

Tokeny software'owe

Przegląd rozwiązań



Spis treści

Streszczenie	3
1. Wprowadzenie	4
2. Bezpieczny przekaz informacji.....	5
2.1. Aktualne zabezpieczenia transakcyjne na rynku bankowym.....	5
2.2. Architektury systemów uwierzytelniających.....	8
2.3. Standardy uwierzytelniania dla tokenów software'owych.....	10
3. Przykłady obecnej implementacji tokenów software'owych.....	11
3.1. Obecne rozwiązania dla sektora bankowego	11
3.2. Prototypowe rozwiązanie firmy Verax Systems	12
Oferta Verax Systems dla sektora finansowego	13

Streszczenie

Niniejsza publikacja prezentuje możliwości zastosowania tokenów software'owych, jako skutecznej metody zabezpieczania komunikacji pomiędzy bankiem a użytkownikami w dwuczynnikowej metodzie uwierzytelniania. Przedstawione zostaną przykłady dostępnych na rynku rozwiązań oraz ich ocena z punktu widzenia poziomu bezpieczeństwa oraz kosztów wdrożenia.

1. Wprowadzenie

Efektywne systemy zabezpieczania transakcji na rynku instytucji finansowych charakteryzują się zazwyczaj wysokimi kosztami. W dużej mierze koszty te ponoszone są przez banki lub przenoszone na klientów końcowych, którzy obecnie muszą płacić za usługi SMS'owego potwierdzania transakcji, wydanie tokena sprzętowego czy też podpisu elektronicznego. Idea tokenów software'owych polega na ograniczeniu tych kosztów poprzez udostępnienie bezpiecznego, efektywnego oraz tańszego w użytkowaniu systemu. Banki są w stanie ograniczyć nie tylko koszty ale również poprawić jakość swoich usług poprzez dostosowanie tego rozwiązania do wymagań klientów. Według PWPW S.A. oraz portalu bankier.pl tokeny software'owe to obecnie najsilniejsza metoda potwierdzania transakcji na polskim rynku i stanowi optymalne zabezpieczenie przed phishingem (wyłudzeniem poufnych informacji), atakami man-in-the-middle (polegającymi na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami) oraz man-in-the-browser (opiera się na trojanie).

2. Bezpieczny przekaz informacji

2.1. Aktualne zabezpieczenia transakcyjne na rynku bankowym

Obecnym standardem w zabezpieczaniu przesyłu informacji pomiędzy klientem a bankiem jest dwuczynnikowa metoda uwierzytelniania. Polega ona na weryfikacji działań użytkowników za pomocą dwóch elementów. Pierwszym z nich jest *something you know* (coś, o co znasz), która opiera się na ustalonym wcześniej ciągu znaków (hasło lub numerze PIN) znanym tylko przez bank oraz klienta. Drugi element to zazwyczaj *something you have* (coś, co posiadasz). Do tej kategorii należą karty, podpisy elektroniczne, tokeny hardware'owe oraz inne urządzenia będące w posiadaniu użytkownika. Same urządzenia często są chronione dodatkowym kodem zabezpieczającym na wypadek dostania się w niepowołane ręce.

Dwuczynnikowa metoda uwierzytelniania

Na dwuczynnikową metodę składają się: *coś, co znasz* (hasło lub numer PIN) oraz *coś, co posiadasz* (na przykład klucz zapisany w tokenie). Wyróżnia się dwa mechanizmy uwierzytelniania:

- Shared Secret
- Architektura klucza publicznego

Tokeny software'owe wykorzystują obecnie trzy metody uwierzytelniania opracowane według standardów ustalonych przez Initiative for Open Authentication (OATH), oparte na:

- Liczniku (ang. counter)
- Czasie (ang. time-synchronised)
- Systemie wezwanie-odpowiedź (ang. challenge-response)

Te trzy mechanizmy są skutecznie wykorzystywane w tokenach software'owych udostępnianych przez następujące instytucje:

- Pekao SA
- Eurobank
- PKO BP (Inteligo)
- mToken PWPW S.A.

W dwuczynnikowym systemie zabezpieczeń można wykorzystać następujące metody:

Hasło lub numer PIN

Hasło lub numer PIN jest jednym z najczęściej stosowanych mechanizmów zabezpieczeń w bankowości elektronicznej. Sprowadza się do nadania przez bank numeru PIN lub sprecyzowania przez klienta hasła. Należą do kategorii *coś, co znasz*. Ich główną zaletą jest łatwość obsługi, uniwersalność oraz relatywnie niski koszt. Niestety hasło nie jest bezpiecznym rozwiązaniem, jeżeli jest używane jako jedyna metoda uwierzytelniania.

OTP hardware token

OTP (ang. *One Time Password*) hardware token to urządzenie, które użytkownik wykorzystuje do generowania haseł jednorazowych wykorzystywanych przy uwierzytelnianiu operacji bankowych. Token generuje kody na bazie zapisanego w nim ukrytego hasła. Plusem tego rozwiązania jest otrzymanie kodu od razu, prostota użytkowania oraz brak możliwości skopiowania przez osoby trzecie. Koszty uzyskania takiego tokena oraz możliwość zgubienia urządzenia przez użytkownika to główne zagrożenia w tej metodzie.

Tokeny software'owe - przegląd rozwiązań

Zabezpieczenie biometryczne

Ten rodzaj zabezpieczeń jest aktualnie najrzadziej stosowany w praktyce. Polega na potwierdzeniu przekazywanej informacji za pomocą unikalnej cechy użytkownika, takiej jak układ linii papilarnych lub wzór siatkówki oka. Takie rozwiązanie jest niezwykle kosztowne, dlatego też nie jest stosowane na szeroka skalę. Niewątpliwym plusem jest bezpieczeństwo, jakie zapewnia.

Mobilny podpis elektroniczny wykorzystujący PKI

Mobilny podpis elektroniczny na bazie infrastruktury klucza publicznego (ang. *Public Key Infrastructure*) to podpis elektroniczny stworzony przy pomocy urządzenia mobilnego i bazujący na autoryzacji lub usługach certyfikujących w środowisku telekomunikacyjnym, niezależnym od aktualnego miejsca pobytu. Zaletami takiego rozwiązania są mobilność oraz prostota użytkowania. Metoda ta wiąże się jednak z przeniesieniem części procesu uwierzytelniającego na operatora telekomunikacyjnego, przez co generuje większe koszty oraz obniża bezpieczeństwo.

Podpis elektroniczny wykorzystujący PKI

Tak jak w przypadku mobilnego podpisu elektronicznego działa na zasadzie klucza publicznego i prywatnego, który jest zazwyczaj przechowywany w urządzeniu bądź programie, zależnie od formy. Urządzenie lub program zawierające podpis elektroniczny szyfruje go za pomocą klucza publicznego i przesyła do banku w celu weryfikacji transakcji. Zaletą tej metody jest uwierzytelnianie klientów za pomocą dwóch czynników (klucza publicznego oraz podpisu elektronicznego). Rozwiązanie niesie ze sobą koszty związane z integracją i wsparciem po stronie użytkownika, niską mobilność oraz wrażliwość na ataki koni trojańskich.

Uwierzytelnienie poprzez jednorazowe hasło SMS

Obecnie w wielu bankach wykorzystuje się wiadomości SMS jako podstawowe medium dla kodów uwierzytelniających. Po zalogowaniu klienta oraz podaniu hasła w celu potwierdzenia złożenia dyspozycji, wysyłany jest SMS z kodem autoryzującym. Po poprawnym wpisaniu otrzymanego kodu następuje uwierzytelnienie operacji. Takie rozwiązanie jest wystarczająco skuteczne z tego względu, iż zapewnia dwa czynniki uwierzytelniające (hasło oraz kod z wiadomości SMS) i mobilność. Telefon komórkowy jest urządzeniem, które zawsze nosimy ze sobą, a koszty SMS'ów nie są na tyle wygórowane, by stanowić dużą barierę. Niestety nie wszyscy pozostają w zasięgu sieci komórkowych cały czas, a możliwości otrzymania odpowiedzi z kodem są głównie uzależnione od ich przepustowości. Dlatego może się zdarzyć sytuacja, że SMS nie dojdzie na czas do klienta, a zawarty w nim kod straci ważność. Koszty jakie ponosi bank przy obsłudze rosnącej liczby klientów korzystających z kodów SMS, są niekiedy większe niż przy wykorzystaniu innych metod uwierzytelniania.

Listy kodów i karty zdrapki

Te dwie metody są tanie i łatwe w użyciu. Wymagają podania podczas uwierzytelniania odpowiedniego kodu z listy lub umieszczonego pod zdrapką na specjalnej karcie. Kody mogą być używane podczas logowania do systemu bankowości elektronicznej lub autoryzacji zleconych przelewów. Charakteryzują się niskim poziomem bezpieczeństwa, ponieważ są łatwe do skopiowania. Niektóre kody mają także krótki cykl życia, przez co nie są efektywną metodą uwierzytelniania dla użytkowników rzadziej korzystających z usług bankowości elektronicznej. Koszty tego rozwiązania dla banku są obecnie porównywalne z jednorazowymi hasłami SMS.

CAP/DPA

CAP (ang. *Chip Authentication Programme*) oraz DPA (ang. *Dynamic Passcode Authentication*) to specyfikacje dotyczące używania kart EMV (*Europay, MasterCard, Visa*) podczas uwierzytelniania transakcji dokonywanych przez Internet oraz telefon. Te dwa systemy charakteryzują się odpowiednim poziomem bezpieczeństwa oraz brakiem dodatkowego hasła zabezpieczającego, ponieważ każda karta posiada swój własny numer PIN. Niestety implementacja odpowiednich czytników kart, które umożliwiałyby autoryzację transakcji jest droga, a użyteczność dla niektórych klientów końcowych niewielka.

Tokeny software'owe - przegląd rozwiązań

Token software'owy

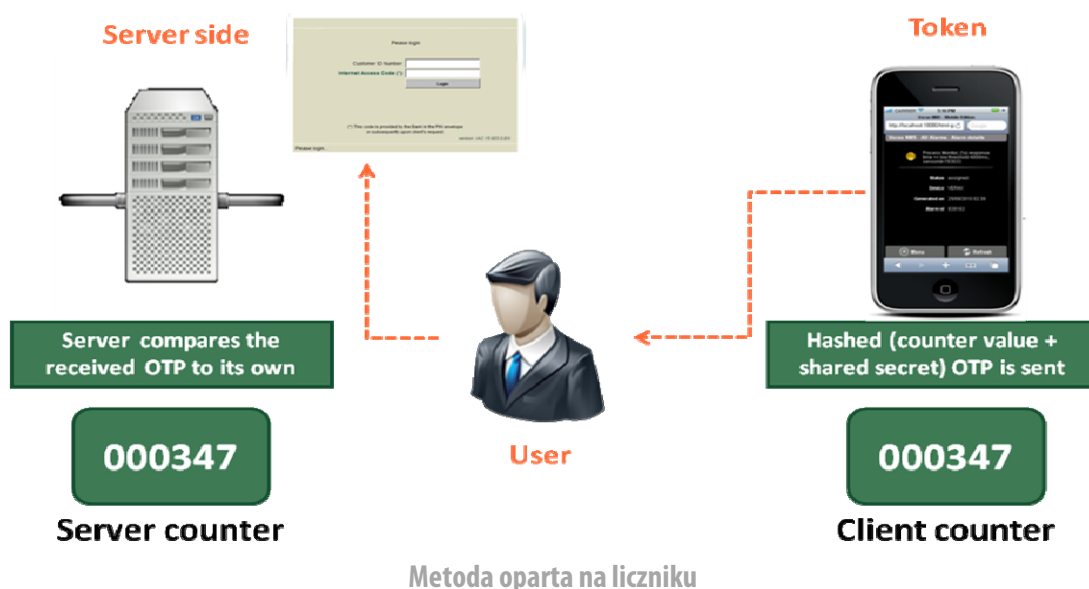
Obecnie tokeny zbudowane w formie programu mogą być stosowane na wielu platformach sprzętowych. Ponadto dają możliwość zastosowania dwuczynnikowej metody uwierzytelniania z uwzględnieniem identyfikacji karty SIM oraz dodatkowym hasłem. Dzięki takiej formie gwarantują wysokie bezpieczeństwo zachowując niski koszt dla użytkownika końcowego. Charakteryzują się wysoką mobilnością, dostępnością i ergonią dzięki możliwości konfiguracji metod i mechanizmów zabezpieczeń przez bank oraz użytkowników końcowych. To rozwiązanie może być zastosowane na wielu platformach zarówno desktopowych jak i mobilnych. Do głównych mankamentów tej metody można zaliczyć możliwość skopiowania tokena oraz utratę lub kradzież telefonu. Obecnie według PWPW S.A. oraz portalu Bankier.pl jest to najsilniejsza metoda potwierdzania transakcji na polskim rynku i stanowi optymalne zabezpieczenie przed phishingem oraz atakami man-in-the-middle i man-in-the-browser.

Metoda zabezpieczenia	Niski koszt	Wysoki poziom bezpieczeństwa	Wygoda użytkownika
Hasło/Numer PIN	+++	+	+++
OTP Hardware Token	++	+++	++
Zabezpieczenie biometryczne	+	+++	++
Mobilny podpis elektroniczny PKI	++	++	+++
Podpis elektroniczny wykorzystujący PKI	++	+++	++
Jednorazowe hasło SMS	++	+++	++
Listy kodów/karty zdrapki	++	++	+
CAP/DPA	+	+++	+
Token software'owy	+++	+++	+++

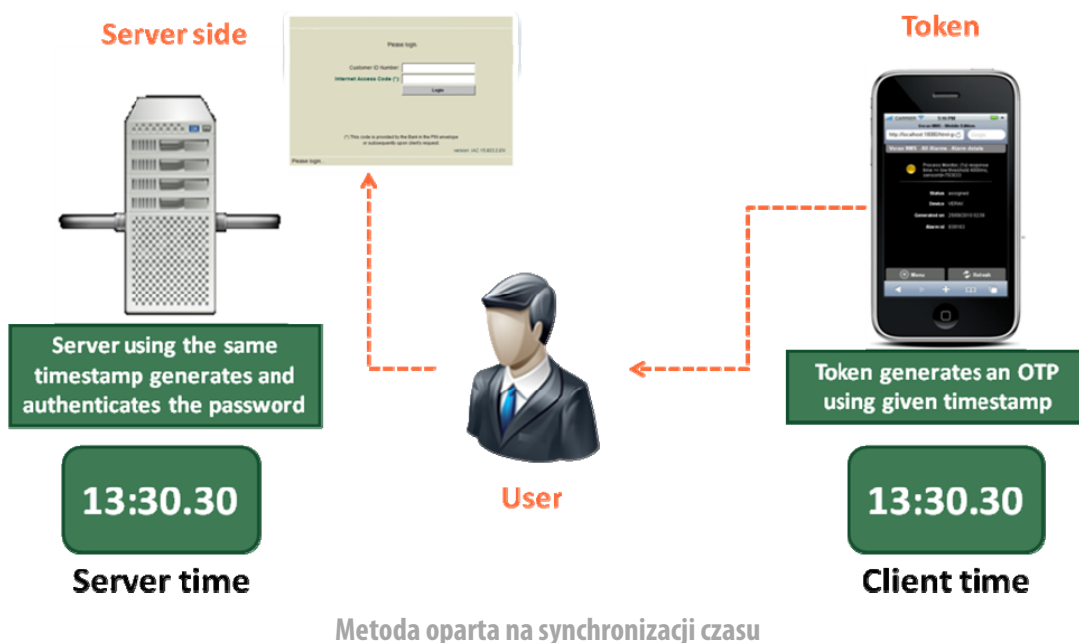
Tabela1: Porównanie dostępnych metod

2.2. Architektury systemów uwierzytelniających

Jednym z systemów uwierzytelniania w architekturze *shared secret* jest metoda wykorzystująca licznik. Polega na generowaniu zaszyfrowanego hasła na podstawie zapisanego w tokenie *shared secret* i wartości licznika. Każda próba wygenerowania hasła potrzebnego do uwierzytelnienia użytkownika zwiększa licznik o jedną jednostkę. Serwer po stronie banku także posiada swój licznik, który zwiększa się o jedną jednostkę podczas każdego poprawnego logowania. Na tej samej zasadzie generuje kod uwierzytelniający i porównuje z otrzymanym z tokena.

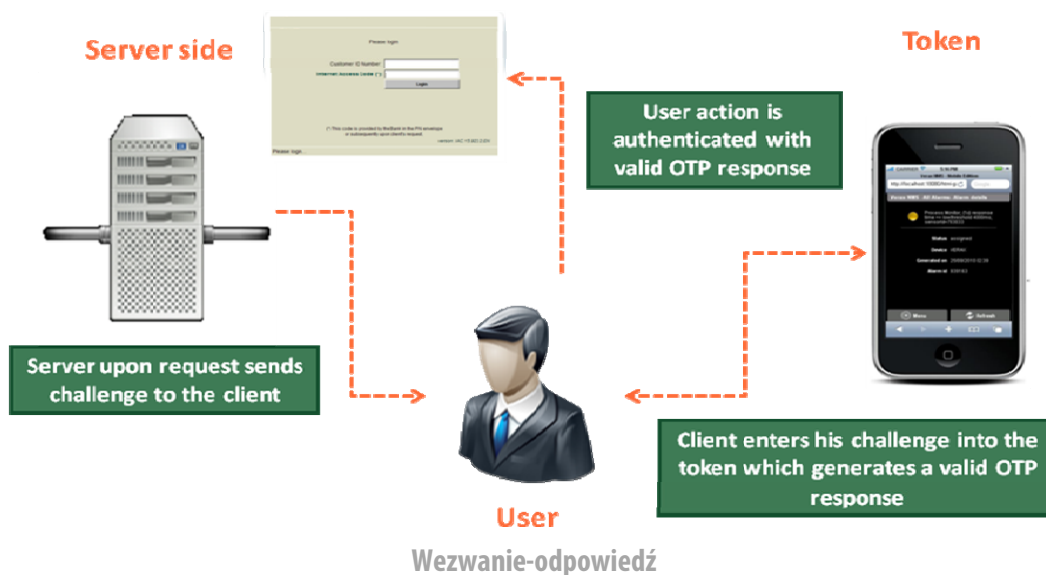


W przypadku gdy występuje zgodność, użytkownik zostaje uwierzytelniony. Jednym z mankamentów tej metody jest możliwość rozszynchronizowania wartości licznika (poprzez niewykorzystanie wygenerowanych przez token kodów). Z tego powodu serwer uwierzytelniający sprawdza od kilku do kilkunastu kodów w przód, aby znaleźć odpowiednią pasującą wartość hasła jednorazowego. W celu ponownej synchronizacji liczników serwer może poprosić użytkownika o podanie kilku (2-3) kolejnych kodów wygenerowanych przez token.

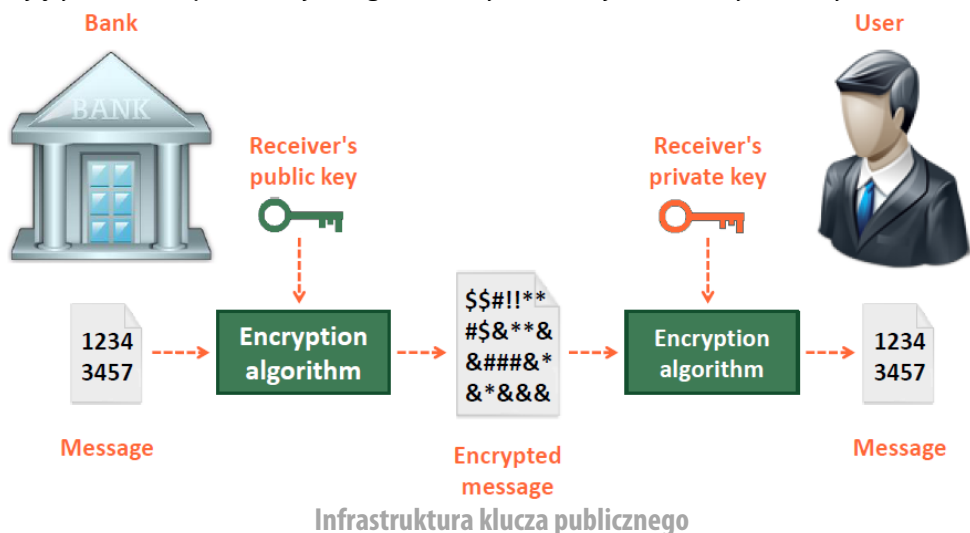


Tokeny software'owe - przegląd rozwiązań

Druga metoda wykorzystuje aktualny czas, określone jego interwały (na przykład 30 sekund) oraz zapisany w tokenie software'owym *shared secret* w celu zaszyfrowania hasła uwierzytelniającego. Zegar tokena jest zsynchronizowany z zegarem na serwerze po stronie banku. Wygenerowane i zaszyfrowane hasło z tokena jest uwierzytelniane w określonym interwale czasowym. Standardowo przyjmuje się liczbę 2 interwałów. Zatem hasło wygenerowane o 15:43.30 będzie ważne między 15:42.30 a 15:44.30 (biorąc pod uwagę przyjęty interwał równy 30 sekund oraz weryfikację serwera na podstawie 2 interwałów w przód i w tył). Zegar tokena oraz serwera podlegają synchronizacji podczas pierwszej instalacji. Z biegiem czasu może nastąpić rozsynchronizowanie zegarów obydwu urządzeń. Jeżeli występuje taka sytuacja, serwer zapisuje, o ile interwałów spiesz się lub spóźnia (wobec zegara serwera uwierzytelniającego) zegar w tokenie. Podczas kolejnych prób uwierzytelniania, serwer uwzględni tę ilość interwałów przy autoryzacji i zaakceptuje dane hasło jednorazowe przy aktualnej dla niego wartości czasu.



Kolejną metodą uwierzytelniania jest wezwanie-odpowiedź. Funkcjonuje na innej zasadzie niż poprzednie. W pierwszej fazie użytkownik tokena software'owego zgłasza swoje żądanie na stronie banku. Bankowy system uwierzytelniający wysyła wezwanie (ciąg znaków), które użytkownik wprowadza do tokena. Ten z kolei korzystając z zapisanego w nim *shared secret* oraz otrzymanego wezwania (opcjonalnie także z innych parametrów) generuje zaszyfowaną odpowiedź. Klient wprowadza odpowiedź na stronie banku (lub w aplikacji klienckiej) po czym jest ona weryfikowana przez serwer uwierzytelniający. Jeżeli odpowiedź jest zgodna, użytkownik jest uwierzytelniany.



Architektura szyfrowania kluczem publicznym to inny rodzaj zabezpieczenia, także oparty na metodzie szyfrowania ciągu znaków. W tym przypadku zamiast jednego klucza *shared secret*, który był znany tylko przez użytkownika oraz bank, używa się dwóch osobnych kluczy: prywatnego oraz publicznego. Klucz publiczny jest znany przez bank i każda informacja przesyłana z banku do klienta jest szyfrowana za pomocą tego klucza oraz odpowiedniego dla niego algorytmu. Do odszyfrowania takiej wiadomości użytkownik korzysta ze swojego klucza prywatnego. Komunikacja w przeciwną stronę odbywa się na tej samej zasadzie. Klucz publiczny jest powszechnie dostępny i łatwy do spreycyzowania, jeżeli jest się w posiadaniu skorelowanego z nim klucza prywatnego. Czas jaki jest potrzebny, aby korzystając z klucza publicznego dojść do tego, jak wygląda klucz prywatny użytkownika, wynosi około sześciu miesięcy nieprzerwanych obliczeń. Z tego powodu ten rodzaj architektury jest uznawany za metodę bezpieczną.

2.3. Standardy uwierzytelniania dla tokenów software'owych

Standardy OATH (Initiative for Open Authentication)

Kradzież oraz nieautoryzowany dostęp do poufnych danych są powodem nieustannego zagrożenia. Brak możliwości bezpiecznego udostępniania danych ogranicza także zdolność organizacji do prowadzenia działalności w sposób efektywny.

Inicjatywa na rzecz otwartego uwierzytelniania (OATH) proponuje rozwiązania standaryzowane - otwartą technologię, która jest dostępna dla wszystkich. OATH używa wszechstronnego podejścia, dostarczając reguły, które pozwalają na uwierzytelnianie wszystkich użytkowników korzystających z różnych urządzeń i środowisk programowych.

Inicjatywa OATH określiła standardy mechanizmów uwierzytelniania dla architektur *shared secret* oraz szyfrowania kluczem publicznym. Poniżej znajduje się ich krótka charakterystyka

Standardowe mechanizmy dla architektury *shared secret*

HMAC (Hashed Message Authentication Code)

Jest to mechanizm uwierzytelniający informacje korzystający z kryptograficznej funkcji *hash*. HMAC może być wykorzystywany z jakąkolwiek kryptograficzną funkcją szyfrującą *hash*, na przykład SHA-1 lub SHA-2, w kombinacji z kluczem *shared secret*.

Rozwinięcie standardu HMAC jest wykorzystywane w następujących systemach uwierzytelniania:

HOTP (Hashed One-Time Password)

W tym systemie do wartości *shared secret* dodawana jest wartość licznika, po czym następuje hashowanie wyniku. Na tej podstawie określana jest wartość hasła jednorazowego.

TOTP (Time-synchronised One-Time Password Algorithm)

Obecne rozwiązanie bazuje na czynniku dynamicznym – wartości czasu. Wariant algorytmu hasła jednorazowego odnoszący się do czasu zapewnia kody z krótkim okresem ważności, które dodatkowo zwiększają bezpieczeństwo.

OCRA (OATH Challenge-Response Algorithms)

OATH zidentyfikowało kilka przypadków, gdzie potrzebna jest asynchroniczna metoda uwierzytelniania danych. Ogólnie akceptowaną metodą wykorzystania tego systemu jest schemat „wezwanie-odpowiedź”. Na rynku istnieją już różne rozwiązania software'owe i hardware'owe, które stosują ten system. W tym przypadku otrzymane hasło jednorazowe generowane jest na podstawie zhashowanej wartości *shared secret* oraz otrzymanego wezwania (ciągu znaków). Otrzymane hasło jednorazowe (OTP) jest przekazywane z powrotem jako odpowiedź.

Standardowe mechanizmy dla architektury szyfrowania kluczem publicznym

PKCS – 11

Standard, który wykorzystuje API o nazwie Cryptoki (ang. cryptographic token interface). Dotyczy urządzeń które posiadają dane i mają wykonywać funkcje kryptograficzne. Cryptoki, stosuje podejście uniwersalne, wykorzystując niezależność technologii (każdy rodzaj urządzenia) oraz współdzielenie zasobów (wiele aplikacji mających dostęp do wielu urządzeń), prezentując aplikacjom wspólny i logiczny obraz urządzenia nazywanego tokenem kryptograficznym.

PKCS – 15

Obejmuje dwie grupy urządzeń. Konwencjonalne tokeny sprzętowe oraz ich wersje software'owe. Standard PKCS - 15 daje użytkownikom możliwość uwierzytelniania podczas korzystania z różnych aplikacji za pomocą tokena kryptograficznego, niezależnie od tego skąd pochodzi Cryptoki (lub interfejs pochodzący od innego dostawcy).

3. Przykłady obecnej implementacji tokenów software'owych

3.1. Obecne rozwiązania dla sektora bankowego

Bank Pekao SA

17 lutego 2010 r. Bank Pekao SA udostępnił bezpłatnie usługę – PekaoToken. Polega ona na generowaniu przy pomocy telefonu komórkowego jednorazowych kodów, służących do akceptowania operacji na rachunkach prowadzonych w Banku Pekao SA oraz w Domu Maklerskim Pekao. Charakterystyka usługi PekaoToken:

- Unikalny kod PekaoToken powiązany z konkretną transakcją
- PekaoToken zainstalowany jest w telefonie
- Token pracuje w trybie opartym na liczniku, czasie lub wezwaniu-odpowiedź
- Został opracowany w technologii Java i może zostać zainstalowany na urządzeniach mobilnych obsługujących ten standard.

Eurobank

TokenGSM posiada własny kod PIN, oddzielny od PIN-u telefonu. Wyświetla na ekranie telefonu informacje o transakcji, która jest autoryzowana i dla tej transakcji generuje kod potwierdzający. Aplikację TokenGSM zainstalować można na każdym telefonie, który posiada funkcję obsługi aplikacji Java. Token wykorzystuje metodę generowania kodów na podstawie licznika oraz wezwaniu-odpowiedź.

Inteligo

Kod wygenerowany przez token jest powiązany tylko z jedną zleconą transakcją. Dodatkowo dostęp do aplikacji chroniony jest kodem PIN. Token nie weryfikuje poprawności wprowadzonego PIN-u – wykorzystywany jest on w procesie generowania odpowiedzi. Jeśli podany zostanie błędny PIN, token będzie generować niewłaściwe kody lub hasła. Token wykorzystuje metody oparte na liczniku, czasie oraz systemie wezwaniu-odpowiedź podczas uwierzytelniania transakcji.

mToken

mToken PWPW S.A. to system uwierzytelnienia dwuskładnikowego, kombinacja hasła statycznego z hasłem jednorazowym, które generowane jest przez aplikację zainstalowaną w telefonie komórkowym. Produkt mToken PWPW S.A. oparty jest na mechanizmach kryptograficznych zgodnych z normami zalecanymi przez OATH Open Authentication Organization. Charakterystyka usługi mToken:

- Wyizolowane środowisko, zarówno po stronie serwera jak i aplikacji telefonicznej, aplikacja nie wykonuje żadnych połączeń sieciowych i nie otrzymuje żadnych informacji tekstowych.
- Przypisanie kodu jednorazowego do konkretnej transakcji

- Krótki okres ważności haseł jednorazowych (time-synchronised)
- Zastosowanie metody challenge-response
- Zabezpieczenie aplikacji kodem PIN użytkownika

3.2. Prototypowe rozwiązanie firmy Verax Systems

Firma Verax Systems przygotowała swoją wersję tokena software'owego opartego na standardach OATH. Obecnie posiada dwa rozwiązania. Pierwszym jest desktopowa wersja tokena oparta o język programowania Borland Turbo C++. Drugim aplikacja na platformy mobilne utworzona w technologii Java Micro Edition. Obydwie rozwiązania funkcjonują przy wykorzystaniu metod licznika, synchronizacji czasu oraz wezwania-odpowiedzi jako systemów uzyskiwania kodów uwierzytelniających. Wersja desktopowa pracuje w środowisku Microsoft Windows, natomiast aplikacja mobilna współpracuje ze wszystkimi urządzeniami obsługujące język Java.

Oferta Verax Systems dla sektora finansowego

Verax Systems to międzynarodowy software house oraz dostawca innowacyjnych i zaawansowanych technologicznie rozwiązań IT.

Verax eBanking Suite składa się z aplikacji i komponentów przeznaczonych dla banków i domów maklerskich dostarczających nowoczesny i zaawansowany graficzny interfejs użytkownika do obsługi elektronicznych kanałów dostępu.

W skład Verax eBanking Suite wchodzi następujące aplikacje:

- Bankowość internetowa dla klientów indywidualnych.
- Narzędzia migracji umożliwiające klientom przenoszenie historii rachunków z innych banków.
- Elektroniczny obrót papierami wartościowymi.
- Bankowość internetowa dla klientów korporacyjnych.
- Bankowość na **urządzenia mobilne i smartfony** (smartbanking).



Cechą charakterystyczną Verax eBanking Suite jest zastosowanie technologii **RIA (Rich Internet Application)** umożliwiającej intuicyjną obsługę (drag and drop, integracja z desktopem) oraz bogate możliwości wizualizacyjne (np. wykresy analizy technicznej).

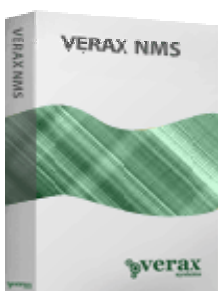


KPI Dashboard to pakiet oprogramowania kontrolingowego z elementami narzędzia typu business intelligence służący do **automatycznego zbierania oraz wizualizacji wskaźników** wydajności przedsiębiorstwa (ang. KPI - Key Performance Indicators) w celu **zwiększenia efektywności** firmy oraz jej zyskowności. Wskaźniki te odzwierciedlają kondycję poszczególnych obszarów działalności przedsiębiorstwa, np. sprzedaży, produkcji, zasobów ludzkich, technicznych i innych.

Oprogramowanie może być stosowane niezależnie od wielkości firmy, jej struktury czy sektora działalności - typy wskaźników, progi itp. są definiowane w zależności od specyficznych potrzeb przedsiębiorstwa i jego wymagań.

APINI jest systemem portalowym Web 2.0 umożliwiającym gromadzenie i wymianę informacji oraz ułatwiającym zarządzanie w przedsiębiorstwach zorientowanych projektowo, których funkcjonowanie oparte jest o wiedzę (knowledge-driven enterprises).

Funkcjonalność systemu obejmuje m. in. bazę wiedzy wiki, bibliotekę dokumentów, zarządzanie zasobami ludzkimi i innymi zasobami, zarządzanie portfelem projektów, **kontroling projektowy** oraz raportowanie. System ułatwia wymianę informacji pomiędzy pracownikami firmy oraz umożliwia gromadzenie **wiedzy w przedsiębiorstwie**, niezależnie od rotacji pracowników lub zmiany ich przydziałów do projektów i zadań.



Verax NMS to wysoce skalowalny, zintegrowany system do zarządzania sieciami, centrami danych oraz aplikacjami, o **pełnej funkcjonalności FCAPS** (fault, configuration, accounting, performance, security) oraz bogatych możliwościach wizualizacyjnych.

Verax NMS redukuje koszty dostarczania usług IT, skraca czasy przestoju oraz zwiększa poziom satysfakcji klienta działów IT **optymalizując procesy** zarządzania, wykrywania problemów oraz ich rozwiązywania.