RSA FEDERATED IDENTITY MANAGER

Extending Trust to the Cloud

EXECUTIVE SUMMARY

In today's global market, effective business models rely heavily on an ecosystem shared by employees, partners, and customers. The need to securely access applications and collaborate across enterprise boundaries is critical as this partner ecosystem expands, and information grows. RSA Federated Identity Manager enables organizations to cost-effectively federate identities and extend trust between multiple organizations. With RSA Federated Identity Manager, organizations can extend the management of digital identities beyond their domain and corporate boundaries to externally hosted or managed applications and resources.

RSA Federated Identity Manager installs on-premise and provides federated single sign-on for both identity provider and service provider models. Federated single sign-on provides a standards-based method to leverage trusted identities between organizations, collaborating with business and service partners. RSA Federated Identity Manager provides access to other cloud service providers, which is a significant benefit with the aggressive adoption of cloud-based applications.

RSA Federated Identity Manager has a highly flexible, open and extensible underlying architecture. This enhances user productivity, enforces internal identity security policies to make stronger security decisions, and allows for more efficient identity integration with partners. Essentially, RSA Federated Identity Manager provides organizations with the ability to address new business problems and use cases, and also scales with customer growth.

SEAMLESS COLLABORATION ACROSS ENTERPRISE BOUNDARIES

RSA Federated Identity Manager enables seamless collaboration and productivity across enterprise boundaries and to/from the cloud. It installs on-premise, and delivers a light-weight solution enabling businesses to quickly and easily federate with partners who do not have the requirements of deploying a complete identity and access management solution.

RSA Federated Identity Manager packages the following features and capabilities into an easy-to-deploy, effective solution for enterprises to access cloud-based applications.

- Quick setup tools, a wizard-based approach, UI configurable security policies, bulk federation, policy cloning and other automated capabilities to speed deployment time.
- Fully-functional, out-of-the-box federation sample application for prototyping, a proof-of-concept and interoperability testing between partner locations

ESSENTIALS:

Secure Access to SaaS Applications

- Federated single sign-on (FSSO) for identity provider (IdP) and service provider (SP) models
- Simple and secure on-premise installation and deployment
- Enables businesses to quickly and seamlessly federate with partners, customers, and employees across enterprise boundaries

Robust Authentication to the Cloud

- Out-of-the-box integration with RSA SecurID two-factor authentication

Increase Business Productivity

- Flexible and extensible architecture
- Leverages industry standard federation protocols for easy integration with existing cloud-based applications.
- Enhances security, reduces administrative expenses, and increases collaboration across enterprise boundaries

– Digital signing and local / remote digital certification validation capabilities

– Flexible plug-in architecture for integration with LDAP and SQL data stores, or with existing identity infrastructures

– Flexible and secure deployment models that accommodate virtually any architecture and partner trust model

MULTI-FACTOR AUTHENTICATION FOR SECURE ACCESS

Since federation is based on trust across enterprise boundaries, it is significantly more challenging to determine the identity of users. By integrating with strong two-factor authentication, enterprises can be confident that the identity is being used by the person it belongs to. RSA Federated Identity Manager supports RSA SecurID two-factor authentication out-of-the-box to ensure the authenticity of federated identities. In addition, RSA Federated Identity Manager also supports the risk-based authentication (RBA) feature set introduced in RSA Authentication Manager 8.0 – this feature set triggers additional step-up authentication methods types based on the risk-score of the transaction.

STANDARDS-BASED FEDERATION SUPPORT FOR OPTIMAL FLEXIBILITY

The OASIS Security Assertion Markup Language (SAML) is the industry standard for the extensible markup language (XML). It enables XML-based applications to securely exchange authentication, attribute, and authorization information between two or more SAML-compliant applications. This removes the need for costly, cumbersome proprietary and one-off solutions.

RSA Federated Identity Manager supports the SAML and WS-FED identity provider/service provider trust relationship. It is designed to be flexible and readily customizable, making it easy to add additional trust relationships, and integrate with a customer's existing user and attribute repositories. Furthermore, RSA Federated Identity Manager is designed to support the most popular federation use cases. With RSA Federated Identity Manager, organizations have the ability to implement the following features:

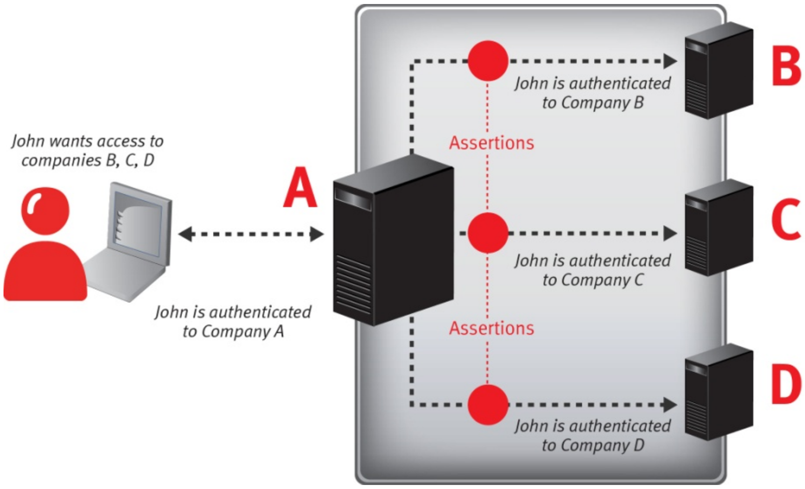
– **Web single sign-on.** Authenticated web users can easily move between applications within their environment or among business partners – without re-authenticating – using consistent and secure mechanisms for the exchange of identity information.

– **Attribute service.** As users move from one web site or service to another, RSA Federated Identity Manager allow applications or web services to capture additional attributes about that user – such as role, employee ID number or account balance. RSA Federated Identity Manager puts you in control of which attributes are shared between business partners and how that information is securely exchanged.

– **Account linking.** Account linking enables end-users to choose which accounts they would like to federate to, and allows end-users to create the linkages between accounts. This capability empowers end-users by enabling easy access to various sites, especially as business transactions continue to build across organizational boundaries.

- **X.509 Attribute Sharing Profile.** The SAML XASP profile enables service provider applications that have successfully authenticated the user with a digital certificate to send a SAML request to the issuing organization, and retrieve sensitive user attributes that not included in the underlying certificate. By supporting this profile, RSA federated Identity Manager enables dynamic retrieval of user attributes and facilitates access control decisions in real time.

A Federation Scenario


John wants access to companies B, C, D
A
John is authenticated to Company A
Assertions
Assertions
John is authenticated to Company B
B
John is authenticated to Company C
C
John is authenticated to Company D
D

PRODUCT SPECIFICATIONS

Currently shipping version	**RSA Federated Identity Manager 4.2**
Supported operating systems	**VMware ESX 5.1 hosting:** – Microsoft® Windows® Server 2008 R2, SP1 (64-bit) – Red Hat Enterprise Linux 6 ES (64-bit x86) – Sun® Solaris™ 10 (64-bit Kernel x86) – SuSe Linux enterprise 10.3 (64-bit Kernel x86) – SuSe Linux enterprise 11 (64-bit Kernel x86) **Native:** – Microsoft Windows® Server 2008 R2, SP1 (64-bit) – Red Hat Enterprise Linux 6 ES (64-bit x86) – SuSe Linux Enterprise 10.3 (64-bit Kernel) – SuSe Linux Enterprise 11 (64-bit Kernel x86)
Supported application servers	**Non-clustered:** – Oracle WebLogic Server 11g R2 (10.3.6) – Oracle WebLogic Server 10.3.5 – Oracle WebLogic Server 10.3 MP2 – Apache Tomcat 7.0 **Clustered:** - Oracle WebLogic Server 11g R2 (10.3.6) - Oracle WebLogic Server 11g R1 (10.3.5)

	- Oracle WebLogic Server 10.3 MP2
Supported data stores	Apache™ Derby 10.8.x (included) PostgresSQL 9.1.x Oracle 11g R2 RAC
Supported browsers	Microsoft Internet explorer 8.x, 9.x Firefox 14.0 and later Chrome
Supported federation protocols	SAML 1.1 SAML 2.0 WS-Federation and ADFS 2.0
Supported plug-ins	RSA Access Manager 6.2, 6.1 SP4 RSA Authentication Manager 7.1, 8.0 SQL / LDAP support **Others** RSA Secured Partner Solutions
Minimum system requirements	Storage space: 2GB Memory: 1 GB RAM (minimum) Processor speed: 1gHz (minimum) Periphery devices: CD-ROM drive connectivity: TCP/IP

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the worldís leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

EMC^2, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. ©2013 EMC Corporation. All rights reserved. Published in the USA. h9040 ds 0413