Securización y comunicación entre aplicativos

Dirección General de Tecnologías de la Información y Comunicaciones

Áreas de Gobierno Tecnológico de SSII y del Dato

Servicio Andaluz de Salud
Consejería de Sanidad, Presidencia y Emergencias

Contenido

Resumen

- **Versión:** v01r08
- **Fecha publicación:** 24 ago 2016
- **Entrada en vigor desde:**13 dic 2016

anterior en JWE quedaría:

- 5. Condiciones
- 6. Resumen

Cumplimiento normativo

Las normas expuestas son de obligado cumplimiento. La STIC podrá estudiar los casos excepcionales los cuales serán gestionados a través de los responsables del proyecto correspondiente y autorizados por el Área de Gobernanza de la STIC. Asimismo cualquier aspecto no recogido en estas normas deberá regirse en primera instancia por las guías técnicas correspondientes al esquema nacional de seguridad y esquema nacional de interoperabilidad según correspondencia y en su defecto a los marcos normativos y de desarrollo software establecidos por la Junta de Andalucía, debiendo ser puesto de manifiesto ante la STIC.

La STIC se reserva el derecho a la modificación de la norma sin previo aviso, tras lo cual, notificará del cambio a los actores implicados para su adopción inmediata según la planificación de cada proyecto.

En el caso de que algún actor considere conveniente y/o necesario el incumplimiento de alguna de las normas y /o recomendaciones, deberá aportar previamente la correspondiente justificación fehaciente documentada de la solución alternativa propuesta, así como toda aquella documentación que le sea requerida por la STIC para proceder a su validación técnica.

Contacto Arquitectura: l-arquitectura.stic@juntadeandalucia.es

Histórico de cambios

Los cambios en la normativa vendrán acompañados de un registro de las modificaciones. De este modo se podrá realizar un seguimiento y consultar su evolución. Ordenándose de mas recientes a menos recientes, prestando especial cuidado a las cabezeras de la tablas dónde se indican las fechas de entrada en vigor y versión.

Versión	v01r07	**Fecha publicación**	24 ago 2016	**Fecha entrada en vigor**	13 dic 2016
Alcance					
• Versión inicial sobre normativa de securización y comunicación entre aplicativos					

Este documento recoge parcialmente la normativa de comunicaciones entre módulos, la OTI será la encargada de definir estas comunicaciones.

Debido a que en ocasiones podremos encontrarnos con transmisiones en entornos no seguros, todo dato con información sensible y/o susceptible a ser recogido bajo la LOPD, debe de seguir las normas de comunicaciones seguras que se expondrán en esta sección.

1. Estándar para la comunicación segura entre Módulos

El estándar que se usara para la comunicación segura entre módulos será **"JSON Object Signing and Encryption"** (JOSE).

Este estandar estara limitado a las comunicaciones HTTP y que se realicen mediante conexiones no seguras (no SSL).

Esta norma proporciona un enfoque general para firmar y encriptar cualquier tipo de contenido. Está concebido deliberadamente sobre JSON y base64url para poder ser usado fácilmente en aplicaciones web.

JOSE está compuesto por varias RFCs:

- **JWA** - JSON Web Algorithms, describe los algoritmos criptográficos usados en JOSE
    - https://tools.ietf.org/html/rfc7518

      Los tres parámetros usados para especificar los algoritmos son "alg" para JWS, "alg" y "enc" para JWE.

      "enc":

      A128CBC-HS256, A192CBC-HS384, A256CBC-HS512 (AES in CBC with HMAC),

      A128GCM, A192GCM, A256GCM

      "alg" for JWS:

      HS256, HS384, HS512 (HMAC with SHA),

      RS256, RS384, RS512 (RSASSA-PKCS-v1_5 with SHA),

      ES256, ES384, ES512 (ECDSA with SHA),

      PS256, PS384, PS512 (RSASSA-PSS with SHA for digest and MGF1)

      "alg" for JWE:

      RSA1_5, RSA-OAEP, RSA-OAEP-256,

      A128KW, A192KW, A256KW (AES Keywrap),

      dir (direct encryption),

      ECDH-ES (EC Diffie Hellman Ephemeral+Static key agreement),

      ECDH-ES+A128KW, ECDH-ES+A192KW, ECDH-ES+A256KW (with AES Keywrap),

      A128GCMKW, A192GCMKW, A256GCMKW (AES in GCM Keywrap),

      PBES2-HS256+A128KW, PBES2-HS384+A192KW, PBES2-HS512+A256KW

      (PBES2 with HMAC SHA and AES keywrap)
- **JWK** - JSON Web Key, describe el formato y el manejo de las claves criptográficas JOSE
    - https://tools.ietf.org/html/rfc7517

Las estructuras de datos para las claves criptográficas incluyen los datos criptográficos y otros atributos.
Ejemplo:

```
{
    "alg": "HS256",
    "kty": "oct",
    "use": "sig",
    "k": "bO5UHaZOo3YzYNXTJcEo1w",
    "kid": "1"
}
```

El parámetro "kty" obligatorio describe el algoritmo criptográfico asociado con la clave. Dependiendo de este parámetro, otros parámetros deberán de ser usados.

- **JWS** - JSON Web Signature, describe la producción y manejo de mensajes firmados
    - https://tools.ietf.org/html/rfc7515
- **JWE** - JSON Web Encryption, describe la producción y manejo de mensajes encriptados
    - https://tools.ietf.org/html/rfc7516
- **JWT** - JSON Web Token, describe la representación de pares clave/valor codificadas en JSON y que pueden ser protegidas por JWS y/o JWE
    - https://tools.ietf.org/html/rfc7519

blocked URL

2. Implementaciones recomendadas

- Java
    - nimbus-jose-jwt
- .NET
    - jose-jwt

3. Acuerdos contractuales

En esta sección ampliaremos el estándar, incluyendo los requisitos para que el uso de las comunicaciones entre los módulos sea aún más específico y se amolde mejor a las necesidades concretas de los sistemas. También permitirá que lenguajes que no posean implementaciones específicas del estándar puedan desarrollar en muy poco tiempo una implementación parcial, solo con las especificaciones obligatorias aquí descritas.

La clave de encriptación y de firma deberán de ser parametrizables y acordadas por el emisor/receptor. Pueden ser diferentes entre ellas.

En concreto se usara JWT firmados y encriptados, en este orden específico.

Debido a la longitud que puede llegar a tener los mensajes generados, y siendo conscientes de que algunos navegadores como IE8 tienen limitación de tamaño en la URL que se puede introducir, se opta por seguir el siguiente patrón de diseño:

- **Apertura de visores:** Se añadirá el parámetro "**credentials**" al header de la comunicación..
- **Otras llamadas (REST, WebServices, etc):** Con el objetivo de respetar el estándar (por ejemplo, las peticiones de datos en REST se hacen con GET), se añadirá el parámetro "**Authorization**" seguido de la palabra JWE (Authorization JWE [Message JWE]) al header de la comunicación.

A continuación se detalla la norma específica que se aplicara adicionalmente al estándar:

1. Especificaciones adicionales de JWT:
    - **Cabecera**

      Obligatorios:

        - "alg", indica el algoritmo usado para la firma. Se usara "HS256".
          Ejemplo: {"alg":"HS256"}
    - **Payload**

      Obligatorios:

        - "exp", fecha de expiración, no podrá ser procesado después de esta fecha.
        - "iat", fecha de creación
        - "jti", identificador único

Opcionales:

- "tipo", Indica el método de comprobación MACO que se llevara a cabo.
  Si el "tipo" es 1 será obligatorio incluir el ticket MACO y la firma MACO
  Si el "tipo" es 2 será obligatorio incluir Código Diraya, cuenta de usuario, Contraseña MD5, Código de modulo, Código de unidad y Código de perfil.
- "codDry", Código Diraya
- "login", Cuenta de usuario
- "passMD5", Contraseña en MD5
- "password", Contraseña en claro
- "codMod", Código de modulo
- "codUni", Código de unidad
- "codPer", Código de perfil
- "tMaco", Ticket MACO
- "fMaco", Firma MACO

Se pueden añadir tantos parámetros adicionales como sea necesario.

Ejemplo JWT

```
{
    "tipo":"1",
    "tMaco":"ticketMACO",
    "fMaco":"firmaMACO",
    "exp":1458214321,
    "iat":1458213721,
    "jti":"5d061a2a-59bc-489d-a8e5-
48a8bf56dcbf",
    "parametroAdicional1":"valorParametroAdici
onal1",
    "parametroAdicional2":"valorParametroAdici
onal2",
    "parametroAdicional3":"valorParametroAdici
onal3"
}
```

1. El token será firmado con la clave compartida especificada (JWK).
2. Se generara el JWE bajo el estándar con las siguientes especificaciones adicionales:
   - **Cabecera**

     Obligatorios:

        - "cty", indica el tipo de contenido, se usara "JWT"
        - "enc", especifica el algoritmo de encriptación, se usara "A128CBC-HS256"
        - "alg", especifica el tipo algoritmo, se usara clave compartida o directa, "dir"
        - "zip", se usara el algoritmo de compresión soportado por el estándar, "DEF"

    Ejemplo JWE

```
{
    "zip":"DEF",
    "cty":"JWT",
    "enc":"A128CBC-HS256",
    "alg":"dir"
}
```

- **Payload**

    El Payload sera el JWT generado anteriormente

4. Ejemplo de uso

Acceda al ejemplo de uso dedicado a REST para ver un ejemplo sobre cómo aplicar esta normativa para securizar las llamadas REST tanto a nivel de servidor como cliente.

En el siguiente fragmento podemos ver un ejemplo de cómo se generaría paso a paso un ticket con JWE:

Algoritmo usado para firmar:

```
{
  "alg": "HS256",
  "kty": "oct",
  "use": "sig",
  "k": "c2VjcmV0MDEyMzQ1Njc4OXNlY3JldDAxMjM0NTY3ODk",
  "kid": "1"
}
```

Algoritmo usado para encriptar:

```
{
  "alg": "HS256",
  "kty": "oct",
  "use": "enc",
  "k": "c2VjcmV0MDEyMzQ1Njc4OXNlY3JldDAxMjM0NTY3ODk",
  "kid": "1"
}
```

Información que queramos transmitir en un mensaje:

Login: nombredeusuariodemaco
Ticket Maco: MACO_CON_OPE+CON_HIS...20161010091352
Firma Maco: 3A7C39A0C58213A35...974A50D1D794B6FCB986 Token JWT construido con la información que se desea transmitir:

{"tMaco":"MACO_CON_OPE+CON_HIS...20161010091352","fMaco":"3A7C39A0C58213A35...974A50D1D794B6FCB986","exp":1493298506,"login":"nombredeusuariodemaco","iat":1493297906,"jti":"74c14b44-36b9-4cb3-a668-ad8edd14de39"}

Tras firmar el token quedaria el siguiente fragmento en:

JWS: eyJhbGciOiJIUzI1NiJ9.eyJ0TWFjbyI6Ik1BQ09fQ09OX09QRStDT05fSElTLi4uMjAxNjEwMTAwOTEzNTIiLCJmTWFjbyI6IjNBN0MzOUEwQzU4MjEzQTM1Li4uOTc0QTUwRDFENzk0QjZGQ0I5ODYiLCJleHAiOjE0OTMyOTg1MDYsImxvZ2luIjoiamdhcnJpYXphcCIsImlhdCI6MTQ5MzI5NzkwNiwianRpIjoiNzRjMTRiNDQtMzZiOS00Y2IzLWE2NjgtYWQ4ZWRkMTRkZTM5In0.nZ10sWLvFwgfDfntz_1ubFcpsag1tyDlvp8i4dWOIPY

Finalmente, al encriptar el fragmento JWS anterior en JWE quedaría:

eyJ6aXAiOiJERUYiLCJjdHkiOiJKV1QiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiZGlyIn0..
2CBQP3KhQAlMBg4mD_pe6g.
26xvVADvnThboJSSul9ywHr8pM6elIfiXN2qCfbkUTiZaqGvUwVH_vQV9oCAtiuHBs4Cht4gZ3Bq1wpiH5yBHUtynE9
KEz0Em-
j96EqksjGTPNyX796v2z1o602p9O4OGLrDsScgm9VecAw8oUSCoQQla9HBpB5WdoZrmXOoKfnM0c_as_AneAd7
VE2DvZDg57WS185qVtHmoeWLdSaTP3q1ZYEEocec1nuc6D7hk5nEn3CitQa_HOQFqlkesR1KH6clNsRRF_0tqlF
J4WDgk_T7spPDYyw7VYGGySOoGjEkE7dAqsDp2aHse_BsTBRwmaCidRz0UjlteJsTabkOkhMSymtzxeacGN-
ezvLDuac.y8ik_hHrLFgIgqueE6oOHQ

5. Condiciones

Las normas y recomendaciones recogidas en esta guía son de obligado cumplimiento. La STIC podrá estudiar los casos excepcionales. Asimismo cualquier aspecto no recogido en esta pagina deberá regirse según las normas establecidas en el marco de desarrollo de la Junta de Andalucía (MADEJA), debiendo ser puesto de manifiesto ante la STIC por el equipo de desarrollo.

La STIC se reserva el derecho a la modificación de la norma sin previo aviso, tras lo cual, notificará del cambio a los actores implicados para su adopción inmediata.

En el caso de que algún actor considere conveniente y/o necesario el incumplimiento de alguna de las normas y/o recomendaciones, deberá aportar previamente la correspondiente justificación fehaciente documentada de la solución alternativa propuesta, así como toda aquella documentación que le sea requerida por la STIC para proceder a su validación técnica.

6. Resumen

Código	Título	Carácter
ARQ.COM.IC.01	Diseño de comunicaciones seguras de acuerdo al estándar JOSE	**Obligatorio**
ARQ.COM.IC.02	Utilización de acuerdos realizados sobre el estándar JOSE	**Obligatorio**
ARQ.COM.IC.03	Envió de JWT firmados(JWS) y encriptados(JWE)	**Obligatorio**
ARQ.COM.IC.04	Parámetro "alg" con valor "HS256" en cabecera de JWT	**Obligatorio**
ARQ.COM.IC.05	Parámetro "exp" en Payload de JWT	**Obligatorio**
ARQ.COM.IC.06	Parámetro "iat" en Payload de JWT	**Obligatorio**
ARQ.COM.IC.07	Parámetro "jti" en Payload de JWT	**Obligatorio**
ARQ.COM.IC.08	Credenciales MACO con formato indicado en el Payload.	**Obligatorio**
ARQ.COM.IC.09	JWT, firmado con clave compartida (JWK)	**Obligatorio**
ARQ.COM.IC.10	JWT firmado (JWS), encriptado con clave compartida (JWK)	**Obligatorio**
ARQ.COM.IC.11	Parámetro "cty" con valor "JWT" en cabecera de JWE	**Obligatorio**
ARQ.COM.IC.12	Parámetro "enc" con valor "A128CBC-HS256" en cabecera de JWE	**Obligatorio**
ARQ.COM.IC.13	Parámetro "alg" con valor "dir" en cabecera de JWE	**Obligatorio**
ARQ.COM.IC.14	Utilización de claves compartidas en la encriptación	**Obligatorio**
ARQ.COM.IC.15	Parámetro "zip" con valor "DEF" en cabecera de JWE	Recomendado
ARQ.COM.IC.16	Uso de implementaciones recomendadas para el estándar JOSE	Recomendado