Confianza en entornos de Servicios Web: WS-Trust y STS

Antonio David Pérez Morales

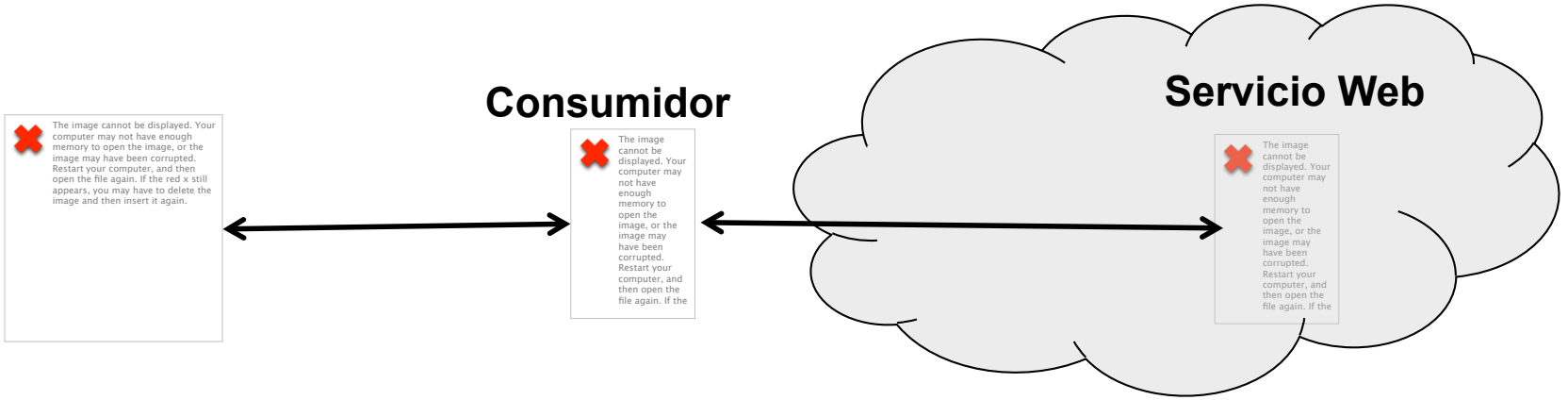
RedIRIS

Índice

- Problema y Motivación
- Objetivos
- WS-Trust y Servicio de Tokens de Seguridad (STS)
  - Modelo de confianza
  - Bases del modelo de confianza
  - Emisión de tokens
  - Validación de tokens
- Escenarios de utilización
- STS en RedIRIS
- Conclusiones
- Referencias

Problema y motivación

¿Cómo se puede obtener esa información de seguridad?



Dominio de seguridad A

-Usuario tiene una cuenta (ej: username, password)

- Usuario hace login

Dominio de seguridad B

- **Recibe un tipo de Información de seguridad**
- **¿Cómo puede saber el Servicio Web que la información de seguridad es válida?**

Objetivos

- Interoperabilidad
  - Permitir a las aplicaciones construir intercambios de mensajes de confianza

- Proporcionar un conjunto flexible de mecanismos que puedan usarse para soportar una amplia gama de protocolos de seguridad

WS-Trust

WS-Trust es una especificación de WS-* y OASIS que ofrece extensiones a WS-Security. Concretamente trata la emisión, renovación y validación de tokens de seguridad, así como la manera de establecer y entablar relaciones de confianza entre los participantes en un intercambio de mensajes seguro

Términos

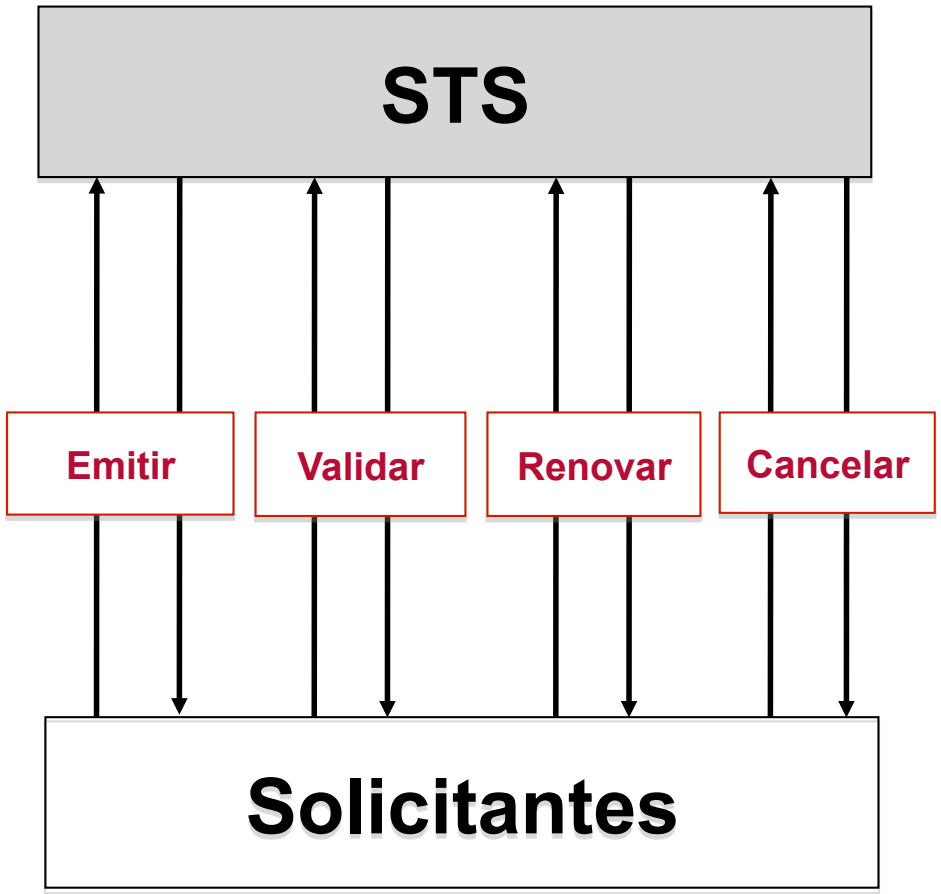
- **Declaración (Claim)**: Es una sentencia hecha sobre un cliente, servicio u otro recurso
- **Token de seguridad**: Representa un conjunto de declaraciones (junto con más información)
- **Servicio de token de seguridad**: Es un servicio que emite tokens de seguridad
- **Confianza**: Es la característica por la que una entidad está dispuesta a depender de una segunda entidad para ejecutar un conjunto de acciones o hacer un conjunto de afirmaciones sobre un conjunto de sujetos

WS-Trust y STS

Servicio Token Seguridad

- Ejerce de autoridad de confianza para
  - Emitir
  - Validar
  - Renovar
  - Cancelar

  tokens de seguridad

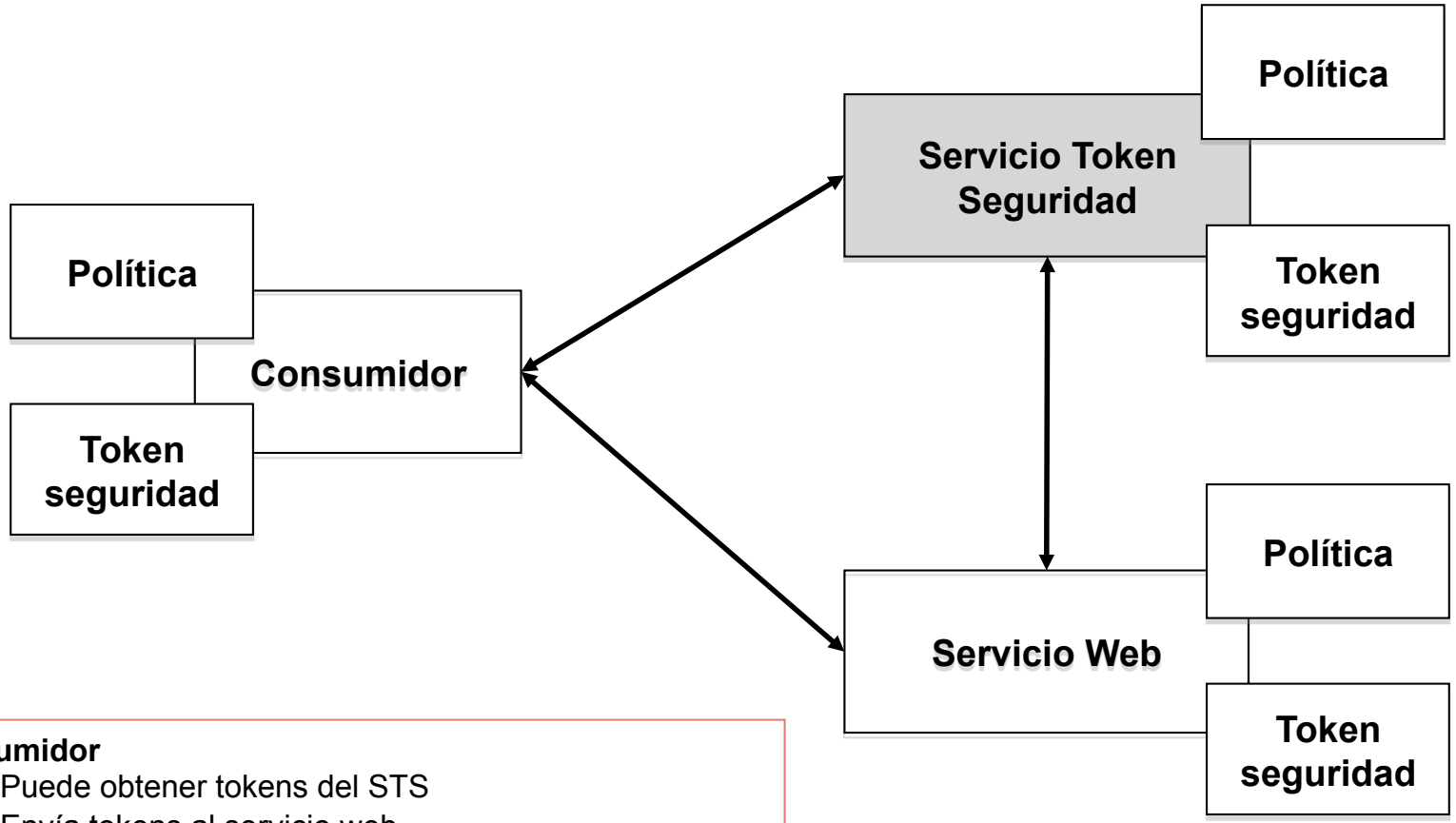


WS-Trust

- Define mecanismos de delegación de
  - Autenticación
  - Autorización
  - Adaptación de información

  a un STS

Modelo de confianza



- **Consumidor**
  - -Puede obtener tokens del STS
  - -Envía tokens al servicio web
- **Servicio Token Seguridad (STS)**
  - -Emite, valida, renueva o cancela tokens de seguridad
- **Servicio Web**
  - - Recibe tokens del consumidor
  - - Puede utilizar el STS para validar el token, o validarlo él mismo

Bases del modelo de confianza

- Un Servicio Web puede requerir que los mensajes entrantes justifiquen un conjunto de declaraciones (claims)
- Estas declaraciones pueden ser:
  - Identidad
  - Permisos
  - Etc
- La forma adecuada de indicar las declaraciones requeridas es a través de políticas
- Si el mensaje entrante (la solicitud) no puede probar las declaraciones requeridas, entonces el Servicio Web debería ignorar o rechazar el mensaje
- El solicitante justifica un conjunto de declaraciones requeridas asociando al mensaje ***tokens de seguridad***
- Si el solicitante no tiene los tokens necesarios para demostrar las declaraciones, puede contactar con las autoridades apropiadas
- Estas autoridades se llaman ***Servicios de token de seguridad (STS)***

Protocolo petición/respuesta de tokens

- El solicitante envía una petición al STS:

  <wst:RequestSecurityToken>

  …

  </wst:RequestSecurityToken>

- El STS responde con:

  <wst:RequestSecurityTokenResponse>

  …

  </wst:RequestSecurityTokenResponse>

Emisión de tokens

Estructura de la petición de emisión

```
<RequestSecurityToken Context="…" xmlns="…">
      <TokenType>…</TokenType>
      <RequestType>…</RequestType>
      <SecondaryParameters>…</SecondaryParameters>
       …
</RequestSecurityToken>
```

- ***TokenType*** ***(opcional)***: Tipo de token solicitado, especificado como URI
- ***RequestType***: El tipo de la petición
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
- ***SecondaryParameters (opcional)***: Otros parámetros RST válidos
- ***…*** : Mecanismo de extensión para añadir otros elementos que no pertenecen a WS-Trust

Emisión de tokens

Estructura de la respuesta de emisión

```
<RequestSecurityTokenResponse Context="…" xmlns="…">
      <TokenType>…</TokenType>
      <RequestType>…</RequestType>
      <RequestedSecurityToken>…</RequestedSecurityToken>
      <SecondaryParameters>…</SecondaryParameters>
        …
</RequestSecurityTokenResponse>
```

- ***TokenType (opcional)***: Tipo de token solicitado, especificado como URI
- ***RequestType***: El tipo de la petición
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
- ***RequestedSecurityToken***: El token de seguridad solicitado
- ***…*** : Mecanismo de extensión para añadir otros elementos que no pertenecen a WS-Trust

Emisión de tokens

Ejemplo de petición de emisión de token

```
<RequestSecurityToken Context="STS" xmlns="…">
    <TokenType>urn: oasis:names:tc:SAML:2.0:assertion</TokenType>
    <RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</RequestType>
    <Claims>
        <User xmlns="…">Test_User</User>
    </Claims>
</RequestSecurityToken>
```

Ejemplo de respuesta de emisión de token

```
<RequestSecurityTokenResponse Context="STS" xmlns="…">
    <TokenType>urn: oasis:names:tc:SAML:2.0:assertion</TokenType>
    <RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</RequestType>
    <RequestedSecurityToken>
        <saml2:Assertion xmlns:saml2="…">…</saml2:Assertion>
    </RequestedSecurityToken>
</RequestSecurityTokenResponse>
```

Validación de tokens

Estructura de la petición de validación

```
<RequestSecurityToken Context="…" xmlns="…">
      <TokenType>…</TokenType>
      <RequestType>…</RequestType>
      <ValidateTarget>…</ValidateTarget>
      <SecondaryParameters>…</SecondaryParameters>
       …
</RequestSecurityToken>
```

- ***TokenType*** ***(opcional)***: Tipo de token, especificado como URI
- ***RequestType***: El tipo de la petición
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/Validate
- ***ValidateTarget***: El token a validar
- ***SecondaryParameters (opcional)***: Otros parámetros RST válidos
- ***…*** : Mecanismo de extensión para añadir otros elementos que no pertenecen a WS-Trust

Validación de tokens

Estructura de la respuesta de validación

```
<RequestSecurityTokenResponse Context="…" xmlns="…">
        <TokenType>…</TokenType>
        <RequestType>…</RequestType>
        <Status>
                <Code>…</Code>
                <Reason>…</Reason>
        </Status>
        <SecondaryParameters>…</SecondaryParameters>
        …
</RequestSecurityTokenResponse>
```

- ***TokenType (opcional)***: Tipo de token, especificado como URI
- ***RequestType***: El tipo de la respuesta
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Status
- ***Status***: Indica si el token es o no válido y una razón
- ***Code***: Indica el estado del token
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/status/valid
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512/status/invalid
- ***Reason***: Descripción sobre la validación
- ***…*** : Mecanismo de extensión para añadir otros elementos que no pertenecen a WS-Trust

Validación de tokens

Ejemplo de petición de validación de token

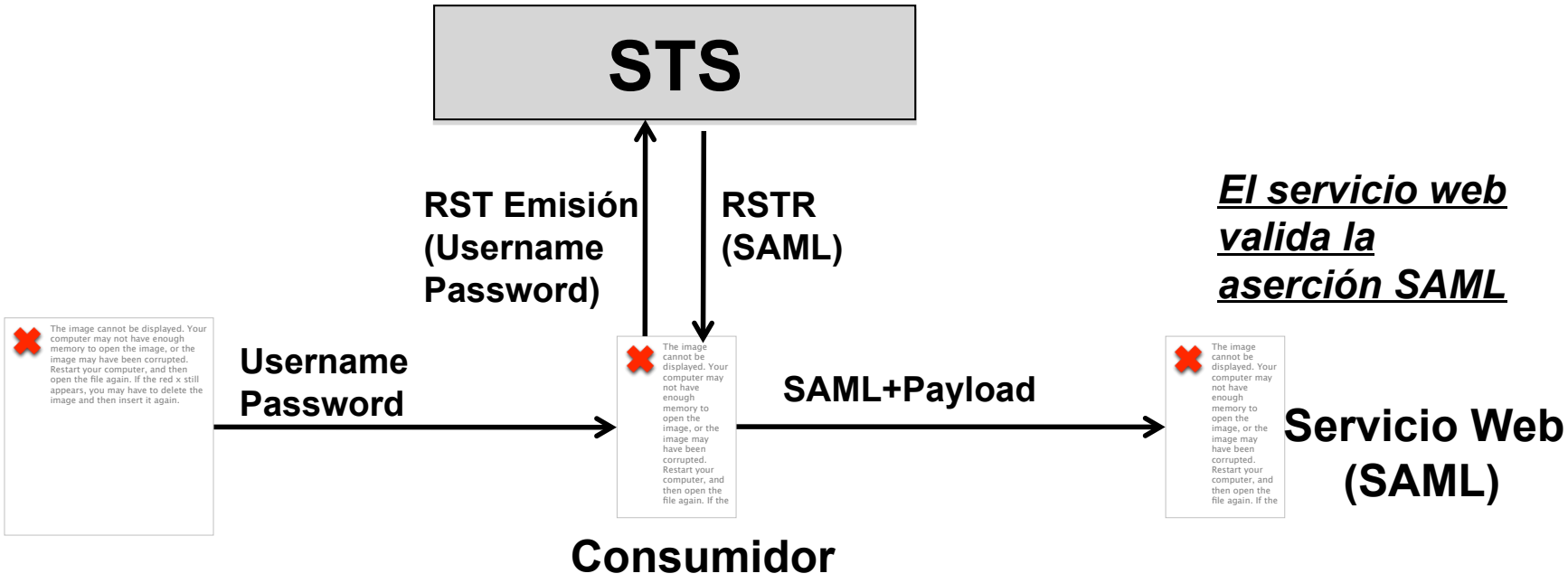
```
<RequestSecurityToken Context="STS" xmlns="…">
    <TokenType>urn: oasis:names:tc:SAML:2.0:assertion</TokenType>
    <RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Validate</RequestType>
    <ValidateTarget>
        <saml2:Assertion xmlns:saml2="…">…</saml2:Assertion>
    </ValidateTarget>
</RequestSecurityToken>
```

Ejemplo de respuesta de validación de token

```
<RequestSecurityTokenResponse Context="STS" xmlns="…">
    <TokenType>urn: oasis:names:tc:SAML:2.0:assertion</TokenType>
    <RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Status</RequestType>
    <Status>
        <Code>http://docs.oasis-open.org/ws-sx/ws-trust/200512/status/valid</Code>
        <Reason>Valid Signature verification</Reason>
    </Status>
</RequestSecurityTokenResponse>
```

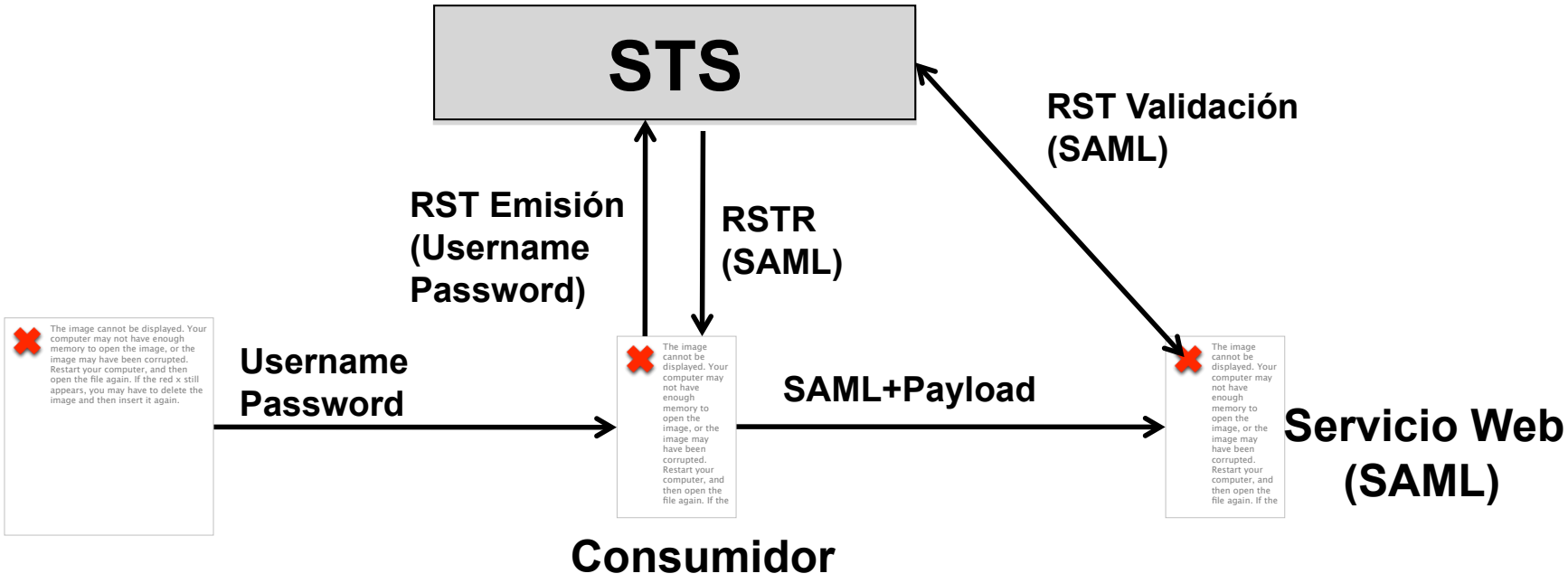
Escenarios de utilización (A)

- El Servicio Web sólo entiende SAML
- El usuario puede autenticarse con su nombre de usuario y contraseña en el STS



Escenarios de utilización (B)

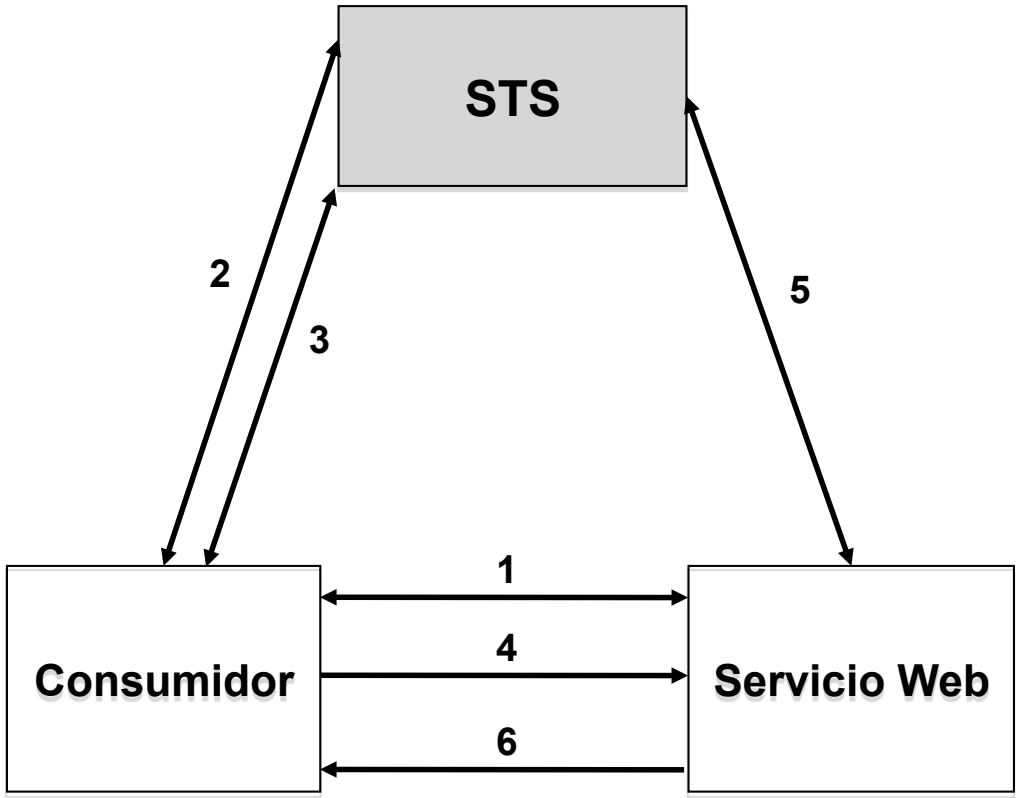
- El Servicio Web sólo entiende SAML
- El usuario puede autenticarse con su nombre de usuario y contraseña en el STS



Escenarios de utilización (C)

Ejemplo más completo

- El Servicio Web requiere (implícito por política) una aserción SAML de un STS de confianza



1. **Consumidor solicita y obtiene metadatos del Servicio Web**
2. **Consumidor solicita y obtiene metadatos del STS**
3. **Consumidor solicita y obtiene un token SAML del STS**
4. **Consumidor invoca al Servicio Web con el token SAML**
5. **Servicio Web delega la validación de la aserción SAML al STS en el que confía**
6. **El Servicio Web responde al Consumidor en caso de que el token SAML sea válido**

STS en RedIRIS

- RedIRIS está trabajando en un STS
  - Estará disponible próximamente e intentará abarcar el máximo posible de tipos de tokens
- Utiliza tokens de sesión además de los tokens de seguridad, ya que el proceso de validación es costoso
  - Los tokens de sesión están basados en JWT (JSON Web Token)
- Trabajamos también en la implementación de un AS de OAuth2
  - El escenario del STS en SOAP es equivalente a OAuth2 en REST

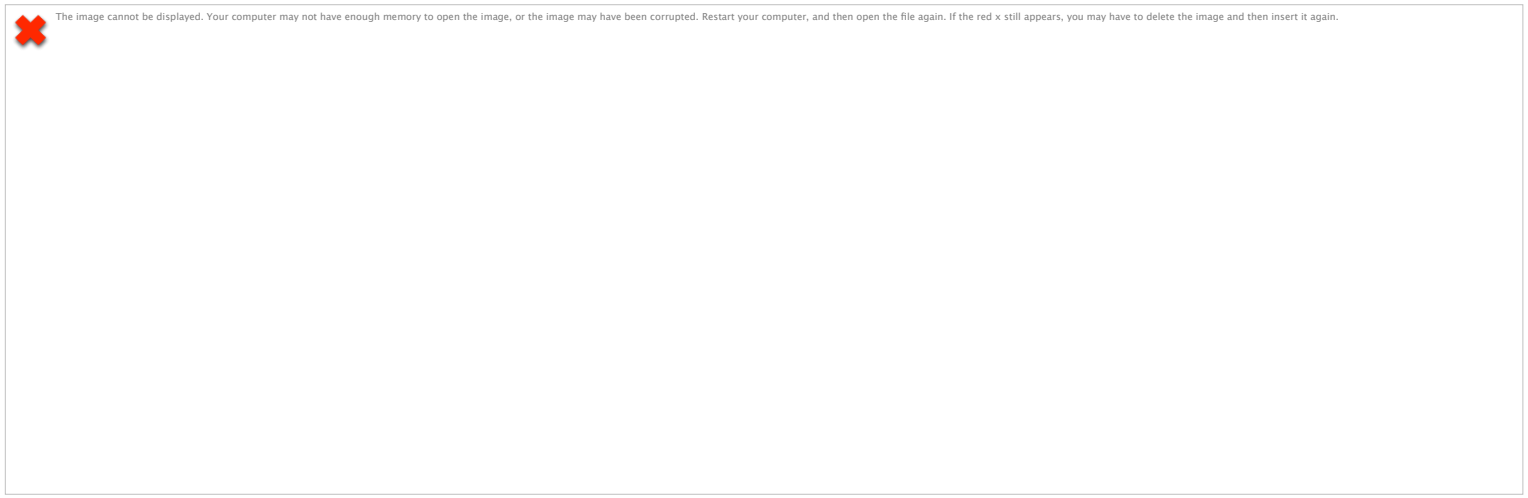
Conclusiones

- Usando las extensiones de WS-Trust, las aplicaciones pueden entablar comunicaciones seguras diseñadas para trabajar con:
  - Frameworks de Servicios Web incluyendo WSDL
  - Servicios Web descubiertos mediante registros de servicios
  - Mensajes SOAP

- El STS permite que:
  - La configuración sea centralizada y más fácil de mantener
  - Los consumidores simplemente solicitan un token para un servicio. La generación del token es transparente, sin importar si el consumidor da soporte a ese tipo de token o no
  - Las relaciones de confianza se establezcan entre los servicios y el STS y no entre servicios, lo que facilita la escalabilidad y uso entre servicios

Referencias

- **WS-Trust**
  - http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust- 1.4-spec-os.pdf
- **Web Services Security Username Token Profile 1.0**
  - http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf
- **Web Services Security UsernameToken Profile 1.1**
  - http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf
- **Web Services Security X.509 Certificate Token Profile**
  - http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf
- **Web Services Security X.509 Certificate Token Profile 1.1**
  - http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf
- **SAML V1.1 Core**
  - http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf
- **SAML V2.0 Core**
  - http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- **Web Service Security SAML Token Profile 1.0**
  - http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf
- **Web Service Security SAML Token Profile 1.1**
  - http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf



Gracias por vuestra atención