The internet has trust issues
About us

Thijs Alkemade

• Security Specialist
• talkemade@computest.nl / @xnyhps

Christiaan Ottow

• Security Coach
• cottow@computest.nl / @cottow
Performance

Security

Test Automation
SECURITY WILL RETURN IN 5 MINUTES

https://www.computest.nl/blog/startencrypt-considered-harmful-today/
Domain Validation
Organization Validation
Extended Validation
www.pine.nl
Issued by: thawte Extended Validation SHA256 SSL CA
Expires: Tuesday 14 November 2017 at 00 h 59 min 59 s Central European Standard Time
✔ This certificate is valid

Trust

Details

<table>
<thead>
<tr>
<th>Subject Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inc. Country</td>
<td>NL</td>
</tr>
<tr>
<td>Business Category</td>
<td>Private Organization</td>
</tr>
<tr>
<td>Serial Number</td>
<td>55116183</td>
</tr>
<tr>
<td>Country</td>
<td>NL</td>
</tr>
<tr>
<td>State/Province</td>
<td>Zuid-Holland</td>
</tr>
<tr>
<td>Locality</td>
<td>'s-Gravenhage</td>
</tr>
<tr>
<td>Organization</td>
<td>Pine Digital Security B.V.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>Security</td>
</tr>
<tr>
<td>Common Name</td>
<td><a href="http://www.pine.nl">www.pine.nl</a></td>
</tr>
</tbody>
</table>
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/\(<\text{Upper case value of MD5 hash of CSR}\).txt

Content (as a plain text file):

\(<\text{Value of SHA1 hash of CSR}\>
comodoca.com

**Note:** The DCV will fail if any redirection is in place.
- GitHub: <user>.github.io/<file>
- bitly: bit.ly/<token>
- Amazon S3: <user>.s3.amazonaws.com/<key>
I want a cert for example.com

Okay, put abc on example.com/cde

Put abc on example.com/cde

Done

GET example.com/cde

abc

Good, here's a cert
Client

I want a cert for example.com

StartCom

Okay, put abc on example.com

example.com

Upload abc

GET /uploads/abc

abc

Done, it’s on /uploads/abc

Good, here’s a cert
I want a cert for example.com

Okay, put abc on example.com

Put abc on attacker.com

Done, it's on /?redir=attacker.com/abc

GET /?redir=attacker.com/abc

Location: attacker.com/abc

GET /abc

abc

Good, here's a cert
Signature Algorithm: SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters: none
Not Valid Before: Sunday 20 December 2015 at 02h 27 min 28 s Central European Standard Time
Not Valid After: Thursday 29 December 2016 at 17h 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

- 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

- **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**
  - Doesn’t solve security implications

- **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