Accessing Secure Web Services

SOAPam provides several different mechanisms to allow you to access Web services securely. Which mechanism you must use, if any, is dictated by Web service.

HTTP Authentication

The Client Process automatically negotiates HTTP Basic or Digest authentication with the Web service host using credentials you provide. Refer to Using HTTP Authentication for details.

Client Certificates

During secure connection negotiation, the Client Process can transmit a provided PKCS12 client certificate in order to identify itself to the Web service host. Refer to Using Client Certificates for details.

Secure Credentials Files

SOAPam can securely store user id and password information in encrypted credentials files that can only be decrypted by the Client Process. This eliminates the need to store credentials in clear text in the Client Process configuration. Refer to Using Credential Files for details.

Secure Connections

By specifying "https" as the protocol scheme for a Web service endpoint, the Client Process will negotiate a secure SSLv3 or TLS v1 connection with the Web service host and verify the host's server certificate against a local list of trusted Certificate Authorities. Refer to Using Secure Connections for details.