GSSException::getOutputToken()

Wang Weijun

weijun.wang@oracle.com

background

- In JGSS-API (RFC 5653), the GSSContext::initSecContext() method could either return a token when the call succeeds or throw a GSSException if there is a failure, but NOT both. The same applies to acceptSecContext() of the same class.
- On the other hand, the C function GSS_Init_sec_context() can fill out an output token even if there is an error.

problem

- Without the ability to emit an error token when there is a failure, a Java application has no chance to tell the other side what the error is. For example, a "reject" NegTokenResp token will never be able to sent out for the SPNEGO mechanism.

solution

- Embed the token into the GSSException:

  ```
  public byte[] getOutputToken()
  ```

  If the method (For example, initSecContext of GSSContext) that throws this GSSException also needs to generate an output token that should be sent to the peer, that token will be returned by this method.

  The return value should be null if no such token is generated. This method should never return an empty byte array.

- An accompany method setOutputToken() will also be added to GSSException

example

```
try {
   do {
      byte[] outTok = context.initSecContext(inTok, 0, inTok.length);
      if (outTok != null) sendToken(outTok);
      if (context.isEstablished()) break;
      inTok = readToken();
   } while (true);
} catch (GSSException e) {
   print("GSSAPI error: " + e.getMessage());
   if (e.getOutputToken() != null) {
      sendToken(e.getOutputToken());
   }
}
```

references

- The current RFC 5653
  http://tools.ietf.org/html/rfc5653
- Intended changes
  http://cr.openjdk.java.net/~weijun/spec/updates-error-token.txt