Redmine - Patch #35217

Replace use of Digest::MD5 / Digest::SHA1 with ActiveSupport::Digest

2021-05-07 05:02 - Jens Krämer

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Rails introduced ActiveSupport::Digest to allow central configuration of the actual digest implementation that is used throughout Rails. This is helpful in environments where certain digest implementations (most notably, MD5) are not available, i.e. to be FIPS compliant.

The attached patch replaces all uses of Digest::SHA1 and Digest::MD5 with ActiveSupport::Digest. Without further configuration, this will result in Digest::SHA1 being used in all these instances since that's the current Rails default. This can be changed by users via the config.active_support.hash_digest_class setting , i.e.:

```
Rails.application.config.active_support.hash_digest_class = OpenSSL::Digest::SHA256
```

History

#1 - 2021-05-07 15:14 - Pavel Rosický

thanks for working on this!

however, the OpenID change isn't safe. The SHA1 algorithm is hardcoded here and your change will break it.
https://github.com/redmine/redmine/blob/49e323ae7af2998fc2785319643a9ac5bc93c425/lib/plugins/open_id_authentication/test/mem_cache_store_test.rb#L126

https://github.com/openid/ruby-openid do support SHA256, maybe add an option to choose it? It has to be a separate option, it can't depend on Rails.application.config.active_support.hash_digest_class

the second missing part is gravatars https://github.com/redmine/redmine/blob/master/lib/plugins/gravatar/lib/gravatar.rb#L68
as discussed in https://www.redmine.org/boards/2/topics/65253 I don't think there's a way to support this feature without MD5, so if the digest isn't available, the feature has to be disabled.

Files

0001-replaces-uses-of-Digest-MD5-and-Digest-SHA1-with-AS-.patch	11.1 KB	2021-05-07	Jens Krämer