Ruby trunk - Bug #6493

OpenSSL::SSL ignores DN if subjectAltName is specified

05/25/2012 07:46 AM - djmitche (Dustin Mitchell)

Status:	Feedback		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	trunk	**Backport:**	

Description

In ext/openssl/lib/openssl/ssl.rb, verify_certificate_identity seems to intentionally *not* check the DN if any subjectAltName extensions are found.

RFC3280 says

The subject alternative names extension allows additional identities
to be bound to the subject of the certificate. ...

which suggests that it contains *additional* identities, and thus does not exclude the subject.

This functionality was added way back in 2005, r7970:

```
* ext/openssl/lib/openssl/ssl.rb
  (OpenSSL::SSL::SSLSocket#post_connection_check): new method.
```

and moved around several times since then.

History

#1 - 05/25/2012 08:22 AM - drbrain (Eric Hodel)

- Category set to ext

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

- Target version set to 2.0.0

#2 - 05/25/2012 09:48 AM - MartinBosslet (Martin Bosslet)

- Status changed from Assigned to Feedback

- Priority changed from Normal to 3

RFC 3280 was obsoleted by 5280 and there, the wording is slightly different:

8<--------

4.2.1.6. Subject Alternative Name

The subject alternative name extension allows identities to be bound
to the subject of the certificate. These identities may be included
in addition to or in place of the identity in the subject field of
the certificate.

8--------

But I think we should orient ourselves at RFC 6125 [1], which
explicitly addresses how to do hostname verification for TLS services.

There, it says:

8<------

6.4.4. Checking of Common Names

As noted, a client MUST NOT seek a match for a reference identifier of CN-ID if the presented identifiers include a DNS-ID, SRV-ID, URI-ID, or any application-specific identifier types supported by the client.

8------

Therefore current behavior is in line with this and correct in doing so. But what's missing is verification of the service type parts and interpretation of the otherName attributes of type srvName (RFC4985), I could imagine adding support in the future, especially if CAs start to follow these recommendations.

But I'll mark this as low prio for now if nobody objects.

[1] http://tools.ietf.org/html/rfc6125

#3 - 02/18/2013 09:46 PM - mame (Yusuke Endoh)

- Target version changed from 2.0.0 to 2.6

#4 - 09/13/2015 03:32 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl