Check a DANE TLS Service

This application checks a DANE TLS Service. It connects to the specified TLS service and then attempts to authenticate its TLS server certificate according to its corresponding DANE TLSA records in the DNS.

Port: 5222
Domain name: babai.ru
STARTTLS application: xmpp-client
DANE-EE Name Checks: Yes

DANE Authentication Successful.

Checking Transcript:

```
TLSA records found: 1
TLSA: 3 1 1 5079a8929a1782bc2626ec8718628152ca4c15bc4e49b94aca377be148b5e108

Connecting to IPv6 address: 2a07:ac80:0:4b::2 port 5222
send: <?xml version='1.0'?><stream:stream to='babai.ru' version='1.0' xml:lang='en' xmlns='jabber:client' xmlns:stream='http://eth
recv: <?xml version='1.0' encoding='UTF-8'?><stream:stream xmlns:stream="http://etherx.jabber.org/streams" xmlns="jabber:client" f
recv: <stream:features><starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"><required/></starttls><mechanisms xmlns="urn:ietf:params:
send: <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
recv: <proceed xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>
TLSv1.2 handshake succeeded.
Cipher: TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
Peer Certificate chain:
 0 Subject CN: www.babai.ru
   Issuer  CN: Thawte TLS RSA CA G1
 1 Subject CN: Thawte TLS RSA CA G1
   Issuer  CN: DigiCert Global Root G2
 SAN dNSName: www.babai.ru
 SAN dNSName: babai.ru
DANE TLSA 3 1 1 [5079a8929a17...] matched EE certificate at depth 0
Verified peername: babai.ru
Validated Certificate chain:
 0 Subject CN: www.babai.ru
   Issuer  CN: Thawte TLS RSA CA G1
 SAN dNSName: www.babai.ru
 SAN dNSName: babai.ru

Connecting to IPv4 address: 185.158.115.215 port 5222
send: <?xml version='1.0'?><stream:stream to='babai.ru' version='1.0' xml:lang='en' xmlns='jabber:client' xmlns:stream='http://eth
recv: <?xml version='1.0' encoding='UTF-8'?><stream:stream xmlns:stream="http://etherx.jabber.org/streams" xmlns="jabber:client" f
recv: <stream:features><starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"><required/></starttls><mechanisms xmlns="urn:ietf:params:
send: <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
recv: <proceed xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>
TLSv1.2 handshake succeeded.
Cipher: TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
Peer Certificate chain:
 0 Subject CN: www.babai.ru
   Issuer  CN: Thawte TLS RSA CA G1
 1 Subject CN: Thawte TLS RSA CA G1
   Issuer  CN: DigiCert Global Root G2
 SAN dNSName: www.babai.ru
 SAN dNSName: babai.ru
DANE TLSA 3 1 1 [5079a8929a17...] matched EE certificate at depth 0
Verified peername: babai.ru
Validated Certificate chain:
 0 Subject CN: www.babai.ru
   Issuer  CN: Thawte TLS RSA CA G1
 SAN dNSName: www.babai.ru
 SAN dNSName: babai.ru

[0] Authentication succeeded for all (2) peers.
```

Check another DANE service?

Other DANE Tools

- Check a DANE TLS SMTP Service
- Generate a DNS TLSA record
- Generate a DNS OPENPGPKEY record
- DANE TLS Test Sites

References

- RFC 6698: DANE and TLSA record specification, August 2012
- RFC 7671: DANE Protocol: Updates and Operational Guidance
- RFC 7672: SMTP Security via opportunistic DANE TLS
- DNSSEC and Certificates; October 19 2012
- How DANE Strengthens Security for TLS, S/MIME, and Other Applications; November 2015
- Shumon Huque's website