CAPÍTULO 10: SEGURIDAD EN SAML

En la siguiente sección se estudiarán una serie de puntos de seguridad que SAML analiza con gran detalle. Para ello primero veremos unos conceptos muy relacionados con la seguridad y cómo podemos cumplirlos. Después añadimos unas consideraciones sobre la seguridad. Entre ellas nos centraremos en la autentificación inicial y detallaremos dos modelos, uno de confianza y otro de amenazas. En este últimos veremos unas técnicas para poder llegar a un sistema más seguro. Seguimos explicando los posibles ataques que pueden sufrir los elementos que componen nuestra implementación (binding y perfiles usados). Explicamos los posibles ataques y cómo podemos remediarlos. Por último explicamos cómo integramos la firma digital sobre documentos XML en SAML. Este punto ha sido puesto ya que durante todo este apartado hemos realizado referencias constantes a la citada especificación de firma.

10.1.- Conceptos básicos de seguridad

A continuación definimos unos conceptos involucrados en la seguridad muy importantes. Relacionamos esos conceptos con la especificación SAML y vemos que requisitos se deben de dar para que se cumplan.

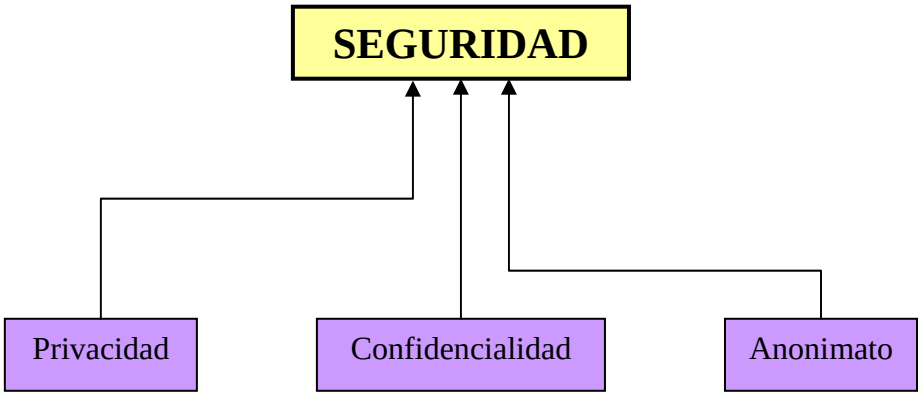

Figura 10. 1: Conceptos importantes de seguridad

10.1.1.- Privacidad

Por privacidad entendemos el control que los clientes tienen sobre la recolección, uso y distribución de su información personal

SAML incluye la capacidad de construir afirmaciones (aserciones) sobre los atributos (incluida la identidad) o sobre autorizaciones concedidas a entidades autentificadas. En muchas situaciones se podría dar el caso de que las entidades o

sujetos sobre los que se realizan las afirmaciones desearan mantener parte de la información oculta, ya sea de atributos o de autorización. Es más, en función del consumidor de la aserción el sujeto podría querer incluir unas u otras declaraciones. Todas las partes que juegan su papel en la creación de declaraciones y emisión, transmisión o consumo de afirmaciones SAML deben de ser conscientes de que pueden existir estas restricciones de privacidad y deberán intentar resolverlas en la implementación de sus sistemas SAML.

10.1.2.- Confidencialidad

El aspecto más importante para asegurar la privacidad de las partes implicadas en una transacción SAML es garantizar la confidencialidad. En otras palabras ¿es posible transmitir la información en una aserción SAML desde el emisor hasta un cierto grupo de receptores, y sólo a este grupo, sin hacerla accesible a ninguna otra parte? Técnicamente es factible transmitir la información de manera confidencial mediante mecanismos criptográficos. Pero observamos que el hecho de hacer invisibles los contenidos de las aserciones puede no cubrir todos los requisitos de privacidad deseados. Existen muchos casos donde el hecho de que esté disponible la información del acceso a un servicio por parte de un cierto usuario (o una dirección IP) podría romper la privacidad.

10.1.3.- Anonimato

Actualmente no existen definiciones sobre el anonimato que satisfagan todos los posibles escenarios en los que este concepto puede ser utilizado. Una definición muy común sobre el término en cuestión guarda relación con un emisor de un mensaje. Según esta definición, el emisor será anónimo si el receptor no es capaz de conocer su identidad a partir del mensaje recibido. Sin lugar a dudas esta definición es correcta para este caso en particular, aunque sería incompleta debido a la posibilidad del receptor de acumular información a lo largo del tiempo y, tras sucesivas interacciones con el emisor, tener una sólida descripción, no quizá sobre su identidad, pero sí sobre su conducta.

Esta noción es muy relevante en SAML debido al uso de las autoridades. Aunque cierto sujeto fuera “anónimo”, aún sería identificable como un miembro del conjunto de posibles sujetos dentro del dominio de cierta autoridad SAML. En el caso de que el usuario disponga de una agregación de atributos, el conjunto puede llegar a ser más pequeño.

De esa manera decimos que los sistemas SAML están limitados a ser, en el mejor de los casos, “**parcialmente anónimos**” debido al uso de las autoridades. Es decir, se limita el conjunto de usuarios a los que se puede referir. Una entidad sobre la que se ha realizado una afirmación pasa a formar parte del conjunto de entidades identificables por pura relación con la autoridad SAML. Las autoridades ubicadas en el origen (como por ejemplo autoridades de autentificación) pueden proporcionar un grado de “anonimato parcial” empleando identificadores que sólo se puedan utilizar una vez o mediante claves. Este anonimato es a lo sumo parcial porque el sujeto SAML se encuentra necesariamente confinado a un conjunto de sujetos por su relación con la

autoridad SAML. Este conjunto se podría reducir (reduciéndose así el anonimato) cuando se utiliza la agregación de atributos para acotar aún más el subconjunto de los posibles usuarios del sitio origen. Los usuarios que verdaderamente se preocupan sobre el anonimato deben tener la precaución de "disfrazar" o evitar patrones no usuales de conducta que pudieran servir para que los usuarios pierdan su anonimato con el paso del tiempo.

10.2.- Otras consideraciones sobre la seguridad en SAML

La comunicación entre sistemas basado en entidades implementadas en computadoras se encuentra sujeta a una amplia variedad de amenazas que conllevan implícitamente una serie de riesgos. La naturaleza de estos riesgos varía desde el propio hecho de la comunicación hasta los entornos en los que se encuentran los sistemas comunicantes pasando por el propio medio de comunicación utilizado.

SAML tiene como propósito ayudar a los desarrolladores a **establecer contextos de seguridad** a nivel de aplicación para las comunicaciones basadas en computadoras. Asumiendo este rol, SAML resuelve el aspecto de "autentificación del interlocutor" dentro de la seguridad de las comunicaciones y, también, el aspecto de "uso no autorizado" perteneciente a los sistemas de seguridad. Algunas de las áreas que impactan ampliamente en la **seguridad** global de un sistema que utiliza SAML están explícitamente **fuera del alcance del propio SAML**. Algunas de ellas son:

10.2.1.- Autentificación inicial

SAML permite crear declaraciones o afirmaciones sobre que cierto proceso de autentificación se ha llevado a cabo, pero no incluye como requisito ni especifica los procesos de autentificación en sí, tan sólo que se llevaron a cabo. Los consumidores de las aserciones de autenticación deberían ser cautos y no confiar ciegamente en estas afirmaciones a menos que conozcan los fundamentos sobre los que fueron hechas. La confianza en las aserciones nunca debe ser mayor que la confianza que llevó a crearla por parte de la entidad que la realizó.

10.2.2.- Modelo de confianza

En muchos casos, la seguridad de una conversación SAML dependerá del modelo de confianza subyacente, el cual está típicamente basado en una infraestructura de gestión de claves (por ejemplo, PKI o clave secreta). Por ejemplo, los mensajes SOAP que incorporan firmas digitales utilizando los mecanismos descritos por la especificación *W3C XML Digital Signature*. Serán seguros en tanto en cuanto las claves utilizadas para generar la firma sean de confianza. Si éstas estuvieran comprometidas la firma digital hecha sobre cierto conjunto de aserciones SAML no serían, desde el punto de vista de seguridad, de confianza. No detectar que las claves han sido comprometidas o que ciertos certificados han sido revocados podría provocar una brecha en la

seguridad. Incluso un fallo por no requerir un certificado podría crear riesgos de ataques de suplantación de identidad.

Por tanto, y a modo de resumen, debemos especificar que **SAML no entiende de procesos de autentificación**, solamente de si se han llevado a cabo o no con éxito, y que la confianza que podemos tener en un sistema que utiliza SAML está directamente relacionada con la confianza que podamos tener en las infraestructuras subyacentes a los sistemas que lo soportan.

10.2.3.- Modelo de amenaza en sistemas SAML

A continuación estudiemos el **modelo de amenaza para los sistemas que utilizan SAML**. Asumiremos aquí que dos o más puntos de comunicación o interlocutores de una transacción SAML no se encuentran comprometidos pero que el atacante posee un control completo sobre el canal de comunicaciones.

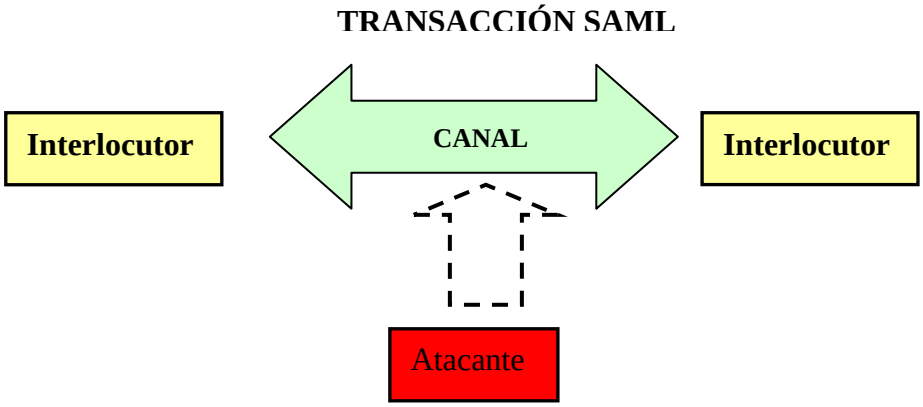

Figura 10. 2: Representación de la situación explicada

Además, debido a la naturaleza de SAML como sistema de autentificación de múltiples partes y como protocolo intercambio de declaraciones de autorización, se deben considerar aquellos casos en los que uno o más de los interlocutores de una transacción SAML legítima, que operan legítimamente dentro de su rol asignado para la transacción, intentan utilizar de manera maliciosa en posteriores transacciones la información conseguida en transacciones previas. Veamos las técnicas de seguridad puestas arriba que podrán servirnos de ayuda y por tanto habría que tener en cuenta cuando desarrollemos sistemas basados en SAML.

Autentificación

La autentificación significa aquí la capacidad que debe tener una parte, implicada en una transacción, de afirmar la identidad de todas y cada una de las otras partes envueltas en la misma transacción. La autentificación podría ser de un solo sentido o bidireccional. Se podrían hacer dos posibles distinciones en cuanto a los **tipos de autentificación** que se pueden dar:

- **Sesión activa**: La autentificación no persistente es ofrecida por el canal de comunicaciones utilizado para transportar los mensajes SAML. Esta autentificación podría ser unilateral, desde el iniciador de la sesión hacia el receptor, o bilateral. Este método específico estará determinado por el protocolo de comunicaciones utilizado. Por ejemplo, el uso de un protocolo de red seguro, habilita al emisor del mensaje a autenticar al destinatario dentro del entorno TCP/IP.

- **Autentificación a nivel de mensaje**: Existen especificaciones que proporcionan métodos de creación de autentificación persistente que está altamente acoplado al documento.

Confidencialidad

La confidencialidad significa que los contenidos de un mensaje pueden ser solamente leídos por los destinatarios que estén autorizados y por nadie más que tenga acceso físico al mensaje. Podemos distinguir **dos tipos** de maneras de asegurar la confidencialidad de los mensajes:

- **Confidencialidad en tránsito**: Utilizar un protocolo de red seguro, proporciona una confidencialidad volátil de un mensaje cuando es transmitido entre dos nodos.

- **Confidencialidad a nivel de mensaje**: Existe una especificación que ofrece una forma de cifrar, de manera selectiva, documentos XML. Este método de cifrado proporciona confidencialidad persistente y selectiva de la información contenido dentro de un mensaje XML.

Integridad de los datos

La integridad de los datos supone la capacidad de confirmar que cierto mensaje recibido en un extremo tiene la misma forma y no ha sufrido alteración alguna respecto a cuando fue enviado por el nodo emisor. La integridad de los datos puede estudiarse a **dos niveles**:

- **Integridad de los datos en tránsito**: Al igual que ocurría con la autentificación y la confidencialidad, el uso de un protocolo de red seguro podría ser suficiente para proporcionar integridad de los paquetes transmitidos vía la conexión de red.

- **Integridad a nivel de mensaje**: Al igual que ocurría con la autenticación a nivel de mensaje, se puede hacer de una especificación de firmado para saber con certeza si cierto mensaje es o no íntegro.

Gestión de las Claves

La seguridad de los sistemas que tienen la capacidad de proporcionar autentificación, integridad, y confidencialidad mediante firmas digitales y técnicas criptográficas está relacionada de manera directa con la seguridad de los sistemas de gestión de claves que utilizan. Se asume que, si los sistemas basados en claves van a ser

utilizados para conseguir autentificación, integridad de los datos y no repudio, se deberán establecer ciertas medidas de seguridad que garanticen que el acceso a las claves no está disponible para los sujetos no autorizados.

En la siguiente tabla ponemos en una lista las técnicas de seguridad y sus tipos.

Técnica	**Tipos**
Autentificación	Sesión activa
	A nivel de mensaje
Confidencialidad	En Tránsito
	A nivel de mensaje
Integridad de datos	En Tránsito
	A nivel de mensaje
Gestión de las claves	

Tabla 10. 1: Técnicas de seguridad y sus tipos

10.3.- Posibles ataques a la seguridad en SAML

En este apartado nos dedicamos a poner los posibles ataques que pueden tener los diferentes elementos que intervienen en nuestra implementación poniendo también una serie de posibles soluciones. En la tabla siguiente ponemos los citados ataques a la seguridad y la parte en la que aparecen.

	Ataque
Perfil ECP	**Man in the Middle**
	Negación de servicio
Binding SOAP	**Escucha secreta**
	Repetición de mensajes
	Inserción de Mensajes
	Cancelación de Mensajes
	Modificación de Mensajes
	Man in the Middle
Binding PAOS	**Negación de servicio**

Tabla 10. 2: Relación de posibles ataques a la seguridad

10.3.1.- Perfil ECP

Dentro de este perfil nos encontramos con dos posibles ataques y con las soluciones que podemos adoptar.

Hombre en el medio (man in the middle, MITM)

Amenaza: Interceptar los mensaje SOAP petición de autentificación (*AuthnRequest*) y su respuesta (*Response*), permitiendo la consiguiente imitación del principal.

Una entidad de sistema falsa puede intervenir como hombre-en-el-medio (MITM) entre el ECP y un proveedor de servicio legítimo. Ésta actuará en el papel del SP con respecto al ECP y de ECP cuando se comunique con el SP legítimo. De esta manera, como primer paso, el MITM es capaz de interceptar el mensaje *AuthnRequest* del proveedor de servicio y cambiar cualquier URL de su elección para el valor de *responseConsumerServiceURL* del boque de cabecera PAOS, antes de mandárselo al ECP. Normalmente, el MITM insertará un valor URL que apunta de vuelta hacia sí mismo. Luego, si el ECP recibe una Response del proveedor de identidad y lo manda junto con el valor de *responseConsumerServiceURL* dado por el MITM, entonces el MITM será capaz de hacerse pasar por el principal en el SP.

Contramedida: El proveedor de identidad especifica al ECP la dirección a la que éste último debe enviar la *Response*. El *responseConsumerServiceURL* de la cabecera PAOS se usa sólo para respuestas de error desde el ECP (como se especifica en el perfil).

Negación de servicio (Denial of Service)

Amenaza: Cambiar una petición de autentificación SOAP (*AuthnRequest*) de modo que no pueda ser procesado, tal como poner un valor desconocido en los atributos de servicio de la cabecera PAOS o cambiando los campos *ProviderID* o *IDPList* de la cabecera ECP con el fin de que falle la petición.

Contramedidas: Proporcionar protección de integridad para el mensaje SOAP, mediante el uso de SOAP Message Security o SSL/TLS.

10.3.2.- Binding SOAP SAML

Como el binding SOAP de SAML no requiere autentificación y no tiene requerimientos de confidencialidad o integridad de mensaje, se abre una amplia variedad de ataques comunes, los cuales los detallamos a continuación. Las consideraciones generales se discuten por separado de aquellas relacionadas con el caso SOAP sobre HTTP.

Escucha secreta (Eavesdropping)

Amenaza: Al no haber requisitos de confidencialidad en tránsito, es posible que una parte que escucha pueda obtener tanto el mensaje SOAP que contiene la petición como el mensaje SOAP con la respuesta. Esta adquisición revela tanto la naturaleza de la petición como los detalles de la respuesta, posiblemente incluyendo una o más aserciones. La exposición de esos detalles debilita la seguridad del solicitante en algunos casos, revelando qué clase de aserción requiere, o sobre quién pregunta ésta.

Por ejemplo, si uno que escucha puede determinar que el sitio X está solicitando aserciones de autentificación con un método de confirmación dado del sitio Y, él puede utilizar esta información para ayudar en el compromiso del sitio X. Semejantemente, el escuchar en una serie de preguntas de autorización podría crear un “mapa” de los recursos que están bajo el control de una cierta autoridad de autorización.

Además, en algunos casos la exposición de la petición por sí misma, puede constituir una violación de la privacidad. Por ejemplo, escuchando una pregunta y su respuesta podemos descubrir que un usuario dado es activo en el sitio donde pregunta, que podría ser una información que no debe ser divulgada como información de sitios médicos, políticos, etcétera. También los detalles de cualquier aserción que lleve dentro la respuesta pueden ser información que debe mantenerse en secreto. Esto es particularmente cierto en respuestas que contienen aserciones de atributos; si dichos atributos representan información que no debe estar disponible para entidades que no formen parte de la transacción (información bancaria, atributos médicos, etcétera), por la amenaza que introduce la escucha es alta.

Contramedidas: En los casos en los que cualquiera de estos riesgos representa una preocupación, las contramedidas por ataques de escucha serán proporcionar, de algún modo, confidencialidad de mensaje durante el tránsito del mismo. Para los mensajes SOAP, la confidencialidad puede ser llevada a cabo tanto a nivel SOAP o en el nivel de transporte SOAP (o alguno inferior). Añadir confidencialidad durante el tránsito del mensaje significa construir dicho mensaje de tal forma que nadie salvo la parte prevista tenga acceso al mismo. La solución general a este problema es probablemente el cifrado de XML [XMLEnc]. Esta especificación permite el cifrado del propio mensaje SOAP, que elimina el riesgo de escucha a menos que la clave usada en el cifrado se haya comprometido. Alternativamente, los desarrolladores pueden depender de la capa de transporte SOAP, o de una capa debajo de ella, para proporcionar confidencialidad durante el transito del mensaje. Los detalles de cómo proporcionar dicha confidencialidad dependen del transporte específico SOAP.

Repetición de Mensajes

Amenaza: Hay poca vulnerabilidad en el ataque de repetición de mensajes en el nivel del binding SOAP. La preocupación principal a este ataque es la negación de servicio.

Contramedidas: En general, la mejor manera de prevenir el ataque de repetición es evitar la captura del mensaje. Algunos de los esquemas del nivel de transporte proporcionan confidencialidad en el transito del mensaje. Por ejemplo, si el intercambio petición/respuesta de SAML ocurre sobre SOAP en HTTP/TLS, se previene de capturar los mensajes. Observamos que no hace falta entender un mensaje para capturarlo por lo que esquemas de encriptación no sirven para proteger contra repeticiones. Si un atacante puede capturar una petición SAML que ha sido firmada por el solicitante y cifrada al respondedor, entonces, el atacante, puede repetir la petición de nuevo en cualquier momento sin necesidad de deshacer el cifrado. La petición SAML incluye información sobre el tiempo de emisión de dicha petición, que permite saber si es una repetición. Otra manera de saber si es una repetición es controlar el identificador de la petición.

Inserción de Mensajes

Amenaza: Una petición o respuesta fabricada se inserta en la corriente de mensajes. Una respuesta falsa tal como una respuesta afirmativa a una petición de decisión de autorización o devolver atributos falsos en respuesta a una petición de atributos que puede dar lugar a una acción inadecuada del receptor.

Contramedidas: La capacidad de insertar una petición no es una amenaza en el nivel del binding SOAP. La amenaza de insertar una respuesta falsa puede ser un ataque de negación de servicio pero es fácilmente reconocido mediante el protocolo SAML. Dicho protocolo trata esto con dos mecanismos: con la correlación de respuestas a las peticiones usando el atributo obligatorio "*InResponseTo*", lo que fuerza un ataque más duro puesto que las peticiones se deben interceptar para generar respuestas, y a través de la autentificación del origen, por medio de respuestas SAML firmadas o a través de una conexión de transporte segura como SSL/TLS.

Cancelación de Mensajes

Amenaza: El ataque de cancelación de mensajes evitaría que una petición alcanzara a un respondedor, o evitaría que la respuesta alcanzara al solicitante.

Contramedidas: En cualquier caso, el binding SOAP no trata esta amenaza. En general, la correlación de los mensajes de la petición y de respuesta puede disuadir tal ataque, por ejemplo usando el atributo "*InResponseTo*".

Modificación de Mensajes

Amenaza: La modificación del mensaje es una amenaza para el binding SOAP en ambas direcciones.

La modificación de la petición para alterar sus detalles puede dar lugar a resultados diferentes que son devueltos, que pueden ser utilizados por un atacante listo para comprometer sistemas dependiendo de las aserciones devueltas. Por ejemplo, alterando la lista de atributos solicitados en el elemento <Attribute> se pueden producir resultados que comprometan o produzca el rechazo de la petición por parte del respondedor. La modificación de la petición puede dar lugar a la negación de servicio o a un incorrecto enrutamiento de la respuesta. Esta modificación se tendría que dar por debajo del nivel SAML, estando fuera de su alcance.

La modificación de la respuesta para alterar los detalles de las aserciones puede dar lugar a graves problemas en la seguridad.

Contramedidas: Para tratar estas amenazas se debe utilizar un sistema que garantice integridad en el tránsito del mensaje. El protocolo SAML y el binding SOAP ni requieren ni prohíben el despliegue de los sistemas que garantizan dicha integridad de mensaje, pero debido a esta gran amenaza, se **recomienda encarecidamente** que tal sistema sea utilizado. En el nivel del binding SOAP se puede lograr firmando digitalmente las peticiones y respuestas con un sistema como firma de XML. La especificación SAML permite tales firmas. Si los mensajes se firman digitalmente entonces podremos decir que el mensaje no ha sido modificado durante el tránsito del mismo, a menos que se haya comprometido la clave. La integridad en tránsito también se puede conseguir usando transporte SOAP que proporcione tal función como HTTP sobre TLS/SSL. El cifrado por si sólo, no proporciona esta protección porque aunque no puede ser alterado si se puede crear otro que lo sustituya.

Hombre-en-el-medio (MITM)

Amenaza: El binding SOAP es susceptible a los ataques MITM. Para evitar que las entidades malévolas funcionen como hombre en el centro (con todos los peligros discutidos tanto en las secciones de modificación de mensajes como en escuchas), se requiere una cierta autentificación bilateral.

Contramedidas: Un sistema bidireccional de autentificación debe permitir que ambas partes puedan comprobar que están relacionándose con la otra. En el binding SOAP esto se consigue mediante el firmado de las peticiones y las respuestas aunque no evita que se puedan producir escuchas de mensajes.

Uso de SOAP sobre HTTP

Como hemos comprobado, muchas amenazas requieren el uso de HTTP sobre TLS/SSL con alguna forma de autentificación bidireccional para atenuarlas o eliminarlas. Esto no significa que sea obligatorio si se puede llegar a un nivel aceptable de protección por otros medios. Sin embargo, en la mayoría de los casos, la mejor opción posible es el uso de HTTP sobre TLS/SSL con algún medio de autentificación bidireccional.

Observamos, sin embargo, que el uso de la seguridad del nivel de transporte (tal como los protocolos SSL o TLS bajo HTTP) solamente proporciona confidencialidad y/o integridad y/o autentificación para “un salto”. Para modelos donde puede haber intermediarios, o en aquellos donde las aserciones necesitan más de un salto, el uso del HTTP con TLS/SSL no proporciona seguridad adecuada.

10.3.3.- Binding Reverse SOAP (PAOS)

Es el último componente que usamos en la implementación y sólo tiene asociado un ataque.

Negación de Servicio

Amenaza: Al eliminar los campos de cabecera PAOS y HTTP PAOS podemos hacer que el respondedor HTTP no reconozca que esta procesando un mensaje PAOS.

Contramedida: Proteger la integridad del mensaje usando TLS/SSL u otro mecanismos de seguridad en la capa de transporte.

4.4.- Integración de SAML con XML Digital Signature

Como ya hemos señalado en varias ocasiones a lo largo de las secciones anteriores, SAML hace uso del mecanismo de firma digital en diversas ocasiones: para firmar las aserciones, y para firmar las peticiones/respuestas SAML.

Las firmas digitales que **firman una aserción** emitida por una autoridad SAML proporcionan:
- **Integridad** del contenido.
- **Autentificación** de la autoridad SAML que emitió la aserción.
- Si la firma está realizada mediante la clave privada de la autoridad SAML además proporciona **no repudio** del origen.

En el caso de las **firmas sobre las peticiones/respuestas** SAML:
- Se garantiza la **integridad** de los mensajes.
- Se **autentifica** frente al receptor la parte emisora del mensaje.
- Si la firma está basada en la clave privada del emisor del mensaje, entonces también se proporciona **no repudio** del origen.

Las firmas digitales no son de uso obligatorio según la especificación SAML. Damos algunos ejemplos de uso en los que no es obligatorio el uso de las firmas digitales:
- En algunas situaciones una aserción no firmada puede heredar una firma aplicada sobre entidades que la contienen. Es decir, una aserción no firmada puede ganar esta propiedad si se introduce dentro de un mensaje de respuesta del protocolo SAML firmado. Las firmas digitales “heredadas” deberían ser utilizadas con cuidado sobre todo cuando el objeto contenido (como por ejemplo una aserción) posee un tiempo de vida persistente y no transitorio. El motivo de esta advertencia es que, para que la firma siempre sea válida, se debe retener todo el contexto para conseguir que su validación siempre sea correcta.

- Las firmas digitales tampoco son de uso obligatorio cuando los canales de comunicaciones entre las partes SAML son los suficientemente seguros.

Salvo en estas dos situaciones la especificación recomienda el uso de las firmas digitales, específicamente en los siguientes casos:
- Una aserción SAML debe firmarse cuando es recibida por un cliente SAML procedente de una entidad que no es una autoridad SAML.

- Un mensaje de protocolo SAML debe ser firmado cuando llega a un destinatario procedente desde una entidad que no es la parte SAML que generó el mensaje original.