# 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 rowiązania zdeterminowany jest przez takie czynniki jak: potrzeby w zakresie autoryzacji, rodzaj wykorzystywanego sprzętu sieciowego (koncentratora VPN), liczby użytkowników, dodatkowych potrzeb (np. integracjiz 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 (tzw.: Smart Cards - „SC")
- tokeny z wyświetlaczem LCD - typu "breloczek"
- tokeny softwarowe, w tym głównie instalowane na telefonach GSM
- autoryzacja poprzez SMS
- inne, np. tokeny HID

### 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 więc kryptografię klucza publicznego. Dostęp do pamięci tokenu chroniony jest PIN-em,



ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

który użytkownik musi podać po podłączeniu tokenu do komputera. (Token może też być wykorzystany jako składnica haseł statycznych jednak to rozwiązanie nie zapewnia takiego poziomu bezpieczeństwa, jak PKI). Wykorzystanie tokena wymaga instalacji drivera oraz programu integrujacego token ze składem certyfikatów systemu operacyjnego. Zaletą rozwiazania autoryzacji bazującej na certyfikatach i PKI jest brak konieczności stosowania serwera uwierzytelniajacego dostępnego on-line – uwierzytelneinie odbywa się na podstawie hierarchii zaufania certyfikatów. Dokładniej wady i zalety rozwiązania przedstawiono w tabelce dalej.

SmartCard to rozwiązanie funkcjonalnie równoważne tokenom USB i bazujace 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 ponizej.

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.

**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).

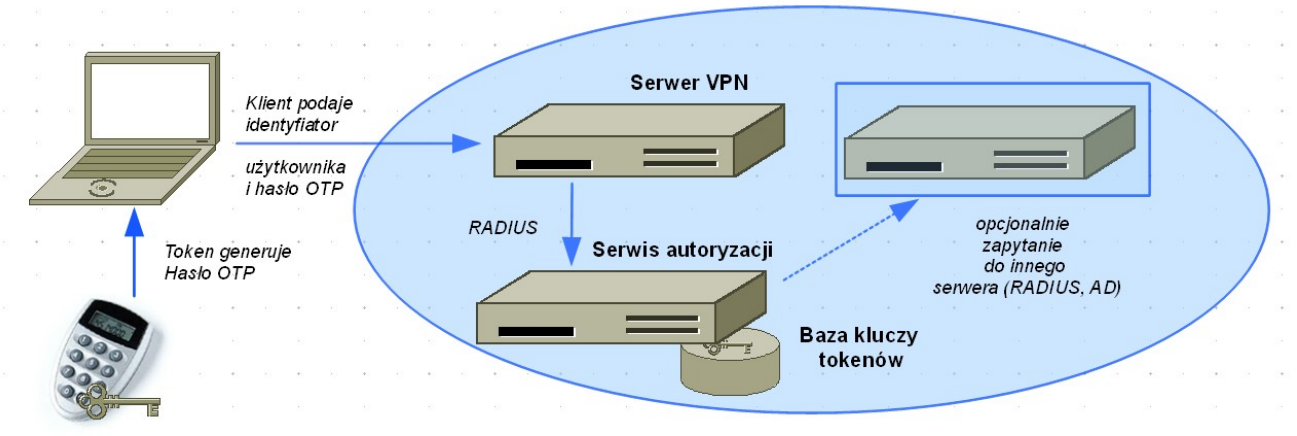

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

### 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 HID

Tokeny HID (Human Interface Device) stanowią specyficzną grupę rozwiązań oferowanych obecnie tylko przez jednego producenta. Zasada działanie tokena HID stanowi połaczenie koncepcji tokena USB z tokenem OTP. Token HID generuje hasło jednorazowe w podobny sposób jak token OTP z wyświetlaczem, tj. hasło generowane jest jak funkcja tajnego klucza, liczby losowej, znacznika czasu lub licznika zdarzeń i kilku dodatkowych parametrów. Ponieważ token funkcjonuje w systemie jako urządzenie typu „klawiatura" to generowane hasło pojawia się w aktualnie wybranym polu aktywnego formularza – nie ma konieczności przepisywania hasła, co jest znaczącym ułatwieniem w stosunku do tokena OTP. Wielką zaletą tokena HID jest to, że nie wymaga on instalacji żadnych sterowników.




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



ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

## 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 | - | - | - |
| **Wymagny serwer on-line** | - | tak, typowo serwer lub middleware RADIUS | tak, typowo terwer lub middleware RADIUS | tak, typowo terwer lub middleware RADIUS |
| **Wymagany dodatkowy software** | System wystawiania certyfikatow: np. MS CA, openssl lub xca<br>dla większych instalacji serwer OCSP oraz system zarzadzania tokenami | - | bramka SMS (np. poprzez serwis webowy) | system dystrybucji na telefony (zintegrowany z serwerem autoryzacji) |
| **Zalety** | • proste wdrożenie<br>• 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<br>• niskie koszty eksploatacji |
| **Wady** | • wymaga dostępu do portu USB użytkownika<br>• wyamga instalacji oprogramowania na końcówce<br>• dla większej liczby użytkowników (>100) zarządzanie może się komplikować | • Wymaga serwera on-line<br>• ograniczone zastosowanie do innych celów niż autoryzacja VPN | • Wymaga serwera on-line<br>• ograniczone zastosowanie do innych celów niż autoryzacja VPN<br>• koszt wysłania SMS | • Wymaga serwera on-line<br>• ograniczone zastosowanie do innych celów niż autoryzacja VPN |


ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

**Przegląd rozwiązań:**

W zakresie systemów autoryzacji sprzętowej oferujemy rozwiązania następujących producentów:

- SafeNet (d. Aladdin)
- ActivIdentity
- DataKey
- Vasco
- YubiCo
- 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 |
|---|---|
| SafeNet (Aladdin) | Tokeny USB, wszechstrona autoryzacja do zasobów lokalnych i sieciowych, w tym VPN, serwery WWW i inne. Dostępne są tokeny zintegrowane z dyskiem flash (1 GB, 2 GB, 4 GB ) oraz zaopatrzone w opcje bezprzewodowe: HID, RFID i inne. Oprogramowanie do integracji z serwerami sieciowymi (ActivDirectory i inne) oraz do zarządzania tokenami. |
| Vasco | Lider rozwiązań OTP. Tokeny autonomiczne OTP typu „breloczek" i „pin-pad", b. szeroka gama tokenów i software-u autoryzacyjnego. |
| Wheel | CERB: systemy dla telefonów komórkowych: tokeny SMS i tokeny na telefon |
| ActivIdentity | Wszechstrona autoryzacja do zasobów lokalnych i sieciowych, w tym VPN. Oprogramowanie do integracji z serwerami sieciowymi (ActiveDirectory). Także rozwiązania typu tokeny OTP i "kalkulator". Sprzęt OEM, przeznaczony głównie do rozwiązań dużej skali. |
| YubiCo | Tokeny HID z interfejsem USB – symulujące wpisanie hasła jednorazowego z klawiatury |


ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

**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 ochrony danych:**

- Auchan Polska sp. z o.o.,
- CA IB S.A.
- Urząd M.st. Warszawa – Ursynów,
- Coffee Heaven Intl. Sp. z o.o.
- Sodexho Pass Polska Sp z o.o.
- FM Polska Sp z o.o. (FM Logistic)
- Metropolitan Life Ubezpieczenia na Życie S.A.,
- Krajowe Biuro Wyborcze
- Narodowe Centrum Badań Jądrowych w Świerku
- Nestle Polska S.A.
- Sodexo Pass Polska Sp. z o.o.
- PZU-CL Agent Transferowy S.A.,
- BRE Corporate Finance S.A.,
- WestLB Bank Polska S.A.,
- Poczta Polska S.A. - Centrum Badawczo Szkoleniowe,
- Provident Polska S.A.,
- RockWool Polska S.A.,
- Opera TFI
- Biuro Trybunału Konstytucyjnego
- Uniwersytet Warszawski, Wydział Chemii
- Teva Kutno S.A.

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

**Osoby kontaktowe:**

Dział Techniczny: tech@cc.com.pl

Dział Handlowy: sales@cc.com.pl


ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/