



## Fehlende Ciphersuiten unter TLS 1.2

Bei der Umstellung auf TLS 1.2 kann eine falsche Auswahl von Ciphersuiten zu Problemen führen. In diesem Beispiel bekomme ich beim Aufruf von <https://www.google.de> folgenden Hinweis angezeigt.

The screenshot shows a web browser window with the following details:

- Address bar: https://www.google.de/?gws\_rd=ssl
- Status bar: Die Seite kann nicht angeze... (The page cannot be displayed)
- Buttons: Back, Forward, Stop, Refresh, Home, Favorites, Stop, Help, Smiley.

The main content area displays the message: "Die Seite kann nicht angezeigt werden." (The page cannot be displayed) in large blue text. Below it is a bulleted list of troubleshooting steps:

- Vergewissern Sie sich, dass die Webadresse https://www.google.de stimmt.
- Suchen Sie die Seite mit Ihrer Suchmaschine.
- Aktualisieren Sie die Seite in ein paar Minuten.

A small button labeled "Verbindungsprobleme beheben" (Fix connection problems) is visible at the bottom left.

Ein Hinweis, wäre die fehlende Unterstützung eines Protokolls.

The screenshot shows a web browser window with the following details:

- Address bar: https://www.google.de/?gws\_rd=ssl
- Status bar: Die Seite kann nicht angeze... (The page cannot be displayed)
- Buttons: Back, Forward, Stop, Refresh, Home, Favorites, Stop, Help, Smiley.

The main content area displays the message: "Diese Seite kann nicht angezeigt werden." (This page cannot be displayed) in large blue text. Below it is a detailed error message:

Aktivieren Sie TLS 1.0, TLS 1.1 und TLS 1.2 in den erweiterten Einstellungen, und versuchen Sie noch einmal, eine Verbindung mit <https://www.google.de> herzustellen. Sollte der Fehler weiterhin auftreten, verwendet diese Website möglicherweise ein nicht unterstütztes Protokoll oder eine nicht unterstützte Verschlüsselungssammlung wie RC4 ([Link zu den Details](#)), die als unsicher angesehen werden. Wenden Sie sich an den Websiteadministrator.

A small button labeled "Einstellungen ändern" (Change settings) is visible at the bottom left.



## Fehlende Ciphersuiten unter TLS 1.2

In dieser Sammlung werden ausschließlich Suiten mit einem RSA Authentifizierungsalgorithmus eingesetzt.

The screenshot shows the Windows Group Policy Management Editor. On the left, the navigation pane shows 'Gruppenrichtlinienverwaltung' with 'Gesamtstruktur' selected. Under 'Server', 'Hardening SChannel' is expanded, showing various sub-options like 'Hardening Auditing Member Server', 'Hardening Baseline Member Server 2016', etc. On the right, the main pane is titled 'Hardening SChannel' and shows the 'Computerkonfiguration (Aktiviert)' section. Under 'Richtlinien', there's a table with columns 'Richtlinie', 'Einstellung', and 'Kommentar'. The 'Einstellung' column for the 'SSL-Verschlüsselungssammlungen' row is set to 'Aktiviert'. The 'Kommentar' column contains a large block of cipher suite names, many of which are highlighted with a red border. Below this table, under 'Einstellungen', there are sections for 'Windows-Einstellungen', 'Registrierung', 'Auflistung: Schannel', 'Gemeinsam', and 'Optionen'.

Aus diesem Grund lässt sich die Webseite <https://www.der-windows-papst.de> auch aufrufen.

The screenshot shows the homepage of 'DER WINDOWS PAPST – IT BLOG ESSEN JÖRN WALTER'. The header features a blue bar with the title and a small German flag. Below the header, there's a navigation menu with links like 'DER WINDOWS PAPST', 'WER BIN ICH', and 'KONTAKTFORMULAR'. The main content area has a sub-header 'DER WINDOWS PAPST' and 'IT BLOG ESSEN'. A text block discusses the blog's purpose and tips. To the right, there's a sidebar with 'KATEGORIEN' and a list of topics. A modal dialog box is open in the center, titled 'Zertifikat', showing certificate details. At the bottom of the page, there's a note about cookie usage and a 'Cookie Settings' button.

Diese Webseite verwendet Cookies. Cookies werden zur Benutzerführung und Webanalyse verwendet und helfen dabei, diese Webseite besser zu machen.

[Akzeptieren](#) [Ablehnen](#) [Zum Datenschutz](#)



## Fehlende Ciphersuiten unter TLS 1.2

Google hingegen nutzt aber ein Zertifikat mit einem Authentifizierungsalgorithmus der Güte **ECDSA**. Keine der oben eingesetzten Cipher-Suiten unterstützt ECDSA. Daher kommt es zu keiner Verbindung, um die Webseite <https://www.google.de> aufrufen zu können.

Nutze ich speziell für dieses Beispiel diese beiden ECDSA Cipher-Suiten...

Richtlinie	Einstellung	Kommentar
Reihenfolge der SSL-Verschlüsselungssammlungen	Aktiviert	
SSL-Verschlüsselungssammlungen	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	

...ist der Aufruf von <https://www.google.de> wieder möglich. Es kommt wieder eine Verbindung zustande.

The screenshot shows a browser window with the Google homepage. A certificate dialog box is overlaid on the page. The dialog box has tabs for 'Allgemein', 'Details', and 'Zertifizierungspfad'. The 'Details' tab is selected, showing a table of certificate information. One row in the table, 'Parameter für öffentlichen Schlüssel', is highlighted with a red box and contains the value 'ECDSA\_P256'. The rest of the page content, including the Google logo and search bar, is visible in the background.



## Fehlende Ciphersuiten unter TLS 1.2

### Optional:

Diese beiden Suiten benötigen ein Zertifikat mit einem RSA Authentifizierungsalgorithmus unterstützen aber zusätzlich **PFS** (Perfect Forwarding Secrecy).

**TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256**  
**TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384**

Diese beiden Suiten benötigen ein Zertifikat mit einem ECDSA Authentifizierungsalgorithmus unterstützen aber zusätzlich **PFS** (Perfect Forwarding Secrecy).

*Der Einsatz von ECDHE ist was die Performance angeht besser als DHE. Der Einsatz von DHE bedeutet einen Leistungsabfall vom 2-8-fachen in Kauf nehmen zu müssen.*

**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256**  
**TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384**

Aus Kompatibilitätssicht nutzt man besser die Hybrideform:

**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256**  
**TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384**  
**TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256**  
**TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384**

### Weitere Informationen:

<https://www.der-windows-papst.de/2018/08/14/was-ist-eine-cipher-suite/>



## Fehlende Ciphersuiten unter TLS 1.2

**Cipher Suiten die in Reihenfolge eingesetzt werden können:**

### PFS mit ECDHE

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256