SSL

Lets Encrypt -- Zertifikate für jedermann

https://gethttpsforfree.com

Bitte beachten Sie, das der Zugriff auf den Ordner ".well-known/acme-challenge/" von All-Inkl.com derzeit blockiert und gefiltert wird.

Wäre es möglich ein Let's Encrypt Zertifikat mit einem 4096 RSA key zu generieren?

meins z.b. hat 2048 bits

die verwechselt doch auch die schlüssellänge mit der verschlüsselungstiefe, oder?

#steffen.dabischa : 15.03.2016 11:46:00
---
wobei man scheinbar auch 4096 anfordern kann:
https://thomas-leister.de/internet/anleitung-fuer-lets-encrypt-kostenlose-tls-zertifikate-fuer-alle/
#steffen.dabischa : 15.03.2016 11:51:51

KUNDE HAT ANTWORT

das bieten wir nicht an, da der Gewinn an Sicherheit die Performancebeeinträchtigung nicht rechtfertigt.

Technisch unterstützt Let'sEncrypt zwar größere Schlüsselstärken, in der Praxis ist dies aber aktuell nicht sinnvoll.

Anbei einige Artikel zur Schlüsselstärke:
https://en.wikipedia.org/wiki/Key_size#Asymmetric_algorithm_key_lengths
https://certsimple.com/blog/measuring-ssl-rsa-keys (performance 2048vs4096)
https://gnupg.org/faq/gnupg-faq.html#no_default_of_rsa4096

Eindeutige ID: #1210
Verfasser: me
Letzte Änderung: 15.03.2016 12:40