pfSense - Feature #9843

allow to generate cert/csr with ECDSA key

10/23/2019 03:50 AM - Viktor Gurov

Status:	Resolved	**Start date:**	10/23/2019
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.5.0		

Description

Add ability to generate certificates/CSRs with ECDSA keys.

Associated revisions

Revision c3cda38e - 11/14/2019 07:43 AM - Jim Pingle

Change default ECSDA curve to prime256v1. Issue #9843

Previous default was brainpool, but brainpool curves are not (widely?)
supported by browsers and were deprecated by IETF for TLS v1.3

Revision cffcf9bf - 11/14/2019 02:59 PM - Jim Pingle

GUI improvements for ECDSA certificate handling

- Make central functions to check and test ECDSA compatibility. Issue #9843
- Filter incompatible certificates from being offered for the GUI or Captive Portal. Implements #9897
- Do the same for IPsec, which implements #4991
- Add a check for key type when generating ipsec.secrets to allow ECDSA certs to work in IPsec for issue #4991

Note that as of this moment, the following curves are known to be compatible:
HTTPS (GUI, Captive Portal): prime256v1, secp384r1
IPsec: prime256v1, secp384r1, secp521r1

Results may vary in other areas which are not yet well-tested, and in packages.

History

#1 - 10/23/2019 03:52 AM - Viktor Gurov

https://github.com/pfsense/pfsense/pull/4104

#2 - 10/23/2019 07:59 AM - Jim Pingle

- Status changed from New to Pull Request Review

- Assignee set to Jim Pingle

#3 - 10/25/2019 07:25 AM - Jim Pingle

- Target version set to 2.5.0

#4 - 10/25/2019 04:05 PM - Jim Pingle

- Status changed from Pull Request Review to Feedback

- % Done changed from 0 to 100

PR has been merged

#5 - 11/10/2019 04:40 AM - Viktor Gurov

Jim Pingle wrote:

> PR has been merged

Tested on 2.5.0.a.20191109.1723

Resolved

#6 - 11/10/2019 10:35 AM - Jim Pingle

- Status changed from Feedback to Resolved

Files

Screenshot from 2019-10-23 11-47-52.png	39.4 KB	10/23/2019	Viktor Gurov