Web site - Feature # 137: keys/ssh.txt should include SHA256 fingerprints

Status:	Closed	**Priority:**	Normal
Author:	admin	**Category:**	
Created:	2016-05-05	**Assigned to:**	
Updated:	2016-05-05	**Due date:**	
Subject:	keys/ssh.txt should include SHA256 fingerprints		

Description:	Modern SSH clients display the server fingerprints using base64-encoded SHA256, but https://bitfolk.com/keys/ssh.txt only contains hex-encoded MD5 fingerprints because that's all that @ssh-keygen@ outputs. As a result it's harder to verify that the server's hostkey is correct:
	
	<pre>
	23:28:39 < lozsui> Hello, ssh to my_username.console.bitfolk.com returns fingerprint SHA256:OgL4oAynSfr6ZI2YviQhVWgHQqjEfvOC3BiZPEVPEtc.
	23:29:38 < lozsui> I can not find that fingerprint on https://bitfolk.com/keys/ssh.txt. How can I verify it?
	23:30:17 <+dne> ssh -oFingerprintHash=md5 ....
	23:32:15 <@grifferz> hmm if there is a way for me to show them as SHA256 then I will add that to keys.txtâ€¦
	</pre>		

History

2016-05-05 03:29 - admin

I found a convoluted shell command line to generate base64-encoded SHA256 hashes of the keys so here is a script to generate the sections for keys.txt:

https://gist.github.com/grifferz/c54fae0d82a5ceecd6b90087b4f87df5

2016-05-05 03:35 - admin

- Subject changed from keys.txt should include SHA256 fingerprints to keys/ssh.txt should include SHA256 fingerprints

2016-05-05 04:00 - admin

- Status changed from New to Closed

The SHA256 hashes have now been added.