



THE READERLESS SMART CARD

ITSEC E4 HIGH CERTIFIED

SIEMENS TECHNOLOGY INSIDE

**Cryptoldentity ITSEC-I** è un dispositivo "all-in-one", in formato chiave USB, che abbina la funzione di una Smart Card crittografica con quella del suo lettore.

Cryptoldentity ITSEC-I nasce per la memorizzazione sicura delle credenziali dell'utente (profili personali, certificati digitali X.509). La chiave privata utilizzata per la firma dei documenti informatici viene conservata in maniera sicura e segreta dal Titolare

che ne è responsabile, proteggendone l'accesso tramite un PIN personalizzabile: il possesso del dispositivo hardware Cryptoldentity ITSEC-I e la conoscenza del PIN sono i due elementi alla base del meccanismo di autenticazione "a due fattori".

Cryptoldentity ITSEC-I consente la generazione della coppia di chiavi di crittografia al suo interno e l'applicazione della firma digitale. Dispone di meccanismi di sicurezza che impediscono l'esportazione e la copia della chiave privata al di fuori del dispositivo in cui è stata generata.

La certificazione ITSEC E4 high del chip crittografico e del sistema operativo CardOS M4.01(a) installati a bordo di Cryptoldentity ITSEC, la rendono conforme alla normativa che regola la firma elettronica qualificata.



## Caratteristiche:

**Chiavi RSA:** generazione "on board" della coppia di chiavi RSA pubblica/privata con lunghezza fino a 1024 bit. La chiave privata non è mai esposta all'ambiente esterno e non può mai abbandonare il dispositivo. Tutte le operazioni che si avvalgono della chiave privata vengono eseguite sul token. La chiave pubblica può essere esportata in qualsiasi momento. E' consentita la memorizzazione multipla di chiavi, gestite da meccanismi di controllo d'accesso separati.

**Accesso utente:** il dispositivo è dotato di un PIN e un PUK alfanumerici per il controllo dell'accesso ai dati a bordo memorizzati. Nel caso di ripetuti tentativi di accesso non andati a buon fine, il PIN utente viene bloccato, rendendo il token inutilizzabile.

**Standard utilizzati:** il dispositivo supporta gli standard ISO 7816 3-4, PKCS#11 v2.11, PC/SC, Microsoft CAPI, S/MIME, IPSec/IKE e X.509 v3.

## Applicazioni supportate:

- Memorizzazione certificati digitali
- Firma digitale qualificata
- Posta sicura
- Crittografia file e dischi
- Microsoft XP e Windows 2000 Smart Card e Network Logon
- Strong Authentication: SSL3, VPN, Wireless, RAS Dialup/RADIUS
- Interoperabilità con soluzioni PKI
- Integrazione applicativa con PKCS#11 e MS CAPI

Algoritmi supportati: RSA fino a 1024 bit

Memoria: 32KB

Specifiche chip: chip della famiglia Infineon SLE66CX (SLE66CX322P) con sistema operativo CardOS M4.01(a), entrambi certificati ITSEC E4 high.

Portabilità: non necessita di lettori aggiuntivi, cavi o batterie di alimentazione, in quanto basta inserirla nella porta USB.

Opzioni: il dispositivo può essere fornito con un cappuccio che protegge il connettore USB.

Dimensioni ridotte: 62x17x7 mm

## **Requisiti di sistema:**

### Requisiti Hardware:

PC IBM o 100% compatibili, Desktop/Notebook/Sub-Notebook/Laptop con porta USB (Pentium 100 Mhz o migliore)

### Requisiti SO:

Windows 98/ME/NT4/2000/XP

### Requisiti applicativi:

Cryptoidentity ITSEC-I è in grado di interoperare, in particolare con Netscape Communicator Suite, Microsoft Internet Explorer, Microsoft Outlook, Lotus Notes 6.x, Acrobat 6 o superiori e tutti gli applicativi che usano gli standard supportati.

## **Specifiche tecniche:**

- USB Spec. 1.1 – USB 2.0 Low Speed
- LED: Luce Verde (alimentazione attiva/connesso)  
Luce Arancio o Rossa lampeggiante (accesso ai dati)
- Transfer rate: fino a 64 Kbps
- Alimentazione da bus USB (4.5V-5.5V)
- Certificazioni: UL/FCC/CE, water-, dust- and shockproof (IEC60529 IP67)



---

Per maggiori informazioni su Cryptoidentity visita:

[www.cryptoidentity.eutron.it](http://www.cryptoidentity.eutron.it)

---