

ORACLE SECURITY TOKEN SERVICE 11gR2

FEATURES

- Secure identity propagation and token exchange between Web Services
- Token issuance, validation and translation via WS-Trust protocol
- Support for multiple token standards, including: Username, X.509, Kerberos, SAML 1.1/2.0 , and OAM
- Centralized policy enforcement, audit and logging

BENEFITS

- Improved application security by decoupling applications and web services from the authentication mechanism
- Rapid deployment of new applications and services by enabling seamless identity propagation
- Lower cost of ownership via integration with Oracle Access Manager and centralizing the trust brokering function between different identity domains

Oracle Security Token Service (OSTS) simplifies access control and identity propagation across heterogeneous platforms, identity systems, and single sign-on (SSO) protocols. Oracle STS provides a standards-based mechanism for propagating identity and security context between web services utilizing different credential types.

WS-Trust Based Token Service

Authentication operations between applications and services typically require a mechanism for bridging multiple security token formats. When interacting with Web services, it's common for providers and consumers to be located in different security domains with different security token types. Oracle STS provides a secure, policy-driven identity propagation service, as a function of the Oracle Access Management platform.

Oracle STS implements the WS-Trust 1.4 specification for STS, offering both consumers and providers of web services a transparent mechanism to securely interact with one another. Oracle STS supports industry standard token formats, as detailed below.

Identity Propagation

Identity propagation is the replication of an authenticated user identity across multiple business systems and processes. In practice, a single logical identity, (a given user) is represented as multiple physical objects (SAML assertions, certificates, etc...). OSTS is able format the user's access token so the target application can accept it. Oracle STS provides a secure, seamless and auditable service to enable identity propagation in federated scenarios. Oracle STS facilitates token translation to and from all key industry standard formats, including:

- SAML 1.0/1.1/2.0
- Kerberos
- X.509
- Oracle Access Manager (OAM)

RELATED PRODUCTS

- Oracle Internet Directory
- Oracle Identity Manager
- Oracle Access Manager
- Oracle Web Services Manager

Summary

Achieving interoperability between the applications, and propagating user identity for end-to-end security and auditing is a significant challenge. This problem becomes even more difficult when application interactions cross security domains. OSTS provides a secure, standard-based solution to the problem in the context of a complete, end-to-end access management platform. Key benefits of Oracle STS include:

- Decoupling applications and services from the authentication mechanism, enabling them to solely focus on authorization
- Supporting federated scenarios where users are authenticated by their domain and granted access to resources in another domain.
- Facilitating identity delegation scenarios where the authenticated user is granted access to downstream services

Contact Us

For more information about Oracle Security Token Service, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0410

SOFTWARE. HARDWARE. COMPLETE.