

RSA SecurID® On-demand Authenticator

Elastyczność i łatwość wdrożenia — mobilne rozwiązanie
uwierzytelniające

Najważniejsze informacje

- Jednorazowy kod dostępu poprzez SMS lub e-mail
- Dostęp w dowolnym miejscu i czasie
- Różnorodność zastosowań biznesowych
- Samoobsługowy interfejs użytkownika

Gwarancja tożsamości użytkownika w świecie usług elektronicznych

Gwarantowanie tożsamości użytkownika to zestaw funkcji i metod, które minimalizują ryzyko biznesowe związane z podszywaniem się pod uprawnionego użytkownika i niewłaściwym korzystaniem z konta. Zwiększa ono zaufanie do przedsiębiorstwa lub instytucji, umożliwiając uprawnionym użytkownikom swobodną i bezpieczną interakcję z systemami oraz dostęp do informacji, co daje nowe możliwości generowania przychodów, spełniania oczekiwań klientów i kontrolowania kosztów. RSA SecurID® On-demand Authenticator to nowatorskie rozwiązanie, które umożliwia użytkownikom bezpieczny dostęp do sieci bez wcześniej przypisanych danych uwierzytelniających. Metoda uwierzytelniania na żądanie nie wymaga fizycznego tokenu ani instalowania oprogramowania na laptopie lub w telefonie. Umożliwia elastyczne, łatwe wdrożenie z zachowaniem wszystkich zasad bezpieczeństwa wymaganych przy dwuskładnikowym uwierzytelnianiu.

On-demand Authenticator wykorzystuje samoobsługową stronę web, na której użytkownik może zgłosić żądanie wysłania kodu. Z komputera podłączonego do internetu użytkownik może uzyskać dostęp do samoobsługowej strony web za pomocą tradycyjnego logowania i numeru PIN. Po pomyślnym przejściu tego etapu może zgłosić żądanie wygenerowania kodu i przesłania go do swojego urządzenia mobilnego obsługującego wiadomości SMS. RSA® Authentication Manager generuje kod analogiczny do tradycyjnego kodu SecurID (8-cyfrowy) i wysyła go do zarejestrowanego

urządzenia mobilnego jako wiadomość SMS za pośrednictwem publicznej sieci telefonii komórkowej. Po odebraniu tej wiadomości użytkownik wprowadza PIN i kod jako jednorazowe hasło (one-time password — OTP) w procesie logowania do sieci VPN, portalu internetowego, systemu Citrix® lub innej aplikacji.

Dostępna jest również metoda dostarczania kodu pocztą elektroniczną zamiast w wiadomości SMS. Działa ona podobnie, z tą różnicą, że hasło jednorazowe jest przesyłane na bezpieczny korporacyjny adres e-mail, gdzie może być odczytane za pomocą urządzenia mobilnego.

Niskie koszty wdrożenia dzięki samoobsłudze

Mechanizmem, który umożliwia uwierzytelnianie na żądanie, jest moduł RSA® Credential Manager, dostępny w konsoli administracyjnej oprogramowania RSA Authentication Manager. Za pomocą narzędzi konfiguracyjnych administrator może definiować procedurę rejestracji użytkowników (obejmującą m.in. samoobsługę) oraz wdrażać procesy i zabezpieczenia zapewniające użytkownikom opcje niezbędne do zarządzania cyklem życia tokenów, z zachowaniem pełnej zgodności z zasadami bezpieczeństwa obowiązującymi w danej instytucji. Umożliwia to zmniejszenie kosztów wdrożenia i bieżących kosztów administracyjnych dzięki całkowitemu zautomatyzowaniu najczęściej wykorzystywanych czynności użytkownika. Użytkownicy, którzy korzystają z samoobsługi, rzadziej kontaktują się z personelem wsparcia IT.*

RSA SecurID® On-demand Authenticator

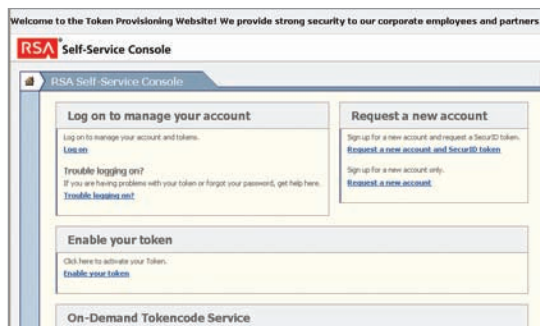


The Security Division of EMC

*Opcja jest dostępna w ramach Enterprise Service License systemu RSA Authentication Manager.



RSA Credential Manager jest wbudowany w konsolę administracyjną programu RSA Authentication Manager, co upraszcza jego instalację, dostęp i użytkowanie. Oprócz uwierzytelniania na żądanie, moduł samoobsługowy może być wykorzystywany jako pomoc dla użytkowników wszystkich tokenów SecurID — sprzętowych, programowych i na żądanie. Ułatwia to wykonywanie typowych zadań bez potrzeby kontaktu ze personelem wsparcia IT



Na samoobsługowej stronie internetowej użytkownicy mogą zarządzać wszystkimi aspektami cyklu życia tokenów

Mnogość zastosowań biznesowych

On-demand Authenticator może mieć wiele różnych zastosowań zwiększających produktywność użytkowników. Ułatwia na przykład elastyczne wsparcie dużej liczby użytkowników, którzy potrzebują bezpiecznego zdalnego dostępu, ale nie korzystają z sieci na tyle często, aby uzasadnione było wydawanie każdemu z nich tokenów sprzętowych lub programowych. Współpracownikom i konsultantom zewnętrznym można przyznawać czasowy dostęp do zasobów korporacyjnych. RSA Authentication Manager może szybko przydzielić dostęp dużej liczbie użytkowników zdalnych, bez używania tradycyjnych tokenów lub angażowania działu informatyki na każdym etapie. Można to wykorzystać przy tworzeniu planów ciągłości operacyjnej lub planów działania w razie katastrof. RSA oferuje opcję Business Continuity (ciągłość biznesowa), która umożliwia firmie czasowe rozszerzenie licencji na serwery Authentication Manager i użycie uwierzytelniania na żądanie (SMS lub e-mail) do obsługi dużego napływu użytkowników, gdy wystąpią zakłócenia w działalności firmy i wielu pracowników musi działać zdalnie.

Bezpieczny awaryjny dostęp do sieci

Innym zastosowaniem uwierzytelniania na żądanie (SMS lub e-mail) może być zapewnienie „awaryjnego” dostępu użytkownikowi tradycyjnego tokenu, jeśli czasowo nie może go użyć (na przykład zostawił go w domu), utracił go bezpowrotnie lub zapomniał numeru PIN. Po udzieleniu prawidłowych odpowiedzi na pytania

bezpieczeństwa zdefiniowane w bazie danych pracownik może uzyskać uwierzytelnienie na żądanie i efektywnie pracować w systemie IT - również poza standardowymi godzinami pracy.

Użytkownik może samoobsługowo rejestrować wnioski związane z wydaniem nowego tokenu sprzętowego lub tokenu na żądanie (SMS/e-mail). Ponieważ informacje są pobierane z tego samego repozytorium, zgłoszenie przez użytkownika utraty tokenu sprzętowego może automatycznie unieważnić jego dotychczasowe tokeny, co oszczędza czas i zapobiega ewentualnym nadużyciom. Moduł samoobsługowy daje dostęp także do innych usług, takich jak testowanie tokenu przez użytkownika, zgłaszanie problemów z tokenem, zmiana numeru PIN, uaktualnienie profilu użytkownika itd.

Globalny zasięg poprzez urządzenia mobilne

Konfigurowanie modułów On-demand Authenticator za pomocą wiadomości SMS wymaga współpracy z dostawcą usług SMS w celu zagwarantowania dostarczania tych wiadomości na całym świecie. Firma RSA podjęła już pierwsze kroki w tym kierunku, nawiązując współpracę z jednym z czołowych operatorów specjalizujących się w dostarczaniu wiadomości SMS, firmą Clickatell™, i wbudowując bezpośrednio w konsolę programu RSA Authentication Manager interfejs umożliwiający konfigurowanie wiadomości wysyłanych do bramki Clickatell. Clickatell może dostarczać wiadomości w prawie 200 krajach i ponad 600 sieciach, co gwarantuje użytkownikom, że dotrą one do nich przez RSA SecurID On-demand Authenticator bez względu na to, gdzie się znajdują.



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

The Security Division of EMC

©2007 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. EMC jest zastrzeżonym znakiem towarowym firmy EMC Corporation. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.

SIDODA DS 0208