Browser TLS 1.3 – Firefox & Chrome & Edge

Am 21. März 2018 wurde der neue TLS 1.3 Standard finalisiert.

TLS steht für Transport Layer Security und ist der Nachfolger von SSL (Secure Socket Layer). TLS bietet eine sichere Verbindung zwischen Server und Webbrowser. Die Verbindung ist sicher, da zur Verschlüsselung der zu übertragenden Daten die symmetrische Kryptografie verwendet wird. Die Schlüssel werden für jede Verbindung eindeutig generiert und basieren auf einem gemeinsamen geheimen Schlüssel, der zu Beginn der Sitzung ausgehandelt wurde und auch als TLS-Handshake bezeichnet wird. Viele IP-basierte Protokolle wie z.B. HTTPS, POP3, SMTP, FTP unterstützen TLS zum Verschlüsseln von Daten.

Die IETF (Internet Engineering Task Force) ist die Gruppe, die für die Definition des TLS Protokolls verantwortlich ist. Der Vorgänger TLS 1.2 wurde in den letzten 8 Jahren von den meisten Webbrowsern verwendet.

Performance:

TLS 1.2 benötigte zwei Round-Trips um den Handshake abzuschließen. TLS 1.3 benötigt nur noch einen Lauf, was wiederum die Latenz halbiert und TLS 1.3 schneller macht. Ein weiterer Vorteil ist der Zero-Round-Trip (0-RTT), dieser verbessert die Ladezeiten zusätzlich.

Sicherheit:

Wenn TLS 1.2 falsch konfiguriert wurde, waren Webseiten anfällig für Angriffe. Unsichere Feature wurden aus TLS 1.2 entfernt, dazu gehören z.B.:

- SHA-1
- RC4
- DES
- 3DES
- AES-CBC
- MD5
- Arbitrary Diffie-Hellman group

Alle Handshake Messages nach dem ServerHello sind nun verschlüsselt, dafür sorgt die neu eingeführte EncryptedExtension Message. Zur Steigerung der Konsistenz wurden zudem überflüssige Messages entfernt wie ChangeCipherSpec. Elliptische Kurven- und Signaturalgorithmen sind jetzt in der Basisspezifikation enthalten, wie ED25519 und ED448.

Nachfolgend 3 Browser die bereits TLS 1.3 unterstützen.

Erstellt von Jörn Walter **28.04.2018**

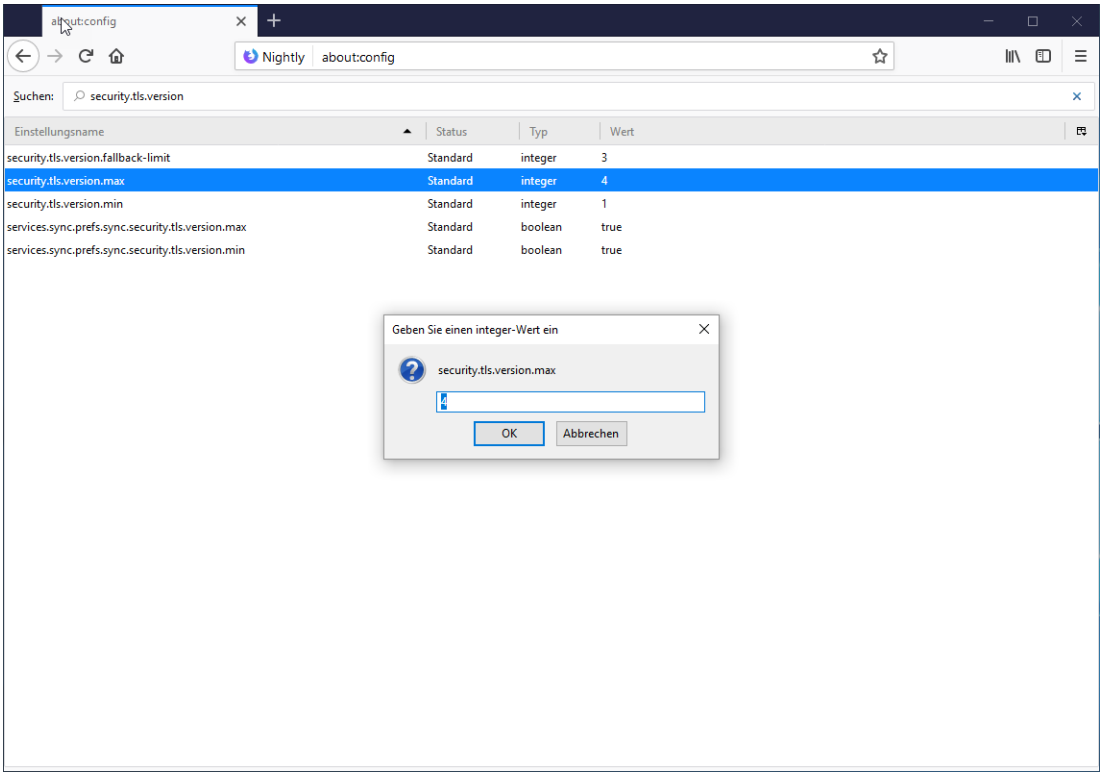
Browser TLS 1.3 – Firefox & Chrome & Edge

Firefox Nightly Download:

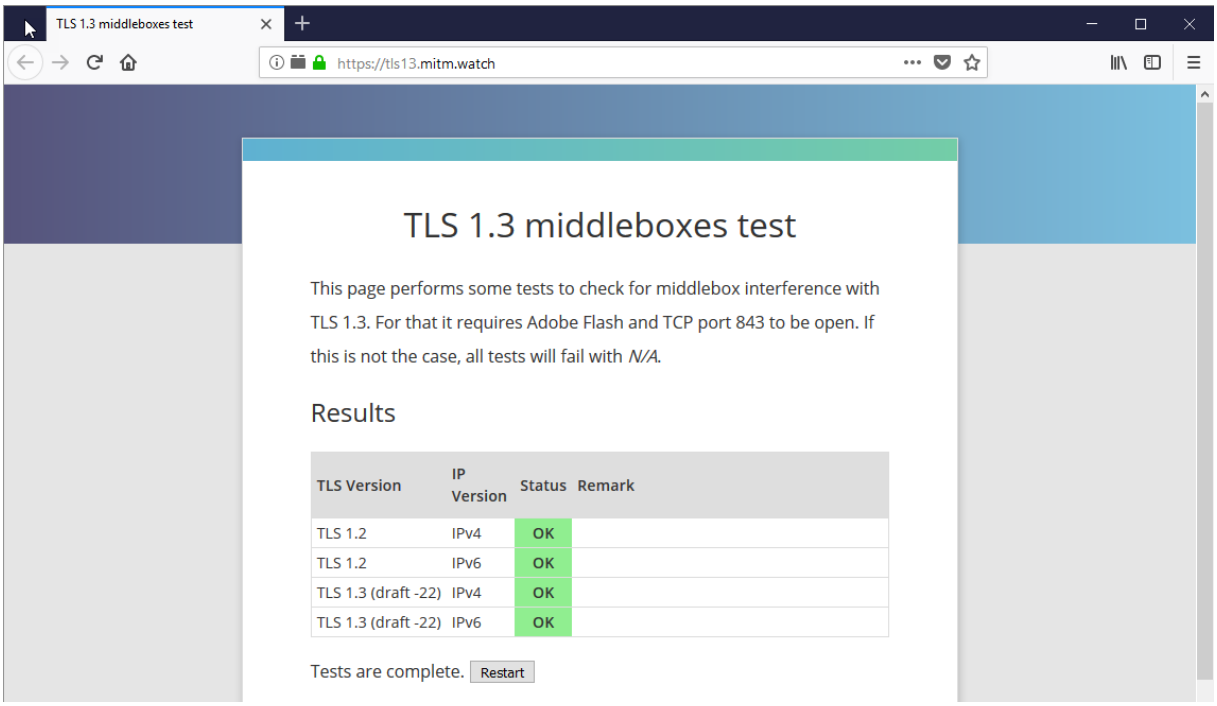
https://nightly.mozilla.org/

Vorbereitung:

about:config > security.tls.version auf 4 setzen



Testseite: https://tls13.mitm.watch/

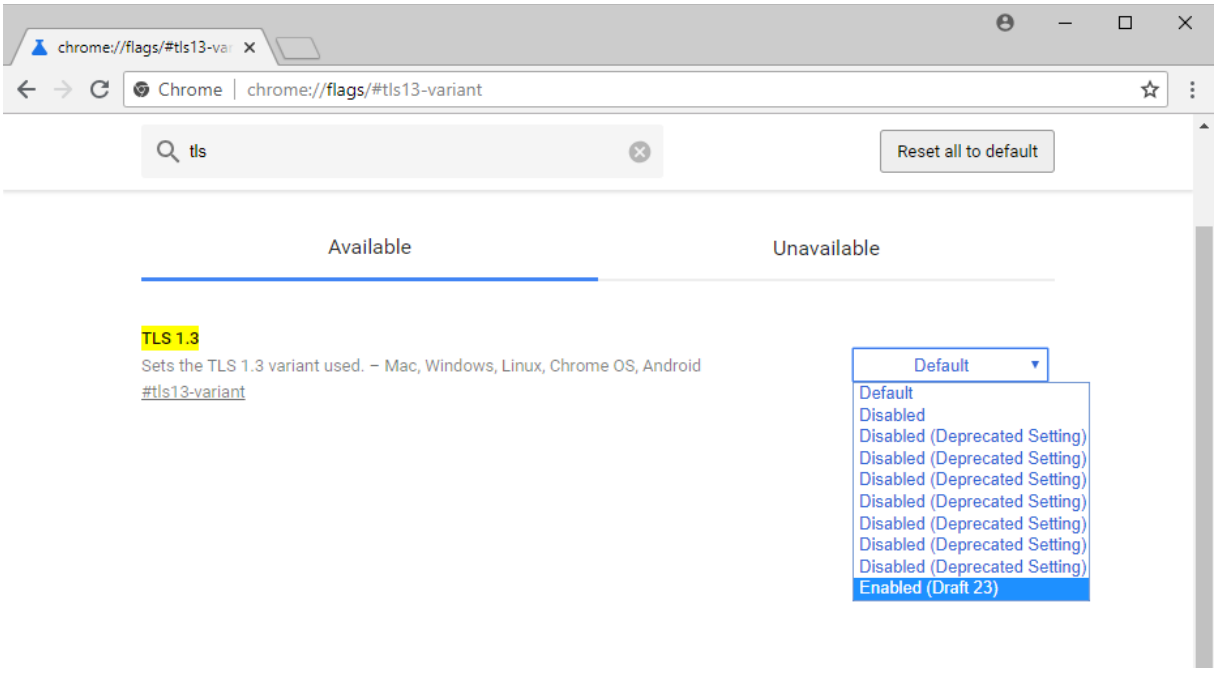


Browser TLS 1.3 – Firefox & Chrome & Edge

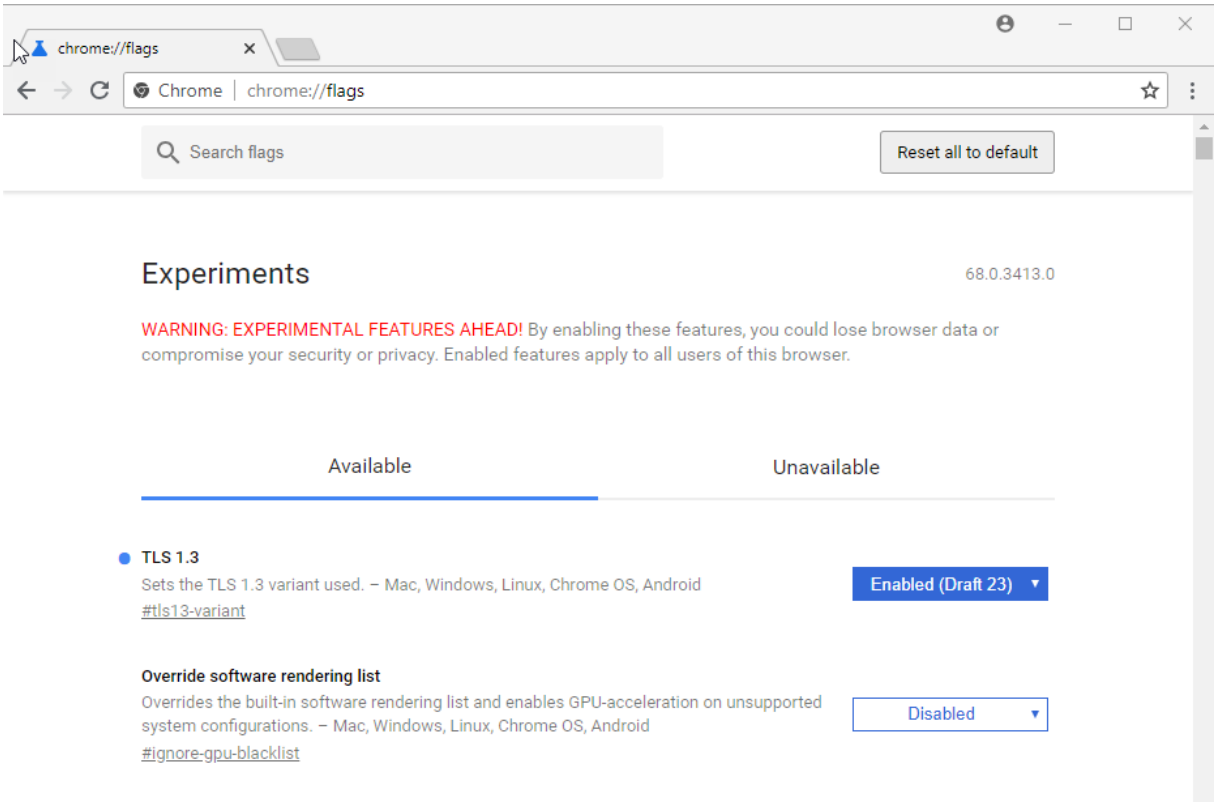
Chrome Canary Download:

https://www.google.com/chrome/browser/canary.html

Vorbereitung: chrome://flags/ > Maximum TLS version enabled

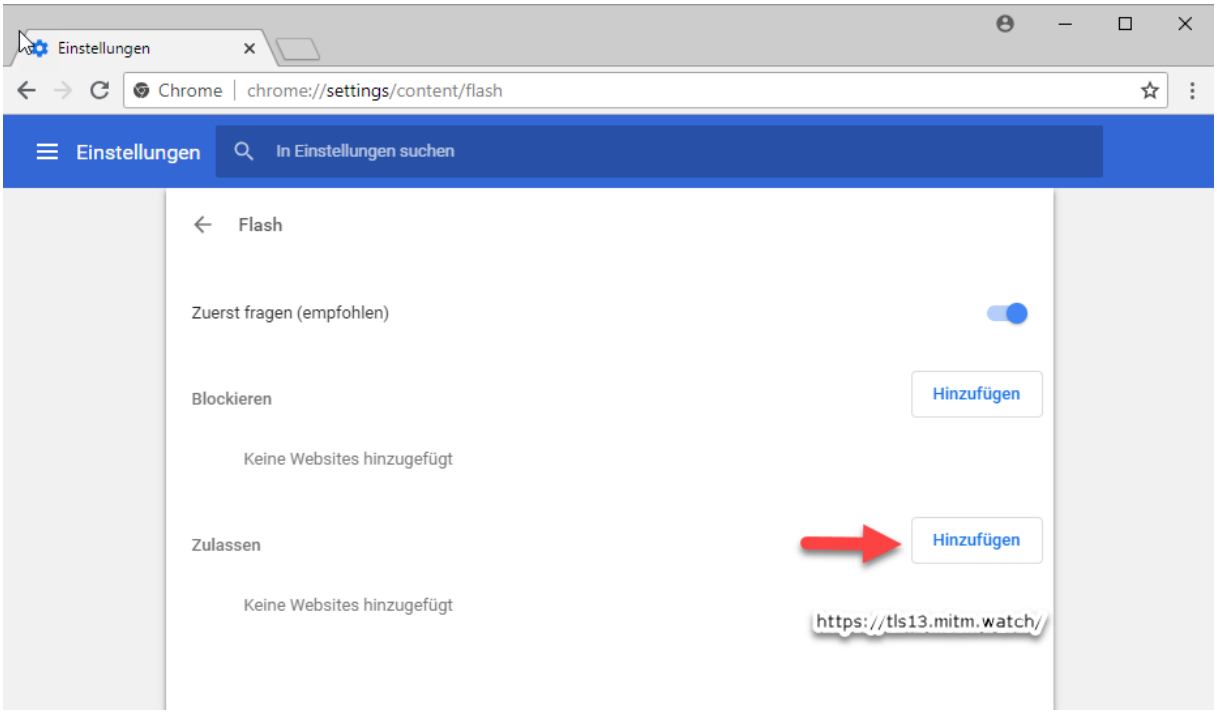


TLS1.3 ist nun aktiviert

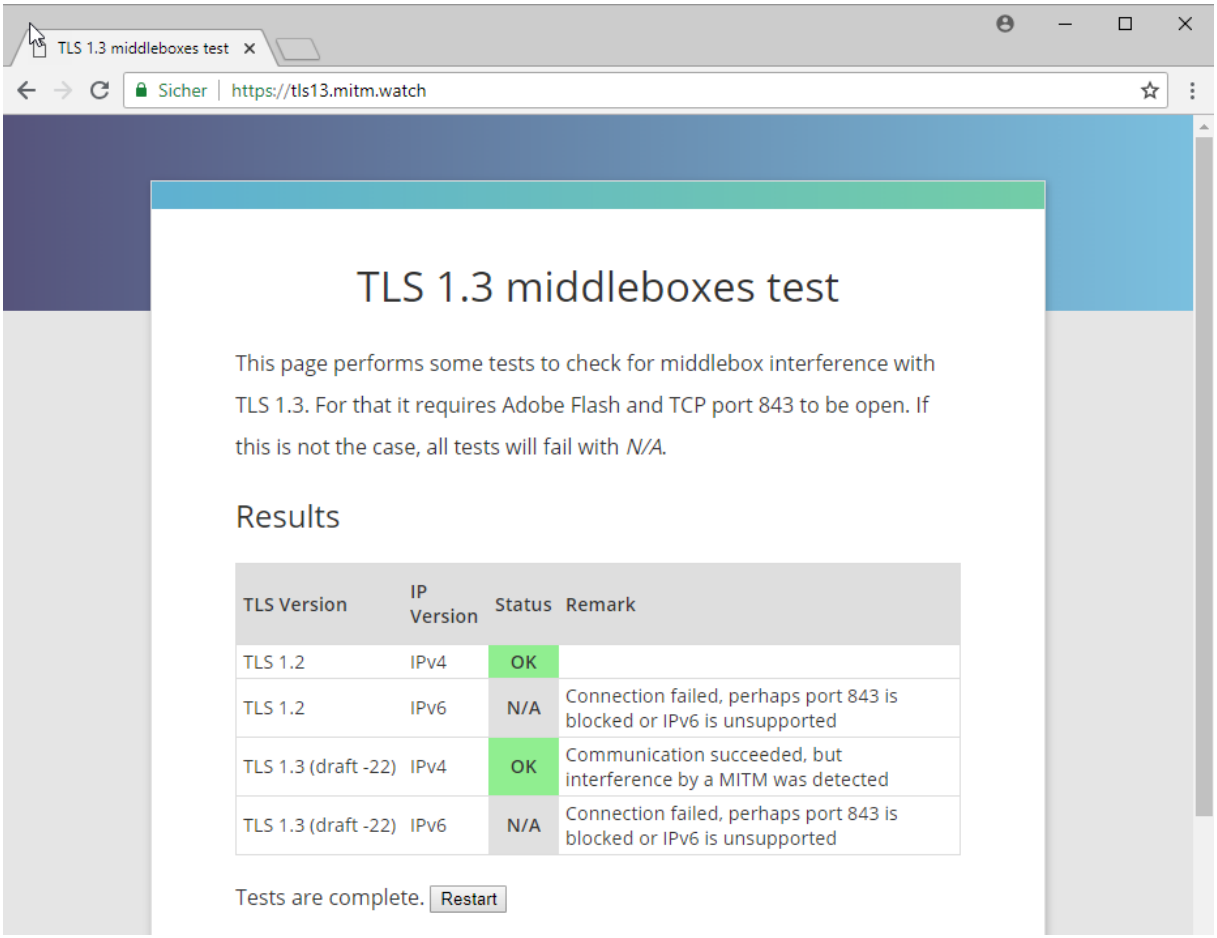


Browser TLS 1.3 – Firefox & Chrome & Edge

Flash aktivieren bzw. Webseite zulassen:



Testseite: https://tls13.mitm.watch/



Browser TLS 1.3 – Firefox & Chrome & Edge

Der Edge Browser unterstützt TLS 1.3 bereits ohne zutun:

Zur Ausführung des Tests muss auch hier Flash aktiviert werden.