



The Security Division of EMC

RSA-Lösungskonzept – Technical Brief

## Neue Funktionen des RSA® Authentication Manager 7.1



Der RSA® Authentication Manager 7.1 ist die nächste Hauptversion der führenden Zwei-Faktor-Authentifizierungslösung von RSA, die ab dem 2. Quartal 2008 weltweit auf ausgewählten Software-Plattformen zur Verfügung steht. Diese Version bietet völlig neue Funktionen und positioniert die Plattform für neue Einsatzbereiche und Anwendungen.

---

## Drei zentrale Erweiterungen

---

### Business Continuity Option

Das Lösungsportfolio von RSA für seine Kunden geht mittlerweile über das „Token-Image“ hinaus und hat sich zur Risikomanagementlösung für strategische Informationen entwickelt. Die in Version 7.1 hinzugefügte Business Continuity Option (BCO) liefert die Antwort auf die Frage: „Wie kann ich meine Sicherheitsrichtlinien einhalten, auch wenn alle Mitarbeiter aufgrund von Störungen im Geschäftsbetrieb von zu Hause aus arbeiten müssen?“

### Erweiterte Authentifizierungsmethoden

In der neuen Version stehen neue Authentifizierungskomponenten für die Benutzer zur Verfügung, die zentral auf dem Server verwaltet werden.

### Verbesserte betriebliche Effizienz

Die Kunden erhalten eine Reihe von Tools, mit denen sie ihre betriebliche Effizienz steigern, die Bereitstellung vereinfachen und die laufenden Verwaltungskosten senken können.

---

## Highlights

---

### Verbesserte betriebliche Effizienz

Der RSA Authentication Manager 7.1 enthält eine Reihe von Funktionen, durch die die Lösung leichter zu verwalten ist, die Total-Cost-of-Ownership sinkt und die vorhandenen IT-Ressourcen effizienter genutzt werden können.

**Native LDAP-Unterstützung.** Die Version bietet eine umfassende native LDAP-Unterstützung für die direkte Integration mit Sun One™ und Active Directory®. **Dabei ist keine Synchronisierung mehr erforderlich**, und mehrere Identitätsquellen können als Datenspeicher dienen. Natives LDAP erfordert keine Änderungen am Datenbankschema.

**Web-basierte Verwaltung.** Die neue Benutzeroberfläche ist Browser-basiert und ermöglicht „Zero-Footprint“, d.h., auf dem PC des Administrators muss keine zusätz-

liche Client-Software installiert werden. Der RSA Authentication Manager 7.1 kann per Remote-Verbindung von beliebigen PCs aus verwaltet werden, die über einen Browser und einen Internetanschluss verfügen.

**Administrationsvollmacht für mehrere Ebenen.** Dieser Ansatz ermöglicht eine differenzierte Zugriffssteuerung bei der Administration bis auf Benutzer-, Gruppen- oder Richtlinien-Ebene. So können Investitionen in Administrationsressourcen optimal genutzt werden, und die Sicherheit steigt, da weniger Personen über den „Schlüssel zum Unternehmen“ verfügen.

**Clustering von Servern.** Clustering ermöglicht das Gruppieren von Authentication Manager Server-Systemen zu einer logischen Einheit. Dadurch lässt sich auf einfache und kostengünstige Weise die Skalierbarkeit und Leistung erhöhen. Außerdem wird durch zusätzliche Funktionen für die Ausfallsicherung eine maximale Betriebszeit gewährleistet.

– *nur mit Enterprise-Server-Lizenz verfügbar* –

**Snap-In für Microsoft® Management Console (MMC).** Bei Kunden, die ihre Verwaltung bereits hauptsächlich mit MMC durchführen, sorgt dieses Plug-In für Einheitlichkeit und Benutzerfreundlichkeit. Über MMC können Administratoren verschiedene grundlegende Verwaltungsaufgaben für Benutzer und Token durchführen, z.B. die Zuweisung oder Deaktivierung eines Tokens für einen Benutzer.

**RADIUS-Server.** Der in Version 7.0 nicht mehr verfügbare 802.1x RADIUS-Server wurde in 7.1 wieder aufgenommen. Die Verwendung des RADIUS-Servers sorgt für niedrigere Kosten im Vergleich zu den Lösungen anderer Anbieter. Da der RADIUS-Server vollständig in die Managementkonsole integriert ist, sind die Einrichtung und laufende Verwaltung ein Kinderspiel.

**RSA® Credential Manager.** Der Ersatz für den RSA® Deployment Manager (Web Express) heißt RSA Credential Manager. Dieses Produkt ist in die Benutzeroberfläche des Authentication Manager integriert, erfordert keine eigene Installation und bietet umfassendere Funktionen als der Deployment Manager. Dazu gehören:

– **Self-Service.** Über die konfigurierbare Self-Service-Konsole können die Benutzer eine Reihe von Services eigenständig anfordern, z.B. die Ausstellung von

On-Demand-Token-Codes für den Notfallzugriff. Durch das Self-Service-Modul kann die Anzahl der Anrufe beim IT-Helpdesk deutlich gesenkt werden, da die Benutzer den gesamten Token-Lebenszyklus selbst verwalten dürfen.

- **Workflow-Bereitstellung.** Administratoren können Prozesse erstellen, durch die Anfragen genehmigt und Zugangsdaten ausgegeben werden (mit Enterprise-Server-Lizenz verfügbar).

### Erweiterte Authentifizierungsmethoden

Der RSA Authentication Manager 7.1 unterstützt die herkömmlichen Zugangsdaten der früheren Versionen und bietet gleichzeitig neue Authentifizierungskomponenten für Benutzer, um eine flexible Bereitstellung und niedrigere Verwaltungskosten zu ermöglichen. Alle Methoden werden weiterhin über die Administrationskonsole zentral verwaltet und unterstützt.

**On-demand Authenticator.** Der RSA SecurID® On-demand Authenticator ist eine Methode für Zugangsdaten, die ab Version 7.1 zur Verfügung steht. Dabei werden Token-Codes per SMS oder E-Mail an den Benutzer gesendet, sodass kein physischer Token ausgegeben und keine Software auf einem Notebook oder Smartphone installiert werden muss. Bei der On-Demand-Authentifizierung gibt es keine Ablaufdaten.

**Dynamische Bereitstellung von Seed-Datensätzen (CT-KIP).** Beim Cryptographic Token Key Initialization Protocol (CT-KIP) handelt es sich um ein Client-Server-Protokoll, das eine schnellere Konfiguration von Software-Token ermöglicht. Durch CT-KIP können sowohl der Client als auch der Server einen eindeutigen Identifikator bzw. eine Seed-Datei generieren, die zur Authentifizierung des Benutzers am Server verwendet werden kann. So müssen keine Seed-Dateien über das Netzwerk an Remote-Benutzer gesendet werden, sodass Software-Token nahtloser und schneller genutzt werden können.

**Integrierte Managementfunktion für globales Messaging.** Das Versenden einer großen Anzahl an SMS-Nachrichten an Benutzer 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.

### Business Continuity Option

Durch die neue Business Continuity Option in Version 7.1 kann die SecurID-Authentifizierung noch einfacher in die organisatorische Planung für unerwartete Geschäftsausfälle eingebunden werden.

**Mit der Lizenzierungsfunktion der Business Continuity Option** kann ein Kunde eine Serverlizenz für einen bestimmten Zeitraum vorübergehend erweitern, um eine hohe Anzahl an Remote-Benutzerzugriffen bewältigen zu können, z.B. weil die Mitarbeiter nach einer Störung im Geschäftsbetrieb von zu Hause aus arbeiten. Die neue Lizenzierungsfunktion darf in jeder Lizenzlaufzeit maximal sechs Mal für einen Zeitraum von jeweils 60 Tagen verwendet werden. Die Lizenzlaufzeit der BCO beträgt 3 Jahre.

Durch die Business Continuity Option kann die Serverlizenz erweitert und eine vordefinierte Anzahl an On-Demand-Authentifizierungskomponenten für RSA SecurID verwendet werden. Beispiel: Ein Kunde erwirbt eine BCO-Lizenz für 1.000 Arbeitsplätze. Wenn die BCO in Anspruch genommen wird, werden sofort weitere 1.000 Arbeitsplätze in Form von On-Demand-Authentifizierung verfügbar. Die Bereitstellung übernehmen die Benutzer selbst mithilfe des Self-Service-Moduls des RSA Credential Manager (im Lieferumfang enthalten), damit sie eigenständig die Arbeit aufnehmen können, ohne den IT-Helpdesk mit Anfragen zu überhäufen.

---

### Neue Anwendungsmöglichkeiten

---

Durch alle diese Anwendungen und Funktionen kann der RSA Authentication Manager ganz neu verwaltet und genutzt werden. So sorgt z.B. die neue On-Demand-Authentifizierung zusammen mit den Self-Service-Tools für die Benutzer dafür, dass ein weiterer Kreis an Nutzern sicheren Zugriff erhalten kann, zum Beispiel:

**Zugriff für Subunternehmer und Lieferanten.** Viele Unternehmen haben Mühe, ihren temporären Mitarbeitern, Subunternehmern und Geschäftspartnern Zugriff auf Netzwerkressourcen zu gewähren. Die Ausgabe von On-Demand-Authentifizierungskompo-

nenen über das Self-Service-Modul stellt eine optimale Lösung zur vorübergehenden Bereitstellung von Zugangsdaten dar, ohne dass Hardware- oder Software-Token erforderlich sind. Außerdem können spezielle Workflows erstellt werden, um für jede dieser Benutzerkategorien eine Genehmigung durch eine verantwortliche Person des Geschäftsbereichs anzufordern und dadurch die Sicherheit zu erhöhen.

**Ergebnis:** Schnellere Integration von Subunternehmern und Lieferanten, niedrigere Implementierungskosten, weniger Verluste durch nicht zurückgegebene Token.

**Zugriff für Gelegenheitsbenutzer.** Viele Mitarbeiter reisen wenig oder arbeiten selten von zu Hause aus, sodass sie keinen herkömmlichen Token benötigen. Wenn diese Situationen aber doch eintreten, müssen die Benutzer durch einen schnellen Prozess unterstützt werden, den sie selbst initiieren können. Die neuen Funktionen des Authentication Manager 7.1 sorgen in solchen Fällen für einen nahtlosen Ablauf.

**Ergebnis:** Die Richtlinie der starken Zwei-Faktor-Authentifizierung wird eingehalten, und jeder Benutzer wird durch einen etablierten Prozess unterstützt.

**Self-Service-Unterstützung für „Vielnutzer“.** Ein Geschäftsreisender vergisst seinen Token zu Hause. Ein anderer muss seine PIN zurücksetzen. Wieder ein anderer möchte seinen Hardware-Token testen oder neu synchronisieren. Normalerweise würde jeder dieser Fälle zu einem Anruf beim IT-Helpdesk führen, doch in Version 7.1 des RSA Credential Manager bekommen die Benutzer die notwendigen Tools an die Hand, um diese Aufgaben selbst durchzuführen.

**Ergebnis:** Produktivitätssteigerung für den Benutzer und Produktivitätssteigerung und Kosteneinsparung beim IT-Helpdesk.

**Planung der Business Continuity.** Viele Unternehmen stehen vor der Herausforderung, dass sie einen Notfall- oder Wiederherstellungsplan für den Fall erstellen müssen, dass alle Mitarbeiter per Remote-Verbindung auf das Netzwerk zugreifen. Dabei müssen die Sicherheitsrichtlinien aber auch für diejenigen Benutzer eingehalten werden, die keine Token erhalten haben. Die neue Business Continuity Option bietet die Lösung für dieses Problem.

**Ergebnis:** Die Sicherheitsrichtlinien werden selbst während einer Störung des Geschäftsbetriebs eingehalten.

### Verfügbarkeit und Plattformunterstützung

Der RSA Authentication Manager 7.1 wird ab dem 2. Quartal 2008 überall erhältlich sein. Zunächst steht die Lösung auf den folgenden Plattformen zur Verfügung: Windows®, Red Hat™ Linux und Sun Solaris™. Die Unterstützung weiterer Plattformen, z.B. der RSA SecurID Appliance, ist für die nächste Version geplant.

## RSA – Ihr vertrauenswürdiger Partner

RSA, The Security Division of EMC, ist der führende Anbieter von Sicherheitslösungen, um Geschäftsprozesse zu beschleunigen und zu optimieren. RSA unterstützt weltweit operierende Unternehmen bei der Bewältigung ihrer anspruchsvollen und sensiblen Sicherheitsanforderungen. Der Sicherheitsansatz von RSA ist hier fokussiert auf die Informationen, um ihren Schutz und die Vertraulichkeit über die gesamte Lebensdauer zu gewährleisten – unabhängig davon, wohin sie bewegt werden, wem sie zugänglich gemacht werden oder wie sie verwendet werden.

RSA bietet führende Lösungen in den Bereichen Identitätssicherung und Zugriffskontrolle, Kryptographie und Schlüssel-Management, Compliance- und Security-Information-Management sowie Fraud Protection. Diese Lösungen schaffen Vertrauen bei Millionen Nutzern von digitalen Identitäten, bei ihren Transaktionen, die sie täglich ausführen, und bei den Daten, die erzeugt werden. Weitere Informationen finden Sie unter [www.RSA.com](http://www.RSA.com) und [www.emc2.de](http://www.emc2.de).



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

©2008 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. Windows und Microsoft sind Warenzeichen oder eingetragene Warenzeichen der Microsoft Corporation 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.

AS71 SB 0108