net.shrine.protocol.version.CouldNotVerifySignature

Summary

The trust relationship between two SHRINE nodes could not be established.

Explanation

This problem can happen for one of several reasons:

1. The system clock on the receiving machine may be incorrect.
2. The certificate offered up by the querying site is not trusted by the hub or adapter due to a configuration problem.

Since

1.26

Resolution

If you are a researcher, forward the details of the error on to your local site administrator.

The rest of these resolution steps must be followed by the site administrator:

The exact path of resolution can vary depending on the underlying cause. These resolutions match with their corresponding number in the **Details** section.

1. Check the server's date and time and make sure the system clock is properly synced using ntpd.
2. Ensure that the certificate used for signing queries is trusted by the site that reported this error, and ensure that your site trusts any certificates used by the site that reported this error.
3. *If using CA trust model:* Make sure that the PrivateKeyEntry in the SHRINE keystore has the SHRINE hub's information on the "Issuer:" line.
4. *If using CA trust model:* Ensure that the CA-signed version of the originating site's certificate was imported properly. Ensure that the Hub or Adapter properly trusts the CA cert.