RFP 181 RSA Security

Draft

7 Pages

Abstract

Remote Service Admin (RSA) provides an abstraction for the topology manager to import and export services to/from the outside world. The API and the rest of the specification do not define what that outside world is, this is deferred to the topology manager. However, this leaves bundles unaware of who is calling them, which has serious security implications. This RFP investigates the issues around protecting calls through/from a distributed OSGi.

0 Document Information

0.1 License

DISTRIBUTION AND FEEDBACK LICENSE, Version 2.0

The OSGi Alliance hereby grants you a limited copyright license to copy and display this document (the “Distribution”) in any medium without fee or royalty. This Distribution license is exclusively for the purpose of reviewing and providing feedback to the OSGi Alliance. You agree not to modify the Distribution in any way and further agree to not participate in any way in the making of derivative works thereof, other than as a necessary result of reviewing and providing feedback to the Distribution. You also agree to cause this notice, along with the accompanying consent, to be included on all copies (or portions thereof) of the Distribution. The OSGi Alliance also grants you a perpetual, non-exclusive, worldwide, fully paid-up, royalty free, limited license (without the right to sublicense) under any applicable copyrights, to create and/or distribute an implementation of the Distribution that: (i) fully implements the Distribution including all its required interfaces and functionality; (ii) does not modify, subset, superset or otherwise extend the OSGi Name Space, or include any public or protected packages, classes, Java interfaces, fields or methods within the OSGi Name Space other than those required and authorized by the Distribution. An implementation that does not satisfy limitations (i)-(ii) is not considered an implementation of the Distribution, does not receive the benefits of this license, and must not be described as an implementation of the Distribution. "OSGi Name Space" shall mean the public class or interface declarations whose names begin with "org.osgi" or any recognized successors or replacements thereof. The OSGi Alliance expressly reserves all rights not granted pursuant to these limited copyright licenses including termination of the license at will at any time.

EXCEPT FOR THE LIMITED COPYRIGHT LICENSES GRANTED ABOVE, THE OSGi ALLIANCE DOES NOT GRANT, EITHER EXPRESSLY OR IMPLIEDLY, A LICENSE TO ANY INTELLECTUAL PROPERTY IT, OR ANY THIRD PARTIES, OWN OR CONTROL. Title to the copyright in the Distribution will at all times remain with the OSGi Alliance. The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted therein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

THE DISTRIBUTION IS PROVIDED "AS IS," AND THE OSGi ALLIANCE (INCLUDING ANY THIRD PARTIES THAT HAVE CONTRIBUTED TO THE DISTRIBUTION) MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DISTRIBUTION ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
NEITHER THE OSGi ALLIANCE NOR ANY THIRD PARTY WILL BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THE DISTRIBUTION.

Implementation of certain elements of this Distribution may be subject to third party intellectual property rights, including without limitation, patent rights (such a third party may or may not be a member of the OSGi Alliance). The OSGi Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

The Distribution is a draft. As a result, the final product may change substantially by the time of final publication, and you are cautioned against relying on the content of this Distribution. You are encouraged to update any implementation of the Distribution if and when such Distribution becomes a final specification.

The OSGi Alliance is willing to receive input, suggestions and other feedback (“Feedback”) on the Distribution. By providing such Feedback to the OSGi Alliance, you grant to the OSGi Alliance and all its Members a non-exclusive, non-transferable,

worldwide, perpetual, irrevocable, royalty-free copyright license to copy, publish, license, modify, sublicense or otherwise distribute and exploit your Feedback for any purpose. Likewise, if incorporation of your Feedback would cause an implementation of the Distribution, including as it may be modified, amended, or published at any point in the future ("Future Specification"), to necessarily infringe a patent or patent application that you own or control, you hereby commit to grant to all implementers of such Distribution or Future Specification an irrevocable, worldwide, sublicenseable, royalty free license under such patent or patent application to make, have made, use, sell, offer for sale, import and export products or services that implement such Distribution or Future Specification. You warrant that (a) to the best of your knowledge you have the right to provide this Feedback, and if you are providing Feedback on behalf of a company, you have the rights to provide Feedback on behalf of your company; (b) the Feedback is not confidential to you and does not violate the copyright or trade secret interests of another; and (c) to the best of your knowledge, use of the Feedback would not cause an implementation of the Distribution or a Future Specification to necessarily infringe any third-party patent or patent application known to you. You also acknowledge that the OSGi Alliance is not required to incorporate your Feedback into any version of the Distribution or a Future Specification.

I HEREBY ACKNOWLEDGE AND AGREE TO THE TERMS AND CONDITIONS DELINEATED ABOVE.

0.2 Trademarks

OSGi™ is a trademark, registered trademark, or service mark of the OSGi Alliance in the US and other countries. Java is a trademark, registered trademark, or service mark of Oracle Corporation in the US and other countries. All other trademarks, registered trademarks, or service marks used in this document are the property of their respective owners and are hereby recognized.

0.3 Feedback

This document can be downloaded from the OSGi Alliance design repository at https://github.com/osgi/design The public can provide feedback about this document by opening a bug at https://www.osgi.org/bugzilla/.

0.4 Table of Contents

0.5 Terminology and Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in 1.

```
Source code is shown in this typeface.
```

0.6 Revision History

The last named individual in this history is currently responsible for this document.

Revision	Date	Comments
Initial	07-01-16	Initial, Peter Kriens

1 Introduction

This RFP was created to address the uncertainty that a remote service has when it is called. This RFP investigates the issues and defines a number of requirements.

2 Application Domain

This RFP is for an extension on 122 Remote Services Admin Specification. It is related to RFP 165 Authorization. This RFP uses terms explicitly defined in these documents.

In a distributed OSGi system, frameworks export and import services. Neither the distributed OSGi specification nor the Remote Services Admin Specification (RSA) specifies where these service originate from. The distributed

OSGi specification defines a number of properties on the imported and exported service registrations and RSA provides an API to discover endpoints and import and export services.

A bundle registering a service it must indicate that export is allowed. This implies that calls to this service can originate remotely or locally. The specification goes out of its way to make it transparent where a call originates from. In the RSA specification it is the topology manager that is responsible for managing the imports and exports.

The current use of RSA is that remote services are treated the same as local services. This means that they are generally not protecting themselves; there is an assumption that the caller is trusted. Most implementations of distribution providers know to the author of this RFP, the topology is limited one domain. Where the domain is generally a cluster of trusted machines.

Distributed OSGi can also be used to represent endpoints as services that come from general protocols like REST and/or JSON RPC. These endpoints generally interface directly with the domain of the outside world. They should therefore authenticate and authorize calls.

2.1 Terminology + Abbreviations

3 Problem Description

The assumption that the caller is trusted does not hold when RSA used in larger systems and the distributed OSGi specification is used to map unprotected endpoints like for example a REST or JSON RPC endpoint. In those cases, external parties can easily call any method on the exported service. In the current model, it is up to the distribution provider to authenticate and authorize the calls to these services. This is policy and should therefore not be part of the distribution provider, it clearly belongs to the topology manager's realm. However, the Remote Services Admin specification does not define API to provide authorization and authentication information for an exported service. This then leaves distribution providers to create ad hoc mechanisms or ignore the issue.

In certain cases, the service needs to be able to handle the authorization because parameters are relevant to the authorization, or the service needs access to the caller's identity. Currently there is no standard for this.

Therefore, this RFP requests a proposal for allowing topology managers to provide authorization information linked to an exported service.

4 Use Cases

4.1 Multiple Domains

An implementation of RSA can export services to other frameworks in the same VM, other frameworks in other processes on the same machine, and other frameworks on other machines. There are a number of services that should only be exported to frameworks in the same VM. For calls to services that are from remote machines, authentication is required. Some services exported to remote machines have a number of methods that are only allowed to be called when these machines belong to the `audit` group.

The topology manager reads a description of the topology from Configuration Admin. This description defines the different groups, the identities of the different machines, and the authorizations.

When the topology manager exports a service, it also provides the authentication & authorization information with that service. The RSA implementation will ensure that the caller for a remote call is authenticated and the proper authorizations are set for this service.

Requirements

4.2 Security

- S0010 – Allow a topology manager to provide authorization information on an exported service
- S0020 – Allow a service implementation to discover the identity of the caller including the originating framework and its machine.

5 Document Support

5.1 References

[1]. Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, RFC2119, March 1997.

[2]. Software Requirements & Specifications. Michael Jackson. ISBN 0-201-87712-0

5.2 Author's Address

Name	Peter Kriens
Company	aQute
Address	9c, Avenue St. Drezery
Voice	+33 633982260
e-mail	Peter.Kriens@aQute.biz

5.3 End of Document