Billing - Bug # 107: Billing e-mails are DKIM signed with a weak key

Status:	Closed	**Priority:**	Normal
Author:	vinaigre	**Category:**	
Created:	2013-09-05	**Assigned to:**	
Updated:	2013-09-08	**Due date:**	
Subject:	Billing e-mails are DKIM signed with a weak key		

Description:

Billing e-mails are DKIM signed with a weak (too small) key. See

   http://www.kb.cert.org/vuls/id/268267

Gmail treats e-mails signed with less than 1024-bit keys as unsigned:

   https://support.google.com/mail/answer/180707?hl=en

and so does OpenDKIM, by default (from version 2.6.8):

```
<pre>
Authentication-Results: foo.example.net; dkim=permerror
 reason="verification error: signing key too small; insecure key"
 header.d=bitfolk.com header.i=@bitfolk.com header.b=T5zEhgDB;
 dkim-adsp=none (insecure policy); dkim-atps=neutral
</pre>
```

History

2013-09-06 15:09 - admin

I think I've fixed this now. Can you have a look, when you get your next email from bitfolk.com?

Thanks for bringing this to my attention!

2013-09-08 13:09 - vinaigre

The last e-mail was DKIM signed with a 2048-bit key, and passed verification by OpenDKIM.

2013-09-08 16:09 - admin

- Status changed from New to Closed