Information about Requiring the SHA-2 Hash Function

Article Number: 1381 | Rating: 1/5 from 3 votes | Last Updated: Wed, Dec 2, 2020 at 6:00 PM
All SSL certificates using the old SHA-1 hash function need to be re-keyed to use the SHA-2 hash function immediately. SHA-1 is potentially insecure, which defeats the purpose of an SSL certificate. **Additional Information** SSL certificates scramble (or encrypt) communication between your website's server and your visitor's browser in such a way that only they understand what the other is saying. This interference prevents others from eavesdropping on the conversation and picking up things you don't want them to know about: typically secure information like credit card and Social Security numbers. This encryption is done using aÂ hash function. Though they encrypt different information, code signing certificates also use the same hash function to "sign" executable code when its developer releases it. If the code is tampered with, the hashed signature doesn't work and the user is warned when they try to run it. The hash function we most commonly used prior to Dec. 23, 2013, was called SHA-1; it has been around since SSL certificates were first developed in the mid-1990s. However, as computers increase in power, it's becoming more feasible for SHA-1-hashed information to get decrypted. Because of that, MicrosoftÂ® is driving a new industry guideline that requires all Certificate Authorities, including us, to begin using SHA-2 as our default hash function. Google is also on board and will have its browser ChromeÂ® begin warning visitors of security issues with certificates using SHA-1. **Does my certificate have to use SHA-2?** New certificates we issue with expiration dates after Jan. 1, 2017, can only use SHA-2. Code-signing certificates with expiration dates after Dec. 31, 2015 must also use SHA-2, with the exception that SHA-1 code signing certificates may continue to be used to sign files for use on Windows Vista and earlier versions of Windows. You can find more information in Microsoft's articleÂ Windows Enforcement of Authenticode Code Signing and Timestamping. Certificates that have already been issued do not need to begin using SHA-2, but we highly recommend it. Moving over to it now future-proofs and improves the security of your server. You can switch your hash function to SHA-2 by simply re-keying your certificate..

Posted - Wed, Dec 2, 2020 at 6:00 PM.
Online URL:
https://www.heartinternet.uk/support/article/information-about-requiring-the-sha-2-hash-function.html