

The internet has trust issues

About us

- Thijs Alkemade
- Security Specialist
- talkemade@computest.nl / @xnyhps

Christiaan Ottow

- Security Coach
- <u>cottow@computest.nl</u> / @cottow







Performance



Security

Test Automation





https://www.computest.nl/blog/startencrypt-considered-harmful-today/





Domain Validation Organization Validation Extended Validation





Certificate

www.pine.nl

Issued by: thawte Extended Validation SHA256 SSL CA

This certificate is valid



Subject Name	
oubject nume	
Inc. Country	NL
Business Category	Private Organization
Serial Number	55116183
Country	NL
State/Province	Zuid-Holland
Locality	's-Gravenhage
Organization	Pine Digital Security B.V.
Organizational Unit	Security
Common Name	www.pine.nl



Expires: Tuesday 14 November 2017 at 00 h 59 min 59 s Central European Standard Time



Domain Validation

1. WHOIS/registrar data 2. {admin, administrator, webmaster, hostmaster, postmaster} @example.com 3. Edit website on example.com



4. "Any other method which is just as secure."





How much control do you need to get a certificate?





The file and it's content should be as follows: http://yourdomain.com/<Upper case value of MD5 hash of CSR>.txt

Content (as a plain text file):

<Value of SHA1 hash of CSR> comodoca.com

Note: The DCV will fail if any redirection is in place.











<user>.github.io/<file>

bit.ly/<token>

<user>.s3.amazonaws.com/<key>











































Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5) Parameters none

Not Valid Before

Sunday 20 December 2015 at 02 h 27 min 28 s Central European Standard Time Not Valid After Thursday 29 December 2016 at 17 h 00 min 00 s Central European Standard Time







Timeline of events

- 23/6 report of issue
- 29/6 StartSSL confirms fix
- **30/6** Computest publishes findings
- ~2/7 StartEncrypt API offline
- 2/7 Google asks for details
- ~4/7 Product suspended
- 24/8 Mozilla opens discussion







Who should intervene if a CA misbehaves?



Mailinglist discussion

- Long list of issues at https://wiki.mozilla.org/CA:WoSign_Issues •
- WoSign improvements •
 - Publish everything to CT, from 2015
 - Always include SCT after July 5, 2016
- Central questions: •
 - Which incidents are CA/Bf BR violations? •
 - How do we punish a CA for those?





Sanctions

- Remove the CA •
- Actively distrust the CA •
- Remove the CA, whitelisting previously issued certs
 - How do we ship the whitelist? Too large
- Distrust certs without CT information.
- Distrust certs without CT information. Whitelist certs before 2016
 - See above, issues with whitelist





Scenarios

- WoSign is removed
 - Continues to issue certs because of cross-signing
 Doesn't solve security implications
- WoSign is distrusted
 - Continues to issue certs under StartCom CA
- WoSign and StartCom are removed
 - Continues to issue certs because of cross-signing



WoSign is distrusted for C != CN

- WoSign is distrusted for CN != *.cn
 - All browsers need to be patched
- WoSign dramatically improves
 - Difficult to prove
- WoSign and StartCom are distrusted
 - Business goes bankrupt



How to minimize risk

1. Blacklist /.well-known/pki-validation/ 2. Reserve {admin, administrator, webmaster, hostmaster, postmaster}@example.com 3. Protect TXT/CAA DNS records









Cheers



