RSA SecurID® On-demand (SMS) Authenticator

Flexibility and ease of deployment in a true “zero-footprint” authenticator

At a Glance

- Delivers one-time token codes via SMS or e-mail
- Maintains traditional anywhere, anytime access
- Enables a range of business-driven applications
- Secures applications using two-factor authentication

Assuring User Identities in an Uncertain World

The RSA SecurID® On-demand Authenticator is an innovation that enables users to securely access sensitive applications and information without requiring a hardware or a software token. The On-demand Authenticator utilizes the technology the user is already carrying: a mobile phone or laptop computer. It provides flexibility and ease of deployment, while still maintaining all the security strictures required for two-factor authentication.

Users simply enter their credentials (username/pin) into the login screen of a web application. If the user's credentials match, RSA Authentication Manager generates a unique one-time password and delivers it to the user via SMS or e-mail. This password is then entered into a field on the web application login screen to complete the authentication. The On-demand Authenticator can also be generated by utilizing a self-service web URL. From an Internet-capable PC, a user accesses the self-service web URL using the traditional login and PIN combination; upon successfully passing this step, a request for a token code can be generated and sent to the user’s device of choice. RSA® Authentication Manager generates the token code (8-digit) and sends it to the registered mobile device via short message service utilizing the public cellular network. The RSA On-demand Authenticator works with a variety of applications including VPN, web portal, Citrix® and others.

Lowering Deployment Costs Through Self Service

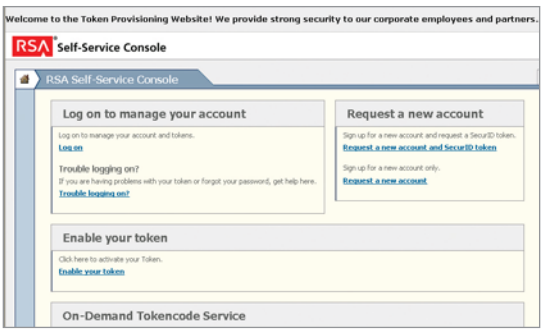
The engine that empowers users to manage various aspects of their token usage is RSA® Credential Manager software, found within the RSA Authentication Manager software. With its self-service and work flow provisioning tools, an IT administrator can design and implement processes and security measures for presenting users with the options necessary for managing token lifecycles, all while maintaining total compliance to organizational security policies. This makes it possible to lower deployment costs and on-going administration by fully automating the most commonly requested user functions. Users who can handle their own requests are less likely to flood the IT help desk with calls.*

RSA SecurID On-demand Authenticator

RSA®
The Security Division of EMC

*work flow provisioning is available in the Enterprise Service License form of RSA Authentication Manager.

RSA Credential Manager is built into the RSA Authentication Manager administration software, and runs on its own embedded web server for simplified installation, access and use. The self-service module can be used as a tool to help all token users – hardware, software and On-demand – perform a variety of first-line tasks without having to call the IT hotline.



Through a Self Service web URL, users are able to manage all aspects of their token lifecycles

A Multitude of Business-Driven Uses

The On-demand Authenticator opens the door to a variety of productivity enhancing applications. For example, flexibly supporting a large base of users that require secure remote access – but do not access the network frequently enough to justify the issuing of hardware or software credentials to each user – is made easier. Contractors and vendors can be assigned temporary access to corporate resources with On-demand Authenticators. Business continuity and pandemic plans can be written around RSA Authentication Manager's ability to rapidly bring on-board large numbers of remote users without deploying tokens or involving IT in every step. RSA even has a Business Continuity Option that allows an organization to temporarily expand its server license and number of On-demand Authenticators to support a large influx of users on occasions such as when a business disruption occurs and the work force must be deployed remotely.

Secure Emergency Access to the Network

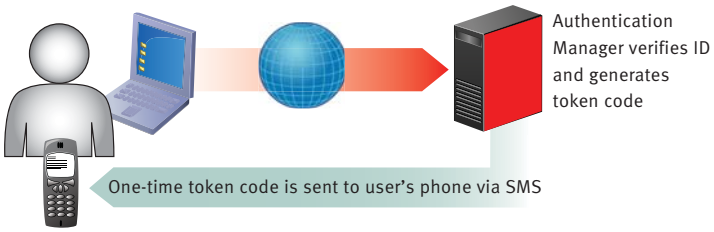
Another application enabled by the On-demand Authenticator is the granting of "emergency" access to a traditional token user who may have temporarily misplaced (left a token at home) a token, irretrievably lost a token or forgotten a PIN. By successfully completing life question challenges from the database, workers can remain productive by requesting on-demand authentication even in off-hour scenarios.

Work flow processes can be triggered for the IT staff to follow up as a result of user requests – such as issuing another hardware token to a user who has permanently lost hers. Since information is taken from a common data store, the reporting of a lost hardware token can automatically disables that user's credential, saving valuable time and heading off potential inappropriate account use. Other services available through the self-service screen include the ability for a user to test a token, report a problem with a token, change a PIN, update the user's profile and more.

Global Mobile Reach

Configuring the On-demand Authenticator with SMS requires partnering with an SMS aggregator for worldwide delivery of SMS messages. RSA has taken the first step by joining forces with a leading SMS delivery vendor Clickatell™, and building an interface directly into the RSA Authentication Manager console for configuring messages to be sent to the Clickatell gateway. Clickatell has delivery capabilities in almost 200 countries and over 600 networks, ensuring that no matter where users are located, they can be reached with an RSA SecurID On-demand Authenticator.

A user can access sensitive applications and information by receiving a dynamically generated one-time token code.



RSA®
The Security Division of EMC

www.rsa.com

SIDODA DS 0310