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

Ente Certificatore InfoCamere

Dike

Manuale Utente

Codice documento: Dike-MU

Nome file: Manuale Dike.sxw

1 Introduzione al documento 3
1.1 Novità introdotte rispetto alla precedente emissione 3
2 Dike - Programma di Firma e Verifica 4
2.1 Accedere agli help del programma 4
2.2 Aprire un documento per firmare 4
2.3 Aprire un documento per verificare la marca temporale 4
2.4 Aprire un documento per verificare le firme 4
2.5 Associare una marca temporale a un documento firmato 5
2.6 Cambiare il PIN di una smart card 5
2.7 Comportamento di Dike con carte rilasciate da altri certificatori 6
2.8 Controllare se la versione di Dike è aggiornata 6
2.9 Effettuare il controllo di una smart card 6
2.10 Esempio: firmare un documento 6
2.11 Impostare i parametri del proxy HTTP 7
2.12 Impostare i parametri del proxy LDAP 7
2.13 Impostare il lettore utente 7
2.14 Marcare temporalmente un documento 7
2.15 Salvare un documento escludendone le firme 8
2.16 Scaricare l'elenco dei certificatori 8
2.17 Separare la marca temporale e il documento firmato da un documento marcato 8
2.18 Stampare la lista dei firmatari 8
2.19 Stampare un documento 8
2.20 Uscire dal programma 8
2.21 Verificare lo spazio libero sulla smart card 8
2.22 Visualizzazione dei certificati 9

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.

In particolare, i files con estensione DOC, XLS, PDF, TIF, RTF, TXT, HTM, XML, JPG sono visualizzati da Dike al momento dell'apertura (finalizzata appunto all'apposizione/verifica di firme); ne viene inoltre consentita la stampa.

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 (ad es. Microsoft WordPad) usato per crearlo. In ogni caso, qualora si riesca ad alterare il file con qualunque altro 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		

2 Dike - Programma di Firma e Verifica

2.1 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).

2.2 Aprire un documento per firmare

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

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

Una volta aperto (e visualizzato nei casi previsti) il file, si passa alla funzione di firma (menu *Modifica Firma– Firma e salva* oppure clic sull'icona corrispondente); è disponibile anche la funzione di firma e marcatura temporale (menu *Modifica –Firma - Firma e marca temporalmente*): questa funzione dopo l'operazione di firma effettua anche la marcatura temporale del documento.

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 segreto (Personal Identification Number) di sblocco.

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.

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.

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 SmartCard sono presenti più di un certificato di sottoscrizione viene comunque dta la psoosibilità di scelta.

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

ATTENZIONE: I documenti elettronici creati con i prodotti Microsoft Word, Microsoft Excel e Adobe Acrobat possono contenere elementi dinamici; data la variabilità di tali elementi, visualizzazioni successive del documento potrebbero differire dal documento originariamente creato.

Nel caso di documenti firmati digitalmente contenenti tali elementi dinamici, **Certicomm ESPRESSAMENTE AVVERTE** gli utenti di Dike che i dati originariamente contenuti nei suddetti elementi potrebbero differire da quelli visualizzati in fase di verifica indipendentemente dall'esito della stessa.

2.3 Aprire un documento per verificare la marca temporale

Per effettuare questa operazione è indispensabile il collegamento Internet attivo.

I files contenenti insieme il documento firmato e la marca hanno l'estensione 'M7M' e sono contrassegnati da un'icona raffigurante un orologio.

Dopo aver selezionato il file marcato che si intende verificare (menu File – Apri oppure clic sull'icona corrispondente) il programma visualizza nella parte inferiore del video il documento originale e nella parte superiore una finestra contenente l'esito della verifica della marca temporale, seguita dall'esito della verifica delle firme apposte al documento. Non è possibile effettuare alcuna operazione sul file visualizzato.

2.4 Aprire un documento per verificare le firme

Si sceglie il file che si intende verificare (menu *File – Apri* oppure clic sull'icona corrispondente), selezionandolo dalla lista composta in base al formato impostato (doc, pdf, tif, rtf, etc.).

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

Se è impostata l'opzione corrispondente (menu *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.

All'apertura del file, nella finestra immediatamente sovrastante appaiono automaticamente gli estremi dei titolari delle firme digitali apposte sul documento, a partire dall'ultima in ordine temporale.

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 visualizzate 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

2.5 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.

Selezionare dal menu:

Strumenti – Associa marca e documento

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 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.

2.6 Cambiare il PIN di una smart card

Per modificare il PIN segreto (Personal Identification Number) di una smart card, dopo averla inserita nel lettore, scegliere la funzione relativa (menu *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 din trasporto. Prima di essere utilizzata la prima volta si deve procedere ad un cambio PIN;
- Smart Card Sysgillo CardOS M4 (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 comicia con 1401) il pin è da 5 a 8 numeri;

Attenzione!

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 CryptoSmartCardE16 (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 CryptoSmartCardE4H (numero di serie che comincia con 1202) il numero di tentativi permesso è 3[1]
– se la smart card è del tipo Sysgillo CardOS M4 (numero di serie che comincia con 1203) il numero di tentativi permesso è 3[1]
– - se la smart card è del tipo Siemens CardOs m4.01 (numero di serie che comicia con 1401) il numero di tentativi permesso è 3[1]

Per informazioni sull'operazione di sblocco visitare la pagina Internet www.card.infocamere.it/servizi/gestione.htm

Per informazioni su nuovi modelli di SamrtCard oltre a quelli descritti sopra visitare pagina Internet http://www.card.infocamere.it/hardware/hardware_home.htm

1Su questo tipo di Smart Card il blocco non è permanente; la carta può essere recuperata tramite lo sblocco del codice segreto PUK.

2.7 Comportamento di Dike con carte rilasciate da altri certificatori

Dike permette di firmare anche con SmartCard rilasciate dal PosteCom; le carte sono GemPlus. Per poterle utilizzare, anche in Dike, si devono avere comunque i driver rilasciati dalla Poste

Dike permette di firmare anche con SmartCard rilasciate dalle CA accreditate gestite da Actalis. Queste carte sono distribuite insieme al prodotto "Firma digitale Actalis file protector" distribuito da Buffetti; il prodotto contiene la versione 2.0 di CardOS API che è più vecchia di quella utilizzata per le carte InfoCamere 1401… Per far funzionare entrambi si deve installare la versione di CardOS API scaricabile dal sito www.card.infocamere.it

Le SmartCard rilasciate dal consiglio nazionale dei notariato e SecurSign, il prodotto di firma digitale dei notai italiani, sono compatibili con Dike. Fanno uso di una versione più vecchia del CardOS API che comunque non va in conflitto con quella scaricabile dal sito www.card.infocamere.it

Non possono essere utilizzate assieme carte Actalis e del notariato, ma solo dopo un cambio di configurazioni.

E' possibile modificare il PIN solo per la SmartCard rilasciate da InfoCamere. Per modificare il PIN delle altre carte utilizzare i prodotti distribuiti dal fornitore.

2.8 Controllare se la versione di Dike è aggiornata

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

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

2.9 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 (menu *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.

Attenzione!
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 CryptoSmartCardE16 (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 CryptoSmartCardE4H (numero di serie che comincia con 1202) il numero di tentativi permesso è 3[2]
- se la smart card è del tipo Sysgillo CardOS M4 (numero di serie che comincia con 1203) il numero di tentativi permesso è 3[1]
- - se la smart card è del tipo Siemens CardOs m4.01 (numero di serie che comicia con 1401) il numero di tentativi permesso è 3[1]

Per informazioni sull'operazione di sblocco visitare la pagina Internet www.card.infocamere.it/servizi/gestione.htm

Per informazioni su nuovi modelli di SmartCard oltre a quelli descritti sopra visitare pagina Internet http://www.card.infocamere.it/hardware/hardware_home.htm

2.10 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)

2Su questo tipo di Smart Card il blocco non è permanente; la carta può essere recuperata tramite lo sblocco del codice segreto PUK.

4. Individuare il file che si intende firmare, scegliendo Unità, Directory, Tipo di file
5. Aprire il file (clic sul file + OK, oppure doppio clic sul file)
6. Scorrere il documento per identificarlo con certezza
7. Attivare il menu Modifica-Firma-Firma e Salva(oppure cliccare sulla relativa icona)
8. Individuare la destinazione del file firmato, scegliendo Unità e Directory
9. Alla richiesta, digitare il PIN della propria smart-card
10. Viene visualizzata la lista dei certificati presenti nella smart card: individuare il certificato con cui si intende firmare scegliendolo tramite un click
11. Attendere la conclusione dell'operazione di firma
12. Confermare con OK le finestre che mostrano esito ed estremi del firmatario
13. 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 files e uscire da Dike

2.11 Impostare i parametri del proxy HTTP

Questa funzionalità (menu *Opzioni – Impostazione parametri proxy HTTP*) deve essere utilizzata solo se l'accesso ad Internet per il protocollo HTTP e HTTPS 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.

2.12 Impostare i parametri del proxy LDAP

Questa funzionalità (menu *Opzioni – Impostazione parametri proxy LDAP*) 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.

2.13 Impostare il lettore utente

Questa funzionalità (menu *Opzioni – Lettore utente*) permette di impostare il lettore della smart card da utilizzare per le operazioni di firma.

Dopo la modifica del lettore il programma Dike viene terminato; 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.

2.14 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 (menu *File – Apri* oppure clic sull'icona corrispondente), selezionandolo dalla lista composta in base al formato impostato (*.*, doc, pdf, tif, rtf, etc.). Possono essere marcati solo i files cui è associata almeno una firma digitale; il file finale (P7M originale + marca temporale) avrà l'estensione M7M.

Una volta aperto (e visualizzato nei casi previsti) il file, si passa alla funzione di marcatura (menu *Modifica – Marca* oppure clic sull'icona corrispondente): 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 (menu *Modifica – Firma* – Firma e *Marca)*

2.15 Salvare un documento escludendone le firme

Questa funzionalità consente di salvare il file originale senza le eventuali firme digitali associate. Con il file aperto lanciare la funzione relativa (menu *File – Salva origine* oppure clic sull'icona corrispondente), selezionando successivamente la directory di destinazione del file. Dike non consente di modificare il nome originario del file.

2.16 Scaricare l'elenco dei certificatori

Questa funzionalità (menu *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.

2.17 Separare la marca temporale e il documento firmato da un documento marcato

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

Selezionare dal menu:

Strumenti – Separa marca da documento
la maschera visualizzata richiede di specificare il file marcato 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.

2.18 Stampare la lista dei firmatari

Con il file P7M aperto (e visualizzato nei casi previsti) questa funzionalità (menu *File – Stampa lista firme* oppure clic sull'icona corrispondente) permette di stampare gli estremi delle firme digitali associate al documento.

2.19 Stampare un documento

Questa possibilità è consentita solo per i files visualizzati da Dike, cioè quelli con estensione DOC, XLS, PDF, TIF, RTF, TXT, HTM, XML, JPG.

Per i documenti con formato XLS e PDF, Dike apre automaticamente i rispettivi visualizzatori (Excel, Adobe Acrobat): si utilizzeranno quindi le normali funzionalità di stampa di tali programmi.

Per i documenti con formato TIF, RTF, TXT, HTM, XML, JPG Dike mette a disposizione invece la funzionalità Windows di stampa, attivabile con il bottone Stampa che comparirà sulla barra Documento.

2.20 Uscire dal programma

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

2.21 Verificare lo spazio libero sulla smart card

Per verificare lo spazio libero sulla smart card scegliere la funzione relativa (menu *Strumenti – Verifica spazio su smart card)*.

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 SmartCard

2.22 Visualizzazione dei certificati

Questa nuova funzione permette di visualizzare TUTTI i certificati presenti sulla SmartCard.

Per accedere, selezionare dal menu *Strumenti* la voce : *Lista certificati su SmartCard*