



(c) CC Otwarte Systemy Komputerowe, 2009-2011

## Rozwiązania w zakresie autoryzacji sprzętowej



### Autoryzacja sprzętowa

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

- **autoryzacja** użytkowników w zakresie:
  - dostępu do lokalnego system operacyjnego (stanowiska pracy - stacji roboczej)
  - dostępu do zdalnych zasobów (np. domeny systemu Windows 2000/2003)
  - dostępu tzw. pre-boot (autoryzacja w celu uruchomienia komputera)
  - dostępu do zasobów sieciowych poprzez VPN (oraz SSL VPN)
- **zabezpieczenia zasobów dyskowych** notebooków, stacji roboczych i serwerów poprzez szyfrowanie
- **zabezpieczenie dokumentów** elektronicznych i poczty elektronicznej poprzez podpisy elektroniczne i szyfrowanie

Należy zaznaczyć, że oprogramowanie współpracujące ze sprzętem autoryzacyjnym może realizować też wiele innych funkcji, w tym np.:

- przechowywanie informacji o kontaktach i hasłach odwiedzanych serwisów web-owych
- kompleksowa funkcjonalność SSO (autoryzacja do wszystkich programowych i serwerowych zasobów firmy)
- dodatkowa ochrona – np. blokowanie komputera w momencie wyjęcia karty, itp.

### Dostępne rozwiązania

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

- karty inteligentne (tzw.: SmartCards, SC)
- tokeny USB
- tokeny typu "kalkulator" (z wyświetlaczem i klawiaturką numeryczną) i "breloczek" (z wyświetlaczem)
- systemy biometryczne (nie omawiane w niniejszym dokumencie)



### SmartCards



Rozwiązanie wykorzystuje kartę chipową, czytnik (z interfejsem USB, RS-232 lub innym) oraz oprogramowanie. Karta SC jest de facto autonomicznym komputerkiem realizującym funkcje: bezpiecznego przechowania danych (określone dane nigdy nie opuszczają karty), funkcje kryptograficzne, a także w niektórych przypadkach oferujące możliwość uruchamiania programów (np. appletów Java – tzw. JavaCard)

### Tokeny USB



Rozwiązanie to funkcjonalnie jest równoważne technologii SmartCard. Jedyna istotna różnica tkwi w sprzęcie: karta i czytnik zintegrowane zostały w jednym tokenie USB (przypominającym popularny pendrive).

### Tokeny z wyświetlaczem



Systemy te generują hasła jednorazowe bazujące na aktualnym czasie (tzw. OTP – One Time Password) lub działają na zasadzie Challenge-Response (hasło-odzew) – tylko tokeny typu kalkulator. Zakres ich zastosowania jest węższy niż kart oraz tokenów USB. Wielką zaletą 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 działania 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” 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.





Rozwiązanie	Realizowane funkcje	Zalety i wady
SmartCard	<ul style="list-style-type: none"><li>• Autoryzacja do systemów operacyjnych i zasobów sieciowych</li><li>• Autoryzacja w VPN</li><li>• Autoryzacja do aplikacji WWW</li><li>• Autoryzacja do arbitralnych aplikacji</li><li>• Podpisywanie i szyfrowanie dokumentów</li></ul>	<ul style="list-style-type: none"><li>• Możliwość integracji z innymi systemami zabezpieczenia, np. RF, RFID</li><li>• Możliwość umieszczenia na karcie: zdjęcia, kodu paskowego, innych dodatkowych informacji</li></ul> <p><b>Wady:</b></p> <ul style="list-style-type: none"><li>• większy koszt w stosunku do pozostałych rozwiązań</li><li>• skomplikowanie techniczne</li><li>• konieczne łącze USB (RS-232, PC Card) i instalacja oprogramowania</li><li>• niekompatybilności pomiędzy czytnikami, kartami i oprogramowaniem różnych producentów</li></ul>
Token USB	<ul style="list-style-type: none"><li>• Tak samo jak dla kart</li></ul>	<ul style="list-style-type: none"><li>• Prosta koncepcja użycia – token umieszczany w łączu USB</li><li>• niski koszt</li></ul> <p><b>Wady:</b></p> <ul style="list-style-type: none"><li>• nie zawsze dostępna możliwość łączenia z inną technologią zabezpieczeń (poza RFID)</li><li>• konieczne łącze USB i instalacja oprogramowania</li></ul>
Tokeny z wyświetlaczem ("breloczek" lub "kalkulator")	<ul style="list-style-type: none"><li>• Autoryzacja do systemach i zasobów sieciowych</li><li>• Autoryzacja w VPN</li><li>• Autoryzacja do aplikacji WWW</li><li>• Autoryzacja do arbitralnych aplikacji</li></ul>	<ul style="list-style-type: none"><li>• Nie wymaga żadnych zasobów sprzętowych lub programowych po stronie klienta - rozwiązania czysto serwerowe</li><li>• niezawodność i prostota</li><li>• niski koszt</li></ul> <p><b>Wady:</b></p> <ul style="list-style-type: none"><li>• ograniczone możliwości (brak kryptografii asymetrycznej, brak "prawdziwego" podpisu)</li><li>• brak możliwości łączenia z inną technologią zabezpieczeń</li></ul>

### Ochrona zasobów (DLP – Data Leak Prevention)

Tokeny i karty SC używane są często w zakresie wykraczającym poza podstawową autoryzację użytkowników. Coraz popularniejsze stają się rozwiązania DLP (Data Leak Prevention), czyli zapobieganie wyciekowi danych. DLP to oprogramowanie, którego celem jest „uszczelnienie” całej infrastruktury informatycznej w celu zapobieżenia celowego lub nieumyślnego wycieku poza firmę cennych i poufnych danych. Najważniejsze funkcje oprogramowania DLP są następujące:

- Szyfrowanie danych – całych dysków lub wybranych katalogów, wybranych plików, itp.



- Ochrona pre-boot – bez podania hasła / użycia tokenu nie jest możliwe uruchomienie komputera (rozwiązanie stosowane najczęściej w przypadku notebooków)
- Kontrola dostępu do nośników zewnętrznych - np. kontrola dostępu do nagrywarek CD/DVD, dysków typu pen-drive, itp.
- Możliwość odzyskania danych w przypadku utraty hasła lub tokena, niedostępności właściciela danych, itp.
- Zabezpieczenie przed odinstalowaniem lub zmianą konfiguracji przez użytkownika końcowego

Oferowane przez nas rozwiązania DLP pochodzą od następujących producentów: McAfee (SafeBoot), checkPoint (PointSec), TrendMicro, Symantec.

### Od czego zacząć?

Przed rozpoczęciem wyboru producenta systemu autoryzacji powinniśmy przygotować następującą (lub podobną) tabelkę:

Całkowita liczba użytkowników	
Czy chcemy autoryzować użytkowników w dostępie do komputera stacjonarnego lub notebooka?	[TAK] [NIE]
Czy chcemy autoryzować w dostępie do komputera stacjonarnego lub notebooka, który nigdy nie posiada dostępu do sieci?	[TAK] [NIE]
Czy chcemy autoryzować w dostępie do zasobów sieciowych (domena Windows, inne)?	[TAK] [NIE]
Czy chcemy autoryzować w dostępie zdalnym poprzez VPN?	[TAK] [NIE]
Czy chcemy stosować szyfrowanie dysków?	[TAK] [NIE]
Czy chcemy wdrożyć autoryzację do różnych aplikacji (w tym nie webowych)?	[TAK] [NIE]
Czy chcemy stosować dodatkowe autoryzacje? Jakież?	[TAK] [NIE]

### Przegląd rozwiązań:

W zakresie systemów autoryzacji sprzętowej oferujemy rozwiązania następujących producentów:

- Aladdin
- ActivIdentity (d. ActivCard)
- DataKey
- Vasco
- SafeWorld (obecnie połączone z Aladdin)
- YubiCo
- CheckPoint (przejęte rozwiązania PointSec)
- WinMagic SecureDoc
- TrendMicro



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:

<b>Producent</b>	<b>Cechy</b>
Aladdin / SafeNet	Tokeny USB, wszechstronna autoryzacja do zasobów lokalnych i sieciowych, w tym VPN, serwery WWW i inne. Dostępne są tokeny zintegrowane z dyskiem flash (512, 1024 MB) oraz zaopatrzone w opcje bezprzewodowe: HID, RFID i inne. Oprogramowanie do integracji z serwerami sieciowymi (ActiveDirectory i inne) oraz do zarządzania tokenami.
ActivIdentity	Karty SC i tokeny USB, wszechstronna 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
YubiCo	Tokeny HID z interfejsem USB – symulujące wpisanie hasła jednorazowego z klawiatury
DataKey	Karty SC i tokeny USB
<b>Tylko oprogramowanie</b>	
SecureDoc	Oprogramowanie do zastosowań indywidualnych oraz przedsiębiorstw – zabezpieczenia pre-boot w oparciu o token oraz szyfrowanie dysków zintegrowan z tokenami i kartami SC
CheckPoint (PointSec)	Oprogramowanie dla przedsiębiorstw – zabezpieczenia pre-boot w oparciu o token oraz szyfrowanie dysków zintegrowan z tokenami i kartami SC. Szyfrowanie całych dysków i nośników zewnętrznych. Centralna administracja.
TrendMicro	Nowatorskie rozwiązanie DLP bazujące na sygnaturach plików. Zapobiega wyciekowi danych nawet w przypadku próby skopiowania ich w części.

### **Jaki system wybrać?**

Wybór optymalnego systemu autoryzacji jest zależny od wielu czynników: wymaganych funkcji, liczby użytkowników, chronionych zasobów (np. - czy wymagane jest szyfrowanie danych na notebookach?), aktualnie posiadanych zasobów sprzętowych i programowych, wreszcie kosztów jakie gotowi jesteśmy ponieść. Nie jest możliwe przedstawienie jednoznacznych reguł pozwalających wybrać system firewall na podstawie powyższych czynników. Można jednak przedstawić kilka ścieżek postępowania.

W zależności od wielkości przedsiębiorstwa i typowych dla niej oczekiwań:



<b>Wielkość i charakter przedsiębiorstwa</b>	<b>Typowe cechy i wymagania</b>
Firma b. mała, zatrudnienie do c.a. 50 osób	<ul style="list-style-type: none"><li>Autoryzacja lokalna w oparciu o tokeny, szyfrowanie danych: Aladdin, ActivIdentity, DataKey, SecureDoc, YubiCo</li></ul>
Firma średnia zatrudnienie c.a. 50 - 250 osób,	<ul style="list-style-type: none"><li>Autoryzacja lokalna i do zasobów sieciowych w oparciu o tokeny, autentykacja dla dostępu zdalnego VPN: Aladdin, ActivIdentity, CheckPoint</li></ul>
Firma duża zatrudnienie powyżej 250 osób, konieczność integracji z fizycznymi systemami kontroli dostępu	<ul style="list-style-type: none"><li>Autoryzacja lokalna i do zasobów sieciowych, autentykacja do VPN, karty identyfikacyjne RFID lub inne hybrydowe: Aladdin, ActivIdentity</li></ul>
Firma świadcząca usługi klientom zewnętrznym wymagające podwyższonego bezpieczeństwa przy autoryzacji	<ul style="list-style-type: none"><li>Vasco, ActivIdentity</li></ul>

### Co oferujemy?

Na wdrożenie systemu autentykacji 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:

- Auchan Polska sp. z o.o.,
- CA IB S.A.
- Urząd M.st. Warszawa – Ursynów,
- Coffee Heaven Intl. Sp. z o.o.
- Sodexo Pass Polska Sp z o.o.
- FM Polska Sp z o.o. (FM Logistic)
- Metropolitan Life Ubezpieczenia na Życie S.A.,
- Krajowe Biuro Wyborcze
- Nestle Polska S.A.
- Sodexo Pass Polska Sp. z o.o.
- Wojskowa Akademia Techniczna,
- 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](mailto:tech@cc.com.pl)

Dział Handlowy: [sales@cc.com.pl](mailto:sales@cc.com.pl)