

Anubis - Bug #2

Les fonctions sha1 et md5 présentent un risque de bug avec les type String

08/03/2007 10:47 PM - Anonymous

Status:	Assigned	Start date:	
Priority:	High	Due date:	
Assignee:	Alain Prouté	% Done:	0%
Category:	Compiler	Estimated time:	0.00 hour
Target version:	1.10	Triage Stage:	
Platform:			
Resolution:			
Description			
Les fonctions sha1 et md5 attendent n'importe quel type sérialisable en entrée. Or lorsqu'on lui passe un String, on s'attend à ce que ce soit le contenu de la chaine qui soit utilisé pour le calcul du SHA1 ou du MD5. Or il se trouve que c'est l'objet String en entier qui est calculé. C'est donc source d'erreur évidente, et très difficile à prévenir. Or pour le cas particulier du String, signer l'objet complet ou signer son contenu, c'est aussi pertinent dans un cas comme dans l'autre. C'est donc absolument équivalent. Donc pour simplifier et réduire les risques, il faudrait directement dans predefined.anubis créer des versions surchargées pour le type String ne fonctionnant que sur le contenu.			

History

#1 - 08/14/2007 09:43 PM - Alain Prouté

Replying to [comment:1 totoro]:

#2 - 08/14/2007 09:56 PM - Anonymous

Comment (by alp)

In my opinion (when I designed these functions), it was not a bug, because I considered that only `[[ByteArray]]?` may be hashed, and consequently, any serializable datum may be hashed. In this context, 'String' (which is serializable) has nothing particular.

Nevertheless, there is a problem because people are used to hash strings. It seems hat the right solution is to modify the whole system so that 'String' becomes just an alias for 'ByteArray?'. There are several other reasons for doing that. Of course, this may be a lot of work.

For the time being, what we could do (but I don't like that) may be to add specific primitives for 'String', named 'md5_String' and 'sha1_String' for example.

#3 - 09/21/2007 10:32 PM - Alain Prouté

- Status changed from New to Assigned

This problem will be resolved automatically when String will be just an alias of `[[ByteArray]]`.

#4 - 10/03/2007 11:26 PM - Anonymous

Same as above, but for blowfish functions too...

#5 - 01/20/2009 09:00 AM - Anonymous

- *Target version changed from 1.9 to 1.10*
- *Platform deleted (All)*