

dKey



Token Crittografico USB con firma digitale

dKey è un token crittografico creato da *SATA HTS* per eseguire funzioni di **sicurezza** e di **firma digitale certificata**. Il token è basato su un chip embedded certificato ITSEC E4+, appositamente sviluppato per la gestione delle chiavi RSA pubblica e privata.

Il token crittografato abbina le funzionalità di **smart card** a quelle del **lettore**, rendendo il suo uso facile e immediato su tutti i pc dotati di porta USB, sia con sistema operativo Windows che Linux.

dKey vi permette di usufruire di un'ampia gamma di servizi di sicurezza come la firma digitale certificata, l'autenticazione e la cifratura. Tali funzionalità soddisfano le esigenze di riservatezza, non ripudiabilità e privacy dei dati.

Il motore crittografico del token USB è costituito da un microprocessore in grado di elaborare l'algoritmo RSA fino a 2048 bit. L'uso delle funzioni di cifratura avviene per mezzo di API dedicate PKCS#11 e Microsoft Cryptographic API. Tali librerie consentono di utilizzare **dKey** con le numerose soluzioni PKI come Verisign, Baltimore ed Entrust.

Firma digitale certificata

Autenticazione

Cifratura

La **Firma Digitale** è il risultato finale di un complesso algoritmo matematico che permette di firmare un documento informatico *con la stessa validità di una firma autografa*.

La firma digitale permette di garantire:

- Autenticità
- Integrità dei contenuti
- Non ripudiabilità del documento informatico

La nuova periferica sviluppata da Sata Hi-Tech Services è in grado di rispondere alle più stringenti esigenze di autenticazione nei settori delle aziende private e soprattutto della pubblica amministrazione: la firma digitale certificata permette di sottoscrivere una dichiarazione ottenendo la garanzia di **integrità** dei dati oggetto della sottoscrizione stessa e la garanzia di **autenticità** delle informazioni relative al sottoscrittore, al pari della firma autografa.

Per ottenere le credenziali di firma digitale è necessario rivolgersi agli **Enti Certificatori** accreditati al **CNIPA** (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), presso i quali è possibile verificare la titolarità del firmatario di un documento elettronico.

La **dKey** è disponibile in versione *Driverless* (non necessita di alcuna installazione di driver sul pc in uso) o con memoria flash integrata (da 1 a 4 Gb).

Caratteristiche tecniche

Algoritmo crittografico: RSA hardware a 2048 bit
Memoria: EEPROM 32 Kbyte
Standard: ISO 7816 1-4, PC/SC. PKCS#11 ver 2.0.1,
Microsoft CAPI, IPSEC/IKE, S-Mime
Sistemi Operativi: Windows 98, 2000, XP, Vista

Disponibile anche con memoria flash da 1 Gb a 4 Gb (**iKey Flash**) e in versione **Driverless**

Il sistema hardware della chiave si basa sul chip Infineon SL66CX320P, certificato ITSEC E4+ e sistema operativo Siemens CardOS M 4.20 B. La velocità di trasferimento dati è di 64 Kbps.

Requisiti hardware:

- Pentium II o superiore
- Ram 64 MB
- Porta USB