DNSSEC Resolver Test

This test determines whether your DNS resolver validates DNSSEC signatures. For this test you need JavaScript turned on.

Yes, your DNS resolver validates DNSSEC signatures.

Most people will experience a negative test result (no DNSSEC validation) – that's ok and no reason to panic.

Help Us

Point your friends to this webpage to help us measure the spread of DNSSEC validation.

If you are operating a website and would like to help us, consider adding our hidden DNSSEC test.

DNSSEC for Users

Few operating systems support DNSSEC validation out of the box. You can install Dnssec-Trigger to run your own validating resolver (more information). Keep in mind that web browsers do not distinguish between DNSSEC validation failures and general DNS failures (there is no security warning like with SSL/TLS errors).

To re-run the above test, you also need to:

- Flush the DNS cache of your OS (Windows: `ipconfig /flushdns`)
- Restart browser or clear browser cache

DNSSEC for DNS Cache Operators

If you're running a recursive DNS cache, follow these steps to enable DNSSEC validation on BIND or Unbound.

BIND

1. Add to options section in your named.conf:
   - BIND ≥ 9.8:
     - `dnssec-enable yes;`
     - `dnssec-validation auto;`
   - BIND ≤ 9.7:
     - `dnssec-enable yes;`
     - `dnssec-validation yes;`
2. Add root KSK as trust anchor (outside options sections):
   - BIND ≥ 9.8: not necessary, trust-anchor is built-in
   - BIND 9.7:
     ```
     managed-keys { "." initial-key 257 3 8
     "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
     FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
     bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
     X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
     W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
     Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0="; };
     ```
   - BIND ≤ 9.6:
     ```
     trusted-keys { "." 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
     FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
     bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
     ```

```
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0="; };
```

3. If you're using forwarders, either remove them or make sure they support EDNS0 and DNSSEC (validation can remain disabled on them)
4. `rndc reload`

Unbound

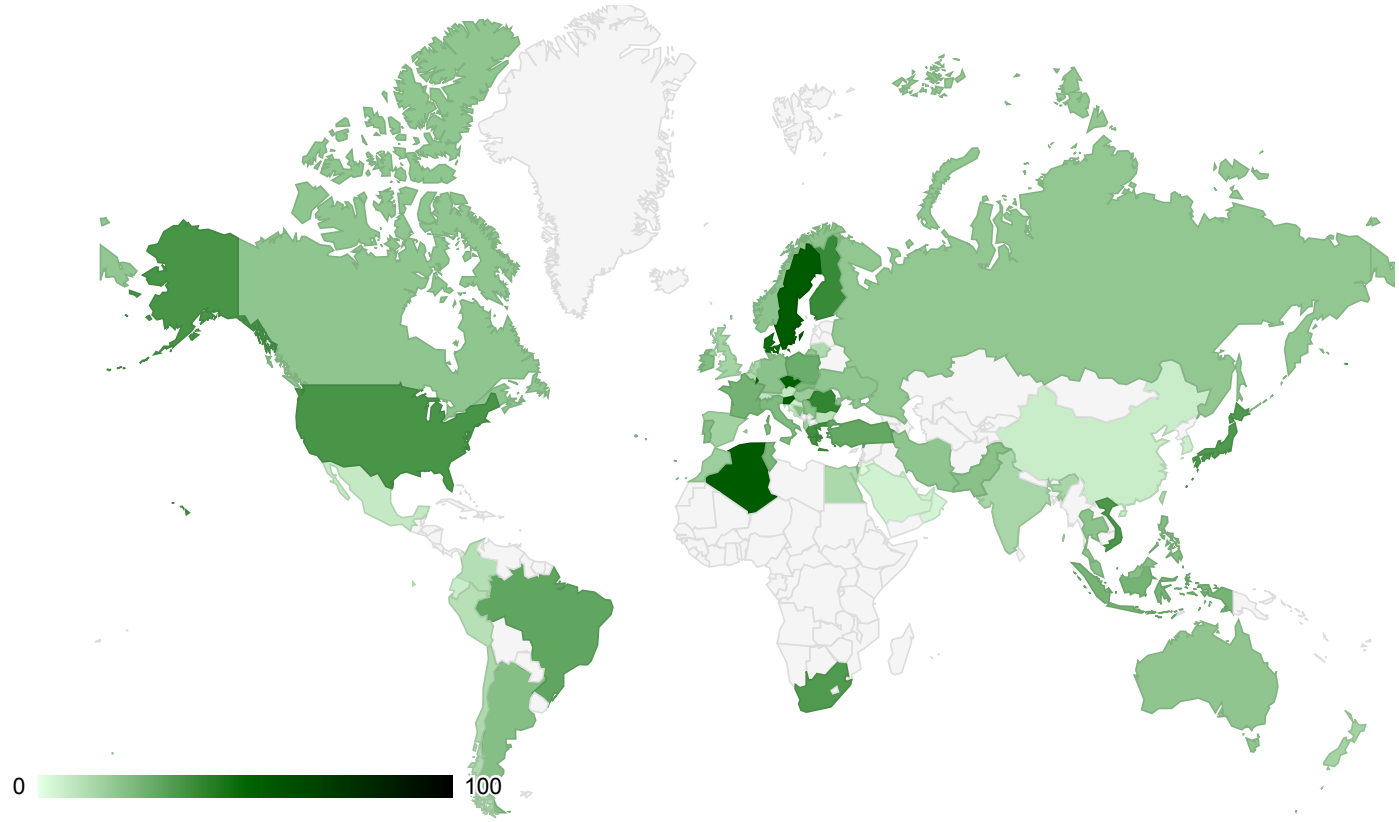
1. Add root KSK as trust-anchor:
   - Unbound ≥ 1.4.7: `unbound-anchor -a /etc/unbound/root.key`
   - Unbound ≤ 1.4.6:
     - `echo ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5" > /etc/unbound/root.key`
     - Make sure you pasted the same fingerprint that is published by iana.org
2. `chown unbound.unbound /etc/unbound/root.key`
3. Add to unbound.conf: `auto-trust-anchor-file "/etc/unbound/root.key"`
4. If you're using forwarders, either remove them or make sure they support EDNS0 and DNSSEC (validation can remain disabled on them)
5. `unbound-control reload`

Test validation

- `dig sigok.verteiltesysteme.net @127.0.0.1` (should return A record)
- `dig sigfail.verteiltesysteme.net @127.0.0.1` (should return SERVFAIL)

Results

- [2013-03-19] Presentation (HTML5), PDF (2.3 MB), Passive and Active Measurement Conference (PAM), Hong Kong.
- [2012-12-17] Paper (PDF), published in the Proceedings of the 2013 Passive and Active Measurement Conference (PAM).
- [2012-10-14] Presentation (HTML5), PDF (1.4 MB), DNS-OARC Workshop, Toronto.



Export SVG

Map shows ratio of validating clients per country, collected from October 2014 to March 2015. Some older result sets of the measurement (anonymized) are available for public download.

Other Tests

These tests use slightly different mechanics. Most users should get the same result on all tests, but in some cases there may be discrepancies. If you get different results, drop us a note with your IP address and we'll be glad to analyze our logs.

- www.dnssec-or-not.com: online test by VeriSign (no JavaScript required)
- validator-search.verisignlabs.com: hidden test by VeriSign with statistics
- dnssectest.sidn.nl: online test by SIDN (with JavaScript)
- www.dnssec-failed.org: webpage with bogus signature by Comcast (will not open at all if you are using DNSSEC)

Acknowledgements

Thanks to Jan-Piet, Zekah and Stefan for providing valuable feedback.

Contact

Matthäus Wander <matthaeus.wander(at)uni-due.de>