

Ruby - Bug #19309

Fix `OpenSSL::X509::CertificateError: invalid digest` on CentOS 9 / RHEL 9

01/05/2023 09:19 AM - vo.x (Vit Ondruch)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.2.0 (2022-12-25 revision a528908271) [x86_64-linux]	Backport: 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN
Description CentOS 9 / RHEL 9 requires prohibits SHA1 for signing purposes, therefore these specs fail: 1) OpenSSL::X509::Name.verify returns true for valid certificate ERROR OpenSSL::X509::CertificateError: invalid digest /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:15:in `sign' /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:15:in `block (2 levels) in <top (required)>' /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:4:in `<top (required)>' 2) OpenSSL::X509::Name.verify returns false for an expired certificate ERROR OpenSSL::X509::CertificateError: invalid digest /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:31:in `sign' /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:31:in `block (2 levels) in <top (required)>' /builddir/build/BUILD/ruby-3.2.0/spec/ruby/library/openssl/x509/name/verify_spec.rb:4:in `<top (required)>' I have opened PR here , but I'd also like see this backported into 3.2, hence also reporting here.		

History

#1 - 01/05/2023 09:22 AM - vo.x (Vit Ondruch)

- Status changed from Open to Closed