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

Ente Certificatore InfoCamere

Dike

Manuale Utente

Codice documento: Dike-MU

Redatto da **Area Sistemi Sicurezza Informatica**

Nome file: manuale dikeV4.sxw

1 Introduzione al documento

Dike è il software necessario alla gestione dell'ambiente locale di firma digitale, e consente di apporre e/o verificare una o più firme su qualunque tipo di file, nonché di marcarlo temporalmente.

I documenti da firmare vengono visualizzati, se ad essi è associata un'applicazione.

Ogni documento, una volta firmato, assumerà l'ulteriore estensione P7M, in conformità alle regole CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) in materia di firma digitale. Un documento firmato non può più essere modificato dal software usato per crearlo. In ogni caso, qualora si riesca ad alterare il file con qualunque strumento, per i princìpi della crittografia asimmetrica non ci potrà più essere corrispondenza tra contenuto del documento e firme associate, e Dike segnalerà l'esito negativo dell'operazione di verifica.

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	1.0	**Data Versione/Release** :	30/11/2004
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione		

Versione/Release n° :	2.0	**Data Versione/Release** :	30/06/2005
Descrizione modifiche:	Aggiornamento del manuale alla versione 3.2.0 del prodotto		
Motivazioni :			

Versione/Release n° :	3.0	**Data Versione/Release** :	14/03/2006
Descrizione modifiche:	Aggiornamento del manuale alla versione 3.3.0 del prodotto in occasione dell'adeguamento del formato dei certificati alla delibera cnipa 4/2005 – Qualche modifica interfaccia utente		
Motivazioni :	Delibera CNIPA 4/2005		

Versione/Release n° :	4.0	**Data Versione/Release** :	22/08/2006
Descrizione modifiche:	Aggiornamento riferimenti al sito internet.		
Motivazioni :	Nuovo sito internet.		

1.2 Accedere agli help del programma

Per visualizzare le note di aiuto lanciare la relativa funzionalità (menu *Guida – Come fare per…* oppure clic sull'icona corrispondente).

Per visualizzare alcune informazioni generiche relative al programma lanciare la relativa funzionalità (menu *Guida – Informazioni su…* oppure clic sull'icona corrispondente).

2 Configurazione del prodotto

In questa sezione sono descritte le operazioni preliminari per un corretto e proficuo uso del prodotto:

1. configurazione dell'accesso alle liste di revoca;
2. impostazione dei parametri di rete per l'accesso ad Internet;
3. selezione del lettore di smart card;
4. selezione automatica o meno del certificato di firma da utilizzare;
5. selezione dell'archivio delle CA “trusted”;
6. opzioni di visualizzazione.

2.1 Configurazione dell'accesso alle liste di revoca

2.1.1 Controllo liste di revoca

Menù *Opzioni -- Controlla lista di revoca*
Se questa opzione è attivata (simbolo ✓), la verifica di firma comprende anche il controllo dell'assenza del certificato del firmatario nella lista di revoca.

2.1.2 Scarica lista di revoca

Menù *Opzioni – Scarica lista di revoca*
Se è stata attivata l'opzione *Controlla lista di revoca*, la lista di revoca viene aggiornata automaticamente alla scadenza. E' possibile richiedere l'aggiornamento per ogni verifica (opzione sconsigliata).

2.2 Configurazione parametri di rete

2.2.1 Configurazione Proxy HTTP

Menù *Opzioni – Configurazione Proxy HTTP...*

Questa funzionalità deve essere utilizzata solo se l'accesso ad Internet per il protocollo HTTP è effettuato tramite un server proxy.

Il sistema permette di impostare il nome del server proxy, la porta cui è collegato, l'identificativo e la password di accesso ad Internet dell'utente di Dike.

2.2.2 Configurazione Proxy LDAP

Menù *Opzioni – Configurazione Proxy LDAP...*

Questa funzionalità deve essere utilizzata solo se l'accesso ad Internet per il protocollo LDAP è effettuato tramite un server proxy SOCKS v5.

Il sistema permette di impostare il nome del server proxy, la porta cui è collegato, l'identificativo e la password di accesso ad Internet dell'utente di Dike.

2.3 Lettore di smart card

Menù *Opzioni – Lettore utente...*

Questa funzionalità permette di impostare il lettore della smart card da utilizzare per le operazioni di firma.

Dopo la modifica del lettore il programma Dike viene chiuso e la modifica diventerà attiva al successivo riavvio.

ATTENZIONE: nel caso sia installato più di un lettore, al primo avvio del programma dopo l'installazione viene richiesta obbligatoriamente la scelta del Lettore Utente da utilizzare.

Se non è stato installato alcun lettore comparirà il messaggio: "Attenzione: nessun lettore è stato installato; non sarà possibile effettuare operazioni di firma"; in questo caso sarà possibile utilizzare Dike solo per le operazioni di visualizzazione dei documenti e verifica delle firme.

2.4 Selezione certificato di firma

Menù *Opzioni – Selezione certificato di firma*
Se questa opzione è selezionata (simbolo ✓), prima della firma viene richiesto di selezionare il certificato presente sulla smart card con il quale firmare, altrimenti viene utilizzato quello di sottoscrizione.

2.5 Controllo parametri in rete

Menù *Opzioni – Controllo parametri in rete*
Se questa opzione è selezionata (simbolo ✓), Dike accede ad Internet per aggiornare i parametri di configurazione.

2.6 Scelta directory archivi CA ...

Menù *Opzioni – Scelta directory archivi CA ...*
Durante la verifica di un file firmato, si verifica anche che la CA che ha emesso il certificato sia tra quelle accreditate presso il CNIPA. I certificati di queste CA sono presenti in un archivio e all'interno di questo archivio viene ricercata la CA.
Utilizzando questa opzione è possibile sostituire l'archivio delle CA accreditate presso CNIPA con un archivio personalizzato, in modo da considerare attendibili anche queste.

ATTENZIONE
L'opzione è rivolta agli utenti più esperti.

2.7 Opzioni di visualizzazione

Menù *Opzioni – Icone grandi*
Se questa opzione è spuntata le icone presenti sulla barra delle icone e quelle della maschera della selezione file vengono mostrate di dimensioni maggiori.

3 La gestione della Smart Card

3.1 Effettuare il controllo di una smart card

Per verificare se una smart card è tra quelle riconosciute dal sistema, dopo averla inserita nel lettore, scegliere la funzione relativa (menù *Strumenti – Verifica smart card* oppure clic sull'icona corrispondente).

Se l'operazione va a buon fine, comparirà la maschera con il messaggio di conferma.

Dopo l'operazione di verifica della smart card viene eseguito il controllo del PIN; è possibile evitare quest'operazione premendo il tasto *Annulla*.

Se il PIN digitato è corretto comparirà la maschera con il messaggio di conferma.

AVVERTENZA

LIMITE AL NUMERO DI VOLTE CHE IL PIN PUÒ ESSERE INSERITO IN MANIERA ERRATA

La carta è protetta da tentativi multipli di accesso casuale. Se si digita il PIN in modo errato per un determinato numero di volte consecutive, la smart card viene bloccata e diventa inutilizzabile; il numero di tentativi permesso prima del blocco dipende dal tipo di smart card utilizzata:

- se la smart card è del tipo SysGillo Cryptosmart cardE16 (numero di serie che comincia con 1201) il numero di tentativi permesso è 7; su questo tipo di smart card non è possibile usare la funzione di sblocco smart card
- se la smart card è del tipo SysGillo Cryptosmart cardE4H (numero di serie che comincia con 1202) il numero di tentativi permesso è 3. Se il PIN è bloccato si può procedere allo sblocco utilizzando il PUK (personal unblock key) .
- se la smart card è del tipo Sysgillo CardOS M4.01 (numero di serie che comincia con 1203) il numero di tentativi permesso è 3. Se il PIN è bloccato si può procedere allo sblocco utilizzando il PUK (personal unblock key) .
- se la smart card è del tipo Siemens CardOS M4.01 (numero di serie che comincia con 1401) il numero di tentativi permesso è 3. Se il PIN è bloccato si può procedere allo sblocco utilizzando il PUK (personal unblock key) .
- se la smart card è del tipo Ghirlanda M4cvToken (numero di serie che comincia con 1601) il numero di tentativi permesso è 3. Se il PIN è bloccato si può procedere allo sblocco utilizzando il PUK (personal unblock key) .
- se la smart card è del tipo InCrypto34 V2 (numero di serie che comincia con 7420,1204 o 6090), carta CNS, il numero di tentativi permesso è 3. Se il PIN è bloccato si può procedere allo sblocco utilizzando il PUK (personal unblock key).

Per informazioni sull'operazione di sblocco e per informazioni su nuovi modelli di smart card oltre a quelli descritti sopra, visitare il sito Internet www.card.infocamere.it.

3.2 Cambiare il PIN di una smart card

Per modificare il PIN (Personal Identification Number) di una smart card, dopo averla inserita nel lettore, scegliere la funzione relativa (menù *Strumenti – Cambio PIN* oppure clic sull'icona corrispondente).

Digitare, in successione nei tre campi, il PIN corrente da modificare e due volte quello nuovo (inserimento e verifica). Il PIN deve essere numerico; la sua lunghezza può variare all'interno di un intervallo dipendente dal tipo di smart card:

- smart card Sysgillo CryptoSmartcard16 (numero di serie che comincia con 1201) il pin è da 5 a 8 numeri;
- smart card Sysgillo CryptoSmartcardE4H (numero di serie che comincia con 1202) il pin è da 6 a 8 numeri. Questa carta viene rilasciata con attivato un PIN di trasporto di 5 cifre. Prima di essere utilizzata si deve procedere ad un cambio PIN;
- smart card Sysgillo CardOS M4.01 (numero di serie che comincia con 1203) il pin è da 5 a 8 numeri;
- smart card Siemens CardOs M4.01 (numero di serie che comincia con 1401) il pin è da 5 a 8 numeri;
- smart card Ghirlanda M4cvToken (numero di serie che comincia con 1601) il pin è da 5 a 8 numeri;

Per le carte CNS si veda il paragrafo relativo.

ATTENZIONE

Se il PIN viene inserito in maniera errata più volte la smart card si blocca. Si veda l'avvertenza nel paragrafo precedente.

3.3 Cambiare il PIN di una smart card di tipo CNS

Questo tipo di smart card è protetta da due diversi PIN (e due PUK):

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

Il cambio PIN prevede di cambiare uno alla volta entrambi i PIN. Se i due PIN sono uguali si può utilizzare questo tipo di smart card come se ne avesse uno solo. In questo caso si deve impostare l'opzione un solo PIN attraverso *(Opzioni – Digitazione PIN CNS – un PIN).*

IMPORTANTE

Questa opzione va scelta solo se i due PIN sono coincidenti.

3.4 Digitazione PIN CNS

Se la smart card è del tipo InCrypto34 V2 (numero di serie che comincia con 7420, 1204 o 6090), la carta (CNS o CNS-like) è protetta da due diversi PIN (e due PUK):

3. Il ***PIN di carta*** che sblocca la smart card.
4. Il ***PIN di firma*** che permette di firmare un documento.

La firma richiede due PIN. La prima volta per sbloccare la carta la seconda per sbloccare la firma digitale.Se i due PIN sono uguali si può utilizzare questo tipo di smart card come se ne avesse uno solo. In questo caso si deve impostare l'opzione un solo PIN.

IMPORTANTE

Questa opzione va scelta solo se i due PIN sono coincidenti.

3.5 Lista dei certificati

Questa funzione permette di visualizzare TUTTI i certificati presenti sulla smart card.

Per accedere, selezionare dal menu *Strumenti* la voce: *Lista certificati su smart card....*

I certificati di sottoscrizione emessi da CA accreditate presso CNIPA sono evidenziati con una coccarda. Cliccando sul certificato è possibile esaminarne il contenuto attraverso il visualizzatore di Windows.

3.6 Verificare lo spazio libero sulla smart card

Per verificare lo spazio libero sulla smart card scegliere la funzione relativa (menù *Strumenti – Verifica spazio su smart card)* ad esempio prima del rinnovo.

La maschera video presenta due pulsanti: '**Certificato di autenticazione**' e '**Certificato di sottoscrizione**'. Premendo uno dei due tasti il sistema, dopo aver richiesto la password della smart card, verifica se sulla smart card è presente spazio sufficiente al rinnovo del certificato indicato dal pulsante.

Questa funzionalità non è disponibile per alcuni modelli di smart card, anche se è possibile comunque procedere al rinnovo.

4 Le funzionalità di base

4.1 Verificare le firme apposte ad un documento

Si sceglie il file che si intende verificare (menù *File – Apri* oppure clic sull'icona corrispondente).

I file ai quali sono già associate una o più firme digitali sono contrassegnati da un'icona raffigurante una chiave.

E' possibile visualizzare il documento contenuto nel file firmato tramite la pressione del pulsante *'visualizza documento...'*.

La visualizzazione viene effettuata dal programma associato all'estensione del file.

Se è impostata l'opzione corrispondente (menù *Opzioni – Controllo lista revoca*), verrà anche effettuato il controllo di validità attuale della firma, esaminando la lista di revoca. In caso contrario, la verifica di firma è parziale perché non viene considerata la possibilità che il certificato sia stato revocato o sospeso.

Per poter controllare le liste di revoca è necessario avere un collegamento internet aperto al protocollo LDAP e HTTP.

Se la stazione si collega ad internet tramite PROXY, impostare i valori (menu *Opzioni – Configurazione Proxy HTTP* ... e *Opzioni – Configurazione Proxy LDAP* ..)

All'apertura del file, nella finestra immediatamente sovrastante appaiono automaticamente gli estremi dei titolari delle firme digitali apposte sul documento. Per ingrandirla usare l'icona con la lente presente sulla barra delle icone.

Nel caso in cui i firmatari successivi al primo abbiano firmato l'intera busta prodotta dal firmatario precedente (la cosiddetta 'firma nidificata'), viene segnalato in colore rosso:

"Documento contenente firme nidificate"

e gli estremi delle verifiche vengono visualizzati in modo da rendere evidente il livello di nidificazione: la verifica della firma più esterna è seguita dalla verifica delle firme più interne spostate verso destra.

Nel caso in cui un firmatario abbia controfirmato la firma prodotta da un altro firmatario del documento stesso (la cosiddetta 'controfirma'), gli estremi delle verifica della controfirma vengono visualizzati spostati verso destra, in modo da rendere evidente il livello di nidificazione; viene inoltre riportata la dicitura *'Controfirma della firma di:'* seguita dal Common Name del firmatario che ha effettuato la firma che è stata controfirmata.

4.2 Verificare le firme apposte ad un documento e la marca temporale

I file contenenti insieme il documento firmato e la marca prodotti tramite Dike hanno l'estensione '.m7m' e sono contrassegnati da un'icona raffigurante un orologio. Questi file sono in formato MIME.

Dopo aver selezionato il file marcato che si intende verificare (menù *File – Apri* oppure clic sull'icona corrispondente) apparirà l'esito della verifica della marca temporale, seguita dall'esito della verifica delle firme apposte al documento.

4.3 Verificare un file marca temporale

I file di marca temporale hanno estensione '.tsr' e sono contrassegnati da un'icona raffigurante un orologio.

Per far la verifica della marca temporale il programma richiede anche il documento sul quale è stata applicata

Selezionare dal menu:

Strumenti – Verifica marca separata

la maschera visualizzata richiede di specificare due file:

– il file contenente la marca temporale, che deve essere del tipo ".tsr" (TimeStampResponse: vedi rfc 3161)

– il file contenente il documento relativo alla marcatura temporale specificata.

Al termine dell'operazione viene visualizzato l'esito della verifica.

4.4 Visualizzare un documento

Il file selezionato per la firma o la verifica, non viene visualizzato subito; per farlo si deve cliccare sul bottone *'visualizza documento...'*.

La visualizzazione viene effettuata aprendo il programma associato all'estensione del file, analogamente a come si comporta il sistema operativo Windows all'evento '*doppio click*' su di un file.

Se ad esempio il file è 'prova.pdf' e all'estensione 'pdf' è associato il programma 'Adobe Reader 7.0', viene lanciata l'esecuzione del programma 'Adobe Reader 7.0' che effettua l'apertura e visualizzazione del file.

E' possibile cambiare l'associazione tra l'estensione e il programma da lanciare usando la procedura standard predisposta dal sistema operativo Windows:

- lanciare il programma 'Esplora risorse' dal menu di Windows
- selezionare la voce di menu 'Strumenti', 'Opzioni cartella', 'Tipi di file'
- individuare l'estensione che si vuole modificare selezionandola con un 'click' del mouse
- premere il pulsante 'cambia...' e selezionare il programma che si vuole associare all'estensione.

Da questo momento sia Dike che il sistema operativo Windows utilizzeranno il programma scelto per gestire (visualizzare, modificare, stampare, ecc...) tutti i file che presentano l'estensione in esame.

Se si vuole ripristinare l'associazione estensione-programma precedente alla modifica effettuata:

- lanciare il programma 'Esplora risorse' dal menu di Windows
- selezionare la voce di menu 'Strumenti', 'Opzioni cartella', 'Tipi di file'
- individuare l'estensione che si vuole modificare selezionandola con un 'click' del mouse
- premere il pulsante 'ripristina'.

Se non ci si limita alla visualizzazione ma si eseguono delle modifiche al documento, è necessario salvarle prima di eseguire la firma del file; in caso contrario il file che verrà firmato sarà quello memorizzato sull'hard disk e quindi privo delle modifiche apportate.

4.5 Salvare un documento escludendone le firme

Questa funzionalità consente di salvare il file originale senza le eventuali firme digitali associate. Selezionare il documento da verificare e una volta effettuata le verifica dal menù *File – Salva origine* oppure clic sull'icona corrispondente; selezionare successivamente la directory di destinazione del file. Dike non consente di modificare il nome originario del file.

Se il file è un '.m7m' si deve prima dissociare la marca al documento (menù *Strumenti – Separa marca da documento...*).

4.6 Selezionare un documento per firmarlo

Bisogna dapprima scegliere il file che si intende firmare (menù *File – Apri* oppure clic sull'icona corrispondente), selezionandolo dalla lista composta in base al formato impostato (*.*, doc, pdf, tif, rtf, etc.).

I file ai quali sono già associate una o più firme digitali sono contrassegnati da un'icona raffigurante una chiave.

E' possibile visualizzare il documento contenuto nel file scelto tramite la pressione del pulsante *'visualizza documento...'*.

La visualizzazione viene effettuata dal programma associato all'estensione del file.

Se non ci si limita alla visualizzazione ma si eseguono delle modifiche al documento, è necessario salvarle prima di eseguire la firma del file; in caso contrario il file che verrà firmato sarà quello memorizzato sull'hard disk e quindi privo delle modifiche apportate.

Una volta selezionato il file si può:

- firmare il file (menù *Modifica – Firma...* oppure clic sull'icona corrispondente);
- firmare il file e richiedere una marca temporale per il file firmato (menù *Modifica –Firma e Marca..*)
- richiedere una marca temporale (menù *Modifica – Marca...*)
- controfirmare la firma di un firmatario (menù *Modifica – Controfirma...* oppure clic sull'icona corrispondente); Tramite questa funzione (attiva solo se il file presenta già almeno una firma) è possibile controfirmare la firma di un firmatario del documento stesso.
  Il sistema visualizza una finestra con l'elenco dei firmatari del file, permettendo la scelta del firmatario di cui si vuole controfirmare la firma.

Se è la prima firma associata al documento, viene richiesta anche la directory in cui salvare il file firmato.

Il sistema controlla che la smart card sia inserita nel lettore, quindi viene richiesta la digitazione del PIN (Personal Identification Number)

Se l'utente digita il PIN in modo errato per un determinato numero di volte consecutive, la smart card viene bloccata permanentemente e diventa inutilizzabile (vd. Paragrafo relativo).

Una volta digitato il PIN segreto il sistema effettua la lettura dei certificati presenti sulla smart card e ne visualizza l'elenco in una maschera, permettendo così all'utente di scegliere il certificato con cui firmare. Il certificato evidenziato con la coccarda indica che è un certificato di sottoscrizione emesso da una CA di firma accreditata presso CNIPA

Se si desidera che il sistema scelga automaticamente il certificato di sottoscrizione senza visualizzare l'elenco bisogna deselezionare la voce di menù *Opzioni – Selezione del certificato di firma* . Se nella smart card sono presenti più di un certificato di sottoscrizione l'utente deve comunque scegliere.

Se l'operazione di firma va a buon fine, comparirà la maschera di conferma con gli estremi del nuovo firmatario.

ATTENZIONE

I documenti elettronici possono contenere elementi dinamici; data la variabilità di tali elementi, visualizzazioni successive del documento potrebbero differire dal documento originariamente creato.

4.7 Firmare con una carta CNS

Questo tipo di smart card è protetta da due diversi PIN (e due PUK):

5. Il ***PIN di carta*** che sblocca la smart card.
6. Il ***PIN di firma*** che permette di firmare un documento.

La firma richiede due PIN. La prima volta per sbloccare la carta la seconda per sbloccare la firma digitale.

Se i due PIN sono uguali si può utilizzare questo tipo di smart card come se ne avesse uno solo. In questo caso si deve impostare l'opzione "un solo PIN" attraverso *(Opzioni – Digitazione PIN CNS – un PIN).*

IMPORTANTE

Questa opzione va scelta solo se i due PIN sono coincidenti.

4.8 Marcare temporalmente un documento

Con questa operazione si applicano ad un documento firmato una data e un'ora certe e immodificabili (validazione temporale).

Per effettuarla, è indispensabile il collegamento Internet attivo.

Scegliere il file che si intende marcare (menù *File – Apri* oppure clic sull'icona corrispondente), selezionandolo dalla lista composta in base al formato impostato (*.*, doc, pdf, tif, rtf, etc.). Può essere marcato qualunque tipo di file:

- Se il documento è firmato viene prodotto un file mime con estensione '.m7m'. Questo file contiene due allegati (marca e documento)
- Se il documento non è firmato viene prodotto un file con estensione '.tsr ' contenente solo la marca temporale

Una volta selezionato il file, si passa alla funzione di marcatura (menù *Modifica – Marca* oppure clic sull'icona corrispondente): verrà chiesta la userid (corrispondente al codice cliente per il quale verrà conteggiata la marca emessa) e la password; subito dopo verrà quindi richiesta la directory in cui salvare il file marcato.

Se l'operazione va a buon fine, comparirà la maschera di conferma con gli estremi della marca temporale.

E' possibile eseguire contemporaneamente la funzione di firma e marcatura (menù *Modifica – Firma* e *Marca..)*

4.9 Associare una marca temporale a un documento firmato

Questa funzionalità permette di accorpare in un file di tipo '.m7m' un file firmato con la sua marca temporale.

L'estensione '.m7m' indica un file in formato mime con due allegati: la marca temporale in formato '.tsr' e il documento formato in formato '.p7m'.

Selezionare dal menù:

Strumenti – Associa marca a documento

la maschera visualizzata richiede di specificare due file:

- il file contenente la marca temporale, che deve essere del tipo ".tsr"
- il file firmato del tipo ".p7m" relativo alla marcatura temporale specificata.

Al termine dell'operazione è effettuata automaticamente la verifica del file '.m7m' creato e ne viene visualizzato l'esito.

4.10 Separare la marca temporale e il documento firmato da un documento '.m7m'

Questa funzionalità permette di separare, da un file di tipo '.m7m'., la marca temporale e il documento firmato che lo compongono.

Selezionare dal menù:

Strumenti – Separa marca da documento

la maschera visualizzata richiede di specificare il file del tipo ".m7m" di cui si vuole eseguire la separazione.

Al termine dell'operazione vengono creati due file:

- un file di tipo 'tsr' contenente la marcatura temporale
- un file di tipo 'p7m' contenente il file firmato.

4.11 Stampare l'esito della verifica

Con il file verificato, questa funzionalità (menù *File – Stampa esito* oppure clic sull'icona corrispondente) permette di stampare gli estremi delle marche temporali e/o delle firme digitali associate al documento verificato

5 Altre funzionalità

5.1 Controllare se la versione di Dike è aggiornata

Con questa funzionalità (menù *Strumenti – Controlla versione*) si accede automaticamente al sito Internet dell'Ente Certificatore, per verificare che la versione di Dike in uso sia l'ultima rilasciata.

Se l'esito è negativo, bisognerà effettuare un aggiornamento, rimuovendo la versione obsoleta, quindi scaricando e installando l'ultima versione.

5.2 Disponibilità marche temporali

Per verificare il numero di marche disponibili selezionare *Strumenti – Disponibilità marche temporali*. Digitare user e password che sono state assegnate quando sono state acquistate.

5.3 Aggiornare l'elenco dei certificatori

Questa funzionalità (menù *Strumenti – Scarica l'elenco dei certificatori*) permette di scaricare sul computer l'elenco pubblico dei certificatori accreditati dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

Lo scarico del file è necessario ogni volta che il CNIPA riconosce ufficialmente un nuovo Ente Certificatore e lo aggiunge all'elenco pubblico dei certificatori accreditati.

N.B.: Il programma Dike utilizza l'elenco dei certificatori all'atto della verifica di un file firmato: se il file non è stato firmato con un certificato emesso da uno dei certificatori presenti nell'elenco, Dike segnala l'errore tramite un appropriato messaggio.

5.4 Uscire dal programma

Dalla maschera iniziale scegliere la funzione relativa (menù *File – Esci* oppure clic sul bottone del menù di controllo nell'angolo in alto a destra della maschera).

5.5 Utilizzo di Dike da linea comando

E' possibile lanciare Dike da linea comando utilizzando dei parametri per specificare le azioni, di seguito le indicazioni

Il programma si avvia e apre il file specificato dal parametro

1° parametro = il nome del file da aprire

ESEMPIO: c:\programmi\infocamere\dike\dike.exe c:\dike\example\a.txt

Il programma si avvia e apre il file specificato, quando si chiude il file si chiude anche il programma

1° parametro = il nome del file da aprire

2° parametro = stringa "CLOSE"

ESEMPIO: c:\programmi\infocamere\dike\dike.exe c:\dike\example\a.txt CLOSE

Il programma si avvia e apre il file specificato richiede subito il PIN per firmarlo;

al termine della firma (o alla chiusura della maschera) il programma si chiude automaticamente

1° parametro = il nome del file da firmare

2° parametro = la directory che conterrà il file firmato

3° parametro = il path completo del file di log che conterrà l'esito della firma

ESEMPIO: c:\programmi\infocamere\dike\dike.exe c:\dike\example\a.txt c:\tmp c:\tmp\logfile.txt

Il programma si avvia e apre il file specificato senza compiere nessun'altra azione; alla chiusura della maschera (o alla fine della firma se l'utente la esegue) il programma si chiude automaticamente

1° parametro = il nome del file da firmare

2° parametro = la directory che conterrà il file firmato

3° parametro = il path completo del file di log che conterrà l'esito della firma

4° parametro = stringa "NOPIN"

ESEMPIO: c:\programmi\infocamere\dike\dike.exe c:\dike\example\a.txt c:\tmp c:\tmp\logfile.txt NOPIN

Il programma si avvia e marca il file specificato; alla chiusura della maschera il programma si chiude automaticamente

1° parametro = il nome del file p7m da marcare

2° parametro = la directory che conterrà il file marcato

3° parametro = il path completo del file di log che conterrà l'esito della marca

4° parametro = stringa "MARCA"

ESEMPIO: c:\programmi\infocamere\dike\dike.exe c:\dike\example\a.txt.p7m c:\tmp c:\tmp\logfile.txt MARCA

6 Esempio: firmare un documento

1. Assicurarsi che la propria smart card sia inserita nel lettore
2. Lanciare Dike cliccando sulla relativa icona nel desktop
3. Attivare il menu File-Apri (oppure cliccare sulla relativa icona)
4. Selezionare il file che si intende firmare
5. Se si vuole identificare il documento con certezza, visualizzarlo
6. Attivare il menù Modifica-Firma (oppure cliccare sulla relativa icona)
7. Individuare la destinazione del file firmato, scegliendo Unità e Directory
8. Alla richiesta, digitare il PIN della propria smart card
9. Se viene visualizzata la lista dei certificati presenti nella smart card: individuare il certificato con cui si intende firmare scegliendolo tramite un click
10. Attendere la conclusione dell'operazione di firma
11. Confermare con OK le finestre che mostrano esito ed estremi del firmatario
12. Riprendere dal punto 4. per firmare un altro file o per aggiungere un'altra firma ad un file già firmato, oppure chiudere la lista dei file e uscire da Dike