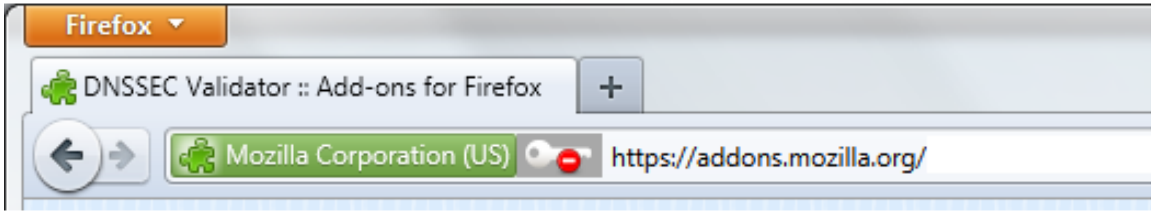
Today

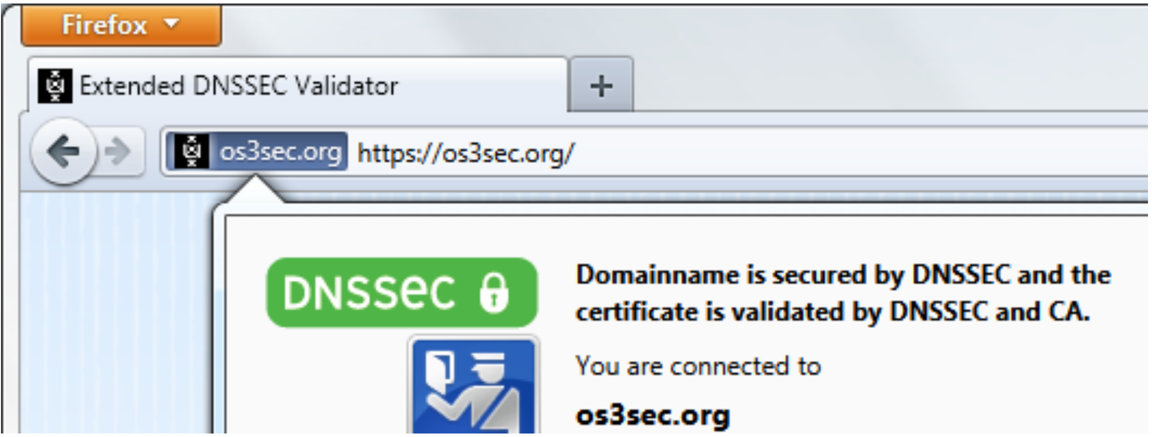
- No explicit support in our core platform
- The OS resolver enforces DNSSEC policy, if any
- Third-party add-ons provide interesting but imperfect of support for DNSSEC now

Example Add-ons

DNSSEC Validator
by CZ.NIC Labs


Firefox
DNSSEC Validator :: Add-ons for Firefox
+
Mozilla Corporation (US)
https://addons.mozilla.org/

Extended DNSSEC Validator by University of Amsterdam System and Network Engineering Students



Domainname is secured by DNSSEC and the certificate is validated by DNSSEC and CA.

You are connected to

os3sec.org

Benefits for Mozilla's Users

- Prevent Certificate Mis-issuance: DANE & CAA
- Email: DKIM, SPF, auto-configuration
- Performance: DANE and Prefetching
- Cross-Protocol Strict Transport Security (HSTS)
- Avoid TLS downgrade

Challenges

- We would need to ship a high-quality, cross-platform, DNSSEC-aware resolver to fully support DNSSEC
- False Negatives: Expiration, Mangling-in-the-Middle
- False Assurance: Key management too difficult?
- Supporting DNSSEC cannot break non-DNSSEC sites
- "It works in my other browser"
- DNSSEC must not slow us down

What to tell the user?

- DNSSEC Validated != “Everything’s Good!”
- Too nuanced: “The site…DNSSEC…but not encrypted to prevent eavesdropping…”
- Which DNSSEC problems are bad enough to break the website? Which problems can we ignore?
- Low and/or poor DNSSEC deployment may mean we couldn’t tell the user anything useful for a long time

Future Support

- Who is building Firefox add-ons supporting DNSSEC?
- What can Mozilla do to help people prototype DNSSEC features?
- Third-party prototypes will influence our future built-in support of DNSSEC
- Email us: **bsmith@mozilla.com**; **lucas@mozilla.com**