pfSense - Feature #2765

Allow generation an x509 certificates with an SHA256 signature hash

01/19/2013 07:09 PM - Dim Hatz

Status:	Resolved	**Start date:**	01/19/2013
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:			

Description

Apparently pfsense's Cert Manager has hard-coded the use of SHA-1 for all PKI operations ("digest_alg" => "sha1" in /etc/inc/certs.inc).

It'd be nice to allow user-selectable digest_alg (options would be sha224/sha256/sha384/sha512), since according to Wiki & NIST "cryptographic weaknesses were discovered in SHA-1 and the standard is no longer approved for most cryptographic uses after 2010".

Associated revisions

Revision ca621902 - 01/21/2013 01:33 PM - Jim Pingle

Allow selecting the digest algorithm when creating a CA or Cert. Implements #2765

History

#1 - 01/19/2013 08:03 PM - Dim Hatz

Just quick update:

1) The relevant keyword in openssl.cnf is default_md = sha256 # (md5/sha512/etc)
2) For openssl command-line -sha256 is correct for commandline req including req -x509, and x509 including x509 -req, but not for "openssl ca". ca uses -md sha256.

#2 - 01/19/2013 08:45 PM - Jim Pingle

- Assignee set to Jim Pingle

I'd hate to hardcode a list, but openssl doesn't appear to have a good way to list the available message digest algorithms in the version we use. "openssl list-message-digest-commands" doesn't contain all the right ones, and "list-message-digest-algorithms" seems to only be in OpenSSL >= 1.0.

Passing an invalid parameter to "openssl dgst" such as "openssl dgst -h" can get one somewhat but it's still would be awkward to parse.

May be better to hardcode in the long run since many of these are probably unsuitable anyhow...

```
-md5            to use the md5 message digest algorithm (default)
-md4            to use the md4 message digest algorithm
-md2            to use the md2 message digest algorithm
-sha1           to use the sha1 message digest algorithm
-sha            to use the sha message digest algorithm
-sha224         to use the sha224 message digest algorithm
-sha256         to use the sha256 message digest algorithm
-sha384         to use the sha384 message digest algorithm
-sha512         to use the sha512 message digest algorithm
-mdc2           to use the mdc2 message digest algorithm
-ripemd160      to use the ripemd160 message digest algorithm
```

#3 - 01/19/2013 09:22 PM - Dim Hatz

Based on some searching I did earlier, it seems that the only ones suitable are:

sha1 (with the above mentioned reservations)
sha224
sha256
sha384
sha512

A quick checking of Root CAs (Verisign, Thawte, Godaddy etc), suggests that they are transitioning to sha256/RSA2048 or better.

PS: Since we're talking about networking gear, there is also a related table by Cisco at
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

#4 - 01/21/2013 01:40 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset ca6219025cabd3edbe53e522b345a167381a0171.

#5 - 04/01/2013 02:01 PM - Jim Pingle

- Status changed from Feedback to Resolved