Uwierzytelnienie hasłami jednorazowymi (OTP) - metody, rozwiązania i zagrożenia

CC Otwarte Systemy Komputerowe Sp. z o.o.

Dr Grzegorz Blinowski

Agenda

- Informacja o firmie CC
- OTP – krótkie przypomnienie metody
- Zastosowania uwierzytelnienia OTP
- Klasyczne rozwiązania OTP:
  - Algorytmy i realizacje OTP
  - OATH
- Co nowego w OTP?
  - Realizacje serwerów
  - Zarządzanie kluczami
  - Obsługa wielu aplikacji
  - Nowe typy tokenów
- Podsumowanie

CC Otwarte Systemy Komputerowe Sp. z o.o.

CC Otwarte Systemy Komputerowe

- Spółka założona w 2001 r.
- Specjalizacja:
  - Bezpieczeństwo systemów i sieci:
    - Systemy firewall, systemy filtracji danych, uwierzytelnianie i autoryzacja
  - Tworzenie oprogramowania na zamówienie
    - Systemy dla klientów finansowych i telco
    - Inne specjalizowane systemy – oprogramowanie naukowe (symulacja, wizualizacja danych); transmisja i konwersja danych, ...

CC Otwarte Systemy Komputerowe Sp. z o.o.

CC Otwarte Systemy Komputerowe

- Przykłady zrealizowanych projektów z zakresu bezpieczeństwa sieci:
  - Zabezpieczenie ogólnopolskiej sieci instytucji rządowej (system firewall-i), 50+ punktów dostępowych, węzeł centralny
  - Zdalny dostęp dla instytucji finansowej: 2000 użytkowników, autoryzacja OTP
  - Filtracja danych e-mail – Operator; Bank: 5000, 8000+ kont pocztowych
  - Sieć WiFi zabezpieczona certyfikatami cyfrowymi z dostępem dla urządzeń mobilnych (zakład produkcyjny)

CC Otwarte Systemy Komputerowe

- Przykłady zrealizowanych projektów z zakresu tworzenia oprogramowania:
  - System bankowości elektronicznej dla klientów biznesowych, autoryzacja za pomocą tokenów OTP
  - System obsługi rejestracji i likwidacji szkód w wyspecjalizowanych polisach ubezpieczeniowych
  - System obsługi windykacji dla banku hipotecznego
  - System obsługi hostingu dla klientów biznesowych operatora telco (kota e-mail serwery WWW, obsługa domen, bazy SQL)

Rozwiązania OTP w naszej ofercie

Vasco –

od ponad 10 lat lider w systemach OTP dla bankowości

Aladdin SafeNet -

czołowy producent rozwiazań PKI token

Wheel –

rozwiązania SMS i „phonetoken” (firma polska)

ActivIdentity –

lider rozwiązań zintegrowanych dla rynku Enterprse

Inne

CC Otwarte Systemy Komputerowe Sp. z o.o.

Trzy podstawowe schematy uwierzytelnienia

- **„Coś co wiemy”**
- Nazwa użytkownika i hasło

Metody klasyczne

- **„Coś co mamy”**
- Nazwa użytkownika, [haslo], sprzętowy generator haseł lub sprzętowy identyfikator

OTP/PKI

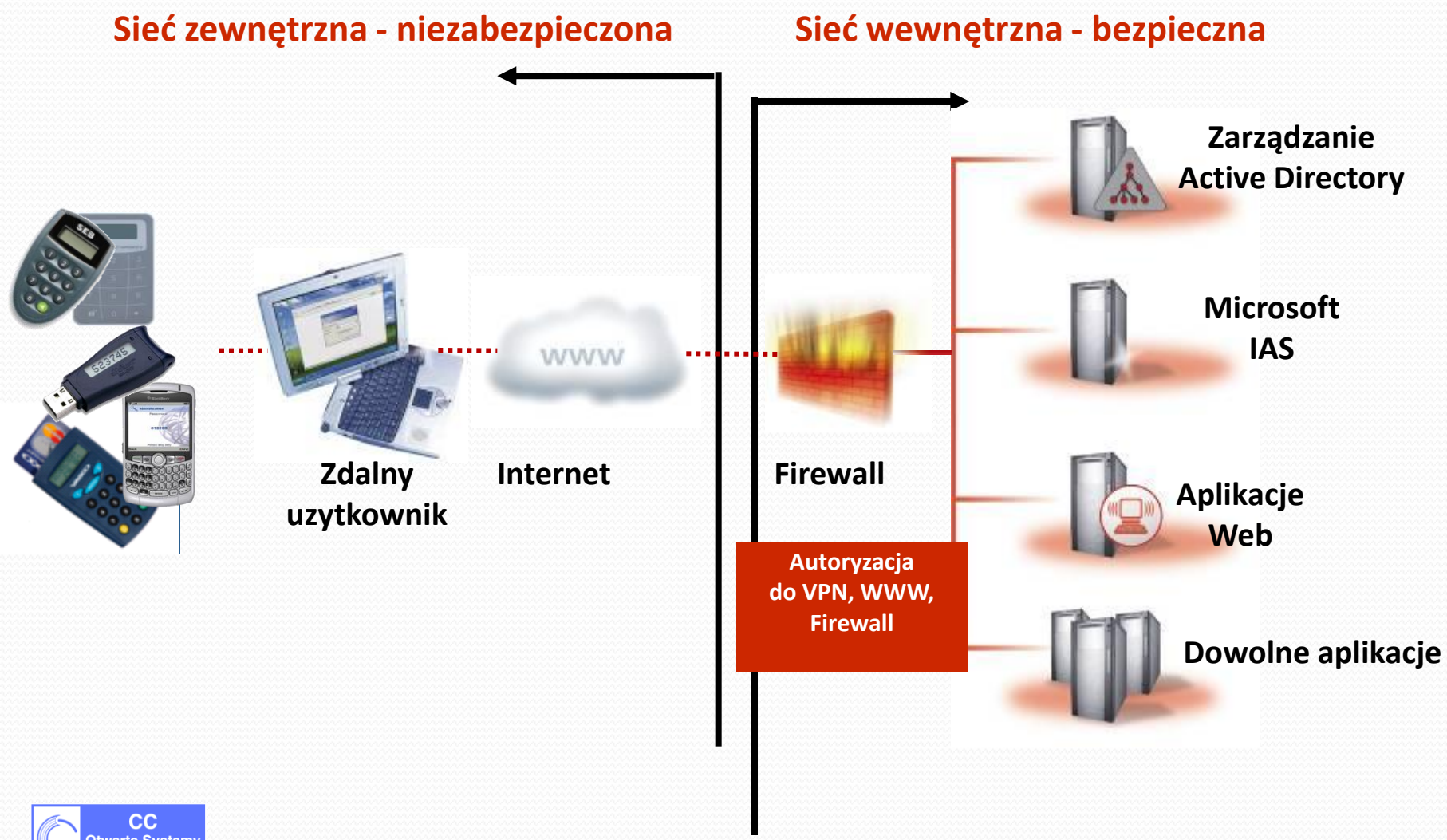
- **„Coś czym jesteśmy”**

Biometria

Do czego może autoryzować OTP?

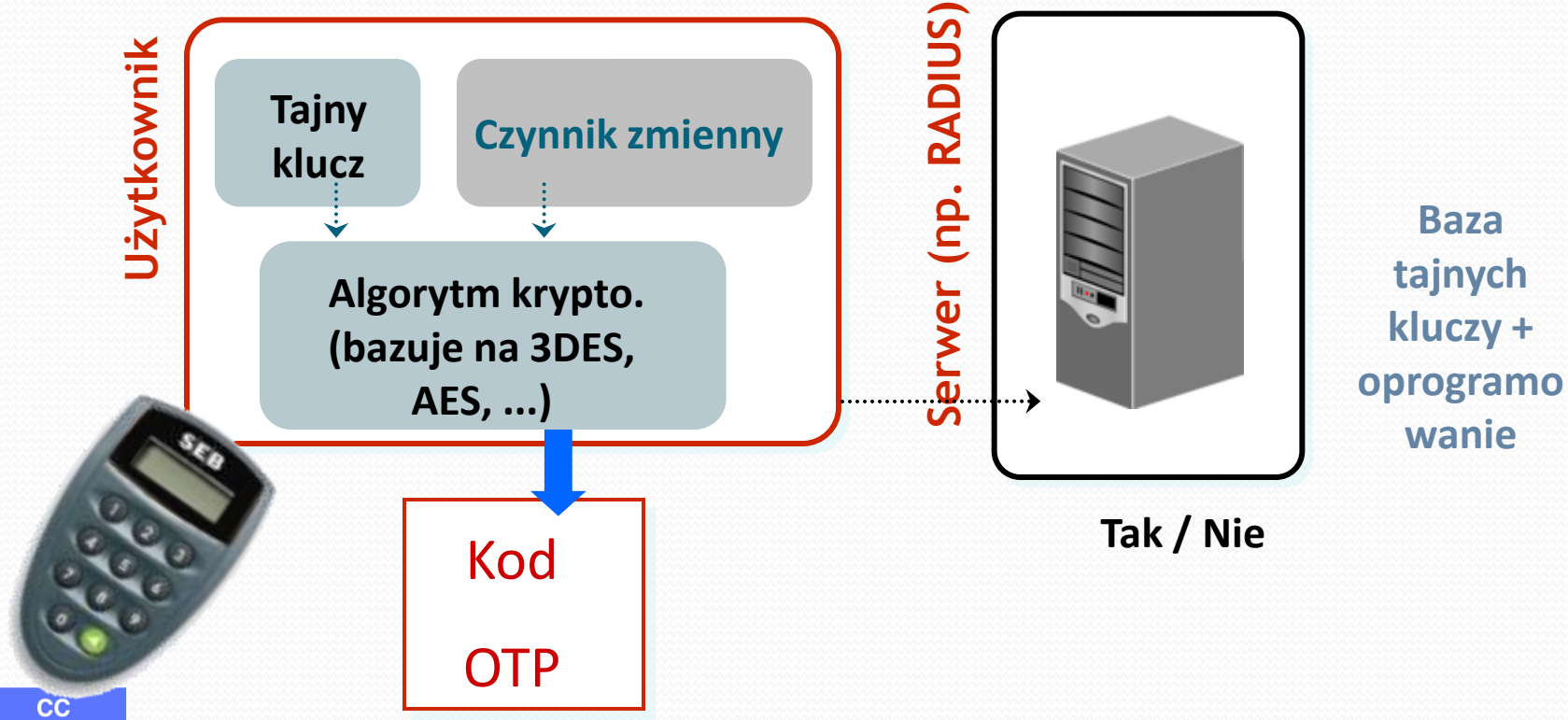
- Dostawca usług:
  - Aplikacje WWW
  - Aplikacje mobilne
- Enterprise:
  - Zdalny dostęp do zasobów sieciowych:
    - IPsec VPN, SSL VPN
    - inne: np. MS ISA
    - potencjalnie wszystkie serwisy kompatybilne z prot. RADIUS
  - Dostęp do poczty (OWA)
  - Autoryzacja WiFi
  - Dostęp do stacji roboczych:
    - bezpośredni i terminalowy (Citrix, itp.)

OTP - podstawy



OTP –podstawy c.d.

Proces generowania hasła OTP i jego weryfikacji



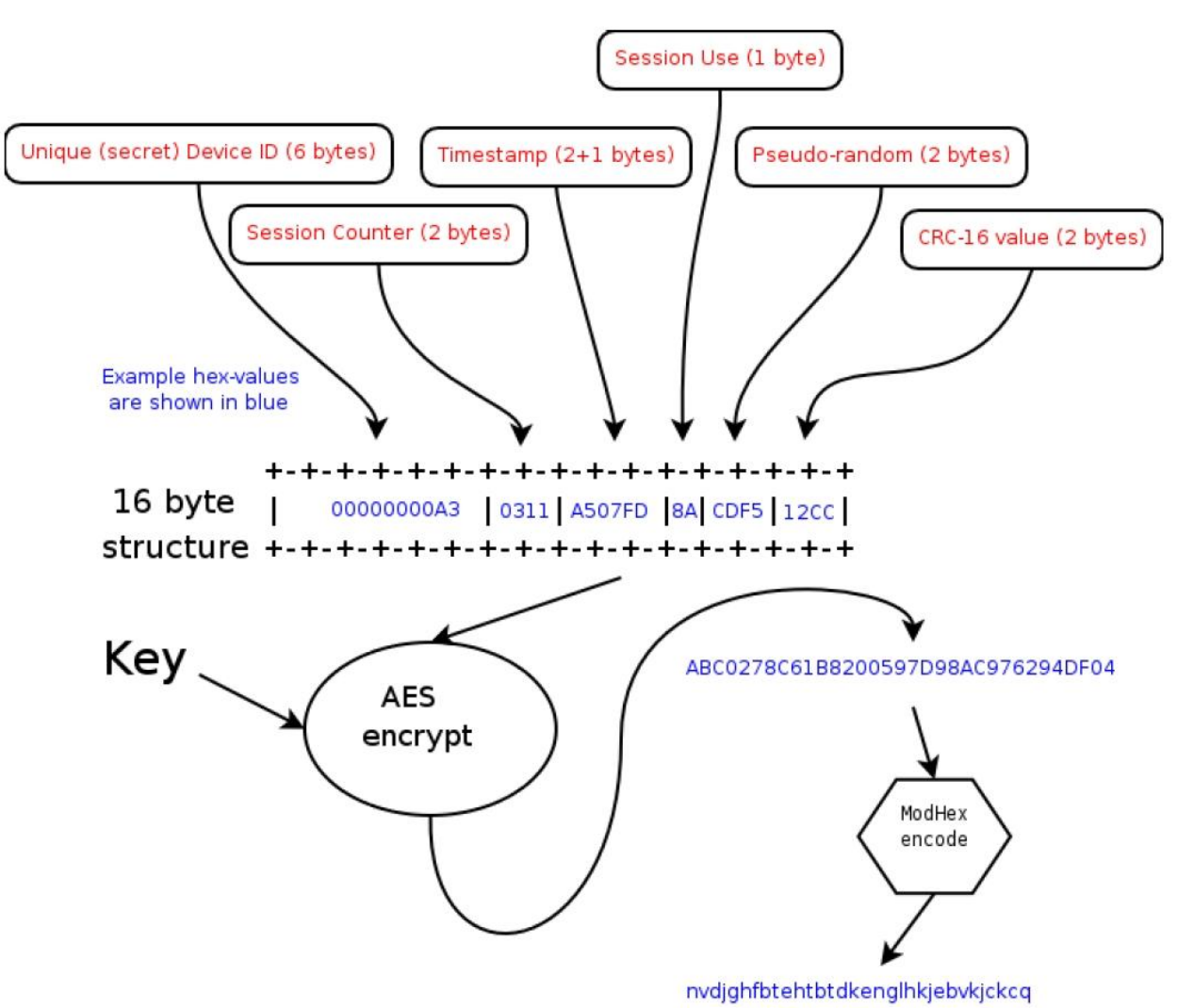
Algorytmy OTP

- Sekwencja haseł musi być (pseudo) losowa
  - Odgadnięcie kolejnego hasła na podstawie obserwacji sekwencji poprzednich nie powinno być możliwe
- „**Event Based**”
  - Bazuje wyłącznie na (pseudo-losowej) sekwencji
  - Hasło generowane jest na podstawie sekretu oraz: poprzedniego hasła lub sewkencyjnego licznika
  - Wrażliwe na atak socjotechniczny (wyłudzenie hasła OTP)
- „**Time based**”
  - Bazuje na wbudowanym zegarze
  - Hasło generowane jest na podstawie sekretu oraz aktualnego czasu
  - Odkrycie sekretu kompromituje token
- **„Time & Event based”**
  - Łączy poprzednie metody, większe bezpieczeństwo

Weryfikacja OTP po stronie serwera

- Serwer musi „przewidzieć” kolejną odpowiedź
- Serwer posiada bazę danych z sekretami tokenów
- Rozsynchronizowanie i synchronizacja
  - Cyfra (bity) kontrolne pozwalają na dostosowanie serwera do dryfu czasowego tokena

Przykładowy algorytm generowania hasła OTP



OATH

- **Initiative for Open Authentication** (**OATH**)
  - Członkowie: ActivIdentity, Entrust, Gemalto, Vasco, Yubico, wielu innych
- Celem organizacji jest opracowywanie, wprowadzanie, certyfikacja zgodności i promocja referencyjnej architektury autoryzacji opartej na otwartych standardach
- Standaryzacja obejmuje:
  - Klienta
  - Serwer walidujący
  - Serwer tworzący konta

OATH HOTP

- HOTP – „HMAC-Based One-Time Password Algorithm”
- RFC 4226 zawiera opis algorytmu:
  - stosuje funkcję skrótu HMAC-SHA-1 przyjmując jako parametry sekretny klucz (K) i licznik (C).
    HS = HMAC-SHA1(K,C) 160 bitów
  - Uzyskany skrót jest redukowany do 32 bitów
    Sbits = DT(HS) 32 bity
  - Uzyskany wynik jest zamieniany na postać liczbową
    D = StToNum(Sbits) mod 10^Digit <Digit> cyfr 6,7,8
- Specyfikacja obejmuje też
  - Wytyczne dot. generowania sekretów
  - liczbę nieudanych prób, dopuszczalny margines przyjętych próbek

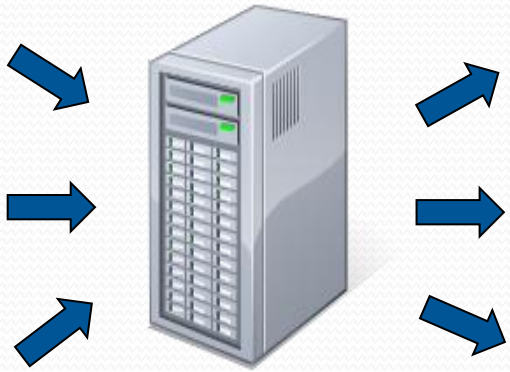
Co nowego w OTP?
TRENDY

Integracja metod po stronie serwera

Sprzęt

Oprogramowanie

EMV-CAP



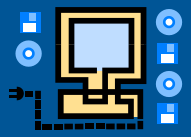
- Bankowość Internetowa
- Bankowość mobilna
- Zdalny dostęp
- IVR
- ATM

CC Otwarte Systemy Komputerowe Sp. z o.o.

Integracja metod po stronie serwera

- Producenci oferują jedno zintegrowane i uniwersalne rozwiązanie serwerowe
- Jeden serwer obsługuje:
  - wiele metod autoryzacji klienckich
  - różne aplikacje wymagające autoryzacji
- Autoryzacja kliencka:
  - Tokeny OTP, karty haseł, SMS/phone-token, EMV-CAP
- Aplikacje serwerowe
  - RADIUS
  - bramka HTTP dla autoryzacji SMS
  - integracja z LDAP i/lub SQL

Realizacja uwierzytelnienia



Zintegrowane rozwiązanie serwerowe

Biblioteka lub middleware

Autonomiczne rozwiązanie serwerowe

Serwer (RADIUS)

SaaS

Rozwiązanie „w chmurze” (SAML)

HSM

Aplikacja na platformę HSM

CC Otwarte Systemy Komputerowe Sp. z o.o.

Zarządzanie kluczami

- Klucz generowany przez producenta (inicjalizacja fabryczna)
  - wygodne dla klienta
  - niższe koszty
- Klucz generowany przez użytkownika
  - wyższe koszty zarządzania
  - rozwiązanie potencjalnie bezpieczniejsze - patrz ostatnie włamanie do serwerów firmy RSA
- W ostatnich latach dostępność programowalnych rozwiązań tokenów OTP stała się ograniczona! (co może ulegnie zmianie)
  - Rozwiązania sprzętowe: interfejs optyczny, indukcyjny lub kontaktowy

Zarządzanie kluczami

- Kroki dystrybucji sekretów (i związane z nimi zagrożenia):
  1. Proces produkcji i fabrycznej inicjalizacji tokenu
  2. Transport sekretów do klienta (dystrybutor, reseller)
  3. Transport i składowanie sekretów w organizacji przed wprowadzeniem do serwera
  4. Wprowadzenie i przechowanie sekretów na serwerze autoryzacyjnym
  5. Przechowanie sekretów (backup) po stronie organizacji
  6. Przechowanie sekretów (backup) po stronie producenta

Obsługa aplikacji w tokenach OTP

- „Aplikacja” – wybrany typ oraz zestaw parametrów dla algorytmu krypto:
  - typ algorytmu: OTP, Challenge/Response, „podpis”
  - podpis: generowany kod zależny jest od wprowadzonych przez użytkownika danych, np. identyfikatora kwoty transakcji
  - po wprowadzeniu PIN użytkownik wybiera aplikację

Push 1 time

Push 2 times

Push 3 times

CC Otwarte Systemy Komputerowe Sp. z o.o.

OTP dla EMV-CAP

DP 805

DP 810

DP 830

DP 831

DP 835

DP836

DP 840 CV

DP 855

DP 865

DP 920

CC Otwarte Systemy Komputerowe Sp. z o.o.

OTP dla EMV-CAP

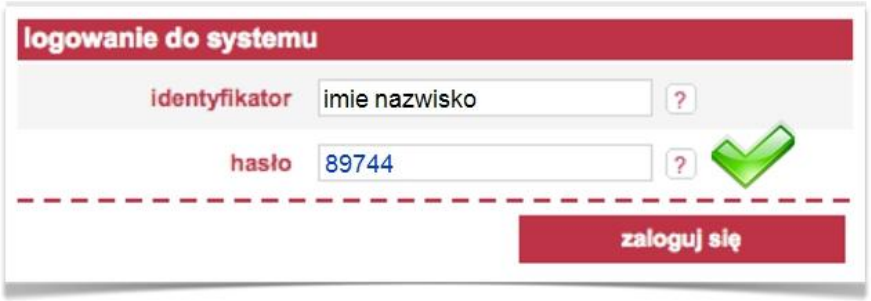
- **Modele autonomiczne i podłączane do komputera**
- Modele autonomiczne (DP 8xx)
  - wykorzystują wyłącznie symetryczny sekret zapisany w karcie
  - typowo używane do płatności przez internet lub mobilnych
- Modele podłączane do komputera (DP 85x, 86x, 9xx)
  - łącze USB
  - dostep do sekretów symetrycznych i asymetrycznych
  - większość może też pracować w trybie autonomicznym
  - typowe zastosowanie: transakcje o dużej wartości oraz „Enterprise”

EMV-CAP WYSIWYS

- Autonomiczny czytnik EMV-CAP
- EMV CAP: Mode 1, Mode 2 (z TDS) , Mode 3
- E-podpis WYSIWYS: What you see is what you sign
- Optyczny interfejs (czytnik ekranowy)
- Wysoka odporność na błędy, przekłamania itp. przy odczycie optycznym

CC Otwarte Systemy Komputerowe Sp. z o.o.

Mobilne tokeny softwarowe



CC Otwarte Systemy Komputerowe Sp. z o.o.

Mobilne tokeny softwarowe

- Token jako aplikacja przeznaczona na daną platformę mobilną
- Dystrybucja:
  - SMS z URL-em (WWW), WAP-push, USB, Bluetooth
- Zgodność:
  - Mogą wystąpić problemy na b. starych telefonach
  - W praktyce token jest aplikacją na tyle prostą, że nie ma problemów z przenośnością)
  - Backend
    - Taki sam (ten sam) jak dla tokenów sprzętowych, programowych i autoryzacji SMS
- Producenci:
  - Vasco
  - Wheel

Token SIM Toolkit

SIM Toolkitmenu

- Sprzętowa „nakładka” na kartę SIM w postaci folii z ultra-cienkim chipem
- Dodaje aplikację SIM-toolkit – niezależne od platformy mobilnej

Tokeny HID

(human interface device)

- Token podłączany do USB działa jak klawiatura – nie wymaga sterowników
- Generuje hasło OTP po naciśnięciu sensora
  - Efekt taki sam jak po wpisaniu z klawiatury
  - Konwersja hasła z postaci binarnej na tekstową pomija problematyczne znaki (np. Z <-> Y).
- Ultra-cienkie i ultra-lekkie rozwiązanie: 18x45x3 mm; 2.5 g
- Możliwość zaprogramowania 2 haseł (krótkie i długie naciśnięcie)
- Nie posiada wewnętrznego źródła zasilania
- Programowane przez użytkownika
- Dostępny wariant z RFID (MIFARE 2k)

Tokeny HID

- Kryptografia bazuje na AES-128
  - Hasło generowane z: licznika, unikalnego identyfikatora tokenu, licznika czasu (ulotnego), sekwencji pseudo-losowej oraz CRC - szyfrowane tajnym kluczem AES
  - Dostępna też wersja OATH
- Programowane fabrycznie lub przez użytkownika
- Obsługa:
  - Biblioteki
  - Cloud
  - Serwer
  - Inne oprogramowanie serwerowe w modelu OpenSource

Partnerzy

VASCO
SECURITY BEYOND E-MAGINATION

axigen
MESSAGING

Ruckus
WIRELESS

CLEAR
SWIFT

nCIPHER

TREND
MICRO

iMPERVA

paloalto
NETWORKS

Tufin
Technologies

Cisco Systems

SOPHOS

Actividentity

WHEEL
SYSTEMS

JUNIPER
NETWORKS

Aladdin
SECURING THE GLOBAL VILLAGE

AVIRA

ARUBA
networks

SOURCEfire

WEBSENSE.