RSA SecurID® 800 Authenticator

Hybrid authenticator that provides a seamless user experience across multiple applications using multiple credentials

At a Glance

— Helps enable two-factor authentication, disk and file encryption, smart card logon, e-mail signing and more

— Provides a seamless user authentication experience across multiple credentials and applications

— Automatically submits credentials to target applications – just insert the token and enter your PIN

— Supports RSA SecurID tokens, digital certificates and domain password credentials

As data breaches become daily news, organizations are protecting their information assets with multiple authentication methods including digital certificates, one-time passcodes (OTP) and traditional passwords. Using all of these methods can be confusing and cumbersome for the end user, resulting in poor security habits and putting organizations' data at greater risk.

The RSA SecurID® 800 Authenticator (800) is a hybrid device that combines the portability of RSA SecurID tokens with the power of a smart card in a convenient USB form factor – giving end users a single device for strong authentication without the hassle of juggling multiple credentials. The 800 generates time-synchronous OTPs for secure remote access,

RSA SecurID 800 Authenticator

supports certificates for disk encryption, authentication and other applications, and strengthens simple password authentication by storing users' domain credentials on a hardened security device. This makes the 800 the ideal choice where diverse system, application and customer needs exist.

One Master Key for Securing Remote Users and Data Assets

The 800 enables employees to adhere to company security policies by acting as one master key for securing both the remote user and the organizations' critical data assets. This makes the complexity of a diverse security infrastructure, and its resulting policies, invisible to the employee. By simply inserting the 800 into a USB port and entering their PIN, end users can quickly:

– Authenticate to the PC/laptop

– Unlock an encrypted hard drive

– Establish a secure network connection to a VPN or wireless access point

– Authenticate to the corporate domain

– Encrypt sensitive documents and files

– Sign and encrypt emails

Additionally, end users need only remove the authenticator to lock down or log off from their laptop.

Flexible Solution Supports Multiple Credentials

Organizations must have the flexibility to choose the most appropriate credential type for securing specific applications. The 800 preserves this flexibility by supporting multiple credentials including:

– RSA SecurID OTP that changes every 60 seconds

– X.509 digital certificates that enable authentication, encryption, and digital signatures

– Username/password credentials for Windows logon, enabling organizations to introduce two-factor authentication and strengthen existing password policy without infrastructure changes or end user inconvenience

RSA®

The Security Division of EMC

Secure data access with disk and file encryption integration

The growth in mobile workers carrying sensitive data on their laptops has increased the risk of data breaches. Disk and file encryption solutions prevent unauthorized access to sensitive information stored on laptop hard drives. The 800 is certified by all leading disk and file encryption vendors for strong authentication, thereby eliminating the weakest link – the password – from these solutions.

Industry leading one-time password solution

RSA SecurID authentication is an industry-leading OTP solution that displays a unique authentication code changing every 60 seconds. The 800 can be used both as a traditional SecurID fob (token code is read from the authenticator's LCD display) and as a connected token that automates the logon process by submitting the token code via the USB port. In either mode, the user is always required to enter their PIN, thereby ensuring two unique factors for authentication.

RSA SecurID is integrated with over 400 certified third-party applications. This helps to lower deployment costs by providing the assurance that important applications are "RSA SecurID Ready."

Ensure your authentication solutions meet your needs today – and tomorrow

Many organizations begin their security strategy by securing remote users and quickly follow by adding protection for those users' PCs and laptops. As business requirements evolve to include secure web access, smart card logon, e-mail signing and more, the many functions of the 800 will continue to meet these needs in a single device while protecting the initial investment made in RSA.

Technical Specifications

PHYSICAL ATTRIBUTES

Dimensions: 86mm(L) x 27mm(W) x 10mm(H)

Weight: 21g

Operating temperature: -20ºC to 65ºC

Battery life: up to 5 years

PKI AND SMART CARD

Smart card memory: 64KB

FIPS 140-2 Level 3 (smart card only)

Data transfer rate: 129 Kbps

Credential storage: X.509 v3 certificates, secure key storage, and Microsoft Windows® credentials

Key generation: RSA 1024-bit, DES/3DES, AES

RSA signature: 1024-bit

Secure hash: MD5, SHA-1, SHA-256

ANSI X9.31 PRNG

ONE TIME PASSCODES

RSA SecurID time-based OTP

Connected (via USB port) or standalone (6-digit LCD) use

API STANDARDS

PKCS11

MSCAPI

USB INTERFACE

USB 2.0 (CCID 1.0 compatible)

TAMPER EVIDENT

Conforms to ISO 13491-1; ISO DIS 13491-2 Annex A, Section A.1.1, Statement A1, A2 and A4

PLATFORM SUPPORT

Windows XP/Server 2003, Windows Vista/Server 2008 (x86 and x64 versions)

For more information about RSA SecurID technology and other RSA SecurID authenticators, please visit us at:
http://www.rsa.com/node.asp?id=1156.

RSA®

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

The Security Division of EMC