



HAK2

Software protection and data encryption USB hardware key



Technical data:

- USB interface:
 - ◆ Speed Low Speed (1,5 Mb/s)
 - ◆ Specification USB 1.1 and USB 2.0
 - ◆ Driver HID - human interface device
 - ◆ VID 0x13AB – manufacturer's id.
 - ◆ PID 0x0001 – product id.
- Encoding:
 - ◆ Algorithm DES, DES3
 - ◆ Keys S0 (168bit) – signature check
S1 (168bit) - encoding
A (168bit) - encoding
- Memory:
 - ◆ capacity 4 kB
 - ◆ organisation 250 pages, 16 bytes each
- Dimensions 54 x 18 x 8 mm

Applications:

- Preventing usage of illegal copies of software - checking key presence at programme startup
- Securing access to software - logging into programme after checking user passwords in the HAK2 key
- Allowing access to restricted software functions (digitally signed licence)
- Encoding data saved on hard disks
- Encoding transmissions between computers
- Encoding data sent to other users (for example: e-mail messages):
 - ◆ encoding for a whole group which has HAK2 keys with the same S1 and A keys
 - ◆ encoding and giving a key number - only one key can decode the data



General device characteristic

The HAK2 key is a USB device plugged directly into the USB port. For communication it uses the lowest speed defined for the USB standard (Low Speed = 1.5 Mb/s).

HAK2 does not require any additional drivers. It uses the standard HID (human interface device) driver. It is available in the Windows® system (Windows®98 and newer). This driver is available in any other system, which supports a USB keyboard.

Software can cooperate with many HAK2 keys, which can be plugged into USB ports at the same time. It is also possible for many programmes to work with their own HAK2 keys simultaneously.

Data transmission between software and the HAK2 key is encoded using the DES algorithm. For each session a different transmission key is created based on the user's password and random numbers.

Key content

Data inserted into the HAK2 key comes from 3 sources:

- MicroMade - the manufacturer of the HAK2 key:
 - VID and PID - manufacturer and device identification
 - SN - unique 4 byte product number, different for each HAK2 key
- The programmer – author of software using HAK2 keys:
 - SID - programme identification
 - S0 - DES3 key for checking signatures
 - S1 - DES/DES3 key for encoding/decoding data
 - MST - maximum session time - if it elapses the session is terminated by the HAK2 key
 - RAC - emergency deleting code
- The administrator - the person who manages the programme installation:
 - AID - installation identification
 - A - DES/DES3 key for encoding/decoding data
 - Other software data - including users/administrators passwords and rights.

Checking HAK2 key presence

Finding the proper HAK2 key is a form of verifying if the key is present. All data used for such verification is public. That is why it is possible to create another USB device which can identify itself in the same way.

The HAK2 uses trustworthy methods of identification:

- checking if the HAK2 codes random data properly with the S1 key (Placing the S1 key in the programme may lead to its revealing. It is better to prepare a suitably big set of random data and proper coding results.)

- encoding fragments of software (such as displayed texts) - the S1 key is used to decode them at each programme startup
- placing a fragment of the software in the memory of the HAK2 key which will be read at each programme startup.

Encoding data

The A key has a different value in each installation. This value is set by the administrator. It can be used for encoding data destined for users of only one installation (including data saved on the hard disk or transmitted between computers).

Using the HAK2 key (with the A key) directly for encoding data is time-consuming and your data is encrypted with the same key each time. One of the easiest methods is to encode data on the computer using a random K key, and then encoding it with the HAK2 key (with the A key). The K key in this encrypted form can be transmitted between computers or added to a block of encrypted data on a hard disk - it will be useless without a HAK2 key with the proper A key.

The HAK2 key can also encode data destined for a specific recipient (among a group of keys with the same A or S1 keys) - the data can then be decoded only by the HAK2 key with the serial number specified during encoding. This allows sending confidential data to specific users.

Digital signature

Signing data with digital signature protects it from being modified by unauthorised persons. Each set of data can be modified to create a byte string with a specified length. Its content depends on each input byte. The obtained byte string is the signature of the data set.

The programmer can use this function for allowing access to restricted software functions by issuing digitally signed licences. A licence can be connected with a specific user or a specific serial number of the HAK2 key (only the user with the specific HAK2 key can access the software or its fragment).

The other possibility is connecting the access rights with specified single HAK2 key. Licence prepared this way is accepted only by this one HAK2 key.

Session

All the essential functions of the HAK2 key are available only after the user logs in (a session is then opened). When a session opens a randomly generated transmission key protects data exchange between the computer and the HAK2 key - the transmission is encoded with the DES algorithm.

Please note!

Cryptology distinguishes algorithms (publicly known) and keys (secret). The description above includes the word 'key' in two meanings. While mentioning the HAK2 key it means the HAK2 device used for software security. In any other case it means a secret key (small size data block, for example a DES algorithm key has 56 bits) used for encoding/decoding data with a specified algorithm.