



RSA® Authentication Deployment Manager

Internetowe rozwiązanie do szybkiego wdrażania systemu RSA SecurID®

Oprogramowanie RSA® Authentication Deployment Manager pozwala obniżyć koszty wdrożenia i obsługi rozwiązania RSA SecurID®, oferując możliwość rozdystrybuowania, przypisania i aktywacji tokenów. System automatyzuje cały proces wydawania tokena - włącznie z wysłaniem żądania przez użytkowników, zatwierdzeniem żądania przez przełożonego, wprowadzaniem danych użytkowników do systemu RSA® Authentication Manager oraz aktywacją / przypisaniem tokenu sprzętowego lub programowego. RSA Authentication Deployment Manager jest rozwiązaniem niezwykle elastycznym, doskonale nadającym się zarówno dla przedsiębiorstw, jak i do zastosowań związanych z e-biznesem.

NAJWAŻNIEJSZE CECHY

- System szybkiego, taniego wdrażania sprzętowych i programowych tokenów RSA SecurID
- Funkcje samoobsługowe pozwalające na zmniejszenie kosztów
- Elastyczność pozwalająca na dopasowanie wdrożenia i samoobsługi użytkowników do zasad obowiązujących w firmie
- Wydajność i skalowalność zaspokajające potrzeby wdrożeń dla różnej liczby użytkowników

SZYBKIE WDRAŻANIE SPRZĘTOWYCH I PROGRAMOWYCH TOKENÓW RSA SECURID

System RSA Authentication Deployment Manager przyspiesza wydawanie użytkownikom sprzętowych i programowych tokenów RSA SecurID. Bez niego zadania identyfikacji zatwierdzonych użytkowników, przypisywania poświadczeń poszczególnym użytkownikom i wprowadzania danych użytkowników do bazy danych uwierzytelniania programu RSA Authentication Manager musiałyby być wykonywane centralnie przez administratorów. Authentication Deployment Manager pozwala zautomatyzować pracę administracyjną związaną z wydawaniem sprzętowych i programowych tokenów SecurID oraz ułatwia szybkie i tanie wdrożenie rozwiązania RSA SecurID.

SAMOBSŁUGOWA ZMIANA KODU PIN PRZEZ UŻYTKOWNIKÓW

Czy to ze względów bezpieczeństwa, czy przez zwykłe zapomnienie, może się czasami zdarzyć, że użytkownik musi zmienić swój kod PIN. Funkcja samoobsługowej zmiany kodu PIN umożliwia każdemu użytkownikowi wybranie nowego kodu bez potrzeby zwracania się do stanowiska pomocy lub administratora. Jeśli użytkownik pamięta swój kod PIN, może po prostu uwierzytelnić się w programie Authentication Deployment Manager za pomocą swojego hasła RSA SecurID, a następnie wprowadzić nowy kod PIN. Jeśli natomiast użytkownik zapomni swój kod PIN, może wybrać nowy, ale musi najpierw uwierzytelnić się w programie Authentication Deployment Manager, udzielając poprawnej odpowiedzi na pewną liczbę pytań zdefiniowanych przez administratora oprogramowania. Po uwierzytelnieniu użytkownik może zmienić swój kod PIN. Cały proces zmiany kodu PIN może przebiegać bez angażowania administratora. Dzięki temu zmniejszają się koszty utrzymania stanowiska pomocy, a jednocześnie zwiększa zadowolenie i wydajność użytkowników.

ZASTĘPOWANIE WYGASAJĄCYCH TOKENÓW SPRZĘTOWYCH

Program RSA Authentication Deployment Manager ułatwia również zastępowanie tokenów sprzętowych, które tracą ważność. Gdy użytkownik zostanie powiadomiony, że jego token sprzętowy wkrótce przestanie być ważny, może za jego pomocą uwierzytelnić się w programie Authentication Deployment Manager, aby zamówić nowy token. Zatwierdzenie zamówienia i wydanie nowego tokenu jest możliwe w ramach tej samej sesji programu Authentication Deployment Manager.



Confidence Inspired™

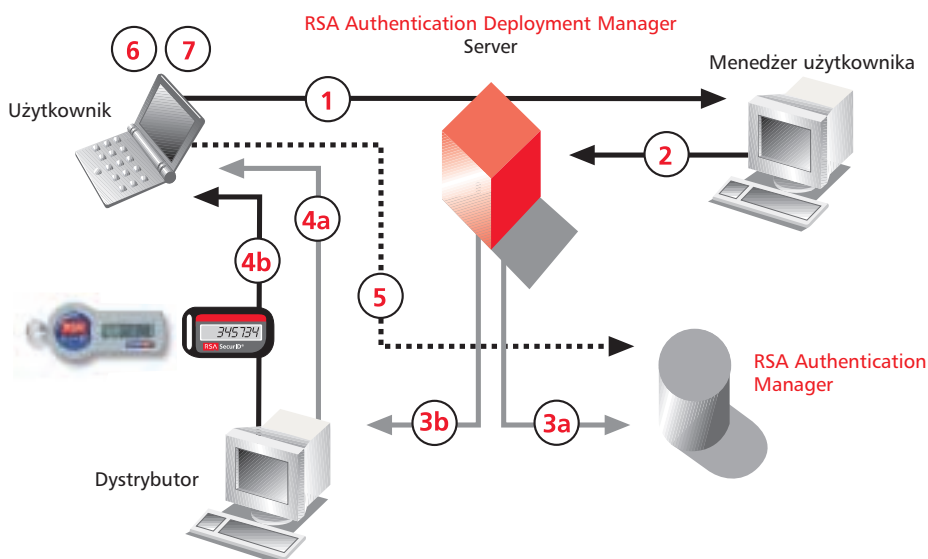
INDYWIDUALNE DOSTOSOWANIE OPROGRAMOWANIA

Program RSA Authentication Deployment Manager można dostosować do dowolnych potrzeb organizacyjnych i wymagań w zakresie zabezpieczeń. Ekran interfejsu użytkownika są napisane w kodzie HTML i mogą zostać rozszerzone o grafikę i terminologię specyficzną dla danej firmy. Bogaty zestaw wbudowanych interfejsów programowania aplikacji (API) umożliwia integrację z dotychczasowymi danymi i procesami. Interfejsy API programu RSA Authentication Deployment Manager umożliwiają weryfikację danych użytkowników. Na przykład przed zatwierdzeniem żądania lub uwierzytelnieniem użytkownika chcącego zmienić kod PIN możliwe jest sprawdzenie hasła użytkownika za pomocą zewnętrznego katalogu LDAP. Następnie można zaimportować wymagane dane, np. adres użytkownika, do wykorzystania w programie Deployment Manager. Zatwierdzone dane można też wyeksportować z programu Deployment Manager do aplikacji zewnętrznych. Interfejsy API mogą być również zastosowane do pełnego zautomatyzowania funkcji menedżera lub dystrybutora, co jeszcze bardziej usprawni proces wdrażania tokenów.

ELASTYCZNOŚĆ I DOSTĘPNOŚĆ

Skalowalne, zawsze dostępne i proste w użyciu oprogramowanie RSA Authentication Deployment Manager pozwala podnieść komfort pracy użytkowników, a jednocześnie skrócić czas wdrożenia, zmniejszyć jego koszty i odciążać administratorów - bez uszczerbku dla bezpieczeństwa systemu dystrybucji i zatwierdzania poświadczeń. Oprogramowanie RSA Authentication Deployment Manager jest dostępne bezpłatnie z licencją RSA Authentication Manager Enterprise Edition lub jako oddzielny produkt do użytku z licencją RSA Authentication Manager Base Edition.

- 1 Użytkownik przesyła zamówienie tokenu.
- 2 Menedżer zatwierdza.
- 3a Informacje o użytkowniku zostają dodane do rekordów oprogramowania RSA Authentication Manager
- 3b Dystrybutor zostaje powiadomiony.
- 4a Kod zatwierdzenia zostaje wysłany.
- 4b Następuje wydanie tokenu.
- 5 Użytkownik przesyła numer seryjny tokenu z kodem zatwierdzenia.
- 6 Aktywacja tokenu.
- 7 Uwierzytelnienie po raz pierwszy (tryb nowego kodu PIN).



RSA, logo RSA, SecurID, ClearTrust, Keon i IntelliAccess są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub w innych krajach. Microsoft i Windows są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach. Sun i Java są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Sun Microsystems Inc. w Stanach Zjednoczonych i/lub w innych krajach. Citrix i MetaFrame są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Citrix Systems Inc. w Stanach Zjednoczonych i w innych krajach. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.

© 2005 RSA Security Inc. Wszelkie prawa zastrzeżone.

Autoryzowany partner:

