Ruby trunk - Feature #6943

pstore in FIPS mode

08/28/2012 03:40 PM - vo.x (Vit Ondruch)

Status:	Closed	
Priority:	Normal	
Assignee:	openssl	
Target version:		

Description

Is there any chance to make PStore compatible with FIPS mode? PStore is using MD5 for data checksum, but MD5 is unsupported algorithm in FIPS mode unfortunately. It would be easy to use different hash algorithm, but I am afraid that backward compatibility would be lost. Thank you.

Related issues:

Related to Ruby trunk - Feature #6946: FIPS support?	**Open**

Associated revisions

Revision 9f9add3e - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@56284 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56284 - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]

Revision 56284 - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]

Revision 56284 - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]

Revision 56284 - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]

History

#1 - 11/20/2012 11:25 PM - mame (Yusuke Endoh)

- Target version set to 2.6

#2 - 12/20/2012 10:23 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

#3 - 09/13/2015 03:15 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl

#4 - 06/07/2016 11:04 AM - vo.x (Vit Ondruch)

Ping? Any chance to change the hashing algorithm?

#5 - 06/10/2016 12:25 PM - naruse (Yui NARUSE)

lib/pstore.rb uses digest/md5, and it uses own implementation (ext/digest/md5/md5.c) if there's no openssl
or it doesn't support MD5, it extconf.rb works correctly.

#6 - 06/28/2016 12:13 PM - vo.x (Vit Ondruch)

Using internal implementation is just hiding the issue. I don't think this would be acceptable solution for FIPS certification, what would be the point then? It is quite easy to generate colliding hashes these days. It might not be that critical for PStore though ...

#7 - 06/28/2016 02:03 PM - nobu (Nobuyoshi Nakada)

Seems nothing to block, since md5 seems used just to see if the data is modified.

https://github.com/ruby/ruby/compare/trunk...nobu:feature/6943-pstore-checksum_algorithm

#8 - 09/28/2016 02:14 PM - nobu (Nobuyoshi Nakada)

- Status changed from Assigned to Closed

Applied in changeset r56284.

PStore: select checksum algorithm

- lib/pstore.rb (PStore::CHECKSUM_ALGO): find available hashing algorithm for checksum. MD5 is not available in FIPS mode. [Feature #6943]