PATHMAKER›GROUP

ORACLE® Silver Partner

Case Study: Wireless Telecommunications Provider:

Leveraging Oracle Security Token Service 11g for Secure Identity Propagation.

Introduction

With the growth of e-business, organizations are struggling with the challenges of managing secure access to information and applications across a wide range of internal and external computing systems and users. Additionally, organizations have to manage identities and profiles to an ever changing number of employees, customers, providers, systems and business partners without diminishing security or exposing sensitive information.

As the proliferation of SOA based infrastructures has continued to rise, mechanisms to provide security to those services have become increasingly important in today's IT landscape. The ability to integrate across vendor line into existing identity infrastructures can also be a factor when designing solutions to any organization's diverse IT portfolio.

Oracle Security Token Service 11g provides an infrastructure to allow for application level security by implementing a services based centralized trust brokering platform for the authentication and authorization of users.

In this case study we would like to highlight how Oracle Security Token Service 11g helped our customer, a wireless telecommunication service provider, solve the problem of services based authentication and authorization across vendor landscapes and hardware platforms.

Challenges

The wireless service provider that this case study refers offers a wireless service for mobile devices whose portfolio includes smartphones, messaging devices and feature phones. Their main priority here is to provide a quality experience, great value and greater flexibility with their services to their subscribers

One of the challenges to be overcome by this wireless communication provider is that access to systems and services is not always limited to PC or Web-Browser based mechanisms. Given the large landscape of diverse mobile handset providers, it is paramount to rely on repeatable standards-based mechanisms for access to content and resources.

This wireless provider successfully leveraged Oracle's Identity & Access Management Suite to provide its subscribers with secure and audit-able access to their web based infrastructure to support functionality like single sign-on (SSO), account management and payment. Additionally, they offered a highly available federation infrastructure utilizing Oracle Identity Federation (OIF) 11g for integration of external partner providers to support federated SSO scenarios for subscribers to access their web applications. The natural evolution of this infrastructure was its extension outside of the browser based mechanisms and into a standard based SOA infrastructure for inclusion of non-PC based identity management activities. This includes access from purpose built mobile telephone handset applications as well as other non-traditional mechanisms such as IVR, etc.

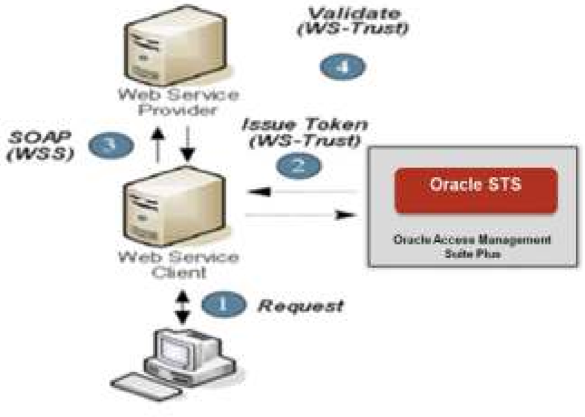
The main challenge presented to the solutions team was how to leverage the existing IdM & security infrastructure (consisting of millions of subscribers) while being flexible enough to integrate with external partner's SOA based platforms.

To overcome these challenges the customer's IT team had to standardize their process to integrate with their business partners, which could enable managing application user accounts across the business-to-business boundaries in a seamless way there-by saving costs in the long run, at the same time meet their company's growing business needs.

Oracle Security Token Service 11g

The burden of security silos in the enterprise increases administrative and integration costs associated with the lack of unified identities. Oracle Security Token Service (OSTS) 11g overcomes the costs and complexity of fragmented security: OSTS 11g brokers trust between apps and downstream web services resulting in seamless access across a heterogeneous environment via propagation of identities and security context which leads to policy transparency, streamlined audit and lower integration costs.

Oracle Security Token Service is an enterprise-grade solution that facilitates standards-based token exchange, identity propagation and end-to-end Security across web services through a single thread of identity. It provides the foundation to the current security infrastructure to facilitate a consistent and streamlined model for token acquisition and token validation that is protocol and security infrastructure agnostic.



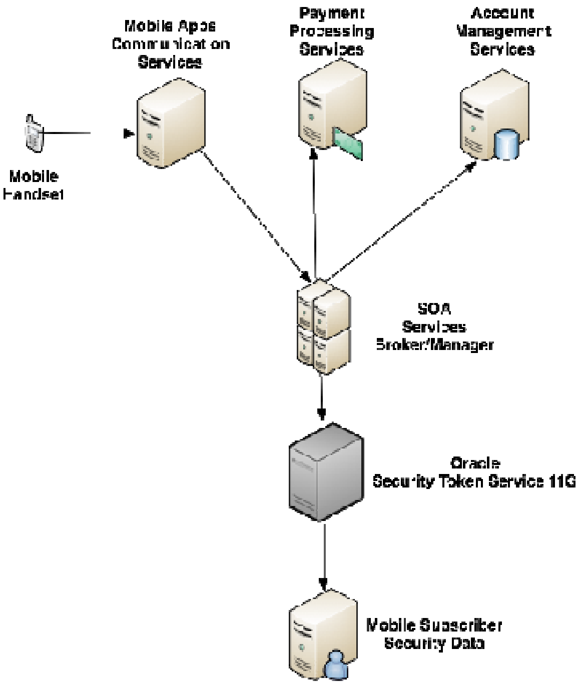
Oracle Security Token Service supports a variety of standards including WS-Trust. The service allows for policy-driven trust brokering and secure identity propagation and token exchange between Web Services. Oracle Security Token Service can be deployed to simplify the integration of distributed Web services within an enterprise and its service providers.

Solution

One of the noticeable challenges which the provider faced during OSTS deployment was to make sure that the web services provided by OSTS were able to be integrated into non oracle SOA based infrastructures. The customer has outsourced all SOA activities related to subscriber interaction to a third party provider that act as a central hub for communication between its partners. Largely due to

OSTS's faithful implementation of standards as well as its dynamic generation of WSDLs based on current configuration, integration was fairly simple. Once the configuration of OSTS was completed, the WSDL was then distributed to the SOA services provider and imported into their environment. By utilizing a standard format for the request and validation of tokens, the time for development and integration into the partners systems was kept to a minimum.

By abstracting the pre-existing security model from the web services logic, we were able to rapidly deploy a solution that will be repeatable across any partner provider that needs to request authentication of subscribers via its SOA partner provider


Mobile Apps Communication Services
Payment Processing Services
Account Management Services
Mobile Handset
SOA Services Broker/Manager
Oracle Security Token Service 11G
Mobile Subscriber Security Data

Benefits

Oracle STS 11g has delivered the following benefits to the customer:

- Decoupled web applications and web services from the authentication mechanism through a centralized trust broker
- Facilitated web services to support multiple credential types through token translation mechanism.
- Supported scenarios where users are authenticated by their domain and granted access to web service resources in another domain
- Facilitated identity propagation scenarios where the authenticated user is granted access to downstream web services.

Conclusion

Sharing applications over the Internet to external divisions and partners or a user interacting with different applications that are hosted in single or different domains is a common scenario in the current application world. The common challenge in any enterprise includes establishing trust between applications in different identity domains or the same domain and propagating user identities securely. For example, a client application in one domain requests information from a Web service residing in a different domain, the client will need to present proof of its identity using a credentialing authority trusted by the Web service. The receiving service will need to be able to understand and evaluate the presenting credentials to determine an identity's validity while also having evidence that the credentials were not tampered with or spoofed during transit.

Oracle STS reduces the cost of ownership by brokering trust between applications in different identity domains or in the same domain.

About Pathmaker Group, Inc.

"Clearing your path through the identity and security management jungle™"

PathMaker Group is a specialized Identity and Security Management consultancy, blending core technical and product expertise, consultative know how and extensive implementation experience. Driven by your unique business, compliance requirements and specific environment, we help you assess, plan, select, and integrate the right mix of products and solutions to optimize and secure your business IT, reduce your project risk, and maximize performance. We provide complete solutions by blending software, hardware, managed service solutions, professional services, and customized training. We work to leverage your investments by integrating new solutions with your current products.

Since 1990, our teams have proven over and over that IT projects can be executed successfully. The value of each of these experiences continues to provide synergistic growth and maturity. Your organization can reap these benefits today. Our high quality, formalized methodologies, grounded in PMI project management principles, have been refined through practical application, and have gleaned best practices from dozens of multimillion dollar projects.

Headquartered in Dallas/Fort Worth area, the employees of PathMaker Group have been delivering successful IT and Security projects for Fortune 500 corporations for more than 15 years.

4209 Gateway Drive, Suite 100
Colleyville, Texas, 76034
www.pathmaker-group.com