



The Security Division of EMC

Skrócony opis techniczny

## Co nowego w pakiecie RSA® Authentication Manager 7.1?



RSA® Authentication Manager 7.1 to kolejna wersja flagowego rozwiązania firmy RSA do dwuskładnikowego uwierzytelniania od drugiego kwartału 2008 r. W wersji tej wprowadzono nowy zestaw funkcji, a także umożliwiono zastosowanie Authentication Manager platformy uwierzytelniającej dla nowych zastosowań.

---

## Trzy główne obszary ulepszeń funkcjonalnych

---

### Opcja ciągłości biznesowej

Propozycja firmy RSA jest obecnie czymś więcej niż ofertą „dostawcy tokenów”. Stała się dla naszych klientów rozwiązaniem do zarządzania ryzykiem związanym z informacjami strategicznymi. Opcja ciągłości biznesowej (ang. Business Continuity Option – BCO) wprowadzona w wersji 7.1 to odpowiedź na pytanie: „W jaki sposób można zapobiec osłabieniu polityki bezpieczeństwa w sytuacji, w której wszyscy pracownicy muszą pracować w domu na skutek przerwania działań w firmie?”.

### Bogatszy wybór metod uwierzytelniania

Nowa wersja oprogramowania zwiększa liczbę rodzajów mechanizmów uwierzytelniających, które można wdrożyć po stronie użytkowników, oraz pozwala zarządzać nimi centralnie z poziomu serwera.

### Zwiększona wydajność operacyjna

Klienci otrzymają zestaw narzędzi, które zwiększą wydajność operacyjną, uproszczą wdrożenia oraz obniżą bieżące koszty zarządzania.

---

## Najważniejsze cechy

---

### Zwiększona wydajność operacyjna

RSA Authentication Manager 7.1 zawiera pakiet oczekiwanych przez klientów funkcji, które ułatwiają zarządzanie oprogramowaniem, obniżają koszty użytkowania i zapewniają wykorzystanie istniejących zasobów informatycznych.

**Bezpośrednia obsługa LDAP.** Nowa wersja zapewnia rzeczywiście obsługę LDAP, co umożliwia bezpośrednią integrację z rozwiązaniami Sun One™ oraz Active Directory®. Koniec z synchronizacją. Wybrana liczba źródeł tożsamości może pełnić rolę repozytoriów. Bezpośrednia obsługa LDAP nie wymaga wprowadzania jakichkolwiek zmian w schemacie bazy danych.

**Zarządzanie z poziomu przeglądarki internetowej.** Nowy interfejs administracyjny jest obsługiwany z poziomu przeglądarki internetowej i nie wymaga instalowania oprogramowania klienckiego na komputerze PC administratora. Rozwiązaniem RSA Authentication Manager 7.1 można zarządzać zdalnie, korzystając z

dowolnego komputera PC z przeglądarką WWW i dostępem do Internetu.

**Delegowana administracja na wielu poziomach.** Funkcja ta umożliwia precyzyjne definiowanie uprawnień dostępu administracyjnego, aż do poziomu użytkownika/grupy lub reguły. Rozwiązanie umożliwia maksymalnie wykorzystanie inwestycji w zasoby, a także zwiększa bezpieczeństwo, gdyż mniej ludzi dysponuje „kluczami do fortecy”.

**Łączenie serwerów w klastry.** Klastry umożliwiają połączenie węzłów serwerowych w jedną grupę, widoczną jako pojedynczy element. Dzięki takiemu rozwiązaniu można łatwo i niedrogo zwiększyć możliwości skalowania oraz wydajność. Zwiększa się również odporność systemu, co uzyskano dzięki dodatkowej warstwie zabezpieczeń przed awariami, zapewniającej maksymalny czas ciągłego działania. — *funkcja dostępna wyłącznie przy zakupie licencji dla serwerów korporacyjnych* —

### Integracja z konsolą zarządzania Microsoft (MMC).

Klienci wykorzystujący konsolę MMC jako główne narzędzie do zarządzania mogą skorzystać z przystawki programowej, która ułatwi ich pracę i zapewni spójność oprogramowania. Takie rozwiązanie umożliwia wykonywanie szeregu podstawowych zadań związanych z zarządzaniem użytkownikami oraz tokenami z poziomu konsoli MMC, na przykład przypisywanie lub wyłączanie tokenu użytkownika.

**Serwer RADIUS.** Serwer RADIUS 802.1x, nieobecny w wersji 7.0, powrócił w wersji 7.1. Obecność wbudowanego serwera RADIUS obniża koszty w porównaniu z wdrożeniem rozwiązań innych firm, a pełna integracja tej funkcji w konsoli zarządzania znacznie ułatwia konfigurację i bieżące zarządzanie.

**RSA® Credential Manager.** Funkcja RSA Credential Manager stanowi zamiennik rozwiązania RSA® Deployment Manager (Web Express). Ścisłe połączenie tej funkcji z interfejsem zarządzania Authentication Manager eliminuje konieczność oddzielnego instalowania oprogramowania, a także zapewnia funkcje wykraczające poza możliwości programu Deployment Manager. Są to:

- **Samoobsługa.** Konsola samoobsługowa z możliwością konfiguracji pozwala użytkownikom na wysyłanie żądań różnych usług, w tym wydania na żądanie kodów umożliwiających dostęp w trybie wyjątkowym. Moduł samoobsługi pozwala znacznie zmniejszyć liczbę zapytań skierowanych do stanowiska pomocy działu informatycznego, ponieważ użytkownicy mają możliwość samodzielnego zarządzania wszystkimi aspektami funkcjonowania swoich tokenów.

- **Organizacja przepływu pracy.** Administratorzy mogą tworzyć procesy do zatwierdzania żądań i wydawania uwierzytelnień (opcja dostępna tylko z licencją dla serwera korporacyjnego).

### **Bogatszy wybór metod uwierzytelniania**

Oprócz obsługi tradycyjnych danych uwierzytelniających z poprzednich wersji, RSA Authentication Manager 7.1 po raz pierwszy obsługuje nowe elementy uwierzytelniające użytkowników, które umożliwiają tworzenie elastycznych wdrożeń i obniżenie kosztów zarządzania. Wszystkie metody nadal są zarządzane centralnie, a ich obsługa odbywa się za pomocą konsoli administracyjnej.

**On-demand Authenticator.** Wraz z premierą wersji 7.1 udostępniono nowe rozwiązanie uwierzytelniające, RSA SecurID® On-demand Authenticator. Funkcja dostarcza kody dostępu za pomocą wiadomości SMS lub e-mail. Nie wymaga przypisywania fizycznych tokenów ani instalowania oprogramowania na komputerze przenośnym czy w smartfonie. Elementy uwierzytelniające na żądanie nie ulegają przedawnieniu.

**Dynamiczne udostępnianie wartości początkowej generatora liczb losowych (CT-KIP).** Protokół inicjowania klucza szyfrowania tokenu jest protokołem typu klient-serwer, który umożliwia szybszą konfigurację tokenów programowych. Podczas korzystania z CT-KIP zarówno klient, jak i serwer mogą generować niepowtarzalny identyfikator, czyli plik wartości początkowej generatora liczb losowych, który może służyć do uwierzytelnienia użytkownika na serwerze. Plik taki nie musi być wysyłany przez sieć do zdalnego użytkownika. Dzięki temu wdrażanie tokenów programowych staje się płynnym i krótkim procesem.

**Wbudowana obsługa zarządzania rozwiązaniami globalnego dostawcy usług wiadomości Clickatell™.** Wysyłanie dużych ilości wiadomości SMS do użytkowników wymaga nawiązania współpracy z dostawcą usług SMS, który skieruje je do bramy operatora. Konsola zarządzania RSA zawiera wbudowany interfejs współpracy z firmą Clickatell – globalnym operatorem obsługującym wiadomości wysyłane na telefony komórkowe i mającym dostęp do ponad 600 sieci w prawie 200 krajach.

### **Opcja ciągłości biznesowej**

Wraz z premierą wersji 7.1 pojawiła się nowa opcja ciągłości biznesowej (BCO). Ułatwia ona wykorzystanie uwierzytelnienia SecurID w planowaniu na wypadek nieoczekiwanego przerwania operacji firmy

**Opcja ciągłości biznesowej** oraz jej funkcja licencjonowania umożliwiają klientom tymczasowe rozszerzenie licencji serwerowej, dzięki czemu mogą oni obsłużyć napływ dużej liczby użytkowników dostępu zdalnego, na przykład w przypadku zakłócenia normalnej pracy, kiedy personel musi pracować z domu. Nową funkcję licencjonowania można przywołać maksymalnie sześć razy w każdym okresie trwania licencji, każdorazowo na 60 dni. Okresy ważności licencji BCO trwają 3 lata.

Opcja ciągłości biznesowej rozszerza licencję serwera i umożliwia obsłużenie większej, określonej wcześniej liczby elementów uwierzytelniających na żądanie RSA SecurID. Jeśli na przykład klient nabył licencję BCO na 1000 stanowisk, to uaktywnienie opcji BCO spowoduje udostępnienie następnych 1000 stanowisk poprzez elementy uwierzytelniające na żądanie. Wdrażanie odbywa się na bieżąco za pomocą modułu samoobsługi wbudowanego w rozwiązanie RSA Credential Manager. Dzięki temu użytkownicy mogą samodzielnie uzyskać dostęp do systemu, bez konieczności kierowania dużej ilości żądań do stanowiska pomocy działu informatycznego.

---

### **Nowe możliwości dla aplikacji**

---

Nowe aplikacje i funkcje to także nowy sposób wdrażania i zarządzania produktem RSA Authentication Manager. Na przykład wprowadzenie elementów uwierzytelniających na żądanie wraz z narzędziami samoobsługi użytkownika umożliwia obsłużenie większej liczby osób korzystających z oprogramowania. Poniżej podano kilka przykładów.

Obsługa pracowników tymczasowych i dostawców. Wiele organizacji boryka się z problemami dotyczącymi obsługi tymczasowych pracowników, wykonawców oraz goszczących w firmie partnerów, którzy wymagają dostępu do zasobów sieciowych. Uwierzytelnianie na żądanie poprzez moduł samoobsługi może być idealnym sposobem na tymczasowe przyznawanie uwierzytelnień, bez potrzeby udostępniania tokenów programowych lub sprzętowych. Istnieje również możliwość takiego dostosowania przepływu pracy, aby obsłużył każdą z tych kategorii użytkowników z zatwierdzeniem odbywającym się w systemach zaplecza dla większego bezpieczeństwa.

**Wynik:** szybsze wdrażanie wykonawców/dostawców, niższe koszty wdrażania, zminimalizowane straty wynikające z nieodzyskanych tokenów.

Obsługa grupy użytkowników okazjonalnych. Wielu pracowników nie podróżuje lub nie pracuje zdalnie na tyle często, aby mieć tradycyjny token. Jeśli jednak wystąpi taka potrzeba, w firmie powinien istnieć szybki, samoczynnie uruchamiany mechanizm obsługi tego typu użytkowników. Nowe funkcje rozwiązania Authentication Manager w wersji 7.1 zapewniają płynną obsługę tego typu sytuacji.

**Wynik:** system wymusza strategię dwuskładnikowe uwierzytelnianie, a także zapewnia proces obsługi każdego użytkownika.

Samoobsługa dla istniejących „użytkowników zaawansowanych”. Pracownik podróżujący w interesach przez przypadek zostawia token w domu. Inny potrzebuje nowego kodu PIN. Jeszcze inny chce przetestować lub ponownie zsynchronizować token sprzętowy. Takie potrzeby zwykle skutkują telefonem do stanowiska pomocy działu informatycznego, ale w wersji 7.1 funkcja zarządzania danymi uwierzytelniania RSA Credential Manager umożliwia użytkownikom przejście kontroli nad dostępnymi narzędziami i własnoręczne wykonywanie tych działań.

**Wynik:** zwiększenie produktywności użytkownika, a także zwiększenie produktywności i obniżenie kosztów stanowiska pomocy działu informatycznego.

Planowanie ciągłości biznesowej. Wiele organizacji często ma problem z wdrożeniem planu na wypadek awarii lub katastrofy, przez którą wszyscy pracownicy potrzebują zdalnego dostępu do sieci, bez zmniejszania poziomu bezpieczeństwa użytkowników nieposiadających tokenów. Nowa opcja ciągłości biznesowej stanowi rozwiązanie tego problemu.

**Wynik:** polityka bezpieczeństwa pozostaje aktywna nawet podczas przerwy w działaniu firmy.

## Dostępność i obsługiwane systemy operacyjne

Rozwiązanie RSA Authentication Manager 7.1 zostanie wprowadzone na rynek w drugim kwartale 2008 r. W dniu premiery oprogramowanie będzie dostępne dla systemów: Windows®, Red Hat™ Linux oraz Sun Solaris™. Obsługa pozostałych systemów, w tym obsługa dla urządzenia RSA SecurID Appliance, zostanie wprowadzona w następnym wydaniu.

## RSA – zaufany partner

RSA, oddział ds. zabezpieczeń firmy EMC, to czołowy dostawca rozwiązań zabezpieczających, które przyspieszają pracę w firmach oraz pomagają czołowym organizacjom na świecie osiągnąć sukces poprzez rozwiązywanie ich najbardziej złożonych i krytycznych problemów z bezpieczeństwem. Podejście do bezpieczeństwa firmy RSA koncentruje się na dostępie do informacji, oraz ochronie jej spójności i poufności przez cały okres jej istnienia – niezależnie od tego, gdzie jest, kto jej używa i w jaki sposób.

RSA oferuje najlepsze w branży rozwiązania do określania tożsamości i kontroli dostępu, zapobiegania utracie danych i ich szyfrowaniu, zarządzaniu zgodnością i bezpieczeństwem informacji, a także ochrony przed oszustwami. Rozwiązania te dają poczucie bezpieczeństwa milionom użytkowników, zarówno podczas przeprowadzania transakcji, jak i w trakcie generowania danych. Więcej informacji można znaleźć pod adresem [www.RSA.com](http://www.RSA.com) oraz [www.EMC.com](http://www.EMC.com).



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

The Security Division of EMC

©2008 RSA Security Inc. Wszelkie prawa zastrzeżone. RSA, RSA Security, SecurID i logo RSA są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub w innych krajach. Windows i Microsoft są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach. EMC jest zastrzeżonym znakiem towarowym firmy EMC Corporation. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.

AS71 SB 0108