"InfoCamere"
Società Consortile di Informatica delle Camere di Commercio Italiane per azioni

# DIKE 3.1.1

| | |
|---|---|
| Funzione emittente | 70500<br>Area Sistemi Sicurezza Informatica |
| Redatto da | GM |
| Verificato da | GM |

# DIKE 3.1.0

Questa versione corregge alcuni errori della versione precedente, migliora la gestione della marche temporali e permette l'utilizzo delle future carte tipo CNS

## *Installazione*

Ci sono due possibilità. Se l'utente ha già installato una precedente versione (3.0.0 e succ.) di DiKe, può semplicemente scaricare e installare l'*aggiornamento*.
Per una installazione completa, disinstallare tutte le versioni precedenti. La nuova installazione non ricorda le impostazioni precedenti. Per questo gli utenti che utilizzano un proxy HTTP e/o LDAP devono riconfigurarli selezionando dal menu "Opzioni"/"Configurazione proxy…."

## *Smart Card rilasciate da InfoCamere*

Le caratteristiche delle Smart Card si possono vedere sul sito www.card.infocamere.it alla voce hardware.

## *Aggiornato il nuovo elenco certificatori*

Dike viene installato con l'ultima lista dei certificatori accreditati presso CNIPA (http://www.cnipa.gov.it/site/it-IT/). C'è comunque la funzione "Scarica Elenco Certificatori.." dal menu "Strumenti", che permette di scaricare sempre la lista aggiornata. L'ultima lista aggiornata risale al 23-09-2004.

## *Marche temporali*

In questa versione di DiKe sono state completate le funzionalità relative all'emissione e verifica di marche temporali.
Le funzionalità sono:

### emissione di una marca per un documento firmato (.p7m) e salvataggio in formato .m7m

Per questa funzione aprire un documento generico e selezionare dal menu *Modifica-Firma-Firma e Marca* (o l'icona corrispondente) oppure aprire un file firmato e selezionare dal menu *Modifica-Marca temporale..* (o l'icona corrispondente). In entrambi i casi subito dopo viene richiesto di selezionare la directory dove salvare il file .m7m

### emissione di una marca per un documento generico e salvataggio della marca in formato .tsr

In questo caso si salva la marca temporale separatamente dal documento per cui è stata richiesta (detached). Aprire un documento generico e selezionare dal menu *Modifica-Marca temporale..* (o l'icona corrispondente). Subito dopo viene richiesta la directory dove salvare il file .tsr

### associazione documento firmato (.p7m) e marca (.tsr) e salvataggio in formato .m7m

E' possibile creare un file mime di tipo .m7m i cui allegati sono il documento firmato (.p7m) e marca temporale (.tsr). Subito dopo l'associazione viene fatta una verifica della marca.
Dal menu *Strumenti-Associa marca e documento*

### separazione dal file .m7m della marca (.tsr) e del documento firmato (.p7m)

Con questa funzione si possono separare i due allegati del file mime (.m7m), marca e documento firmato. Dal menu *Strumenti-Separa marca da documento*

### verifica di un documento firmato e marcato (.m7m)

Per fare una verifica di un file .m7m: basta semplicemente aprire il documento. Nella lista dei file sono quelli contrassegnati con un orologio. Verranno verificate marca temporale e firme apposte al documento.

### verifica della marca (.tsr) contenuta in un file di tipo mime i cui allegati sono la marca stessa e il documento generico a cui è stata applicata

E' possibile verificare la marca temporale contenuta in un file mime (.eml, .mim ecc.) insieme al suo documento. Per farlo selezionare dalla lista il file in questione.

### verifica di una marca (.tsr) e del documento generico ad essa associato

Per verificare una marca di tipo detached (.tsr) selezionare *Strumenti-Verifica marca separata.* Verranno richiesti il documento e la marca.

## *Informazioni sulle firme e marche temporali*

Per aumentare il livello di interoperabilità tra i vari certificatori vengono fornite alcune informazioni in più dopo le verifiche della firma e della marca

### Signing time

Alcuni prodotti di firma inseriscono anche l'attributo SigningTime che indica la data e ora della firma. Purtroppo questo attributo non da nessuna indicazione della fonte da cui è stata presa l'informazione. Di solito viene indicata la data e ora del PC nel momento in cui avviene l'imbustamento del file firmato.

### Time Stamping Authority

Durante la verifica della marca temporale viene indicata anche la TSA emittente il certificato che ha firmato quella marca temporale.

## *Carta Nazionale dei Servizi*

Questa versione di DiKe è predisposta per riconoscere la carta nazionale dei servizi (Carta CNS). Questo tipo di SmartCard è protetta da due diversi PIN (e due PUK):

1. Il ***PIN di carta*** che sblocca la SmartCard e permette l'utilizzo del certificato CNS.
2. Il ***PIN di firma*** che permette l'utilizzo delle chiavi di firma digitale.

**La lunghezza dei PIN e PUK è di 8 caratteri numerici**

Le conseguenze derivanti da questa caratteristica sono:

- Per *sottoscrivere un documento* vengono richiesti due PIN;
- Il *cambio PIN* permette di modificare entrambi i PIN oppure uno solo dei due;
- La *verifica della SmartCard* richiede il solo *PIN di carta*.

### Primo utilizzo della Firma Digitale

- Per poter apporre una Firma Digitale con la carta CNS è necessario effettuare, solo per la prima volta, una procedura di attivazione del PIN di firma. I passi da seguire con DiKe sono i seguenti:
    1) richiamare la funzione *Strumenti-Cambio PIN...;*
    2) inserire il **PUK di firma** (rilasciato con la SmartCard);
    3) inserire il **PIN di firma** (rilasciato con la SmartCard).

## DIKE 3.1.1

In questa versione sono state corrette alcune malfunzioni legate alla verifca delle marche temporali. **Ricordiamo che le marche temporali sono a pagamento**. E' possibile acquistarle anche attraverso il sito all'indirizzo www.card.infocamere.it/servizi/marcatura.htm.
Si può verificare la quantità di marche temporali non ancora utilizzate attraverso il menu *Strumenti - Disponibilità marche tmporali*

Questa versione di Dike contiene l'ultima lista aggiornata dei certficatori che risale al 03-12-2004.

E' stata aggiornata una libreria per permettere un migliore utilizzo con carte CNS.

Insieme a questa versione viene rilasciata un utility per lo sblocco delle carte CNS. Dopo l'installazione di Dike apparirà sul desktop un'icona relativa all'utility "icCNS".

## icCNS

Questa utility permette le operazioni di sblocco del PIN, cambio del PUK e la prima attivazione del PIN di firma relativamente alle Smart Card CNS; tutte le funzioni sono presenti nella voce di menù 'Utility'."

**La lunghezza dei PIN e PUK della carta CNS è di 8 caratteri numerici**

### Sblocco Pin:

Questa funzione permette di sbloccare entrambi i PIN di una Smart Card CNS: il PIN di firma forte e il PIN CNS. E' possibile sbloccare, con una sola operazione, entrambi i PIN o soltanto uno dei due. La finestra video è suddivisa in due sezioni, una relativa al PIN CNS e un'altra al PIN di firma forte, e richiede la digitazione del PUK e del nuovo PIN che si vuole impostare sulla Smart Card; sia il PUK che il PIN devono essere composti da 8 caratteri numerici.

### Cambio PUK:

Questa funzione permette di cambiare entrambi i PUK di una Smart Card CNS: il PUK di firma forte e il PUK CNS. E' possibile cambiare, con una sola operazione, entrambi i PUK o soltanto uno dei due. La finestra video è suddivisa in due sezioni, una relativa al PUK CNS e un'altra al PUK di firma forte, e richiede la digitazione del PUK attuale e del nuovo PUK che si vuole impostare sulla Smart Card; il PUK deve essere composti da 8 caratteri numerici.

### Attivazione PIN:

Questa funzione permette di attivare il PIN di firma forte di una Smart Card CNS. La finestra video richiede la digitazione del PUK e del PIN da attivare; sia il PUK che il PIN devono essere composti da 8 caratteri numerici. La stessa funzione è presente in DiKe, solo se la Smart Card non è mai stata usata.