

## This server supports TLS 1.3. HTTP Strict Transport Security (HSTS) with long duration deployed on this serv DNS Certification Authority Authorization (CAA) Policy found for this domain

Certificate #1: RSA 2048 bits (SHA256withRSA)

Valid from

Valid until

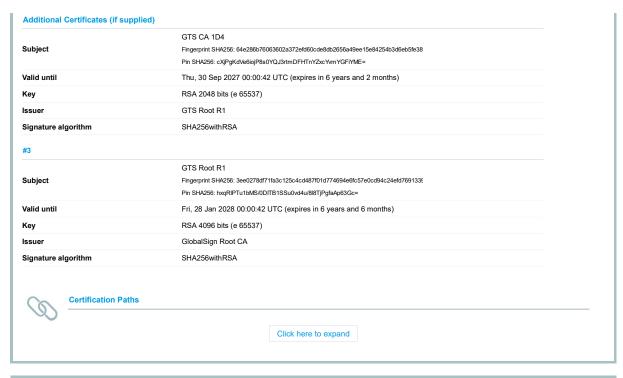
This site works only in browsers with SNI support.

## Server Key and Certificate #1 Fingerprint SHA256: 8e461f08a11149c79a4ef8c5ed4345900105aa0639e11 Subject Pin SHA256: P7YpVDZk5+TgFQuj0Q+HIU+ls62UHOvxuzn4dJluUBo= Common names Alternative names web.app \*.web.app Serial Number 22552726b3fa5e1d0a00000000d6dfe7

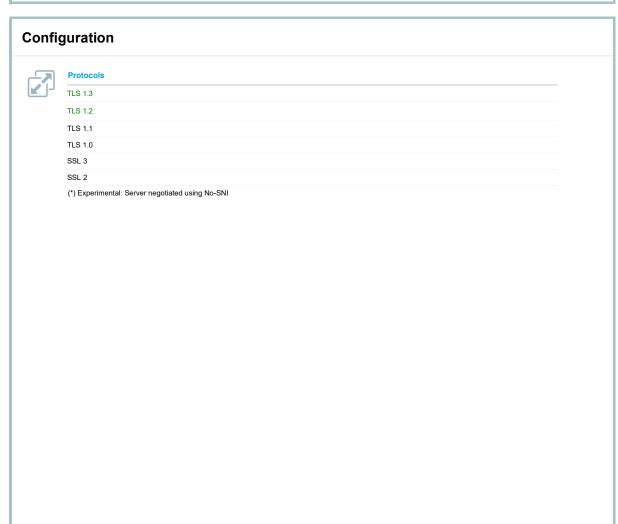
Tue, 17 Aug 2021 21:19:32 UTC (expires in 29 days, 23 hou

Wed, 19 May 2021 21:19:33 UTC

1 of 5 18/07/2021 19:07



## Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI Click here to expand



2 of 5 18/07/2021 19:07

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS ECDHE RSA WITH AES 12		
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12		
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACH		
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACH		
Android 8.1		TLS 1.3	TLS_CHACHA20_POLY1305_SHA:		
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA:		
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Chrome 69 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c   TLS_AES_128_GCM_SHA256				
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC		
Chrome 80 / Win 10 R	•	TLS 1.3	TLS_AES_128_GCM_SHA256 EC		
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Firefox 62 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c   TLS_AES_128_GCM_SHA256				
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC		
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
E 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
E 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12		
E 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12		
E 11 / Win Phone 8.1 Update F	R RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12		
E 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12		
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Java 11.0.3	•	TLS 1.3	TLS_AES_128_GCM_SHA256 EC		
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC		
OpenSSL 1.0.1I R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 EC		
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12		

3 of 5 18/07/2021 19:07

ated server-side (more info) SSL 3 not supported (more info) nore info) nore info) TLS 12: 0xc027 nore info) TLS 12: 0xc027 nore info) TLS 12: 0xc027 TLS_FALLBACK_SCSV supported (more info)
SSL 3 not supported (more info) nore info) nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027
SSL 3 not supported (more info) nore info) nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027
SSL 3 not supported (more info) nore info) nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027
nore info) nore info) TLS 1.2: 0xc027
nore info) TLS 1.2: 0xc027
nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027 nore info) TLS 1.2: 0xc027
nore info) TLS 1.2: 0xc027
nore info) TLS 1.2: 0xc027
nore info) TLS 1.2: 0xc027
TLS_FALLBACK_SCSV supported (more_into)
nore info)
with most browsers) ROBUST (more info)
h2 http/1.1
ge=31556926; includeSubDomains; preload
me Edge Firefox IE
nore info)
nore info)
NUE quites not supported
T T

18/07/2021 19:07 4 of 5

Ty Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including on								

5 of 5