



**Gobierno
de Canarias**

Consejería de Presidencia,
Justicia y Seguridad
Dirección General de
Telecomunicaciones
y Nuevas Tecnologías



Platino
Plataforma de Interoperabilidad del
Gobierno de Canarias

Interoperabilidad de los servicios telemáticos de la
Administración Pública de la CAC

Página 1 de 19

Manual del desarrollador Servicio de Sello Electrónico y Compulsa Electrónica

Rev.	Fecha	Descripción
0	09/06/10	
1	29/09/10	Se actualiza a la versión 20100929 del servicio
2	11/11/10	Actualización de documentación para incorporar algoritmo para el código de seguridad aplicación de compulsa y modificación de la respuesta del método de compulsa de documento (CU-SSECE-01)
Documento :		PLA-DOC-FIN-10-11-11-SSECE-Manual del programador.odt
Ubicación en eRoom:		
Preparado por		Revisado por
D. Gral. de Telecomunicaciones y Nuevas Tecnologías		Aprobado por
Fecha: 11/11/2010		Fecha:
		Fecha:

 <p>Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías</p>	 <p>Platino Plataforma de Interoperabilidad del Gobierno de Canarias</p>
Servicio de Sello Electrónico y Compulsa Electrónica	Página 2 de 19

ÍNDICE

<u>1 INTRODUCCIÓN.....</u>	<u>3</u>
<u>1.1 CAMBIOS DEL DOCUMENTO RESPECTO A VERSIONES ANTERIORES.....</u>	<u>4</u>
<u>2 VERSIÓN DEL SERVICIO.....</u>	<u>4</u>
<u>3 CASOS DE USO.....</u>	<u>4</u>
<u>3.1 CU-SSECE-01: COMPULSAR DOCUMENTO.....</u>	<u>5</u>
<u>3.1.1 Compulsar documento.....</u>	<u>5</u>
<u>3.2 CU-SSECE-02: COMPULSAR DOCUMENTO DE FORMA AUTOMATIZADA....</u>	<u>9</u>
<u>3.2.1 Sellar documento.....</u>	<u>9</u>
<u>3.3 CU-SSECE-03: VERIFICAR SELLO.....</u>	<u>11</u>
<u>3.3.1 verificar sello.....</u>	<u>11</u>
<u>3.4 CU-SSECE-04: SELLAR DOCUMENTO.....</u>	<u>13</u>
<u>3.4.1 Sellar documento.....</u>	<u>13</u>
<u>4 INFORMACIÓN ADICIONAL.....</u>	<u>15</u>
<u>4.1 CONTROL DE EXCEPCIONES.....</u>	<u>15</u>
<u>4.1.1 SSECEEXCEPTION.....</u>	<u>15</u>
<u>5 GENERACIÓN DEL CÓDIGO DE SEGURIDAD DE LA APLICACIÓN DE</u>	
<u>COMPULSA</u>	<u>16</u>

 <p>Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías</p>	 <p>Platino Plataforma de Interoperabilidad del Gobierno de Canarias</p>
Servicio de Sello Electrónico y Compulsa Electrónica	Página 3 de 19

1 INTRODUCCIÓN

El servicio de sello electrónico y compulsa electrónica tiene como objetivo posibilitar la tramitación electrónica integral de expedientes administrativos, incorporando a los sistemas informáticos de tramitación, imágenes electrónicas de los documentos en soporte papel, con plenas garantías jurídicas.

Además, se pretende facilitar la generación de copias electrónicas a partir de documentos originales en formato papel, tal y como define el artículo 30 de la Ley 11/2007.

El sello electrónico de órgano, basado en certificado electrónico, es un sistema de firma electrónica para la identificación y la autenticación de documentos en las actuaciones administrativas automatizadas. Además, mediante la firma electrónica del personal al servicio de la Administración Pública actuante, podrá realizarse la identificación y autenticación de documentos para la tramitación electrónica integral de expedientes administrativos.



1.1 CAMBIOS DEL DOCUMENTO RESPECTO A VERSIONES ANTERIORES

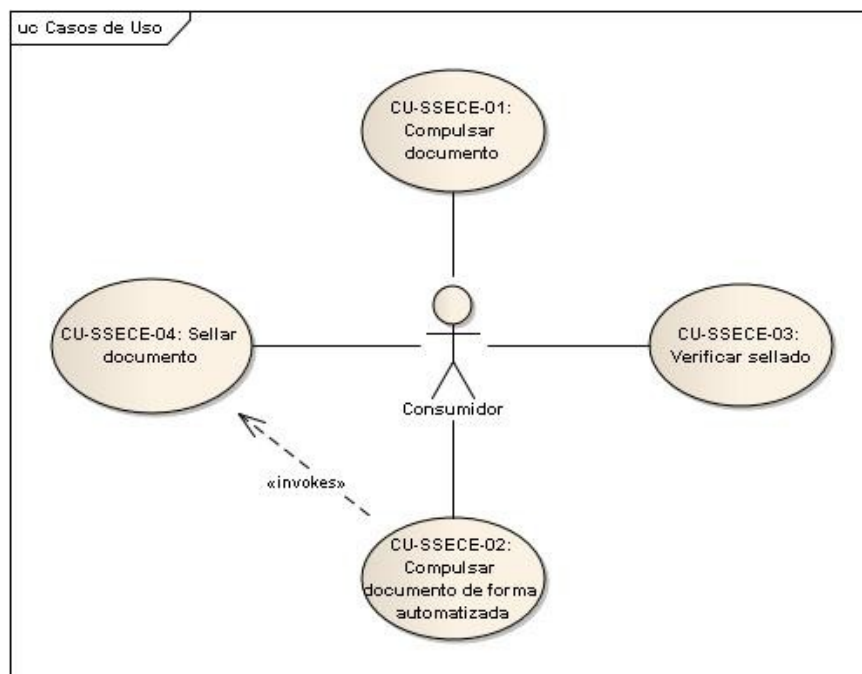
La versión del servicio v20100929, con respecto a la versión anterior v20100906, incorpora la corrección del método para compulsar documentos cuando se copia el documento compulsado en la Carpeta de Documentos del Ciudadano.

2 VERSIÓN DEL SERVICIO

Este documento corresponde a la versión **20100929** de servicio.

3 CASOS DE USO

A continuación de muestra el diagrama de casos de uso del Servicio de Sello Electrónico y Compulsa Electrónica:



3.1 CU-SSECE-01: COMPULSAR DOCUMENTO

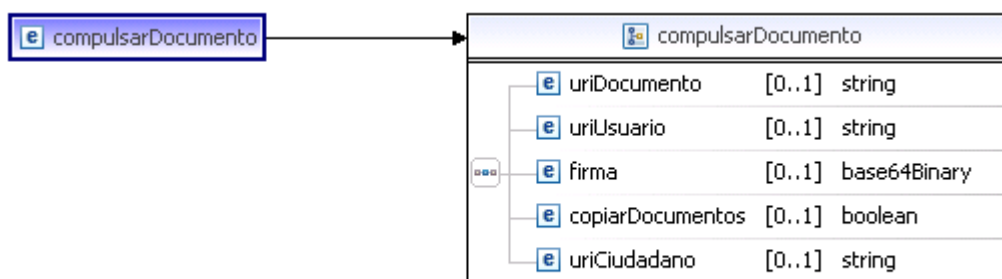
3.1.1 Compulsar documento

Método para compulsar un documento. Se debe especificar el documento y la firma del sellado, así como la URI del usuario firmante. Además, si se va a realizar una copia a la Carpeta de Documentos Administrativos del Ciudadano se necesita la URI del ciudadano.

Interfaz:

compulsarDocumento		
input	parameters	compulsarDocumento
output	parameters	compulsarDocumentoResponse
SseceException	SseceException	SseceException

Entrada del servicio:



Parámetro	Descripción	Tipo
uriDocumento	URI que identifica al documento a compulsar en el repositorio de PLATINO.	string
uriUsuario	URI que identifica al funcionario firmante.	string
firma	Contenido de los datos firmados en formato XMLSignature.	bytes
copiarDocumentos	Indica si los documentos compulsados van a ser	boolean

 <p>Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías</p>	 <p>Platino Plataforma de Interoperabilidad del Gobierno de Canarias</p>
Servicio de Sello Electrónico y Compulsa Electrónica	Página 6 de 19

	copiados a la Carpeta de Documentos Administrativos del Ciudadano.	
uriCiudadano	URI que identifica al ciudadano propietario del documento de la compulsa. Se debe especificar en caso de que el parámetro copiarDocumentos sea true.	string

EJEMPLO DE ENTRADA



Gobierno de Canarias

Consejería de Presidencia,
Justicia y Seguridad
Dirección General de
Telecomunicaciones
y Nuevas Tecnologías



Platino
Plataforma de Interoperabilidad del
Gobierno de Canarias

Servicio de Sello Electrónico y Compulsa Electrónica

Página 7 de 19

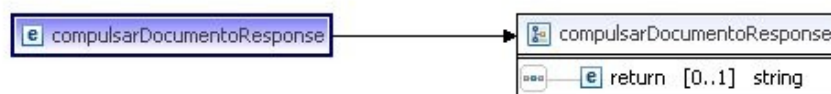
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:compulsarDocumento>
      <uriDocumento>urn:uuid:17f4fab3-a954-11dc-9786-9f28d1e72c791272903742223</uriDocumento>
      <uriUsuario>platino://gobcan.es/servicios/organizacion/funcionario/3279410_DADEE_01092002</uriUsuario>
      <firma><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
    <ds:Reference URI="http://www.mat.ucm.es/~ome2007/prueba.pdf">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
      <ds:DigestValue>UlcXYDIdetAaIDRGUs71d1SpwUs=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
OfQp7xUGb1Y5Ns+kj2ak+ConxqBvLriqXTsTHuV9V1PWcrtxF3JQsX1ZYkv6eg2X8Xf5SEC+RrWS
N+G7bFwfJ8ucCCSNB0je8OxhL4QVrbtEKufQAOEwzIRYBCIlirZjgvTTy9TCHK+z0w2CV9X5cka
1IVDKli5ImxuO3wY3Ws=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>CN=cibercentro,OU=DGTI,O=Gobierno de
Canarias,ST=Canarias,C=ES,EMAILADDRESS=cibercentro@gobiernodecanarias.org</ds:X509IssuerName>
<ds:X509SerialNumber>294005470306486901017480</ds:X509SerialNumber>
</ds:X509IssuerSerial>
<ds:X509Certificate>
MIIEOTCCA+OgAwIBAgIKPkRiAACAAALiDANBgkqhkiG9w0BAQUFADCBlzExMC8GCSqGSIb3DQEJ
ARYiY2liZXJjZW50cm9AZ29iaWVybm9kZWVhbmFyaWFzLm9yZzELMAkGA1UEBhMCrVMxETAPBgNV
BAGTCENhbmFyaWFzMR0wGwYDVQQKEExRHb2JpZXJubyBkZSBZDlY5hcmllhczENMAAsGA1UECmEREdU
STEUMBIGA1UEAaXMLEy2liZXJjZW50cm8wHhcNMDcwNjEzMTExMzEyWWhcNMDgwNjEzMTExMzEyWjCB
jTEhMCUGCSqGSIb3DQEJARYYanBhZHZHb2kvcGVuY2FuYXJpYXMuY29tMQswCQYDVQQGEwJFUzER
MA8GA1UECmIQ2FuYXJpYXMuY29tMQswCQYDVQQGEwJFUzERMA8GA1UECmIQ2FuYXJpYXMuY29tMQswCQYDVQQGEwJFUzER
EwRER1RjRmRwEgYDVQQDEwtleHQtanBhZGxvcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
rg5O7I0PqnBKGDHlnPmKP9pTrjwJigwuh8lIKX7hLNDAlEcTcTPyskesVPm9KYWNpEozuD1Yolor
ww9cMX9NnrQGz8887w7nmz6luCEBva+QeA2mfY4p4k5kDoOHw/uaSPJqxY7xUmSkQtCEnddewyG
+uS07hd7QbpR+t273I8CAwEAaOCAdMwggHPMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggr
BgEFBQcDAjAdBgNVHQ4EFgQU3N3sRosdglUOUrONw4IDQEOQzsEwgDMGA1UdIwSByzCByIAUcOOk
rLNBKRzd4albEFxWolX1nxKhgZ2kgZowgZcxMTAvBgkqhkiG9w0BCQEWImNpYmVvY2VudHJvQGdv
Ymllcm5zVzGvYjW5hcmllhcy5vcmcxCzAJBgNVBAYTAkVTMREwDwYDVQQIEWhDYW5hcmllhczEdMBsG
A1UEChMUR29iaWVybm9kZWUgQ2FuYXJpYXMuY29tMQswCQYDVQQGEwJFUzERMA8GA1UECmIQ2FuYXJpYXMuY29tMQswCQYDVQQGEwJFUzER
Y2VudHJvghAZZsd2bMjlrkCEiAcS60oDMFMGA1UdHwRMMEowSKBGoESGQmhd0HA6Ly9jb2d2d29y
dGguZ29iaWVybm9kZWVhbmFyaWFzLm9yZy9jZXJ0ZW5y2xsl2NpYmVvY2VudHJvLmNybDBBeBggr
```

```

BgEFBQcBAQRSMFAwTgYIKwYBBQUHMAKGMh0dHA6Ly9jb2dzd29ydGguZ29iaWVyb9kZWNhbmFy
aWFzLm9yZy9jZlJ0ZW5yb2xsL2NpYmVvY2VudHJvLmNydDANBgkqhkiG9w0BAQUFAANBAGk7MHeB
VTA/ygxmLwOyL551yzSjPlauj3bc18d3Dy76+GCCkxw9OsjNs9Dr35uNggaovLzQaaZyuIGVfPZ
++k=
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
rg5O7I0PqnBKGdHlnPmKP9pTrjwJigwuh8IIKX7hLNDAIEcTcTPyskesVPm9KYWNpEozuD1Yolor
ww9cMX9NnrQGz8887w7nmz6luCEBva+QeA2mfY4p4kc5kDoOHw/uaSPJqxY7xUmSkQtCEnddewyG
+uS07hd7QbpR+t273I8=
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>]]</firma>
  <copiarDocumentos>true</copiarDocumentos>
  <uriCiudadano>platino://gobcan.es/servicios/terceros/tercero/80965f0a-d843-4412-91de-4fa9b0ded07f2</uriCiudadano>
</ssec:compulsarDocumento>
</soapenv:Body>
</soapenv:Envelope>

```

Salida del servicio:



Parámetro	Descripción	Tipo
return	URI que tiene el documento compulsado en la Carpeta del Ciudadano si se especificó la opción de copiarlo en la misma.	String

 Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías	 Platino Plataforma de Interoperabilidad del Gobierno de Canarias
Servicio de Sello Electrónico y Compulsa Electrónica	Página 9 de 19

EJEMPLO DE SALIDA

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:compulsarDocumentoResponse/>
  </soapenv:Body>
</soapenv:Envelope>
```

3.2 CU-SSECE-02: COMPULSAR DOCUMENTO DE FORMA AUTOMATIZADA

3.2.1 Sellar documento

Método para aplicar un sello electrónico a un documento del repositorio. Se debe especificar la URI documento, el tipo de sello a aplicar (Compulsa) y el alias del certificado que se utilizará para firmar. El certificado debe estar almacenado en el servidor.

Interfaz:

sellarDocumento		
input	parameters	sellarDocumento
output	parameters	sellarDocumentoResponse
SseceException	SseceException	SseceException

Entrada del servicio:



Gobierno de Canarias

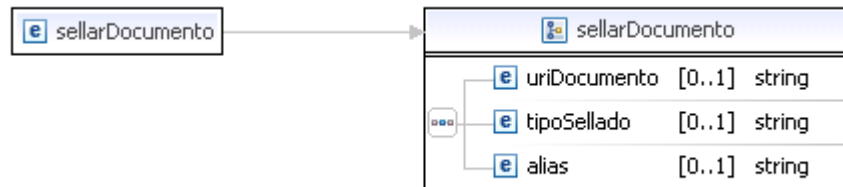
Consejería de Presidencia,
Justicia y Seguridad
Dirección General de
Telecomunicaciones
y Nuevas Tecnologías



Platino
Plataforma de Interoperabilidad del
Gobierno de Canarias

Servicio de Sello Electrónico y Compulsa Electrónica

Página 10 de 19



Parámetro	Descripción	Tipo
uriDocumento	URI que identifica al documento en el repositorio de PLATINO	string
tipoSellado	Tipo de sellado a realizar (Compulsa).	string
alias	Alias del certificado, almacenado en el servidor, con el que se va firmar el documento.	string

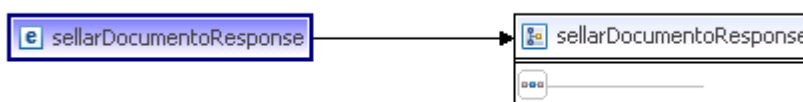
EJEMPLO DE ENTRADA

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:sellarDocumento>
      <uriDocumento>urn:uuid:17f4fab3-a954-11dc-9786-9f28d1e72c791272903742223</uriDocumento>
      <tipoSellado>Compulsa</tipoSellado>
      <alias>camerfirma</alias>
    </ssec:sellarDocumento>
  </soapenv:Body>
</soapenv:Envelope>
```

 Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías	 Platino Plataforma de Interoperabilidad del Gobierno de Canarias
Servicio de Sello Electrónico y Compulsa Electrónica	Página 11 de 19

```
</soapenv:Envelope>
```

Salida del servicio:



Parámetro	Descripción	Tipo
No hay parámetros		

EJEMPLO DE SALIDA

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:sellarDocumentoResponse/>
  </soapenv:Body>
</soapenv:Envelope>
```

3.3 CU-SSECE-03: VERIFICAR SELLO

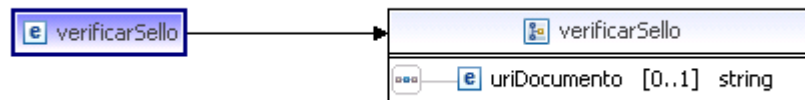
3.3.1 VERIFICAR SELLO

Método para verificar si a un documento se le ha aplicado un sello electrónico. En caso de que posea información de sellado se verifica si la firma en formato XMLSignature es válida.

Interfaz:

verificarSello		
input	parameters	verificarSello
output	parameters	verificarSelloResponse
SseceException	SseceException	SseceException

Entrada del servicio:



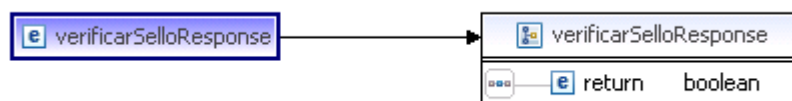
Parámetro	Descripción	Tipo
uriDocumento	URI de PLATINO que identifica al documento al que se le quiere verificar su sellado.	string

EJEMPLO DE ENTRADA

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:verificarSello>
      <uriDocumento>urn:uuid:17f4fab3-a954-11dc-9786-9f28d1e72c791272903742223</uriDocumento>
    </ssec:verificarSello>
  </soapenv:Body>
</soapenv:Envelope>
  
```

Salida del servicio:



 Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías	 Platino Plataforma de Interoperabilidad del Gobierno de Canarias
Servicio de Sello Electrónico y Compulsa Electrónica	Página 13 de 19

Parámetro	Descripción	Tipo
return	Resultado de la verificación del sellado.	boolean

EJEMPLO DE SALIDA

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:verificarSelloResponse>
      <return>true</return>
    </ssec:verificarSelloResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

3.4 CU-SSECE-04: SELLAR DOCUMENTO

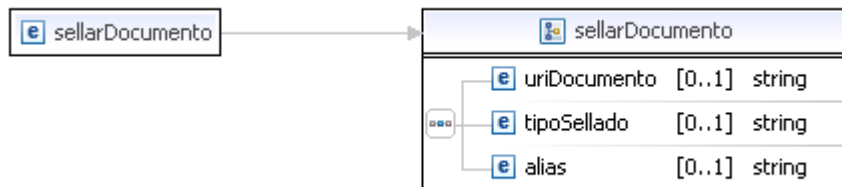
3.4.1 SELLAR DOCUMENTO

Método para aplicar un sello electrónico a un documento del repositorio. Se debe especificar la URI documento, el tipo de sello a aplicar (Compulsa, Representación o Conformidad) y el alias del certificado que se utilizará para firmar. El certificado debe estar almacenado en el servidor.

Interfaz:

sellarDocumento		
input	parameters	sellarDocumento
output	parameters	sellarDocumentoResponse
SseceException	SseceException	SseceException

Entrada del servicio:

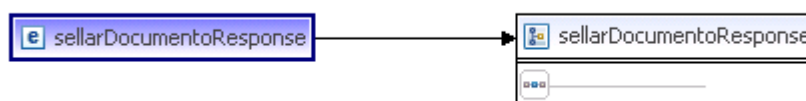


Parámetro	Descripción	Tipo
uriDocumento	URI que identifica al documento en el repositorio de PLATINO	string
tipoSellado	Tipo de sellado a realizar (Compulsa, Conformidad o Representación).	string
alias	Alias del certificado, almacenado en el servidor, con el que se va firmar el documento.	string

EJEMPLO DE ENTRADA

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece">
  <soapenv:Header/>
  <soapenv:Body>
    <ssec:sellarDocumento>
      <uriDocumento>urn:uuid:17f4fab3-a954-11dc-9786-9f28d1e72c791272903742223</uriDocumento>
      <tipoSellado>Conformidad</tipoSellado>
      <alias>camerfirma</alias>
    </ssec:sellarDocumento>
  </soapenv:Body>
</soapenv:Envelope>
```

Salida del servicio:



 Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías	 Platino Plataforma de Interoperabilidad del Gobierno de Canarias
Servicio de Sello Electrónico y Compulsa Electrónica	Página 15 de 19

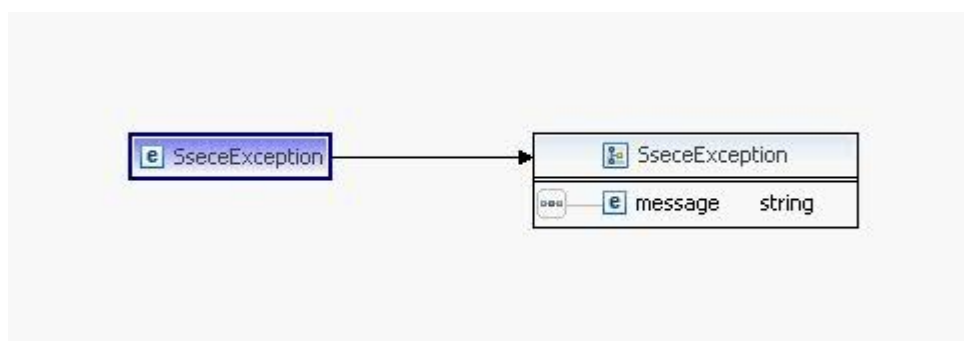
Parámetro	Descripción	Tipo
No hay parámetros		

EJEMPLO DE SALIDA
<pre><soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssec="http://platino.gobcan.es/servicios/ssece"> <soapenv:Header/> <soapenv:Body> <ssec:sellarDocumentoResponse/> </soapenv:Body> </soapenv:Envelope></pre>

4 INFORMACIÓN ADICIONAL

4.1 CONTROL DE EXCEPCIONES

4.1.1 SSECEEXCEPTION



Parámetro	Descripción	Tipo
message	Descripción textual del error.	String

 <p>Gobierno de Canarias Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías</p>	 <p>Platino Plataforma de Interoperabilidad del Gobierno de Canarias</p>
Servicio de Sello Electrónico y Compulsa Electrónica	Página 16 de 19

5 GENERACIÓN DEL CÓDIGO DE SEGURIDAD DE LA APLICACIÓN DE COMPULSA

La aplicación de compulsa está destinada a la compulsa de documentos por parte de los funcionarios en el servicio SSECE. Puede ser utilizada haciendo login en la aplicación o invocada por parámetros.

Cuando la aplicación es invocada por parámetros habrá que pasar en la URL de la aplicación la URI del funcionario que realizará la compulsa (“uriUsuario”), la URI del documento a compulsar (“uriDocumento”) y las URL de navegación al finalizar el proceso dependiendo de si éste fue correcto (“urlOK”) o hubo algún error (“urlNoOK”). Si se quiere copiar el documento una vez compulsado a la Carpeta de Documentos Administrativos del Ciudadano (“copiarDocumento” con valor true) habrá de especificarse también la URI del ciudadano que aporta el documento (“uriCiudadano”). Por último, se deberá pasar también un código de seguridad generado a partir de los parámetros anteriores (“codSeguridad”). A continuación se detalla el algoritmo para la generación de dicho código.

El primer paso es generar una cadena basada en los parámetros con los que va a ser llamada la aplicación. Se construye de la siguiente manera:

URI del documento+”&”+URI del usuario+”&”+URI del ciudadano

Como la URI del ciudadano es opcional si no va a ser utilizada en la invocación de la aplicación la cadena se construiría obviando la misma, es decir, quedaría como:

URI del documento+”&”+URI del usuario

A esta cadena obtenida se le pasará el algoritmo de reducción criptográfica “MD5” y al resultado el algoritmo de cifrado “Blowfish”. Para la utilización de este último algoritmo es necesario conocer la clave para encriptar definida para el servicio.

A continuación se detalla la implementación en lenguaje Java del algoritmo de generación del código de seguridad. El método inicial a invocar es “execute”. Las variables globales “uriCiudadano”, “uriDocumento” y “uriUsuario” estarían definidas con las URI de platino correspondientes. La variable “keyEncrypt” se establece con la clave para encriptar definida para el servicio. El método “hexToBytes” transforma una cadena en hexadecimal a un array de bytes y el método “bytesToHex” hace lo

 <p>Gobierno de Canarias</p> <p>Consejería de Presidencia, Justicia y Seguridad</p> <p>Dirección General de Telecomunicaciones y Nuevas Tecnologías</p>	 <p>Platino Plataforma de Interoperabilidad del Gobierno de Canarias</p>
<p>Servicio de Sello Electrónico y Compulsa Electrónica</p>	<p>Página 17 de 19</p>

contrario. El código de seguridad final queda definido en la variable global “parametroSeguridad”.



Algoritmo generación código de seguridad

```
public void execute() {

    String paramOpcional = (uriCiudadano != null && !"".equals(uriCiudadano) ? "&"+uriCiudadano : "");
    String parametros = uriDocumento+"&"+uriUsuario+paramOpcional;
    try {
        String keyEncrypt= "560e05d3dff8a4f82b87d5f44a0a697a";
        byte[] data = getMD5(parametros.getBytes());
        parametroSeguridad = encrypt(data,keyEncrypt);
    } catch (Exception e) {
        e.printStackTrace();
    }
}

public static byte[] getMD5(byte[] data) throws Exception {
    MessageDigest digest = java.security.MessageDigest.getInstance("MD5");
    digest.update(data);
    byte[] hash = digest.digest();
    return hash;
}

public static byte[] hexToBytes(char[] hex) {
    int length = hex.length / 2;
    byte[] raw = new byte[length];
    for (int i = 0; i < length; i++) {
        int high = Character.digit(hex[i * 2], 16);
        int low = Character.digit(hex[i * 2 + 1], 16);
        int value = (high << 4) | low;
        if (value > 127)
            value -= 256;
        raw[i] = (byte) value;
    }
    return raw;
}

public static String encrypt(byte[] input, String key) throws Exception {

    byte[] bytes = hexToBytes(key.toCharArray());
    SecretKeySpec keySpec = new SecretKeySpec(bytes, "Blowfish");
    Cipher cipher = Cipher.getInstance("Blowfish");
    cipher.init(Cipher.ENCRYPT_MODE, keySpec);
    byte[] encrypted = cipher.doFinal(input);
    String encryptedHex = bytesToHex(encrypted);
    return encryptedHex;
}
```



**Gobierno
de Canarias**

Consejería de Presidencia,
Justicia y Seguridad
Dirección General de
Telecomunicaciones
y Nuevas Tecnologías



Platino
Plataforma de Interoperabilidad del
Gobierno de Canarias

Servicio de Sello Electrónico y Compulsa Electrónica

Página 19 de 19

```
public static String bytesToHex (byte buf[]) {  
    StringBuffer strbuf = new StringBuffer(buf.length * 2);  
    int i;  
    for (i = 0; i < buf.length; i++) {  
        if (((int) buf[i] & 0xff) < 0x10)  
            strbuf.append("0");  
        strbuf.append(Long.toString((int) buf[i] & 0xff, 16));  
    }  
    return strbuf.toString();  
}
```

Ejemplo:

A continuación se detalla el resultado de aplicar el algoritmo para un caso de uso concreto.

Ejemplo generación de código de seguridad

Clave para encriptar: 560e05d3dff8a4f82b87d5f44a0a697a

URI del documento: urn:uuid:2ead783a-6973-11df-8331-51bdc27e640b

URI funcionario: platino://gobcan.es/servicios/organizacion/funcionario/3301810_EVSUASAN_18012010

URI del ciudadano: platino://gobcan.es/servicios/terceros/tercero/da43a7bf-629b-4269-b756-65b5cec6a2c2adf

Construcción de cadena con los parámetros: urn:uuid:2ead783a-6973-11df-8331-51bdc27e640b&platino://gobcan.es/servicios/organizacion/funcionario/3301810_EVSUASAN_18012010&platino://gobcan.es/servicios/terceros/tercero/da43a7bf-629b-4269-b756-65b5cec6a2c2

Cadena resultante tras pasar algoritmo MD5 a la cadena anterior(en hexadecimal): b850b55b86babb6f5d5452358163ed9b

Código de seguridad final: c6208e7e0a474297ca4dc6f5d3168830e45e78d8b637515b