

## HAK2

Klucz USB do zabezpieczenia oprogramowania i kodowania danych



### Dane techniczne:

- Interfejs USB:
  - ◆ Prędkość Low Speed (1,5 Mb/s)
  - ◆ Specyfikacja USB 1.1 i USB 2.0
  - ◆ Driver HID - human interface device
  - ◆ VID 0x13AB - identyfikator producenta
  - ◆ PID 0x0001 - identyfikator produktu
- Kodowanie:
  - ◆ Algorytmy DES, DES3
  - ◆ Klucze S0 (168bit) - sprawdzanie podpisu  
S1 (168bit) - kodowanie  
A (168bit) - kodowanie
- Pamięć:
  - ◆ pojemność 4 kBajty
  - ◆ organizacja 250 stron po 16 bajtów
- Wymiary 54 x 18 x 8 mm

### Zastosowania:

- Zabezpieczenie przed użyciem nielegalnych kopii programu – sprawdzanie obecności klucza przy uruchamianiu programu
- Zabezpieczenie dostępu do programu – logowanie do programu poprzez sprawdzanie haseł użytkowników w kluczu HAK2
- Udostępnianie poszczególnych funkcji programu poprzez wydanie licencji podpisanej cyfrowo
- Kodowanie danych zapisywanych na dysku komputera
- Kodowanie transmisji pomiędzy komputerami w tej samej instalacji
- Kodowanie danych przesyłanych do innych osób np. przez e-mail
  - ◆ kodowanie do całej grupy, która posiada klucze HAK2 z takimi samymi kluczami S1 lub A
  - ◆ kodowanie z podaniem numeru klucza – tylko ten jeden klucz potrafi odkodować dane.



## Ogólna charakterystyka urządzenia

Klucz HAK2 jest wykonany w formie wtyczki włączanej bezpośrednio w złącze USB. Do komunikacji z komputerem wykorzystuje najniższą ze zdefiniowanych w standardzie USB prędkości transmisji (Low Speed = 1,5Mb/s).

HAK2 nie wymaga instalowania specyficznego dla siebie drivera. Korzysta on ze standardowego drivera HID (human interface device), który jest dostępny w systemie Windows od wersji Windows'98. Driver ten jest dostępny również w każdym innym systemie operacyjnym, który umożliwia podłączenie do komputera klawiatury USB.

Program może współpracować z wieloma kluczami HAK2 jednocześnie włączonymi w gniazda USB. Możliwa jest również bezkonfliktowa praca kilku aplikacji, z których każda komunikuje się ze swoim kluczem HAK2.

Transmisja danych między programem a kluczem HAK2 jest kodowana algorytmem DES. Dla każdej sesji tworzony jest inny klucz transmisyjny w oparciu o hasło użytkownika i liczby losowe.

## Zawartość klucza

Dane do klucza HAK2 wprowadzone są przez 3 podmioty:

- MicroMade - producenta kluczy HAK2:
  - VID i PID - identyfikator producenta i urządzenia
  - SN - niepowtarzalny 4 bajtowy numer fabryczny danego egzemplarza HAK2
- Programista - autor programu wykorzystującego klucze HAK2:
  - SID - identyfikator programu
  - S0 - klucz DES3 do sprawdzania podpisów
  - S1 - klucz DES/DES3 do kodowania/dekodowania danych
  - MST - maksymalny czas sesji - czas po którym zostanie ona zerwana przez klucz HAK2
  - RAC - awaryjny kod kasujący
- Administrator - osoba zarządzająca daną instalacją programu:
  - AID - identyfikator instalacji
  - A - klucz DES/DES3 do kodowania/dekodowania danych
  - Inne dane programu - w tym hasła i uprawnienia użytkowników (również administratorów)

## Sprawdzanie obecności klucza HAK2

Znalezienie 'swojego' klucza HAK2 jest w pewnym sensie sprawdzeniem jego obecności. Jednak wszelkie wykorzystywane w tym celu informacje są jawne. Istnieje więc możliwość zrobienia urządzenia USB, które zgłosi się tak samo.

Wiarygodne sposoby identyfikacji klucza HAK2 to:

- sprawdzenie, czy klucz HAK2 prawidłowo zakoduje losowe dane kluczem S1 (zamiast umieszczać w programie klucz S1 narażając go na ujawnienie można posłużyć się przygotowanym wcześniej odpowiednio dużym zestawem losowych danych i wyników ich zakodowania)

- zakodowanie fragmentu programu (np. wyświetlanych tekstów) - do rozkodowania wykorzystywany jest klucz S1 przy każdym uruchomieniu,
- umieszczenie fragmentu programu w pamięci klucza HAK2 i wczytywanie przy uruchomieniu programu.

## Kodowanie danych

Klucz A ma w każdej instalacji programu inną wartość ustaloną przez administratora programu. Dlatego może on być wykorzystany do kodowania danych, które mają być dostępne tylko dla użytkowników tej instalacji programu. Dotyczy to zarówno danych przechowywanych na dysku jak i danych przesyłanych między poszczególnymi komputerami.

Bezpośrednie zastosowanie klucza HAK2 (z kluczem A) do kodowania danych jest nieefektywne czasowo i nie zapewnia zmienności kluczy stosowanych do kodowania danych. Jedną z najprostszych możliwości jest kodowanie danych na komputerze za pomocą wygenerowanego losowo klucza K, a następnie zakodowanie go kluczem HAK2 (z kluczem A). Klucz K w tej zakodowanej postaci może być jawnie przesyłany między komunikującymi się ze sobą komputerami lub dołączony do szyfrowanego bloku danych na dysku - jest on bezużyteczny bez klucza HAK2 z właściwym kluczem A.

Klucz HAK2 umożliwia również zakodowanie porcji danych z określeniem ich adresata (wewnątrz grupy o tych samych kluczach A lub S1) - odkodować potrafi je tylko HAK2 o numerze fabrycznym wskazanym przy kodowaniu. Dzięki temu możliwe jest przesyłanie poufnych danych do wybranych członków grupy.

## Podpisywanie danych

Podpisywanie danych pozwala na ich zabezpieczenie przed modyfikowaniem przez nieuprawnione osoby. Każdy zestaw danych można przetworzyć w taki sposób, aby uzyskać ciąg bajtów o konkretnej długości zależny od każdego z bajtów danych wejściowych. Uzyskany ciąg bajtów jest podpisem tego zestawu danych.

Programista może to wykorzystać w celu niezależnego udostępniania poszczególnych funkcji programu poprzez wydanie licencji podpisaną cyfrowo. Plik licencji może zostać związany z konkretnym użytkownikiem poprzez wpisanie nazwy użytkownika.

Inną możliwością jest związanie informacji o uprawnieniach z konkretnym egzemplarzem klucza HAK2. Tak przygotowana licencja będzie zaakceptowana tylko przez jeden klucz HAK2.

## Sesja

Wszystkie istotne funkcje klucza HAK2 stają się dostępne dopiero po zalogowaniu się użytkownika, czyli otwarciu jego sesji. Wygenerowany wówczas (losowo) klucz transmisyjny chroni wymianę danych pomiędzy programem a kluczem HAK2 - transmisja szyfrowana jest algorytmem DES.

*Uwaga!*

*W kryptologii wyróżnia się algorytmy (ogólnie znane) i klucze (tajne). W niniejszym opisie słowo klucz występuje w dwóch znaczeniach. W połączeniu z symbolem HAK2 oznacza urządzenie jakim jest klucz HAK2 przeznaczony do zabezpieczenia oprogramowania. W każdym innym wypadku oznacza tajny klucz (ciąg danych, zwykle małych rozmiarów, np. klucz do algorytmu DES ma 56 bitów) przeznaczony do kodowania/dekodowania danych za pomocą określonego algorytmu.*