Servicios Web Seguros

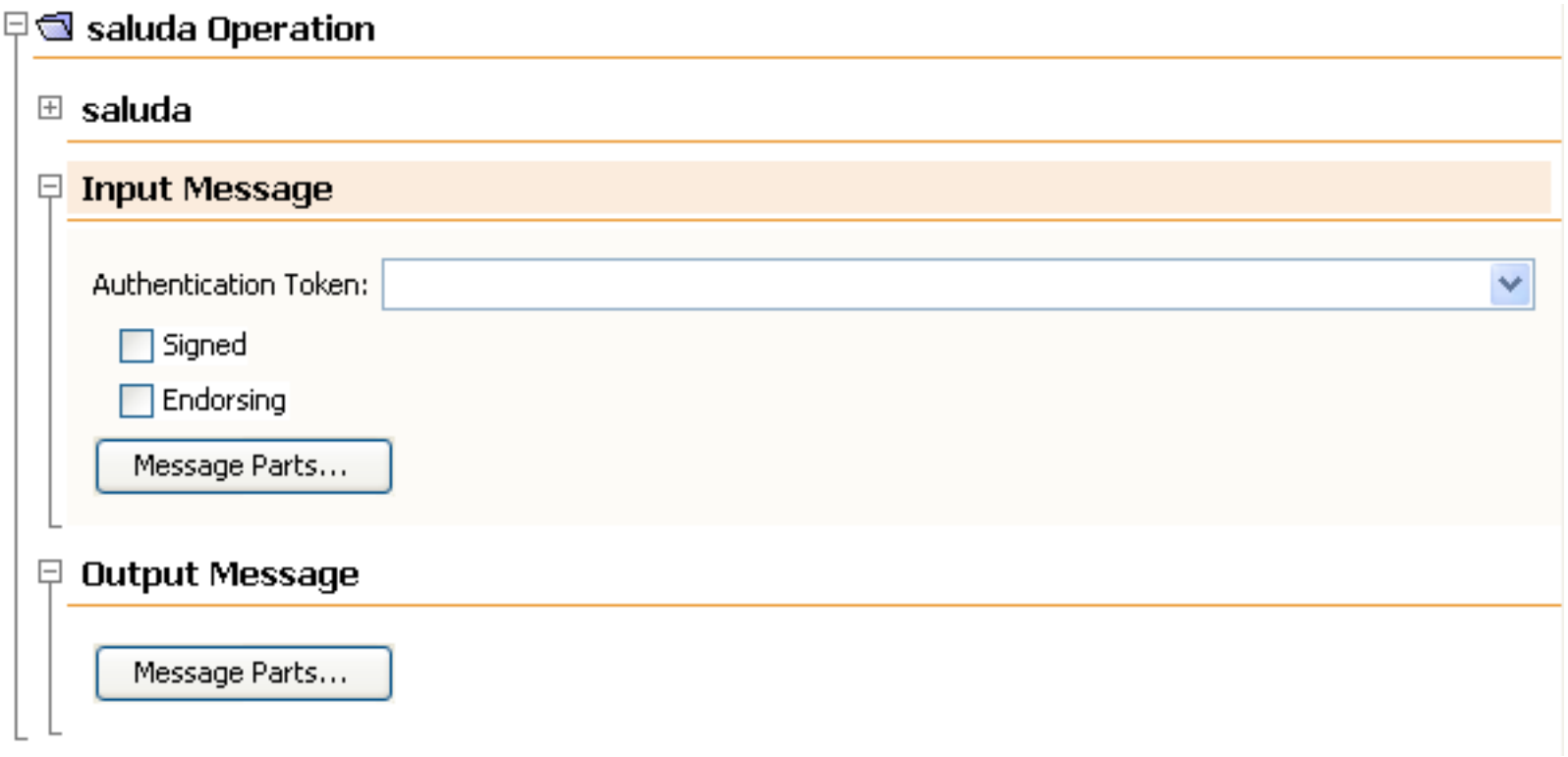
Sesión 12: Metro. Seguridad de nivel de mensaje

Puntos a tratar

- Configuración de la seguridad a nivel de mensaje en NetBeans
- Seguridad a nivel de mensaje con clave asimétrica
- Clave simétrica y autentificación mediante nombre de usuario
- Clave simétrica y autentificación mediante certificado digital
- Entorno *Single Sign-On*

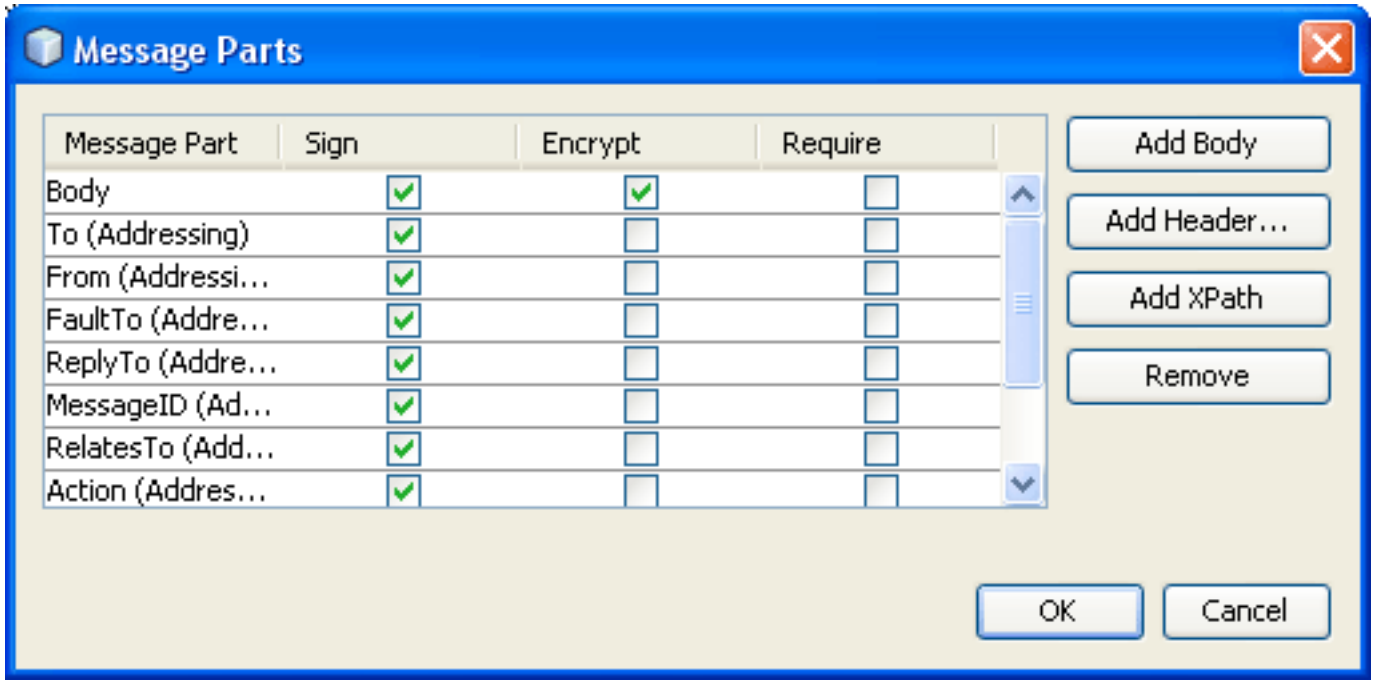
Configuración en NetBeans

- Petición, respuesta, y partes del mensaje



Partes del mensaje

- Firmadas, cifradas, y obligatorias



Clave asimétrica

- *Mutual Certificates Security*
- Especificar *keystore* y *truststore* tanto en el cliente como en el servicio
- El cliente no se crea con la dirección segura
- Certificado del cliente (*InitiatorToken*)
  - Firma la petición (va adjunto)
  - Cifra la respuesta
- Certificado del servicio (*RecipientToken*)
  - Firma la respuesta (no se adjunta)
  - Cifra la petición

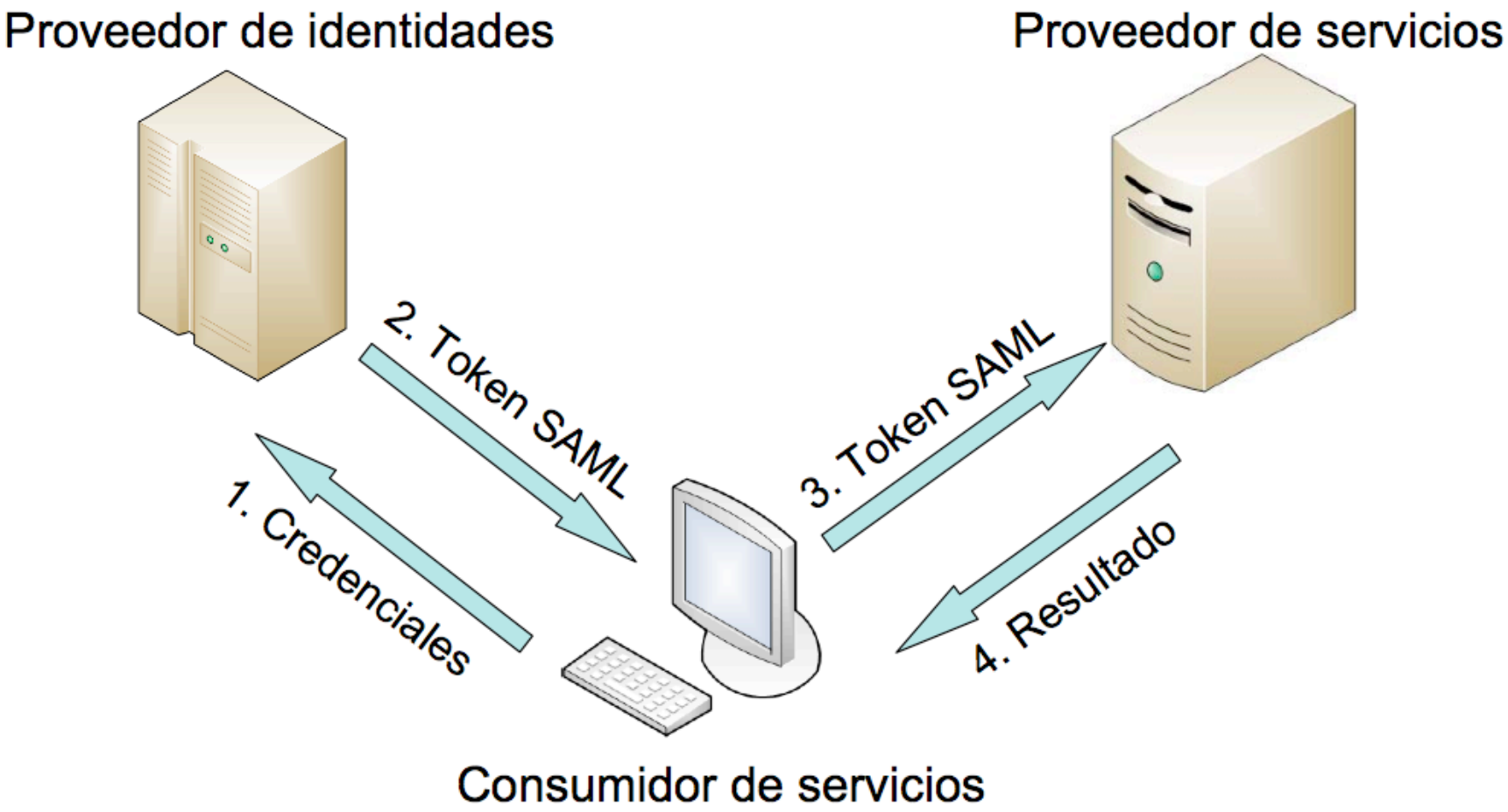
Clave simétrica y *username token*

- *Username Authentication with Symmetric Key*
- Indicar *keystore* y alias en el servicio y *truststore* en el cliente
- Configurar usuarios (en cliente y servidor)
- Certificado del servicio (*ProtectionToken*)
  - Genera una clave simétrica
  - Se utiliza para la protección (firmar y cifrar) tanto de la petición como de la respuesta
- Login y password
  - Se adjunta al mensaje de petición firmado y cifrado

Clave simétrica con *token* X.509

- *Endorsing Certificate*
- Configurar *keystore* y *truststore* tanto en el cliente como en el servicio
- Certificado del servicio (*ProtectionToken*)
  - Genera una clave simétrica
  - Se utiliza para la protección (firmar y cifrar) tanto de la petición como de la respuesta
- Certificado del cliente
  - Se adjunta en la petición
  - Se utiliza de respaldo (firma la firma original)

Entorno *Single Sign-On*



Proveedor de identidades

- Servicio *Secure Token Service (STS)*
  - Tipo especial de servicio web
  - Proporciona *tokens* de seguridad
  - Normalmente SAML, pero puede ser de cualquier tipo
  - Podemos crearlo con NetBeans
- Otros proveedores
  - Sun Access Manager

Tokens de seguridad para SSO

- SAML Sender Vouches (SV)
  - Acceso mediante un intermediario
  - Relación de confianza entre intermediario y servicio
- SAML Holder of Key (HoK)
  - *Token* firmado por el proveedor
  - El servicio debe poder confiar en el *token*
- Kerberos
  - *Ticket* emitido por un CDC de Kerberos
- STS Issued token
  - Cualquier *token* emitido por un servicio STS

Solución SSO con STS

- Crear proveedor STS
  - Autentificación mediante login y password
  - ¡Cuidado! Múltiples *bugs* en NetBeans 6.8
- Crear servicio
  - Autentificación mediante *STS Issued Token*
- Crear cliente
  - Referencia a proveedor STS
    - Accede con login y password
  - Referencia a servicio
    - Accede con *token* proporcionado por STS

¿Preguntas...?