



# RSA AUTHENTICATION MANAGER EXPRESS

Krótki opis  
produktu



EMC<sup>2</sup>  
where information lives<sup>®</sup>

Ryzyko związane ze stosowaniem uwierzytelniania opartego tylko na hasłach nie jest niczym nowym. Obecnie jednak aż 44% firm właśnie hasłami zabezpiecza dostęp zdalny swoich pracowników i partnerów<sup>1</sup>. Zaawansowane zagrożenia i stale rosnąca liczba przypadków łamania zabezpieczeń danych sprawiają, że systemy chronione hasłami statycznymi są podatne na ataki i wystawione na ryzyko nieautoryzowanego dostępu.

Silne uwierzytelnianie jest często stosowanym rozwiązaniem w zakresie ochrony dostępu do najważniejszych danych i aplikacji. Jednak w małych i średnich firmach wdrożenie zabezpieczeń niejednokrotnie stanowi problem, ponieważ firmy te nie mają wystarczających zasobów, by w pełni chronić swoją sieć; zresztą niejednokrotnie dominuje w nich przekonanie, że przypadki łamania zabezpieczeń danych ich nie dotyczą. Według badań przeprowadzonych niedawno przez National Cyber Security Alliance 85% małych i średnich firm stoi na stanowisku, że są w znacznie mniejszym stopniu narażone na ataki komputerowe niż duże przedsiębiorstwa<sup>2</sup>. Niestety cyberprzestępcy świetnie zdają sobie sprawę z faktu, że wiele takich firm nie ma zaawansowanych systemów kontroli zabezpieczeń, i coraz częściej to komputery właśnie małych i średnich firm padają łupem złodziei poufnych danych.

## Pokonywanie przeszkód na drodze do silnego uwierzytelniania

Małe i średnie firmy muszą pokonać szereg przeszkód, aby zastosować uwierzytelnianie dwuskładnikowe. Oto trzy największe problemy uniemożliwiające wielu małym i średnim firmom wdrożenie mechanizmu silnego uwierzytelniania:

- Wysokie koszty
- Niewygoda dla użytkowników
- Złożoność wdrożenia i zarządzania

### *Koszty*

Małe i średnie firmy często wskazują wysokie koszty rozwiązań dostępnych na rynku jako największą barierę blokującą im dostęp do silnego uwierzytelniania. Na przykład wdrożenie systemu haseł jednorazowych wymaga inwestycji w specjalny sprzęt, taki jak urządzenia dla użytkowników końcowych oraz serwer uwierzytelniający. Do tego dochodzą koszty zarządzania związane z pomocą techniczną dla użytkowników i aktualizacjami oprogramowania. Dysponując ograniczonym budżetem na rozwiązania IT, większość małych i średnich firm decyduje się na podstawowe zabezpieczenie dostępu za pomocą nazwy użytkownika i hasła.

### *Niewygoda dla użytkowników*

W kontekście wdrażania silnego uwierzytelniania istotną kwestią jest wygoda użytkowników. Należy rozważyć, czy dodatkowe zabezpieczenie nie obniży wydajności pracowników firmy i czy użytkownicy nie będą się przeciwstawiać stosowaniu nowej technologii. Nowe rozwiązanie może też mieć wpływ na całkowite koszty rozwiązania, jeśli nastąpi duży wzrost zapotrzebowania użytkowników na pomoc techniczną.

### *Wdrożenie i zarządzanie*

Wdrożenie mechanizmu silnego uwierzytelniania może wymagać od działu IT dużego zaangażowania zasobów. Ponadto należy uwzględnić takie kwestie jak bieżące zarządzanie danym rozwiązaniem, które może obejmować różne zadania, na przykład udostępnianie użytkownikom elementów niezbędnych do użytkowania danego

---

1 Forrester Research, „Best Practices: Implementing Strong Authentication in Your Enterprise”, lipiec 2009.

2 2010 NCSA/Visa Inc. Small Business Study

systemu oraz odzyskiwanie ich, a także dystrybucję sprzętu lub oprogramowania. Małe i średnie firmy już mają ograniczone zasoby IT. Dlatego konieczność poświęcenia dodatkowego czasu i oddelegowania pracowników w celu właściwego zarządzania mechanizmem silnego uwierzytelniania nie jest zachęcającą perspektywą dla i tak już mocno obciążonego personelu informatycznego.

## Mechanizm silnego uwierzytelniania dla małych i średnich firm

RSA Authentication Manager Express stanowi rozwiązanie problemów małych i średnich firm związanych z kosztami, niewygodną obsługą i ograniczonymi możliwościami w zakresie zarządzania środowiskiem IT — rozwiązanie niedrogie i wygodne, a jednocześnie zapewniające wysoki poziom bezpieczeństwa. Jest to platforma silnego uwierzytelniania wieloskładnikowego, obsługująca bezpieczne uwierzytelnianie dostępu zdalnego dla nawet 2500 użytkowników. RSA Authentication Manager Express współpracuje z popularnymi systemami SSL VPN oraz aplikacjami WWW, umożliwiając małym i średnim firmom wdrożenie silnego uwierzytelniania oraz zapewniając bezpieczny dostęp do chronionych aplikacji i danych.

RSA Authentication Manager Express działa przy zastosowaniu technologii uwierzytelniania z uwzględnieniem poziomu ryzyka opracowanej przez RSA. Fundamentem tego rozwiązania jest mechanizm RSA Risk Engine — zaawansowany system, który ocenia każdą próbę logowania i inne działania w czasie rzeczywistym, monitorując dziesiątki wskaźników ryzyka i przypisując poziom ryzyka każdemu żądaniu przychodzącemu od użytkownika. W przypadku narzędzia RSA Authentication Manager Express podczas określania poziomów ryzyka związanego z poszczególnymi żądaniami dostępu jest uwzględnianych wiele czynników, m.in.:

- coś, co użytkownik wie, na przykład nazwa użytkownika i hasło;
- coś, co użytkownik ma: na przykład laptop lub komputer stacjonarny;
- coś, co użytkownik robi, na przykład ostatnie operacje uwierzytelniania i czynności wykonywane na koncie.

Mechanizm RSA Risk Engine umożliwia firmom określanie niestandardowych zasad, które mają być stosowane w zależności od prognozy ryzyka — zdefiniowanych jest kilka poziomów ryzyka (od wysokiego do niskiego), które organizacja może przypisywać.

RSA Authentication Manager Express umożliwia też ustawianie poziomów ryzyka w zależności od populacji użytkowników. Dobrym rozwiązaniem w firmie mogą być różne zasady uwierzytelniania dla różnych grup użytkowników — zależnie od ich relacji z firmą. Na przykład w przypadku dostępu uzyskiwanego przez pracowników tolerancja ryzyka może być większa niż w przypadku dostępu uzyskiwanego przez partnerów. Jeśli mechanizm RSA Risk Engine oceni, że poziom ryzyka w przypadku danego żądania dostępu jest poniżej dopuszczalnej granicy, użytkownik jest bez problemu uwierzytelniany. Jeśli jednak mechanizm RSA Risk Engine oceni, że poziom ryzyka przekracza dopuszczalną granicę, użytkownik musi przedstawić dodatkowy dowód tożsamości.

### *Profil urządzenia: coś, co użytkownik ma*

Mechanizm RSA Risk Engine analizuje informacje dotyczące poszczególnych żądań dostępu wedle dwóch kategorii: profil urządzenia i wzorzec zachowań. Pierwszy składnik, profilowanie urządzenia, umożliwia uwierzytelnienie znacznej większości użytkowników na podstawie analizy profilu komputera przenośnego lub stacjonarnego, którego dany użytkownik zazwyczaj używa w celu uzyskania dostępu, oraz sprawdzenia, czy w systemie są zarejestrowane informacje dotyczące powiązania urządzenia z tym użytkownikiem. Dwie podstawowe składowe profile urządzenia to jednoznaczna identyfikacja urządzenia oraz statystyczna identyfikacja urządzenia.

Jednoznaczna identyfikacja urządzenia wspomaga identyfikowanie użytkownika dzięki umieszczeniu na jego urządzeniu dwóch ważnych elementów:

- (a) bezpiecznych plików cookie rozwiązania uwierzytelniającego oraz
- (b) współużytkowanych obiektów flash (flashowych plików cookie, flash cookies).

Bezpieczne pliki cookie rozwiązania uwierzytelniającego odgrywają niebagatelną rolę w identyfikacji komputerów przenośnych i stacjonarnych. Jest to mechanizm powszechnie stosowany do ustalania tożsamości użytkownika na podstawie unikatowego identyfikatora kryptograficznego umieszczonego na urządzeniu. Flashowe pliki cookie są stosowane w połączeniu z plikami cookie rozwiązania uwierzytelniającego, zapewniając dodatkową kontrolę wiarygodności. RSA Authentication Manager Express stosuje flashowe pliki cookie do oznaczenia komputera użytkownika — zasada jest taka sama jak w przypadku plików cookie rozwiązania uwierzytelniającego, przechowujących informacje, które później są pobierane z urządzenia. Zaletą flashowych plików cookie jest to, że nie są one usuwane tak często jak pliki cookie rozwiązania uwierzytelniającego, ponieważ większość użytkowników nie zdaje sobie sprawy z ich istnienia, a ci, którzy mają taką świadomość, nie zawsze wiedzą, jak te pliki usunąć.

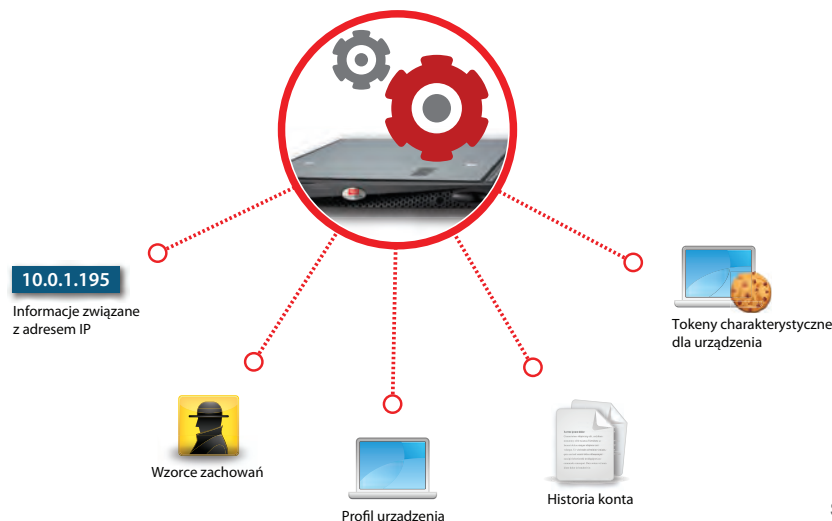
Statystyczna identyfikacja urządzenia to technologia, która statystycznie identyfikuje użytkownika i kojarzy go z urządzeniem na podstawie parametrów charakterystycznych dla tego urządzenia. Technologia ta jest zwykle stosowana jako mechanizm awaryjny w sytuacji, gdy brakuje unikatowego identyfikatora kryptograficznego (jeśli na przykład został usunięty z urządzenia).

Do elementów ocenianych w ramach procedury statystycznej identyfikacji urządzenia należą m.in. dane zbierane z nagłówek HTTP za pomocą skryptu Java™, takie jak wersja systemu operacyjnego, wersje poprawek do systemu operacyjnego, rozdzielczość ekranu, wersja przeglądarki internetowej, dane agenta użytkownika, wersje programów, parametry wyświetlania (wielkość ekranu i głębia kolorów), języki, ustawienia strefy czasowej, zainstalowane obiekty przeglądarki, zainstalowane oprogramowanie, ustawienia regionalne i językowe oraz adres IP.

#### *Wzorzec zachowań: coś, co użytkownik robi*

Zanim RSA Authentication Manager Express przypisze poziom ryzyka danemu żądaniu dostępu, poddaje analizie nie tylko profil urządzenia, lecz także zachowanie użytkownika. Wzorce zachowań służą do identyfikowania operacji logowania o wysokim poziomie ryzyka w drodze oceny takich elementów jak aktywność, informacje związane z adresem IP oraz działania związane z uwierzytelnianiem i wykonywane na koncie (np. niedawne zmiany w profilu użytkownika i kilka nieudanych prób uwierzytelnienia). Jeśli na przykład użytkownik zwykle loguje się z biura we Wrocławiu, a spróbuje się zalogować z nieznanego miejsca w Moskwie, dla systemu będzie to niestandardowe zachowanie. Jeśli jednak użytkownik często podróżuje i loguje się z różnych miejsc na całym świecie, wówczas ta sytuacja nie będzie niczym niezwykłym.

Rysunek 1. Mechanizm RSA Risk Engine przypisuje poziom ryzyka każdemu żądaniu użytkownika, uwzględniając dziesiątki elementów



## Dodatkowe uwierzytelnianie w przypadku żądań dostępu o wysokim poziomie ryzyka

Jeśli żądanie dostępu przekracza próg dopuszczalnego ryzyka ustalony w danej firmie, RSA Authentication Manager Express może uruchomić proces uwierzytelniania przy użyciu dodatkowych metod. Dzieje się tak zwykle wtedy, gdy użytkownik zdalny loguje się z urządzenia, które nie zostało rozpoznane i nie było wcześniej używane w celu uzyskania dostępu do sieci. RSA Authentication Manager Express umożliwia wybranie jednej z dwóch metod: wiadomość SMS oraz pytania weryfikujące.

### *Wiadomość SMS*

Wiadomość SMS zostanie zainicjowana w przypadku wysokiego poziomu ryzyka związanego z danym żądaniem dostępu. W takiej sytuacji RSA Authentication Manager Express wymaga od użytkownika przedstawienia dodatkowego dowodu tożsamości przez wykonanie pewnej prostej procedury.

Najpierw system monitoruje o wprowadzenie poufnego kodu PIN wybranego podczas rejestracji. Następnie generuje automatyczną wiadomość SMS i wysyła ją na numer telefonu komórkowego zarejestrowany przez użytkownika. Wiadomość SMS zawiera unikatowy 8-cyfrowy kod, który użytkownik ma wprowadzić w przeglądarce internetowej. Po pomyślnej weryfikacji kodu system natychmiast udziela użytkownikowi dostępu. RSA Authentication Manager Express obsługuje także dostarczanie hasła jednorazowego pocztą e-mail.

Największą zaletą uwierzytelniania za pomocą wiadomości SMS jest możliwość jego przeprowadzenia przy użyciu dowolnego telefonu komórkowego (użytkownik nie musi dysponować żadnym specjalnym urządzeniem ani oprogramowaniem).

### *Pytania weryfikujące*

Pytania zadawane w ramach uwierzytelniania to pytania, które użytkownik wybrał z listy i na które udzielił odpowiedzi podczas rejestracji lub po wprowadzeniu w firmie silnego uwierzytelniania użytkowników. Podczas uwierzytelniania użytkownik musi odpowiedzieć na część tych pytań — w ten sposób ogranicza się do minimum ryzyko, że poufne pytania i odpowiedzi wpadną w niepowołane ręce. Nie trzeba przy tym korzystać z zestawu pytań dostępnego w narzędziu RSA Authentication Manager Express — w firmie może być stosowany niestandardowy zestaw pytań.

## Wdrożenie i zarządzanie

RSA Authentication Manager Express jest urządzeniem podłączanym metodą „plug-and-play”, fabrycznie kompatybilnym z popularnymi systemami SSL VPN i serwerami WWW. Ponadto, dzięki narzędziu konfiguracyjnemu RSA Quick Setup do pełnego wdrożenia serwera wystarczy zaledwie kilka prostych kroków.

Oddanie rozwiązania do dyspozycji użytkowników jest równie łatwe. RSA Authentication Manager Express można podłączyć bezpośrednio do serwera katalogowego firmy. Podczas następnego uwierzytelniania użytkownicy automatycznie otrzymają instrukcje umożliwiające im samodzielną rejestrację. Dzięki pełnej automatyzacji procesu rejestracyjnego administratorzy nie muszą poświęcać czasu na udostępnienie rozwiązania użytkownikom, jak to ma miejsce w przypadku innych mechanizmów uwierzytelniania

## Główne zalety

RSA Authentication Manager Express został opracowany z myślą o zaspokojeniu potrzeb małych i średnich firm w zakresie silnego uwierzytelniania.

**Niewygórowany koszt.** RSA Authentication Manager Express został opracowany i wyceniony z uwzględnieniem potrzeb firm mających do 2500 użytkowników..

**Wygoda użytkowników.** RSA Authentication Manager Express umożliwia uwierzytelnianie większości operacji logowania za pomocą nazw użytkowników i haseł. Na ogół więc system uwierzytelniania wieloskładnikowego jest niewidoczny dla użytkowników, ponieważ mechanizm RSA Risk Engine działa w tle. Użytkownik musi podjąć dodatkowe zabiegi uwierzytelniające dopiero wtedy, gdy mechanizm RSA Risk Engine oceni, że dane żądanie dostępu wiąże się z wysokim ryzykiem.

**Łatwość wdrożenia i zarządzania.** RSA Authentication Manager Express jest dostępny jako urządzenie podłączane metodą „plug-and-play”, fabrycznie kompatybilne z popularnymi systemami SSL VPN i serwerami WWW. Ponadto zapewnia on pełną automatyzację procesu rejestracyjnego, dzięki czemu administratorzy poświęcają znacznie mniej czasu na udostępnianie użytkownikom elementów niezbędnych do użytkowania danego systemu oraz odzyskiwanie ich.

**Sprawdzona technologia.** Narzędzie RSA Authentication Manager Express jest oparte na technologii uwierzytelniania z uwzględnieniem poziomu ryzyka, która znalazła zastosowanie w ponad 8000 firm działających w różnych branżach, takich jak usługi finansowe, służba zdrowia, ubezpieczenia, handel detaliczny i administracja publiczna. Obecnie technologia uwierzytelniania z uwzględnieniem poziomu ryzyka opracowana przez RSA zapewnia ochronę ponad 250 milionom użytkowników i gwarantuje bezpieczny dostęp do różnych aplikacji i systemów, w tym witryn internetowych i portali oraz aplikacji SSL VPN.

## Podsumowanie

RSA Authentication Manager Express umożliwia małym i średnim firmom wdrożenie mechanizmu silnego uwierzytelniania, który jest niedrogi i wygodny zarówno dla użytkowników, jak i administratorów środowisk informatycznych. Dzięki narzędziu RSA Authentication Manager Express małe i średnie firmy mogą — nie przekraczając swojego budżetu — zapobiegać uzyskiwaniu nieuprawnionego dostępu, ograniczać ryzyko złamania zabezpieczeń danych, utrzymywać zgodność z obowiązującymi przepisami oraz bezpiecznie udzielać uprawnień dostępu zdalnego nowym użytkownikom.

## Silne uwierzytelnianie — mity i fakty

Mit	Fakty
W mojej firmie są stosowane silne hasła, które pracownicy muszą je regularnie zmieniać, co skutecznie obniża ryzyko.	Silne hasła, zawierające cyfry, wielkie litery i znaki nieliterowe, trudno odgadnąć hakerom, ale też trudno zapamiętać pracownikom. Bywa więc, że pracownicy zapisują hasła na kartkach lub podejmują inne działania, które ostatecznie jeszcze bardziej zwiększają ryzyko. Prawdziwie silne uwierzytelnianie wymaga więcej niż jednego składnika — czegoś więcej niż po prostu hasła.
Mojej firmie nie stać na mechanizm silnego uwierzytelniania.	Mechanizm silnego uwierzytelniania może mieć bardzo przystępną cenę, mieszczącą się w budżecie nie tylko wielkich firm. Na przykład RSA Authentication Manager Express został opracowany — i wyceniony — specjalnie z myślą o firmach obsługujących do 2500 użytkowników i dysponujących skromnym budżetem na rozwiązania IT.
Silne uwierzytelnianie ma wadę, która przeważa nad wszystkimi zaletami: wysoki koszt.	Koszt mechanizmu silnego uwierzytelniania jest znacznie niższy od kosztów, jakie firma ponosi w razie złamania zabezpieczeń danych lub konieczności uregulowania grzywny za brak zgodności z przepisami. Ponadto silne uwierzytelnianie sprzyja generowaniu okazji biznesowych owocujących dodatkowymi przychodami, a także uproszczeniu procesów biznesowych. W obliczu tych korzyści koszt silniejszego systemu zabezpieczeń jest nieznaczący.
Cyberprzestępcy atakują tylko duże firmy i instytucje rządowe.	Wprost przeciwnie. Cyberprzestępcy często atakują małe i średnie firmy, ponieważ firmy te zwykle mają słabe zabezpieczenia, przez co są łatwym celem.

## Informacje o firmie RSA

RSA, oddział EMC zajmujący się zabezpieczeniami, jest czołowym dostawcą rozwiązań w dziedzinie zabezpieczeń, zarządzania ryzykiem i zapewniania zgodności z przepisami. Najlepszym firmom z całego świata ułatwia przetrwanie — eliminuje najbardziej zaawansowane zagrożenia, w tym te związane z niedostateczną ochroną poufnych danych. Zagrożenia te obejmują zarządzanie ryzykiem w firmie, ochronę dostępu i współpracy ze strony pracowników mobilnych, utrzymywanie zgodności z przepisami oraz zabezpieczenia środowisk wirtualnych i systemów cloud computing.

Łącząc istotne metody kontroli potwierdzania tożsamości, zapobiegania utracie danych, szyfrowania i tokenizacji, ochrony przed oszustwami oraz platformy SIEM z najlepszymi w branży funkcjami eGRC i usługami konsultingowymi, firma RSA zapewnia wiarygodność i przejrzystość milionów tożsamości użytkowników, transakcji dokonywanych przy ich użyciu oraz generowanych w związku z tym danych.

RSA, logo RSA, EMC<sup>2</sup>, EMC oraz where information lives to zastrzeżone znaki towarowe lub znaki towarowe firmy EMC Corporation w Stanach Zjednoczonych i innych krajach. Wszystkie inne wymienione znaki towarowe stanowią własność odpowiednich podmiotów. ©2011 EMC Corporation. Wszelkie prawa zastrzeżone. Opublikowano w Stanach Zjednoczonych.

AMX SB 0111

[www.rsa.com](http://www.rsa.com)



**EMC<sup>2</sup>**  
where information lives<sup>®</sup>