Rozwiązania w zakresie uwierzytelnienia sprzętowego dla łączności VPN

Autoryzacja sprzętowa w systemach VPN

Uwierzytelnienie sprzętowe bazuje na koncepcji identyfikacji użytkownika poprzez „coś, co użytkownik ma" w przeciwieństwie do tradycyjnego uwierzytelnienia opartego na hasłach - „coś, co użytkownik wie". W systemach VPN bazujących na protokole IPsec lub SSL uwierzytelnienie sprzętowe zapewnia podwyższony poziom bezpieczeństwa autoryzacji użytkowników i w rezultacie podnosi bezpieczeństwo całości systemu zdalnego dostępu.

Dostępne rozwiązania

Uwierzytelnienie sprzętowe może wykorzystywać różne technologie, przy czym wybór właściwego rozwiązania zdeterminowany jest przez takie czynniki jak: potrzeby w zakresie autoryzacji, rodzaj wykorzystywanego sprzętu sieciowego (koncentratora VPN), liczby użytkowników, dodatkowych potrzeb (np. integracji z domeną Windows) i oczywiście ceny zakupu, wdrożenia oraz utrzymania.

Dostępne na rynku i w naszej ofercie rozwiązania występują w następujących wariantach:

- tokeny USB i karty inteligentne (tj. Smart Cards - „SC")
- tokeny z wyświetlaczem LCD - typu "breloczek"
- tokeny softwarowe, instalowane na smartfonach
- autoryzacja poprzez SMS
- inne, np. tokeny hybrydowe OTP/USB, tokeny Cronto

Tokeny USB i karty inteligentne

Rozwiązanie wykorzystuje kryptograficzny token realizujący funkcje sprzętowej kryptografii symetrycznej i asymetrycznej oraz bezpiecznego przechowania kluczy (klucze prywatne nigdy nie opuszczają pamięci tokena). W niektórych przypadkach token oferuje możliwość uruchamiania programów (np. appletów Java – tzw. JavaCard). Token kryptograficzny wyglądem zewnętrznym łudząco przypomina pendrive, nie należy jednak utożsamiać go ze zwykłą pamięcią USB.

Kryptograficzny token USB widoczny jest przez system operacyjny jako składnica certyfikatów cyfrowych zgodnych ze standardem X509v3 (PKI). Autoryzacja wykorzystuje kryptografię klucza publicznego. Dostęp do pamięci tokenu chroniony jest PIN-em, który użytkownik musi podać po podłączeniu tokenu do komputera. Zaletą rozwiązania autoryzacji bazującej na certyfikatach i PKI jest brak konieczności stosowania serwera uwierzytelniajacego dostępnego on-line – uwierzytelnienie odbywa się na podstawie hierarchii zaufania certyfikatów. Dokładniej wady i zalety rozwiązania przedstawiono w tabelce dalej.

SmartCard to rozwiązanie funkcjonalnie równoważne tokenom USB i bazujące zazwyczaj na tych samych chipach. Jedyna istotna różnica tkwi w sprzęcie: w przypadku tokenu USB karta i czytnik zintegrowane zostały w jednym urządzeniu, zaś w przypadku kart czytnik USB jest zewnętrznym urządzeniem. Karta jest rozwiązaniem mniej wygodnym niż token, pozwala jednak na umieszczenie dodatkowej informacji: zdjęcia użytkownika, nadruku, kodu paskowego, itp.

Tokeny z wyświetlaczem

Systemy te generują hasła jednorazowe OTP (OTP - One Time Password). Hasło jest pseudo-losowe i bazuje na aktualnym czasie (time based) lub na poprzednio wygenerowanej sekwencji (event based). Wielką zaletą tokenów OTP jest możliwość wykorzystania w każdych warunkach, gdyż nie są one fizycznie podłączane do komputera. Dostępne są też od niedawna tokeny hybrydowe łączące cechy tokena USB oraz OTP. Hasło jednorazowe generowane przez token może być używane zamiast lub w połączeniu z tradycyjnym hasłem statycznym. Autoryzacja OTP wymaga serwera uwierzytelniającego dostępnego on-line (typowo jest to serwer RADIUS). Serwer ten może być autonomiczny lub współpracować z innym serwisem autoryzacji - np. z Microsoft AD. Dokładniej wady i zalety rozwiązania przedstawiono w tabelce poniżej.

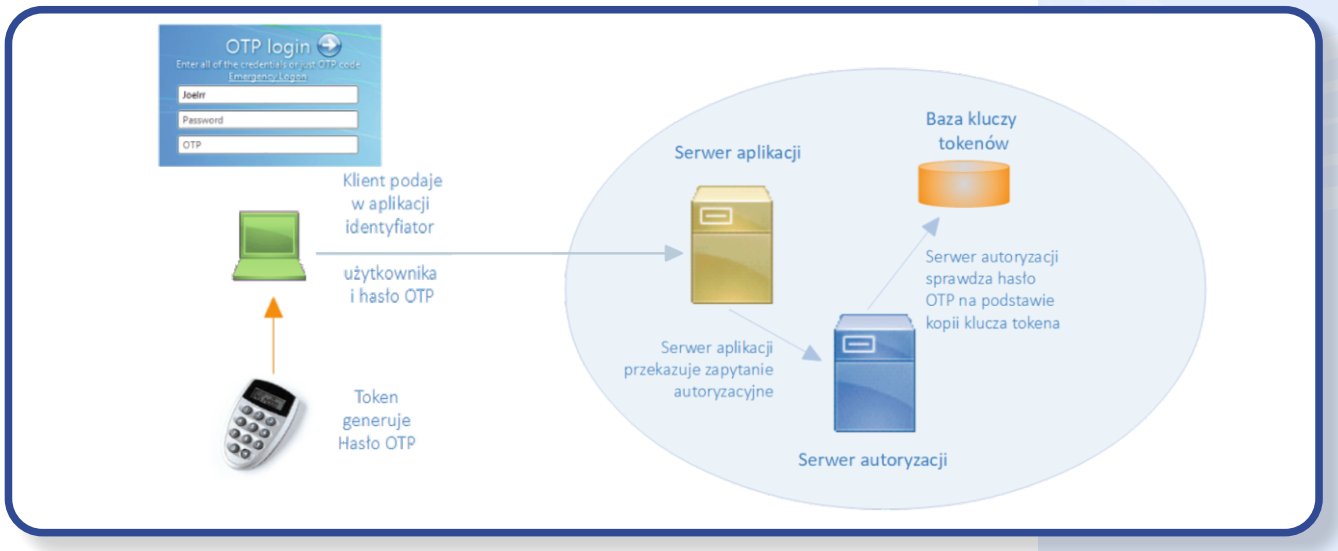
Dostępne są też tokeny zaopatrzone w klawiaturę (tzw. token „kalkulator" lub „pin-pad") działające na zasadzie Challenge-Response (hasło-odzew). Typowo nie wykorzystuje się ich jednak w autoryzacji VPN.

Token softwarowy zainstalowany na telefonie

Token softwarowy jest „emulacją" tokena OTP na telefonie komórkowym; posiada wszystkie cechy standardowego „sprzętowego" tokena: sekret i możliwość zabezpieczenia PIN-em. Podobnie jak w przypadku „sprzętowego" tokena nie ma fizycznego połączenia pomiędzy telefonem, a serwerem autoryzacyjnym, weryfikacja następuje po przepisaniu hasła OTP z telefonu do okienka aplikacji. Dystrybucja tokenów i ich danych inicjalizacyjnych odbywać się może na kilka sposób - np. poprzez WWW lub WAP-push.

Tokeny wirtualne SMS

Token SMS to wirtualny token realizowany wyłącznie po stronie serwerowej, autoryzacja sprowadza się do przesłania SMS-a z systemu autoryzacji na telefon użytkownika. Kod przesłany SMS-em powinien być przez użytkownika zwrotnie wprowadzony do aplikacji celem weryfikacji. Sprzętowy czynnik autoryzacji to fakt posiadania przez użytkownika telefonu o określonym numerze. Integracja systemu uwierzytelnienia SMS z infrastruturą VPN odbywa się podobnie do integracji z systemem OTP - wymagany jest serwer uwierzytelniający dostępny on-line, najczęściej jest to serwer zgodny z protokołem RADIUS. Dodatkowo konieczne jest wysyłanie SMS - funkcję tę realizować można bezpośrednio - np. poprzez modem GSM lub za pośrednictwem bramki Web-owej (usługa dostępna w abonamencie).



Rysunek 1 – system VPN z autoryzacją tokenową (dotyczy autoryzacji przy pomocy: tokenów OTP, tokenów HID, haseł SMS oraz tokenów instalowanych na telefonach).

Systemy chmurowe - SaaS (Software as a Service)

W modelu tym wdrożenie autoryzacji 2FA bardzo się uprościło - użytkownicy otrzymują tokeny fizyczne lub instalują aplikację na smartfonie, administrator konfiguruje reguły dostępu i przeprowadza integrację systemu autoryzacji z firewallem lub bramką VPN, jednak cały system autoryzacji znajduje się na serwerach chmurowych. Dzięki temu firma posiada kontrolę administracyjną nad dostępem użytkowników, nie ponosi jednak kosztów amortyzacji i eksploatacji serwerów uwierzytelniających.

Podsumowanie i porównanie parametrów

Cecha / rozwiązanie	Tokeny USB i karty	Tokeny OTP (z wyświetlaczem)	Hasła SMS	Tokeny na telefonie
sposób autoryzacji	certyfikat	hasło jednorazowe	hasło jednorazowe	hasło jednorazowe
wymagany software na końcówce	driver & klient	-	-	-
wymagany serwer on-line	-	tak, lub serwer chmurowy	tak, lub serwer chmurowy	tak, lub serwer chmurowy
wymagany dodatkowy software	System wystawiania certyfikatów: np. MS CA lub OpenSSL dla większych instalacji wskazany system zarządzania tokenami	-	bramka SMS (np. poprzez serwis webowy)	system dystrybucji na telefony (zintegrowany z serwerem autoryzacji)
zalety	• proste wdrożenie • wiele innych zastosowań: np. szyfrowanie dysków i dokumentów, autoryzacja SSL, ...	• nie wymaga instalacji oprogramowania na końcówkach	• nie wymaga instalacji oprogramowania na końcówkach	• nie wymaga instalacji • oprogramowania na końcówkach • niskie koszty eksploatacji
wady	• wymaga dostępu do portu USB użytkownika • wymaga instalacji oprogramowania na końcówce • dla większej liczby użytkowników (>100) zarządzanie może się komplikować	• wymaga serwera on-line • ograniczone zastosowanie do innych celów niż autoryzacja VPN	• wymaga serwera on-line • ograniczone zastosowanie do innych celów niż autoryzacja VPN • koszt wysłania SMS	• wymaga serwera on-line • ograniczone zastosowanie do innych celów niż autoryzacja VPN

Przegląd rozwiązań:

W zakresie systemów autoryzacji sprzętowej oferujemy rozwiązania następujących producentów:

gemalto HID VASCO WHEEL SYSTEMS

Poniżej podsumowaliśmy najważniejsze cechy oferowanych przez nas rozwiązań. Należy zaznaczyć, że podsumowanie to ma charakter ogólny i poglądowy, gdyż producenci oferują zazwyczaj produkty o bardzo dużej rozpiętości funkcji oraz cen:

Producent	Cechy
Gemalto (dawniej SafeNet)	szeroka gama rozwiązań 2FA: tokeny wszystkich rodzajów, system autoryzacji chmurowej SAS, systemy zarządzania tokenami.
Vasco	Lider rozwiązań OTP. Tokeny autonomiczne OTP typu „breloczek" i „pin-pad", bardzo szeroka gama tokenów i software-u autoryzacyjnego.
Wheel Systems	CERB: systemy dla telefonów komórkowych: tokeny SMS i tokeny na telefon
HID Global (dawniej ActivIdentity)	szeroka gama rozwiązań 2FA: karty SC, tokeny OTP, oprogramowanie zarządzające.

Bezpieczeństwo Sieci

Co oferujemy?

Na wdrożenie systemu autoryzacji składa się: określenie założeń technicznych i biznesowych, wybór producenta i rozwiązania, dostarczenie licencji, sformułowanie polityki bezpieczeństwa, instalacja, konfiguracja, testowanie (audyt bezpieczeństwa) oraz szkolenia. Jesteśmy gotowi do współpracy w każdym z tych obszarów, dysponujemy wiedzą, doświadczeniem oraz odpowiednio przeszkoloną kadrą. Szeroki wybór oferowanych przez nas rozwiązań gwarantuje, że system przez nas zaproponowany będzie nie tylko bezpieczny, wydajny i funkcjonalny, ale także optymalnie dostosowany do Państwa potrzeb - zapraszamy do współpracy!

Wybrane referencje CC w zakresie rozwiązań zdalnego dostępu i autoryzacji:

- Allianz S.A.
- Bank BPS S.A.
- Banki Spółdzielcze
- GPW S.A. w Warszawie
- Krajowa Izba Rozliczeniowa S.A.
- Lufthansa Systems Poland sp. z o.o.
- mBank S.A.
- Opera TFI S.A.
- Ubezpieczeniowy Fundusz Gwarancyjny
- TUiR Warta S.A.

CC Otwarte Systemy Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: sales@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach: http://www.cc.com.pl/

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Techniczny: tech@cc.com.pl