net.shrine.adapter.service.CouldNotVerifySignature

Summary

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

Explanation

This problem can happen for one of several reasons:

1. Clock drift between the site that the query originated at and the receiving site. Messages are time-sensitive, and although the allowable gap in time is somewhat forgiving, a misconfigured system clock can cause failure.
2. The certificate offered up by the querying site is not trusted by the adapter due to a configuration problem.
3. *If using CA trust model:* Ensure that the CA-signed version of the originating site's certificate was imported properly. Ensure that the Adapter properly trusts the CA cert.

Resolution

If you are a user, 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 **Explanation** 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.