DESkey®
protect your software.

DK2USB/B

datasheet

- **HID Device – no custom kernel driver required**
- **Pseudo-Random Number Generator**
- **Through Encryption**
- **Unique 6 Byte Password**
- **Memory (256KB – 64KB)**
- **Down-Counter**
- **Variable Response Algorithm Commands**
- **Remote Commands**

RoHS compliant
WEEE-Reg-No:
DE 90465365

Description

Within the DESkey is a very large 'seedable' Pseudo-Random number generator, capable of producing vast quantities of data. This data may be used by your application in many ways, such as providing unique encryption keys for protecting vital areas of your code. You can also pass code or data through this function for in-line encryption, this keeps the encryption key within the hardware.

As standard, 224 bytes of memory are available: split into 16-byte 'Public' and 208-byte 'Private' sectors. The Public sector can be read and written to at any time, the Private sector requires a customer specific 6-byte password for writing. This feature enables licensing and configuration information to be written to the Private sector.

The down counter is programmable between 0 and 16 million, provides the means to stop your software working after a pre-programmed number of executions or metering the run of a process.

As per the Private sector of the memory this is protected with the same 6-byte password. Attempts at random guessing this password will cause the DESkey to shut down until reset at the factory.

The Anti-Emulation Algorithm works in conjunction with an algorithm run on the host system, which encrypts and sends data to the DK2 where an embedded complementary algorithm decrypts it. Similarly, data returned is encrypted in the DK2 and sent to the host which decrypts it. The command sent and data returned has a different form each time it is used, even if the same command is used repeatedly, thereby preventing functional emulation by a device driver or any other means. The powerful Anti-Emulation Algorithm is being used to provide additional 'Hidden Commands' such as Secure Memory Read, Reading the Down Counter, Updating Private Memory, Disabling Main Commands, Re-writing the Down Counter and Returning Junk Data. Called as often as required, the command sent and returned data will never appear to be the same.

Using certain Hidden Commands, the Private Memory or the Down Counter may be securely updated in the field. The DK2 contains a special Update Counter, of which the current value must be known and supplied as part of the encrypted Remote Command. Using this, it is possible to create an encrypted sequence that can be given to an end-user to update their DK2. This Command is totally secure because it is encrypted using data unique to the end-user's specific DESkey and the state of its Update Counter. Since the Remote Command increments the Update Counter, it can only ever be used once. To update the DK2 again, a new Command sequence must be generated.

Technical Specifications

- Interface: USB A-type connector, Full Speed USB 2.0 – USB 3.2 compatible
- Communication protocol: Mass Storage Device (MSD) or Human Interface Device (HID), HID default
- Power supply: 5V bus-powered, < 20 mA
- Operating and storage temperature:
- -40° C ... +90° C, non-condensing
- MTBF (Mean Time Between Failures): > 3 Million hours
- Case / Dimensions: 12.1 mm x 22 mm x 4.5 mm
- Weight: 3,1 g
- Warranty: 36 months

Certificates

Tested and qualified in accordance with the following standards:

CE-Conformity | European Certificates

Fully compliant with all applicable European regulations.

- 2014/30/EU EMC: Report Bureau Veritas File CECFPE-WTW-P22020697, 2022-03-22
- EN55032:2015+A11:2020 Class B, IEC/CISPR 32:2015+Cor1:2016
- EN55035:2017+A11:2020, IEC/CISPR 35:2016
- AS/NZS CISPR32:2015+AMD1:2020, Class B, IEC/CISPR32:2015+AMD1:2019
- All CmStick/B units are fully compliant with EU Directives 2011/65/EU (RoHS), 2015/863/EU (RoHS amendment), SJ/T 11364-2014 (China RoHS2), 2012/19/EU (WEEE), 1907/2006/EC (REACH), 207/2011/EU (PFOS -REACH Annex XVII), 1272/2013/EU (PAH-REACH Annex XVII), and 1272/2013/EU (DINP-REACH Annex XVII).

D43250
RoHS

International Certificates

Fully compliant with all applicable European regulations.

- 47 CFR FCC, Part 15, Subpart B (2017), class B: Report Bureau Veritas File CICFPE-WTW Veritas File CICFPE-WTW
- ICES-003:2017 Issue 7, Class B
- VCCI 32-1 Class B ITE: Acceptance No 2021067439
- KCC (South Korea): R-R-XWK-CmStick, 2018-08-08
- BSMI (Taiwan): D43250 RoHS
- ACMA (RCM): RCM20180091804-C, 2018-09-19
- EAC TP 037/2016: ЕАЭС N RU Д DE.PA01.B.25142/20

방송통신위원회

Other Certificates

- VDE License No. 129382
- C-UL-US listed I.T.E. Accessory 10 WB, E-File 211202, 2018-07-30

The encryption device is only for use with UL Listed PCs (low power system). Meets UL 60950-1 and CSA C22.2 No. 60950-1 Safety of Information Technology Equipment specifications.

Ordering Information

- P/N 1001-03-560-0291 DESkey DK2USB/B

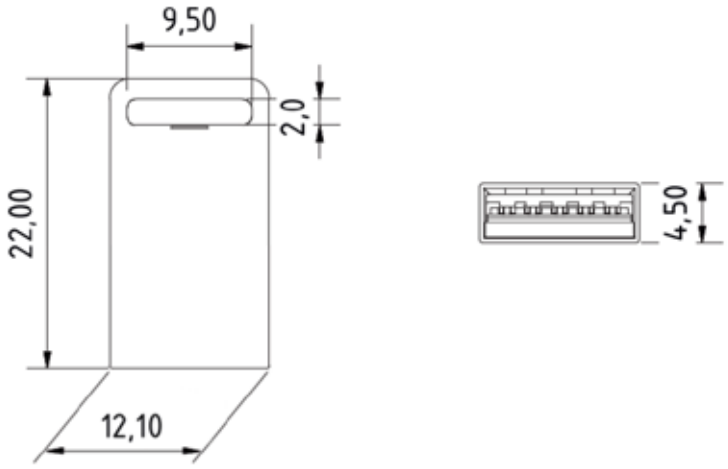
Individual cases or laser engraving are available on demand.

DESkey®
protect your software.

DK2USB/B

technical drawing

RoHS compliant
WEEE-Reg-No:
DE 90465365



D43250
RoHS

방송통신위원회