

Security Planning for Service-Oriented Architecture

At a Glance

- Identity and access management
- Authentication
- Policy enforcement
- Centralized security audit
- Secure integration with web applications
- Governance

Securing Service-Oriented Architecture (SOA) implementations is of prime concern as enterprises extend their interactions with customers and partners. Risks to financial information, personal information and corporate reputation make companies justifiably cautious in sharing their applications and data. With this in mind, RSA is ready to help organizations achieve effective SOA implementations, by providing the security planning that is critical for its success.

Service-Oriented Architecture

To be competitive, today's enterprises must adapt. Traditional security implementations extend only to enterprise boundaries, while SOA is an open-standards vision of application and IT systems as a collection of services extending beyond traditional trust boundaries. This can include trusted partners and even external entities that may not be completely trustworthy. Securing SOA helps enterprises safely exploit these transformational opportunities.

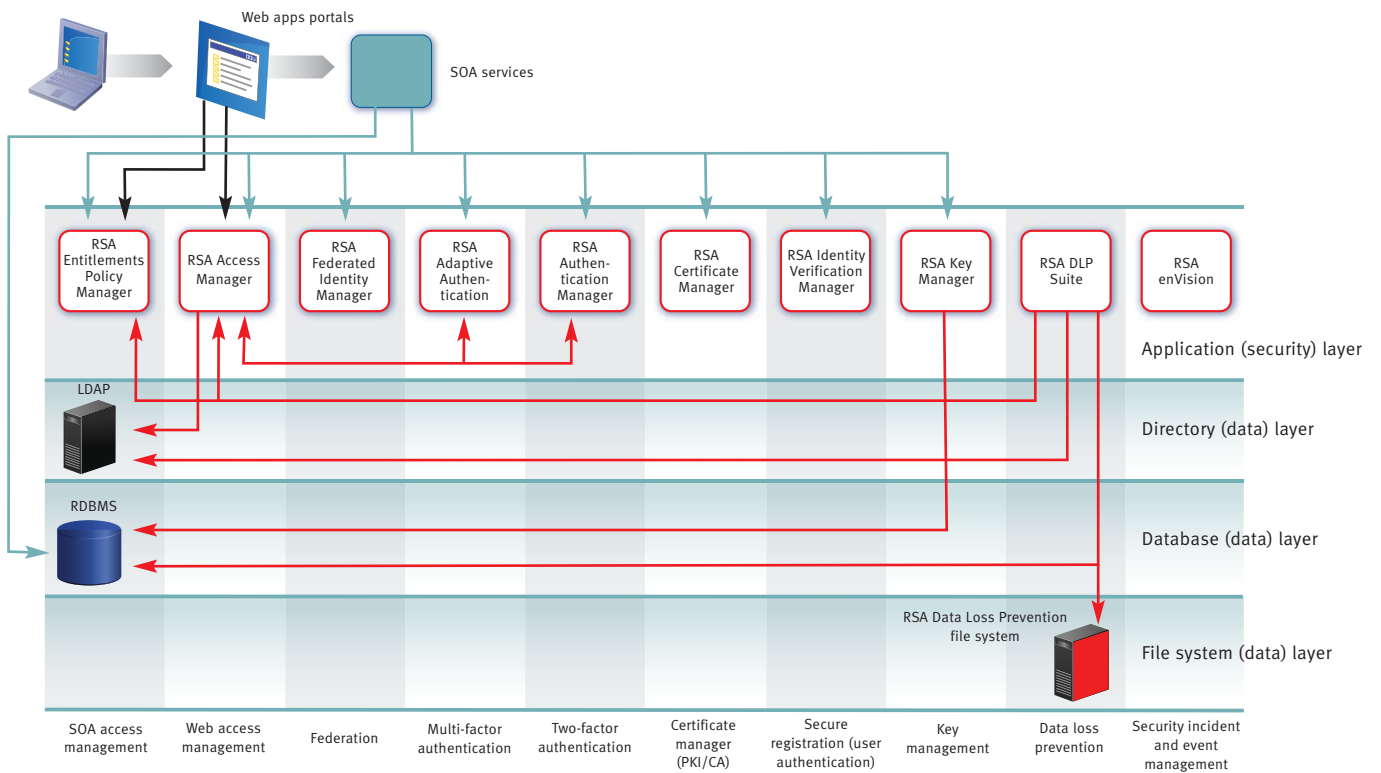
Planning Security for SOA

Traditional security architectures are inadequate for SOA. Their approaches are application-centric and limited to protecting enterprise trust boundaries. While the functional aspects of security, such as authentication, authorization, confidentiality, integrity and non-repudiation remain vital, introducing SOA forces the reevaluation of current security approaches. SOA's cornerstone is services leveraging other services and existing legacy frameworks; enterprises must adapt their security architectures to provide appropriate protections. The Secure SOA Planning service is designed to help organizations understand their present IT and application infrastructure and craft security that fits their service-oriented environment.

The Secure SOA Planning service can address these areas:

- Review and analysis of the current SOA strategy and architecture, including governance and policy from an architecture point of view
 - Discussion of SOA needs within the enterprise and current plans to address them
 - Examination of the level of existing web services and SOA
 - Assessment of security controls across existing and planned services-based infrastructures, including management, operational and technical aspects.
- Focusing on SOA, key areas for review will include:
- Access management for web services, web applications and portals
 - Policy management of access control requirements across the services-based infrastructure
 - Identification of data at risk with assessment of proactive remediation options
 - Security event monitoring requirements across the services-based infrastructure
 - Management of system-based trust in federated services-based connections with external partners
 - Authentication and encryption control requirements with policy enforcement mechanisms





The RSA SOA security team will review and analyze existing assets and through an efficient, comprehensive approach, make security recommendations incorporating SOA technologies, platforms and strategies. The Service can also provide recommendations for integrating RSA Entitlements Policy Manager, which has been designed to secure and extend SOA infrastructures seamlessly, and:

- Discover policies from application containers and web services automatically
- Create role-based and attribute-based access control on resources
- Create, manage and enforce messaging and application policies in compliance with open standards
- Log user activity to enable auditable reports on who, what, where and when
- Extend existing security technologies to incorporate native SOA policy and end point controls

Results

Led by a senior RSA enterprise security architect, the SOA Security Planning engagement will review existing and planned SOA security postures. The SOA Security Strategy Report will provide recommendations for improvements across the existing and planned SOA infrastructures based on RSA and industry best practices.

Why RSA?

RSA, the Security Division of EMC, is the expert in information-centric security, helping to enable the protection of information throughout its lifecycle. RSA helps you to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way. RSA also helps you to manage security information and events, easing the burden of compliance. As the chosen security partner of more than 90 percent of the Fortune 500, RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges.

Take the next step

Implementing a robust and scalable security infrastructure can be a complex task in an enterprise environment. RSA has extensive experience in solving complex information security issues and deploying RSA security infrastructure solutions for companies across the globe. Contact your sales representative for more information, or visit www.RSA.com.

 RSA Security Inc.
 RSA Security Ireland Limited
www.rsa.com
 The Security Division of EMC

©2008 RSA Security Inc. All Rights Reserved.
 RSA, RSA Security and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.