# 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 operacynego (stanowiska pracy - stacji roboczej)
  - dostępu do zdalnych zasobów (np. domeny systemu Windows 2000/2003)
  - dostepu 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 porzez 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 kontach 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 wystepują 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),



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/

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. Z reguły tokeny te nie posiadają klawiatury.

| Rozwiązanie | Realizowane funkcje | Zalety i wady |
|---|---|---|
| SmartCard | • Autoryzacja do systemów operacyjnych i zasobów sieciowych<br>• Autoryzacja w VPN<br>• Autoryzacja do aplikacji WWW<br>• Autoryzacja do arbitralnych aplikacji<br>• Podpisywanie i szyfrowanie dokumentów | • Możliwość integracji z innymi systemami zabezpieczenia, np. RF, RFID<br>• Możliwość umieszczenia na karcie: zdjęcia, kodu paskowego, innych dodatkowych informacji<br>**Wady:**<br>• większy koszt w stosunku do pozostałych rozwiązań<br>• skomplikowanie techniczne<br>• konieczne łącze USB (RS-232, PC Card) i instalacja oprogramowania<br>• niekompatybilności pomiędzy czytnikami, kartami i oprogramowaniem różnych 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/

| Rozwiązanie | Realizowane funkcje | Zalety i wady |
|---|---|---|
| Token USB | • Tak samo jak dla kart | • Prosta koncepcja użycia – token umieszczany w łączu USB<br>• niski koszt<br>**Wady:**<br>• nie zawsze dostepna możliwości łączenia z inną technologią zabezpieczeń (poza RFID)<br>• konieczne łącze USB i instalacja oprogramowania |
| Tokeny z wyświetlaczem ("breloczek" lub "kalkulator" | • Autoryzacja do systemach i zasobów sieciowych<br>• Autoryzacja w VPN<br>• Autoryzacja do aplikacji WWW<br>• Autoryzacja do arbitralnych aplikacji | • Nie wymaga żadnych zasobów sprzętowych lub programowych po stronie klienta - rozwiązania czysto serwerowe<br>• niezawodność i prostota<br>• niski koszt<br>**Wady:**<br>• ograniczone możliwości (brak kryptografii asymetrycznej, brak "prawdziwego" podpisu)<br>• brak możliwości łączenia z inną technologią zabezpieczeń |

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

Tokeny i karty SC używane są często w zakresie wykraczającym poza podstawową autoryzację użytkowników. Coraz popularniejsze stają się rozwiazania 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 zewnętrznycyh - 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.


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/

**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 autoryzowac 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? Jakie? | [TAK] [NIE] |

**Przegląd rozwiązań:**

W zakresie systemów autoryzacji sprzętowej oferujemy rozwiązania następujących producentów:

- Aladdin
- ActivIdentity (d. ActivCard)
- DataKey
- Vasco
- McAfee (przejęte rozw. SafeBoot)
- 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:


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/

| Producent | Cechy |
|---|---|
| Aladdin | Tokeny USB, wszechstrona autoryzacja do zasobow lokalnych i sieciowych, w tym VPN, serwery WWW i inne. Dostępne są tokeny zintegrowane z dyskiem flash (512, 1024 MB) oraz zaopatrzone w opjce bezprzewodowe: HID, RFID i inne. Oprogramowanie do integracji z serwerami sieciowymi (ActivDirectory i inne) oraz do zarządzania tokenami. |
| ActivIdentity (ActivCard) | 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 |
| DataKey | Karty SC i tokeny USB |
| **Tylko oprogramowanie** | |
| McAfee (SafeBoot) | Oprogramowanie dla przedsiebiorstw – zabezpieczenia pre-boot w oparciu o token oraz szyfrowanie dysków zintegrowan z tokenami i kartami SC. Szyfrowanie całych dysków i wybranych plików – lokalne i na serwerach. Centralna administracja. |
| SecureDoc | Oprogramowanie do zastosowań indywidualnych oraz przedsiebiorstw – zabezpieczenia pre-boot w oparciu o token oraz szyfrowanie dysków zintegrowan z tokenami i kartami SC |
| CheckPoint (PointSec) | Oprogramowanie dla przedsiebiorstw – 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:


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/

| Wielkość i charakter przedsiebiorstwa | Typowe cechy i wymagania |
|---|---|
| Firma b. mała, zatrudnienie do c.a. 50 osób | • Autentykacja lokalna w oparciu o tokeny, szyfrowanie danych: Aladdin, ActivIdentity, DataKey, SecureDoc |
| Firma średnia zatrudnienie c.a. 50 - 250 osób, | • Autentykacja lokalna i do zasobów sieciowych w oparciu o tokeny, autentykacja dla dostępu zdalnego VPN: Aladdin, ActivIdentity, CheckPoint, SafeBoot |
| Firma duża zatrudnienie powyżej 250 osób, konieczność integracji z fizycznymi sytemami kontroli dostepu | • Autentykacja lokalna i do zasobów sieciowych , autentykacja do VPN, karty identyfikacyjne RFID lub inne hybrydowe: SafeBoot, ActivIdentity |
| Firma świadcząca usługi klientom zewnętrznym wymagajace podwyższonego bezpieczeństwa przy autoryzacji | • Vasco, ActivIdentity |

**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,
- Monitel S.A.
- Sodexho Pass Polska Sp z o.o.
- FM Polska Sp z o.o. (FM Logistic)
- Metropolitan Life Ubezpieczenia na Życie S.A.,
- MMI Sp. z o.o.
- Nestle Polska S.A.
- Media Planning 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.,
- SNN Poligrafia Sp. z o.o.,
- WinterThur TU Polska S.A.
- Uniwersytet Warszawski, Wydział Chemii
- Zelmer

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

**Osoby kontaktowe:**
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/