and DNS operation for successful DNSSEC implementation.

Integrating DNS management will make DNSSEC easier to implement. More importantly, it will make DNSSEC easy to monitor and maintain so you can gain ongoing security benefits for your organization and keep your customers safe.

1. Audit your DNS network

The first step in securing your DNS network is to conduct an APEX-level DNS audit. Identify all domain registrars and managed DNS providers active and/or touching your digital assets and network. Test for a pass/fail status of DNSSEC on every domain. Similarly validate other DNS security measures including: DMARC, SPF, and TLS/SSL certificates on all domains and re-direct domains. An audit report can identify DNS security weaknesses across an entire domain portfolio.

2. Standardize security policies

Every domain and its associated DNS zone file require common compliance policies, including rules for DNSSEC. Organizations should codify their policies such that every domain (out of hundreds or thousands) is subject to a consistent security standard. Inconsistencies in the use of Start of Authority (SOA), SPF, DMARC, and DNSSEC are gaps in your DNS security posture that malicious parties actively target and exploit.

© 2021 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

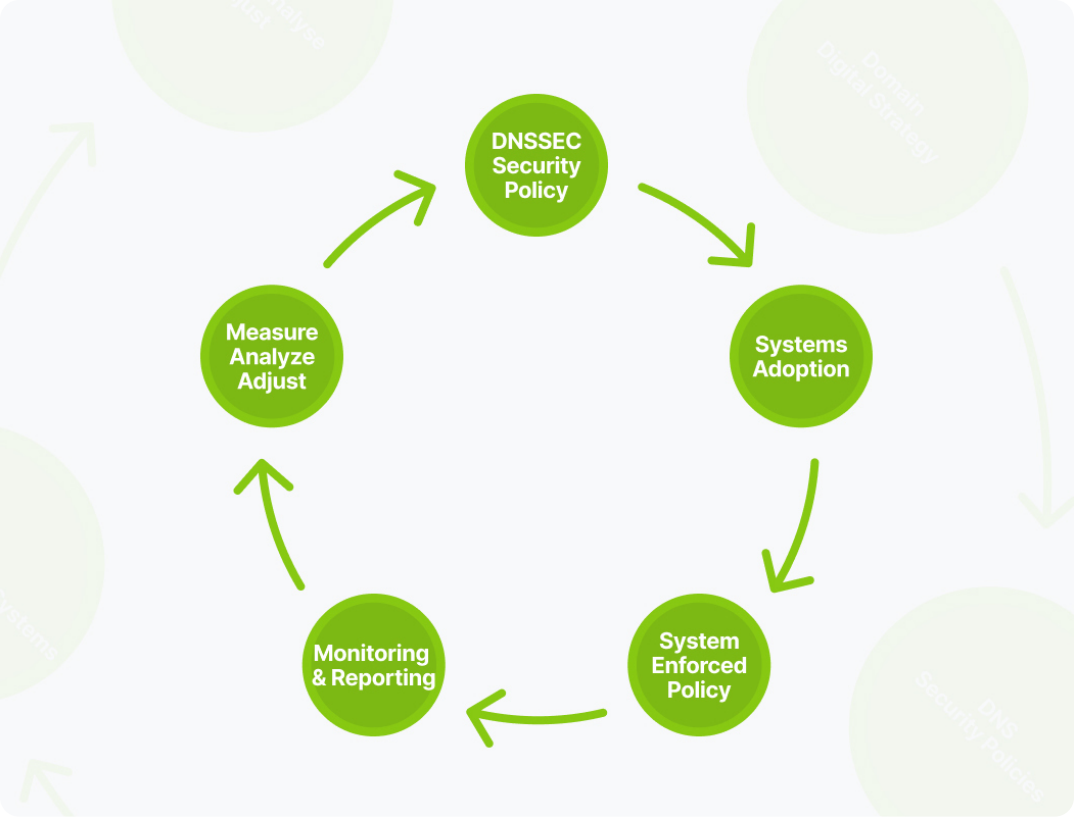
3. Consolidate your managed DNS service providers

DNSSEC is prohibitively complicated when companies use multiple providers and platforms such as domain registrars and DNS services. If a DNSSEC test turns up an invalid DSKEY, for example, the administrator must choose the specific DNS admin portal to log into to remediate the issue, then copy those keys into a domain registrar system. Multiply this task by hundreds or thousands of domains across multiple DNS providers and change management becomes a time-consuming and costly nightmare. It is simply not going to be done. The only solution is to consolidate to a single domain registrar and DNS provider that integrate DNSSEC support.

4. Adopt unified control systems to address change management

Instead of using multiple, disconnected administrative systems for domains, and DNS-related tasks, implement a unified change management system that integrates domain registration and DNS management under a single, secure management interface. When you do, ensure that DNSSEC and other DNS security measures are included in the change management controls of the system. An integrated, end-to-end management suite offers a single source of truth for all elements and a centralized management hub.

DNSSEC is a highly recommended DNS security measure because it authenticates DNS queries, effectively preventing DNS hijacking and cache poisoning. Effective DNSSEC deployment demands efficient DNS management.



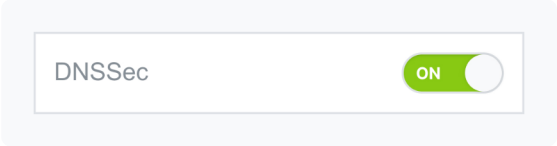
© 2021 Authentic Web Inc. All rights reserved.

1.855.436.8853 | info@authenticweb.com

A systems-based approach to successful DNSSEC implementation and management

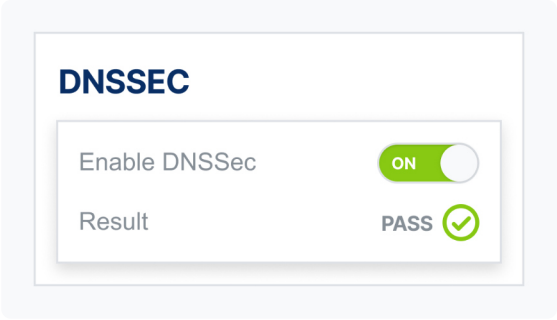
DNSSEC should be as easy to implement as opening any domain record in a secure, administration portal and clicking a toggle button and let the automation do the work.

The system creates the DS Keys and RRSIGs on the DNS and copies them to the TLD Registry.
DONE! You're compliant!



One year later...

A DNSSEC monitor gives the result. You don't need to know the details. You just need to know everything is A-OK and compliant.
DONE! You're still compliant!



Summary

An automated domain and DNS change management system should not only seamlessly activate DNSSEC (and all other essential DNS security measures), it should also:

- Manage and monitor signing key expiry dates and rollovers
- Monitor DNSSEC settings with scheduled scans, to report problems for remediation
- Log all administrative change and system changes in a tamper-proof audit record
- Report all changes via alerts and digests to an authorized hierarchy

Only a systems-based approach can eliminate the manual and error-prone processes that have made effective DNSSEC implementation so difficult for most organizations.

When you're ready to streamline your DNS and domain management with a platform that supports DNSSEC and other security controls, reach out to our team. We can help you discover the security and management gaps and issues within your own organization and work with you to apply system controls to protect your brand and keep your customers safe.

Learn more

Contact us to learn how easy DNS security can be with a control system to keep your brand secure and customers safe.

authenticweb.com
info@authenticweb.com | NA: 1-855-436-8853 | INT: +1-416-583-3770

©Authentic Web Inc. 2021. All rights reserved