



The Security Division of EMC

Artykuł przeglądowy

## RSA Authentication Decision Tree: jak wybrać najlepsze dla Twojej firmy rozwiązanie uwierzytelnianiające



# „Który mechanizm uwierzytelniania jest najodpowiedniejszy dla mojej firmy?”

To pytanie często pada w wielu firmach na całym świecie. Analitycy zachwalają skuteczność nowych lub właśnie opracowywanych produktów z dziedziny zabezpieczeń, a na rynku jest dostępna szeroka gama mechanizmów uwierzytelniania. Zanim dokona się ostatecznego wyboru takiego rozwiązania uwierzytelniającego, które najlepiej się sprawdzi w danej firmie, należy ustalić, jakie firma ma potrzeby w zakresie uwierzytelniania, na jakie zagrożenia jest narażona, jakie są jej cele biznesowe oraz jakie przepisy i wytyczne regulują działalność w danej branży.

Firma RSA opracowała drzewo decyzyjne służące wyborowi rozwiązania uwierzytelniającego. RSA Authentication Decision Tree to kompleksowe narzędzie ułatwiające poznanie, ocenienie i wybranie najodpowiedniejszego mechanizmu uwierzytelniania — takiego, które zaspokoi potrzeby użytkowników i spełni wymogi danej działalności gospodarczej. Narzędzie RSA Authentication Decision Tree pomaga zawęzić pulę rozpatrywanych mechanizmów uwierzytelniania na podstawie pięciu najważniejszych czynników. W niniejszym raporcie przedstawiamy narzędzie Authentication Decision Tree, analizujemy pięć czynników decydujących o wyborze mechanizmu uwierzytelniania i dajemy przejrzyste wskazówki dotyczące wyboru właściwego rozwiązania, zapewniającego optymalną równowagę między ryzykiem, kosztami i wygodą użytkowników końcowych.

---

## Potrzeba silnego uwierzytelniania

---

Ochrona dostępu do informacji oraz potwierdzanie tożsamości użytkowników proszących o ten dostęp to kluczowe elementy każdego systemu zabezpieczeń. Uwierzytelnianie użytkowników ma na celu przede wszystkim zabezpieczenie zdalnego dostępu do informacji firmy, ale obecnie występuje szereg czynników, które powodują wzrost zapotrzebowania na stosowanie silnego uwierzytelniania w całej firmie.

### Udostępnianie nowych aplikacji biznesowych online.

Dostrzegając nowe okazje biznesowe i oszczędności finansowe, jakie daje zapewnienie dostępu do informacji online, wiele firm zaczyna oferować więcej biznesowych aplikacji WWW.

**Wzrost zapotrzebowania na dostęp zdalny.** Działalność w skali globalnej oraz mobilność pracowników zmusza firmy do zapewniania im dostępu z każdego miejsca i o każdej porze — wymaga tego charakter ich pracy.

### Uprawnienia dostępu dla nowych populacji użytkowników.

Obecnie wykonawcy, partnerzy i dostawcy wymagają dostępu na żądanie do takich informacji firmy jak prognozy sprzedaży, analizy danych o konkurencji, cenniki, stany magazynu oraz dane o klientach.

**Wzrost liczby portali dla klientów.** Klienci coraz częściej chcą mieć dostęp do kont w czasie rzeczywistym oraz możliwość zarządzania nimi przez Internet.

### Konieczność zachowania zgodności z przepisami.

W ostatnich latach wprowadzono wiele przepisów zobowiązujących firmy do stosowania zabezpieczeń uniemożliwiających uzyskiwanie nieuprawnionego dostępu do informacji.

**Zaawansowane zagrożenia.** W zależności od użytkownika i charakteru informacji istnieją zagrożenia, które wymagają zminimalizowania ryzyka przez zastosowanie silnego uwierzytelniania. W przypadku użytkowników z dużych przedsiębiorstw trzeba zapewnić silne uwierzytelnianie w celu ochrony przed uzyskiwaniem nieuprawnionego dostępu do najważniejszych informacji firmy oraz wyeliminowania ryzyka ataku od wewnątrz. W przypadku klientów indywidualnych trzeba zastosować środki prewencyjne, aby zapewnić ochronę przed phishingiem i koźmi trójjańskimi oraz innym szkodliwym oprogramowaniem.

---

## Stan uwierzytelniania użytkowników

---

Mimo że uwierzytelnianie samym hasłem jest uznawane za zabezpieczenie stosunkowo słabe, wciąż powszechnie stosuje się je jako środek służący potwierdzeniu tożsamości użytkownika. Jednak ta metoda uwierzytelniania, postrzegana niegdyś jako „darmowa”, jest dość kosztowna z perspektywy bieżącego zarządzania i pomocy technicznej. Według raportu firmy Forrester Research średni koszt pracy specjalistów działu pomocy technicznej, którą należy wykonać w celu zresetowania jednego hasła, wynosi ok. 70 USD.

Na rynku nieustannie pojawiają się nowe mechanizmy, co jeszcze bardziej utrudnia firmom wybranie właściwej strategii silnego uwierzytelniania. W dużym przedsiębiorstwie dostęp do zasobów firmy najczęściej jest zabezpieczany za pomocą sprzętowych generatorów haseł jednorazowych. Jednak mobilność pracowników oraz powszechność korzystania z telefonów komórkowych i urządzeń PDA zwiększają zapotrzebowanie na programowe rozwiązania uwierzytelniające. W przypadku portali dla klientów powszechne jest uwierzytelnianie z uwzględnieniem poziomu ryzyka oraz uwierzytelnianie na podstawie wiedzy — ze względu na łatwość ich stosowania oraz skalowalność, umożliwiającą obsługiwanie dużych grup użytkowników.

W obliczu tak dużej liczby mechanizmów uwierzytelniania dostępnych na rynku trudno jest ustalić firmową strategię uwierzytelniania. W wielu firmach odpowiednie mogą być różne mechanizmy uwierzytelniania — zależy to od takich czynników jak populacja użytkowników, wartość chronionych informacji, przenośność oraz łatwość stosowania przez użytkownika końcowego. Firma RSA opracowała narzędzie Authentication Decision Tree, które ułatwia dokonanie obiektywnej oceny różnych rozwiązań oraz znalezienie właściwej równowagi między potrzebami użytkowników a wymogami danej działalności. Efektem jest wybór optymalnego rozwiązania.

---

## Najważniejsze aspekty, które należy uwzględnić podczas opracowywania strategii uwierzytelniania

---

Dążąc do opracowania odpowiedniej strategii uwierzytelniania, należy uwzględnić pięć najważniejszych czynników. Oto one:

- Wartość chronionych informacji
- Wymagana siła uwierzytelniania użytkowników
- Planowane użytkowanie
- Potrzeby populacji użytkowników końcowych
- Warunki techniczne

### Wartość chronionych informacji

Pierwszym czynnikiem wartym uwzględnienia jest wartość informacji, które mają podlegać ochronie, oraz koszt ewentualnego nieuprawnionego dostępu do tych informacji. Dane własne firmy, dane dotyczące kont bankowych i kart kredytowych, karty pacjentów lub dane osobowe — wszystkie te informacje należy traktować jako wartościowe. Nieuprawniony dostęp do takich informacji może być

bardzo kosztowny (np. w banku trzeba wziąć pod uwagę koszty nieuprawnionych przelewów środków pieniężnych na kontach klientów) oraz bardzo szkodliwy dla marki i reputacji firmy. Im większa wartość informacji, tym większe zagrożenie dla firmy, jeśli wpadną w niepowołane ręce, a więc i tym silniejszy mechanizm uwierzytelniania należy zastosować do ich ochrony.

### Wymagana siła uwierzytelniania użytkowników

Uwzględnienie specyfiki danej populacji użytkowników oraz informacji, do których uzyskują oni dostęp, może pomóc w ustaleniu wymaganego poziomu uwierzytelniania. Na przykład firmy nie mogą wymuszać uwierzytelniania na swoich klientach, więc podstawowym kryterium wyboru rozwiązania dla tej grupy może być wygoda oraz skłonność użytkowników do jego stosowania. Jednak już w przypadku pracowników i partnerów można się pokusić o większą kontrolę nad uwierzytelnianiem i uwzględnić takie aspekty jak przenośność, całkowity koszt eksploatacji oraz ogólne funkcje zarządzania.

### Planowane użytkowanie

Zazwyczaj mechanizm uwierzytelniania wdraża się w celu osiągnięcia więcej niż jednego celu biznesowego. Innymi słowy, w zależności od użytkownika oraz rodzaju wykonywanych przez niego działań w firmie może zostać podjęta decyzja, że oprócz standardowej procedury potwierdzania tożsamości użytkowników są potrzebne dodatkowe metody uwierzytelniania. Na przykład instytucja finansowa poszukująca sposobów na ograniczenie strat ponoszonych w wyniku oszustw może wdrożyć rozwiązanie do monitorowania transakcji i za jego pomocą monitorować przelewy środków pieniężnych o wysokim poziomie ryzyka. Inny przykład stanowią użytkownicy w dużych przedsiębiorstwach. Firma może wymagać, by pracownicy korzystający z wysoce poufnych informacji, np. personel działu kadr, działu płac lub działu księgowości, stosowali mechanizm uwierzytelniania umożliwiający szyfrowanie plików i wiadomości e-mail.

### Populacja użytkowników końcowych

Udostępniając mechanizm uwierzytelniania użytkownikom końcowym, należy uwzględnić wiele czynników — w zależności od danej populacji użytkowników końcowych. Z perspektywy użytkownika należy wziąć pod uwagę takie kwestie jak łatwość obsługi, chęć użytkownika do posługiwania się danym mechanizmem oraz informacje, do których użytkownik będzie uzyskiwać dostęp. Z perspektywy firmy należy wziąć pod uwagę takie kwestie jak całkowity koszt eksploatacji, konieczność przeszkolenia użytkowników, skalowalność oraz mobilność rozwiązania.

## Warunki techniczne

Wreszcie podczas ustalania wymaganej siły uwierzytelniania liczą się także warunki techniczne środowiska, w którym rozwiązanie ma zostać wdrożone. Na przykład w środowisku, w którym komputery stacjonarne są lepiej kontrolowane i istnieje duże prawdopodobieństwo, że oprogramowanie antywirusowe jest aktualne, wymagania w zakresie zabezpieczeń mogą nie być tak rygorystyczne jak na przykład w sytuacji, gdy środowisko użytkownika nie jest dobrze kontrolowane i gdy duży odsetek populacji użytkowników uzyskuje dostęp do sieci firmy z różnych miejsc na całym świecie.

Kolejnym aspektem technicznym, który należy mieć na względzie, są urządzenia używane przez użytkowników w celu uzyskania dostępu. Zarówno w przypadku dużych firm, jak i portali dla klientów użytkownicy końcowi prawdopodobnie będą uzyskiwać dostęp z różnych urządzeń — od komputerów przenośnych i stacjonarnych, przez urządzenia PDA i telefony komórkowe, po publiczne punkty dostępu do Internetu. Typy urządzeń używanych do uzyskiwania dostępu mają duży wpływ na wybór rozwiązań uwierzytelniających oferowanych użytkownikom końcowym.

---

## Narzędzie Authentication Decision Tree

---

W obliczu dużej liczby nowych metod i technologii uwierzytelniania, coraz większej wartości informacji, nowych populacji użytkowników wymagających dostępu do sieci i aplikacji, szybko rosnącej liczby zaawansowanych zagrożeń oraz skomplikowanych przepisów firmy muszą rewidować swoje strategie uwierzytelniania.

Duża liczba rozwiązań uwierzytelniających do sprawdzenia oraz zalew przekazów marketingowych o pewnych technologiach uwierzytelniania sprawiają, że w wielu firmach pojawiają się trudności z właściwą oceną. Na przykład systemy biometryczne cieszą się nadzwyczaj dużym zainteresowaniem mediów w porównaniu z rzeczywistą skalą ich stosowania na rynku. Takie systemy wymagają drogich i kłopotliwych w użyciu czytników, przez co się wręcz nie nadają do obsługi dostępu zdalnego bądź

uzyskiwanego za pomocą urządzeń przenośnych i nie cieszą się zainteresowaniem masowego odbiorcy.

Narzędzie RSA Authentication Decision Tree zostało opracowane z myślą o firmach, w których jest konieczne dokonanie obiektywnej oceny potrzeb użytkowników i wymogów danej działalności pod kątem technologii uwierzytelniania łatwo dostępnych na rynku. Ma pomóc kierownictwu podjąć właściwą decyzję. Ponieważ wciąż nie ma rozwiązania uniwersalnego, które spełniałoby wymagania wszystkich firm i zaspokajało potrzeby w zakresie zabezpieczeń wszystkich użytkowników we wszystkich sytuacjach, narzędzie RSA Authentication Decision Tree może posłużyć jako pomoc w wyborze najodpowiedniejszego rozwiązania uwierzytelniającego (bądź zestawu rozwiązań) — takiego, które zapewnia dobre wyważenie czynników ryzyka, kosztów i wygody użytkowników końcowych.

### Korzystanie z narzędzia Authentication Decision Tree

W ramach procesu ustalania, które rozwiązania najlepiej sprawdzą się w danej firmie, narzędzie RSA Authentication Tree przeprowadza analizę według następujących kryteriów:

- Kontrola nad środowiskiem użytkowników końcowych
- Planowane metody dostępu
- Potrzeba dostępu z każdego miejsca o dowolnej porze
- Potrzeba szyfrowania dysków, plików lub wiadomości e-mail
- Zapobieganie oszustwom

### Kontrola nad środowiskiem użytkowników końcowych

Aspekt kontroli nad środowiskiem użytkowników końcowych odgrywa bardzo istotną rolę podczas ustalania właściwej metody uwierzytelniania. Należy uwzględnić m.in. to, czy firma ma możliwość instalowania oprogramowania na komputerze użytkownika końcowego i czy może narzucać użytkownikom, w jakim systemie operacyjnym będą pracować.

Dlaczego to takie ważne? Możliwość decydowania o systemie operacyjnym jest istotna, ponieważ mechanizmy uwierzytelniania bywają niekompatybilne z niektórymi systemami operacyjnymi. W środowisku przedsiębiorstwa firma ma bezpośrednią kontrolę nad systemami operacyjnymi zainstalowanymi w urządzeniach użytkowników. Nie ma jednak kontroli nad systemami operacyjnymi użytkowników zewnętrznych (np. klientów i partnerów), w wyniku czego metoda uwierzytelniania oferowana tym populacjom może być inna.

**Kontrola nad środowiskiem użytkowników końcowych jest bardzo istotną kwestią podczas ustalania właściwej metody uwierzytelniania.**

### Metody dostępu, które będą stosowane

Metody dostępu to bardzo ważny czynnik podczas opracowywania strategii uwierzytelniania. Niektóre metody uwierzytelniania działają tylko w przypadku uzyskiwania dostępu do aplikacji WWW, inne zaś mogą służyć do uwierzytelniania dostępu do wielu aplikacji niebędących aplikacjami WWW. Dlatego profil użytkownika, jego prawa dostępu i planowane użytkowanie będą miały bezpośredni wpływ na wybór metod uwierzytelniania.

### Potrzeba dostępu z każdego miejsca o dowolnej porze

Działalność w skali globalnej oraz coraz większa mobilność pracowników wygenerowały zapotrzebowanie na dostęp w dowolnym czasie i miejscu. Zapewnienie użytkownikom bezpiecznego dostępu do informacji jest decydujące dla ciągłości działalności firmy. W przypadku pracowników lub partnerów dostęp z każdego miejsca i o każdej porze służy podtrzymaniu wydajności pracy; w przypadku klientów – osiągnięciu ich zadowolenia. Należy uwzględnić m.in. następujące czynniki:

- Czy użytkownicy muszą mieć dostęp z różnych lokalizacji zdalnych?
- Czy użytkownicy muszą mieć dostęp z nieznanymi systemów, np. publicznych punktów dostępu do Internetu, systemów hotelowych bądź współdzielonych stacji roboczych?
- Czy użytkownicy muszą mieć dostęp z różnych rodzajów urządzeń, takich jak PDA czy telefony komórkowe?

### Szyfrowanie dysków, plików lub wiadomości e-mail

Opracowując strategię uwierzytelniania, należy rozważyć inne cele biznesowe firmy, które dana metoda uwierzytelniania pozwoliłaby osiągnąć. Na przykład w celu zachowania zgodności z przepisami w firmach zajmujących się opieką zdrowotną może być konieczne szyfrowanie informacji dotyczących stanu zdrowia lub innych danych osobowych pacjenta na potrzeby przesyłania ich między poszczególnymi działami i placówkami. Wówczas w firmie może obowiązywać zasada, że użytkownicy mający prawa dostępu do tych danych mogą uzyskiwać ten dostęp tylko z wiarygodnych urządzeń.

### Zapobieganie oszustwom

W przypadku niektórych metod uwierzytelniania w celu zapobieżenia oszustwom wymagane jest monitorowanie transakcji i działań podejmowanych przez użytkownika po początkowym uwierzytelnieniu w ramach logowania. Taka sytuacja najczęściej ma miejsce w sektorze usług

finansowych, ale i firmy z innych branż zaczynają padać ofiarami ukierunkowanych ataków, takich jak phishing czy instalacja szkodliwego oprogramowania, podejmowanych przez przestępców w celu zebrania danych osobowych i kradzieży tożsamości.

---

## Mnóstwo możliwości uwierzytelniania

---

### Hasła

Hasła stanowią metodę uwierzytelniania jednoskładnikowego dokonywanego w celu potwierdzenia tożsamości użytkownika. Samo nabycie rozwiązania ochrony hasłem wprawdzie nic nie kosztuje, ale później pojawiają się koszty bieżącego zarządzania i pomocy technicznej (na przykład związane z resetowaniem hasła), które w dłuższej perspektywie mogą być wysokie. Poziom bezpieczeństwa jest bardzo niski i hasła są szczególnie podatne na ataki hakerów oraz przekazywanie innym użytkownikom.

### Uwierzytelnianie na podstawie wiedzy

Uwierzytelnianie na podstawie wiedzy polega na sprawdzaniu, czy użytkownik zna pewne określone informacje osobiste. Uwierzytelnianie ma postać interaktywnej wymiany pytań i odpowiedzi w czasie rzeczywistym. Pytania są generowane na podstawie informacji zebranych w wyniku przeszukiwania baz danych z rekordami dostępnymi publicznie, wybierane losowo i nieznanymi (dotąd niezadawane) użytkownikowi.

### Uwierzytelnianie z uwzględnieniem poziomu ryzyka

Uwierzytelnianie z uwzględnieniem poziomu ryzyka to system potwierdzania tożsamości użytkowników i/lub uwierzytelniania działań wykonywanych w trybie online. Jest realizowany w sposób niezakłócający pracy, na podstawie pomiaru szeregu wskaźników ryzyka. Wskaźniki obejmują m.in. pewne atrybuty urządzenia, wzorce zachowań i funkcję geograficznej lokalizacji adresów IP. Im wyższy poziom ryzyka, tym większe prawdopodobieństwo fałszywej tożsamości lub oszustwa. Jeśli mechanizm oceny ryzyka oceni, że żądanie uwierzytelnienia wykracza poza przyjęte reguły, funkcja uwierzytelniania z uwzględnieniem poziomu ryzyka może zaostrić procedurę. W przypadku zaostżenia procedury uwierzytelniania użytkownik może zostać poproszony o udzielenie odpowiedzi na kilka pytań bądź podanie kodu autoryzacyjnego otrzymanego przez SMS lub e-mail.

### Uwierzytelnianie za pomocą haseł jednorazowych

Uwierzytelnianie za pomocą haseł jednorazowych jest jednym z najpopularniejszych rozwiązań w zakresie uwierzytelniania dwuskładnikowego. Opiera się na czymś, co użytkownik wie

(numer PIN lub hasło), oraz czymś, co ma (generator haseł jednorazowych, tzw. token). Token generuje nowe hasło jednorazowe co 60 sekund, co utrudnia komukolwiek poza uprawnionym użytkownikiem podanie prawidłowego kodu w danym czasie.

Aby uzyskać dostęp do informacji lub zasobów chronionych przy użyciu technologii haseł jednorazowych, użytkownicy po prostu łączą swój poufny numer identyfikacji osobistej (PIN) z kodem widocznym w danym czasie na wyświetlaczu tokena. W efekcie powstaje unikatowe hasło jednorazowe, zapewniające wiarygodne potwierdzenie tożsamości użytkownika.

Technologia haseł jednorazowych jest dostępna w wielu formach, m.in.:

- **Tokeny Sprzętowe** Tradycyjne tokeny sprzętowe to urządzenia przenośne (tak małe, że można je założyć na kółko z kluczami), zaspokajające potrzeby użytkowników preferujących namacalne zabezpieczenie lub uzyskujących dostęp do Internetu z różnych miejsc.
- **Tokeny Programowe** Dostępne dla komputerów, napędów USB lub urządzeń przenośnych. Tokeny Programowe są zwykle oferowane w postaci aplikacji lub paska narzędzi bezpiecznie umieszczonego w komputerze stacjonarnym, laptopie lub urządzeniu przenośnym użytkownika.
- **Uwierzelnianie na żądanie** Uwierzelnianie na żądanie wymaga dostarczenia użytkownikowi unikatowego hasła jednorazowego „na żądanie” przez SMS do urządzenia przenośnego lub pocztą e-mail na adres zarejestrowany przez użytkownika. Otrzymałszy unikatowe hasło jednorazowe, użytkownik po prostu je wprowadza wraz z wymaganym numerem PIN i w ten sposób uzyskuje dostęp do sieci firmy lub aplikacji online.

Uwierzelnianie za pomocą haseł jednorazowych opiera się na czymś, co użytkownik wie (numer PIN lub hasło), oraz czymś, co ma (token).

### Certyfikaty cyfrowe

Certyfikat cyfrowy to unikatowy dokument elektroniczny zawierający informacje identyfikujące osobę lub komputer, których dotyczy. Certyfikat cyfrowy można przechowywać w komputerze stacjonarnym, karcie inteligentnej lub urządzeniu USB. Aby uzyskać silniejsze uwierzelnianie dwuskładnikowe, można zablokować certyfikat cyfrowy w karcie inteligentnej lub urządzeniu USB, a odblokowanie go i skorzystanie z poświadczeń będzie wymagało od użytkownika podania kodu PIN. Certyfikatu cyfrowego można następnie użyć do uwierzelnienia użytkownika w sieci lub aplikacji. Certyfikaty cyfrowe nie tylko służą do uwierzelniania użytkowników, ale też wnoszą do firmy dodatkową wartość, udostępniając funkcje podpisów cyfrowych i szyfrowania wiadomości e-mail.

Ponadto certyfikaty cyfrowe można połączyć z systemami haseł jednorazowych przy użyciu sprzętowego tokenu hybrydowego. W tym przypadku hybrydowy token przechowuje wiele poświadczeń i upraszcza użytkownikom stosowanie się do procedur uwierzelniania. Typowym przypadkiem użycia certyfikatu i systemu haseł jednorazowych jest odblokowanie szyfrowania dysku twardego za pomocą certyfikatu cyfrowego, a następnie uwierzelnienie się w sieci VPN za pomocą hasła jednorazowego.

---

### Analizowanie atrybutów uwierzelniania

---

Kiedy firma ocenia wymogi swojej działalności i potrzeby użytkowników, wybranie odpowiedniej strategii uwierzelniania na podstawie rozwiązań dostępnych do wyboru jest ostatecznie kompromisem między następującymi elementami:

- Siła zabezpieczeń
- Typowe przypadki użycia
- Wymagania po stronie klienta
- Przenośność
- Mnogość zastosowań
- Trudności z perspektywy użytkowników
- Wymagania związane z dystrybucją
- Wymagania systemowe
- Koszt

Narzędzie RSA Authentication Decision Tree ułatwia firmie porównanie metod uwierzytelniania, które wydają się spełniać ich wymagania. Korzystając z tej prostej platformy, firma może obiektywnie ocenić najpopularniejsze rozwiązania uwierzytelniające.

Wprawdzie koszt jest kwestią istotną, ale wybierając rozwiązanie, firmy muszą uwzględnić kilka innych elementów. Nader często firmy koncentrują się na kosztach nabycia

rozwiązania, lecz jeśli taki jest priorytet, wystarczy zainteresować się mechanizmem uwierzytelniania opartego tylko na hasłach, by się przekonać, że ten koszt nie powinien być jedynym kryterium. Hasła są w zasadzie „darmowe”, jeśli chodzi o koszt nabycia rozwiązania, jednak zaskakująco drogie, jeśli uwzględni się bieżące zarządzanie i pomoc techniczną. W tabeli na stronach 8 i 9 przedstawiono porównanie i analizę mechanizmów uwierzytelniania z uwzględnieniem powyższych dziewięciu cech.

## Authentication Decision Tree — scenariusz

### Profil firmy

Duża firma zajmująca się opieką zdrowotną, obejmująca kilka szpitali regionalnych oraz centra specjalistyczne i obsługująca ponad 1,5 miliona pacjentów.

### Grupy użytkowników

Lekarze, płatnicy i ubezpieczyciele, pacjenci, kierownicy placówek

### Potrzeby działalności i użytkowników

Lekarze są stale w ruchu. Przemieszczają się między placówkami i bez przerwy korzystają z danych dotyczących firmy i pacjentów, posługując się smartfonami Blackberry lub innymi urządzeniami przenośnymi. Dzięki nim mogą błyskawicznie uzyskać bezpieczny dostęp do kart pacjentów, co umożliwia im zapewnienie opieki najwyższej jakości.

Płatnicy i ubezpieczyciele muszą — w celu rozpatrzenia i uregulowania roszczeń — mieć dostęp do danych o pacjentach i historii leczenia oraz zrealizowanych usług.

Kierownicy placówek zawsze muszą mieć dostęp do chronionych informacji o stanie zdrowia oraz danych osobowych pacjentów. Dostęp do informacji o pacjentach jest potrzebny do pracy wielu ludziom — od pracowników opieki społecznej po specjalistów ds. rozliczeń.

Pacjenci otrzymują dostęp do swoich informacji osobistych i historii leczenia za pośrednictwem portalu internetowego. Mogą aktualizować swoje dane osobowe, a także korzystać z szerokiej gamy innych dogodnych usług online, takich jak rejestrowanie się na wizyty lekarskie, przesyłanie próśb o nowe recepty na zażywane leki i opłacanie rachunków za wizyty lekarskie.

### Dostępne opcje uwierzytelniania

Mając zróżnicowaną grupę użytkowników, której członkowie uzyskują dostęp do różnych systemów i mają różne potrzeby, z pewnością trzeba rozpatrzyć wiele rozwiązań do uwierzytelniania:

Lekarze: programowy system haseł jednorazowych do urządzeń przenośnych

Płatnicy i ubezpieczyciele: tokeny sprzętowe

Kierownicy placówek: tokeny sprzętowe

Pacjenci: mechanizm uwierzytelniania z uwzględnieniem poziomu ryzyka

Nader często firmy koncentrują się na kosztach nabycia rozwiązania, lecz jeśli taki jest priorytet, wystarczy zainteresować się mechanizmem uwierzytelniania opartego tylko na hasłach, by się przekonać, że ten koszt nie powinien być jedynym kryterium.

	Hasła	Uwierzytelnianie na podstawie wiedzy	Uwierzytelnianie z uwzględnieniem poziomu ryzyka	Hasła jednorazowe: tokeny sprzętowe	Uwierzytelnianie hybrydowe: hasła jednorazowe i certyfikaty cyfrowe
<b>Siła zabezpieczenia</b>	Jednoskładnikowe, podatność na ataki łamaczy haseł, przekazywanie innym itp.	Silniejsze (jednoskładnikowe) Unikatowa wiedza	Co najmniej dwuskładnikowe, w zależności od oceny poziomu ryzyka	Silne dwuskładnikowe — PIN oraz kod tokenu	Silne dwuskładnikowe — PIN oraz kod tokenu lub certyfikat
<b>Typowe użycie</b>	Nieobwarowane warunkami Mało ważne aplikacje	Rejestrowanie nowych użytkowników, dostęp awaryjny, reset numeru PIN	Ważne oprogramowanie dla konsumentów lub dostęp do systemów SSL VPN	Dostęp dla pracowników mobilnych	Użytkownicy wewnętrzni i pracownicy podróżujący
<b>Wymagania po stronie klienta</b>	Brak	Brak	Brak	Brak	Oprogramowanie pośredniczące obsługujące kartę inteligentną
<b>Przenośność</b>	Działa wszędzie	Działa wszędzie	Aplikacje dostępne przez przeglądarkę	Działa wszędzie	Funkcja haseł jednorazowych działa wszędzie
<b>Mnogość zastosowań</b>	Nie	Nie	Platforma monitorowania transakcji i wykrywania oszustw	Nie	Szyfrowanie plików i wiadomości e-mail Podpisywanie cyfrowe Dostęp zdalny
<b>Trudności z perspektywy użytkowników</b>	Łatwo ulegają zapomnieniu, często są zapisywane na kartkach	Minimalne	Od minimalnych do dużych	Minimalne	Minimalne
<b>Wymagania związane z dystrybucją</b>	Brak	Brak	Brak	Przydzielanie i dostarczanie tokenów	Oprogramowanie klienckie Certyfikat Token
<b>Wymagania systemowe</b>	Katalog użytkowników	Usługa subskrypcji	Serwer uwierzytelniania Agenci niestandardowi Aplikacje WWW Opcja usługi subskrypcji	Serwer uwierzytelniania Agenci w aplikacjach	Urząd certyfikacji Serwer uwierzytelniania
<b>Koszt</b>	Niski koszt nabycia, ale wysoki koszt pomocy technicznej	Umiarkowany	Niski koszt w przypadku zintegrowania niektórych aplikacji	Wysoki koszt nabycia, ale niewielkie nakłady na zarządzanie	Większe wydatki na infrastrukturę i zarządzanie

Hasła jednorazowe: tokeny programowe w komputerach	Hasła jednorazowe: tokeny programowe w napędach USB	Hasła jednorazowe: tokeny programowe w urządzeniach przenośnych	Hasła jednorazowe dostarczane na żądanie	Certyfikaty cyfrowe
Silne dwuskładnikowe – PIN oraz token	Silne dwuskładnikowe (może być biometryczne)	Silne dwuskładnikowe – PIN oraz kod tokenu programowego	Silne dwuskładnikowe – PIN oraz kod dostarczany do telefonu	Możliwa blokada zdejmowana przez podanie numeru PIN w celu uzyskania uwierzytelnienia dwuskładnikowego
Dostęp dla pracowników mobilnych	Dostęp dla pracowników mobilnych	Dostęp dla pracowników mobilnych	Dostęp awaryjny, Dostęp dla użytkowników okazjonalnych lub tymczasowych, jako drugi składnik – oprócz IDA	Uwierzytelnianie użytkowników końcowych w obrębie przedsiębiorstwa lub uwierzytelnianie komputerów/urządzeń
Kompatybilny komputer	Kompatybilne urządzenie USB	Kompatybilna platforma	Każde urządzenie obsługujące wiadomości e-mail lub SMS	Kontener lub urządzenie (USB, karta inteligentna lub komputer stacjonarny)
Działa tylko w przypisanym systemie	Działa wszędzie, ale wymaga portu USB	Działa wszędzie	Zależy o zakresu usług	Zależy od kontenera – karta inteligentna wymaga czytnika lub portu USB
Nie	Magazyn plików	Nie	Nie	Tak – uwierzytelnianie, podpisywanie cyfrowe i szyfrowanie
Minimalne	Minimalne	Minimalne	Proces dwuetapowy	Minimalne
Przydzielanie i dostarczanie oprogramowania oraz kluczy początkowych	Przydzielanie i dostarczanie oprogramowania oraz kluczy początkowych	Przydzielanie i dostarczanie oprogramowania oraz kluczy początkowych	Brak	Brak
Serwer uwierzytelniania Agenci w aplikacjach	Serwer uwierzytelniania Agenci w aplikacjach	Serwer uwierzytelniania Agenci w aplikacjach	Serwer uwierzytelniania Agenci w aplikacjach Dostarczanie przez SMS	Rejestrowanie użytkowników lub automatyczne dostarczanie certyfikatów do urządzenia klienckiego
Mniejszy niż w przypadku tokenów sprzętowych	Wysoki – urządzenie oraz token	Mniejszy niż w przypadku tokenów sprzętowych	Mniejszy niż w przypadku tokenów sprzętowych i programowych	Należy uwzględnić okres eksploatacji

---

## Rozwiązania firmy RSA

---

RSA jest od ponad 20 lat jednym z najpopularniejszych dostawców rozwiązań w zakresie silnego uwierzytelniania dwuskładnikowego przeznaczonych dla firm każdej wielkości. RSA oferuje szereg rozwiązań, które mają zapewniać silne uwierzytelnianie przy jednoczesnym zachowaniu równowagi między ryzykiem, kosztami i wygodą użytkowników końcowych.

### RSA® Identity Verification

W oprogramowaniu RSA Identity Verification tożsamość użytkowników jest potwierdzana w czasie rzeczywistym przez uwierzytelnianie oparte na wiedzy. Narzędzie RSA Identity Verification zadaje użytkownikowi kilka losowo wybranych pytań wygenerowanych na podstawie informacji dotyczących danej osoby, uzyskanych w ramach skanowania dziesiątek baz danych z rekordami dostępnymi publicznie. W ciągu sekund narzędzie RSA Identity Verification udostępnia potwierdzenie tożsamości, przy czym nie jest wymagana żadna uprzednia relacja z użytkownikiem.

Ponadto narzędzie RSA Identity Verification zapewnia większą precyzję uwierzytelniania użytkowników za pomocą modułu Identity Event Module. Identity Event Module zwiększa bezpieczeństwo, szacując poziom ryzyka związanego z daną tożsamością i umożliwiając zmiany w konfiguracji systemu w celu automatycznego dostosowywania stopnia trudności pytań zadawanych w ramach procesu uwierzytelniania w celu odzwierciedlenia szczególnego charakteru danego zagrożenia. Uwzględniane są m.in. następujące aspekty dotyczące tożsamości:

- **Przeszukiwanie danych dostępnych publicznie.** Raporty dotyczące podejrzanych przypadków uzyskania dostępu do danych użytkownika dostępnych publicznie.
- **Aktywność tożsamości.** Duża liczba działań związanych z daną osobą w różnych obszarach firmy.
- **Aktywność adresu IP.** Wiele żądań uwierzytelnienia wygenerowanych z tego samego adresu IP.

### RSA® Authentication Manager Express

RSA® Authentication Manager Express to platforma silnego uwierzytelniania wieloskładnikowego, zapewniająca ekonomiczną ochronę dla firm. Authentication Manager Express współpracuje z najlepszymi systemami SSL VPN oraz aplikacjami WWW, zapewniając silne uwierzytelnianie oraz bezpieczny dostęp do chronionych aplikacji i danych.

Authentication Manager Express działa przy zastosowaniu technologii uwierzytelniania z uwzględnieniem poziomu ryzyka opracowanej przez RSA. Jest to zaawansowany system potwierdzania tożsamości użytkowników dokonywanego w sposób niezakłócający pracy na podstawie pomiaru szeregu wskaźników ryzyka. 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 komputer przenośny lub stacjonarny
- Coś, co użytkownik robi, na przykład ostatnie operacje uwierzytelniania i czynności wykonywane na koncie

Jeśli żądanie dostępu nie osiąga wymaganego poziomu wiarygodności, RSA Authentication Manager Express może wywoływać metody dodatkowego uwierzytelniania. Ma to miejsce szczególnie wtedy, gdy użytkownik zdalny loguje się z urządzenia, które nie zostało rozpoznane i nie zostało wcześniej użyte w celu uzyskania dostępu do sieci. Uwierzytelnianie przy użyciu rozwiązań RSA Manager Express udostępnia dwie metody dodatkowego uwierzytelniania: wiadomości SMS oraz pytania.

*RSA Authentication Manager Express jest dostarczany w postaci urządzenia podłączanego metodą „plug and play” i obsługuje do 2500 użytkowników.*

### RSA® Adaptive Authentication

RSA® Adaptive Authentication to platforma uwierzytelniania wielokanałowego i wykrywania oszustw, zapewniająca ekonomiczną ochronę wszystkim użytkownikom. Narzędzie Adaptive Authentication umożliwia wprowadzenie dodatkowych identyfikatorów w postaci prostego dodatku: pliku cookie i/lub współużytkowanego obiektu flash (tzw. „flash cookie”), który może służyć jako bardziej unikatowy identyfikator urządzenia użytkownika. To rozwiązanie zapewnia silną i wygodną ochronę, monitorując i uwierzytelniając działania użytkowników z uwzględnieniem poziomów ryzyka, zasad obowiązujących w obrębie całej firmy i segmentacji populacji użytkowników. Narzędzie Adaptive Authentication, obsługiwane przy użyciu technologii RSA w zakresie uwierzytelniania z uwzględnieniem poziomu ryzyka, monitoruje ponad setkę wskaźników i rozpoznaje ewentualne oszustwa. Wskaźniki te to m.in. identyfikacja urządzeń, geograficzna lokalizacja adresów IP oraz wzorce zachowań użytkowników.

Każdemu działaniu jest przypisany stopień ryzyka. Im wyższy stopień, tym większe prawdopodobieństwo, że dane działanie jest wykonywane w złej wierze.

Narzędzie Adaptive Authentication zapewnia monitorowanie w sposób niezakłócający pracy (jest niewidoczne dla użytkowników). Użytkownik musi podjąć dodatkowe zabiegi uwierzytelniające (zwykle w postaci udzielenia odpowiedzi na pytania lub uwierzytelnienia przy użyciu telefonu i danych przestanych „pozapasmowo”) dopiero wtedy, gdy poziom ryzyka związanego z danym działaniem zostanie określony jako wysoki. W przypadku niewielkiego ryzyka i wysokiego stopnia realizacji wymaganej procedury narzędzie Adaptive Authentication udostępnia silną ochronę i cechuje się nadzwyczajną użytecznością — jest znakomitym rozwiązaniem dla dużych grup użytkowników.

*Narzędzie RSA Adaptive Authentication jest dostępne zarówno w postaci oprogramowania jako usługi (SaaS), jak i wdrażane w placówce docelowej. Rozwiązanie to jest wysoce skalowane i może obsłużyć miliony użytkowników.*

#### **RSA SecurID®**

Technologia hasel jednorazowych RSA SecurID® stanowi jedno z najlepszych rozwiązań do uwierzytelniania dwuskładnikowego — opiera się ono na czymś, co użytkownik wie (numer PIN lub hasło), oraz czymś, co ma (moduł uwierzytelniający). Token RSA SecurID udostępnia unikatowy klucz symetryczny („seed record”), na podstawie którego sprawdzony algorytm co 60 sekund generuje nowe hasło jednorazowe. Ta opatentowana technologia synchronizuje każdy token z serwerem zabezpieczeń, zapewniając wysoki poziom bezpieczeństwa.

Aby uzyskać dostęp do zasobów chronionych za pomocą systemu RSA SecurID, użytkownicy muszą po prostu połączyć swój poufny numer identyfikacji osobistej (PIN) z kodem widocznym w danym czasie na wyświetlaczu tokenu. W efekcie powstaje unikatowe hasło jednorazowe, zapewniające wiarygodne potwierdzenie tożsamości użytkownika. Aby sprostać wymaganiom firm i zaspokoić

potrzeby użytkowników, token RSA SecurID jest udostępniany w następujących postaciach:

#### **Tokeny Sprzętowe**

Z perspektywy łatwości użytkowania tradycyjne tokeny sprzętowe to urządzenia przenośne (tak małe, że można je założyć na kółko z kluczami), zaspokajające potrzeby użytkowników preferujących namacalne zabezpieczenie lub uzyskujących dostęp do Internetu z różnych miejsc.

#### **Hybrydowy token z funkcją przechowywania certyfikatów w cyfrowych**

RSA SecurID 800 to urządzenie hybrydowe łączące prostotę i przenośność tokenu SecurID z zaawansowanymi możliwościami i elastycznością karty inteligentnej w jednym wygodnym w użyciu urządzeniu USB. Moduł 800 obsługuje standardowe certyfikaty cyfrowe na potrzeby szyfrowania dysków i plików, uwierzytelniania, podpisywania i innych zastosowań. Ponadto wzmacnia proste uwierzytelnianie za pomocą hasła, ponieważ stosowane w domenie poświadczenia użytkowników są przechowywane w urządzeniu o specjalnie wzmocnionych zabezpieczeniach. Łącząc kilka poświadczeń i aplikacji w jednym urządzeniu, moduł 800 stanowi klucz uniwersalny, obsługujący silne uwierzytelnianie w całym heterogenicznym (zawierającym elementy różnych producentów) środowisku IT — w sposób prosty i nieuciążliwy z perspektywy użytkownika.

#### **Tokeny Programowe**

W tokenach programowych RSA SecurID znajduje zastosowanie ten sam algorytm co w tokenach sprzętowych RSA SecurID, ale wyeliminowana jest konieczność noszenia przez użytkowników specjalnych urządzeń. W ich przypadku klucz symetryczny nie jest przechowywany w urządzeniu SecurID, lecz bezpiecznie przetrzymywany w komputerze, smartfonie lub urządzeniu USB użytkownika.

#### **Urządzenia przenośne**

Programowe tokeny RSA SecurID są dostępne w wersjach do różnych platform smartfonów, takich jak BlackBerry®, Microsoft Windows® Mobile, Java™ ME, Palm OS, Symbian OS i UIQ.

Aby uzyskać dodatkowe informacje na temat oceniania dostępnych do wyboru mechanizmów uwierzytelniania za pomocą narzędzia Authentication Decision Tree, skontaktuj się z opiekunem klienta w firmie RSA bądź naszym partnerem handlowym albo odwiedź witrynę [www.rsa.com](http://www.rsa.com).

## Komputery stacjonarne z systemem Microsoft Windows®

RSA SecurID Token for Windows Desktops to wygodne narzędzie instalowane w komputerze, które zapewnia automatyczną integrację z najpopularniejszymi klientami dostępu zdalnego.

## Token w formie paska narzędzi

RSA SecurID Toolbar Token stanowi połączenie wygody funkcji automatycznego wypełniania formularzy w aplikacjach WWW oraz zabezpieczeń w postaci mechanizmów zapobiegających phishingowi.

## Mechanizm uwierzytelniania na żądanie (dostarczenie przez SMS lub e-mail)

Uwierzytelnianie na żądanie wymaga dostarczenia użytkownikowi unikatowego hasła jednorazowego „na żądanie” przez SMS do urządzenia przenośnego lub pocztą e-mail na adres zarejestrowany przez użytkownika. Otrzymałszy unikatowe hasło jednorazowe, użytkownik po prostu je wprowadza wraz z wymaganym numerem PIN i w ten sposób uzyskuje dostęp do sieci firmy lub aplikacji online.

## RSA® Certificate Manager

RSA® Certificate Manager to internetowy urząd certyfikacji obsługujący podstawowe funkcje wydawania i weryfikowania certyfikatów cyfrowych oraz zarządzania nimi. Rozwiązanie to obejmuje zabezpieczony serwer WWW, zaawansowany mechanizm podpisywania do cyfrowego podpisywania certyfikatów użytkowników końcowych oraz zintegrowane repozytorium danych do przechowywania certyfikatów, danych o systemach oraz informacji o statusach certyfikatów. RSA Certificate Manager to pierwsze oprogramowanie, które otrzymało certyfikat Common Criteria oraz certyfikat Identrust.

Oprogramowanie Certificate Manager opracowano zgodnie z otwartymi standardami branżowymi, dzięki czemu od razu po zainstalowaniu współpracuje z setkami standardowych aplikacji. Dzięki temu rozwiązanie to można stosować z innymi aplikacjami, takimi jak przeglądarki internetowe oraz klienci e-mail i VPN — to pozwala uzyskać maksymalny zwrot z inwestycji. Ponadto umożliwia ono przechowywanie poświadczeń w przeglądarkach internetowych, kartach inteligentnych bądź tokenach USB. Na przykład certyfikaty cyfrowe RSA można połączyć z hybrydowym tokenem

SecurID 800 w celu skonsolidowania wielu poświadczeń w ramach jednego urządzenia, co ułatwia użytkownikom korzystanie z tego rozwiązania. Dodatkowe składniki rozwiązania RSA Digital Certificate Solution to m.in. RSA Registration Manager, RSA Validation Manager, RSA Key Recovery Module oraz RSA Root Signing Services.

## Informacje o firmie RSA

RSA, oddział EMC zajmujący się zabezpieczeniami, jest czołową 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.



www.rsa.com

EMC2, EMC, RSA, SecurID oraz logo RSA to zastrzeżone znaki towarowe i/lub znaki towarowe firmy EMC Corporation w Stanach Zjednoczonych i/lub innych krajach. Pozostałe wymienione produkty i usługi stanowią znaki towarowe odpowiednich podmiotów.

DECTR WP 1210