Bezpieczeństwo danych w laptopie

₥@ʁ€₭ ‽ud3£k0

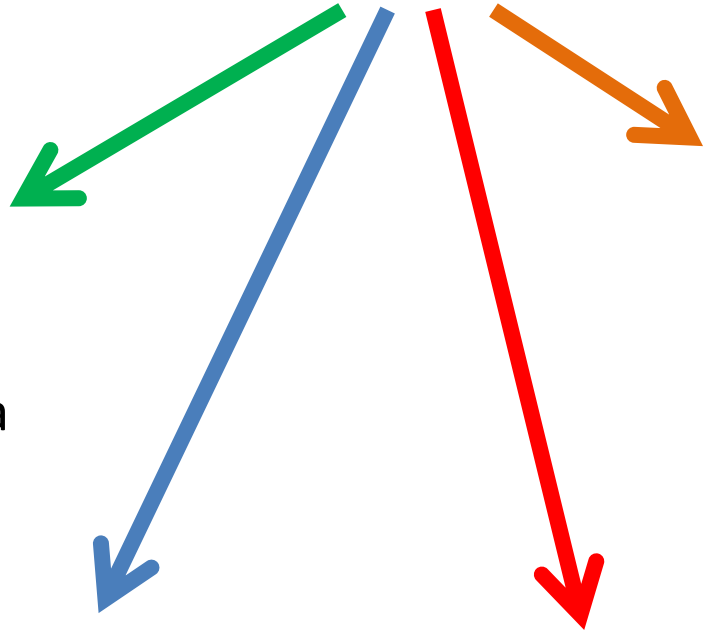
Urządzenia Techniki Komputerowej

Ochrona laptopa

Sposoby zabezpieczania laptopa

- Hasła systemowe i na BIOS
- Szyfrowanie danych na dysku
- TPM (Trusted Platform Module)
- Karta kryptograficzna (identyfikująco – szyfrująca)
- Czytnik linii papilarnych
- Linka mocująca
- Naklejka zabezpieczająca
- Stacja blokująca
- Blokada otwarcia
- Czujnik wynoszenia sprzętu
- Kopia bezpieczeństwa danych
- Torba ochronna
- Aplikacje śledzące
- Redukcja promieniowania elektromagnetycznego
- Ubezpieczenia i zachowanie dowodu zakupu

Sposoby zabezpieczania laptopa



- **Fizyczne**
- Linka mocująca
- Naklejka zabezpieczająca
- Stacja blokująca
- Blokada otwarcia
- Torba ochronna

- **Organizacyjne**
- Przestrzeganie odpowiednich zasad bezpieczeństwa
- Ubezpieczenie
- Zachowanie dowodu zakupu

- **Sprzętowe**
- TPM (Trusted Platform Module)
- Karta kryptograficzna (identyfikująco – szyfrująca)
- Czytnik linii papilarnych
- Czujnik wynoszenia sprzętu
- Redukcja promieniowania elektromagnetycznego

- **Programowe**
- Hasła systemowe i na BIOS
- Szyfrowanie danych na dysku
- Kopia bezpieczeństwa danych
- Aplikacje śledzące

HASŁA SYSTEMOWE

Logowanie

- Logowanie to proces uwierzytelniania i autoryzacji użytkownika komputera.
- Polega na podaniu identyfikatora użytkownika i hasła uwierzytelniającego.
  - Celem jest uzyskanie dostępu do komputera (przenośnego), jego programów, danych i zasobów.
- Procesem odwrotnym do logowania jest wylogowanie, czyli rezygnacja z uzyskanego dostępu.

Hasła systemowe

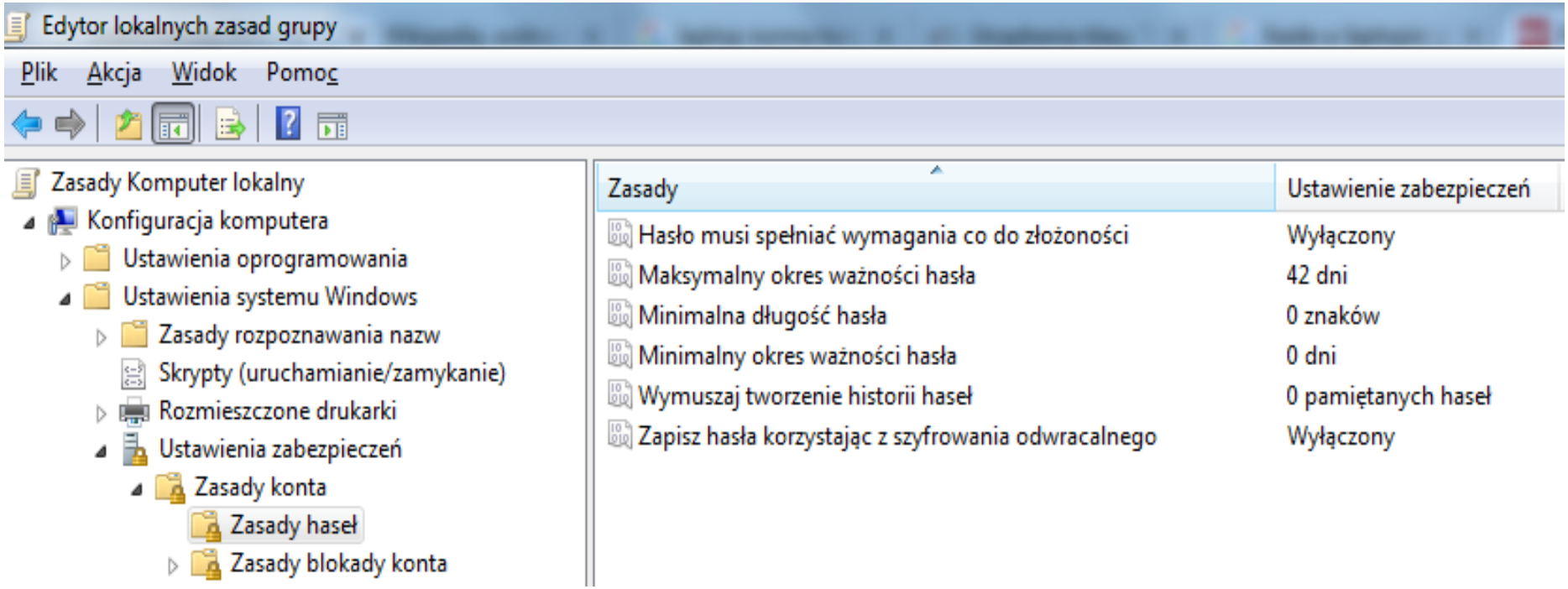
- Laptopy są szczególnie narażone na kradzież danych. Osoba, która wejdzie w jego posiadanie może się zalogować i sprawdzić zgromadzone na dysku dane.
- Hasła powinny być bezpieczne, by jak najdłużej uniemożliwić dostanie się do zawartych w nim danych.
- Hasło powinno być długie, urozmaicone, nietrywialne, niezwiązane z użytkownikiem laptopa.
- Użytkownik nie powinien zapisywać zapisujemy haseł i trzymać je gdzieś w pobliżu laptopa (np. na karteczce przylepionej do ekranu lub napisane flamastrem na obudowie).

- W ważnych instytucjach zmienia się go co 30 dni.
- Nie należy udostępniać hasła innym.
- W przypadku choćby podejrzenia o poznanie hasła przez inną osobę trzeba je zmienić.

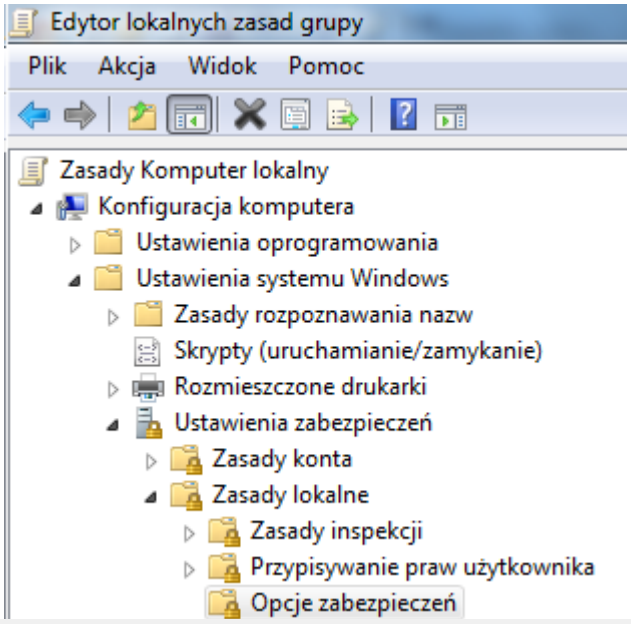
Zasady tworzenia haseł systemowych

- Dostateczna długość hasła,
- Słowo, które nie jest łatwe do zgadnięcia,
- Używanie znaków, które nie są literami i cyframi,
- Używanie dużych i małych liter,
- Hasło powinno być jak najdłuższe (co najmniej 8 znaków).
- Zalecane jest uwzględnianie w haśle:
  - Dużych i małych liter
  - Polskich liter (ą, ę itp.),
  - Cyfr
  - Spacji, znaków podkreślenia, @,!,$,&,%, nawiasów, znaków niewystępujących na klawiaturze (używamy kombinacji ALT + numer>127).

Zasady bezpieczeństwa haseł w laptopach



Zasady bezpieczeństwa logowania w laptopach



Zasady	Ustawienie zabezpieczeń
Kontroler domeny: wymagania podpisywania serwera LDAP	Niezdefiniowane
Kontroler domeny: zezwalaj operatorom serwera na planowanie zadań	Niezdefiniowane
Kryptografia systemu: użyj zgodnych algorytmów FIPS dla celów szyfrowania, tworzenia skrótu i podpisywania	Wyłączony
Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze	Niezdefiniowane
Logowanie interakcyjne: liczba poprzednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)	10 logowania
Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem	5 dni
Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL	Niezdefiniowane
Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika	Wyłączony
Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować	
Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować	
Logowanie interakcyjne: wymagaj karty inteligentnej	Wyłączony
Logowanie interakcyjne: wymagaj uwierzytelnienia kontrolera domeny do odblokowania stacji roboczej	Wyłączony
Logowanie interakcyjne: wyświetlaj informacje o użytkowniku, gdy sesja jest zablokowana	Niezdefiniowane
Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentej	Brak akcji

Nie zapisuj hasła na kartce

SZYFROWANIE DYSKÓW

Szyfrowanie dysków

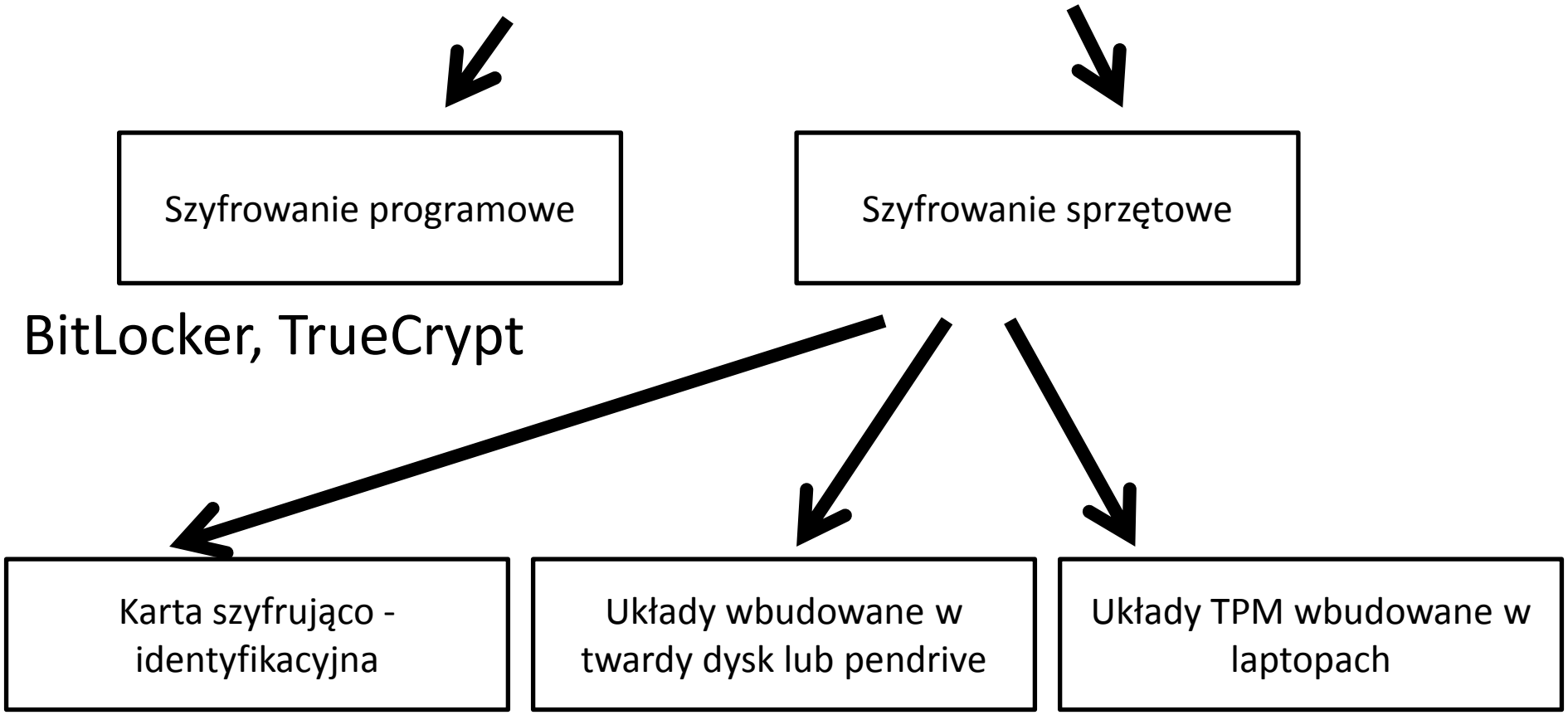
- Szyfrowanie dysku pozwala na ochronę zawartych na nim danych.
  - Zabezpieczone zostają pliki na poszczególnych partycjach, wrażliwa na analizę przestrzeń wymiany (swap) i pliki tymczasowe. Ukrywa strukturę katalogów, nazwy plików, ich rozmiary oraz czasy modyfikacji i dostępu.

- Nawet gdy ktoś ma dostęp do laptopa lub dysku, nie dostanie się do tych danych.
- Dane na dysku zaszyfrowanym można odzyskać bez wiedzy o zawartych na nim danych – nawet serwis nie wie wtedy co było na dysku.
- Dysk zaszyfrowany chodzi nieco wolniej (kilka procent).

Szyfrowanie plików

- Szyfrowanie całego dysku chroni dane na komputerze tylko wtedy, gdy komputer jest fizycznie wyłączony.
- Cała zawartość zaszyfrowanego dysku jest dostępna zaraz po przedstawieniu przez użytkownika właściwego klucza/hasła. Pracując z laptopem istnieje dostęp do wszystkich danych.
- Kiedy napastnik przechwyci włączony laptop, może przejąć klucze kryptograficzne zawarte w pamięci RAM.
- Środkiem zapobiegawczym jest jednoczesne szyfrowanie na poziomie plików pozwalające zabezpieczyć najważniejsze dane.

Rodzaje szyfrowania

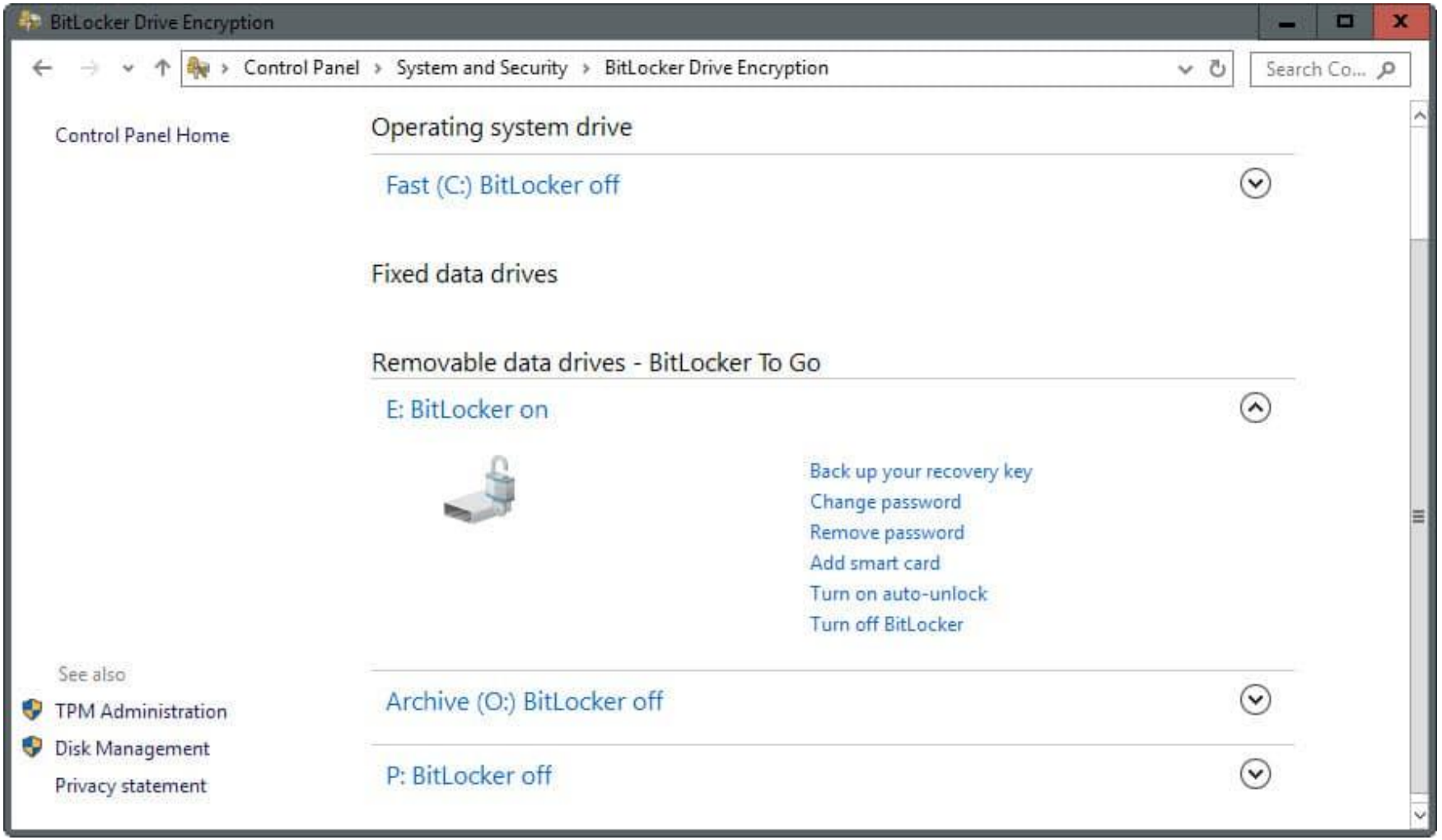


BITLOCKER

Bitlocker

- Oprogramowanie systemów Microsoft Windows, pozwalające na kryptograficzną ochronę danych na dyskach. Może wykorzystywać sprzętowe moduły.
- BitLocker szyfruje przy pomocy algorytmu AES (128 lub 256 bitów) każdy sektor partycji. Szyfrowanie i odszyfrowanie odbywa się w najniższej możliwej warstwie, przez co mechanizm jest praktycznie niewidzialny dla systemu i aplikacji.
- Szyfrowana może być partycja podstawowa lub rozszerzona.
- Jeżeli szyfrowana jest partycja systemowa, konieczne jest istnienie na dysku twardym niezaszyfrowanej partycji startowej o rozmiarze rzędu kilkuset MB. Znajdują się na niej niezaszyfrowane programy pozwalające na odczytanie kluczy szyfrujących i start całego mechanizmu.
  - Jest ona chroniona przez TPM lub klucze z USB.
  - Inne partycje nie mogą być chronione przez TPM, Ale klucze do nich można zapisać w rejestrze i automatycznie go używać przy każdym uruchomieniu systemu.
- Dane umożliwiające dostęp do danych mogą pochodzić z:
  - TPM – tylko dla partycji systemowej
  - pliku (na przykład na nośniku USB)
  - wprowadzonego z klawiatury kodu, składającego się z 48 cyfr
  - rejestru – tylko dla partycji innych niż systemowa i pod warunkiem zaszyfrowania partycji systemowej
- BitLocker nie wymaga obecności modułu TPM. Jeśli go brak, to klucz trzeba wprowadzić w inny sposób. TPM robi to automatycznie w sposób niezauważalny dla użytkownika. Składający się z 48 cyfr kod, wprowadzany podczas startu systemu wprowadza się za pomocą klawiszy numerycznych lub klawiszy funkcyjnych [F1] dla 1, [F2] dla 2 itd., gdzie [F10] oznacza zero.
- Konieczność wprowadzenia kodu pojawić się może w sytuacji, gdy TPM nie może wygenerować klucza automatycznie. Wynikać to może ze zmian w sprzęcie lub oprogramowaniu. Wtedy po użyciu kodu odzyskiwania należy wygenerować klucz dla TPM. Przy ponownym uruchomieniu będzie użyty automatycznie.
  - W systemie Windows 7 wprowadzona została obsługa mechanizmów BitLocker dla nośników wymiennych, w tym pamięci USB Flash, nazywana **BitLocker to Go**.

Bitlocker


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Co...
Control Panel Home
Operating system drive
Fast (C:) BitLocker off
Fixed data drives
Removable data drives - BitLocker To Go
E: BitLocker on
Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker
See also
TPM Administration
Disk Management
Privacy statement
Archive (O:) BitLocker off
P: BitLocker off

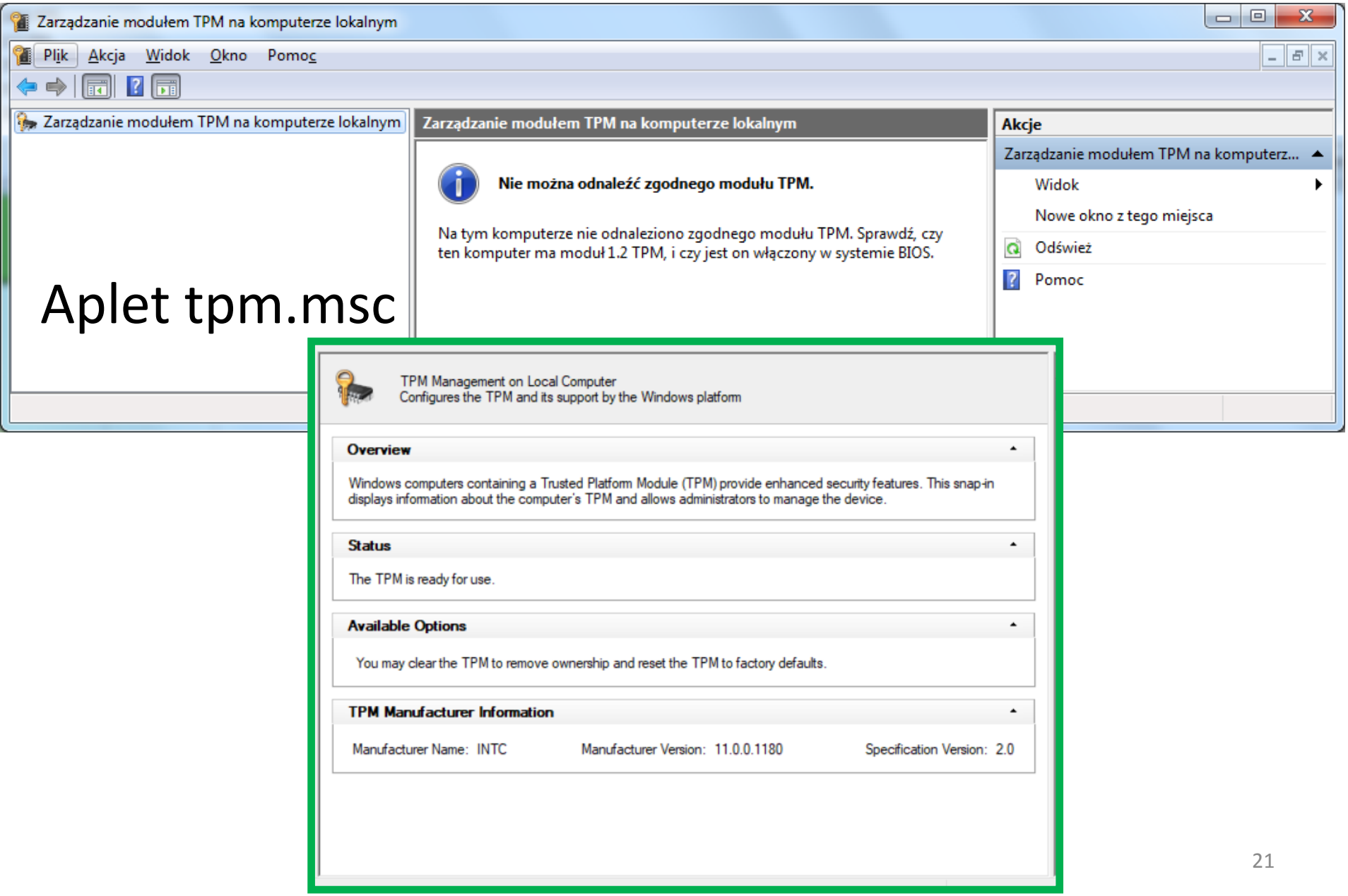
TRUSTED PLATFORM MODULE

Trusted Platform Module (TPM)

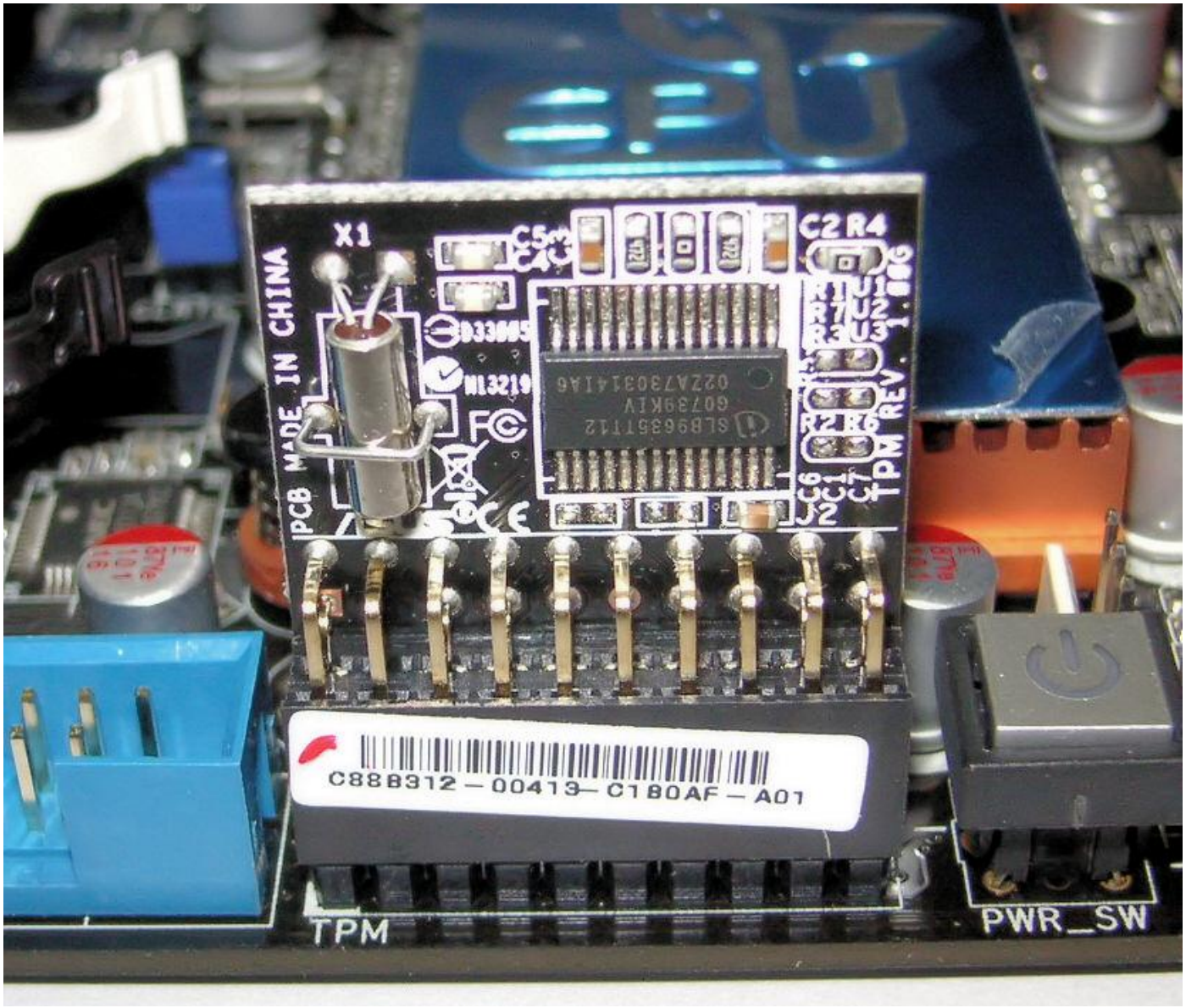
- Układ scalony zawierający pary kluczy prywatnych i publicznych PKI (Public Key Infrastructure) oraz poświadczenia kluczy.

- Układy TPM najczęściej spotyka się w laptopach, co skutecznie chroni dane. W desktopach układy TPM są rzadkie. Spotyka się też rozwiązania serwerowe.
  - TPM wspiera BitLocker stosowany w systemach Windows (od Visty).
- TPM ma wspierać wszelkie operacje kryptograficzne realizowane w systemie komputerowym. TPM może wspierać zarówno instrukcje realizowane w systemie operacyjnym, oprogramowaniu jak i szyfrowania na poziomie sprzętowym.
- Pary kluczy prywatnych i publicznych PKI (Public Key Infrastructure) oraz poświadczenia kluczy nie są one nigdzie wysyłane ani zapisywane na zewnątrz. Praktycznie uniemożliwia to jego zdalne przechwycenie.
- TPM wspiera szyfrowanie danych na dyskach twardych. Komputer z TPM może tworzyć klucze szyfrowania, które można odszyfrować tylko za pomocą tego samego modułu TPM. Powiązanie klucza z konkretnym egzemplarzem laptopa sprawia, że wyjęcie dysku twardego nie pozwoli na odczytanie go w innym komputerze.
  - Problem przy awarii laptopa.

Trusted Platform Module (TPM)



Trusted Platform Module (TPM)



KARTA KRYPTOGRAFICZNA

Karta kryptograficzna

- Karta kryptograficzna – urządzenie, które ma na celu zabezpieczyć fizycznie i logicznie klucze prywatne właściciela.
- Zabezpieczenie fizyczne polega na takiej konstrukcji urządzenia, by nie dało się zajrzeć do jego wnętrza, bez jednoczesnego zniszczenia wszystkich poufnych danych ze środka.
- Na zabezpieczenie logiczne składają się następujące czynniki:
  - Klucze kryptograficzne generowane są wewnątrz karty.
  - Nie istnieje możliwość eksportu kluczy prywatnych na zewnątrz karty.
  - Operacja szyfrowania danych odbywa się wewnątrz karty.
  - Operacja podpisywania danych odbywa się wewnątrz karty.
  - Użycie karty zabezpieczone jest systemem haseł.
- Poziom szyfrowania kart kryptograficznych jest względnie niski
  - Standardowo RSA-1024, co jest najniższą obecnie długością klucza.
- Sprzętowa ochrona klucza powoduje, że cały system jest bardzo bezpieczny.
- Karta kryptograficzna może występować w różnych postaciach: Smart Card, karty Express Card, moduł USB, karty PCI lub PCI Express.

Karty kryptograficzne

CZYTNIK LINII PAPILARNYCH

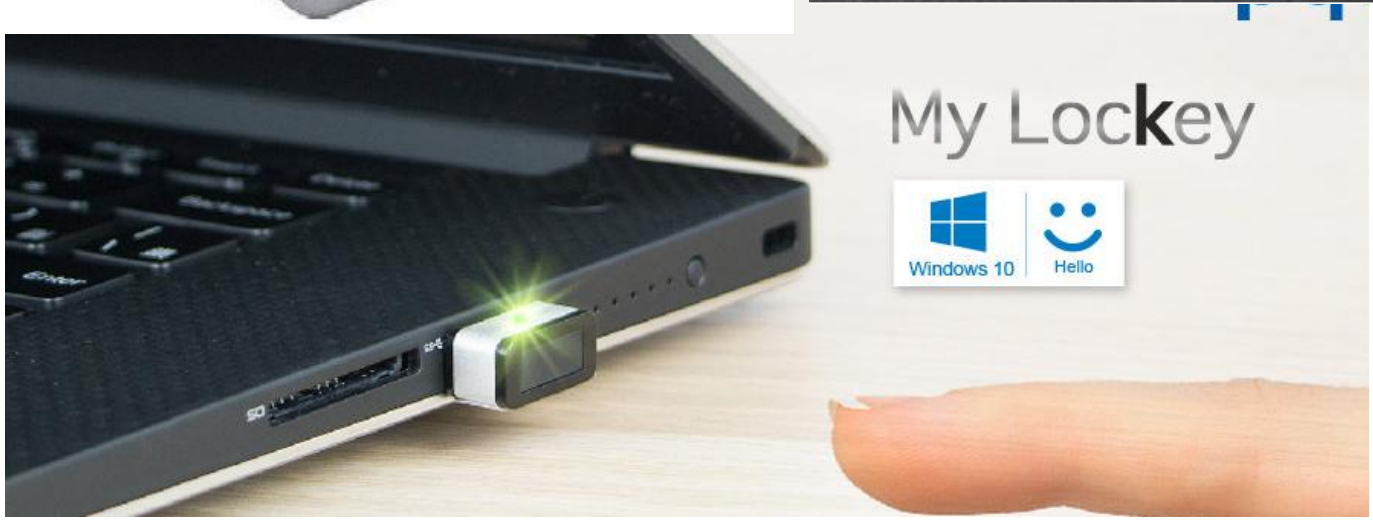
Czytnik linii papilarnych

- Czytnik linii papilarnych to urządzenie rozpoznające ludzi po niepowtarzalnym wzorze linii skóry na palcach dłoni.
- Jest to świetny sposób na jednoznaczną identyfikację danej osoby.
  - Należy położyć palec na czujniku.
  - Czytnik analizuje rozkład linii i porównuje go ze wzorcem.
  - Czytnik nie analizuje całego układu linii papilarnych, a tylko kilka jego charakterystycznych elementów zwanych *minucjami*. (zazwyczaj rozgałęzienia linii papilarnych lub ich zakończenia). Skaner "fotografuje" ich względny układ i odległości między nimi.
- To zabezpieczenie uniemożliwia uruchomienie laptopa przez niepowołaną do tego osobę.
  - To zabezpiecza nawet w wypadku kradzieży sprzętu
- System kojarzy dany wzór linii papilarnych z daną osobą. Utworzy ***profil skojarzony z liniami papilarnymi***.
- W wypadku wielu użytkowników należy utworzyć oddzielne profile w systemie.

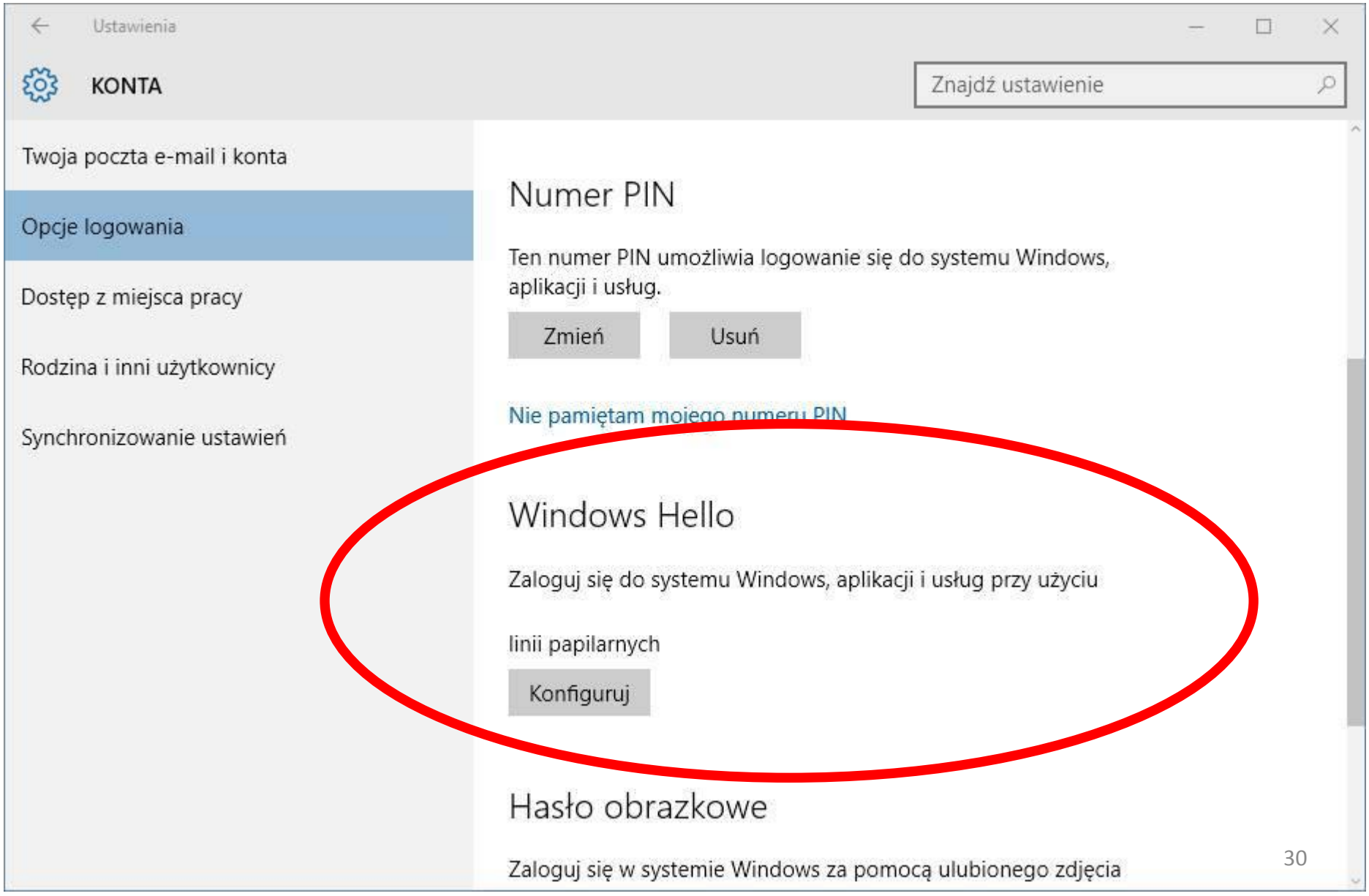
Czytnik linii papilarnych

- Bezpieczne logowanie
  - Może to być dodatkowe zabezpieczenie lub odcisk palca może zastąpić logowanie do komputera.
- *Single Sign On* – jednorazowe logowanie
  - Może zastąpić logowanie do różnych programów, poczty elektronicznej, serwisów społecznościowych lub stron internetowych.
  - Należy zapisać odpowiednie hasła w swoim profilu.
  - Zamiast wpisywać hasło w pustych polach wystarczy przesunąć zarejestrowany palec na czytniku linii papilarnych, a program dokona logowania do programu lub strony internetowej.
-

Czytnik linii papilarnych



Logowanie w Windows 10

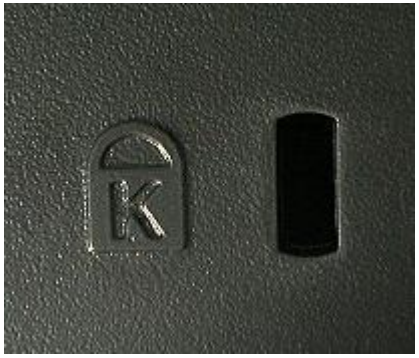


LINKA MOCUJĄCA

Linka mocująca laptop

- Linka mocująca to zabezpieczenie fizyczne przed kradzieżą laptopa.
- Częste sytuacje to miejsca publiczne, pełne ludzi:
  - Biuro, miejsce pracy, kawiarnia, restauracja, środki komunikacji masowej, samochód (laptop na siedzeniu obok lub z tyłu samochodu)
  - Charakterystyczna torba na laptopa
- Ochroną jest stalowa linka wpinana w gniazdo zabezpieczające laptopa i umocowana do elementu trwałego i trudnego do przeniesienia (stół, szafa, ławka).
- W nowych laptopach zwykle znajdują się dwa takie gniazda – jedno z boku, drugie z tyłu obudowy.
- Ułatwia to użytkownikowi podpięcie linki w miejscu, w którym nie będzie przeszkadzała w pracy.
- Otwory te są zgodne ze standardem Kensington Lock firmy *Kensington Technology Group*.
- Linka jest stalowa, co utrudnia jej przecięcie.
- Możliwe jest wyrwanie głowicy zabezpieczającej z laptopa. Laptop jest dalej sprawny, ale obudowa jest uszkodzona, co wskazuje na kradziony model.
  - Powinno to uniemożliwić próbę odsprzedaży komputera przenośnego.

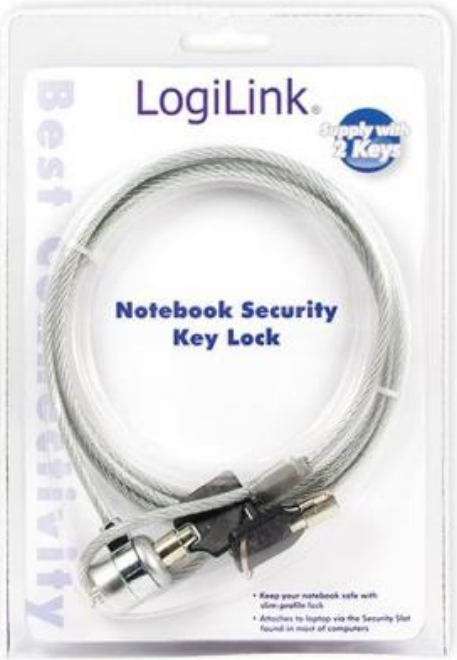
Mocowanie laptopa w K-Slot



- Otwór na linkę to złącze Kensington Lock, Kensington Slot lubK-Slot.
- To odpowiednio wyprofilowana szczelina w obudowie notebooka. Jej kształt pozwala na wpięcie stalowej linki zakończonej specjalną głowicą.
- W głowicy jest umieszczony zamek, po zamknięciu którego nie da się już wyjąć głowicy z otworu bez poważnego uszkodzenia obudowy notebooka. Zamek w głowicy zamykany jest na kluczyk lub coraz częściej stosuje się zamiast zamka na kluczyk zamek szyfrowy z trzema lub czterema pokrętłami z cyframi.
- Drugi koniec stalowej linki zakończony jest pętlą, przez którą przekłada się koniec linki z głowicą. Linkę powinno się owinąć wokół trwałego elementu wyposażenia pokoju lub trudnego do przesunięcia bądź podniesienia przedmiotu tak, by niemożliwe było jej zdjęcie (rura kaloryfera, noga ciężkiego biurka czy szafy).

Typy złączy zabezpieczających

Linka mocująca laptop



NAKLEJKA ZABEZPIECZAJĄCA

Naklejka zabezpieczająca

- Niektóre z uchwytów zabezpieczających są połączone z linką mocującą. Uchwyty umocowane są do oznaczeń ostrzegających. Te oznaczenia nazywane są po angielsku **STOP Tag Identification**.
- Zerwanie linki wraz z gniazdem z obudowy z odpowiednio dużą siłą odsłania przyklejoną na stałe do obudowy laptopa **płytkę z informacją**, że ten **notebook został skradziony**.
- Na płytce takiej podaje się również nazwę firmy lub nazwisko właściciela do którego należy notebook oraz numerem kontaktowy.

STACJA BLOKUJĄCA

Stacja blokująca

- Stacja blokująca to rozwiązanie przydatne dla laptopów nie posiadających gniazd zabezpieczających lub do stosowania jako ochrona dodatkowa.
- Laptop wkłada się za specjalne rączki i jest on trwale umieszczony w podstawce.
- Stacja jest następne mocowana do biurka lub zabezpieczana linką mocującą.

Stacja blokująca

Stacja blokująca

BLOKADA OTWARCIA LAPTOPA

Blokada otwarcia laptopa

- Blokada otwarcia laptopa ma uniemożliwić otworzenie laptopa przez niepowołana osobę.
- Jednocześnie pełni rolę umocowania uniemożliwiającego wyniesienie sprzętu komputerowego z pomieszczenia.
- Ma postać obręczy, płaskownika lub specjalnego zamka blokujące otwarcie pokrywy laptopa. Może być połączona z linką mocującą.

Blokada otwarcia laptopa

Blokada otwarcia laptopa

Blokada otwarcia tabletu

CZUJNIK WYNOSZENIA SPRZĘTU

Czujnik wynoszenia sprzętu

- Zadaniem czujnika jest poinformowanie użytkownika o próbie wyniesienia komputera przenośnego.
- Rodzaj zagrożenia
  - Urządzenie może być czujnikiem ruchu, który reaguje na próbę ruszenia chronionego laptopa.
  - Innym sposobem jest powiązanie urządzenia w komputerze z ochroną pomieszczenia, która reaguje przy próbie wyniesienia poza pomieszczenia sprzętu.
- Rodzaj alarmu
  - Urządzenia mogą wysyłać sygnał alarmowy do systemu alarmowego instytucji lub uruchamia alarm akustyczne (głośniki laptopa).
  - Inną opcją jest zablokowanie HDD i OS.
  - System bezpieczeństwa może też wykorzystać moduł GPS do informowania o położeniu wyniesionego sprzętu.
  - Zabezpieczenie może być wmontowane w BIOS co uniemożliwia dezaktualizację przez zmianę dysku lub reinstalację OS.
- Alarmy mogą być wbudowane w laptop (specjalne płyty główne lub dodatkowe karty) ewentualnie w postaci zewnętrznych czujników na USB.
- Mogą też wspomagać inne systemy ochrony (jak linki)

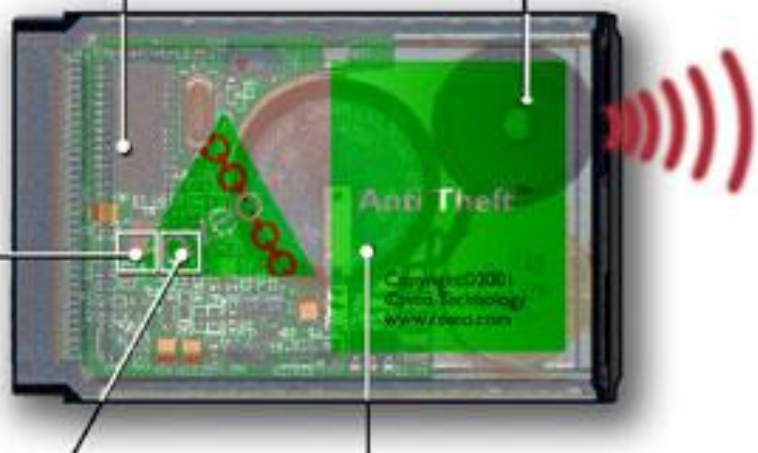
Czujnik wynoszenia sprzętu

Karta alarmowa

Processor
- analyzes motion history
- determines threat
- implements responses

Sounder
- issues alert and warning signals
- sounds alarm

Motion Sensor
- detects movement



Secure Storage
- protects confidential information

Rechargeable Battery
- powers system when computer is off

CZUJNIK IDENTYFIKACJI

Czujnik identyfikacji

- Wireless PC Lock
- Czujnik ogranicza możliwość skorzystania z laptopa, do grona wyznaczonych osób.
  - Jeżeli osoba uprawniona oddali się poza wyznaczoną odległość, komputer przenośny się blokuje. Gdy wraca do maszyny, notebook z powrotem jest odblokowany.
- Całość składa się z modułu montowanego w gnieździe USB chronionego komputera i części noszonej przez człowieka.

Czujnik identyfikacji

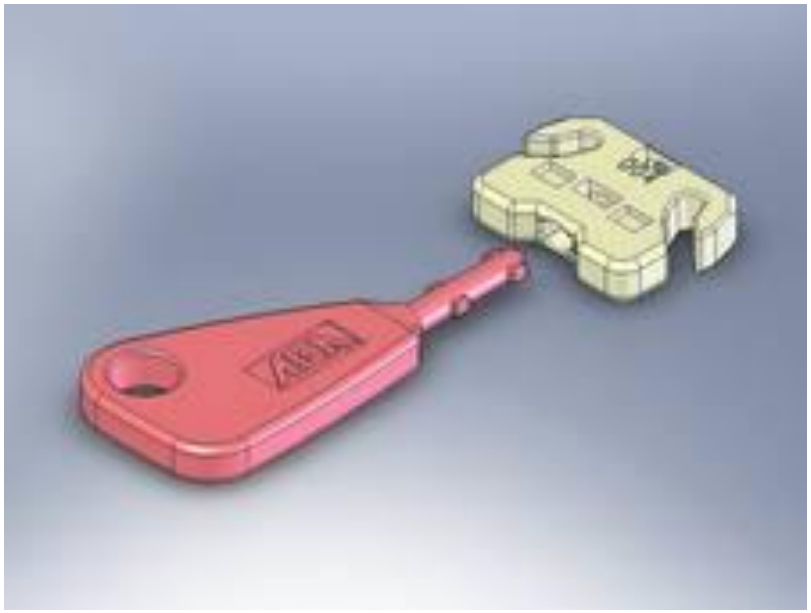
BLOKADA PORTÓW USB

Blokada portów USB

- Lock USB Ports
- Urządzenie blokuje fizycznie port USB, uniemożliwiając włożenie tam innego nośnika danych lub urządzenia czytającego.
  - Rozwiązanie składa się z zaślepek wkładanych do portu, które można wyjąć tylko specjalnym narzędziem.
  - Innym sposobem jest programowe zablokowanie korzystania z gniazd USB.

Blokada portów USB

Blokada portów USB

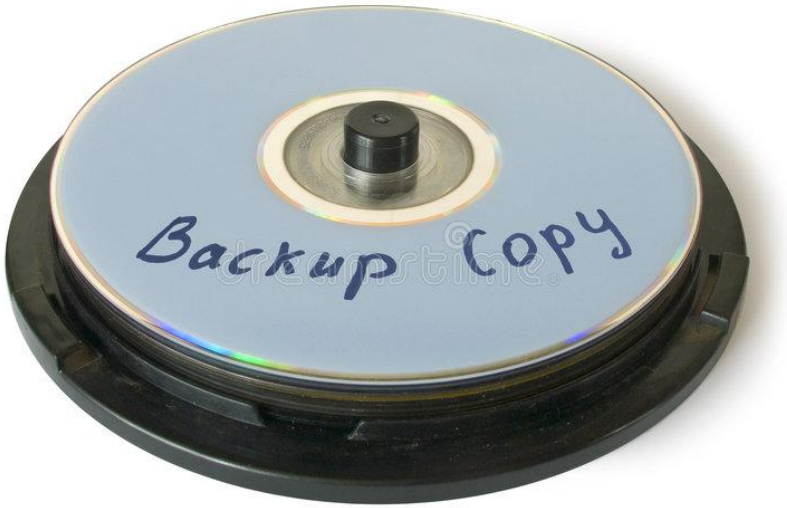


KOPIA BEZPIECZEŃSTWA DANYCH

Kopia bezpieczeństwa danych

- Kopia danych pozwoli na odtworzenie ważnych informacji w wypadku uszkodzenia, lub kradzieży laptopa.
- Metody tworzenia kopii:
  - Na zewnętrznym twardym dysku
  - Dysk sieciowy
  - Napędy taśmowe
  - Kopia na DVD
  - Chmura internetowa
- Zalecane jest robienie automatycznych kopii bezpieczeństwa (najlepiej codziennie).
  - Harmonogram zadań systemu operacyjnego

Kopia bezpieczeństwa danych



REDUKCJA PROMIENIOWANIA ELEKTROMAGNETYCZNEGO

Redukcja promieniowania elektromagnetycznego

- Każde urządzenie przez które płynie prąd, jest źródłem promieniowania elektromagnetycznego. Przepływ danych w odbywający się między poszczególnymi elementami komputerów (kablami, portami, gniazdami, monitorem) generuje promieniowanie elektromagnetyczne o określonej częstotliwości. Każde z tych elementów poprzez promieniowanie elektromagnetyczne ujawnia pewne informacje, które przy użytej odpowiedniej technologii można odczytać.
- Emisja, której odbiór, rejestracja a następnie analiza da możliwość odtworzenia fragmentu przetwarzanej informacji niejawnej jest **emisją ujawniającą**.
- Pole elektromagnetyczne powstałe podczas przetwarzania informacji niejawnych jest tak silne, że posiadając odpowiednie urządzenia można w prosty sposób przechwycić emisję ujawniającą i po jej analizie odczytać przetwarzaną informację. Informacje z komputera można odczytać poprzez wykorzystanie specjalnie przystosowanych anten oraz wykorzystując np. sieć wodną, elektryczną, grzewczą, oraz przewody klimatyzacyjne.

Redukcja promieniowania elektromagnetycznego

- W laptopie jesteśmy w stanie podsłuchać transmisję WiFi, Bluetooth, przesył danych wewnątrz komputera, polecenia wpisywane na klawiaturze, ruchy na touchpadzie.

Norma Tempest

- Norma TEMPEST (*temporary emanation and spurious transmission*) to program ochrony przed niekontrolowaną emisją ujawniającą.
  - Program powstał w latach 50-tych w USA na zlecenie Pentagonu. Na przestrzeni lat standard ten był wielokrotnie rewidowany i publikowany pod różnymi nazwami.
- OD 1984 jednostką koordynującą wprowadzanie tej normy jest NSA - *Narodowa Agencja Bezpieczeństwa Stanów Zjednoczonych*.
  - Jest upoważniona do przyjmowania i modyfikowania wszystkich standardów, systemów oraz sprzętu związanych z bezpieczeństwem elektronicznym, w tym z zagadnieniami TEMPEST.
  - Producenci mogą współpracować przy produkcji sprzętu TEMPEST, ale muszą mieć zgodę Agencji.
- Organem upoważnionym w Polsce do przeprowadzania badań i certyfikacji wyrobów o przeznaczeniu specjalnym jest *Jednostka Certyfikująca Urządzeń i Systemów Kryptograficznych oraz Kompatybilności Elektromagnetycznej* powołana w Biurze Bezpieczeństwa Łączności i Informatyki ABW.
  - Urządzeniami są kategorii TEMPEST.

Zabezpieczenia elektromagnetyczne laptopów

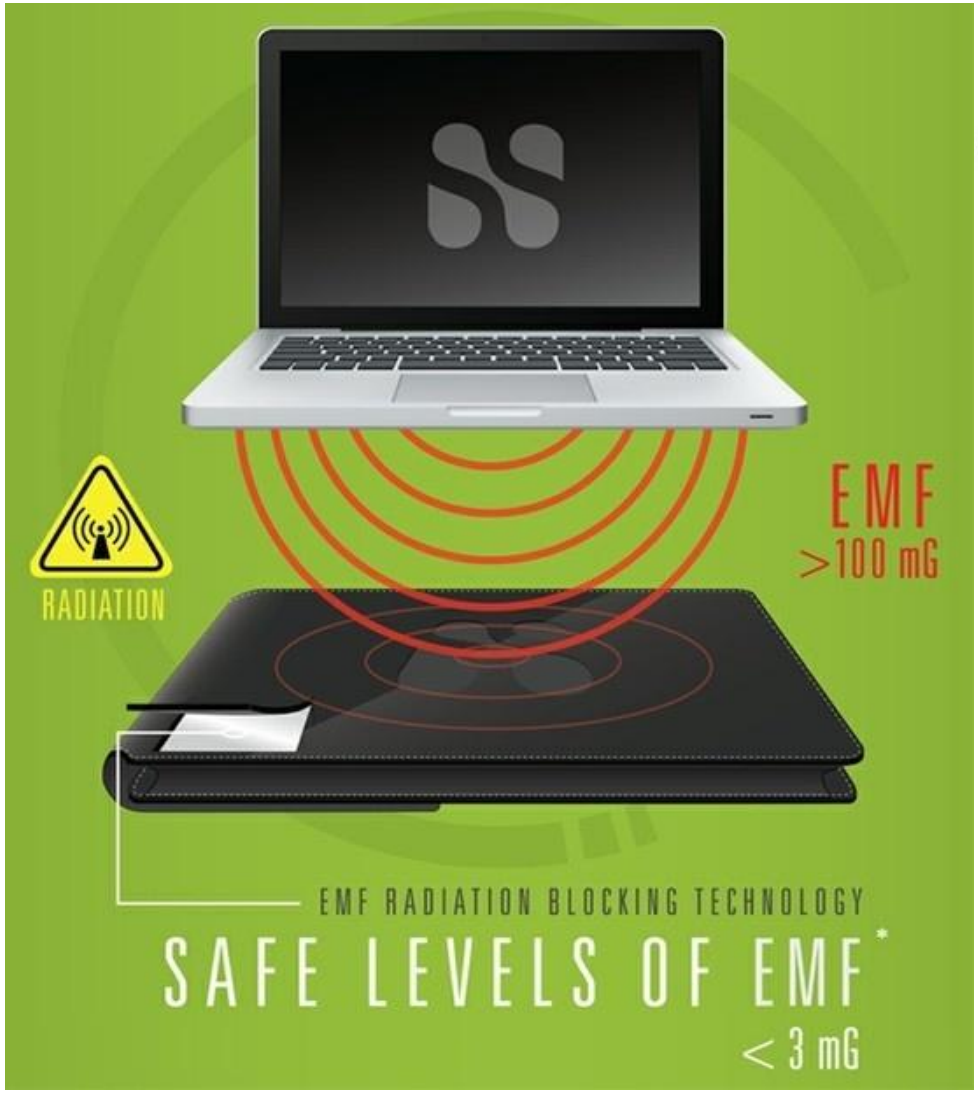
- Pomieszczenia ochronne
  - kabiny elektromagnetyczne odpowiednio uziemione, gdzie poziom promieniowania elektromagnetycznego wychodzący na zewnątrz jest tak niski, że nie jest możliwe jego odczytanie;
  - Wyklejanie ścian pomieszczeń metalowymi foliami i siatkami, o słabszym poziomie ochrony;
- Zewnętrzne osłony komputerów
  - metalowe pudełka, w których umieszcza się sprzęt, emitujący promieniowanie. Mogą być to nie tylko komputery, ale także urządzenia nadawczo — odbiorcze lub szyfratory;
- Zabezpieczenie komputerów przenośnych
  - Ekranowana obudowa
  - Zaślepki magnetyczne na nieużywane porty zewnętrzne
  - Ekranowane przewody

Laptop militarny

Pomieszczenie ochronne

Klatka ekranująca

Podkładki ekranowane



Pomiar natężenia pola EMG

Radiation test before use Radiation shield

Before use: Display 1378 V/M
Kyeboard: 311 V/M
Mouse: 265 V/M
Comupter Host: 719 V/M

Radiation test after use Radiation shield

After use: Display 11 V/M
Kyeboard: 0.0 V/M
Mouse: 0.0 V/M
Comupter Host: 10V/M

TORBA OCHRONNA

Torba ochronna

- Częstym powodem kradzieży notebooka jest przechowywanie go w charakterystycznej torbie.
  - Logo firmy przykuwa uwagę i wskazuje na cenną zawartość
  - Typowe torby nie gwarantują bezpieczeństwa
- Dobrym rozwiązaniem jest sportowy plecak
  - Nie wskazuje na zawartość
  - Wiele modeli jest przystosowanych do transportu notebooków
- Dodatkowe zabezpieczenie
  - Kłódka
  - Linka zabezpieczająca
- Torba i plecak antykradzieżowy
  - zabezpieczają laptopa przed niepostrzeżonym jego wyciągnięciem ze środka torby
  - specjalny zamek nie pozwala na niepostrzeżone jej otwarcie
  - Ścianki torby wykonane są ze specjalnego kompozytowego materiału, dodatkowo wzmacnianego metalową siatką. Uniemożliwia to rozcięcie ścianek i wyciągnięcie komputera z torby.
  - Ramiona plecaka czy pasek torby są wzmacniane i nie da się ich łatwo przeciąć.
  - Specjalna linka zabezpieczająca mocuje notebooka do torby.

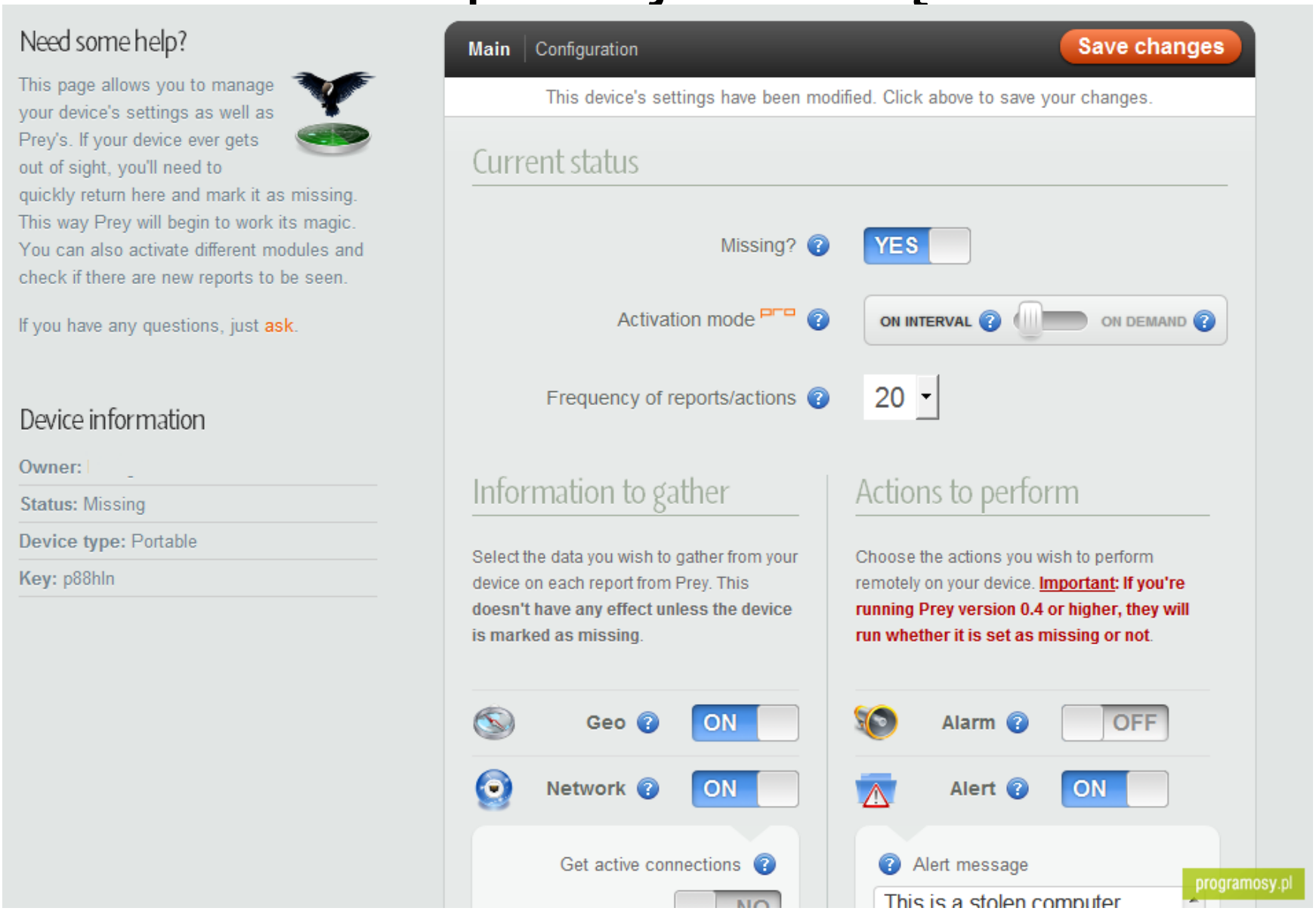
Torba ochronna

APLIKACJE ŚLEDZĄCE

Aplikacje śledzące

- Zadaniem takich aplikacji jest dyskretnie informowanie o bieżącym położeniu laptopa, telefonu lub tabletu na podstawie GPS-u lub triangulacji z WiFi.
- Do raportów dołącza się często zrzuty ekranu i zdjęcia zrobione aparatem skradzionego urządzenia.
  - Wymagane jest połączenie z Internetem
- Aplikacje mogą mieć wiele przydatnych funkcji:
  - Skradzione urządzenie można zdalnie zablokować,
  - Włączenie zdalnego dźwięku uniemożliwia pracę i ułatwia znalezienie złodzieja (syreną są głośniki komputera),
  - Wyświetlenie na ekranie odpowiednich komunikatów pomoże ewentualnemu znalazcy oddać sprzęt,
  - Robienie zdjęć z kamery może wskazać miejsce gdzie znajduje się skradziony sprzęt, a nawet sfotografować twarz złodzieja,
  - Zdalne wymazanie danych z laptopa pozwoli je ochronić
  - Sformatowanie lub skasowanie systemu uniemożliwi pracę,
  - Zdalne odzyskanie plików na odległość pozwoli odtworzyć nawet te dane usunięte przez sprawcę.
- Część z tych funkcji może działać nawet bez dostępu do Internetu.
- System działający na poziomie BIOSu i współpracujący z modułem sprzętowym przetrzyma nawet wymianę dysku twardego.

Aplikacje śledzące



UBEZPIECZENIE

Ubezpieczenie

- Celem ubezpieczenia jest ochrona danych i sprzętu przed uszkodzeniem i kradzieżą.
- Głównym obiektem chronionym jest sprzęt. Można też ochronić dane: np. zainstalowane programy czy dane kupione.
- Popularna oferta
  - Dostępna w każdym towarzystwie ubezpieczeniowym (typowa polisa)
  - Oferowana w sklepie przy zakupie produktu (przedłużona gwarancja)
- Warunki umowy:
  - Mogą być zróżnicowane i nie zawsze obejmują wszystkie opcje
  - Awarie lub uszkodzenie sprzętu
  - Kradzież laptopa
  - Wartość minimalna szkody
  - Nieuprawnione użycie
  - Zalanie sprzętu
- Ochrona danych
  - Użytkownik musi wykonywać regularne kopie danych
  - polisa obejmuje tylko dane utracone w okresie od ostatniego back-upu.

Dowód zakupu

- Niezbędny podczas zgłaszania kradzieży na policji oraz wypłaty ewentualnego odszkodowania w ramach wykupionej polisy.
- Może być faktura lub paragon. Przydatne są też dowody wpłaty lub wyciągi z konta.

POWTÓRZENIE

1. Jakie znamy kategorie zabezpieczeń komputerów przenośnych?
2. Dlaczego laptopy są szczególnie narażone na wyciek i uszkodzenie danych?
3. W jakim celu stosujemy hasła systemowe?
4. Jak zbudowane powinny być hasła systemowe?
5. Jakie są reguły bezpieczeństwa dotyczące korzystania z haseł?
6. Jak MS Windows wspiera prawidłowe korzystania z haseł systemowych?
7. W jakim celu stosuje się szyfrowanie danych na dysku?
8. Czym się różni szyfrowanie dysku od szyfrowania plików?
9. Co to jest TPM (Trusted Platform Module)?
10. Jak działają programy szyfrujące typu BitLocker?
11. Jak działa karta kryptograficzna?
12. Jakie są zalety korzystania z czytnika linii papilarnych?
13. Co to jest *Single Sign On (*jednorazowe logowanie)?
14. Jak chroni linka mocująca notebooka?
15. Jak chroni komputer naklejka mocująca?

16. Opisz mechanizm obrony przez stację blokującą.
17. Co uniemożliwia blokada otwarcia laptopa?
18. Jak chroni czujnik wynoszenia sprzętu?
19. Do czego służy czujnik identyfikacji?
20. W jakim celu stosuje się blokadę portów USB?
21. Jak wykonywać kopie bezpieczeństwa danych z laptopa?
22. Co to jest norma Tempest?
23. Jak zredukowanie wyciek promieniowania danych z laptopa?
24. Przed czym zapobiega torba ochronna?
25. Jak działają aplikacje śledzące?
26. Czym się różni ubezpieczenie i gwarancja przedłużona?

Dbaj o bezpieczeństwo