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

DIKE 3.3.0

Funzione emittente	70500 Area Sistemi Sicurezza Informatica
Redatto da	GM

DIKE 3.3.0

Sistemi operativi

La versione di Dike 3.3.0 è compatibile con Microsoft Windows nelle versioni 2000/XP/2003 ®.

Installazione

Prima di iniziare 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…."
Dike è compatibile con il protocollo di autenticazione di Microsoft NTLM. In questo caso non impostare nulla nella configurazion proxy.

Il programma può essere installato solo con i *privilegi di amministratore*;

L'utilizzo del programma invece è permesso anche collegandosi al sistema con privilegi ridotti purché alla directory ove è stato installato il programma (di solito c :\programmi\infocamere\dike) siano assegnate le proprietà di scrittura.
Per fare ciò bisogna:
- collegarsi al sistema con i privilegi di amministratore
- aprire 'Gestione risorse' e selezionare la cartella ove è stato installato Dike
- fare click con il tasto destro del mouse, scegliere la voce 'Proprietà', 'Protezione'
- selezionare l'utente cui si vuole concedere l'uso del programma Dike (oppure tutti gli utenti)
- nella colonna 'Consenti' selezionare con un click la riga corrispondente alla voce 'scrittura'
- premere 'OK'

Adeguamento alla delibera CNIPA 4/2005

Sono state apportate le necessarie modifiche per adeguarsi alla delibera CNIPA 4/2005 - **Regole per il riconoscimento e la verifica del documento informatico.**
La delibera definisce le regole a cui si devono attenere i certificatori accreditati per la firma e la verifica del documento informatico e sostitisce la precedente circolare n° AIPA/CR/24.

Le nuove implementazioni riguardano un nuovo profilo per il certificato, e nuove regole sulle buste crittografiche. Rimangono invariate quelle relative ai certificati e delle buste utilizzati prima dell'entrata in vigore della delibera.

Il testo della delibera si può trovare sul sito del CNIPA
http://www.cnipa.gov.it/site/it-IT/Normativa/Circolari_e_Deliberazioni/

Formato dei certificati
La delibera descrive un nuovo profilo per i certificati qualificati; mentre prima le principali informazioni erano descritte nel campo commonName ("cn" o "nome comune") del certificato ora sono definite in altri campi.

Inoltre la delibera introduce un nuovo tipo di certificato, in cui il titolare viene individuato da uno pseudonimo.

Di seguito una tabella con le più importanti differenze nel certificato tipo vecchio, nuovo o di pseudonimo.

	Old-Cerificate	***New-Certificate***	***New-Certifcate Pseudonym***
Firmatario (Nome Cognome)	estratti dal commonName	givenname surname	pseudonym
Codice Fiscale	estratto dal commonName	serialNumber	
Ruolo	description	title	
Codice Identificativo (IUT)	estratto dal commonName	dnQualifier	

Per i nuovi certificati inoltre sono presenti anche le seguenti estensioni
OID: 0.4.0.1862.1.1 -> Il certificato è qualificato conforme la direttiva europea 199/93/EC

OID: 0.4.0.1862.1.2 -> Può contenere un limite di valore.....

OID: 0.4.0.1862.1.3 ->Il certificato viene conservato dalla CA per 10 anni

OID: 0.4.0.1862.1.4 -> La chiave privata associata la certificato è memorizzata in un dispositivo sicuro conforme la direttiva europea 199/93/EC

Formato delle buste crittografiche
La busta crittografica, il formato del file firmato, rimane il PKCS7 (ver 1.5) e l'estensione che viene aggiunta al file firmato è sempre "P7M".
Le firme multiple parallele continuano ad essere gestite come prima, mentre sono state introdotte delle novità per le controfirme (firma della firma del firmatario precedente). In base alla delibera la busta PKCS7 potrà contenere l'elemento counterSignature.
Per ottenere una controfirma selezionare un file firmato e selezionare dal menu *modifica / controfirma.* Verrà mostrata la lista dei precedenti firmatari, scegliere quello alla cui firma va applicata la controfirma.

Verifica delle firme
Dike gestisce la verifica delle vecchie e nuove buste crittografiche; si può fare la verifica anche per firme con certificati degli altri certificatori che si sono allineati alla delibera.

Nuova modalità visualizzazione file

Rispetto alle versioni precedenti di Dike, 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 al comportamento del 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 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 firmato sarà quello privo delle modifiche.

Smart Card rilasciate da InfoCamere

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

Correzione malfunzioni

Sono state corrette alcune malfunzioni. Una di questa era la mancata segnalazione del certifcato scaduto.