



Servicio Andaluz de Salud
CONSEJERÍA DE IGUALDAD, SALUD Y POLÍTICAS SOCIALES

*OTI / Subdirección de Tecnologías de la
Información / Servicio Andaluz de Salud*

POLÍTICA DE AUTENTIFICACIÓN DE UN OPERADOR EN MACO

Sevilla, 30 de Junio de 2011

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 2 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

Información del documento

Título del documento:	SAS – Política de Autenticación de un Operador MACO
Proyecto:	MACO
Equipo:	OTI
Propietario del Servicio de negocio:	STI

Documentos relacionados

Nombre del documento	Link al documento

Resumen de modificaciones al documento

Versión	Fecha	Realizada por	Revisada por	Modificaciones introducidas
1.0	30/06/2011	OTI		Versión inicial.
1.1	01/08/2011	OTI		Se ha establecido en un día el periodo de validez de un ticket de MACO. Además se ha actualizado el ejemplo de código que realiza la validación del ticket.
1.2	10/10/2010	OTI		Actualización del documento con algunas tareas a realizar por parte de la OTI al dar de alta un módulo en MACO. Inserción en la validación del ticket de MACO, la validación de si el ticket está caducado, comprobar la fecha del mensaje frente a la fecha de validez del ticket insertado en dicho mensaje (solución propuesta para los reintentos). Actualización de la clave pública de MACO en el entorno de Preproducción.
1.3	07/12/2011	OTI		Corrección errata en la descripción de la información del ticket de MACO.
1.4	11/01/2012	OTI		Actualización de algoritmo de ejemplo. Actualización del ticket y firma de ejemplo. Anotación de variables configurables en la validación del ticket. Necesidad de devolver información detallada del error producido en la validación.
1.5	10/02/2012	OTI		Se elimina el algoritmo y se insertan dos referencias a dicho algoritmo implementado en C#.NET y en JAVA, para que pueda ser utilizado por cualquier sistema en la medida de lo posible. Actualización de la forma de actuar, en referencia al ticket de MACO, para un sistema que no está dado de alta en MACO.
1.6	20/12/2012	OTI		Actualización correo de solicitud de algoritmos de validación de la firma y ticket de MACO.
1.7	13/12/2013	OTI		Actualización correo de solicitud de algoritmos de validación de la firma y ticket de MACO.
1.8	07/07/2014	OTI		Diversos cambios: - Anotación para indicar la contraseña de entrada al método de MACO para devolver el ticket.

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 3 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

				- Anotación para devolución de NACK síncrono en el servicio y no a través del S067. - Actualización método de solicitud algoritmos de ejemplo para la validación del ticket de MACO. - Modificación procedimiento de validación de la firma y ticket MACO. Solamente se validará contra la fecha del mensaje, no contra la fecha actual del sistema.
--	--	--	--	--

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 4 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

ÍNDICE

1	OBJETIVO DEL DOCUMENTO	5
2	PROTOCOLO DE AUTENTIFICACIÓN DE UN OPERADOR EN MACO	5
2.1	ANTECEDENTES.....	5
2.2	PROTOCOLO de validación.....	5
2.3	ALTA EN MACO DE UN MÓDULO	6
2.4	TICKET DE MACO Y SU FIRMA.....	6
2.5	FLUJO DEL PROCESO	6
2.5.1	Sistema con Operador MACO	7
2.5.2	Sistema sin Operador MACO	7
2.6	NODOS MACO PARA TICKET Y FIRMA DE MACO.....	7
2.7	NODOS HL7 PARA TICKET Y FIRMA DE MACO	7
2.8	CLAVE PÚBLICA RSA DE MACO.....	8
3	Anexo	8
3.1	EJEMPLO ALGORITMO VALIDACIÓN TICKET Y FIRMA DE MACO.....	8
3.2	EJEMPLO DE TICKET DE MACO Y SU FIRMA CORRESPONDIENTE	8
3.3	GLOSARIO DE TÉRMINOS	9

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 5 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

1 OBJETIVO DEL DOCUMENTO

Este documento tiene como objetivo describir el protocolo de autenticación de operadores en MACO dentro de las transacciones dentro de los distintos proyectos del SAS.

2 PROTOCOLO DE AUTENTIFICACIÓN DE UN OPERADOR EN MACO

2.1 ANTECEDENTES

Ante la necesidad de securizar el uso de los servicios, ha salido la necesidad de implantar un modelo de autenticación de un operador en MACO que garantice que el operador está dado de alta en MACO y a su vez tiene permisos para acceder al servicio invocado.

2.2 PROTOCOLO DE VALIDACIÓN

Un sistema que va a invocar servicios deberá primeramente dar de alta en MACO a su módulo si todavía no lo ha realizado. Una vez dado de alta podrá realizar llamadas al servicio web de MACO (Prevalidar) para obtener el ticket de MACO correspondiente. El sistema origen, por lo tanto, antes de llamar a un servicio tendrá que llamar a MACO para obtener el ticket de seguridad. Este ticket de MACO deberá obtenerlo una vez el operador se loga en su aplicación y mantener en cache dicho ticket durante la sesión abierta o mientras el ticket de MACO sea válido en tiempo. Es decir, tendrá que generar un nuevo ticket si el operador es distinto entre una llamada y otra, si los permisos son distintos o bien si el periodo de validez ha caducado.

La validación de un operador se realiza a través de este ticket de MACO que el sistema origen de una transacción deberá enviar en el mensaje de entrada de la misma. De esta forma, la validación es más rápida y se ahorran llamadas constantes al servicio web de MACO.

La validación del ticket de MACO se va a realizar en los sistemas de destino de las transacciones. Esta validación del ticket de MACO implica tres acciones una vez se recibe el ticket en el sistema de destino:

- Validar que el ticket y la firma son correctos a través de un algoritmo. Para validar la firma se ha de generar el hash MD5 del ticket, decodificar la firma mediante la clave pública de MACO y verificar que los dos hash coinciden. En el anexo 3.1 existe un ejemplo de algoritmo para esta validación y las dos siguientes.
- Validar la fecha que se incluye en el ticket con la fecha en la que se mandó el mensaje para asegurar que este no está caducado. Para esto, la diferencia entre la fecha del mensaje (siempre deberá ser mayor que el ticket, ya que cuando se genera el mensaje el ticket de MACO ya debe estar en poder del sistema que inserta el ticket) y la fecha de validez del ticket debe ser menos a 24 horas.
- Validar que el servicio al que se está invocando está dentro de la lista de operaciones permitidas para ese operador. Se trata de validar que la operación a la que se está llamando está incluida en la lista de operaciones que aparece en el ticket. Posteriormente se indicará la estructura del ticket de MACO. Notar aquí, que ese valor de la operación a validar en la lista de operaciones del ticket que se recibe, debe ser configurable fuera del desarrollo, para evitar así tener que realizar modificaciones en dicho desarrollo ante un cambio de nombre de la operación en MACO.

En caso de error de cualquiera de las validaciones indicadas en los puntos anteriores, sería conveniente que el origen recibiera en el mensaje de respuesta una descripción precisa del error, es decir, ticket y firma no coinciden, ticket caducado, operación no permitida, ...

En caso de devolverse error de validación deberá reportarse el mismo en el ACK síncrono de respuesta y nunca en los mensajes de notificación de errores funcionales S067.

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 6 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

2.3 ALTA EN MACO DE UN MÓDULO

Tal y como se ha indicado en punto anterior, lo primero a realizar por parte de un sistema, si aún no se ha realizado anteriormente, es dar de alta su módulo en el sistema de MACO.

Para realizar dicho alta en MACO se realizarán los siguientes pasos:

1. El sistema deberá contactar con el Responsable OTI correspondiente a su línea de integración para dar de alta su sistema en MACO.
2. Indicar a dicho responsable de datos relacionados con su módulo. A continuación será tarea interna de la OTI el identificar los servicios que este módulo ofrece al resto de módulos y qué servicios podrán ser accedidos por dicho módulo y la relación de confianza de dichos accesos (de momento todas las relaciones de confianza son fuertes, no nos planteamos de momento que existan relaciones de confianza débiles).
3. Una vez dado de alta un módulo proveedor en MACO, se le tendrá que indicar a la empresa desarrolladora los nombres de operaciones ("especificación de contenido" en lenguaje MACO) dados en MACO a los servicios que dicho proveedor ofrece al resto de módulos. Los nombres de las operaciones serán asignados por la OTI, que llevará un registro de las mismas al margen de MACO, ya que MACO no las asigna por defecto. Las operaciones ya existentes en MACO, que hasta ahora han sido indicadas por la propia empresa desarrolladora, serán incorporadas también a dicho registro.
4. Las operaciones (servicios) multiproveedor comparten el mismo módulo funcional en MACO y por lo tanto las mismas especificaciones de contenido. Es tarea de la OTI llevar la gestión de qué aplicaciones proveedoras se engloban dentro de cada módulo funcional. Respecto a estas operaciones (servicios) multiproveedor, la OTI solicitará la creación en MACO de los módulos funcionales correspondientes que los engloban y de los propios servicios, indicando el nombre del módulo, de los servicios y las "especificaciones de contenido" (nombre del servicio) correspondientes. Posteriormente, se indicará a las distintas aplicaciones que proveerán realmente dichos servicios las "especificaciones de contenido" (nombre del servicio) que los identifican a fin de que puedan realizar la correcta validación del ticket.

2.4 TICKET DE MACO Y SU FIRMA

Cuando un sistema realiza una llamada al servicio web de MACO llamado Prevalidar indicando la **versión 4.3.00 o superior y el password del usuario convertida a MD5 y referenciada en el mensaje en mayúsculas**, MACO devuelve dos cadenas de caracteres:

- El tique de MACO consiste en los siguientes campos separados por asteriscos (*):
 - o Todos los servicios que tiene acceso el operador separados por +
 - o Código del operador.
 - o Ámbito organizativo (unidad funcional a efectos prácticos). No es obligatorio.
 - o Tipo de ámbito organizativo (unidad funcional, área hospitalaria, ...). No es obligatorio.
 - o Login.
 - o Fecha de creación del ticket.
- Firma hash de MACO (hash MD5 cifrado con RSA con la clave privada de MACO).

Indicar que el periodo de validez de un ticket es una sesión diaria, es decir, debe ser renovado cada día. Se debe tener en cuenta que este periodo de validez deberá ser configurable por todos los sistemas, ya que en cualquier momento se puede definir un periodo de validez mayor o menor.

Anotar también que en el ticket de MACO solo aparecen reflejadas las operaciones que un módulo puede indicar siempre que tenga relación de confianza fuerte definida en MACO.

2.5 FLUJO DEL PROCESO

Podemos encontrar dos casos:

- ✓ Que el sistema origen esté dado de alta en MACO y por lo tanto tenga un operador asociado en MACO.
- ✓ Que el sistema origen no esté dado de alta en MACO por cualquier motivo y no se pueda/deba dar de alta este sistema en MACO.

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 7 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

Veamos el flujo de proceso en cada caso.

2.5.1 Sistema con Operador MACO

El sistema que origina las transacciones deberá obtener el ticket de MACO llamando al servicio correspondiente de este (servicio de prevalidar). En esta llamada que realiza indicará en un parámetro del mensaje de llamada la **versión 4.3.00 o superior y el password del usuario convertida a MD5 y referenciada en el mensaje en mayúsculas**, MACO devuelve dos cadenas de caracteres:

- El tique de MACO.
- Firma hash de MACO (hash MD5 cifrado con RSA con la clave pública de MACO).

Una vez obtenido el ticket completo (ticket más firma) deberá enviarlo en el mensaje que envía en la llamada al servicio correspondiente.

El sistema de destino cuando recibe el mensaje, obtendrá el ticket y la firma y realizará las validaciones indicadas anteriormente para validar que el ticket es correcto (en estructura, en firma, caducidad y en operación). Si no cumple cualquiera de las validaciones indicadas, se devolverá un error correspondiente y no se continúa con el proceso correspondiente. **En caso de devolverse error de validación deberá reportarse el mismo en el ACK síncrono de respuesta y nunca en los mensajes de notificación de errores funcionales S067.** En caso de que las validaciones sean correctas, el sistema destino continuará con el proceso correspondiente.

2.5.2 Sistema sin Operador MACO

En este caso hablamos de sistemas que no están dados de alta en MACO y que por lo tanto ni tienen operador MACO ni pueden obtener el ticket correspondiente en MACO. En este caso vamos a distinguir entre si este sistema no MACO es el sistema origen de la transacción o por el contrario es el sistema destino:

- Si son emisores del servicio: el ESB identificará a estos sistemas que no tienen ticket y les presta su ticket para enviar al destino. En el momento en que vayan teniendo ticket, quitamos dicho préstamo del ESB y empezarían a funcionar con su ticket.
- Si son receptores del servicio: van a recibir el ticket y la firma, pero no van a realizar ninguna validación al respecto, ya que no tiene sentido que validen algo que ellos no utilizan. En el momento en que vayan teniendo ticket deberán realizar la validación y notificar de posibles errores en la firma y/o el ticket de MACO que reciben en la mensajería correspondiente.

2.6 NODOS MACO PARA TICKET Y FIRMA DE MACO

Cuando un sistema realiza una llamada al servicio web de MACO para obtener su ticket, recibe un mensaje que cumple un esquema propio de MACO. Para obtener la información del ticket y de la firma que estamos tratando en este documento deberá consultar los siguientes nodos:

- Ticket de MACO: Diraya_respuesta/cabecera_msj/entidad_origen/operador/accesos.
- Firma correspondiente al ticket informado en el nodo anterior: Diraya_respuesta/cabecera_msj/entidad_origen/operador/accesos/@firma. Indicar que al poner @firma se quiere indicar el atributo firma del nodo accesos.

2.7 NODOS HL7 PARA TICKET Y FIRMA DE MACO

A continuación se informan los nodos HL7 a utilizar para enviar el ticket y su firma correspondiente a otro módulo. Sabiendo que lo que se debe enviar en el mensaje es el ticket y la firma, necesitamos los siguientes nodos:

- MSH.3.2: En este nodo se enviaría el ticket de MACO.
- MSH.8: Aquí se debe insertar la firma correspondiente al ticket informado en el nodo anterior.
- MSH.7.1: Fecha del mensaje enviado.

 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 8 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

2.8 CLAVE PÚBLICA RSA DE MACO

A continuación se indican la clave pública RSA de MACO para el entorno de Preproducción e MACO y para su entorno de Producción:

- o Entorno de Preproducción:

```
<RSAKeyValue><Modulus>v299Y/52vsd9sNJUUITL9GU7d3MA9co1FgYHwhY4ZzbBgg04Va2qDBFdyHGBdyGUDx48N8UaXNf92epXe5hWDMPEy2OCuLriXYvYyB/AL/1WINr/G81kT0oGNNpMREuPW5tupAaiwYJz3k8pRxxgJ3NxTLbQ2/j109pvLTs40aQsBov+2hLI5mcAHsjf/VSP4rjx+VcpbNIwWK7XWpaCGrnoxM7+Y787G64KaGgW3E2yWo4VSxvmmeuQ1AIMUH5caD8ymNcMRzAoYfxvVwfl22ckMfx1nowerS4XMp7CuXyjPzUqyht7jUaOCuM0Wr7gB/9LI9/YNM8XJQiEPTb9siQ==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>
```

- o Entorno de Producción:

Se irá suministrando con forme los sistemas vayan realizando las tareas de despliegue en sus entornos de Producción.

3 ANEXO

3.1 EJEMPLO ALGORITMO VALIDACIÓN TICKET Y FIRMA DE MACO

En manos de la Oficina de Calidad del SAS, existen dos algoritmos que permiten realizar la validación del ticket y firma de MACO, uno es la implementación de dicho algoritmo en C#.NET y otro es el mismo algoritmo implementado en Java. Anotar, que NO nos hacemos responsables de si el funcionamiento es totalmente correcto, pero se ha probado y la validación la realiza correctamente, por lo que pensamos que es un buen ejemplo y un buen comienzo para quien desee realizar la validación de MACO:

Para acceder a dichos desarrollos se deberá solicitar vía solicitud CGES el algoritmo o algoritmos, indicando que se necesita el algoritmo de validación de ticket MACO existente en el subversion de OCA suministrados por el SAS para realizar la validación del ticket y firma de MACO, indicando si se quiere el algoritmo en C#.NET o en JAVA o en ambos.

3.2 EJEMPLO DE TICKET DE MACO Y SU FIRMA CORRESPONDIENTE

- ✓ Ticket de MACO:

```
MACO_VAL*7147553****usugenesb*20111209124821
```

- ✓ Firma hash de MACO (hash MD5 cifrado con RSA con la clave privada de MACO):

```
41AAB2D4A438B2350D5F01EA20A68F08915AF0D69F29805C051EE8157A750E28003444A8DA076DE612D4BED3BBDDBEAE1B057586FD7A231E44FE4B0CE5029A6DDB5E3A6DBEBB57C158E195D44E8A6D71A899603934195F89FAB1277B4DB703BC7ACB1266D2A045266AA8EB1B32AA42EC4A9E9E099C9BDDC8A3EBF03C11AE578032BECB7D45BFDEC3A7DC15A62AB9BA50E8EAB77A478EC0BF4D0531927F840F36C509CB08EB4EF767C1521EC6205A916797B8F7FF512F0EEB51BC5AF628CDB3E448DBDE4DEF894EF55645FC3A9179074D29889B724A8A877E24946A5CA44EB4DC0304432F813586ACEAD3F42799B0E40D0771176CB3E0B3E418219C8BC1BE82FB
```


 Servicio Andaluz de Salud CONSEJERÍA DE SALUD	OFICINA TÉCNICA DE INTEROPERABILIDAD	Página 9 de 9
	Política de Autenticación de un Operador MACO	Actualizado: 28/07/2014

3.3 GLOSARIO DE TÉRMINOS

Tabla 4 Glosario

Término	Definición
MACO	Módulo de Acceso Centralizado de Operadores