Rozwiązania w zakresie autoryzacji OTP
(One Time Password - hasła jednorazowe)

Autoryzacja sprzętowa

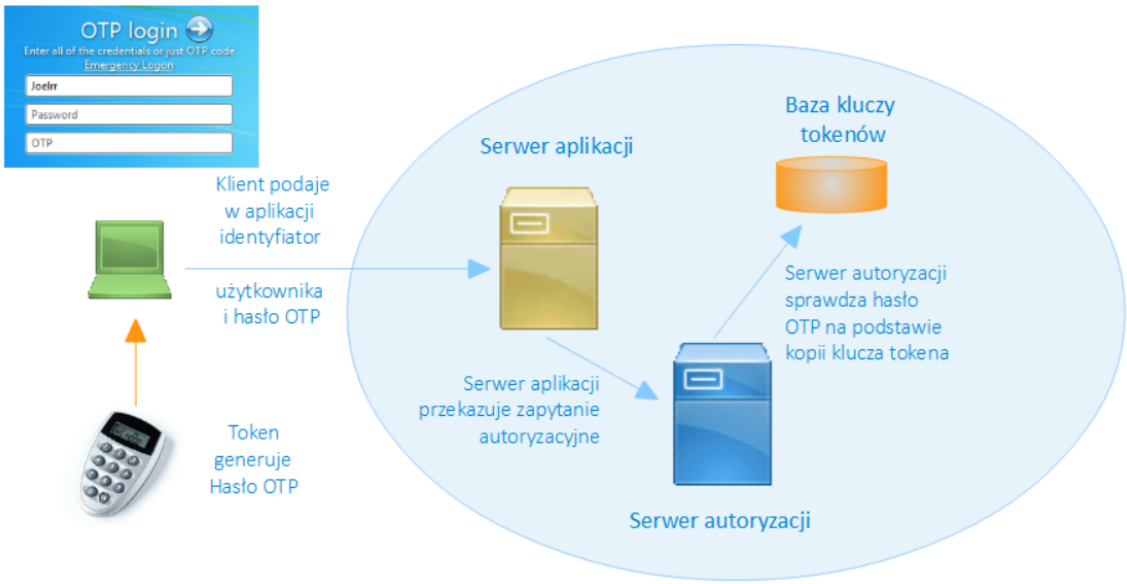
Systemy autoryzacji sprzętowej pełnią wiele funkcji w przedsiębiorstwie, do najważniejszych należą:

- autoryzacja użytkowników w zakresie:
    - dostępu do zasobów sieciowych poprzez VPN (IPsec, SSL VPN),
    - dostępu do aplikacji, w szczególności aplikacji Web
    - dostępu do lokalnego system operacyjnego (stanowiska pracy - stacji roboczej),
    - dostępu do zdalnych zasobów (np. domeny systemu Windows),
    - dostępu tzw. pre-boot (autoryzacja w celu uruchomienia komputera).
- 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 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 kolejnego hasła. 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.

Ogólny sposób autoryzacji OTP w dostępie do aplikacji (podobnie dla systemów zdalnego dostępu i innych systemów IT)



Integracja z systemem autoryzacji

Klient 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 (API)** – wymaga dostosowania i rekompilacji kodu, najczęściej wykorzystywane w dedykowanych aplikacjach (np. e-bankowości),
- **protokół autoryzacyjny** – łączy cechy obydwu powyższych rozwiązań, protokoły autoryzacyjne buduje się na bazie XML – np. SAML lub metodyki REST.

Dostępne typy tokenów

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

- **tokeny typu "kalkulator"** (pinpad) - z wyświetlaczem i klawiaturką numeryczną,
- **tokeny typu "breloczek"** - z wyświetlaczem,
- **tokeny "Cronto"** – z kamerką i wyświetlaczem rozpoznające kody 2D,
- **tokeny OTP** ze zintegrowanym **czytnikiem kart EMV**
- **tokeny hybrydowe** – OTP / PKI
- **token HID** – z interfejsem USB,
- **token SMS** – wirtualny token bazujacy na wysyłce kodów i informacji weryfikacyjnych poprzez SMS,
- **token softwarowy** zainstalowany na telefonie,
- **token chmurowy** – działający zgodnie z koncepcją SaaS (Software as a Service)

token typu "kalkulator"

Tokeny te generują pseudo-loso hasła jednorazowe w określonej sekwencji. Hasło generowane jest na podstawie sekretnego klucza wbudowanego w token. Klawiatura pozwala na odblokowanie tokenu poprzez podanie PIN-u. Tokeny te 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. Challenge, podawany przez użytkownika w aplikacjach typu e-banking, może być kilkuczynnikowy i może zawierać np. kwotę transakcji oraz fragmentu numeru konta. Dzięki takiej autoryzacji aplikacje bankowe zgodne są z aktualnymi normami i wytycznymi branżowymi, zarówno **PCI-DSS** jak i np. dyrektywą **PSD2** obowiązującą w UE.

token 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: dłuższy czas życia baterii, większa trwałość i niższy koszt.

token typu "Cronto" – z kamerką i wyświetlaczem rozpoznający kody 2D

Tokeny typu Cronto działają na zasadzie podobnej do aplikacji rozpoznających kody QR – token posiada kamerkę i wyświetlacz, użytkownik wczytuje kod wyświetlany na ekranie komputera przez aplikację wymagającą uwierzytelnienia (np. aplikację e-bankingu wymagającą autoryzacji przelewu), token wyświetla szczegóły transakcji i generuje hasło jednorazowe, które należy wprowadzić do aplikacji. Rozwiązanie to zwalnia użytkownika z etapu wprowadzania frazy „Challenge" zachowując jednocześnie bezpieczeństwo uwierzytelnienia sprzętowego.

tokeny OTP ze zintegrowanym **czytnikiem kart EMV**

Tokeny te działają podobnie jak tokeny typu kalkulator, jednak sekretny klucz przechowywany jest na wymiennej karcie „bankowej" zgodnej ze standardem EMV-CAP. Tokeny takie znajdują zastosowanie w bankowości elektronicznej i mogą służyć np. do realizacji autoryzacji w płatnościach internetowych. Tokeny zintegrowane z czytnikiem kart są dostępne w wariancie „standalone": token generuje hasło OTP na wyświetlaczu oraz w wariancie z Bluetooth: token współpracuje ze smartfonem poprzez Bluetooth – telefon automatycznie uwierzytelnia się poprzez token w aplikacji zaś użytkownik nie musi wykonywać żadnych dodatkowych działań.

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 tokeny hybrydowe łączące cechy tokena USB oraz OTP. Tokeny te mogą być zaopatrzone w klawiaturę, nie jest to jednak wymogiem.

Tokeny typu 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.

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.

Tokeny chmurowe

Token chmurowy funkcjonuje jako oprogramowanie dostępne w modelu **SaaS** (Software as a Service), tj. emulacja tokena ma miejsce na serwerach chmurowych. Zaletą tego rozwiązania jest wysoka dostępność, prostota wykorzystania i minimalizacja kosztów administracyjnych – czynności administracyjne sprowadzają się tu do działań operatorskich takich jak: wygenerowanie lub usunięcie wirtualnego tokena, administracją serwerami i platformą systemu zajmuje się operator chmury. Wadą tokenów SaaS jest kompromis związany z bezpieczeństwem – sekrety tokenów umieszczone są poza naszą organizacją.

Jakie rozwiązanie tokenowe wybrać?

Poniżej przedstawiamy możliwe scenariusze rozwiązań tokenowych dla różnych zastosowań i branż:

Autoryzacja **zdalnego dostępu** (systemy VPN: Ipsec oraz SSL VPN):

- Tokeny PKI
- Tokeny OTP typu breloczek
- Tokeny SMS i instalowane na telefonie
- Tokeny chmurowe

Autoryzacja **loginu do systemu** i autoryzacja w aplikacjach niekrytycznych:

- Tokeny PKI
- Tokeny hybrydowe
- Tokeny chmurowe

Autoryzacja dostępu do **aplikacji bankowych i transakcyjnych** oraz innych aplikacji dla których obowiązują dodatkowe regulacje branżowe narzucające podwyższony poziom bezpieczeństwa autoryzacji:

- Tokeny OTP typu pinpad
- Tokeny Cronto
- Tokeny EMV

Autoryzacja pre-boot i dostępu do lokalnego systemu:

- Tokeny PKI/USB lub hybrydowe

Producenci: