

## Sichern Sie sich ab mit Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung mit RSA SecurID® basiert auf etwas, das Sie kennen (Passwort oder PIN) und auf etwas, das Sie besitzen (Authentifikator). Sie erhalten eine wesentlich sicherere Anwenderauthentifizierung als bei der Nutzung immer wieder verwendeter Passwörter.

- Verfügbar als Hardware, App und per SMS (on-demand)
- 20 Jahre Innovation im Bereich Sicherheit

CuC implementiert RSA Lösungen seit vielen Jahren und in allen Größenordnungen. Fragen Sie uns zu Referenzinstallationen (Kontakt oben rechts).

RSA bietet Unternehmen eine breite Palette von Optionen für die Anwenderauthentifizierung, damit Anwender eindeutig identifiziert werden können, bevor diese über folgende Kanäle auf geschäftskritische Daten und Anwendungen zugreifen können:

- VPNs und WLANs
- E-Mail
- Intranets und Extranets
- Microsoft® Windows®-Desktops
- Web-Server
- Andere Netzwerkressourcen



Sicher, bewährt und bekannt sind vielen die klassischen Hardware-Token von RSA als starke Anmeldung am internen Portal-System für die Mitarbeiter. Die vom Token alle 60 Sekunden neu generierte PIN ergänzt hier das statische Passwort und den Benutzernamen des Mitarbeiters mehrere Faktoren für Ihre Sicherheit. Mittlerweile ist dieser Mechanismus auch ohne die Ausgabe von Hardware oder der Installation einer App auf mobilen Devices verfügbar: Per SMS.

## RSA SecurID® On-Demand Authenticator

## 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 Internetanschluss Internetanschluss 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. Neben diesen klassischen Anmeldemethoden bietet RSA seit dem Frühjahr Anfang 2011 noch eine weitere Variante der starken Authentisierung an, bei der nicht in jedem Fall die Eingabe einer zusätzlichen PIN notwendig ist:

## RSA Authentication Manager Express (AMX)

Benutzerfreundlichkeit, Verwaltung: Die komfortable Sicherheitslösung RSA Authentication Manager Express erfüllt die Ansprüche von KMUs in genau diesen drei Punkten. Es ist eine starke Multi-Faktor-Authentifizierung für bis zu 2500 Benutzer, die den Zugriff auf geschützte Anwendungen und Daten absichert und mit führenden SSL-VPNs und webgestützten Anwendungen funktioniert.

Der AMX nutzt das RSA-Verfahren der risikobasierten Authentifizierung, deren Herzstück eine ausgefeilte sogenannte Risk-Engine ist. Diese verfolgt jeden Anmeldeversuch und jede Online-Aktivität in Echtzeit, wertet Dutzende Risikoindikatoren aus und weist jeder Anfrage eine bestimmte Risikostufe zu. Zur Ermittlung der Risikostufe berücksichtigt die Engine Faktoren aus verschiedenen Kategorien:

- Wissen: Benutzername und Passwort eines Benutzers
- Besitz: Laptop oder Desktop eines Benutzers
- Benutzerverhalten

Auf Wunsch berücksichtigt die RSA Risk-Engine dabei die eigenen Sicherheitsrichtlinien eines Unternehmens; von niedrig bis hoch sind verschiedene Risikostufen definierbar.

Diese Risikostufen lassen sich im RSA Authentication Manager Express bestimmten Benutzergruppen zuweisen und mit der Einhaltung jeweils unterschiedlicher Sicherheitsrichtlinien verknüpfen. So kann z. B. für die Mitarbeiter eines Unternehmens eine höhere Toleranz gelten als für Kunden oder Geschäftspartner. Entspricht die Risikostufe eines Zugriffsversuchs den Richtlinien des Unternehmens, wird der Benutzer umgehend authentifiziert. Ermittelt der AMX jedoch eine höhere Risikostufe, fordert das System vom Benutzer weitere Identitätsbelege.

## **Ergänzende Authentifizierung für Zugriffsversuche mit hohem Risiko**

Entspricht ein Zugriffsversuch nicht der definierten Sicherheitsstufe, fordert der AMX vom Benutzer weitere Identitätsbelege an, insbesondere wenn die Anmeldung per Fernzugriff von einem dem System bisher unbekanntem Gerät aus erfolgt. Hierfür bietet die Lösung zwei Methoden: den Versand eines Berechtigungscode per SMS auf das Handy des Benutzers oder das Stellen persönlicher Fragen.

### **Berechtigungscode per SMS**

Bei Zugriffsversuchen mit hoher Risikostufe erfolgt ein weiterer Authentifizierungsschritt, bei dem ein Berechtigungscode per SMS verschickt wird. Der Benutzer folgt einem einfach zu verstehenden Ablauf, um seine Identität zu belegen.

Zuerst fordert das System ihn auf, die beim Anlegen seines Benutzerkontos gewählte PIN einzugeben. Darauf schickt ihm das System auf das zum Erhalt von Nachrichten angegebene Handy eine SMS mit einem achtstelligen Einmalpasswort, das er im Browser eingeben muss. Nach Verifizierung dieses Passworts erhält der Benutzer Zugriff. Der Versand eines solchen Einmalpassworts ist auch an eine dem System vorab bekanntgegebene E-Mail-Adresse möglich.

Der Vorteil dieses Verfahrens ist seine universelle Verwendbarkeit mit jedem Handy, ohne dass eine spezielle Hardware angeschafft oder Software installiert werden müsste.

### **Persönliche Fragen**

Dies sind Fragen, die dem Benutzer üblicherweise beim Anlegen seines Benutzerkontos gestellt werden, beispielsweise im Zuge der Einführung eines starken Authentifizierungsverfahrens in einem Unternehmen. Bei der Authentifizierung wird dem Benutzer immer nur eine Auswahl dieser Fragen gestellt, um das Risiko zu minimieren, dass Unbefugte die Fragen und Antworten des betreffenden Benutzers erfahren. Der RSA Authentication Manager Express lässt außerdem das Anlegen eines eigenen Fragenkatalogs zu.