

# Surfen - sicher und komfortabel

Computerlabor im KuZeB  
[computerlabor.kire.ch](http://computerlabor.kire.ch)

12.10.2009

**Kire**

[www.kire.ch](http://www.kire.ch)

Layout-Template von Chih-Hao Tsai  
[chtsai.org](http://chtsai.org)

- World Wide Web
  - Hintergründe
  - Clients & Server
- Mozilla Firefox
  - Hintergründe
  - Wissenswertes & Grundeinstellungen
  - Suchmaschinen
  - Erweiterungen
- Sichere Verbindungen per HTTPS
- Browser-Spuren
  - Technisch & rechtlich
  - Browser-Einstellungen
  - Nützliche Add-ons für Firefox



# World Wide Web - Hintergründe

- Hypertext-System von Tim Berners-Lee
  - als Projekt 1989 am CERN entstanden
- WWW ≠ Internet
  
- Kernstandards
  - HTTP (Übertragungsprotokoll)
  - HTML (Seitenbeschreibungssprache)
  - URL (Ressourcenbezeichner)
- Weitere Standards
  - CSS (Trennung von Darstellung und Inhalt in HTML)
  - JavaScript (Clientseitige Skriptsprache)
  - HTTPS (Verschlüsselung & Authentisierung)

# World Wide Web - Clients & Server

## • Webserver

- Apache HTTP Server
- Microsoft Internet Information Services (IIS)

## • Webbrowser

- Windows Internet Explorer
- Mozilla Firefox
- Safari, Opera, Google Chrome



## • Hypertext Transfer Protocol

- Beispiel: HTML-Seite von Server anfordern

GET /datenschutz/browserspuren.htm HTTP/1.1

Host: www.kire.ch

- Antwort vom Server

HTTP/1.1 200 OK

Date: Sat, 10 Oct 2009 09:53:55 GMT

Server: Apache

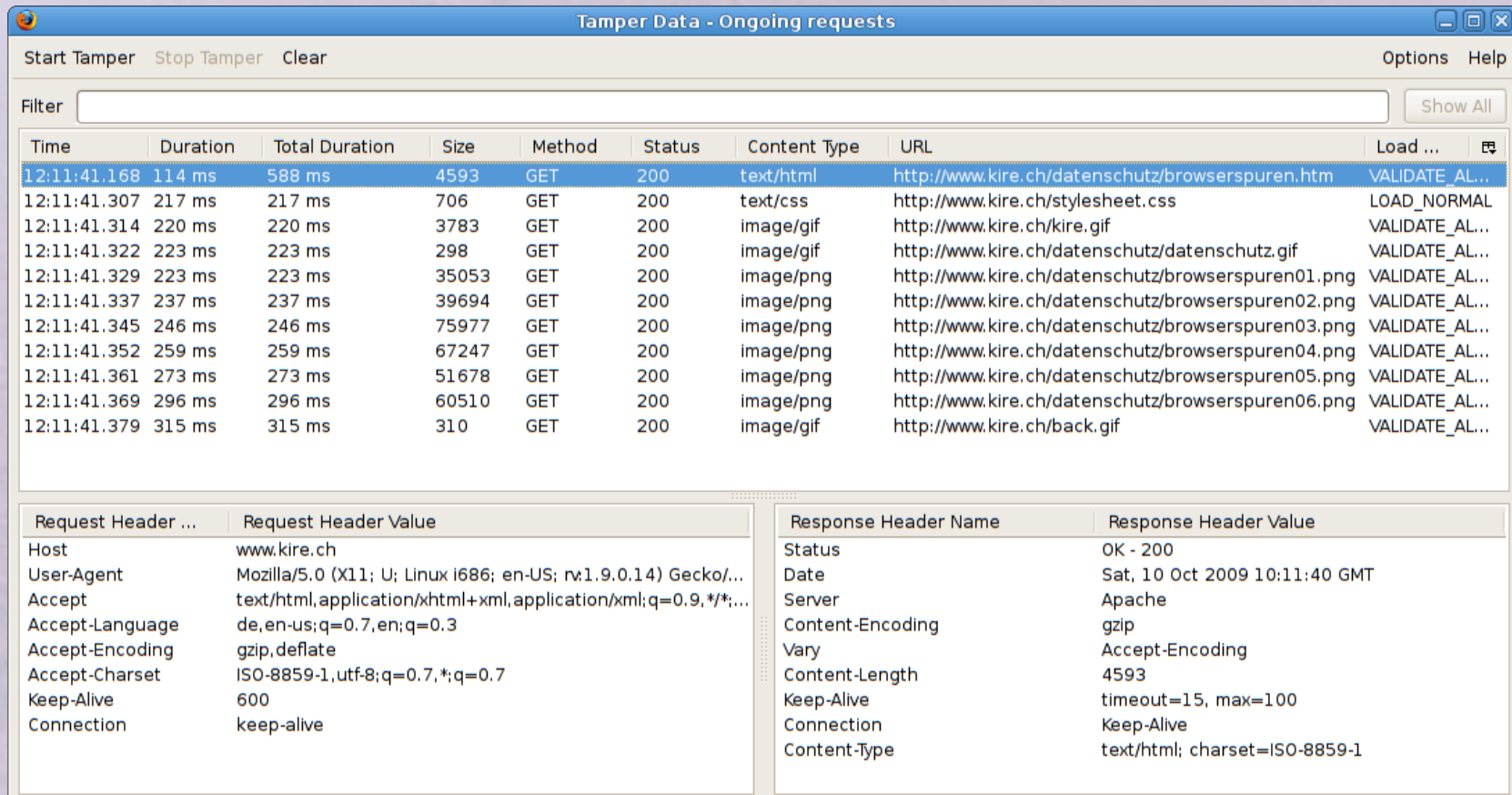
Transfer-Encoding: chunked

Content-Type: text/html; charset=ISO-8859-1

(und direkt angehängt der Inhalt des HTML-Dokuments)

# World Wide Web - HTTP

## Mit Firefox-Erweiterung „Tamper Data“ mitgeschnitten



Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear Options Help

Filter  Show All

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load ...
12:11:41.168	114 ms	588 ms	4593	GET	200	text/html	http://www.kire.ch/datenschutz/browserspuren.htm	VALIDATE_AL...
12:11:41.307	217 ms	217 ms	706	GET	200	text/css	http://www.kire.ch/stylesheet.css	LOAD_NORMAL
12:11:41.314	220 ms	220 ms	3783	GET	200	image/gif	http://www.kire.ch/kire.gif	VALIDATE_AL...
12:11:41.322	223 ms	223 ms	298	GET	200	image/gif	http://www.kire.ch/datenschutz/datenschutz.gif	VALIDATE_AL...
12:11:41.329	223 ms	223 ms	35053	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren01.png	VALIDATE_AL...
12:11:41.337	237 ms	237 ms	39694	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren02.png	VALIDATE_AL...
12:11:41.345	246 ms	246 ms	75977	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren03.png	VALIDATE_AL...
12:11:41.352	259 ms	259 ms	67247	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren04.png	VALIDATE_AL...
12:11:41.361	273 ms	273 ms	51678	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren05.png	VALIDATE_AL...
12:11:41.369	296 ms	296 ms	60510	GET	200	image/png	http://www.kire.ch/datenschutz/browserspuren06.png	VALIDATE_AL...
12:11:41.379	315 ms	315 ms	310	GET	200	image/gif	http://www.kire.ch/back.gif	VALIDATE_AL...

Request Header ...	Request Header Value	Response Header Name	Response Header Value
Host	www.kire.ch	Status	OK - 200
User-Agent	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.14) Gecko/...	Date	Sat, 10 Oct 2009 10:11:40 GMT
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;...	Server	Apache
Accept-Language	de,en-us;q=0.7,en;q=0.3	Content-Encoding	gzip
Accept-Encoding	gzip,deflate	Vary	Accept-Encoding
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7	Content-Length	4593
Keep-Alive	600	Keep-Alive	timeout=15, max=100
Connection	keep-alive	Connection	Keep-Alive
		Content-Type	text/html; charset=ISO-8859-1

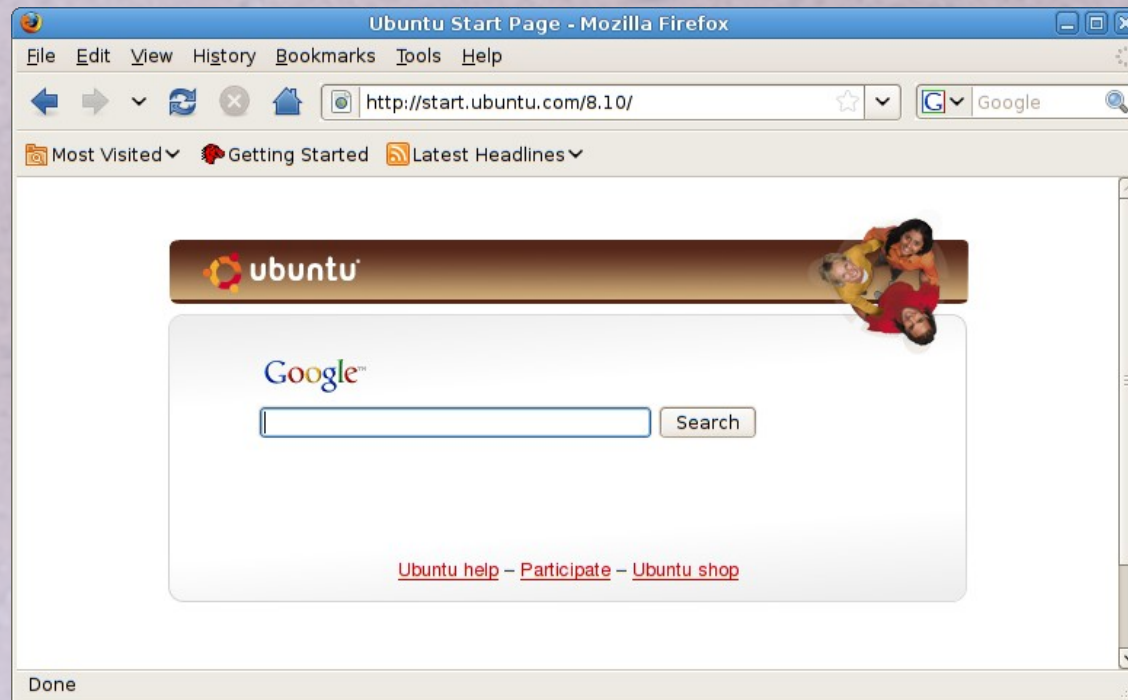


## • Dabei übertragene HTML-Seite

```
Source of: http://www.kire.ch/datenschutz/browserspuren.htm - Mozilla Firefox
File Edit View Help
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>kire.ch - Datenschutz - Browser-Spuren</title>
<meta name="description" content="kire.ch: Datenschutz und Datensicherheit, Linux, Fotografie, Rollenspiel, Crossgolf">
<meta name="keywords" content="kire.ch, Datenschutz, Datensicherheit, Linux, Fotografie, Rollenspiel, Rollenspiele, Crossgolf,
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="../stylesheet.css" type="text/css">
</head>
<body>
<table>
<tr>
<td valign=top rowspan=2>
<a href="../index.htm"></a>
</td>
<td>
<a href="index.htm"></a>
</td>
<td width=50 rowspan=2></td>
</tr>
<tr>
<td>
<center><b>Browser-Spuren - die beim Surfen im Netz hinterlassen werden</b></center><p>
Beim Surfen im World Wide Web hinterlassen wir verschiedenste Spuren. Mit Hilfe von Cookies und anderen Identifikationsmerkmale
Zuerst wird bei einer Seitenanfrage eine weltweit eindeutige IP-Adresse &uuml;bertragen, welche es dem angefragten Server &uuml;
Zus&auml;tzlich &uuml;bertr&auml;gt der Browser Informationen &uuml;ber sich selbst und zum verwendeten Betriebssystem. Mit auf
Line 69, Col 9
```

# Mozilla Firefox - Hintergründe

- Basiert auf Gecko (ursprünglich von Netscape)
- Open Source Software
- Linux, Mac OS X, Windows
- Inoffizielle Portierungen
  - für verschiedenste Plattformen





# Mozilla Firefox - Wissenswertes & Grundeinstellungen

- Grundeinstellungen sind ziemlich gut
  - Security → Use a master password
- Wirklich mächtig wird der Browser durch
  - „Suchmaschinen“
  - Add-ons
    - Extensions, Themes, Languages, Plugins
- RSS Feed-Reader bereits integriert
  - Bessere gibt es als Extensions
- Ev. interessant
  - Bookmarks als HTML-Datei exportieren

# Mozilla Firefox - Suchmaschinen

- Nicht nur Suchmaschinen im Sinne von Google
- Beziehen von mycroft.mozdev.org
  - eTools.ch (etools.ch)
    - In ~/.mozilla/firefox/\*.default/searchplugins/etoolsch.xml unmittelbar an {searchTerms} anhängen:
      - &country=web&language=all
        - Für weltweite Suche als Standard
  - Wikipedia (de) - Artikel (wikipedia-de)
  - Deutscher Wortschatz (wortschatz)
  - LEO de<->en (leo\_deen)
  - [map.search.ch] Schweiz (map\_search\_ch)



# Mozilla Firefox - Erweiterungen

- German Dictionary (Switzerland)
- Tab Mix Plus
  - Für komfortable Tab-Steuerung
    - Enable built-in session restore and disable the Tab Mix Session Manager
    - Tab Opening & Tab Closing
      - Einstellungen nach Gusto vornehmen
- Adblock Plus
  - Werbeblocker

# Sichere Verbindungen per HTTPS

- **Public-Key-Infrastruktur nach X.509-Standard**
  - Hierarchisches System von vertrauenswürdigen Zertifizierungsstellen
  - Server weist sich gegenüber dem Browser aus und ermöglicht Verschlüsselung
- **Browserhersteller**
  - prüft Zertifizierungsstelle (Hardware, Software, Abläufe)
  - und nimmt dessen Root-Zertifikat(e) in den Browser auf



# Sichere Verbindungen per HTTPS

- Zertifizierungsstelle (Certification Authority CA)
  - prüft BesitzerIn einer Domäne
  - stellt Zertifikate für (i.d.R.) Hostnamen
  - und/oder Zwischenzertifizierungsstellen aus
    - welche ihrerseits wiederum Zertifikate ausstellen können
      - Baumhierarchie
  - und pflegt eine Sperrliste
- CAcert
  - Freie Zertifizierungsstelle für Gratis-Zertifikate
  - Identität wird von mindestens zwei voll beglaubigten Mitgliedern geprüft
  - Zertifizierung gegenüber Browserherstellern ist teuer und aufwändig
    - Root-Zertifikate müssen (noch) manuell importiert werden

# Sichere Verbindungen per HTTPS

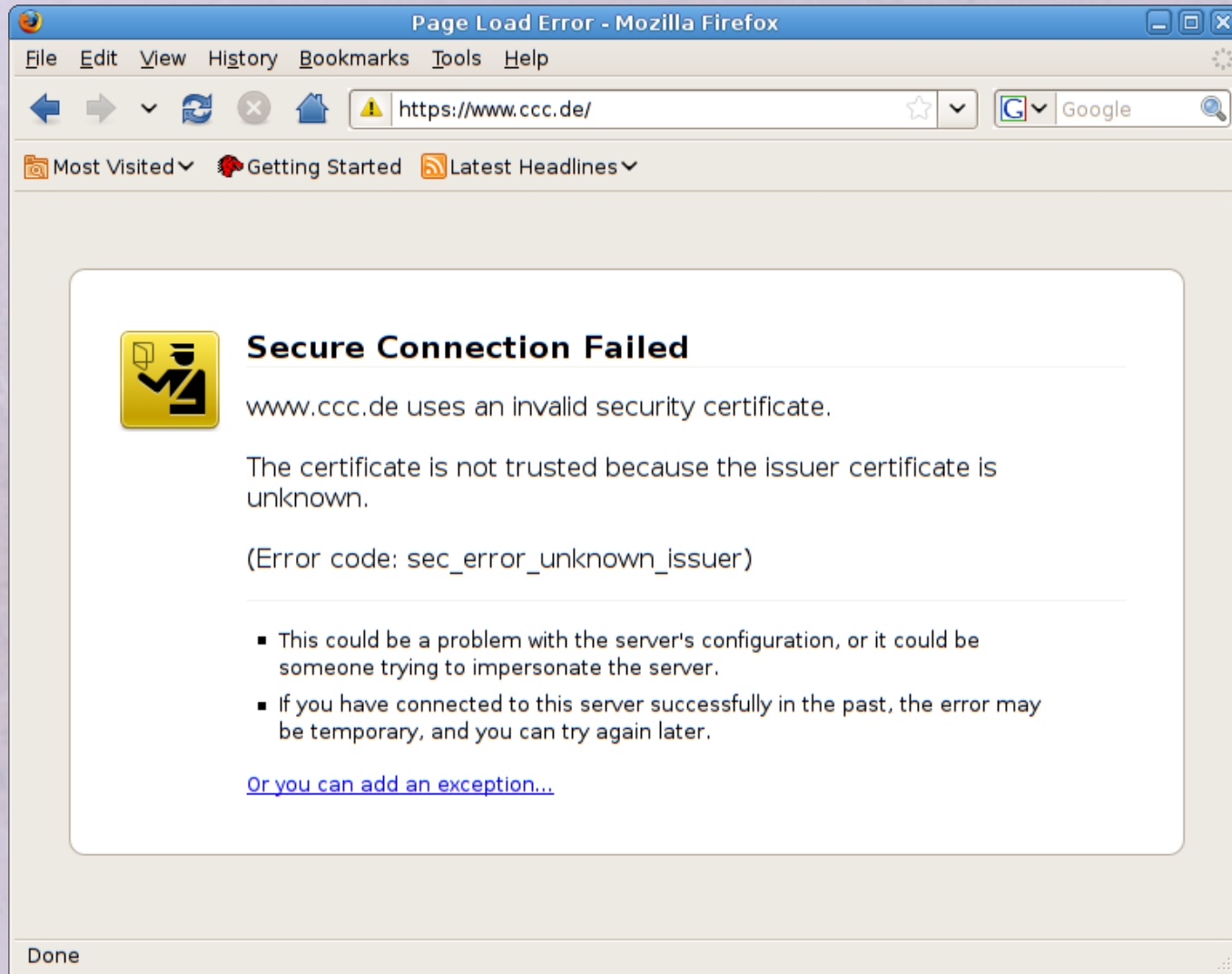
## • Webbrowser

- bezieht beim Verbindungsaufbau zum Server das Zertifikat
- und prüft, ob
  - sich dieses auf durch eine vertrauenswürdige Zertifizierungsstelle ausgestelltes Zertifikat zurückführen lässt
  - der aufgerufene Hostnamen zum Zertifikat passt
  - das Gültigkeitsdatum nicht abgelaufen ist
  - das Zertifikat nicht gesperrt worden ist
- Falls die Prüfung fehl schlägt, wird ein Fehler angezeigt
  - der übersteuert werden kann
- Für bessere Kennzeichnung in Adresszeile
  - `about:config` → `browser.identity.ssl_domain_display = 1`



# Sichere Verbindungen per HTTPS

## ❗ Aussteller-Zertifikat ist unbekannt



# Sichere Verbindungen per HTTPS

## • Aussteller ist CAcert



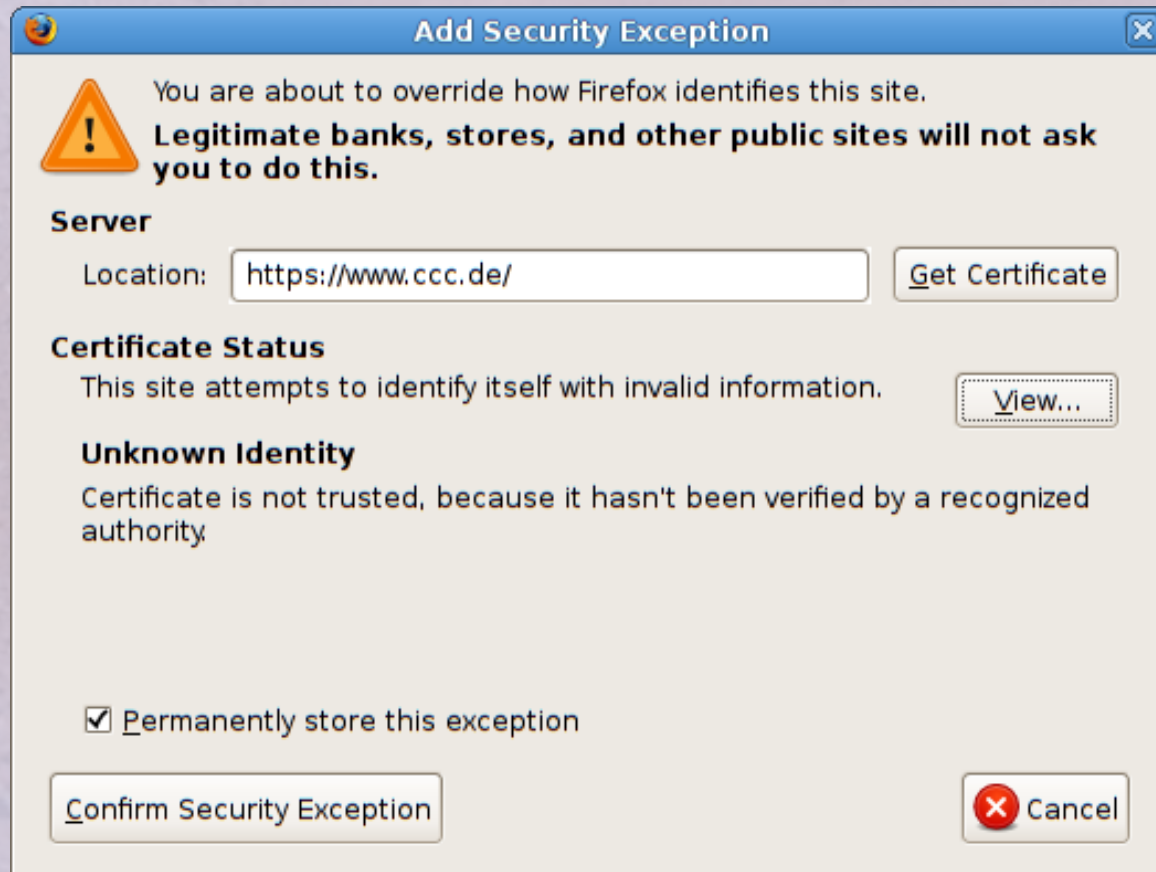
The screenshot shows a Windows Certificate Viewer window titled "Certificate Viewer: 'www.ccc.de'". The window has two tabs: "General" (selected) and "Details". The main content area displays a warning: "Could not verify this certificate for unknown reasons." Below this, the certificate details are listed in a structured format.

<b>Issued To</b>	
Common Name (CN)	www.ccc.de
Organization (O)	Chaos Computer Club e.V.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	48:A0
<b>Issued By</b>	
Common Name (CN)	CAcert Class 3 Root
Organization (O)	CAcert Inc.
Organizational Unit (OU)	http://www.CAcert.org
<b>Validity</b>	
Issued On	03/21/2008
Expires On	03/21/2010
<b>Fingerprints</b>	
SHA1 Fingerprint	5A:91:B7:EA:C4:99:F6:72:30:BF:B0:B8:F7:05:F6:85:5C:ED:5D:EC
MD5 Fingerprint	B3:72:18:38:13:53:99:E4:C0:19:34:8B:E3:FA:04:2B



# Sichere Verbindungen per HTTPS

- Diesem Server-Zertifikat könnte nun vertraut werden
  - Mit „Confirm Security Exception“
    - Besser nicht permanent



# Sichere Verbindungen per HTTPS

- ❖ Noch besser, das Root-Zertifikat der CA importieren
  - ❖ Falls CA vertrauenswürdig
    - ❖ Und Root-Zertifikat (und/oder Fingerprint) von vertrauenswürdiger Stelle
      - ❖ <https://...>
  - ❖ Für CAcert
    - ❖ <http://www.cacert.org/index.php?id=3>
    - ❖ Klick auf Dateien im PEM-Format
      - ❖ „Trust this CA to identify web sites“ wählen
      - ❖ und vor dem Speichern Fingerprint prüfen
        - ❖ CAcert Class 1 PKI Key - SHA1:  
13:5C:EC:36:F4:9C:B8:E9:3B:1A:  
B2:70:CD:80:88:46:76:CE:8F:33
        - ❖ CAcert Class 3 PKI Key - SHA1:  
DB:4C:42:69:07:3F:E9:C2:A3:7D:  
89:0A:5C:1B:18:C4:18:4E:2A:2D



# Sichere Verbindungen per HTTPS

## • Sicherheit

- HTTPS gilt als sicher
- Standard-Zertifikate bestätigen, dass der Hostnamen unter der administrativen Kontrolle der beantragenden Person steht
  - Teilweise reicht Prüfung der E-Mail
    - an zu beglaubigende Domain

## • Extended-Validation-SSL-Zertifikate

- Identität der Besitzerin (Person, Unternehmung) einer Domäne wird von CA genau geprüft
- Adresszeile verfärbt sich grün anstatt blau

# Browser-Spuren - technisch & rechtlich

- Server-Logfiles
  - Webserver
    - IP-Adresse, Browser, Betriebssystem, Referrer, Datum
  - Mailserver
  - Nameserver (DNS)
- Aufbewahrungspflicht der IP-Zuordnungen
  - CH: 6 Monate durch Provider
  - EU: 6 - 24 Monate
- Eindeutige Merkmale
  - MAC-Adresse
  - "Einwahl"
  - Cookies & IDs
- lokaler Computer
  - Cache & Browser-History



# Browser-Spuren - Browser-Einstellungen

- Cookies
  - Generell alle Cookies annehmen
  - und beim Schliessen des Browsers löschen
- Browserhistory nur einen Tag aufbewahren
  - und Eingaben sowie Downloads nicht merken
- Cache auf 0 MB stellen
- Super-Cookies
  - `about:config` → `dom.storage.enabled = false`
  - `~/.mozilla/firefox/*.default/webappsstore.sqlite` löschen
- Genauere Beschreibung und Screenshots
  - <http://www.kire.ch/datenschutz/browserspuren.htm>

# Browser-Spuren - Browser-Einstellungen

## ❖ Adobe Flash Player

- [http://www.macromedia.com/support/documentation/de/flashplayer/help/settings\\_manager07.html](http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html)

## ❖ ev. weitere Plugins

- Google-Toolbar
- allenfalls (Google) Search Suggestions
- Adobe Reader
  - mit standardmässig aktiviertem JavaScript
- RealPlayer



# Browser-Spuren - Nützliche Add-ons für Firefox

- User Agent Switcher
  - Browserinformationen ändern
- RefControl
  - Referrer unterdrücken
  - Default-Einstellung auf "<Block> (3rd Party)" stellen
- QuickJava
  - Ein-/Ausschalter für Java & JavaScript
- Flashblock
  - Adobe Flash nicht automatisch ausführen

# Browser-Spuren - Nützliche Add-ons für Firefox

## • NoScript

- Anstatt Flashblock und QuickJava
- Einstellungen pro Site, permanent oder temporär
- Viele Möglichkeiten und daher auch komplizierter
  - Whitelist ausser (about:\*) löschen
  - Unter Plugins "Forbid <IFRAME>" auswählen
  - Unter Notifications ausschalten:
    - Show message about blocked scripts
    - Display the release notes on updates
- Viele Sites benötigen JavaScript
  - Prüfung von Formulardaten
  - Web 2.0

## • Test

- <http://centralops.net/asp/co/BrowserMirror.vbs.asp>