RSA®

RSA SECURID® ACCESS
PROTECTION AND PEACE OF MIND DURING A TIME OF BUSINESS DISRUPTION

AT A GLANCE

- Flexibly expands your RSA SecurID Access deployment to accommodate users during a business disruption
- Supports users with "zero footprint" On-demand authenticators
- Self activates at any time
- Ideal tool for business continuity and pandemic planning processes

RSA SecurID Access provides a solution for maintaining a consistent multi-factor authentication policy during a business emergency, when large numbers of users may be required to work remotely for a period of time. RSA SecurID Access enhances the security of your organization by ensuring that no matter the state of your business user identities are assured and access to critical applications and data remain intact. The solution is a critical part of any business continuity or pandemic plan.

In many organizations oftentimes only users who work outside of the firewall on a consistent basis use multi-factor authentication. Users that work inside the firewall may not have tokens. In the event that a user may require remote access, IT simply issues an authenticator to the individual. The problem is that this process is not scalable to a business disruption. In that scenario, often unexpectedly, large numbers of users may have to work remotely. This creates a "crisis within a crisis" as IT staff – who themselves may not be able to make it into the office – now must scramble to support these users. With a significant number of users in the organization who do not have authenticators, many times IT disables two-factor authentication temporarily to allow these users access. But doing so can expose the organization to unacceptable risks.

PROTECTING DATA AND ASSURING USER IDENTITIES DURING A DISRUPTION

There are two ways to solve this problem. The first way is to require every user to use multi-factor authentication. This is a sensible solution for organizations which have a mobile workforce. The other way, the Business Continuity Option, provides a flexible method to expand the number of users in an organization without expanding your multi-factor authentication budget.

RSA®

HOW IT WORKS

The Business Continuity Option is a licensing feature optionally available with the RSA SecurID Access. Once added to the licensing page, an administrator with rights can simply view, select and activate the feature when necessary. The activation "unlocks" the corresponding number of server seats and On-demand Authenticators which can then be deployed to any remote user needing access. On-demand Authenticators deliver one-time passwords via short message service (SMS) or e-mail. No hardware authenticator is required and no software needs to be installed on the user's mobile phone device or PC.

Users request On-demand Authenticators through the Self Service web portal included in RSA SecurID Access. The portal provides a convenient 7x24 service for users to manage all aspects of their token lifecycles and request access. In order for a user to be issued an On-demand Authenticator, they must login to the Self Service portal, which then sends a one-time password to the user's pre-designated destination, such as the mobile phone number in the database. The rules of multi-factor authentication are enforced: something you know (login/password) and something you have (one-time password delivered to the mobile device via SMS or e-mail).

ABOUT RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to **rsa.com.**