

RSA SecurID® On-Demand Authenticator

Authentifizierung mit „Zero-Footprint“ für Flexibilität und einfache Bereitstellung

Übersicht

- Bereitstellung einmalig gültiger Token-Codes per SMS oder E-Mail
- Standort- und zeitunabhängiger Zugriff
- Unterstützt zahlreiche Geschäftsanwendungen
- Ermöglicht Self-Service der Benutzer über den gesamten Token-Lebenszyklus

Vertrauenswürdige Benutzeridentitäten in einer unsicheren Welt

Die Identitätsprüfung umfasst alle Funktionen und Methoden zur Minimierung der Geschäftsrisiken, die mit Identitätsbetrug und Benutzerkontenmissbrauch verbunden sind. Durch die Identitätsprüfung schaffen Unternehmen mehr Vertrauen, da Benutzer mit zuverlässigen Identitäten auf flexible und sichere Weise mit Systemen interagieren und auf Informationen zugreifen können. Dadurch ergeben sich neue Möglichkeiten, den Umsatz zu steigern, die Kunden zufriedenzustellen und die Kosten im Griff zu behalten.

Beim RSA SecurID® On-Demand Authenticator handelt es sich um eine innovative Lösung, die Benutzern einen sicheren Netzwerkzugriff ohne im Vorfeld erteilte Zugangsdaten ermöglicht. Da kein physischer Hardware-Token ausgegeben und keine Software auf einem Notebook oder Smartphone installiert werden muss, sorgt die On-Demand-Authentifizierung für Flexibilität und einfache Bereitstellung, bietet aber gleichzeitig alle erforderlichen Sicherheitsvorkehrungen für eine starke Zwei-Faktor-Authentifizierung.

Der On-Demand Authenticator enthält einen Self-Service mit einer Web-URL, über die Benutzer einen Token-Code anfordern können. Der Benutzer ruft über einen PC mit Internet-

anschluss die Self-Service-URL auf und meldet sich dort wie gewohnt mit einem Benutzernamen und einer PIN an. Nach erfolgreicher Anmeldung kann er einen Token-Code anfordern, der auf sein SMS-fähiges Mobiltelefon gesendet werden soll. Der RSA® Authentication Manager generiert den 8-stelligen Token-Code und sendet ihn per SMS über das Mobilfunknetz auf das registrierte Mobilgerät des Benutzers. Nach dem Erhalt werden die PIN und der Token-Code als einmalig gültiges Passwort eingegeben, um sich am VPN, Webportal, an Citrix® oder einer anderen Anwendung anzumelden.

Die Bereitstellung kann statt per SMS auch per E-Mail erfolgen. Dies funktioniert wie zuvor beschrieben, außer dass der Token-Code an die sichere E-Mail-Adresse des Benutzers im Unternehmen gesendet wird.

Niedrigere Bereitstellungskosten durch Self-Service

Der On-Demand Authenticator basiert auf dem RSA® Credential Manager, der in die Managementkonsole des RSA Authentication Manager integriert ist. Mit den Funktionen für Self-Service und Workflow-Bereitstellung können IT-Administratoren eigene Prozesse und Sicherheitsmaßnahmen entwerfen und implementieren, so dass Benutzer Ihre Token selbst verwalten können, ohne dabei die Sicherheitsrichtlinien zu verletzen. Da die am häufigsten verwendeten Benutzerfunktionen automatisiert sind, sinken die Kosten für die Nutzung

RSA SecurID On-demand Authenticator

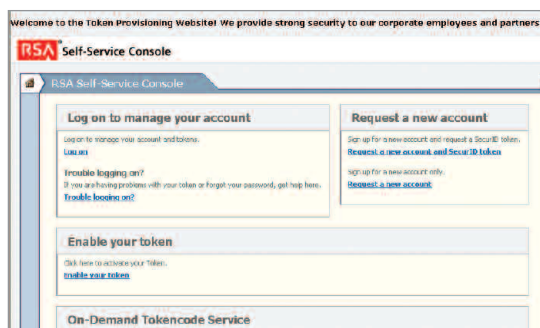


The Security Division of EMC

*Hinweis: Workflow-Bereitstellung ist nur mit der Enterprise-Server-Lizenz des RSA Authentication Manager verfügbar.



und der Aufwand für die laufende Verwaltung. Die Self-Service Funktionen des RSA Credential Managers ermöglichen Token-Benutzern die selbständige Durchführung aller gängiger Installations- und Verwaltungsaufgaben für Hardware-, Software- und On-Demand-Token ohne dabei auf ihr IT-Helpdesk zurückgreifen zu müssen. Das Self-Service-Modul dient nicht nur zur On-Demand-Authentifizierung, sondern hilft zudem allen Token-Benutzern (Hardware-, Software- und On-Demand-Token) bei der Durchführung gängiger Aufgaben und entlastet so die IT-Hotline.



Über einen Self-Service mit Web-URL können die Benutzer alle Aspekte von Token-Lebenszyklen verwalten.

Vielfältige Geschäftsanwendungen

Der On-Demand Authenticator ermöglicht den Einsatz verschiedenster Anwendungen zur Produktivitätssteigerung. So kann beispielsweise Subunternehmern und Lieferanten durch On-Demand-Authentifizierung ein temporärer Zugriff auf Unternehmensressourcen gewährt werden ohne die permanente Zuweisung von Hardware- oder Software-Zugangskomponenten. Bei der Erstellung von Business Continuity- und Notfallplänen kann berücksichtigt werden, dass mit dem RSA Authentication Manager schnell eine große Anzahl an Remote-Benutzern aktiv werden kann, ohne dass Token oder die ständige Mithilfe der IT-Abteilung erforderlich sind. RSA bietet sogar eine Business Continuity Option, mit der ein Unternehmen seine Serverlizenz und On-Demand-Authentifizierung vorübergehend erweitern kann, um eine hohe Anzahl an Benutzern bewältigen zu können, z.B. weil die Mitarbeiter nach einer Störung im Geschäftsbetrieb über Remote-Zugriff arbeiten müssen.

Sicherer Notfallzugriff auf das Netzwerk

Der On-Demand Authenticator bietet außerdem die Möglichkeit, einem Benutzer mit herkömmlichem Token einen „Notfallzugriff“ zu gewähren, wenn er seinen Token verlegt (z.B. zu Hause vergessen hat), ihn verloren oder die PIN vergessen hat.

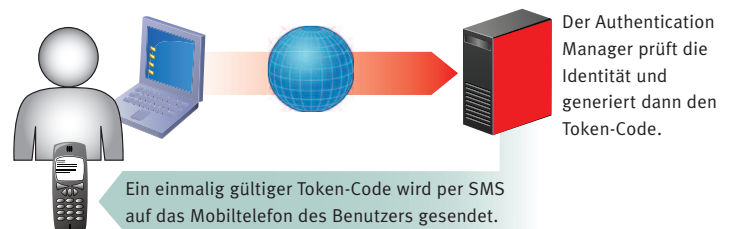
Mithilfe von Workflow-Prozessen können weitere Maßnahmen durch die IT-Mitarbeiter durchgeführt werden, z.B. zur Ausgabe eines neuen Hardware-Tokens an einen Benutzer, der seinen verloren hat. Da sich alle Informationen in einem gemeinsamen Datenspeicher befinden, können nach dem gemeldeten Verlust eines Hardware-Tokens automatisch die Zugangsdaten des Benutzers deaktiviert werden, um wertvolle Zeit zu sparen und möglichem Betrug vorzugreifen. Außerdem kann der Benutzer über den Self-Service u.a. folgende Funktionen nutzen: einen Token testen, ein Problem mit einem Token melden, eine PIN ändern und sein Benutzerprofil aktualisieren.

Globaler Mobilfunkversand

Die Verwendung der SMS-Funktion des On-Demand Authenticator erfordert die Zusammenarbeit mit einem SMS-Aggregator, damit die Nachrichten zum Gateway des Mobilfunkbetreibers geleitet werden können.

RSA hat die Managementkonsole mit einer SMTP Schnittstelle (Simple Mail Transfer Protocol) ausgestattet, um die einfache Anbindung an einen SMS-Provider sicher zu stellen. Für den Anbieter „Clickatell“ ist die Anbindung bereits vorkonfiguriert.

Der Benutzer fordert einen Token-Code über die Web-URL an, bei der er sich auf herkömmliche Weise mit Benutzername und PIN anmeldet.



Der Authentication Manager prüft die Identität und generiert dann den Token-Code.



©2007 RSA Security Inc. Alle Rechte vorbehalten. RSA, RSA Security, SecurID und das RSA Logo sind Warenzeichen oder eingetragene Warenzeichen von RSA Security Inc. in den Vereinigten Staaten und anderen Ländern. EMC ist ein eingetragenes Warenzeichen der EMC Corporation. Alle weiteren hier aufgeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.

SIDODA DS 0208