

Spring BlazeDS Integration Reference Guide

Jeremy Grelle

Version 1.0.0.M2

Copies of this document may be made for your own use and for distribution to others, provided that you do not charge any fee for such copies and further provided that each copy contains this Copyright Notice, whether distributed in print or electronically.

Published March 2008

Table of Contents

1. Spring BlazeDS Integration Overview	1
1.1. Background	1
1.2. What Spring BlazeDS Integration requires to run	1
1.3. Where to get support	1
2. Configuring the BlazeDS MessageBroker with Spring	2
2.1. Introduction	2
2.2. Configuring the Spring DispatcherServlet	2
2.3. Configuring the MessageBroker in Spring	2
2.4. Mapping Requests to the MessageBroker	4
2.5. Advanced MessageBroker Customization	5
3. Exporting Spring Beans for Flex Remoting	7
3.1. Introduction	7
3.2. Using the remote-service Tag	7
3.3. Configuring the Remoting Service	8
3.4. Using Exported Destinations in the Flex Client	9
4. Securing BlazeDS Destinations with Spring Security	10
4.1. Introduction	10
4.2. Configuring the Spring Security Integration	10
Security Exception Translation	11
secured Configuration Attributes	11
4.3. Configuring Endpoint and Destination Security	12
Securing Specific BlazeDS Channels	12
Securing BlazeDS Channels by Endpoint URL Path	12
Securing Exported Spring Services	13
5. Integration with the BlazeDS Message Service	15
5.1. Introduction	15

1. Spring BlazeDS Integration Overview

1.1. Background

Spring has always aimed to be agnostic to the client technologies being used to access its core services, intentionally leaving options open and letting the community drive the demand for any new first-class integration solutions to be added to the Spring project portfolio. Spring BlazeDS Integration is an answer to the community demand for a top-level solution for building Spring-powered Rich Internet Applications using Adobe Flex for the client-side technology.

[BlazeDS](#) is an open source project from Adobe that provides the remoting and messaging foundation for connecting a Flex-based front-end to Java back-end services. Though it has previously been possible to use BlazeDS to connect to Spring-managed services, it has not been in a way that feels "natural" to a Spring developer, requiring the extra burden of having to maintain a separate BlazeDS xml configuration. Spring BlazeDS Integration turns the tables by making the BlazeDS MessageBroker a Spring-managed object, opening up the pathways to a more extensive integration that follows "the Spring way".

1.2. What Spring BlazeDS Integration requires to run

Java 5 or higher

Spring 2.5 or higher

Adobe BlazeDS 3.2 or higher

1.3. Where to get support

Professional from-the-source support on Spring BlazeDS Integration is available from [SpringSource](#), the company behind Spring.

2. Configuring the BlazeDS MessageBroker with Spring

2.1. Introduction

The central component that must be configured to use Spring BlazeDS Integration is the MessageBroker. HTTP messages from the Flex client will be routed through the Spring DispatcherServlet to the Spring-managed MessageBroker. There is no need to configure the BlazeDS MessageBrokerServlet when using the Spring-managed MessageBroker.

2.2. Configuring the Spring DispatcherServlet

The DispatcherServlet must be configured as normal in web.xml to bootstrap a Spring WebApplicationContext. For example:

```
<!-- The front controller of this Spring Web application, responsible for handling all application requests -->
<servlet>
  <servlet-name>Spring MVC Dispatcher Servlet</servlet-name>
  <servlet-class>org.springframework.web.servlet.DispatcherServlet</servlet-class>
  <init-param>
    <param-name>contextConfigLocation</param-name>
    <param-value>/WEB-INF/config/web-application-config.xml</param-value>
  </init-param>
  <load-on-startup>1</load-on-startup>
</servlet>
```

2.3. Configuring the MessageBroker in Spring

A simplified Spring XML config namespace is provided for configuring the MessageBroker in your WebApplicationContext. To use the namespace support you must add the schema location in your Spring XML config files. A typical config will look something like the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:flex="http://www.springframework.org/schema/flex"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
         http://www.springframework.org/schema/beans
         http://www.springframework.org/schema/beans/spring-beans-2.5.xsd
         http://www.springframework.org/schema/flex
         http://www.springframework.org/schema/flex/spring-flex-1.0.xsd">
  ...
</beans>
```

This makes the Spring BlazeDS Integration configuration tags available under the `flex` namespace in your configuration files. The above setup will be assumed for the rest of the configuration examples to follow. For the full detail of every attribute and tag available in the config namespace, be sure to refer to the `spring-flex-1.0.xsd` as every element and attribute is fully documented there. Using an XSD-aware XML editor such as the one in Eclipse should bring up the documentation automatically as you type. (Note that until the final xsd is published to the above web address, you would need to manually add the XSD to your XML catalog in Eclipse for auto-completion to work correctly.)

At a minimum, the `MessageBrokerFactoryBean` must be configured as a bean in your Spring `WebApplicationContext` in order to bootstrap the `MessageBroker`, along with a `MessageBrokerHandlerAdapter` and an appropriate `HandlerMapping` (usually a `SimpleUrlHandlerMapping`) to route incoming requests to the Spring-managed `MessageBroker`.

These beans will be registered automatically by using the provided `message-broker` tag in your bean definition file. For example, in its simplest form:

```
<flex:message-broker/>
```

This will set up the `MessageBroker` and necessary supporting infrastructure using sensible defaults. The defaults can be overridden using the provided attributes of the `message-broker` tag and its associated child elements. For example, the default location of the BlazeDS XML configuration file (`/WEB-INF/flex/services-config.xml`) can be overridden using the `services-config-path` attribute. The `MessageBrokerFactoryBean` uses Spring's `ResourceLoader` abstraction, so that typical Spring resource paths may be used. For example, to load the configuration from the application's classpath:

```
<flex:message-broker services-config-path="classpath*:services-config.xml"
```

The equivalent `MessageBrokerFactoryBean` definition using vanilla Spring configuration would be:

```
<!-- Bootstraps and exposes the BlazeDS MessageBroker -->  
<bean id="_messageBroker" class="org.springframework.flex.messaging.MessageBrokerFactoryBean" >  
  <property name="servicesConfigPath" value="classpath*:services-config.xml" />  
</bean>
```

Note especially that with the `message-broker` tag, it is not necessary to assign a custom id to the `MessageBroker`, and it is in fact discouraged so that you won't have to continually reference it later. The only reason you would ever need to provide a custom id is if you were bootstrapping more than one `MessageBroker` in the same `WebApplicationContext`.

2.4. Mapping Requests to the MessageBroker

To properly route incoming requests to the Spring-managed MessageBroker, request mapping must be configured in three places:

1. DispatcherServlet mapping in web.xml
2. HandlerMapping in the Spring WebApplicationContext
3. Channel definitions in the BlazeDS services-config.xml

The simplest request mapping scenario is when the Flex front-end is the only client type for the application. In this case you can just map /messagebroker as the top-level path for requests. The mapping in web.xml would be:

```
<!-- Map all /messagebroker requests to the DispatcherServlet for handling -->
<servlet-mapping>
  <servlet-name>Spring MVC Dispatcher Servlet</servlet-name>
  <url-pattern>/messagebroker/*</url-pattern>
</servlet-mapping>
```

When using the message-broker config tag, a SimpleUrlHandlerMapping is installed that by default maps all incoming DispatcherServlet requests to the Spring-managed MessageBroker using a /*path pattern. The default mapping can be overridden by providing one or more mapping child elements. If you want to provide your own HandlerMapping bean configuration, you can disable the default using the disable-default-mapping attribute of the message-broker tag.

Then the SimpleUrlHandlerMapping in the Spring WebApplicationContext maps all requests to the Spring-managed MessageBroker via the MessageBrokerHandlerAdapter. The default setup installed by the message-broker config tag is equivalent to the following bean definitions:

```
<!-- Maps request paths at /* to the BlazeDS MessageBroker -->
<bean class="org.springframework.web.servlet.handler.SimpleUrlHandlerMapping">
  <property name="mappings">
    <value>
      /*=_messageBroker
    </value>
  </property>
</bean>

<!-- Dispatches requests mapped to a MessageBroker -->
<bean class="org.springframework.flex.messaging.servlet.MessageBrokerHandlerAdapter"/>
```

Channel definitions in the BlazeDS services-config.xml must correspond to the chosen mapping. For example, to set up a typical AMF channel in BlazeDS that matches the above mapping strategy:

```
<channel-definition id="my-amf" class="mx.messaging.channels.AMFChannel">
  <endpoint url="http://{server.name}:{server.port}/{context.root}/messagebroker/amf" class="flex.messaging.e
```

```

<properties>
  <polling-enabled>>false</polling-enabled>
</properties>
</channel-definition>

```

See the [BlazeDS documentation](#) for more information on configuring communication channels in `services-config.xml`.

It could often be the case that your application needs to serve more than just Flex-based clients. For example, you may be constructing a RESTful architecture that is meant to serve multiple client-types. You could potentially even be consuming RESTful endpoints using the Flex `HTTPService` component. In this case, you will want to choose a more flexible mapping strategy, such as mapping `/spring/*` to the `DispatcherServlet`, mapping `/messagebroker/*` to the Spring-managed `MessageBroker`, and modifying any BlazeDS channel definitions accordingly. You would override the default mapping strategy of the `message-broker` tag as follows:

```

<flex:message-broker>
  <flex:mapping pattern="/messagebroker/*" />
</flex:message-broker>

```

and you would have to account for the `/spring/*` mapping in your BlazeDS channel definitions. For example:

```

<channel-definition id="my-amf" class="mx.messaging.channels.AMFChannel">
  <endpoint url="http://{server.name}:{server.port}/{context.root}/spring/messagebroker/amf" class="flex.mess
  <properties>
    <polling-enabled>>false</polling-enabled>
  </properties>
</channel-definition>

```

2.5. Advanced MessageBroker Customization

The initialization of the `MessageBroker` by the `MessageBrokerFactoryBean` logically consists of two phases:

1. Parsing the BlazeDS XML configuration files and applying their settings to a newly created `MessageBroker`
2. Starting the `MessageBroker` and its services

A special `MessageBrokerConfigProcessor` callback interface is provided that allows custom processing to be done on the newly created `MessageBroker` after each phase, before it is made available for request processing. This interface is used internally by Spring BlazeDS Integration, but is also available for general use in advanced programmatic introspection and customization of the `MessageBroker`. A custom `MessageBrokerConfigProcessor` can be configured as a Spring

bean and then registered with the `MessageBrokerFactoryBean` via the `config-processor` tag. For example, given a trivial implementation to log some additional info about the `MessageBroker`:

```
package com.example;

import org.springframework.flex.messaging.config.MessageBrokerConfigProcessor;

import flex.messaging.MessageBroker;
import flex.messaging.services.RemotingService;

public class MyDestinationCountingConfigProcessor implements MessageBrokerConfigProcessor {

    public MessageBroker processAfterStartup(MessageBroker broker) {
        RemotingService remotingService =
            (RemotingService) broker.getServiceByType(RemotingService.class.getName());
        if (remotingService.isStarted()) {
            System.out.println("The Remoting Service has been started with "
                +remotingService.getDestinations().size()+" Destinations.");
        }
        return broker;
    }

    public MessageBroker processBeforeStartup(MessageBroker broker) {
        return broker;
    }
}
```

This class could be configured and registered with the `MessageBroker` as follows:

```
<flex:message-broker>
  <flex:config-processor ref="myConfigProcessor" />
</flex:message-broker>

<bean id="myConfigProcessor" class="com.example.MyDestinationCountingConfigProcessor" />
```

3. Exporting Spring Beans for Flex Remoting

3.1. Introduction

Using a Spring-managed `MessageBroker` enables Spring beans to be easily exported for direct remoting calls from a Flex client. This approach is quite similar to that taken with other remoting technologies in the core Spring Framework. Remoting is applied to existing Spring-managed beans as an external configuration concern. The `MessageBroker` transparently handles the process of serialization and deserialization between the Flex AMF data format and Java.

3.2. Using the `remote-service` Tag

The `remote-service` configuration tag can be used to export existing Spring-managed services for direct remoting from a Flex client. Given the following Spring bean definition for a `productService` bean:

```
<bean id="productService" class="flex.samples.product.ProductServiceImpl" />
```

and assuming the existence of a Spring-managed `MessageBroker` configured via the `message-broker` tag, the following top-level `remote-service` tag will expose the service for remoting to the Flex client as a remote service destination named `productService`:

```
<!-- Expose the productService bean for BlazeDS remoting -->  
<flex:remote-service ref="productService" />
```

By default, the remote service destination exposed to the Flex client will use bean name of the bean being exported as the service id of the destination, but this may be overridden using the `service-id` attribute on the `remote-service` tag.

An alternate way of using the `remote-service` tag is as a child element of an top-level bean definition. This is even more concise and works well if you don't have a need to keep your domain-layer bean definitions separate from infrastructure concerns such as Flex remoting. (Keep in mind that keeping them separate can lead to easier testability of the core domain layer.) The following achieves the an equivalent result to the previous example:

```
<bean id="productService" class="flex.samples.product.ProductServiceImpl" >  
  <flex:remote-service />  
</bean>
```

The methods that are exposed to be called by the Flex client can be more tightly controlled through use of the `include-methods` and `exclude-methods` attributes of the `remote-service` tag. The BlazeDS channels over which the destination is exposed can also be controlled using the `channels` attribute. (These attributes are available whether using the top-level or the nested version.) A more extensively customized example would look something like:

```
<flex:remote-service ref="productService" include-methods="read, update" exclude-methods="create, delete" channels="my-amf, my-secure-amf" />
```

The `remote-service` tag is transparently configuring a `FlexRemotingServiceExporter` bean instance for each bean being exported. The equivalent full bean syntax without the namespace support would be:

```
<!-- Expose the productService bean for BlazeDS remoting -->
<bean id="product" class="org.springframework.flex.messaging.remoting.FlexRemotingServiceExporter">
  <property name="messageBroker" ref="_messageBroker"/>
  <property name="service" ref="productService"/>
  <property name="serviceId" value="productService"/>
  <property name="includeMethods" value="read, update"/>
  <property name="excludeMethods" value="create, delete"/>
  <property name="channels" value="my-amf, my-secure-amf"/>
</bean>
```

3.3. Configuring the Remoting Service

The BlazeDS `RemotingService` has traditionally been configured by the inclusion of a `remoting-config.xml` file in the BlazeDS XML configuration. When using only Spring-managed remoting destinations, this config file can be left out completely as the inclusion of the `message-broker` tag in your Spring configuration will cause the `RemotingService` to be configured with sensible defaults if none already exists at startup time. The end result is essentially equivalent to including the following minimal `remoting-config.xml` in your BlazeDS configuration:

```
<?xml version="1.0" encoding="UTF-8"?>
<service id="remoting-service"
  class="flex.messaging.services.RemotingService">

  <adapters>
    <adapter-definition id="java-object" class="flex.messaging.services.remoting.adapters.JavaAdapter" default="true" />
  </adapters>

  <default-channels>
    <channel ref="my-amf" />
  </default-channels>

</service>
```

Note that this assumes that there is already an equivalent application-wide `default-channels` configuration. If no application-wide defaults exist, a best guess will be made by configuring the first

available channel with an `AMFEndpoint` as the default.

If you wish to have more explicit control over the defaults that will be set on the `RemotingService`, you can customize them via the `remoting-service` child element of the `message-broker` tag. For example:

```
<flex:message-broker>
  <flex:remoting-service default-adapter-id="my-default-adapter"
    default-adapter-class="com.example.MyCustomJavaAdapter" default-channels="my-amf, my-secure-amf" />
</flex:message-broker>
```

If you have an existing `remoting-config.xml` for a legacy BlazeDS application, the `FlexRemotingServiceExporter` will be able to work transparently with it, allowing you to gradually migrate to all Spring-managed remoting destinations.

3.4. Using Exported Destinations in the Flex Client

Explicit channel definition is a requirement when using dynamic destinations (meaning any destination that is added programmatically and not defined in the BlazeDS `services-config.xml`, i.e. the destinations created by the `remote-service` tag). See Adobe's documentation [here](http://livedocs.adobe.com/blazeds/1/blazeds_devguide/runtimeconfig_5.html#194376) for more detail: http://livedocs.adobe.com/blazeds/1/blazeds_devguide/runtimeconfig_5.html#194376

The only way you don't have to explicitly define the `ChannelSet` on the client is if

1. you are using explicitly defined destinations in `services-config.xml` (i.e. not dynamic destinations) AND you compile your flex client against that file
2. your destination is using the application-wide default channel AND you compile your flex client against that file

Even if you weren't using dynamically created destinations it is debatable whether it is a good idea to ever compile your client against `services-config.xml`, thus coupling your client to your server configuration. It is often desirable to keep your flex client and your server side code as two distinct modules, but compiling against `services-config.xml` blurs the lines between those modules.

Our recommendation is that it is generally cleaner to keep the client-side configuration of `ChannelSets` explicitly contained within the client module. An excellent way to do this without having to hard-code the URLs in your client code is to use an ActionScript DI framework such as Spring Actionscript (a Spring Extensions project, formerly known as Prana).

If you choose to go the route of compiling your client against `services-config.xml`, note that you can at least keep the URL information out of the client code by using `ServerConfig.getChannel` as described in the referenced BlazeDS documentation.

4. Securing BlazeDS Destinations with Spring Security

4.1. Introduction

Spring Security provides a an extremely flexible alternative to the container-based security support provided out-of-the-box with BlazeDS. Spring BlazeDS Integration provides explicit integration support for incorporating Spring Security smoothly into your Flex/BlazeDS application. Spring Security provides a wealth of different configuration options, but rather than go into the many different combinations here, we'll leave most of that to the Spring Security documentation.

Here is a typical simple Spring Security starting configuration for use in conjunction with the explicit integration features provided by Spring BlazeDS integration:

```
<beans:beans xmlns="http://www.springframework.org/schema/security"
  xmlns:beans="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd
    http://www.springframework.org/schema/security http://www.springframework.org/schema/security/spring-security.xsd"

  <http entry-point-ref="preAuthenticatedEntryPoint" />

  <beans:bean id="preAuthenticatedEntryPoint" class="org.springframework.security.ui.preauth.PreAuthenticatedEntryPoint" />

  <authentication-provider>
    <user-service>
      <user name="jeremy" password="atlanta" authorities="ROLE_USER, ROLE_ADMIN" />
      <user name="keith" password="melbourne" authorities="ROLE_USER" />
    </user-service>
  </authentication-provider>

</beans:beans>
```

We will assume the above configuration is in place for the remainder of the examples in this chapter.

4.2. Configuring the Spring Security Integration

Spring Security integration is enabled through the `secured` child element of the `message-broker` tag. The simplest possible configuration would be:

```
<flex:message-broker>
  <flex:secured />
</flex:message-broker>
```

This enables the basic security features. A special BlazeDS `LoginCommand` implementation is

automatically installed that enables `ChannelSet.login` and `ChannelSet.logout` requests to integrate with Spring Security's Authorization mechanisms. Additionally, the special `LoginCommand` enables Spring Security granted authorities to be referenced in BlazeDS XML security constraints. For example, if we were using a traditional BlazeDS remoting destination defined in `remoting-config.xml`, we could have something like the following:

```
<destination id="productService">
  ...
  <security>
    <security-constraint>
      <auth-method>Custom</auth-method>
      <roles>
        <role>ROLE_USER</role>
      </roles>
    </security-constraint>
  </security>
</destination>
```

As you can see, we are referencing the "ROLE_USER" authority from our simple Spring Security setup. The invocation of this remote destination would cause the provided `LoginCommand` to be invoked to both verify that the user is logged in and to check that they have the appropriate role. Violation of either will result in an exception being thrown by Spring Security.

Security Exception Translation

Another feature that is automatically installed when the `secured` tag is used is automatic exception translation from any thrown `SpringSecurityException` to the proper BlazeDS `SecurityException`. The exceptions are caught and translated at the proper point in the execution chain such that it will result in the proper AMF error message being serialized and sent back to the client.

This is alternative to the normal Spring Security behavior where a filter in the chain catches the exception and sends back a corresponding HTTP status code. The problem with sending back HTTP status codes other than 200 is that this causes the Flex client to throw a generic and rather unhelpful exception, and often the status code can't be determined from the Flex client. Sending back specific AMF error messages instead causes a `FaultEvent` to be thrown client-side that contains the proper security fault code that can then be reasoned on and appropriate action can be taken. This behavior is equivalent to that of the out-of-the-box container-based security mechanisms provided with BlazeDS, so the programming model client-side remains the same.

secured Configuration Attributes

The `secured` tag has several additional attributes that allow further customization.

If you are not using Spring Security's default bean ids for the `AuthenticationManager` or `AccessDecisionManager`, you can specify your custom bean references using the corresponding `authentication-manager` and `access-decision-manager` attributes respectively on the `secured` tag.

The configuration of the provided `LoginCommand` can be further controlled via the `secured` tag. The `invalidate-flex-session` attribute controls whether the current Flex session is invalidated when the `logout()` method is called on the `LoginCommand`, and defaults to "true" if not specified. The `per-client-authentication` attribute turns BlazeDS's per-client authentication mode on when true, and defaults to "false" if not specified. (See the BlazeDS docs for further information on the difference between per-session and per-client authentication.)

NOTE - Though the configuration attribute is present, per-client authentication is not yet supported by Spring BlazeDS Integration in the M2 release. Special integration will be required to store and retrieve a unique `SecurityContext` per `FlexClient` instance. This will be included in future 1.0 milestones.

4.3. Configuring Endpoint and Destination Security

The Spring Security integration allows flexible control over how you secure your application. You can secure BlazeDS endpoints in a manner similar to Spring Security's traditional URL security, and you can secure your Spring services using the many existing object security mechanisms of Spring Security just as if you were writing a traditional web application.

Securing Specific BlazeDS Channels

You can set security constraints on specific BlazeDS channels using the `secured-channel` child element of the `secured` tag. For example:

```
<flex:message-broker>
  <flex:secured>
    <flex:secured-channel channel="my-amf" access="ROLE_USER" />
  </flex:secured>
</flex:message-broker>
```

This results in any request being routed to the "my-amf" channel to require the user to be logged in and to have the "ROLE_USER" authority. If either of those is violated, a `FaultEvent` will be signaled on the client.

Securing BlazeDS Channels by Endpoint URL Path

You can set security constraints on multiple BlazeDS channels at once using the `secured-endpoint-path` child element of the `secured` tag. In this case you specify a URL pattern to be secured instead of a specific channel id. For example:

```
<flex:message-broker>
  <flex:secured>
    <flex:secured-endpoint-path pattern="**/messagebroker/**" access="ROLE_USER" />
  </flex:secured>
</flex:message-broker>
```

This results in any request being routed to any channel whose endpoint URL contains `"/messagebroker/"` in the path to require the user to be logged in and to have the `"ROLE_USER"` authority. If either of those is violated, a `FaultEvent` will be signaled on the client.

Securing Exported Spring Services

Earlier in this chapter you saw an example of using the BlazeDS XML configuration to secure a BlazeDS-managed destination. Since most of the time you will instead be defining destinations by exporting Spring beans using the `remote-service` tag, an alternate approach to securing destinations is needed. This is where Spring Security comes in, as all of its existing authorization mechanisms should "just work" when security integration is enabled using the `secured` tag.

One of the major strengths of Spring Security is the multiple levels of granularity it provides you when securing your Spring services. You can go from securing your entire service layer in one concise statement:

```
<global-method-security>
  <protect-pointcut expression="execution(* com.mycompany.*Service.*(..))" access="ROLE_USER"/>
</global-method-security>
```

to controlling access in a more fine-grained manner at the method layer using XML:

```
<bean id="myService" class="com.mycompany.myapp.MyService">
  <flex:remote-service/>
  <security:intercept-methods>
    <security:protect method="set*" access="ROLE_ADMIN" />
    <security:protect method="get*" access="ROLE_ADMIN,ROLE_USER" />
    <security:protect method="doSomething" access="ROLE_USER" />
  </security:intercept-methods>
</bean>
```

to using a combination of XML and annotations:

```
<security:global-method-security secured-annotations="enabled" jsr250-annotations="enabled"/>
...
<flex:remote-service ref="myBankServiceImpl" />
```

```
public interface BankService {

    @Secured("IS_AUTHENTICATED_ANONYMOUSLY")
    public Account readAccount(Long id);

    @Secured("IS_AUTHENTICATED_ANONYMOUSLY")
    public Account[] findAccounts();
}
```

```
@Secured("ROLE_TELLER")  
public Account post(Account account, double amount);  
}
```

to even more fine-grained ACL-based domain object permissions. For more details on the options available, see the [Spring Security documentation](#).

5. Integration with the BlazeDS Message Service

5.1. Introduction

Coming in Future 1.0 Milestones