



# sign'nCrypt II

La soluzione platform independent per la firma elettronica avanzata e la crittografia.



**sign'nCrypt II** è il sistema applicativo di digitaltrust ([www.digitaltrust.biz](http://www.digitaltrust.biz)) - Strategic Business Unit di ICE (Internet Centre of Excellence) - che permette di firmare e crittografare digitalmente documenti informatici confidenziali per essere poi trasmessi attraverso le reti pubbliche ed, in particolare, Internet.

Nato dall'esigenza di garantire l'impersonificazione, l'integrità e la confidenzialità delle informazioni trasmesse **sign'nCrypt II** è la soluzione avanzata per la firma digitale con valore legale (DPCM 8 Febbraio 1999, Testo Unico 445/2000, Deliberazione AIPA 24/98) che integra tutte le funzionalità dell'infrastruttura PKI in una applicazione potente e di semplice utilizzo.

- Firma digitale con valore legale
- Crittografia
- Marcatura temporale

Grazie ad un'interfaccia estremamente user friendly l'applicativo permette all'utente di firmare digitalmente e criptare un documento contemporaneamente a più destinatari con pochi semplici passaggi.

## // firma elettronica avanzata

La firma digitale è il risultato di una procedura informatica e crittografica basata su un sistema di chiavi asimmetriche a coppia, in grado di consentire ad ambo le parti (mandatario e destinatario) rispettivamente di rendere manifesta e verificare la **provenienza** e l'**integrità** di un documento informatico.

**sign'nCrypt II** supporta tutte le principali smart card contenenti certificati qualificati per apporre firme digitali con valore legale grazie alla potenza e alla versatilità di **sign'nCrypt II**, puoi:

- **firmare digitalmente** documenti garantendone l'autenticità, la provenienza e l'integrità, soddisfacendo le richieste formali e funzionali della normativa europea ed italiana.

## // headlines

- Platform independent
- AIPA compliant
- Supporto per tutte le principali smart card/token
- Firme multiple (CoSigning)
- Marcatura temporale
- Multiple Encryption
- Semplicità d'utilizzo
- Personalizzabile graficamente
- High encryption
- Certificate store interno
- Importazione certificati da Internet Explorer e Netscape
- LDAP search
- Interfacciamento PKCS#11
- Java™ based

## // interoperabile

Sistemi Operativi:

- Windows
- Linux
- Mac osX
- Win CE
- Cellulari con ambiente Java™

Smart-Card supportate:

- Eutron
- IPM
- Gemplus
- Siemens
- Etc ...

- firmare dichiarazioni dei redditi per essere poi inviati direttamente alla camera di commercio competente (se dotati di un certificato rilasciato da un certificatore accreditato AIPA)
- firmare **contratti digitali** con valenza legale

## // appliance edition

- shared version
- sistema signncrypt centralizzato
- Web-based (intranet/extranet)
- nessuna installazione a livello client
- scalabile

## // garanzia di

- integrità
- confidenzialità
- paternità

## // obiettivi

- Dotarsi di uno strumento efficace indipendente dal sistema operativo per l'apposizione delle firme digitali
- Fornire uno strumento per poter crittografare con facilità documenti sensibili

## // target

Tutte quelle aziende che:

- Utilizzano internamente ed esternamente la firma elettronica per la gestione documentale
- Gestiscono informazioni confidenziali
- Firmano digitalmente contratti elettronici

Tutte gli utenti che:

- Fanno uso della firma elettronica avanzata per sottoscrivere documenti
- Utilizzano internet e per la trasmissione di documenti confidenziali.

## // crittografia

Grazie alla crittografia a 1024/2048 bit è possibile trasmettere attraverso reti pubbliche tramite l'utilizzo dell'**email** documenti **riservati** e **confidenziali**, sicuri che solo i destinatari prescelti siano in grado di decifrare il contenuto inviato.

La crittografia garantisce la **confidenzialità** dei dati permettendo all'azienda di scambiare informazioni in sicurezza con dipendenti, partner, consulenti utilizzando internet in particolare:

- informazioni price sensitive trasmesse tra istituzioni finanziarie
- informazioni sensibili delle risorse umane gestite in outsourcing
- dati tecnici e di prodotti non ancora brevettati confidenziali.

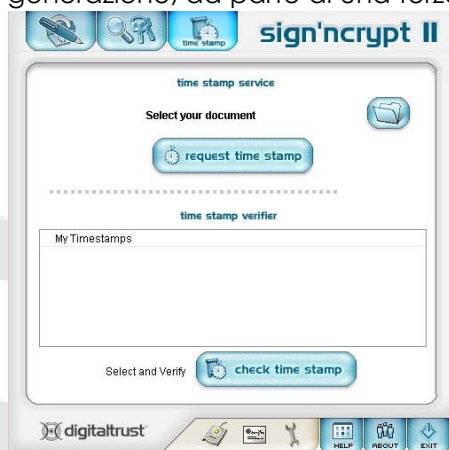
grazie alla funzionalità "multiple receiver" è possibile criptare il file per più destinatari in un unico passaggio.

Con **sign'ncrypt II** puoi :

- crittografare documenti riservati e spedirli via email con la certezza che solo i destinatari selezionati siano in grado di leggerli.
- crittografare file sul tuo PC con la garanzia che solo la tua smart card sarà in grado di decifrarli e riportarli al loro formato originale
- La soluzione ideale per società quotate che gestiscono informazioni price sensitive in formato elettronico.

## // marcatura temporale

La marcatura temporale di un documento informatico consiste nella generazione, da parte di una terza parte fidata, di una firma digitale del documento cui è associata l'informazione relativa ad una **data e ad un'ora certa**.



La marcatura temporale assume una notevole rilevanza consentendo di poter stabilire in modo assoluto il momento nel quale un documento è stato generato, trasmesso od archiviato e, quindi, il momento a partire dal quale, per esempio, un certo contratto spiega i propri effetti.

In sostanza la marcatura temporale consente di:

- datare in modo certo ed opponibile a terzi un documento;

- stabilire un riferimento temporale certo per il momento della sottoscrizione;
- estendere nel tempo la validità del documento.

## // facile

- In due click è possibile firmare un documento
- Interfaccia user friendly

## // sicuro

- conforme ai requisiti della legge italiana ed europea per la firma digitale con valore legale



## // interoperabile

- utilizzabile su qualsiasi sistema operativo
- supporta tutte le principali smartcard

## // caratteristiche tecniche

L'unico applicativo per la firma digitale Aipa compliant ad essere completamente platform independent utilizzabile su:

- Windows
- Linux
- Mac osX
- Win CE
- Cellulari con ambiente Java™



<b>Public Key Formats</b>	X.509
<b>Public Key Algorithms</b>	Diffie-Hellman, DSS, RSA
<b>Symmetric Key Algorithms</b>	TripleDES, AES, CAST, IDEA, Twofish, Blowfish
<b>Hashes</b>	SHA-1, MD5, RIPEMD-160
<b>Interoperability</b>	X.509 certificates, Certificate Authority integration, LDAP directory integration
<b>SmartCard / eToken</b>	Integrazione e gestione device hardware per lo storage dei certificate: Eutron cryptoidentity, Alladin eToken, Siemens card, Gemplus Gemsave, IPM, Java ibutton,...
<b>Update</b>	Live-update digitaltrust

### **digitaltrust**

è la divisione aziendale dedicata alla sicurezza informatica di:

Internet Centre of Excellence SpA  
Via Tazzoli, 6 Milano  
Tel: +39 02-29061262  
Fax: +39 02-6598897  
info@digitaltrust.biz

**security is not an option**