Sinn und Unsinn von SSL

Walter Ebert

PHP Usergroup Frankfurt

18.09.2014

https://www.flickr.com/photos/vonderauvisuals/9778832892

Mehr Sicherheit

Mehr Sicherheit

Mehr besser?

Providing Transport Layer Protection with SSL/TLS

Benefits

The primary benefit of transport layer security is the protection of web application data from unauthorized disclosure and modification when it is transmitted between clients (web browsers) and the web application server, and between the web application server and back end and other non-browser based enterprise components.

The server validation component of TLS provides authentication of the server to the client. If configured to require client side certificates, TLS can also play a role in client authentication to the server. However, in practice client side certificates are not often used in lieu of username and password based authentication models for clients.

TLS also provides two additional benefits that are commonly overlooked; integrity guarantees and replay prevention. A TLS stream of communication contains built-in controls to prevent tampering with any portion of the encrypted data. In addition, controls are also built-in to prevent a captured stream of TLS data from being replayed at a later time.

It should be noted that TLS provides the above guarantees to data during transmission. TLS does not offer any of these security benefits to data that is at rest. Therefore appropriate security controls must be added to protect data while at rest within the application or within data stores.

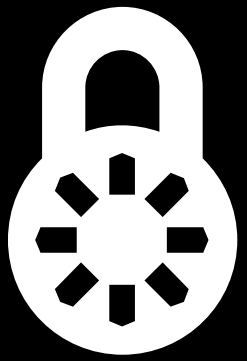
Basic Requirements

The basic requirements for using TLS are: access to a Public Key Infrastructure (PKI) in order to obtain certificates, access to a directory or an Online Certificate Status Protocol (OCSP) responder in order to check certificate revocation status, and agreement/ability to support a minimum configuration of protocol versions and protocol options for each version.

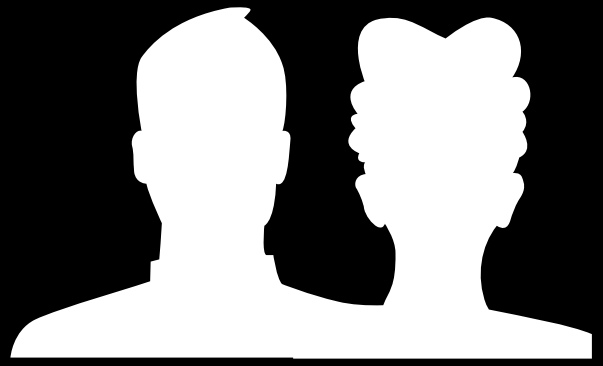
SSL vs. TLS

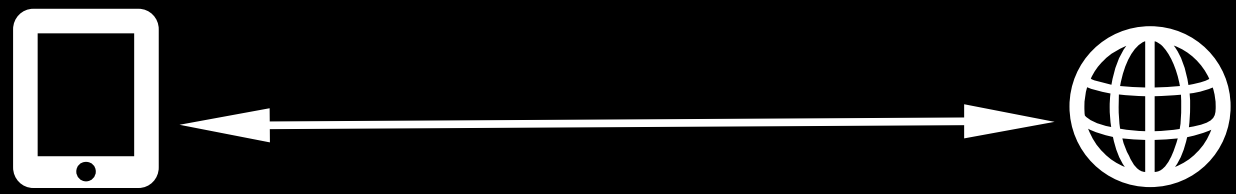
The terms, Secure Socket Layer (SSL) and Transport Layer Security (TLS) are often used interchangeably. In fact, SSL v3.1 is equivalent to TLS v1.0. However, different versions of SSL and TLS are supported by modern web browsers and by most modern web frameworks and platforms. For the purposes of this cheat sheet we will refer to the technology generically as TLS. Recommendations regarding the use of SSL and TLS protocols, as well as browser support for TLS, can be found in the rule below titled "Only Support Strong Protocols".

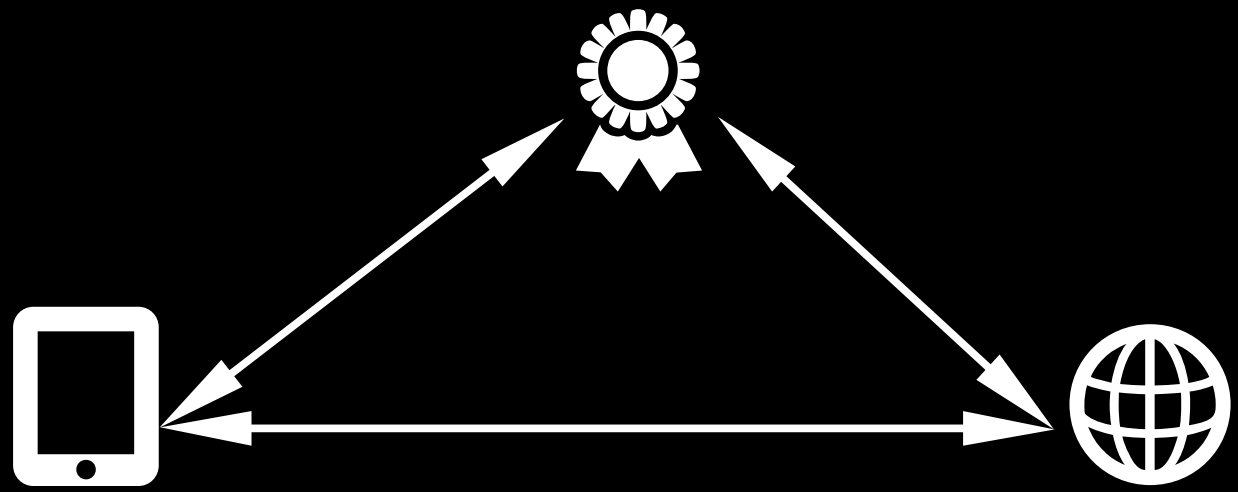
Verschlüsselung



Identitätsprüfung







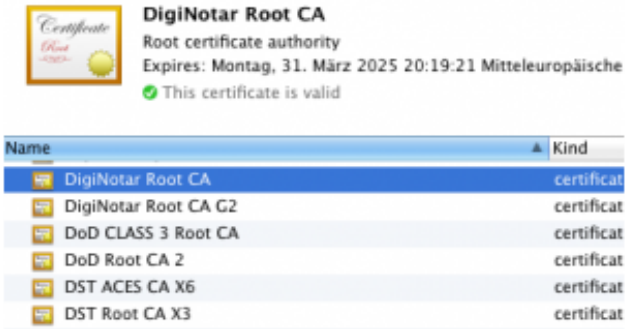
SSL-VORFALL

Gefälschtes Google-Zertifikat seit Mitte Juli 2011 im Umlauf

Der jüngste SSL-Vorfall hat weitreichende Konsequenzen. Mit einem gefälschten Google-Zertifikat sind Man-in-the-Middle-Angriffe auf Google-Nutzer möglich. Microsoft und Mozilla reagieren mit drastischen Schritten und entziehen der Ausgabestelle des gefälschten Zertifikats ihr Vertrauen.

Diginotar hat ein gefälschtes Zertifikat in Umlauf gebracht, das alle Subdomains von google.com betrifft. Das berichten übereinstimmend Microsoft im Security Advisory 2607712 und Mozilla in seinem Security-Blog. Auch Google bestätigt den Vorfall. Laut Mozilla hat Diginotar das Zertifikat mittlerweile widerrufen. Da es aber bereits benutzt wurde, kann davon ausgegangen werden, dass es inzwischen Geschädigte gibt.

Nutzer von Windows Vista und 7 sowie den darauf aufbauenden Servervarianten werden mittlerweile automatisch geschützt, sofern die Zertifikatsüberprüfung durch Windows-Komponenten durchgeführt wird. Microsoft hat gleich das Diginotar-Root-Zertifikat von der Certificate Trust List entfernt. Für Windows XP und Windows Server 2003 wird es einen Patch geben.



Diginotar-Zertifikat unter Mac OS X (Bild: Golem.de)

Artikel: SSL-VORFALL
Gefälschtes Google-Zertifikat seit Mitte Juli 2011 im Umlauf

Inhalt:
- Diginotars zu erwartende Verluste ohne Tragweite

Datum: 30.8.2011, 18:33

Autor: Andreas Sebayang

Themen: Security, Diginotar, EFF, HSTS, SSL, Google, Internet

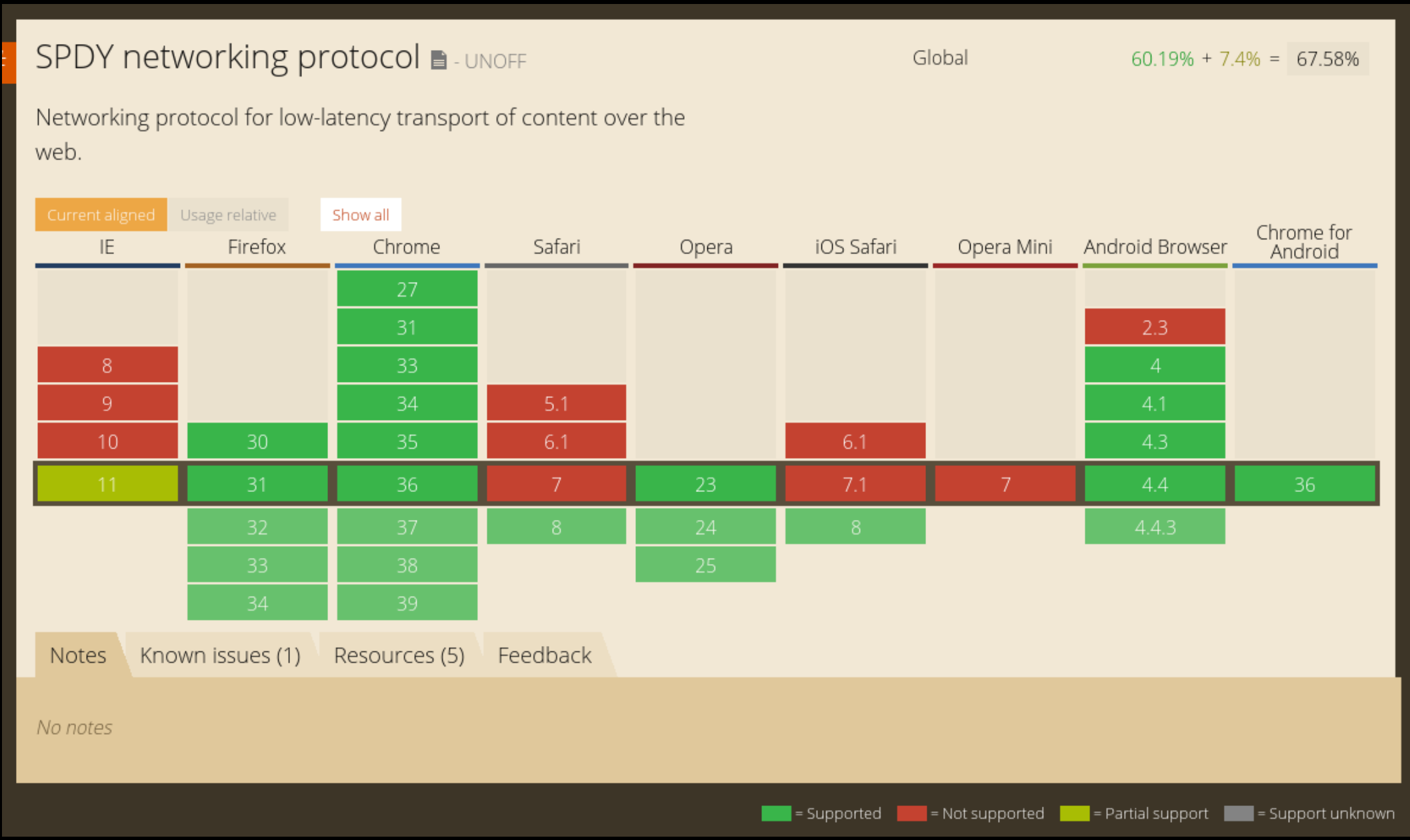
Teilen: 0 22 24 6

Tools: Drucken

Google I/O 2014: HTTPS Everywhere

„Data delivered over an unencrypted channel is insecure, untrustworthy, and trivially intercepted. We must protect the security, **privacy**, and integrity of our users data. In this session we will take a hands-on tour of how to make your websites secure by default: the required technology, configuration and performance best practices, how to migrate your sites to HTTPS and make them user and search friendly, and more. Your users will thank you.“

https://www.youtube.com/watch?v=cBhZ6SoPFCY



https://developers.google.com/speed/spdy/
http://caniuse.com/#feat=spdy

Mark Nottingham
@mnot

Folgen

HTTP/2.0 will only work for https:// URIs -- part of @ietf response to pervasive monitoring. lists.w3.org/Archives/Publi...

Antworten Retweeten Favorisieren ••• Mehr

RETWEETS	FAVORITEN
219	62

02:04 - 13. Nov. 2013

Verwandte Schlagzeilen

Snowden's legacy: The open web could soon be encrypted by default
Gigaom @gigaom

Ivan Ristic @ivanristic · 13. Nov.
@mnot Any thoughts on opportunistic encryption for HTTP/1.1, though? (I sent you that email you asked for.)

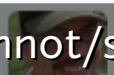
Antworten Retweeten Favorisieren ••• Mehr

M.Nafees Sharif Butt @mnsbutt · 13. Nov.
@mnot @ietf How does this effect web services' deployments. So SOAP/HTTP and JSON will be made secure if used with HTTP 2, is that so?

Antworten Retweeten Favorisieren ••• Mehr

Jon Gretar @JonGretar · 13. Nov.
@mnot didn't they already break the ssl security? There was some israeli 1u box that allowed spying on ssl traffic.

Antworten Retweeten Favorisieren ••• Mehr



Jared Armstrong @jlarmstrong · 13. Nov.
@mnot @mirable What world do we need a spec to force

https://twitter.com/mnot/status/400564763559620608

Google | Webmaster Central Blog

Official news on crawling and indexing sites for the Google index

HTTPS as a ranking signal

Posted: Wednesday, August 06, 2014

Webmaster level: all

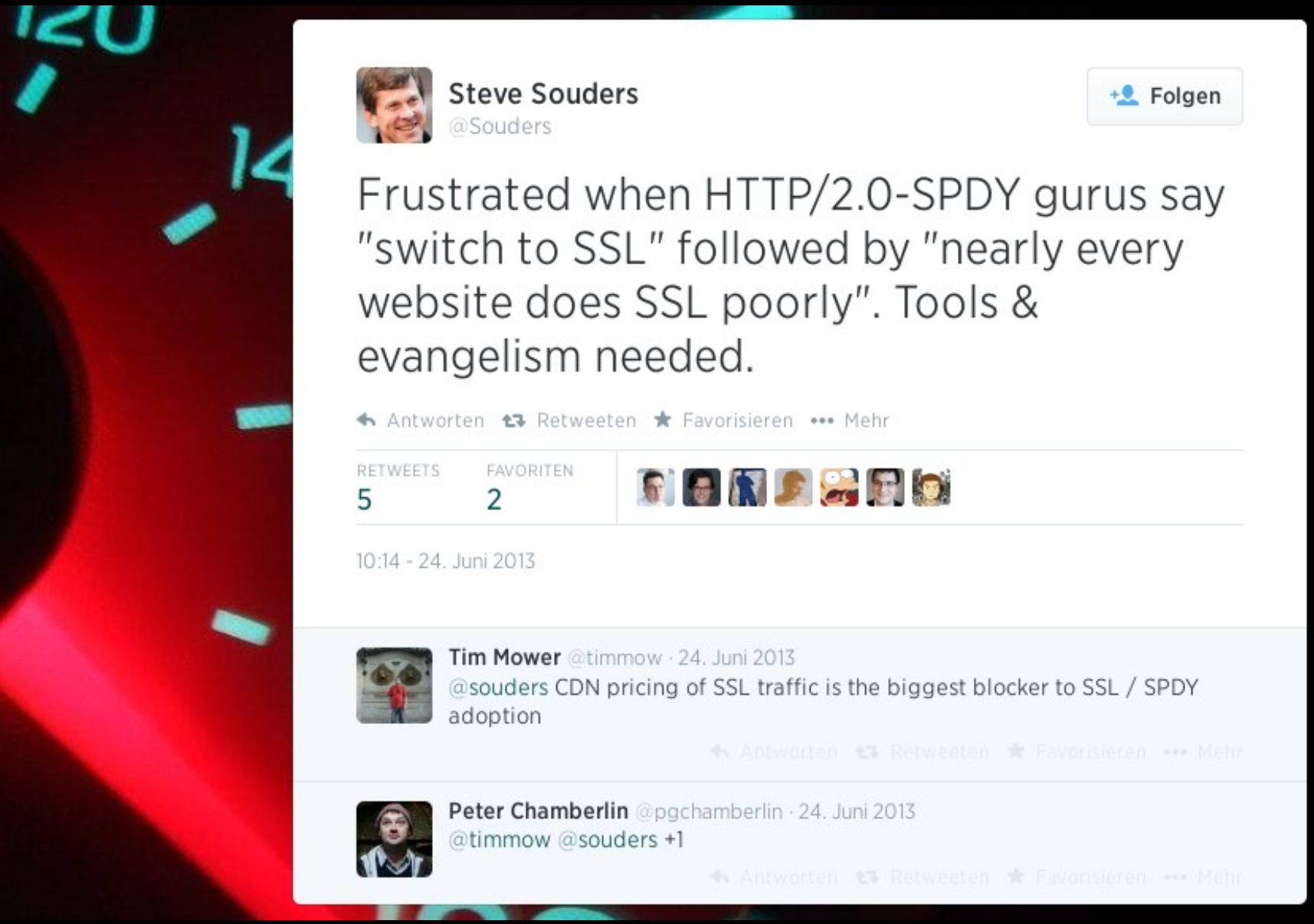
Security is a top priority for Google. We invest a lot in making sure that our services use industry-leading security, like strong HTTPS encryption by default. That means that people using Search, Gmail and Google Drive, for example, automatically have a secure connection to Google.

Beyond our own stuff, we're also working to make the Internet safer more broadly. A big part of that is making sure that websites people access from Google are secure. For instance, we have created resources to help webmasters prevent and fix security breaches on their sites.

We want to go even further. At Google I/O a few months ago, we called for "HTTPS everywhere" on the web.

We've also seen more and more webmasters adopting HTTPS (also known as HTTP over TLS, or Transport Layer Security), on their website, which is encouraging.

For these reasons, over the past few months we've been running tests taking into account whether sites use secure, encrypted connections as a signal in our search ranking algorithms. We've seen positive results, so we're starting to use HTTPS as a ranking signal. For now it's only a very lightweight signal — affecting fewer than 1% of global queries, and carrying less weight than other signals such as high-quality content — while we give webmasters time to switch to HTTPS. But over time, we may decide to strengthen it, because we'd like to



https://twitter.com/Souders/status/349214019070078977

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM | TAKE ACTION | SHOP

HTTPS Everywhere

HTTPS Everywhere

FAQ

Report Bugs / Hack On The Code

Creating HTTPS Everywhere Rulesets

How to Deploy HTTPS Correctly

HTTPS Everywhere Atlas

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

Install in Firefox
Version 4 Stable

Install in

Install in Opera

https://www.eff.org/https-everywhere

Donate to EFF $

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more about what the program is, how it works, and what you can do.

Follow EFF

Bad news for anonymous speech in Brazil: A judge orders no more

Redirect HTTPS traffic for Drupal.org subdomains to HTTP

Posted by walterebert on *December 14, 2012 at 7:14pm*

Visiting https://groups.drupal.org/ returns a HTTP 403 error message: You don't have permission to access / on this server.

I am using the HTTPS Everywhere browser add-on (https://www.eff.org/https-everywhere) that automatically redirects requests to https, if it is available for the given domain. So it would be nice if https://groups.drupal.org/ returns a usable page.

Closed (won't fix)

Project:	Groups.drupal.org
Component:	Other
Priority:	Normal
Category:	Bug report
Assigned:	Unassigned

Log in or register to update this issue

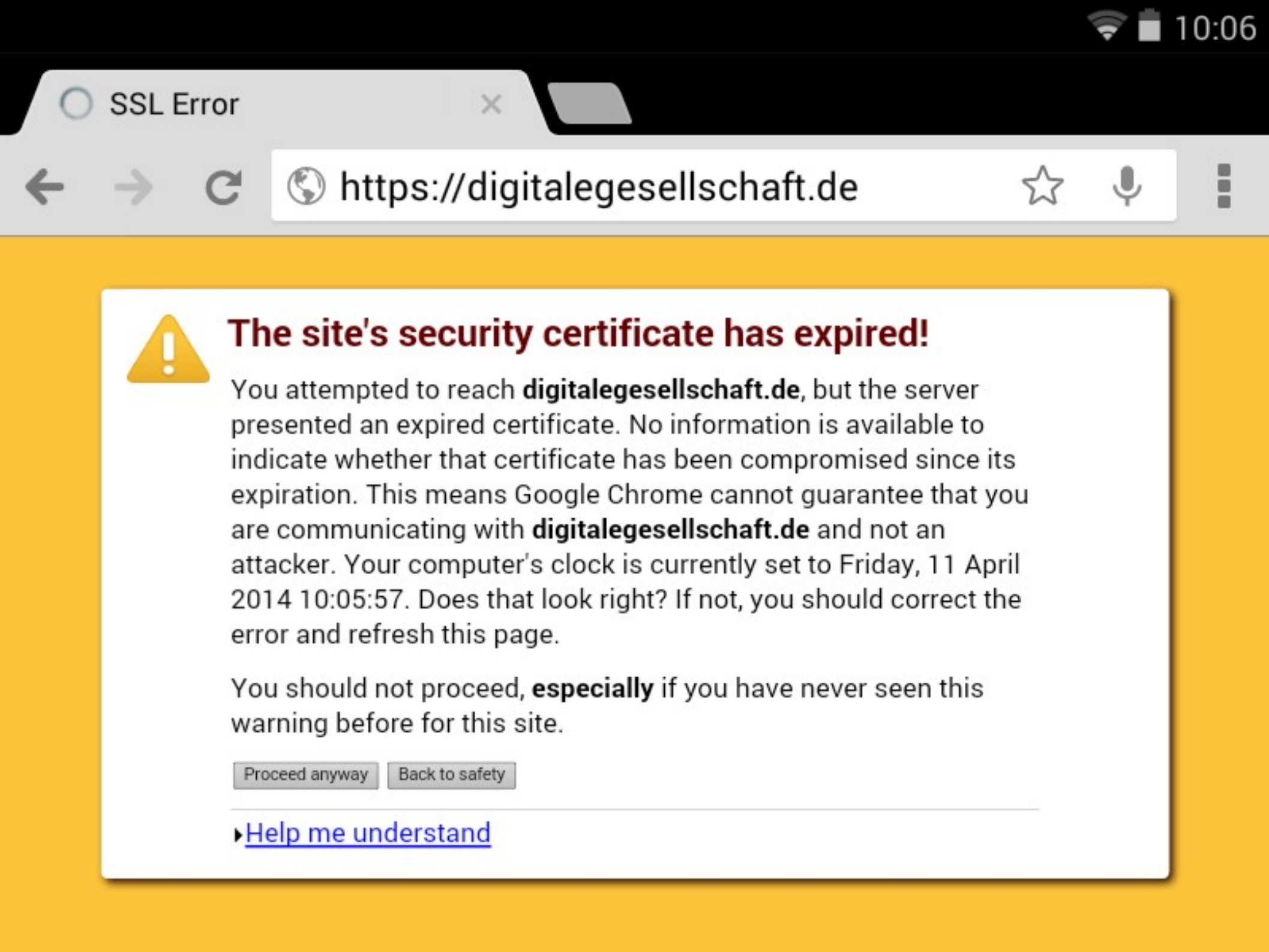
Last updated on *Aug 21, 2014 at 9:00pm*

Comments

erikwebb *commented about a year ago* #1

Title:	groups.drupal.org is not working over SSL	groups.drupal.org returns 403 Forbidden when using HTTPS
Component:	User interface	» Miscellaneous
		» Major

Jump to:
Most recent comment


10:06
SSL Error
https://digitalegesellschaft.de
The site's security certificate has expired!
You attempted to reach digitalegesellschaft.de, but the server presented an expired certificate. No information is available to indicate whether that certificate has been compromised since its expiration. This means Google Chrome cannot guarantee that you are communicating with digitalegesellschaft.de and not an attacker. Your computer's clock is currently set to Friday, 11 April 2014 10:05:57. Does that look right? If not, you should correct the error and refresh this page.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

jQuery
@jquery

Folgen

We have had multiple reports that the SSL certificate for code.jquery.com has expired. We are on it now and will keep you posted.

Antworten Retweeten Favorisieren ••• Mehr

RETWEETS 59 FAVORITEN 12

12:07 - 31. Juli 2014

Daniel Crothers @dancrodev · 31. Juli
@jquery
hey, your SSL certificate for code.jquery.com has expired. You should get on that and keep me posted.

With love.

Antworten Retweeten Favorisieren ••• Mehr

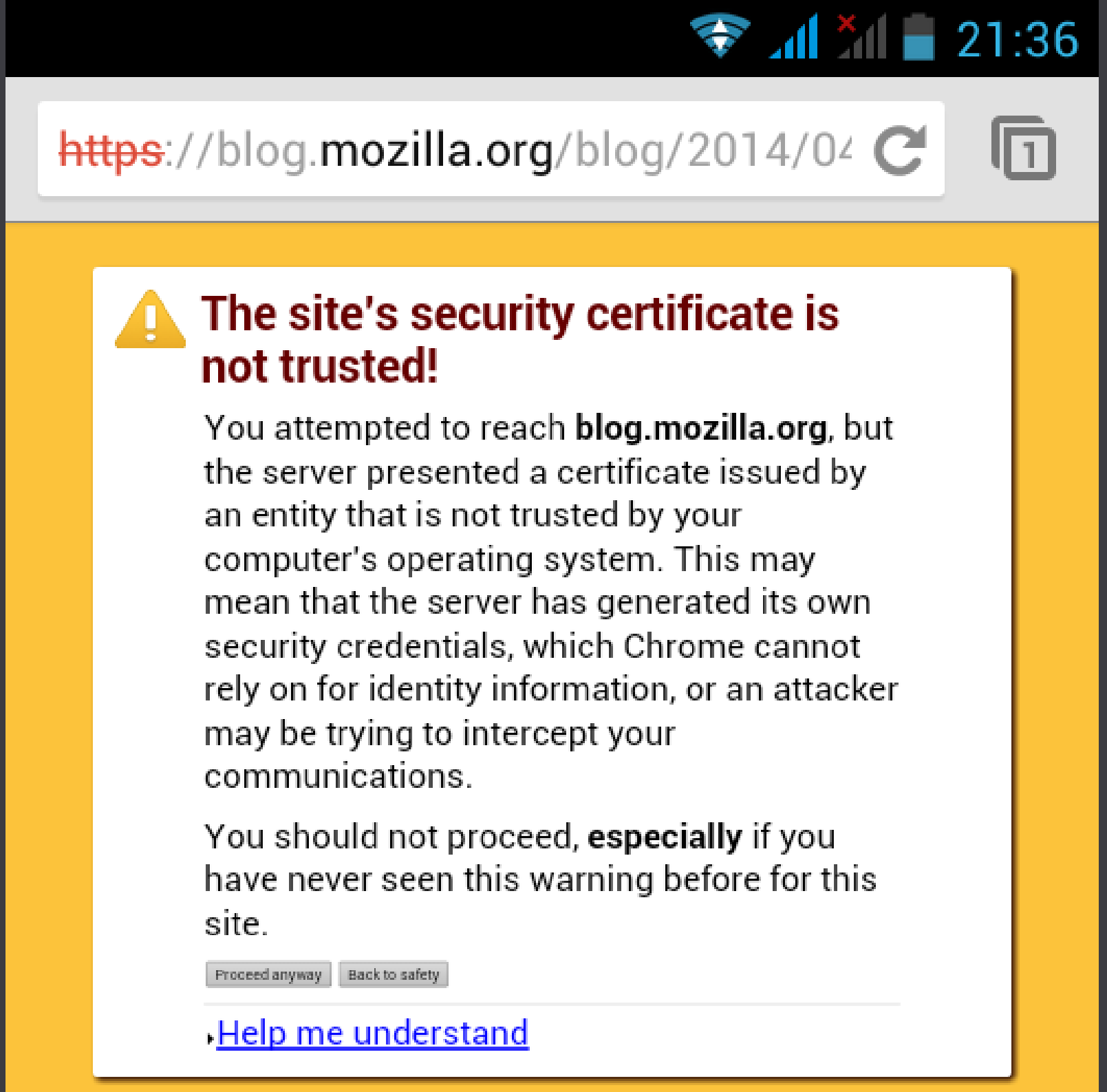
Greg Fazekas @dinchamion · 31. Juli
RT @jquery We have had multiple reports that the SSL certificate for bit.ly/1kp3IGm has expired. We are on it now.

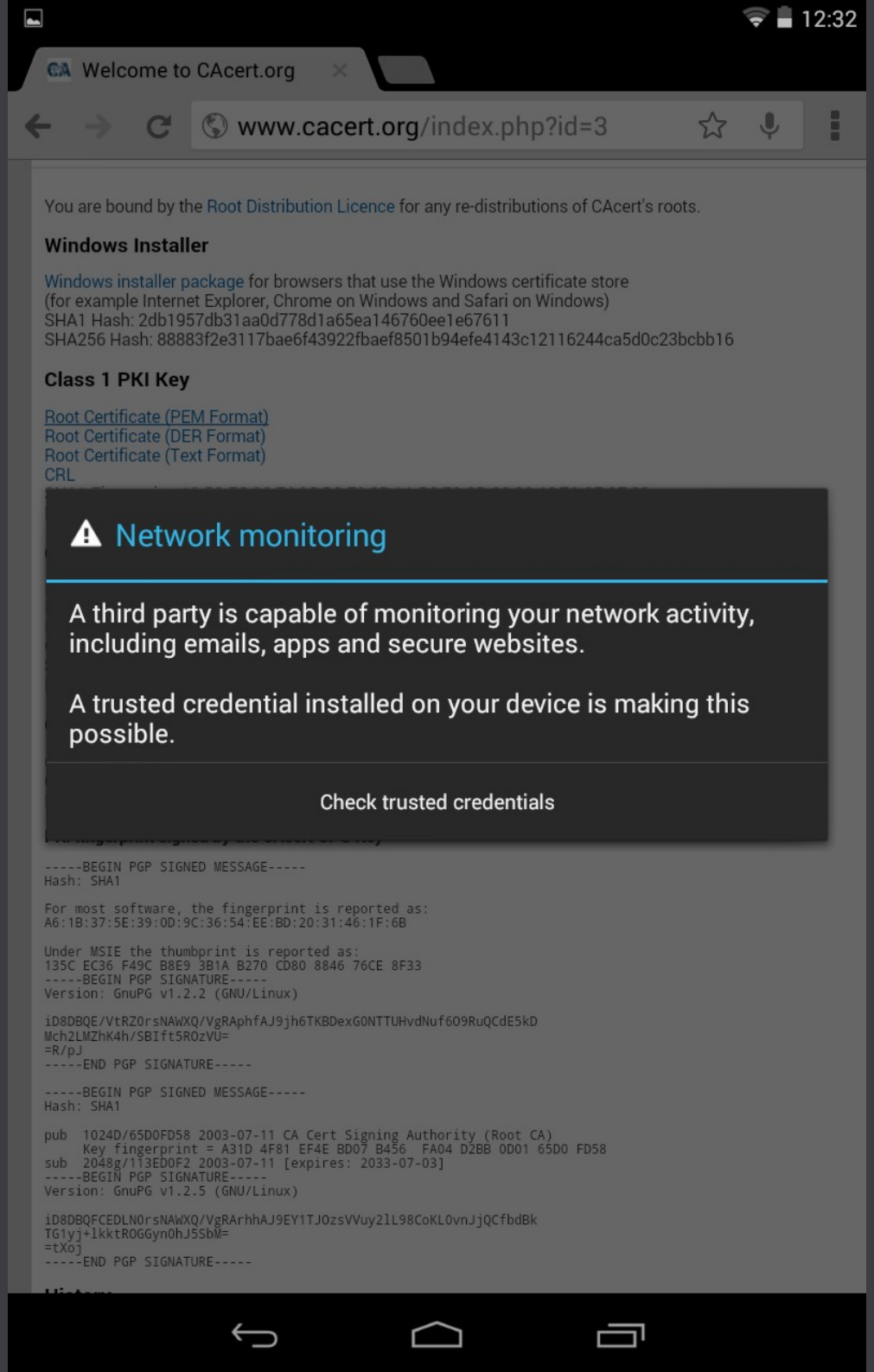
Antworten Retweeten Favorisieren ••• Mehr

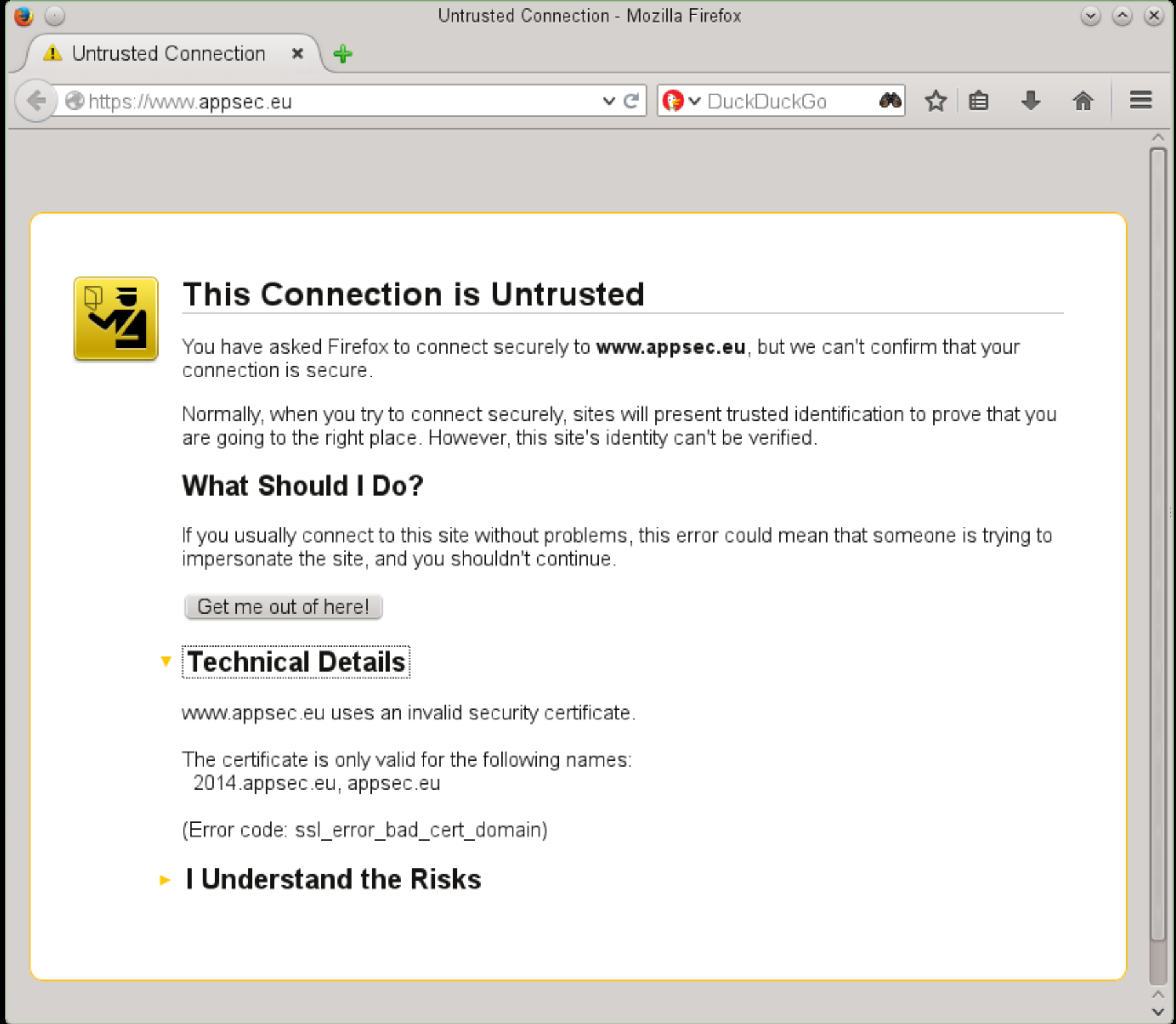
Joshua Frankel @frankelfrankel · 31. Juli
#nerdalert #adjustsglasses MT @jquery SSL certificate for code.jquery.com has expired. We are on it and will keep you posted.

Antworten Retweeten Favorisieren ••• Mehr

https://twitter.com/jquery/status/494922194351181824


21:36
https://blog.mozilla.org/blog/2014/04
The site's security certificate is not trusted!
You attempted to reach blog.mozilla.org, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand


12:32
Welcome to CAcert.org
www.cacert.org/index.php?id=3
You are bound by the Root Distribution Licence for any re-distributions of CAcert's roots.
Windows Installer
Windows installer package for browsers that use the Windows certificate store
(for example Internet Explorer, Chrome on Windows and Safari on Windows)
SHA1 Hash: 2db1957db31aa0d778d1a65ea146760ee1e67611
SHA256 Hash: 88883f2e3117bae6f43922fbaef8501b94efe4143c12116244ca5d0c23bcbb16
Class 1 PKI Key
Root Certificate (PEM Format)
Root Certificate (DER Format)
Root Certificate (Text Format)
CRL
Network monitoring
A third party is capable of monitoring your network activity, including emails, apps and secure websites.
A trusted credential installed on your device is making this possible.
Check trusted credentials
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
For most software, the fingerprint is reported as:
A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B
Under MSIE the thumbprint is reported as:
135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.2 (GNU/Linux)
iD8DBQE/VtRZOrsNAWXQ/VgRAphfAJ9jh6TKBDexGONTTUHvdNuf6O9RuQCdE5kD
Mch2LMZhK4h/SBIft5ROzVU=
=R/pJ
-----END PGP SIGNATURE-----
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
pub 1024D/65D0FD58 2003-07-11 CA Cert Signing Authority (Root CA)
Key fingerprint = A31D 4F81 EF4E BD07 B456 FA04 D2BB 0D01 65D0 FD58
sub 2048g/113ED0F2 2003-07-11 [expires: 2033-07-03]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.5 (GNU/Linux)
iD8DBQFCEDLNOrsNAWXQ/VgRArhhAJ9EY1TJOzsVVuy2lL98CoKLOvnJjQCfbdBk
TG1yj+lkktROGGynOhJ5SbM=
=tXoj
-----END PGP SIGNATURE-----


Untrusted Connection - Mozilla Firefox
Untrusted Connection
https://www.appsec.eu
DuckDuckGo
This Connection is Untrusted
You have asked Firefox to connect securely to www.appsec.eu, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
www.appsec.eu uses an invalid security certificate.
The certificate is only valid for the following names:
2014.appsec.eu, appsec.eu
(Error code: ssl_error_bad_cert_domain)
I Understand the Risks

example.com uses an invalid security certificate.

The certificate is only valid for the following names:
gp1.wac.edgecastcdn.net, wac.edgecastcdn.net, ne.wac.edgecastcdn.net, swf.mixpo.com, cdn.traceregister.com, s.tmocache.com, s.my.tmocache.com, e1.boxcdn.net, e2.boxcdn.net, e3.boxcdn.net, www.sonos.com, static-cache.tp-global.net, ssl-cdn.sometrics.com, cache.vehicleassets.captivelead.com, static.woopra.com, images.ink2.com, assets-secure.razoo.com, ec.pond5.com, images.esellerpro.com, use.typekit.com, static.iseatz.com, static.www.turnto.com, inpath-static.iseatz.com, secure.avelleassets.com, static.dubli.com, www-cdn.cinamuse.com, www-cdn.cineble.com, www-cdn.cinemaden.com, www-cdn.filmlush.com, www-cdn.flixaddict.com, www-cdn.itshd.com, www-cdn.moviease.com, www-cdn.movielush.com, www-cdn.reelhd.com, www-cdn.pushplay.com, cdn1.fishpond.co.nz, cdn1.fishpond.com.au, www.isaca.org, cdn.optimizely.com, static.shoedazzle.com, www.travelrepublic.co.uk, cdn.nprove.com, sslbest.booztx.com, www.travelrepublic.com, www.blacklabelads.com, cdn.whois.com.au, ne1.wac.edgecastcdn.net, gs1.wac.edgecastcdn.net, c1.socialcastcontent.com, www.steepandcheap.com, www.whiskeymilitia.com, www.chainlove.com, www.tramdock.com, www.bonktown.com, www.brociety.com, edgecast.onegrp.com, cdn.psw.net, cdn.gaggle.net, www-cdn.reelvidz.com, fast.fonts.com, ec.xnglobalres.com, images.vrbo.com, beta.fileblaze.net, cdn.brandsexclusive.com.au, www-cdn.ireel.com, cdcssl.ibsrv.net, cdn.betchoice.com, player.vzaar.com, framegrabs.vzaar.com, thumbs.vzaar.com, stylistlounge.stelladot.com, www.stelladot.com, content.aqcdn.com, content.ebgames.com.au, content.ebgames.co.nz, images.pagerage.com, images.allsaints.com, cdnb1.kodakgallery.com, cdn.orbengine.com, cdn.quickoffice.com, content.glscrip.com, cdn.bidfan.com, media.quantumads.com, cdn.allenbrothers.com, pics.intelius.com, pics.peoplelookup.com, pics.lookupanyone.com, cdn1-ssl.iha.com, s.cdn-care.com, cdn2-b.examiner.com, cdn.trtk.net, edgecdn.ink2.com, ec.dstimage.disposolutions.com, cdn.clytel.com, welcome2.carsdirect.com, s1.card-images.com, update.alot.com, www.outsystems.com, www.drwmedia.com, lookup.bluecava.com, cdn.taxact.com, cdn.taxactonline.com, cdn.200581.com, img.vxcdn.com, js.vxcdn.com, www.goal.com, cdns1.kodakgallery.com, edge.dropdowndeals.com, edge.pagerage.com, edge.sanityswitch.com, edge.yontoo.com, layers.yontoo.com, cdn.widgetserver.com, www.cloudwords.com, edge.actaads.com, images.skincarerx.com, ssl.cdn-redfin.com, small.outso-media.com, cdn.foxycart.com,

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

What leaks in practice?

We have tested some of our own services from attacker's perspective. We attacked ourselves from

How to stop the leak?

As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > mayflower.de

SSL Report: [redacted]

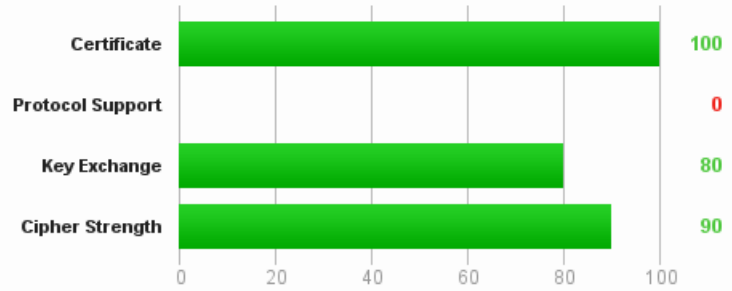
Assessed on: Fri Aug 08 10:29:15 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

F



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, OpenSSL Cookbook and known issues.

Experimental: This server is vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224) and exploitable. Grade set to F.

This server is not vulnerable to the Heartbleed attack.

Authentication

https://www.ssllabs.com/ssltest/

Mixed Content - Mozilla Firefox

Mixed Content

https://walterebert.de/mixed-content/

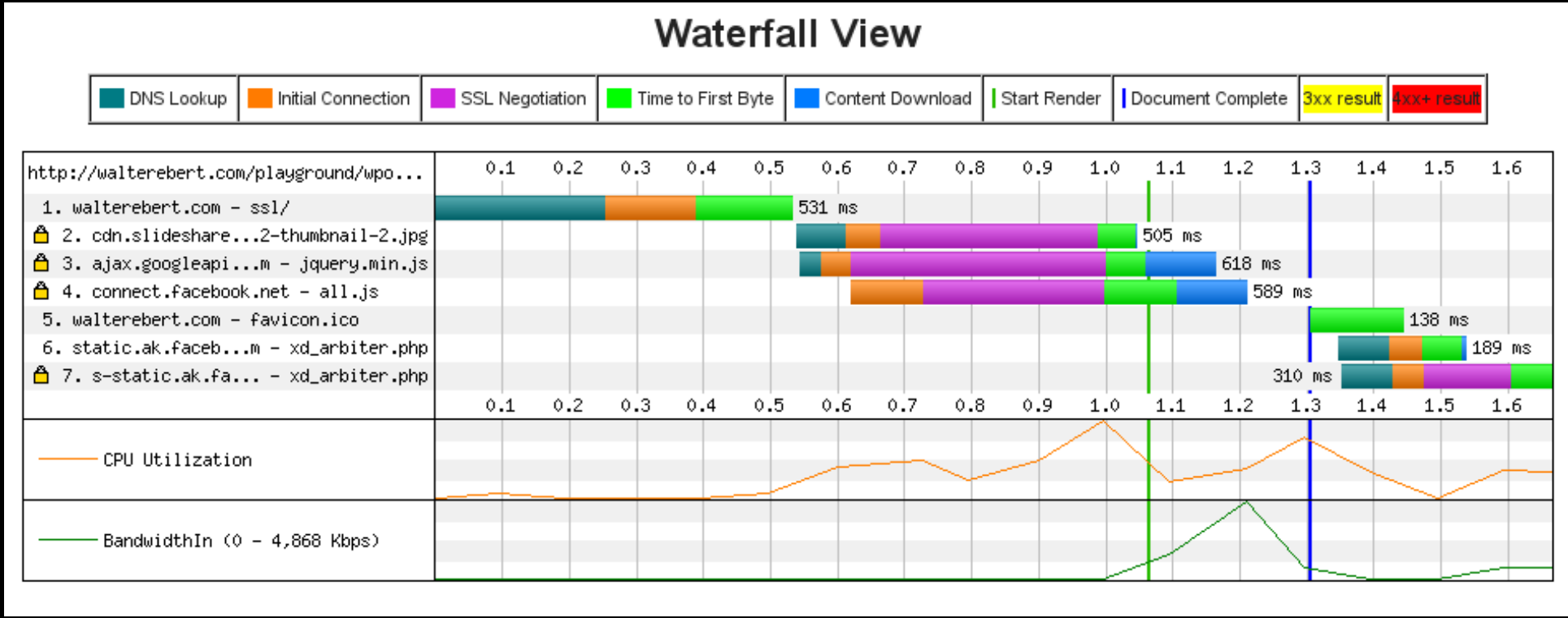
This website does not supply identity information.

The connection to this website is not fully secure because it contains unencrypted elements (such as images).

More Information…

Kontakt

Ladezeiten



http://www.webpagetest.org/result/130616_3E_AoH/1/details/

HTTP(S)

```
<script src="//connect.facebook.net/de_DE/all.js"></script>
```

~~HTTP(S)~~

```
<script src="//connect.facebook.net/de_DE/all.js" async defer></script>
```

https://www.igvita.com/2014/05/20/script-injected-async-scripts-considered-harmful/

Content Security Policy (CSP)

```
# Apache
Header set Content-Security-Policy "default-src https:"

# Nginx
add_header Content-Security-Policy "default-src https:";
```

https://www.owasp.org/index.php/Content_Security_Policy

HTTP Strict Transport Security (HSTS)

```
# Apache
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

# Nginx
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";
```

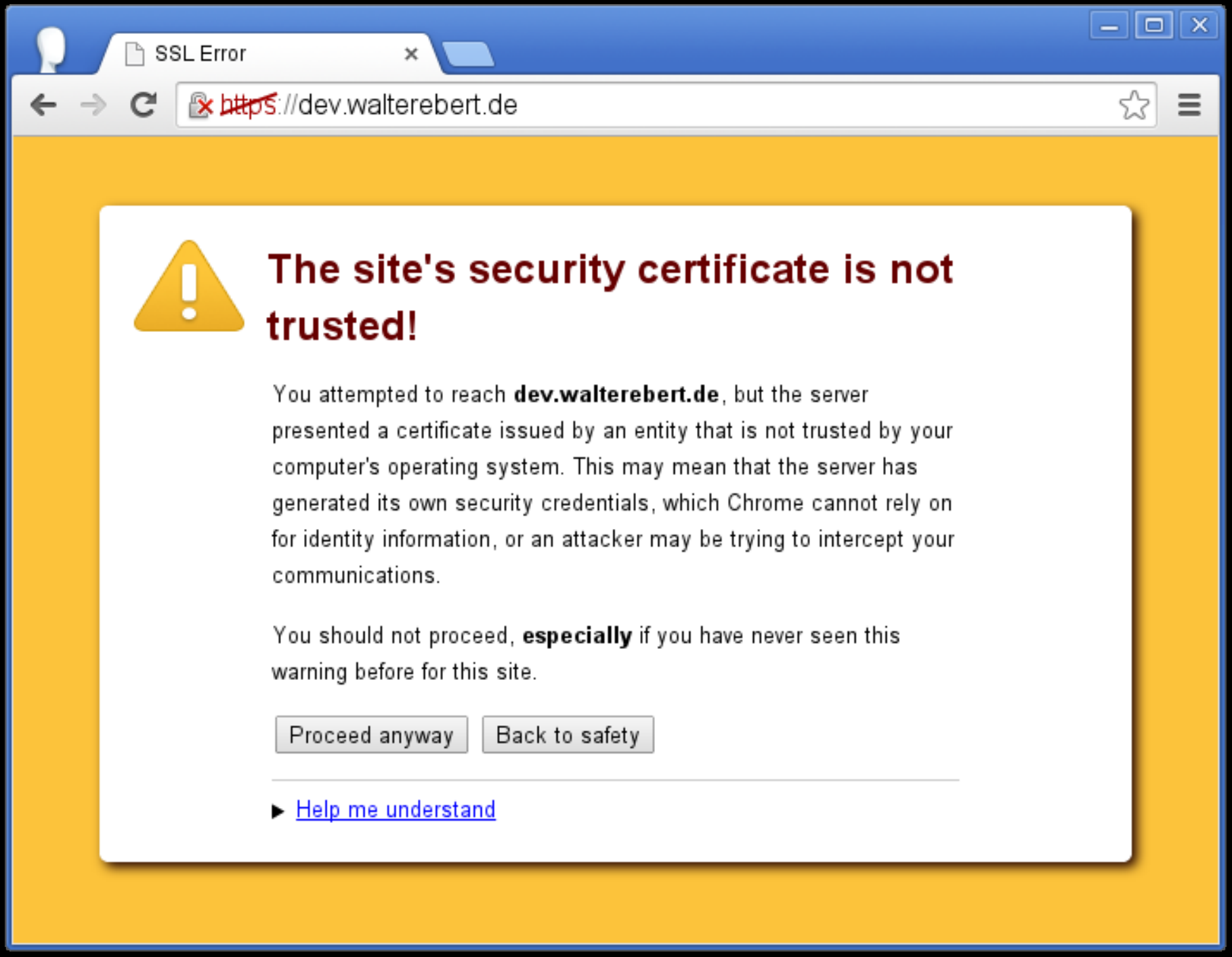
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

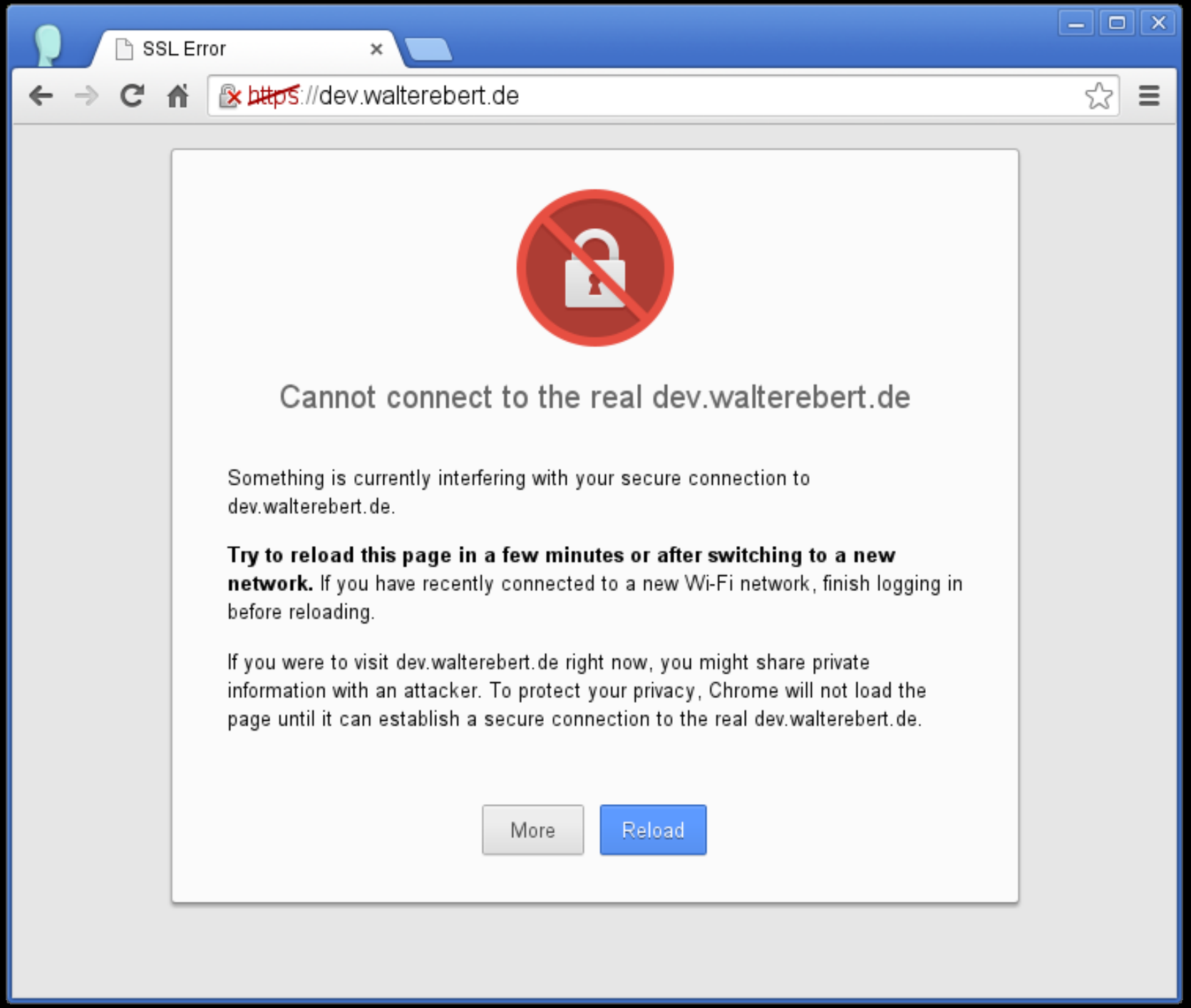
Lokale Entwicklungsumgebung

http://dev.walterebert.de/

→

https://dev.walterebert.de/


SSL Error
https://dev.walterebert.de
The site's security certificate is not trusted!
You attempted to reach dev.walterebert.de, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand


SSL Error
https://dev.walterebert.de
Cannot connect to the real dev.walterebert.de
Something is currently interfering with your secure connection to dev.walterebert.de.
Try to reload this page in a few minutes or after switching to a new network. If you have recently connected to a new Wi-Fi network, finish logging in before reloading.
If you were to visit dev.walterebert.de right now, you might share private information with an attacker. To protect your privacy, Chrome will not load the page until it can establish a secure connection to the real dev.walterebert.de.
More
Reload

HSTS

```
# Apache
Header always set Strict-Transport-Security "max-age=31536000"

# Nginx
add_header Strict-Transport-Security "max-age=31536000";
```

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security#Excessively_Strict_STS

Public Key Pinning

```
Header set Public-Key-Pins "max-age=2592000; \
  pin-sha256=E9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g=; \
  pin-sha256=LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ=; \
  includeSubDomains; \
  report-uri=http://example.com/pkp-report.php"
```

https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

Server Name Indication (SNI)

Mehrere Domains unter einer IP-Adresse

https://de.wikipedia.org/wiki/Server_Name_Indication

Android 2.3

Internet Explorer auf Windows XP

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Jun 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Chrome 36 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Firefox 31 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Jun 2014	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail [3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
OpenSSL 1.0.1h	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 8 / iOS 8.0 Beta R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Yahoo Slurp Jun 2014 No SNI [2]	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128

https://www.ssllabs.com/ssltest/analyze.html?d=walterebert.de&hideResults=on

Nicht nur Browser

Webservices, RSS-Reader, Webcrawler, Monitoring, ...

PHP 5.3.2: Added SNI_enabled and SNI_server_name

```
$ php -r "echo file_get_contents('https://s.walterebert.com/');"

$ php -a
Interactive mode enabled
php > echo file_get_contents("https://s.walterebert.com/");

<?php $client = new SoapClient("some.wsdl");

$ http https://s.walterebert.com/
http: error: SSLError: hostname 's.walterebert.com' doesn't
match either of 'www.walterebert.de', 'walterebert.de'
```

https://www.mnot.net/blog/2014/05/09/if_you_can_read_this_youre_sniing

Fehlermeldung für veraltete Clients

```
SSLStrictSNIVHostCheck on
ErrorDocument 403 "TLS SNI Required."
Listen 443
<VirtualHost *:443>
  ...
  SSLStrictSNIVHostCheck on
  <Directory ...>
    ErrorDocument 403 default
    SSLRequireSSL
    SSLOptions +StrictRequire
  </Directory>
</VirtualHost>
```

https://wiki.apache.org/httpd/NameBasedSSLVHostsWithSNI

Perfect Forward Secrecy

Langzeitschlüssel ▸ Sitzungsschlüssel

https://de.wikipedia.org/wiki/Perfect_Forward_Secrecy
https://community.qualys.com/blogs/securitylabs/2013/08/05/configuring-apache-nginx-and-openssl-for-forward-secrecy

PHP Sessions

```
ini_set('session.cookie_httponly', 1);
ini_set('session.cookie_secure', 1);
```

http://de.php.net/manual/de/session.configuration.php

PHP Cookies

```
setcookie(
  $name,
  $value,
  0, // expire
  '/',
  '', // domain
  true, // secure
  true // httponly
);
```

http://de.php.net/manual/de/function.setcookie.php

PHP cURL

```
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_USERAGENT, 'PHP ' . PHP_VERSION);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$data = curl_exec($ch);
curl_close($ch);
```

http://de.php.net/manual/de/book.curl.php

PHP cURL

```
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_USERAGENT, 'PHP ' . PHP_VERSION);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
$data = curl_exec($ch);
curl_close($ch);
```

:-S

http://de.php.net/manual/de/function.curl-setopt.php

PHP cURL

```
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_USERAGENT, 'PHP ' . PHP_VERSION);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, true);
curl_setopt($ch, CURLOPT_CAINFO, '/etc/ssl/ca-bundle.pem');
$data = curl_exec($ch);
curl_close($ch);
```

http://de.php.net/manual/de/function.curl-setopt.php

PHP Streams

```
$uri = 'https://walterebert.de/';
$ctx = stream_context_create(array('ssl' => array(
    'verify_peer' => true,
    'cafile' => '/etc/ssl/ca-bundle.pem',
    'CN_match' => 'walterebert.de'
)));
$data = file_get_contents($uri, FALSE, $ctx);
```

https://wiki.php.net/rfc/tls-peer-verification

PHP 5.6

```
$uri = 'https://walterebert.de/';
$cafile = '/etc/ssl/ca-bundle.pem';

ini_set('openssl.cafile', $cafile);
$data = file_get_contents($uri);

// oder
$ctx = stream_context_create(['ssl'=>['cafile'=>$cafile]]);
$data = file_get_contents($uri, FALSE, $ctx);
```

https://wiki.php.net/rfc/tls-peer-verification

Links

https://www.owasp.org/index.php/SSL_TLS_Knowledge_Center
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
https://www.eff.org/https-everywhere/deploying-https
https://www.ssllabs.com/ssltest/
https://www.ssllabs.com/projects/best-practices/
https://istlsfastyet.com/
http://chimera.labs.oreilly.com/books/1230000000545/ch04.html
https://httpd.apache.org/docs/current/ssl/ssl_howto.html
http://nginx.com/blog/nginx-ssl/

Walter Ebert

@wltrd
walterebert.de
slideshare.net/walterebert