



RSA® Authentication Deployment Manager

Web-based solution for rapid deployment of the RSA SecurID® solution

At a Glance

- Workflow system for rapid, low-cost deployment of RSA SecurID hardware and software tokens
- User self-service functionality to reduce ongoing administrative costs
- Flexibility to customize deployment and user self-service in accordance with business policies
- Robustness and scalability to meet the needs of small and large user deployments

The RSA® Authentication Deployment Manager can reduce deployment and ongoing administrative costs by offering end users a self-service platform for requesting, activating and initiating deployment of RSA SecurID® credentials. The system automates the entire credential deployment process—including user requests for credentials, approvals and populating the RSA® Authentication Manager with user data and hardware or software token assignment / activation. Flexible and scalable, the RSA Authentication Deployment Manager is ideal for both enterprise and e-business related deployments.

Rapid Deployment of RSA SecurID Hardware and Software Tokens

The RSA Authentication Deployment Manager workflow automation system speeds deployment of RSA SecurID hardware and software tokens to end users. Without it, the tasks of identifying approved users, assigning credentials to each user and populating the RSA Authentication Manager authentication database with user data have to be performed centrally by security administrators, prior to

credential distribution. The Authentication Deployment Manager solution has been created to automate the administrative work involved in issuing RSA SecurID hardware and software tokens—helping to enable a fast, cost-effective rollout of the RSA SecurID solution.

User Self-Service PIN Change

Whether due to security policy or as a result of simple forgetfulness, a user may occasionally need to change their PIN. The user self-service PIN change feature allows him or her to select a new PIN without requiring help desk or administrative assistance. If the user remembers their PIN, they may change it simply by authenticating to the Authentication Deployment Manager with their RSA SecurID passcode and then entering a new PIN. If the user forgets their PIN, they may select a new one, but must first authenticate to the Authentication Deployment Manager by correctly answering a number of questions defined by the software administrator. Once authenticated, the user may change their PIN; the entire PIN change process can occur without administrative involvement. This may significantly reduce help-desk costs and improve end user productivity and satisfaction.

Replacement of Expiring Hardware Tokens

The RSA Authentication Deployment Manager also facilitates the replacement of expiring hardware tokens. Once notified that a hardware token will soon be expiring, a user can use the expiring token to authenticate to the Authentication Deployment Manager and request a replacement token. The existing Authentication Deployment Manager process can then be used to approve the request and distribute a new token.



The Security Division of EMC



Flexible, Compatible and Customizable

The RSA Authentication Deployment Manager can be customized to suit security and business requirements. User interface screens are HTML-based and can be enhanced with company-specific graphics and terminology.

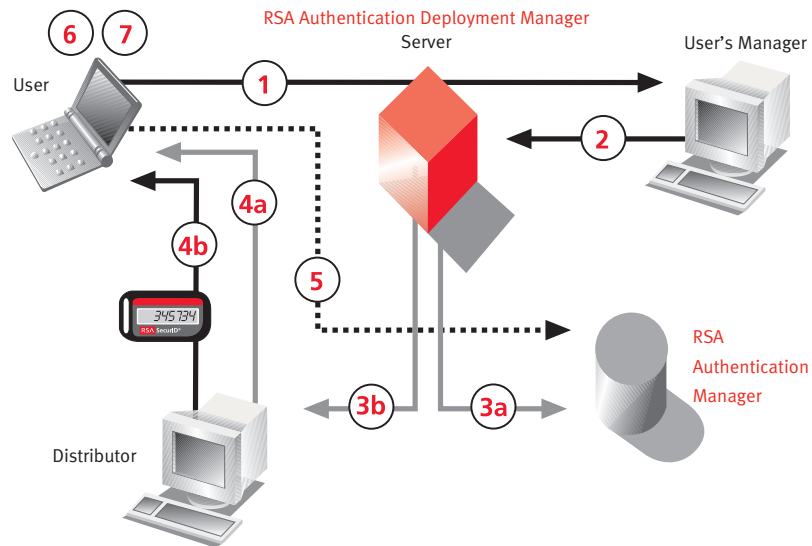
A powerful set of built-in application programming interfaces (APIs) are provided to enable integration with existing data and processes. RSA Authentication Deployment Manager APIs allow verification of user data; for example, prior to approving an end user or authenticating the user for a PIN change, the user's password can be checked against an external LDAP directory. Required data, e.g., user address information, could then be imported into the Deployment Manager workflow. Additionally, approved data can be exported to applications outside the Deployment Manager. These APIs may also be used to fully automate the manager or distributor functions to further streamline the token deployment process.

Anytime, Anywhere Issuance of RSA SecurID Credentials

Scalable, available around-the-clock and simple to use, the RSA Authentication Deployment Manager software is built to improve the end users' experience while significantly reducing deployment time, deployment cost and administrative burden—all without compromising the security of the credential approval and distribution system.

The RSA Authentication Deployment Manager is available at no extra charge with an RSA Authentication Manager Enterprise Edition license and is available as a separate purchase for use with an RSA Authentication Manager Base Edition license.

- 1 End user submits token request
- 2 Manager approves
- 3a User information added to RSA Authentication Manager software records
- 3b Distributor notified
- 4a Approval code sent
- 4b Token issued
- 5 End user submits token serial number with approval code
- 6 Token enabled
- 7 First-time authentication (new PIN mode)



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2004-2007 RSA Security Inc. All Rights Reserved.
RSA, SecurID 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.

ADM_DS_0507