

dKey



USB cryptographic token with digital signature

dKey is a cryptographic Token created by SATA HTS in order to accomplish functions of **security and certified digital signature**. This Token is based on a ITSEC E4+ certified embedded chip, which has been specifically developed for the management of public and private RSA keys.

The cryptographic Token combines the functions of a **smart card** to that of a **reader**, thus making its usage easy and immediate on all kinds of computers that have an USB door, both with a Windows and a Linux operative system.

dKey allows you to use a wide range of security services, such as the certified digital signature, the authentication and the ciphering procedure. These functions satisfy the needs for confidentiality, non-repudiability and privacy of the data.

The cryptographic motor of the USB Token is made up of a microprocessor that is able to process the RSA algorithm till 2048 bit. The usage of the ciphering functions happen by means of API that are PKCS#11 dedicated and of Microsoft Cryptographic API. These libraries allow you to use **dKey** with all the numerous PKI solutions, such as Verisign, Baltimore and Entrust.

Certified digital signature

Authentication

Encryption

The certified **digital signature** is the final result of a complex mathematical algorithm which enables you to sign a computerised document *with the same validity of an autographic signature*.

The digital signature guarantees:

- Authenticity
- Integrity of contents
- Non-ripudiability of the computerised document

The new device developed by SATA Hi-Tech Services is able to answer to all the most pressing needs for authentication both in private and in particular in public administration: the certified digital signature enables you to subscribe a statement, thus getting the guarantee of the **integrity** of the data that are the object of the subscription itself and the guarantee of the **authenticity** of information concerning the subscriber, as an autographic signature does.

In order to get the credentials of a digital signature it is necessary to apply to the **Certification Authorities** that are accredited to the CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione – which is the national authority that deals with computer matters in the public administration field). By these institutions you can verify the legal ownership of the signatory of an electronic document.

Technical features

Cryptographic algorithm: 2048 bit RSA hardware

Memory: EEPROM 32 Kbyte

Standard: ISO 7816 1-4, PC/SC. PKCS#11 ver 2.0.1

Microsoft CAPI, IPSED/IKE, S-Mime

Operative systems: Windows® 98, 2000, XP and Vista

It is also available with a flash memory from 512 Mb to 4 Gb (dKey Flash)

The hardware system of the key is based on Infineon SL66CX320P, ITSEC e4+ certified, and on a Siemens CardOS M 4.20 B operative system. The transferring speed of the data is 64 Kbps.

Requirements:

- Pentium II or higher
- Ram 64 MB
- USB Port