

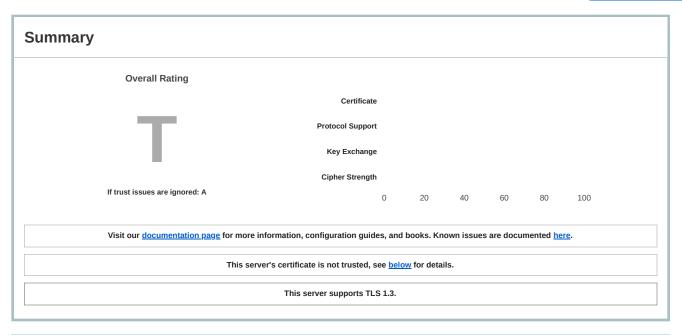
Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > a3.tuyaeu.com > 18.195.249.137

SSL Report: <u>a3.tuyaeu.com</u> (18.195.249.137)

Assessed on: Mon, 10 Jun 2024 19:32:28 UTC | Hide | Clear cache

Scan Another »



Certificate #1: RSA 2048 bits (SHA256withRSA)

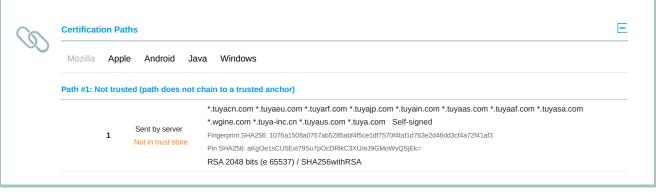


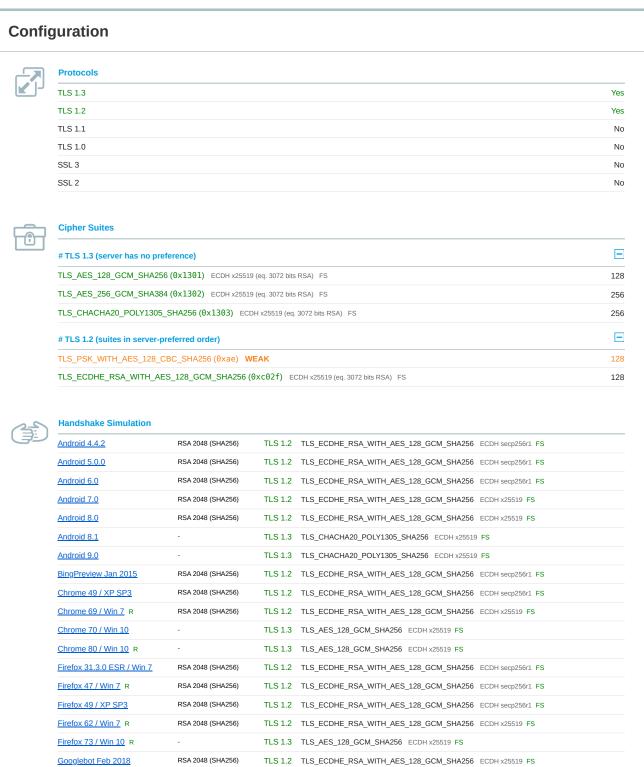
Server Key and Certificate #1	
Subject	*.tuyacn.com *.tuyaeu.com *.tuyarf.com *.tuyajp.com *.tuyain.com *.tuyaas.com *.tuyaaf.com *.tuyasa.com *.wgine.com *.tuya-inc.cn *.tuyaus.com *.tuya.com Fingerprint SHA256: 1076a1508a0757ab5285abf4f5ce1df7570f4bd1d763e2d46dd3cf4a72f41af3 Pin SHA256: aKgOe1sCU5Ext79Su7pOcDRIkC3XU/eJ9GMoWvQSjEk=
Common names	*.tuyacn.com *.tuyaeu.com *.tuyarf.com *.tuyajp.com *.tuyain.com *.tuyaas.com *.tuyaaf.com *.tuyasa.com *.wgine.com *.tuya-inc.cn *.tuyaus.com *.tuya.com
Alternative names	- INVALID
Serial Number	0086cd856e1ee3ae33
Valid from	Wed, 31 Oct 2018 05:30:48 UTC
Valid until	Fri, 07 Oct 2118 05:30:48 UTC (expires in 94 years and 3 months)
Кеу	RSA 2048 bits (e 65537)
Weak key (Debian)	No
ssuer	*.tuyacn.com Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
ONS CAA	No (more info)
Trusted	No NOT TRUSTED (<u>Why2</u>) Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	1 (2002 bytes)
Chain issues	None





<u>IE 11 / Win 7</u> R	Server sent fatal alert:	handshake	<u> failure</u>			
<u>IE 11 / Win 8.1</u> R	Server sent fatal alert:	handshake	_failure			
IE 11 / Win Phone 8.1 R	Server sent fatal alert:	handshake	_failure			
IE 11 / Win Phone 8.1 Update	R Server sent fatal alert:	handshake	_failure			
<u>IE 11 / Win 10</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS			
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS			
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS			
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
<u>Java 8u161</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS			
OpenSSL 1.0.1I R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS			
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS			
Safari 6 / iOS 6.0.1	Server sent fatal alert:	handshake	<u>_failure</u>			
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure					
<u>Safari 7 / OS X 10.9</u> R	Server sent fatal alert: handshake_failure					
Safari 8 / iOS 8.4 R	Server sent fatal alert:	Server sent fatal alert: handshake_failure				
<u>Safari 8 / OS X 10.10</u> R	Server sent fatal alert:	handshake	<u>_failure</u>			
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
<u>Safari 9 / OS X 10.11</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
<u>Safari 12.1.2 / MacOS 10.14.6</u> <u>Beta</u> R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS			
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS			
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS			
"Net simulated alients (Dont						
# Not simulated clients (Proto						
Android 2.3.7 No SNI ²	Protocol mismatch (no		,			
Android 4.0.4	Protocol mismatch (not simulated)					
Android 4.1.1	Protocol mismatch (not simulated)					
Android 4.2.2	Protocol mismatch (not simulated)					
Android 4.3	Protocol mismatch (no		<u> </u>			
Baidu Jan 2015	Protocol mismatch (no					
IE 6 / XP No FS ¹ No SNI ²	Protocol mismatch (no					
IE 7 / Vista	Protocol mismatch (no	t simulated)			
IE 8 / XP No FS ¹ No SNI ²	Protocol mismatch (no	t simulated)			
<u>IE 8-10 / Win 7</u> R	Protocol mismatch (no	t simulated)			
IE 10 / Win Phone 8.0	Protocol mismatch (no	t simulated)			
Java 6u45 No SNI ²	Protocol mismatch (no	t simulated				
Java 7u25	Protocol mismatch (no	t simulated				
OpenSSL 0.9.8y	Protocol mismatch (no	t simulated				
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (no	t simulated				
Safari 6.0.4 / OS X 10.8.4 R	Protocol mismatch (no	t simulated				

 $^{(3) \} Only \ first \ connection \ attempt \ simulated. \ Browsers \ sometimes \ retry \ with \ a \ lower \ protocol \ version.$

⁽R) Denotes a reference browser or client, with which we expect better effective security.

Handshake Simulation

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.



Protocol Details

Protocol Details	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	Unknown (more info)
GOLDENDOODLE	Unknown (more info)
OpenSSL 0-Length	Unknown (more info)
Sleeping POODLE	Unknown (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



1 https://a3.tuyaeu.com/ (HTTP/1.1 404 Not Found)



Miscellaneous

Test date Mon, 10 Jun 2024 19:30:08 UTC

Test duration	70.483 seconds	
HTTP status code	404	
HTTP server signature	https	
Server hostname	ec2-18-195-249-137.eu-central-1.compute.amazonaws.com	

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

- 1. Invalid certificate
- 2. Invalid configuration
- 3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- · It is used before its activation date
- · It is used after its expiry date
- · Certificate hostnames don't match the site hostname
- · It has been revoked
- · It has insecure signature
- · It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.3.0

Copyright © 2009-2024 Qualys, Inc. All Rights Reserved. Privacy Policy.

Terms and Conditions

Iry Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.