# Anexo 28, Guía de Desarrollo

## Integración con DataPower en el desarrollo del proyecto

*Área de explotación y sistemas*

GERENCIA INFORMÁTICA
JOSEFA VALCÁRCEL, 44
28027-MADRID

# Índice General

*1 INTRODUCCIÓN ..... 4*

**1.1 OBJETIVO ..... 4**
**1.2 AUDIENCIA ..... 4**
**1.3 ESTRUCTURA DEL DOCUMENTO ..... 4**
**1.4 GLOSARIO ..... 5**
*1.4.1 Términos ..... 5*
*1.4.2 Acrónimos ..... 5*

*2 ARQUITECTURA ACTUAL ..... 6*

**2.1 ESQUEMA ESTÁNDAR PARA SERVICIOS WEB (WS) ..... 6**
**2.2 ESQUEMA ESTÁNDAR PARA INTERACCIONES WEB ..... 7**
*2.2.1 Imagen del esquema estándar ..... 8*

*3 INTEGRACIÓN DE LAS APLICACIONES CON DATAPOWER ..... 9*

*3.1.1 Sin autenticación ..... 9*
*3.1.2 Usuario y contraseña ..... 9*
*3.1.3 Certificado ..... 10*
*3.1.4 Token LTPA ..... 10*
**3.2 FORMATOS DE ENTRADA O SALIDA ..... 11**
*3.2.1 Non-XML ..... 11*
*3.2.2 XML ..... 11*
*3.2.3 SOAP ..... 11*
*3.2.4 JSON ..... 12*
*3.2.5 Otros ..... 12*
**3.3 OPERACIONES CRIPTOGRÁFICAS ..... 12**
*3.3.1 Firma de la DGT hacia terceros (sello electrónico) ..... 12*
*3.3.2 Firma de la DGT hacia aplicaciones internas ..... 12*
*3.3.3 Validación de firma ..... 13*
*3.3.4 Verificación de firma ..... 13*
**3.4 PROTECCIÓN OFRECIDA ..... 13**
*3.4.1 Cifrado/firma de mensajes ..... 14*
*3.4.2 Validación de esquema ..... 14*
*3.4.3 Protección contra SQL injection ..... 14*
*3.4.4 Protección ante ataques XDoS ..... 14*
*3.4.5 Protección ante ataques MMXDoS ..... 15*
*3.4.6 Protección ante ataques de fuerza bruta ..... 15*
**3.5 OTROS SERVICIOS ..... 16**
*3.5.1 SLA (nivel de servicio) ..... 16*
*3.5.2 Single Sign-On ..... 16*

*4 INTEGRACIÓN DE APLICACIONES CON DATAPOWER ..... 17*

**4.1 INTEGRACIÓN DE APLICACIONES WEB EN EL ENTORNO DE DESARROLLO ..... 18**
*4.1.1 Ejemplo de integración de una aplicación WEB ..... 21*
**4.2 INTEGRACIÓN DE UN WS EN DESARROLLO ..... 22**
*4.2.1 Ejemplo de integración de un WS en desarrollo ..... 23*

*5 OTRAS CONSIDERACIONES ..... 25*

**5.1 DUDAS Y CONTACTO CON EL EQUIPO DE *DATAPOWER* ..... 25**

# Índice de Ilustraciones y Tablas

Ilustración 1: Esquema estándar de los accesos con *DataPower* ..... 8
Ilustración 2: Procedimiento de *single sign-on*..... 17

Tabla 1: Ejemplo de nombres DNS para aplicaciones WEB..... 20
Tabla 2: Ejemplo de asociación de roles en el servidor WAS..... 22
Tabla 3: Ejemplo de roles de aplicación..... 24

## Control de versiones

| Versión | Fecha | Autor | Descripción / Comentarios |
|---|---|---|---|
| 1.0 | 11/03/2013 | Arquitectura ESB | Creación del documento. |
| 1.1 | 05/06/2014 | Arquitectura ESB | Revisión y actualización. |
| 1.2 | 28/10/2015 | Arquitectura ESB | Se añade el apartado 4 (Integración de aplicaciones) |
| 1.3 | 13/01/2017 | Arquitectura ESB | Actualización de información obsoleta |
| 1.4 | 04/02/2019 | Arquitectura ESB | Revisión y actualización del documento completo |
| | | | |

# 1 Introducción

Para evitar retrasos en la implantación de nuevas aplicaciones o evoluciones de las existentes, es conveniente que los equipos de desarrollo conozcan las acciones que se pueden realizar y de qué manera con respecto al elemento de integración *DataPower*, para así poder diseñar una arquitectura realista desde el primer momento, evitando redefiniciones de la misma y retrasos innecesarios.

## 1.1 Objetivo

Este documento tiene la finalidad de exponer las funcionalidades de *DataPower* utilizadas en la Dirección General de Tráfico, dentro de todo el espectro de funcionalidades que ofrece el producto.

## 1.2 Audiencia

Este documento está dirigido a los equipos de desarrollo y, en general, a cualquier equipo o departamento que requiera integrarse con el *gateway DataPower*.

## 1.3 Estructura del documento

Este documento está distribuido en 5 capítulos, con los siguientes contenidos:

- Capítulo 1: Introducción, contiene información relativa al propio documento.
- Capítulo 2: Posibles usos que las aplicaciones pueden realizar de DataPower, consideraciones de seguridad e integración.
- Capítulo 3: Consideraciones a tener en cuenta que no estén directamente relacionados con la implantación de servicio en DataPower o integración de las aplicaciones con el mismo.
- Capítulo 4: Procedimiento para integrar una aplicación WEB y un WS en desarrollo con DataPower.
- Capítulo 5: Flujos de comunicación con los equipos de DataPower.

# 1.4 Glosario

## 1.4.1 Términos

En este apartado se incluyen, organizados por orden alfabético, los términos que se utilizan en el propio documento, para facilitar su lectura y comprensión.

- ***DataPower***: IBM *DataPower Gateway* es un producto de aceleración, securización e integración de servicios.

## 1.4.2 Acrónimos

En este apartado se incluyen, organizados por orden alfabético, los acrónimos que se utilizan en el propio documento para facilitar su lectura y comprensión.

En este apartado se incluyen, organizados por orden alfabético, las abreviaturas que se utilizan en el propio documento, para facilitar su lectura y comprensión.

- **CA**: Certification Authority
- **DGT**: Dirección General de Tráfico
- **DNS**: Domain Name System
- **DP**: *DataPower*
- **FTP**: File Transfer Protocol
- **SOAP**: Simple Object Access Protocol

- **SSL**: Secure Sockets Layer
- **HTTP**: Hypertext Transfer Protocol
- **HTTPS**: Hypertext Transfer Protocol Secure
- **IHS**: IBM HTTP Server
- **JMS**: Java Message Service
- **JSON**: JavaScript Object Notation
- **NFS**: Network File System
- **SLM**: Service Level Monitor
- **XDoS**: XML Denial of Service
- **XML**: eXtensible Markup Language
- **WAS**: Websphere Application Server
- **WS:** Web Service

# 2 Arquitectura actual

## 2.1 Esquema estándar para servicios WEB (WS)

Dependiendo del punto de acceso de la aplicación a la red de la DGT central, la petición seguirá uno de estos dos caminos:

**a)** Si la petición llega desde Internet, la autenticación entre usuario (o aplicación externa) y el *DataPower* de Internet se realiza mediante *certificado* y *firma digital*, garantizando así la autenticidad del emisor y la seguridad que el mensaje no ha sido alterado durante la transmisión. Se comprueba la existencia del certificado y se envía a la plataforma de validación @Firma, que realizará una serie de comprobaciones para asegurar la validez del mismo. Si el usuario se autentica correctamente, se genera un token *LTPA* con las credenciales que servirá para *autenticar* al usuario en el segundo *DataPower* (si la petición llega a intranet) y también para *autorizar* la petición en el servidor de aplicaciones WAS. Además del *token* LTPA también se generan unas *cookies* con la información del peticionario, que servirá a la aplicación para identificar de manera inequívoca al usuario llamante. Esta identificación se realiza programáticamente mediante las librerías del *módulo de login*.

Cabe recordar que hay dos *clusters* DP en producción, uno situado en el segmento de Internet (DMZ) y el otro en la intranet (DGT central). Esto implica que las aplicaciones que accedan por Internet y que tengan como destino final el WAS de intranet, tendrán que pasar por ambos *DataPower*, aunque el usuario sólo se autenticará en el primero de ellos. Por el contrario, si accede desde la intranet, la petición sólo pasará por el DP de intranet, autenticándose en este.

La comunicación entre el DP de Internet y el DP de intranet se realiza mediante el protocolo HTTPS.

**b)** Si la aplicación accede desde la red de intranet (red de la DGT central –por ejemplo, desde otras aplicaciones de esta red), el mensaje se autenticará mediante *usuario y contraseña* (*WS-Security UsernameToken*) en la petición SOAP contra el LDAP. Si la autenticación es correcta, se generará el *token* LTPA (y las *cookies*) y la petición se enviará al servidor de aplicaciones WAS.

En caso de que se acceda a la capa de intranet desde otra red (Red SARA, JPT, ayuntamientos...), la autenticación será la misma que la provista en la capa de Internet (*certificado y firma*), aunque si es necesario por obligación del negocio, técnicamente es posible autenticar los mensajes con *usuario y contraseña*, como si proviniesen de la intranet de DGT.

## 2.2 Esquema estándar para interacciones WEB

Al igual que en el apartado anterior, la petición puede llegar hasta *DataPower* bien entrando a la capa de Internet o hacia la de intranet. En cualquier caso, la conexión entre el usuario y el *DataPower* se establecerá mediante el protocolo HTTPS:

**a)** Si la petición llega desde Internet, la autenticación del usuario ha de realizarse mediante certificado digital. Para ello se abre una nueva conexión contra un puerto específico (5555 o 9443 en SEDE) que requiere SSL mutuo. El mismo certificado que proporciona el usuario para cerrar el túnel TLS, es enviado a @Firma para su validación. Una vez autenticado el usuario, se crea un *token* LTPA (y unas *cookies*) que servirán para autorizar e identificar al usuario ante el WAS de la capa de Internet.

En este caso, tanto la autenticación como el enrutamiento hacia la aplicación final la realiza únicamente el *DataPower* de Internet, sin mediación de ningún tipo del *DataPower* de intranet. Es decir, no existen aplicaciones WEB intranet publicadas en Internet, como sí sucede con los WS.

También existe la posibilidad de autenticarse mediante el sistema Cl@ve, que es método recomendado

dado que es el estándar utilizado en las administraciones públicas. Además se obtiene el beneficio añadido de no utilizar puertos no estándar como el 5555 o 9443. De cara a la aplicación el sistema utilizado es transparente, ya que en ambos se genera la misma información (*token* LTPA y *cookies*).

**b)** Si el usuario accede desde la red de intranet, se puede autenticar por usuario y contraseña (dominio apl.p3.trafico.es) contra el LDAP o, si la aplicación lo requiere, mediante certificado digital (dominio apl.p3.traficocert.es); aunque esto último se sale de la norma y debe tratarse como una excepción. En el caso de autenticación por certificado, el procedimiento es análogo al utilizado en la capa de Internet.

### 2.2.1 Imagen del esquema estándar

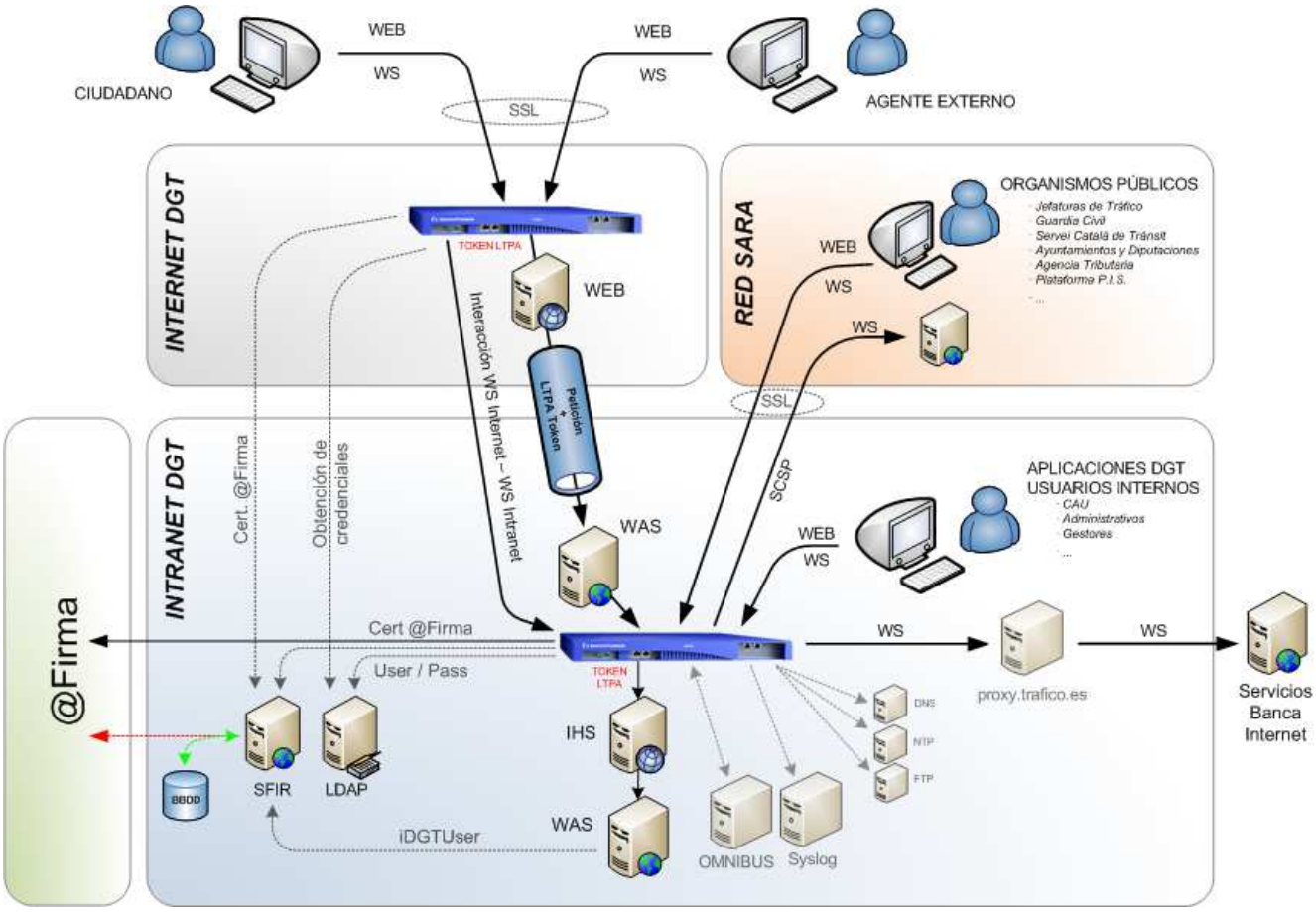


**Ilustración 1: Esquema estándar de los accesos con *DataPower***

# 3 Integración de las aplicaciones con *DataPower*

Para verificar que la petición procede de un usuario legítimo, *DataPower* realiza funciones de validación y autenticación de credenciales, tal como ya se ha comentado (*certificado* con @Firma y *usuario y contraseña* con LDAP). Sin embargo, la comprobación de si el usuario tiene permisos o no para ejecutar la operación pedida, se realiza por el *backend* (WAS) mediante el rol asignado al usuario.

Hay que tener en cuenta que, por definición de la arquitectura de la DGT, *DataPower no realiza autorización* de recursos, esto es, no limita a qué *backends* puede acceder un usuario una vez su *autenticación* se haya realizado satisfactoriamente. Es decir, *DataPower* **autentica** la petición del cliente, pero es el servidor de aplicaciones WAS quien la **autoriza**.

*DataPower* permite múltiples métodos de autenticación y validación de usuarios para realizar las funciones de securización definidas. También es posible definir servicios que atraviesen *DataPower* sin necesidad de autenticación por parte del usuario.

### 3.1.1 Sin autenticación

Por su naturaleza, algunas peticiones pueden atravesar el bus sin necesidad de autenticación (principalmente elementos estáticos y fuera de la lógica de negocio, tales como imágenes o estilos CSS). En estos casos, DP añade funciones tales como verificación de conformación correcta de datos y prevención contra algunos tipos de ataques.

### 3.1.2 Usuario y contraseña

Debido a *restricciones legales*, el acceso a los servicios mediante *usuario y contraseña* sólo es posible a través de intranet. Para accesos desde Internet, se habrá de utilizar autenticación por certificado.

Si la autenticación se realiza mediante este método, *DataPower* comprobará las credenciales en LDAP (primero verificará que existe el usuario y posteriormente comprobará la contraseña). En caso

de que las credenciales aportadas sean correctas, DP generará el *token* LTPA correspondiente, el cual se utilizará como credencial para el resto de interacciones de la petición. Por tanto, las credenciales originales de *usuario y contraseña* no estarán disponibles una vez generado el *token*, hecho que aumenta la seguridad de las transacciones posteriores.

El *DataPower* está capacitado para **comprobar la fecha de expiración de la contraseña** del usuario. En caso de intentar autenticar un usuario que contenga una fecha próxima de caducidad, *DataPower* presentará una página indicando esta situación y mostrando dos botones, uno enlazando a la aplicación que permita al usuario cambiar su contraseña y otro que permite al usuario continuar con la operativa normal. Conviene aclarar que, **aunque esta funcionalidad ha sido implementada, nunca ha sido comprobada** dado que le LDAP actual no soporta la caducidad de contraseñas.

Si el usuario no está correctamente autenticado o su contraseña ha caducado, se realizará una redirección a la página de login para que vuelva introduzca sus credenciales.

### 3.1.3 Certificado

Para realizar accesos desde el exterior de la infraestructura de la DGT o de la red SARA, es necesario el uso de autenticación del usuario mediante *certificado y firma digital*, ya que toda la información viajará a través de Internet, la cual es una red altamente insegura.

En este caso, DP comprobará la existencia del certificado y se lo enviará a la plataforma @Firma para que compruebe si el certificado es válido o no y obtenga los datos del usuario. Si se confirma la validez de dicho certificado, se generará el *token* LTPA que servirá para realizar la autorización en el WAS y las *cookies* correspondientes, que servirán para identificar al usuario en la aplicación, a través de las librerías del *módulo de login*.

### 3.1.4 Token LTPA

Sólo las peticiones recibidas por el DP en intranet pueden contener un *token* LTPA.

Si este *token* está presente, es debido a que la petición ha sido ya autenticada en el DP de Internet. No hay ninguna aplicación en producción que genere la petición con un token LTPA directamente, por lo que las peticiones que llegan al *DataPower* de intranet sin haber pasado por el de Internet, han de utilizar algunos de los métodos de autenticación mencionados anteriormente.

## 3.2 Formatos de entrada o salida

*DataPower* puede manejar varios formatos de datos, *realizando transformaciones de los mismo si es preciso.*

Excepto para el procesamiento *passthrough*, es posible realizar transformaciones de los datos recibidos, tanto a nivel lógico (generación, eliminación o modificación de los datos) como a nivel morfológico (formato en que se presentan los datos).

Un ejemplo de esta transformación se ha realizado para ofrecer retrocompatiblidad para los clientes de ATEX4 en la aplicación ATEX5. *DataPower* recibe la petición en formato ATEX4 y la transforma para hacerla compatible con ATEX5. Y cuando el *backend* devuelve el resultado, vuelve a transformar la respuesta de ATEX5 en una compatible con ATEX4. Este sistema está actualmente funcionando en producción para más de 100.000 peticiones que se reciben diariamente.

### 3.2.1 Non-XML

Diseñado para entradas cuya estructura no se corresponde con ninguna de las posteriores pero que necesita procesado por parte de *DataPower*. DP puede realizar labores de verificación y autenticación, así como convertir los parámetros de la petición en formato XML (por ejemplo, en caso de una petición HTTP, convertirá los datos aportados en el campo PostData de esa petición).

Este tipo de procesamiento es el utilizado para el tráfico WEB de las aplicaciones.

### 3.2.2 XML

*DataPower* permite realizar validación de esquemas XML, así como verificación de la estructura XML para evitar cierto tipo de ataques.

### 3.2.3 SOAP

Permite realizar validación de esquemas y verificación de la estructura SOAP (incluye las validaciones de XML y algunas más para verificar que es un mensaje SOAP válido).

Es el tipo utilizado para los *proxys* de servicios WEB (WS).

### 3.2.4 JSON

Formato de datos serializados de Java. *DataPower* es capaz de transformar las peticiones con formato JSON en formato XML si así se requiere.

Este tipo de dato es el utilizado por el proyecto TRAMO. *DataPower* realiza la transformación de JSON a SOAP, para llamar a los WS de las aplicaciones, y vuelve a transformar la respuesta SOAP en JSON, para ser consumida por la *tablet*.

### 3.2.5 Otros

Es posible enviar cualquier otro tipo de mensaje, configurando *DataPower* como *passthrough*, de este modo DP no realizará ninguna acción sobre el mensaje, por lo que será el *backend* (WAS) quien procese la petición tal como fue enviada por el usuario o aplicación.

## 3.3 Operaciones criptográficas

### 3.3.1 Firma de la DGT hacia terceros (sello electrónico)

En ocasiones, es necesario enviar mensajes SOAP a aplicaciones externas a los servicios centrales de la DGT, por lo que conviene que esas peticiones sean firmadas por la propia DGT para que el receptor pueda verificar la autenticidad de la petición.

En dichos casos, conviene delegar en *DataPower* la firma del mensaje, tanto por velocidad (cabe recordar que *DataPower* trabaja de forma nativa con procesos criptográficos) como porque *DataPower* dispone de un sistema cifrado de almacenamiento de certificados, evitando el almacenamiento de datos sensibles en sistemas de ficheros poco seguros. Además, se obtiene el beneficio de la centralización de firma, que simplifica enormemente el mantenimiento de los certificados cuando sea necesario actualizarlos.

### 3.3.2 Firma de la DGT hacia aplicaciones internas

Es posible configurar *DataPower* para firmar la respuesta de una llamada a un servicio web, de esta manera, la aplicación que originó la comunicación obtendrá la respuesta de la aplicación final,

firmada por la DGT.

*DataPower* verificará que los datos de los campos del mensaje que firma coinciden con el descriptor que se haya desplegado, si no fuese así, devolvería un *soapfault* en lugar del mensaje firmado.

### 3.3.3 Validación de firma

*DataPower* valida la firma y el certificado para cualquier aplicación que requiera de estos mecanismos de seguridad. Si la petición no supera esta validación, será rechazada automáticamente y no seguirá procesándose, indicando *DataPower* la razón por la que la petición fue rechazada.

### 3.3.4 Verificación de firma

Una vez validada la firma, se ha de confirmar la autenticidad del firmante, para ello, debido a requisitos legales, *DataPower* se vale de los servicios ofrecidos por @Firma, es decir, la verificación no se hace en un entorno local.

Si el certificado fue emitido por la CA de la DGT y la comprobación mediante @Firma es incorrecta, se buscará el certificado contra el LDAP de la DGT, en caso de hallarse, se validará la petición. Este procedimiento es necesario para validar certificados antiguos de la CA de la DGT, pues estos no están incluidos en @Firma.

## 3.4 Protección ofrecida

*DataPower* dispone de una serie de funcionalidades, las cuales aumentan considerablemente la seguridad de las comunicaciones, tanto a nivel de mensaje (mediante el uso de certificados) como a nivel de aplicación (previniendo un posible exceso de carga para la aplicación que podría provocar la denegación de servicio de esta).

Cabe destacar que todos los ataques pueden estar provocados, no sólo por usuarios malintencionados, sino que es posible que se produzca algún tipo de ataque debido a la mala programación de alguna aplicación que produzca el funcionamiento indebido de la misma, por lo que es necesario proteger también los servicios internos, aunque sólo puedan ser llamados desde las

propias oficinas centrales de la Dirección General de Tráfico.

### 3.4.1 Cifrado/firma de mensajes

La protección derivada del uso de certificados para la autenticación, tal como se ha mostrado en anteriores apartados, es necesaria no sólo por cuestiones legales, si no que constituyen el método básico (aunque no por ello deficiente) de seguridad en cualquier comunicación que pretenda ser segura.

Para cifrar los mensajes, es necesario del uso de un protocolo que permita esta funcionalidad. HTTPS con certificados SSL es el estándar en la DGT en este tipo de comunicación.

### 3.4.2 Validación de esquema

Cada vez que una petición es procesada por *DataPower*, este comprueba que dicha petición se ajusta al esquema que se le ha indicado, de no ser así, se descarta.

El esquema XML para la verificación, debe ser proporcionado por la aplicación.

### 3.4.3 Protección contra SQL injection

Para evitar el acceso de manera no autorizada a las bases de datos del backend o incluso la ejecución de código malintencionado, DataPower contiene filtros automáticos para evitar los ataques de tipo *SQL injection*.

En caso de detectarse algún caso de inyección SQL, DataPower descartará automáticamente el mensaje, enviando un mensaje de error al cliente y evitando que el backend (servidor de aplicaciones) reciba dato alguno de esta transacción maliciosa.

La protección contra estos ataques no es automática y ha de ser configurada por el equipo técnico correspondiente previa solicitación por parte de la aplicación.

### 3.4.4 Protección ante ataques XDoS

Un ataque XDoS consiste en un intento de denegación del servicio de una plataforma a través del contenido de un mensaje XML, el cual está formado de tal manera que consuma el máximo tiempo y

porcentaje de CPU en la plataforma destino posible.

Para proteger los servicios de la DGT de este tipo de ataques, se establecen limitaciones para todas las aplicaciones en los varios parámetros de la petición. Entre otros, no se parsearán peticiones XML que excedan los siguientes límites:

- Tengan un tamaño superior a 4194304 bytes (4 megas).
- Profundidad de 512 elementos.
- Contengan un tag con más de 128 atributos.

Un nodo no podrá contener más de 33554432 bytes (32 megas) de información.

### 3.4.5 Protección ante ataques MMXDoS

Estos ataques consisten en el envío masivo de peticiones (desde una máquina o varios) para provocar la denegación de servicio debido a la falta de recursos de la máquina objetivo. Otra variante resulta del *secuestro* de recursos, los cuales el atacante tardará lo máximo posible en liberar.

Para evitar ataques de este tipo, es necesario limitar tanto las peticiones que se pueden realizar por máquina (IP) en un período de tiempo, como el tiempo de ejecución de dichas peticiones, ofreciendo DataPower soporte para ambas limitaciones.

Los límites máximos establecidos para las aplicaciones en la DGT son:

El procesamiento de una petición no podrá tardar más de 120 segundos en el DataPower de intranet o de 150 segundos en el de Internet.

- Un host podrá realizar 10 peticiones por segundo.
- El servicio soportará no más de 800* peticiones por segundo.

** Este parámetro dependerá de cada aplicación, se muestra el límite máximo admitido en la DGT (ninguna aplicación puede superar este límite).*

### 3.4.6 Protección ante ataques de fuerza bruta

Dada la peligrosidad de este tipo de ataques (un usuario malintencionado que lograse un ataque

exitoso, podría obtener acceso a varios servicios de la DGT), se restringe la comprobación de credenciales a 10 intentos por segundo. Este límite es el mismo para autenticaciones por usuario y contraseña como para autenticaciones mediante certificado, aunque es posible definirlo por separado si fuese necesario.

# 3.5 Otros servicios

## 3.5.1 SLA (nivel de servicio)

Para cada aplicación, es necesario definir un nivel de servicio para garantizar el mismo. Es importante destacar que sin este parámetro, exponemos a la aplicación a posibles ataques de denegación de servicios y vulnerable a exceso de mensajes causado por problemas en la aplicación o uso indebido (voluntario o no).

El SLM limita el número de peticiones por segundo y por hora, así como el tiempo máximo de ejecución de un único mensaje, previniendo así que el backend consuma demasiados recursos debido a mensajes malintencionados o erróneos. Esta limitación se establece para cada IP que utilice el servicio de manera global para la aplicación.

Cada aplicación debe concretar con el equipo de *DataPower* el SLM (cantidad de mensajes por segundo y por hora) que necesitará procesar de acuerdo a sus previsiones de volumen de negocio.

## 3.5.2 Single Sign-On

*DataPower* participa activamente en la solución de Single Sing-On adoptada en la DGT; para ello, se interpone entre el cliente y las aplicaciones, redirigiendo al usuario no autenticado a la página de Single Sign-On correspondiente.

Una vez recuperadas las credenciales y autenticado el usuario, *DataPower* devolverá el control a la aplicación solicitada por el usuario y el mismo podrá realizar todas las consultas que estime oportunas siempre y cuando conserve el *token* correspondiente y la sesión no haya caducado.

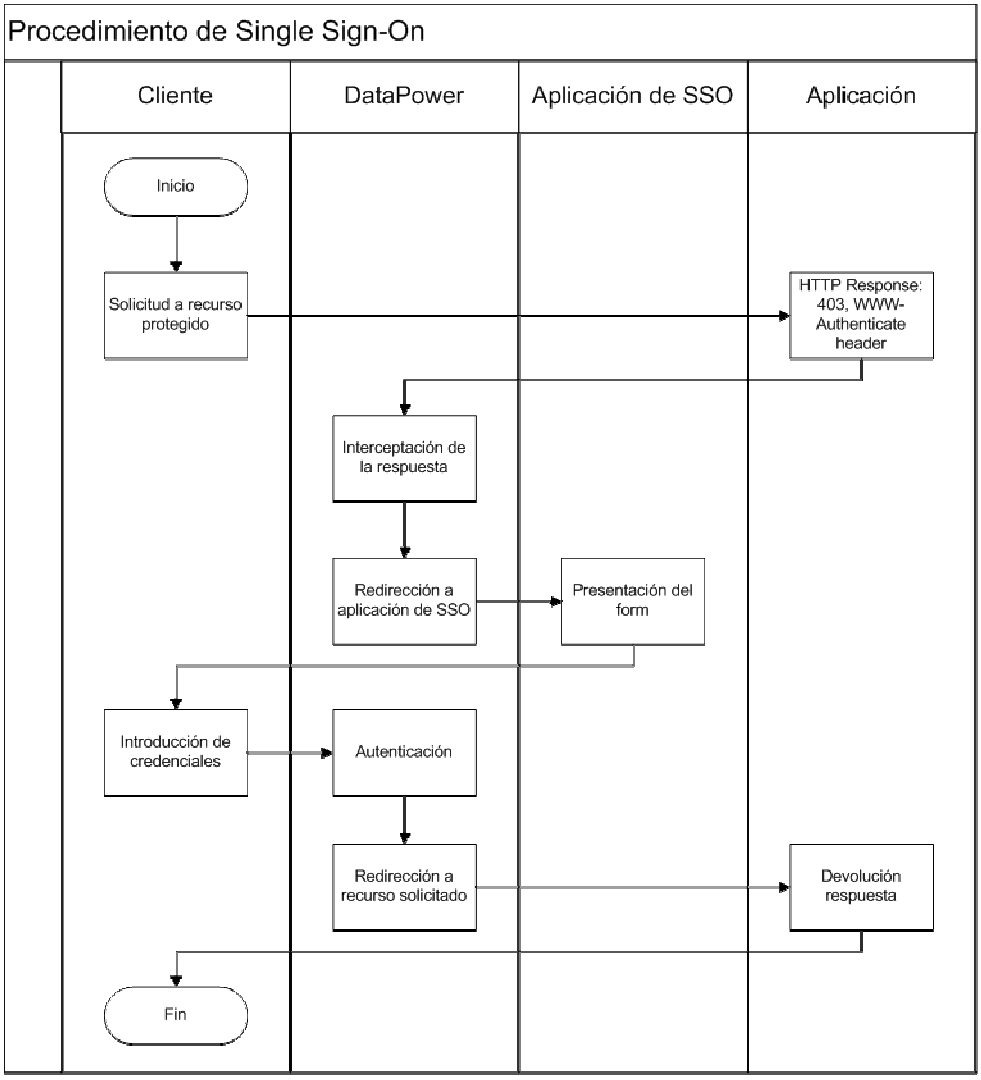


**Ilustración 2: Procedimiento de *single sign-on***

# 4 Integración de aplicaciones con *DataPower*

Para los equipos de desarrollo existe un entorno en *DataPower* que permite integrar las nuevas aplicaciones con el bus y su entorno (@Firma, LDAP, etc). Actualmente se soportan varios métodos de autenticación: *usuario y contraseña* para intranet y *certificado digital* o *Cl@ve* (solo WEB) para Internet. A efectos de este capítulo se parte de la base de que el equipo de desarrollo tiene desplegada su aplicación o servicio WEB (WS) en una maqueta de WAS, que ya viene preconfigurada para operar en DGT.

Los puertos donde debe escuchar el frontal WEB (IHS) del WAS son los siguientes:

90: Aplicaciones web en el dominio *trafico.es* (autenticación por *usuario y contraseña*).

91: Aplicaciones web en el dominio *traficocert.es* (autenticación por *certificado digital*).

93: Recursos REST.

94: Servicios WEB (WS) SOAP.

La norma indica que las raíces de contexto de las URIs de publicación deben comenzar por **WEB_** para aplicaciones web y **WS_** para servicios SOAP, como por ejemplo:

- /WS_ATEX5/services/ATEX
- /WEB_COPACI3/certificado/verSaldoPuntosCert.faces

Las URIs y métodos de los recursos REST deben cumplir con los estándares de Arquitectura DGT (dep.arquitectura@dgt.es). Por favor, póngase en contacto con este departamento para que le facilite la guía que se ha elaborado al respecto.

## 4.1 Integración de aplicaciones WEB en el entorno de desarrollo

**NOTA**: Para el entorno de desarrollo *y solo para este entorno y las aplicaciones WEB* es necesario realizar el alta de varios nombres en el DNS de DGT (dominios *trafico.es* y/o *traficocert.es*). Esto es debido a que los servidores donde están alojadas las aplicaciones están distribuidos en diferentes IPs de la red 10.50.105.0/24. Como se verá más adelante, para los servicios WEB (WS) no es necesario pedir ningún nuevo DNS, ya que el *bus* puede dirigir este tráfico de manera personalizada.

Para integrar una aplicación WEB en este entorno es necesario lo siguiente:

- El virtual host del IHS, que hace de frontal web para el WAS, donde está desplegada la aplicación debe escuchar en el puerto 90 si pertenece al dominio *trafico.es* o en el 91 si pertenece al dominio *traficocert.es*.
- Comprobar la conectividad entre el *DataPower* y el servidor de desarrollo, en caso de que no exista solicitar una regla de *firewall* para habilitar la conexión entre el *DataPower* de

desarrollo (IP de salida 10.50.104.4) y el servidor de desarrollo.

- Dar de alta un nombre de *DOMINIO* que punte a la IP del *DataPower* de desarrollo en función del tipo de autenticación requerida. A este nombre de dominio se le asignará una IP dependiendo de si la validación se realiza mediante u*suario y contraseña* o mediante *certificado digital* o *Cl@ve*.
  - Actualmente el *DataPower* desarrollo escucha en tres IPs:
    - Usuario y contraseña (intranet): 10.50.104.5 (trafico.es)
    - Certificado digital (intranet): 10.50.104.10 (traficocert.es)
      - El dominio *traficocert.es* se utiliza para simular los accesos desde Internet, pero no está asociado a ninguna IP pública y por tanto solo se puede acceder desde la intranet de DGT.
    - Cl@ve (Internet): 10.50.104.17 (trafico.es)
      - El acceso por Cl@ve, aunque se utilice el método de certificado digital, el certificado nunca llega a la DGT y por tanto no es posible extraer los datos del mismo (tales como SFIR_RESPONSABLE).
- Crear otro DNS en el dominio apropiado (*trafico.es* o *traficocert.es*) con nombre *in.DOMINIO* que apunte a la IP del servidor donde está desplegada la aplicación.

Ejemplos de nombres de DNS de los dos puntos anteriores:

| **Nombre** | **Dominio** | **IP *DataPower* / IP IHS-WAS** | **Tipo de autenticación** |
|---|---|---|---|
| `eitv-des2` | `trafico.es` | `10.50.104.5` | Usuario y contraseña |
| `in.eitv-des2` | `trafico.es` | `10.50.105.58` | |
| `exam3-des` | `trafico.es` | `10.50.104.5` | Usuario y contraseña |
| `in.exam3-des` | `trafico.es` | `10.50.105.72` | |
| `eitv-des2` | `traficocert.es` | `10.50.104.10` | Certificado digital |
| `in.eitv-des2` | `traficocert.es` | `10.50.105.58` | |
| `exam3-des` | `traficocert.es` | `10.50.104.10` | Certificado digital |
| `in.exam3-des` | `traficocert.es` | `10.50.105.72` | |
| `eitv-clave-des` | `trafico.es` | `10.50.104.17` | Cl@ve |
| `in.eitv-clave-des` | `trafico.es` | `10.50.105.58` | |
| `exam3-clave-des` | `trafico.es` | `10.50.104.17` | Cl@ve |

| | | | |
|---|---|---|---|
| in.exam3-clave-des | trafico.es | 10.50.105.72 | |

**Tabla 1: Ejemplo de nombres DNS para aplicaciones WEB**

- En caso de **autenticación por usuario y contraseña**:
  - Si se utiliza un usuario nuevo, es necesario enviar un correo a sistemas solicitando que se de alta el mismo en el LDAP.
- En caso de **autenticación por certificado**:
  - *DataPower* asignará siempre la credencial de usuario técnico "cn=UsuarioTecnico,ou=Usuarios Genéricos,o=dgt.es" *si no encuentra el identificador del certificado devuelto por @Firma en el LDAP de la DGT*. Esta circunstancia es muy útil para autenticar al ciudadano, ya que si el certificado es válido, dicha credencial es válida para autorizar la aplicación con el sujeto especial "*Todos los autenticados en los reinos de confianza*" en la definición de los roles.

Este usuario técnico, como es lógico, no tiene ningún ROL asignado.

- En caso de **autenticación por Cl@ve**:
  - Para acceder por Cl@ve es necesario dar de alta la aplicación en una base de datos, ubicada en el DSS, que proporciona los datos necesarios al *bus* para poder efectuar correctamente el acceso. Por favor, póngase en contacto con el departamento de Arquitectura de la DGT (dep.arquitectura@dgt.es) para que le indique los pasos a seguir.
- **ROLES** de la aplicación (*necesario en todos los casos*):
  - Si el rol o roles son nuevos, hay que solicitar su creación en el LDAP mediante *ticket* a sistemas operativos.
  - Si el acceso a la aplicación es mediante certificado digital o Cl@ve, será necesario añadir los roles a los usuarios personales correspondientes de los NIFs de los certificados en el LDAP, o bien utilizar el sujeto especial "*Todos los autenticados en los reinos de confianza*" si la aplicación está destinada al ciudadano. O también una mezcla de ambos métodos.
  - Si el acceso es por usuario y contraseña será necesario asignar a cada usuario de LDAP

autorizado utilizar la aplicación su rol o roles correspondientes definidos en el WAS.

### 4.1.1 Ejemplo de integración de una aplicación WEB

En este ejemplo de integración la aplicación WEB utiliza **autenticación por certificado y roles de usuario**:

Un equipo de desarrollo tiene desplegada su aplicación WEB de gestión de vehículos en *http://10.50.105.123:90/WEB_APLI* y se requiere que el acceso sea por Internet mediante autenticación por certificado digital. Todos los usuarios accederán con el rol *CIUDADANO*, además de otros específicos para la gestión. Para invocar esta aplicación a través de *DataPower* el equipo de desarrollo crea varios *tickets* a sistemas solicitando:

- Alta en el DNS del *host miaplicacion-des en el dominio traficocert.es* apuntando a la IP de *DataPower* de acceso por Internet (10.50.104.10).
- Alta en el DNS del *host in.miaplicacion-des en el dominio traficocert.es* apuntando a la IP del WAS donde está hospedada la aplicación (10.50.105.123).
- Alta de los siguientes roles en el LDAP de preproducción:
  - cn=APLI Grupo Supervisor, cn=APLI,cn= Aplicaciones de Vehiculos, ou=Groups, o=dgt.es
  - cn=APLI Grupo Funcionario, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es
  - cn=APLI Test, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es
  - Ejemplo de asociación de ROLES en el servidor de aplicación WAS:

| **Rol** | **Sujetos especiales** | **Grupos correlacionados** |
|---|---|---|
| Supervisor | | cn=APLI Grupo Supervisor, cn=APLI,cn= Aplicaciones de Vehiculos, ou=Groups, o=dgt.es |
| Funcionario | | cn=APLI Grupo Funcionario, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es |
| Test | | cn=APLI Test, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es |
| Ciudadano | Todos los autenticados en los | |

| | | |
|---|---|---|
| | reinos de confianza | |

**Tabla 2: Ejemplo de asociación de roles en el servidor WAS**

- Asignación de los siguientes roles para los usuarios indicados:
  - S0000000J: cn=APLI Test, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es
  - 12345678Z: cn=APLI Grupo Supervisor, cn=APLI,cn= Aplicaciones de Vehiculos, ou=Groups, o=dgt.es

A partir de ahora, cada vez que se accede a *https://miaplicacion-des.trafico.es:443/WEB_ APLI* la llamada pasa por *DataPower* y una vez autenticada la petición con certificado, se reenvía al servidor de aplicaciones *http://in.miaplicacion-des.trafico.es:91/WEB_APLI* con el correspondiente *token* LTPA para poder autorizar el acceso en el WAS según el ROL y las *cookies* con la identidad del usuario para su consumo a través del *módulo de login* por parte de la aplicación.

## 4.2 Integración de un WS en desarrollo

Para integrar un WS en el entorno de desarrollo de *DataPower* el procedimiento es similar al de una aplicación WEB, aunque en este caso no habrá que dar de alta nuevos DNSs. Es importante recordar se sólo se permite la autenticación por *usuario y contraseña* en intranet y por *certificado digital* en Internet y/o Red SARA.

Para integrar un WS en *DataPower* hay que aportar los siguientes datos:

- WSDL del servicio y ficheros de esquema xsd. El WSDL debe apuntar a los xsd con rutas relativas, no absolutas, indicando únicamente el nombre del fichero, por ejemplo:

```
<xsd:schema>
  <xsd:import namespace="http:/xxx.xxx.trafico.es/" schemaLocation="Miesquema.xsd"/>
</xsd:schema>
```

- *Endpoint* o URL donde está desplegada la aplicación, por ejemplo: http://10.50.105.123:94/WS_APLI.

- Descripción de la funcionalidad del WS (ver categorías, más abajo)

La descripción del WS es el apartado más importante para una correcta integración con *DataPower*, ya que dependiendo de esta, se publicará en un *proxy* o en otro. Los servicios web suelen pertenecer a una de las siguientes tres categorías:

- Acceso desde Internet mediante *certificado digital*.
- Acceso desde intranet mediante *usuario/contraseña* (para ser consumido desde la intranet de DGT) y/o *certificado digital* (para ser consumido desde Red SARA)
- Acceso desde intranet e Internet: Es la suma de los dos casos anteriores, realmente son dos despliegues, se cargará varias veces el mismo WSDL en diferentes *DataPower*.

Estos tres casos cubren el 90% de los despliegues, sin embargo existen algunos más especiales:

- Servicios que invocan a la AEAT.
- Servicios que llaman directamente a @Firma.
- Servicios de llamadas a bancos. Ejemplo: Servicio de EEFF para llamadas al banco Santander.
- Servicios que invocan a la plataforma de *Intermedianción*. Ejemplo: servicios de FVER
- Servicios de llamada al exterior.

Por otra parte, el alta de usuarios y roles se realiza de la misma forma que el caso de una aplicación WEB.

### 4.2.1 Ejemplo de integración de un WS en desarrollo

En este ejemplo de integración, se publicará un WS con autenticación por certificado y se limitará su consumo a tres clientes.

El servicio web del equipo de desarrollo está publicado en el servidor http://10.50.105.123:94/WS_APLI

Dado que en la publicación de un servicio web en el bus se puede definir de manera individual el *backend*, tan solo hay que crear un *ticket* a sistemas con la siguiente información. Es decir, no será

necesario crear nuevos nombres en el DNS:

- Fichero WSDL del servicio
- Tipo de autenticación requerida (*certificado digital* y/o *usuario y contraseña*) y entorno (Internet y/o intranet)
- Dirección donde está ubicado el servicio en el WAS de desarrollo.

Una vez publicado el servicio, será accesible a través de la dirección: http://desapl-p3.trafico.es:[PUERTO según tipo de autenticación]/WS_APLI

- Para proteger el servicio web se generarán los siguientes roles en el LDAP de preproducción, mediante nuevo *ticket* a sistemas.

| **Rol** | **Sujetos especiales** | **Grupos correlacionados** |
|---|---|---|
| Consulta | | cn=APLI Consulta, cn=APLI,cn= Aplicaciones de Vehiculos, ou=Groups, o=dgt.es |
| Test | | cn=APLI Test, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es |

**Tabla 3: Ejemplo de roles de aplicación**

- Por último, se creará una nueva petición a sistemas para añadir el rol "cn=APLI Consulta, cn=APLI,cn= Aplicaciones de Vehiculos, ou=Groups, o=dgt.es" a los tres usuarios que tienen permiso para ejecutar la aplicación y también se incluirá el NIF del usuario de test en el rol "cn=APLI Test, cn=APLI, cn=Aplicaciones de Vehiculos, ou=Groups, o=dgt.es" para ejecutar las pruebas internas de la aplicación.

Cuando un cliente se autentica con certificado, el *bus* valida el mismo y asigna el NIF que incluye dentro como credencial para realizar la autorización. Este credencial se busca en el LDAP para conocer los roles que deben aplicarse en la fase de autorización por parte del WAS y si no existe en el LDAP, se asignará la credencial (sin ROLES) *usuarioTecnico*. En este caso, el usuario técnico no tendría autorización para llamar a la aplicación, ya que como hemos dicho, se trata de un usuario sin roles asociados.

# 5 Otras consideraciones

## 5.1 Dudas y contacto con el equipo de *DataPower*

Para resolver cualquier tipo de duda con respecto a las posibilidades que ofrece *DataPower* para la integración de las aplicaciones en la DGT, puede dirigirse al equipo de *Arquitectura DataPower*.

En cualquier caso, si se requiere el uso de una arquitectura distinta a la estándar, aún cuando dicha arquitectura o funcionalidad esté especificada en el *redbook* de *DataPower*, habrá que consultar la propuesta con el equipo de arquitectura de *DataPower* para comprobar si tanto la arquitectura de la DGT como las licencias del producto permiten la utilización de la funcionalidad que se pretende utilizar, proponiendo este equipo alternativas que satisfagan los requisitos de la aplicación si fuese necesario.

Para realizar peticiones de servicio o tratar incidencias, puede abrir un ticket mediante los mecanismos que provee DGT.