

RSA SecurID® 800-Authentifizierungskomponente

Hybride Authentifizierungskomponente für nahtlose Nutzung bei mehreren Anwendungen mit verschiedenen Zugangsdaten

Übersicht

- Bereitstellung von Zwei-Faktor-Authentifizierung, Festplatten- und Dateiverschlüsselung, SmartCard-Anmeldung, E-Mail-Signatur usw.
- Einrichtung einer nahtlosen Benutzerauthentifizierung für verschiedene Zugangsdaten und Anwendungen
- Automatische Übermittlung von Zugangsdaten an Zielanwendungen - einfach Token anschließen und PIN eingeben
- Unterstützung von RSA SecurID-Token, digitalen Zertifikaten und Passwortdaten für Domänen

Angesichts der täglichen Medienberichte über Datenverluste schützen Unternehmen ihre Informationsbestände durch verschiedene Authentifizierungsmethoden, darunter digitale Zertifikate, einmalig gültige Passcodes und herkömmliche Passwörter. Diese Methoden empfinden Endanwender oft als komplex und umständlich, sodass sie Sicherheitsmaßnahmen nicht immer einhalten und dadurch die Unternehmensdaten höheren Risiken aussetzen.

Bei der RSA SecurID® 800-Authentifizierungskomponente (kurz SID 800) handelt es sich um ein hybrides Gerät, das die Mobilität von RSA SecurID-Token mit der Leistungsstärke einer SmartCard in einem praktischen USB-Formfaktor vereint. So erhalten die Endanwender ein



RSA SecurID 800 Authenticator



The Security Division of EMC

einziges Gerät für die starke Authentifizierung und müssen keine verschiedenen Zugangsdaten mehr verwenden. Der SID 800 generiert zeitsynchrone, einmalig gültige Passwörter für sicheren Fernzugriff, unterstützt Zertifikate für Festplattenverschlüsselung, Authentifizierung und andere Anwendungen und verstärkt die einfache Passwortauthentifizierung, indem die Domänenzugangsdaten des Anwenders auf einem robusten Sicherheitsgerät gespeichert werden. Dadurch eignet sich der SID 800 optimal für Umgebungen mit verschiedensten System-, Anwendungs- und Kundenanforderungen.

Ein Master-Schlüssel zum Schutz von Remote-Anwendern und Datenbeständen

Der SID 800 unterstützt die Mitarbeiter beim Einhalten unternehmensweiter Sicherheitsrichtlinien, da er als Master-Schlüssel sowohl die Remote-Anwender als auch die kritischen Datenbestände des Unternehmens schützt. Die Komplexität der Sicherheitsinfrastruktur und die daraus resultierenden Richtlinien bleiben den Mitarbeitern verborgen. Die Benutzer verbinden den SID 800 einfach mit einem USB-Anschluss und geben ihre PIN ein, um folgende Vorgänge auszuführen:

- Authentifizierung am PC bzw. Notebook
- Entsperrten eines verschlüsselten Festplattenlaufwerks
- Aufbau einer sicheren Netzwerkverbindung zu einem VPN oder WLAN-Access-Point
- Authentifizierung an der Unternehmensdomäne
- Verschlüsselung vertraulicher Dokumente und Dateien
- Signatur und Verschlüsselung von E-Mails

Außerdem müssen Endanwender nur die Authentifizierungskomponente entfernen, um das Notebook zu sperren oder sich abzumelden.

Flexible Lösung für verschiedene Zugangsdaten

Unternehmen müssen den geeigneten Zugangsdatentyp zum Schutz bestimmter Anwendungen flexibel auswählen können. Der SID 800 bietet diese Flexibilität durch die Unterstützung verschiedener Zugangsdaten, darunter:

- Einmalig gültige RSA SecurID-Passwörter, die sich alle 60 Sekunden ändern



- Digitale X.509-Zertifikate für Authentifizierung, Verschlüsselung und digitale Signaturen
- Benutzernamen und Passwortdaten für die Windows-Anmeldung, damit Unternehmen die starke Zwei-Faktor-Authentifizierung nutzen und ihre Passwortrichtlinien verstärken können, ohne die Infrastruktur oder Anwendergewohnheiten ändern zu müssen

Sicherer Datenzugriff durch integrierte Festplatten- und Dateiverschlüsselung

Durch die steigende Anzahl mobiler Mitarbeiter, die vertrauliche Daten auf Notebooks bei sich tragen, hat das Risiko von Datenverlusten zugenommen. Lösungen für Festplatten- und Dateiverschlüsselung verhindern den unberechtigten Zugriff auf vertrauliche Daten, die auf Festplattenlaufwerken von Notebooks gespeichert sind. Der SID 800 wurde von allen führenden Festplatten- und Dateiverschlüsselungsanbietern für starke Authentifizierung zertifiziert, um die schwächste Komponente - das Passwort - aus diesen Lösungen zu entfernen.

Branchenführende Lösung für einmalig gültige Passwörter

Die RSA SecurID-Authentifizierung stellt eine branchenführende Lösung für einmalig gültige Passwörter bereit, bei der alle 60 Sekunden ein anderer, eindeutiger Authentifizierungscode angezeigt wird. Der SID 800 kann entweder als herkömmlicher SecurID-Schlüsselanhänger (Token-Code wird vom Display der Authentifizierungskomponente abgelesen) oder als USB-Token verwendet werden, der den Anmeldeprozess automatisiert, indem der Token-Code über den USB-Anschluss übermittelt wird. In beiden Fällen muss der Anwender stets seine PIN eingeben, um zwei eindeutige Authentifizierungsfaktoren zu gewährleisten.

RSA SecurID ist in über 400 zertifizierten Anwendungen von Drittanbietern integriert. Dadurch sinken die Kosten für Inbetriebnahme und Bereitstellung, denn wichtige Anwendungen sind „RSA SecurID Ready“ - von vornherein für die Verwendung mit RSA SecurID-Technologie geeignet.

Authentifizierungslösungen für Ihre Anforderungen - jetzt und in Zukunft

Viele Unternehmen schützen durch ihre Sicherheitsstrategie zunächst die Remote-Anwender und fügen kurze Zeit später auch Schutzmaßnahmen für deren PCs und Notebooks hinzu. Dank der zahlreichen Funktionen des SID800 werden neue Anforderungen wie sicherer Webzugriff, SmartCard-Anmeldung, E-Mail-Signatur usw. durch ein einziges Gerät erfüllt.

Technische Daten

PHYSISCHE MERKMALE

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

Gewicht: 21g

Betriebstemperatur: -20°C bis 65°C

Batterielebensdauer: bis zu 5 Jahre

PKI UND SMARTCARD

SmartCard-Speicher: 64KB

FIPS 140-2 Level 3 (nur SmartCard)

Datenübertragungsrate: 129 Kbps

Zugangsdatenspeicher: X.509 v3-Zertifikate, sicherer Schlüsselspeicher und Microsoft Windows®-Zugangsdaten

Schlüsselerzeugung: RSA 1024-bit, DES/3DES, AES

RSA-Signatur: 1024-bit

Sicheres Hash-Verfahren: MD5, SHA-1, SHA-256

ANSI X9.31 PRNG

EINMALIG GÜLTIGE PASSCODES

Zeitabhängiges, einmalig gültiges RSA SecurID-Passwort

Verwendung durch Anschluss (USB) oder eigenständig (6-stellige Anzeige)

API-STANDARDS

PKCS11

MSCAPI

USB-SCHNITTSTELLE

USB 2.0 (CCID 1.0-kompatibel)

FÄLSCHUNGSSICHERHEIT

Konform zu ISO 13491-1; ISO DIS 13491-2 Anhang A, Abschnitt A.1.1, Punkt A1, A2 und A4

UNTERSTÜTZTE PLATTFORMEN

Windows XP/Server 2003, Windows Vista/Server 2008 (Versionen x86 und x64)

Weitere Informationen über RSA SecurID-Technologie und andere RSA SecurID-Authentifizierungskomponenten finden Sie im Internet unter: <http://www.rsa.com/node.asp?id=1156>.



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

The Security Division of EMC

©2005-2008 RSA Security Inc. Alle Rechte vorbehalten. RSA, SecurID und das RSA-Logo sind eingetragene Warenzeichen oder Warenzeichen von RSA Security, Inc. in den Vereinigten Staaten oder anderen Ländern. EMC ist ein eingetragenes Warenzeichen der EMC Corporation. Microsoft, Vista, XP und Windows sind eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den Vereinigten Staaten oder anderen Ländern. Alle weiteren angeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.

SID800 DS 0908