Rozwiązania w zakresie autoryzacji OTP

(One Time Password - hasła jednorazowe)

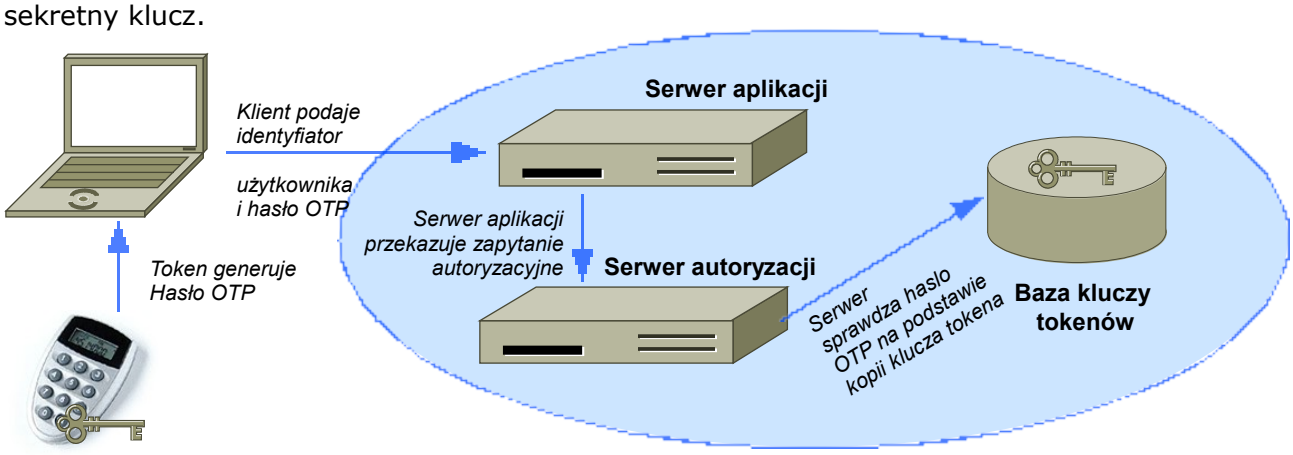
Autoryzacja sprzętowa

Systemy autoryzacji sprzętowej pełnią wiele funkcji w przedsiębiorstwie, do najważniejszych należą:

- **autoryzacja** użytkowników w zakresie:
  - dostępu do aplikacji, w szczególności aplikacji Web
  - dostępu do lokalnego system operacyjnego (stanowiska pracy - stacji roboczej),
  - dostępu do zdalnych zasobów (np. domeny systemu Windows 2003/2008),
  - dostępu tzw. pre-boot (autoryzacja w celu uruchomienia komputera),
  - dostępu do zasobów sieciowych poprzez VPN (IPsec, SSL VPN),
- **zabezpieczenia zasobów dyskowych** notebooków, stacji roboczych i serwerów porzez szyfrowanie,
- **zabezpieczenie dokumentów** elektronicznych i poczty elektronicznej poprzez podpisy elektroniczne i szyfrowanie.

Autoryzacja OTP

Autoryzacja OTP (One Time Password) polega najogólniej mówiąc na wykorzystaniu sprzętowego lub programowego generatora haseł jednorazowych. Każda operacja wymagająca autoryzacji (np. zlecenie przelewu, zalogowanie się do systemu, itp.) musi być uwierzytelniona poprzez podanie hasła. Hasła jednorazowe mają charakter pseudo-losowy – na podstawie dowolnie długiego ciągu ostatnio wykorzystanych haseł nie da się odgadnąć hasła kolejnego. Dodatkowo, haslo może też być generowane na podstawie aktualnego czasu, co tym bardziej utrudnia jego odgadnięcie. W rzeczywistości hasła nie są całkowicie losowe, lecz generowane na podstawie tajnego klucza wbudowanego w token. Kopia tego klucza znajduje się na serwerze autoryzacyjnym, serwer po otrzymaniu identyfikatora użytkownika oraz hasla OTP jest w stanie sprawdzić, czy hasło zostalo faktycznie wygenerowane przez token posiadający właściwy sekretny klucz.



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/

Integracja z systemem autoryzacji

Klient zazwyczaj podaje swoje dane identyfikacyjne i hasło OTP do serwera aplikacji (np. aplikacji webowej, systemu operacyjnego, koncentratora VPN), z którego zostaje przekazane do właściwego systemu autoryzacyjnego. Serwerowy komponent systemu OTP przechowuje zawsze bazę kluczy tokenów, tzw. „sekretów", dzięki temu serwer jest w stanie stwierdzić, czy hasło generowane przez dany token jest poprawne. Istnieją trzy najbardziej popularne rozwiązania integracji z systemem autoryzacji:

- **serwer RADIUS** – usługa dostępna w sieci, zazwyczaj stosowana przy autoryzacji logowania do systemu operacyjnego i VPN,
- **biblioteka** – wymaga dostosowania i rekompilacji kodu, najczęściej wykorzystywane w dedykowanych aplikacjach (np. e-bankowości),
- **dedykowany protokół sieciowy** – łączy cechy obydwu powyższych rozwiązań.

Dostępne typy tokenów

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

- tokeny typu "kalkulator" - z wyświetlaczem i klawiaturką numeryczną,
- tokeny typu "breloczek" - z wyświetlaczem,
- token HID – z interfejsem USB,
- token SMS,
- token softwarowy zainstalowany na telefonie.

Tokeny typu kalkulator (pinpad)

Tokeny te generują hasła jednorazowe wg. określonej sekretem sekwencji lub bazujące na aktualnym czasie, niektóre mogą też działać w trybie Challenge-Response (hasło-odzew). W trybie Ch-Rp użytkownik wprowadza tzw. „Challenge" - sekwencję cyfr wygenerowaną przez aplikację przeprowadzajacą autoryzację, token generuje odpowiedź - „Response", którą wprowadza się do aplikacji. Ponieważ powiązanie Ch – Rp następuje poprzez sekret tokenu serwer autoryzacyjny może sprawdzić, czy właściwy token wygenerował odpowiedź. Tokeny typu kalkulator zazwyczaj chronione są PIN-em, który użytkownik musi wprowadzić przed dokonaniem jekiejkolwiek innej operacji.

Tokeny typu breloczek

Tokeny typu breloczek są uproszczoną wersją tokenów typu kalkulator: nie posiadają możliwości ochrony PIN-em i pracy w trybie Challenge-Response, cechuje je za to większa trwałość i niższy koszt.

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/

Tokeny hybrydowy OTP-USB

Wielką zaletą sprzętowych tokenów OTP z wyświetlaczem jest możliwość ich 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. Tokeny te mogą być zaopatrzone w klawiaturę, nie jest to jednak wymogiem.

Tokeny HID

Tokeny HID (Human Interface Device) stanowią specyficzną grupę rozwiązań oferowanych obecnie tylko przez jednego producenta. Zasada działanie tokena HID stanowi połączenie 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" (urządzenie HID) 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.

Tokeny EMV-CAP

Tokeny te działają podobnie jak tokeny typu kalkulator, jednak sekretny klucz przechowywany jest na wymiennej karcie zgodnej ze standardem EMV-CAP. Tokeny takie znajdują zastosowanie w bankowości elektronicznej i mogą służyć np. do realizacji autoryzacji w płatnościach internetowych.

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.

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.

Rozwiązanie	Zastosowania	Zalety i wady
Tokeny z wyświetlaczem "breloczek" lub "kalkulator"	• Autoryzacja do systemach i zasobów sieciowych • Autoryzacja w VPN • Autoryzacja do aplikacji WWW • Autoryzacja do arbitralnych aplikacji	• Prócz tokena nie wymaga żadnych zasobów sprzętowych lub programowych po stronie użytkownika - rozwiązania czysto serwerowe • niezawodność i prostota • niski koszt **Wady:** • ograniczone możliwości (brak kryptografii asymetrycznej, brak "prawdziwego" podpisu)
Token SMS	• Autoryzacja do aplikacji, zazwyczaj „konsumenckich"	• Nie wymaga zadnych z zasobów lub oprogramowania po stronie użytkownika, • prostota użytkownia. **Wady:** • dodatkowe koszty eksploatacji związane z wysyłaniem SMS-ów, • ograniczone możliwości (brak kryptografii asymetrycznej, brak "prawdziwego" podpisu).
Token softwarowy zainstalowany na telefonie	• Autoryzacja do systemach i zasobów sieciowych • Autoryzacja do aplikacji, zazwyczaj „konsumenckich"	• Nie wymaga żadnych zasobów lub oprogramowania po stronie użytkownika, • możliwość realizacji, dodatkowych funkcji autoryzacji w aplikacji, • brak kosztów telekomunikacyjnych. **Wady:** • wymaga instalacji aplikacji na telefonie – kwestie wsparcia dla użytkowników i zgodności sprzętowej

Przegląd rozwiązań:

W zakresie systemów autoryzacji sprzętowej oferujemy rozwiązania następujących producentów:

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/

- Aladdin / SafeNet
- ActivIdentity (d. ActivCard)
- Vasco
- YubiCo

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**
Aladdin / SafeNet	Tokeny USB, OTP i hybrydowe USB-OTP oferują wszechstronną autoryzację do zasobow lokalnych i sieciowych, w tym: VPN i serwerów WWW. Dostępne są tokeny zintegrowane z dyskiem flash (4, 8, 16 GB) oraz zaopatrzone w opcje bezprzewodowe: HID, RFID i inne. Oprogramowanie do integracji z serwerami sieciowymi (ActivDirectory i inne) oraz do zarządzania tokenami.
ActivIdentity	Karty SC i tokeny USB, wszechstrona autoryzacja do zasobów lokalnych i sieciowych, w tym VPN. Oprogramowanie do integracji z serwerami sieciowymi (ActiveDirectory). Także rozwiązania typu tokeny OTP i "kalkulator".
Vasco	Tokeny autonomiczne OTP, tokeny SMS, tokeny EMV-CAP
YubiCo	Tokeny HID z interfejsem USB – symulujące wpisanie hasła jednorazowego z klawiatury.
Wheel	Tokeny SMS i token softwarowey na telefon.

Co oferujemy?
Na wdrożenie systemu autoryzacji składa się: określenie założeń technicznych i biznesowych, wybór 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:

- Agencja Mienia Wojskowego,
- Biuro Trybunału Konstytucyjnego
- BRE Corporate Finance S.A.,
- Coffee Heaven Intl. Sp. z o.o.
- Krajowe Biuro Wyborcze
- Ministerstwo Sprawiedliwości
- Nestle Polska S.A.
- Najwyższa Izba Kontroli
- Wojskowa Akademia Techniczna,
- Opera TFI
- PGE Dystrybucja S.A.
- Provident Polska S.A.,
- WestLB Bank Polska S.A.,
- Ubezpieczeniowy Fundusz Gwarancyjny
- Unicredit CA IB S.A.
- Urząd M.st. Warszawa – Ursynów,
- Sodexho Pass Polska Sp z o.o.
- Teva Kutno S.A.

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

Kontakt:
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/