LINEE GUIDA PER GLI ENTI ADERENTI

Verifica di un documento Firmato Digitalmente

Versione 5.0 del 01/02/2017

EmPULIA
CENTRO ACQUISTI PER LA PUBBLICA AMMINISTRAZIONE ®

InnovaPuglia

SOGGETTO AGGREGATORE DELLA REGIONE PUGLIA

Indice

Introduzione

Cos'è la Firma Digitale?

La firma digitale è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali. La differenza tra firma autografa e firma digitale è che la prima è legata alla caratteristica fisica della persona che appone la firma, vale a dire la grafia, mentre la seconda al possesso di uno strumento informatico e di un PIN di abilitazione, da parte del firmatario. La firma digitale può essere quindi definita l'equivalente elettronico di una tradizionale firma apposta su carta, assumendone lo stesso valore legale. E' associata stabilmente al documento informatico e lo arricchisce di informazioni che attestano con certezza l'integrità, l'autenticità e la non ripudiabilità dello stesso. L'elemento di rilievo del sistema firma è rappresentato dal certificato digitale di sottoscrizione che viene rilasciato dagli enti certificatori. Il certificato di sottoscrizione è un file generato seguendo precise indicazioni e standard stabiliti per legge (al suo interno sono conservate informazioni che riguardano l'identità del titolare, la chiave pubblica attribuitagli al momento del rilascio, il periodo di validità del certificato stesso oltre ai dati dell'Ente Certificatore). Il certificato digitale di un titolare, una volta entrato a far parte dell'elenco pubblico dei certificati tenuto dall'Ente Certificatore, garantisce la corrispondenza tra la chiave pubblica e l'identità del titolare.

Ministero degli Interni – Repubblica Italiana

La firma digitale consente di scambiare in rete documenti con piena validità legale. Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni.

Per dotarsi di firma digitale è necessario rivolgersi ai certificatori accreditati autorizzati da AgID ***(Agenzia per l'Italia Digitale)*** che garantiscono l'identità dei soggetti che utilizzano la firma digitale.

AgID svolge attività di vigilanza sui certificatori.

Le modifiche apportate al CAD dal d.lgs. 30 dicembre 2010, n. 235, prevedono l'emanazione di nuove regole tecniche che regolano la materia firma digitale,

firma elettronica qualificata e firma elettronica avanzata. Il 14 maggio 2012 si è ultimata la procedura di notifica alla Commissione Europea e agli altri Stati Membri. L'iter previsto per la loro emanazione, a cura dell'Ufficio Legislativo del Ministro proponente, è quindi ripreso.

La Determinazione Commissariale 28 luglio 2010, che modifica la Deliberazione CNIPA n. 45/2009 - Testo consolidato, introduce nuovi e più robusti algoritmi crittografici di firma digitale e nuovi formati di firma. In particolare, è interessante notare che i nuovi formati di firma rientrano nel novero dei formati che tutti gli Stati membri dell'Unione Europea si accingono ad introdurre. Questo è uno dei passi necessari per giungere al riconoscimento dei documenti sottoscritti con firma digitale a livello europeo e, conseguentemente, al libero scambio di documenti informatici giuridicamente rilevanti.

Le modifiche di interesse generale sono:

1. I certificatori rendono disponibili nuove applicazioni che implementano i nuovi formati di firma digitale (con anche il più robusto algoritmo SHA-256);

2. L'utente che, nonostante la disponibilità delle nuove applicazioni, non abbia proceduto all'aggiornamento continuerà a generare firme conformi alle precedenti regole tecniche. La Determinazione sancisce la conformità alle regole tecniche di dette firme se generate entro il 30 giugno 2011.

A chi richiedere la Firma digitale?

Coloro che desiderano dotarsi di un dispositivo di firma digitale spesso hanno difficoltà a capire a quale certificatore rivolgersi.
Per orientarsi in tale scelta viene resa disponibile una tabella con alcune informazioni utili. Nella tabella sono indicati i siti web dei certificatori che invitiamo a visitare per poter conoscere le condizioni d'uso.
La verifica della firma digitale

L'applicazione europea "Digital Signature Service" (DSS), utilizzabile anche per verificare firme digitali basate su certificati emessi da certificatori stabiliti in altri Stati membri, resa disponibile sul sito, conta oltre mille accessi mensili.

Ulteriori informazioni nella sezione Software di verifica.

La marca temporale

La marca temporale è il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi.

Il servizio di marcatura temporale si basa sull'uso delle funzioni di hashing. L'hash è una sorta di impronta digitale che consente di identificare univocamente il documento.

Nel caso di documenti su cui sia stata apposta una firma digitale, la presenza di una marca temporale consente di attestare che il documento aveva quella specifica forma in quel preciso momento temporale, pertanto, se anche il certificato qualificato scadesse o fosse revocato dal tutolare, si potrebbe sempre dimostrare che la firma digitale è stata apposta durante il periodo di validità dello stesso.

Agenzia per l'Italia Digitale – Repubblica Italiana

Software di Verifica della Firma Digitale

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in modo conforme alla Deliberazione CNIPA 21 maggio 2009, n. 45. I produttori dei seguenti software rendono disponibili i propri prodotti gratuitamente:

- ✓ Digital Signature Service(link is external)
- ✓ DigitalSign
- ✓ Firma OK!gold
- ✓ PkNet
- ✓ DIKE
- ✓ Firma Certa
- ✓ DSTK
- ✓ View2Sign
- ✓ MnlSignVerifier
- ✓ File Protector

La verifica della firma elettronica digitale può essere effettuata anche grazie ad applicazioni messe a disposizioni rispettivamente da:

- ✓ AgID (Attenzione richiede Java 6 installato. Non funziona con Java 7 - Attention: it works only with Java 6. It does not work using Java 7) - applicazione DSS per la verifica di firme europee
- ✓ AndXor - verifica anche le firme PDF (PAdES), le firme basate su certificati rilasciati da certificatori qualificati stabiliti nell'Unione Europea e la "firma digitale verificata" introdotta con la Determinazione 63/2014.
- ✓ Consiglio Nazionale del Notariato
- ✓ Infocert - verifica anche le firme PDF (PAdES)
- ✓ Postecom

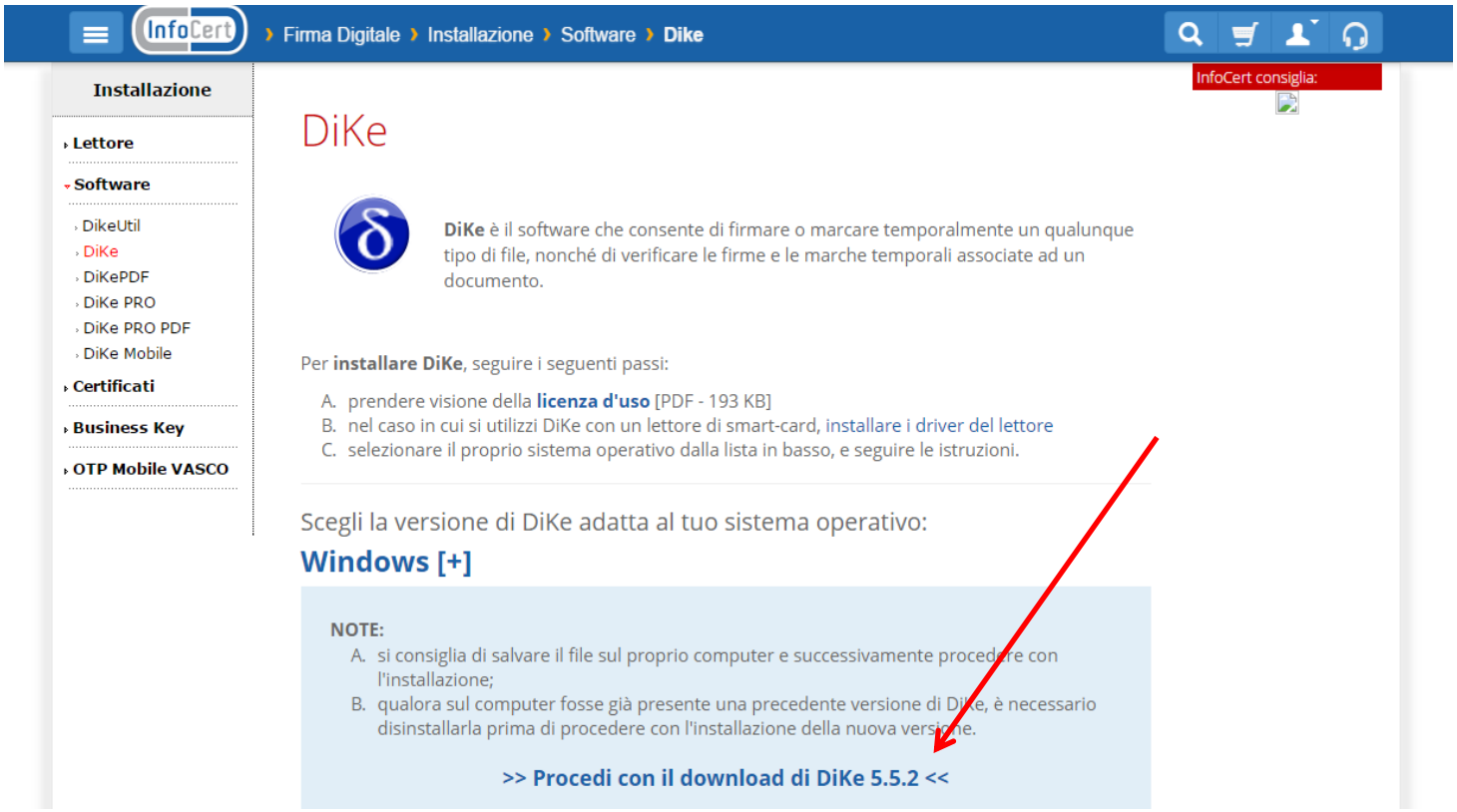
A livello europeo, la Commissione europea sta cercando di favorire il pieno riconoscimento dei documenti informatici sottoscritti nei diversi Stati Membri. A tal fine la Commissione ha reso disponibile il Digital Signature Service (DSS) , un software di firma e verifica che può essere gratuitamente scaricato e utilizzato. Il software è reso disponibile dall'Agenzia per l'uso diretto degli interessati.
Le società che intendono comunicare all'Agenzia per l'Italia Digitale ulteriori software di verifica possono scrivere a protocollo@pec.agid.gov.it.

L'Agenzia per l'Italia Digitale non è responsabile per danni, perdite, malfunzionamenti o altri inconvenienti derivanti direttamente o indirettamente dall'uso dei suddetti prodotti.

Agenzia per l'Italia Digitale – Repubblica Italiana

Software consigliato: Dike (InfoCert)

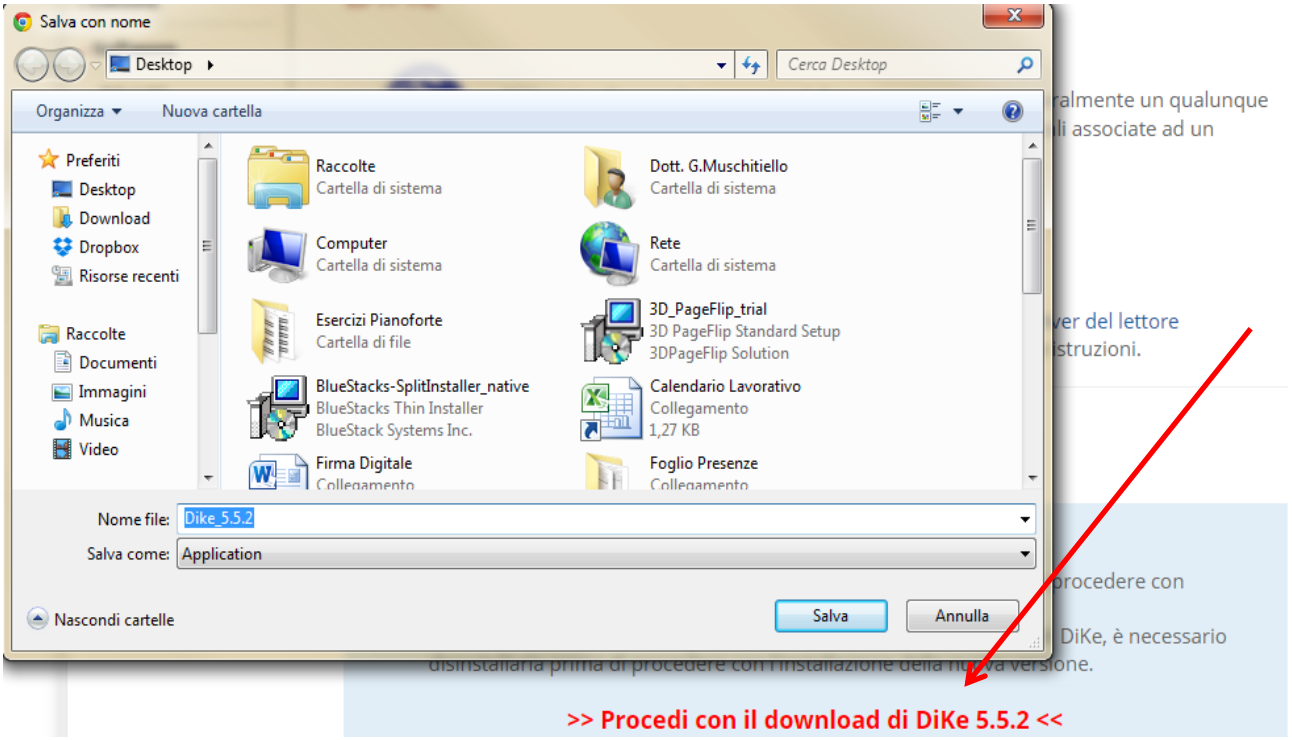
Il software è presente sul sito della Inforcert con il seguente link: https://www.firma.infocert.it



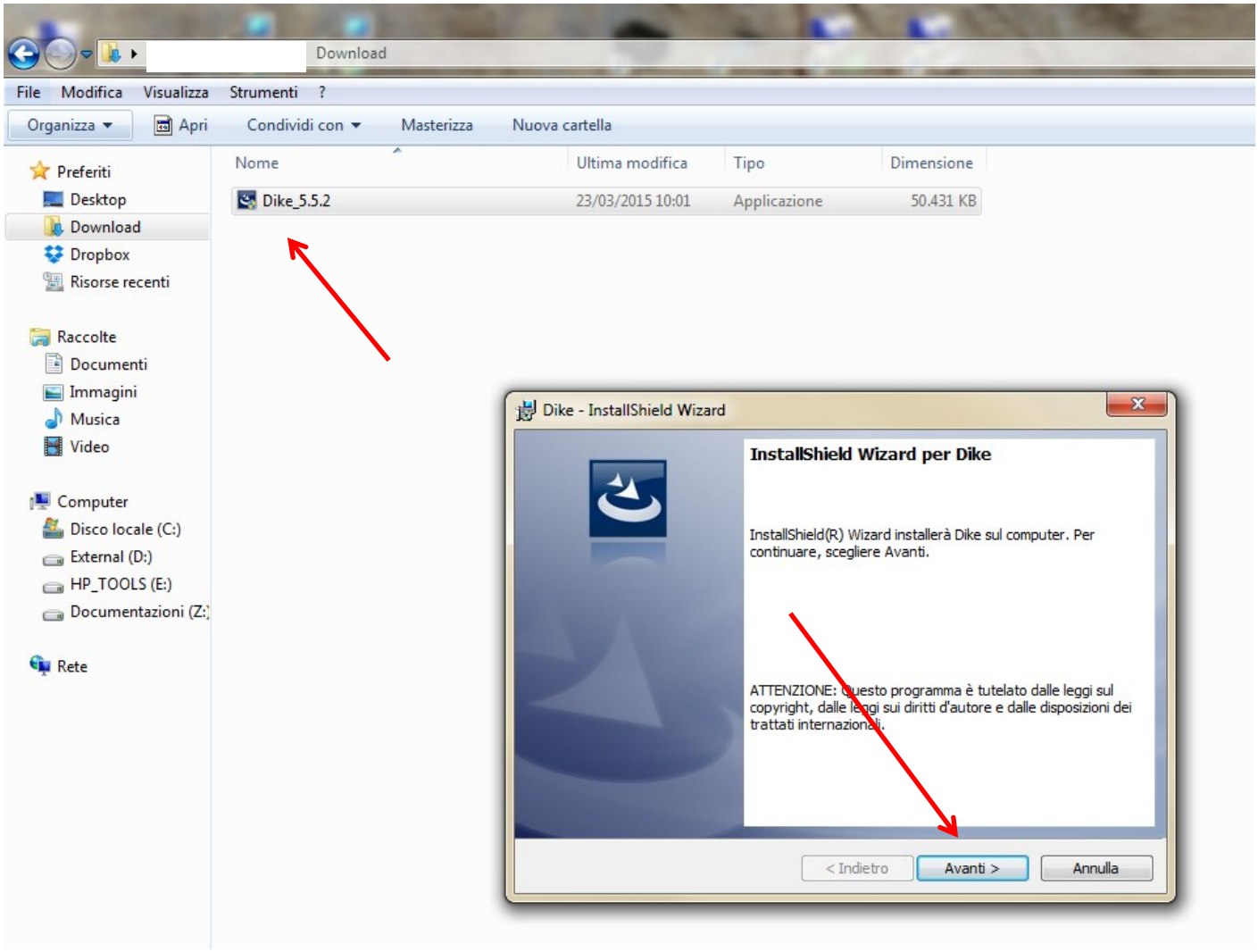
Istallazione del Software

Per l'installazione del Software Dike è necessario come prima operazione scaricare il file Eseguibile di setup.
Il suddetto file è scaricabile cliccando sul link "**Procedi con il download di Dike 5.5.2**" sul sito della Infocert nella seguente sezione:

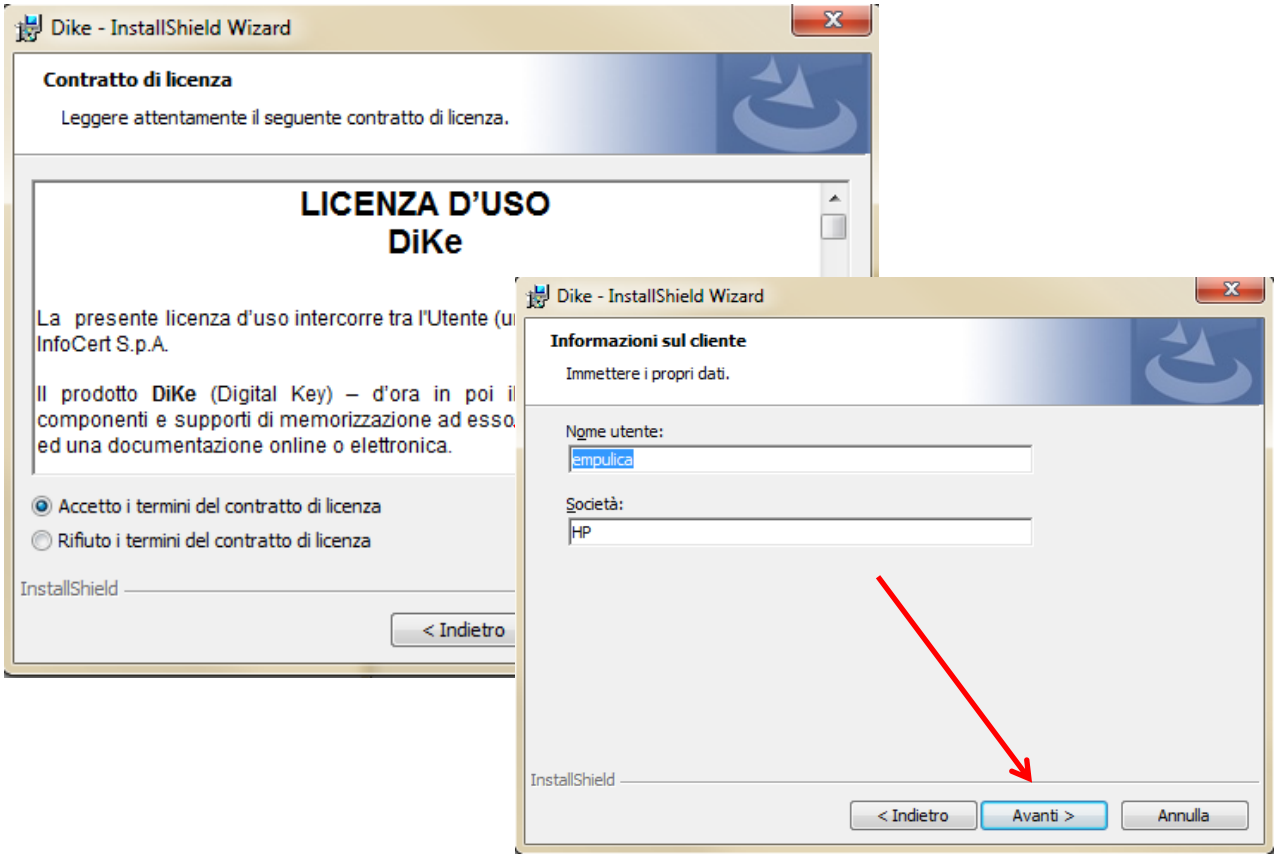
corrispondente al link
https://www.firma.infocert.it/installazione/installazione_DiKe.php



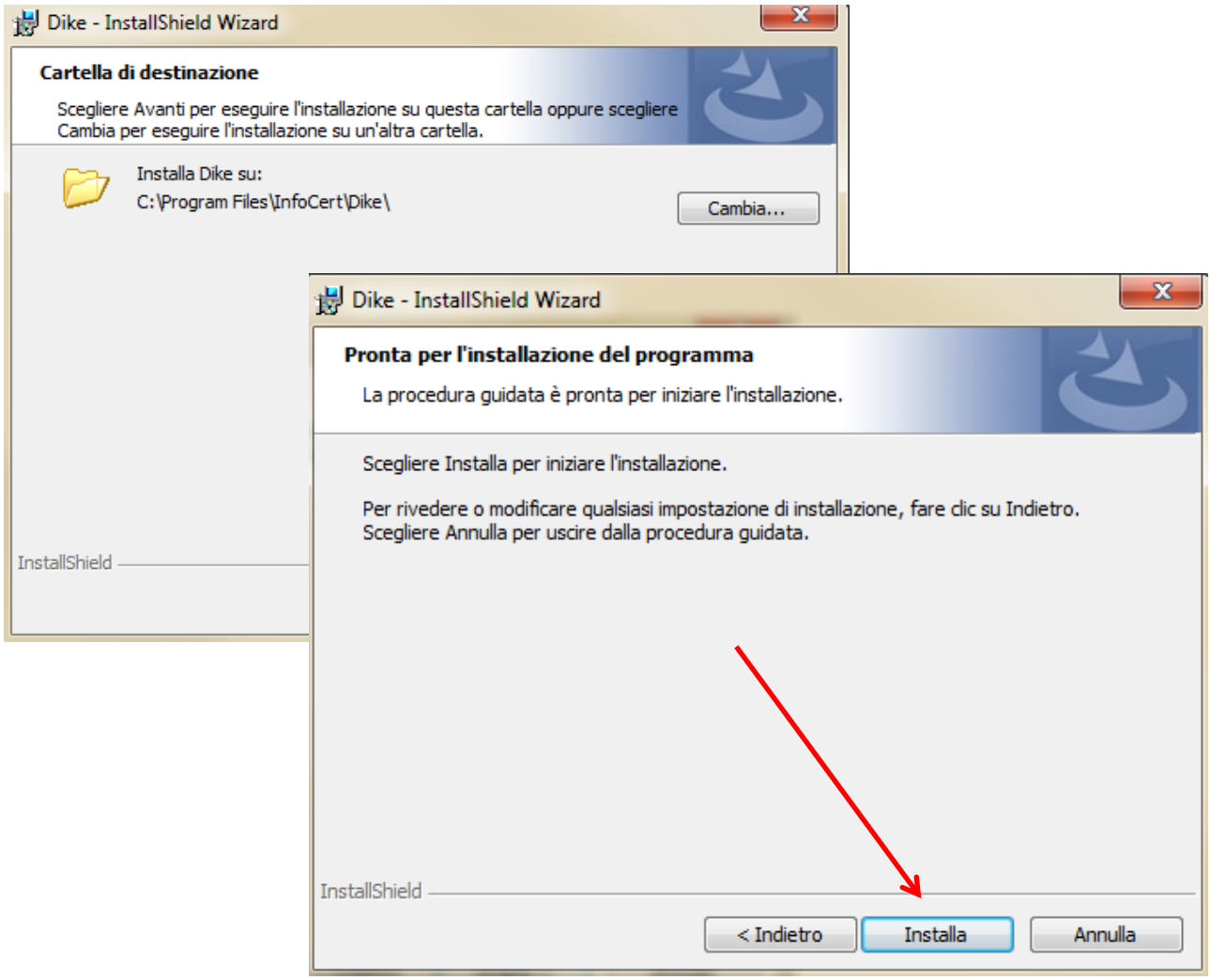
Una volta scaricato il file di installazione cliccare due volte su di esso per avviare il programma di installazione:



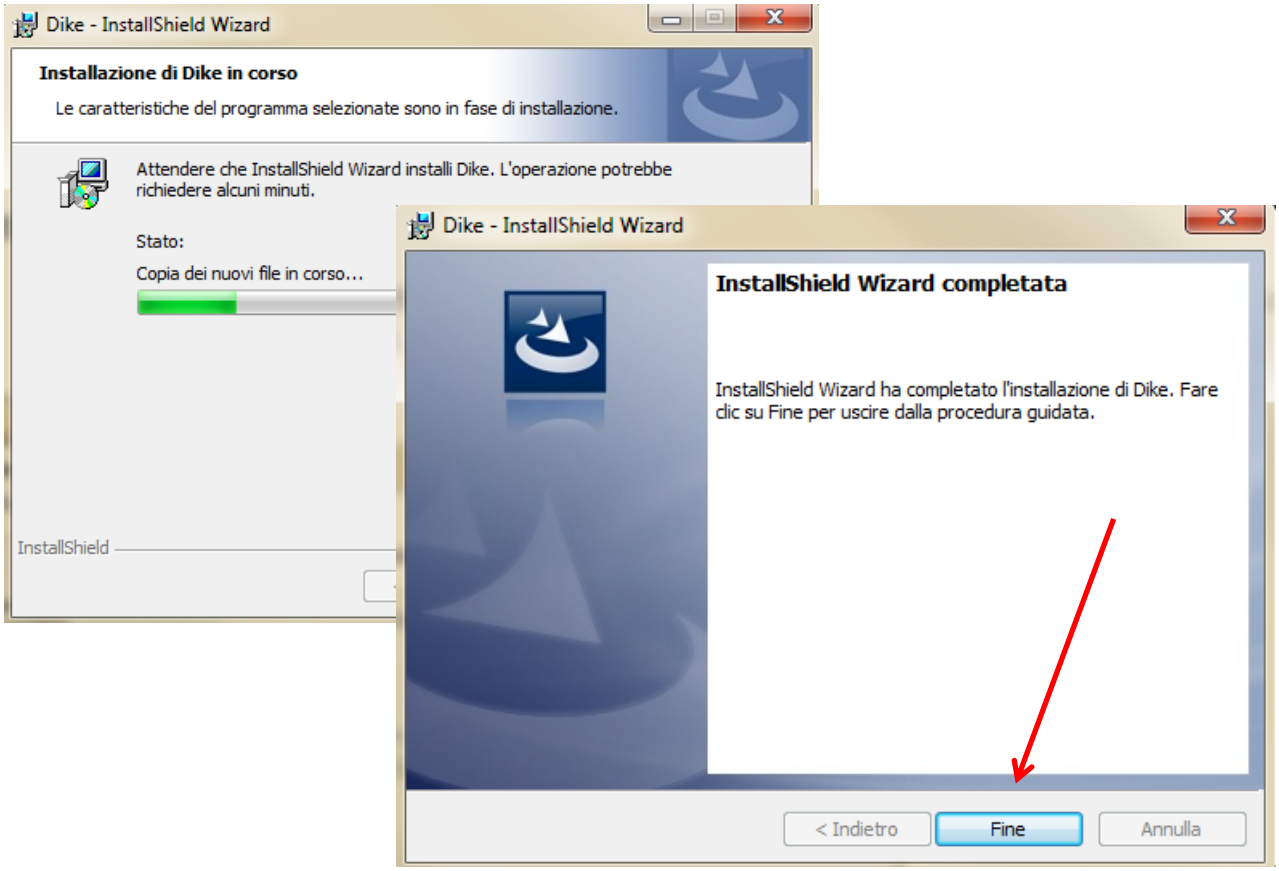
Cliccare "avanti" e procedere con l'accettazione della "Licenza d'uso", successivamente cliccare nuovamente su "avanti" dove il sistema richiede l'inserimento di un "nome utente" e un identificativo della "società":



Cliccando su "avanti" il sistema farà visionare la directory di installazione del software (si consiglia di lasciare invariata quella di default). Cliccando ancora "avanti" viene proposta la schermata successiva che avvierà l'installazione dei file, dopo il click sul comando "installa".



Al termine della copia dei file, l'ultima schermata che visualizzeremo e quella di termine. Il tasto "fine" concluderà l'operazione di istallazione.



Passi per la verifica di un documento firmato digitalmente

Cos'è un certificato

Nella crittografia asimmetrica un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.

Tale certificato, fornito da un ente terzo fidato e riconosciuto come autorità di certificazione (CA), è a sua volta autenticato per evitarne la falsificazione sempre attraverso firma digitale ovvero cifrato con la chiave privata dell'associazione la quale fornisce poi la rispettiva chiave pubblica associata per verificarlo.

Un certificato tipicamente include:

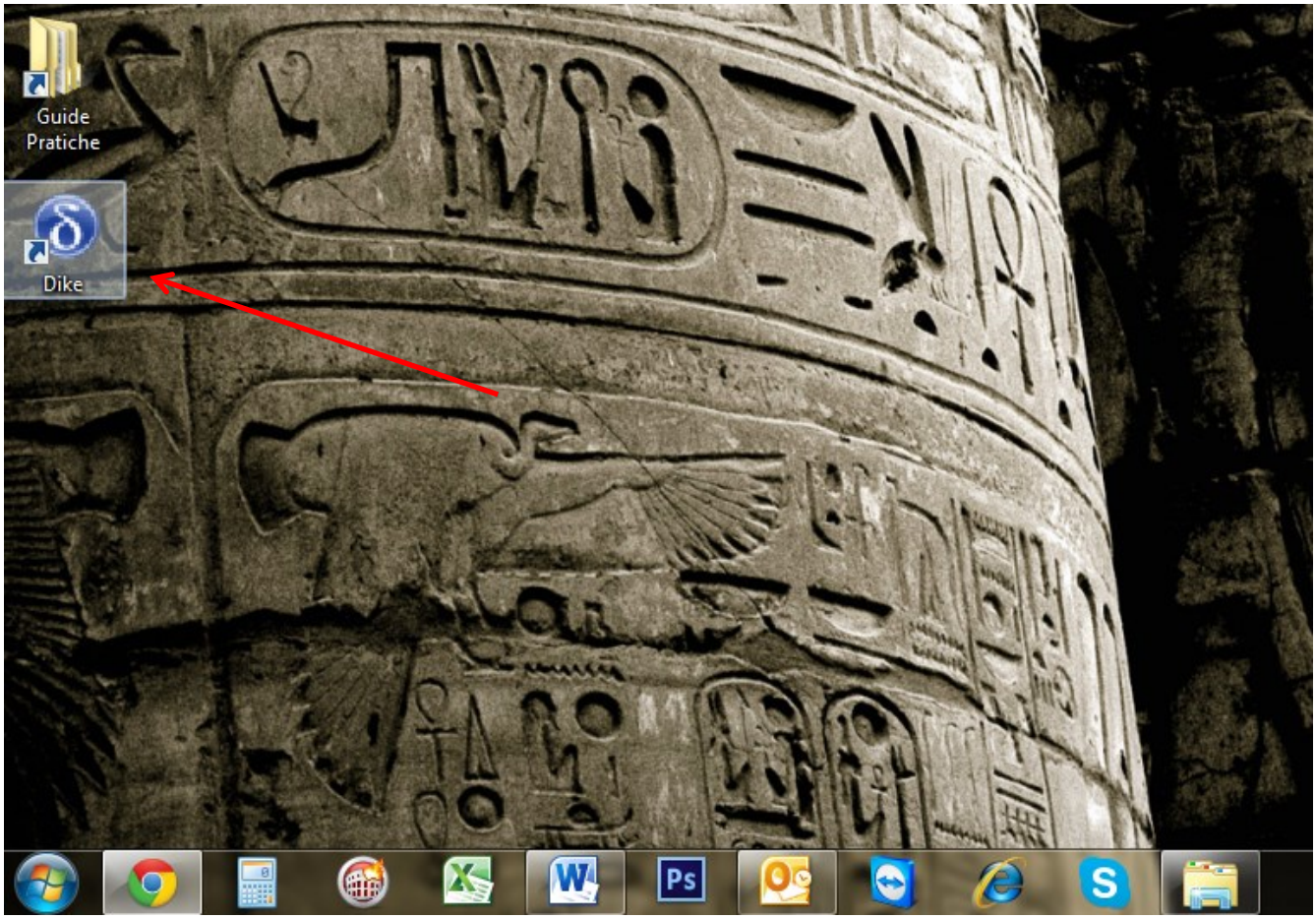
- una chiave pubblica;
- dei dati identificativi, che possono riferirsi ad una persona, un computer o un'organizzazione;
- un periodo di validità;
- l'URL della lista dei certificati revocati (CRL);

Il tutto è firmato da una terza parte fidata.

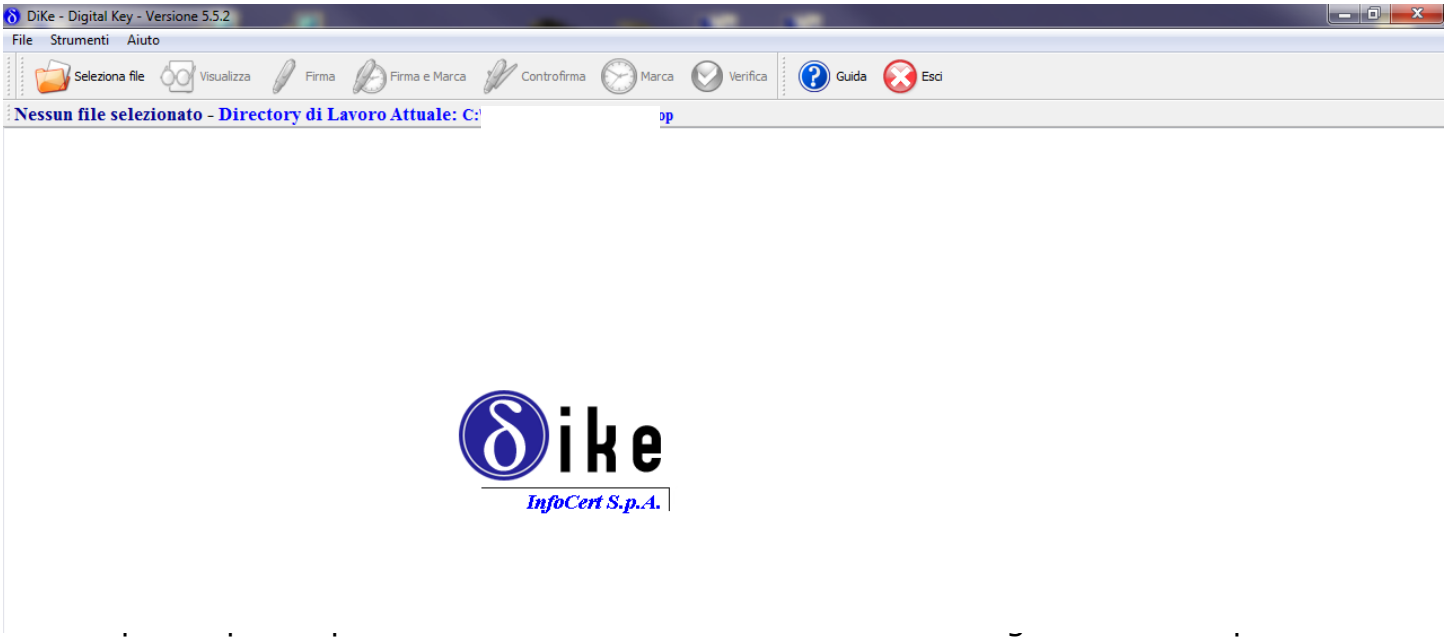
Wikipedia

Verifica

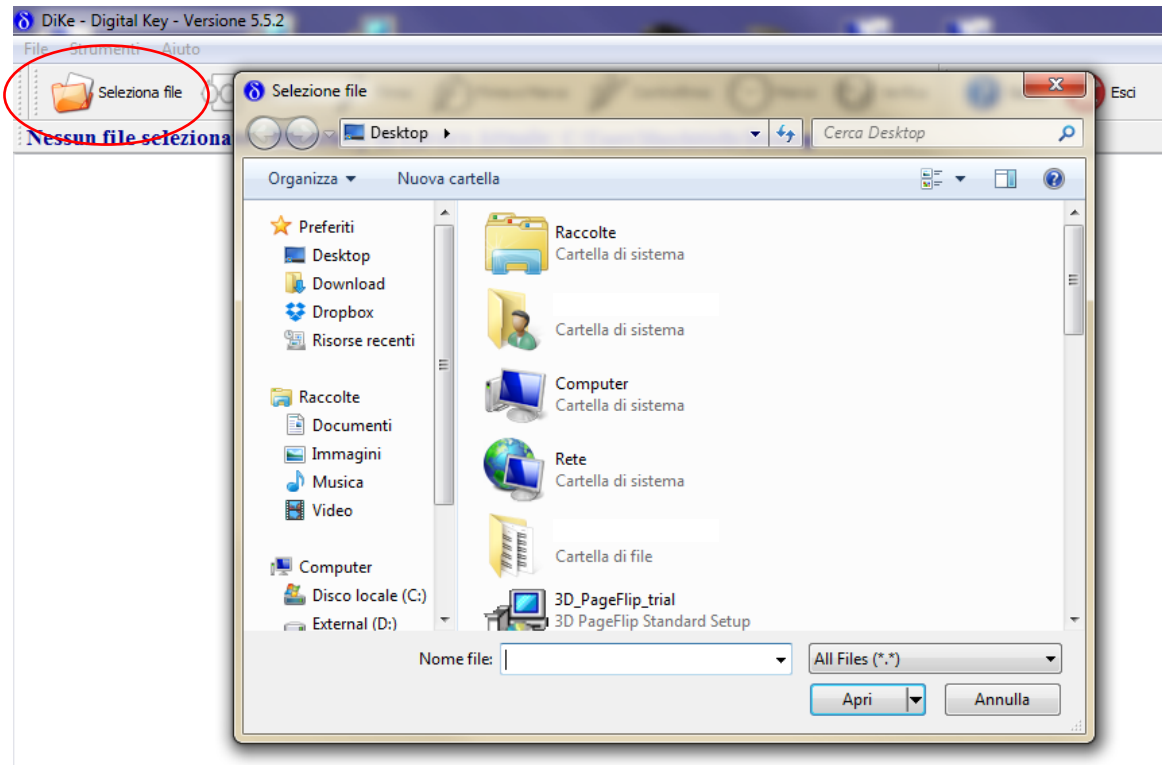
Ora vedremo come verificare la correttezza di un documento firmato digitalmente.
Come prima operazione avviare il programma cliccando sull'icona di riferimento:



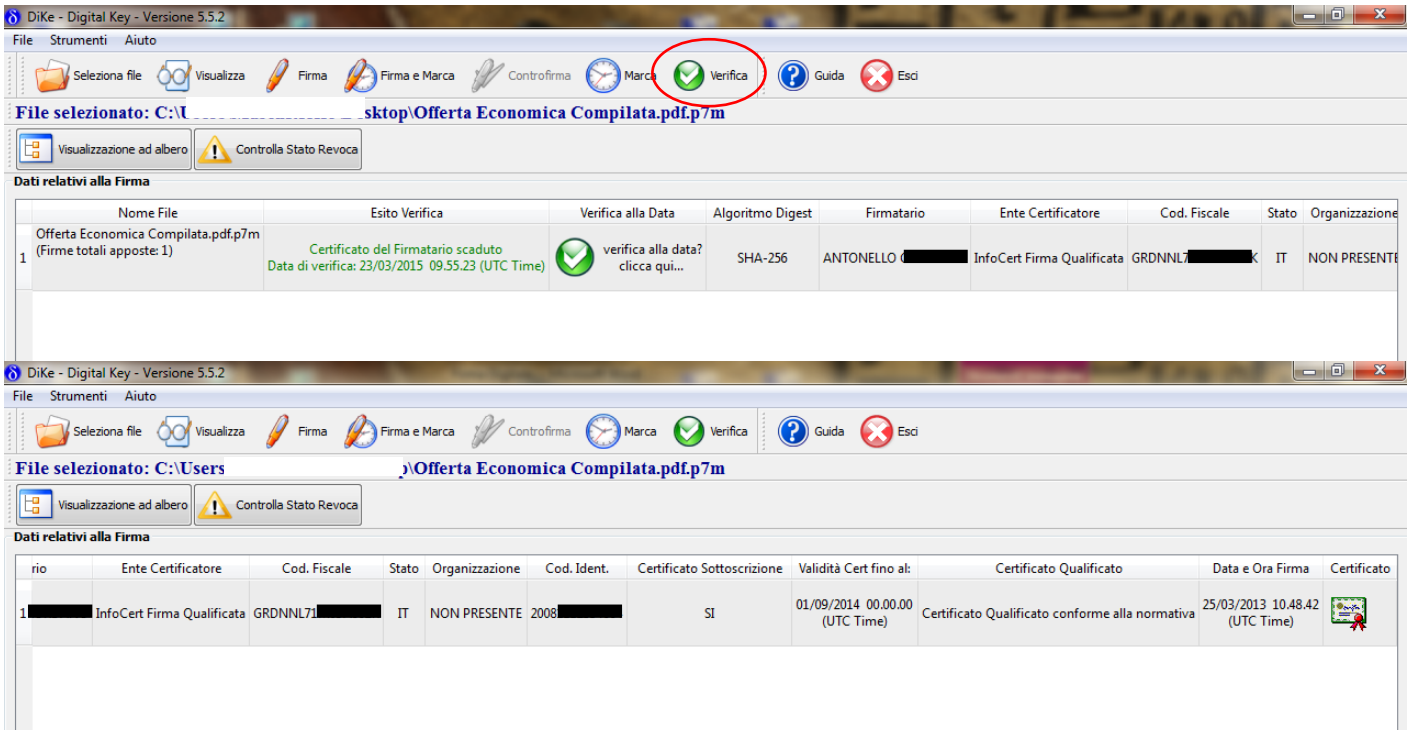
In seguito il sistema visualizza l'interfaccia del programma Dike.



caricare lo stesso all'interno di Dike utilizzando il comando "Seleziona File". Cliccando sul comando in questione ci viene aperta una finestra di ricerca e selezione del file di interesse:



Una volta caricato il file d'interesse cliccare sulla voce "verifica" per visualizzare i dati relativi al firmatario come sotto illustrato:



Dike illustra nella schermata principale una riga per ogni firmatario che ha firmato digitalmente il documento. Nel caso precedentemente illustrato il firmatario del file è unico.

I campi presenti all'interno della riga sono i seguenti:

- Nome File (Nome del documento esaminato)
- Esito Verifica (Esito della verifica della firma apportata al documento)
- Verifica alla data (Impostare la data di verifica della firma)
- Algoritmo Digest (Algoritmo utilizzato per la criptazione della firma sul documento)
- Firmatario (Nome e Cognome del firmatario)
- Ente Certificatore (Ente che certifica la firma)
- Codice Fiscale (Codice Fiscale del firmatario)
- Stato (Inteso come nazione di riferimento)
- Organizzazione (Organizzazione firmatario)
- Codice Identificativo (Codice identificativo del certificato)
- Certificato sottoscrizione
- Validità certificato fino al: (Validità del certificato utilizzato per apportare la firma al documento)

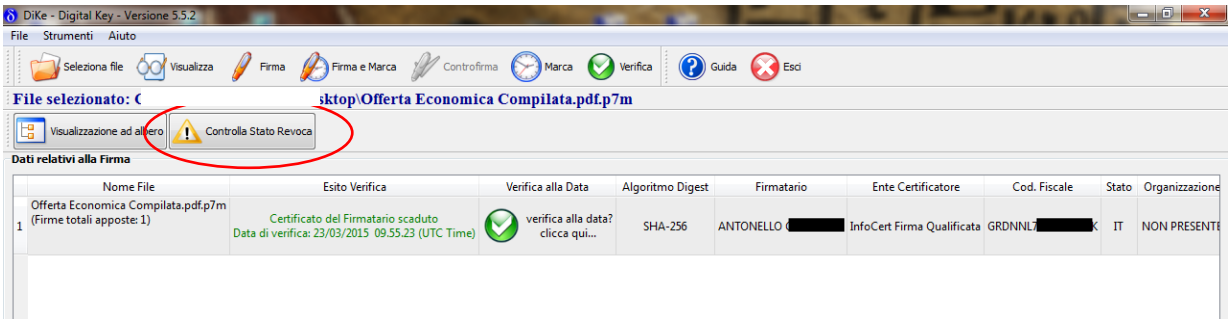
- Certificato Qualificato (Verifica se il certificato è conforme alla normativa)
- Data e ora firma (Data e Ora relativi al momento di firma)
- Certificato (Possibilità di scaricare il documento certificato in modo da tenerlo agli atti digitalmente)

Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore	Cod. Fiscale	Stato

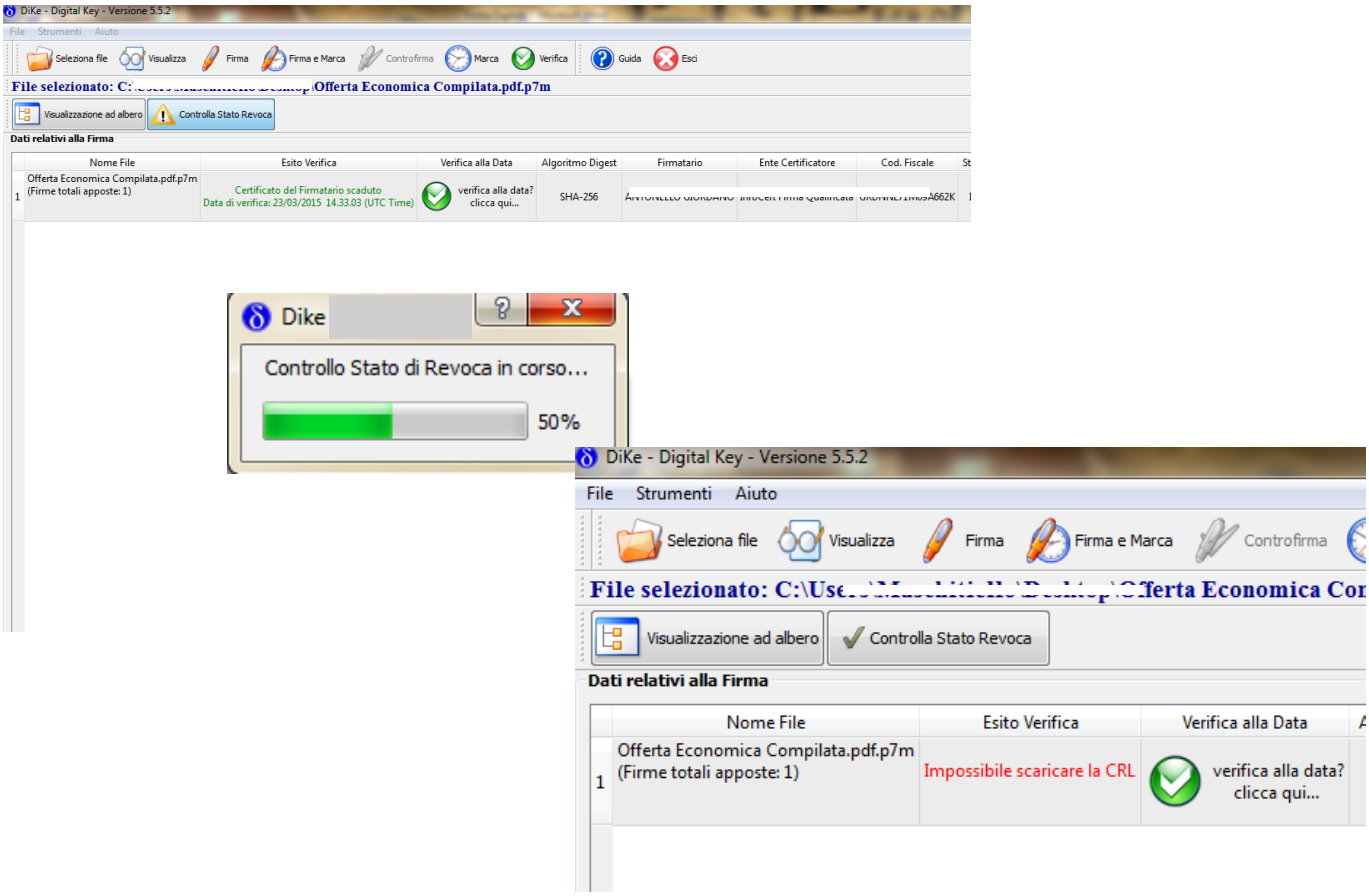
Organizzazione	Cod. Ident.	Certificato Sottoscrizione	Validità Cert fino al:	Certificato Qualificato	Data e Ora Firma	Certificato

Ai fini della nostra verifica sarà necessario controllare che il Nome, Cognome e Codice Fiscale del firmatario siano identici a quelli del rappresentate legale contenuto all'interno del documento di gara. Inoltre è necessario verificare che la data e ora di firma siano antecedenti alla data di scadenza dei termini di gara di presentazione delle offerte.

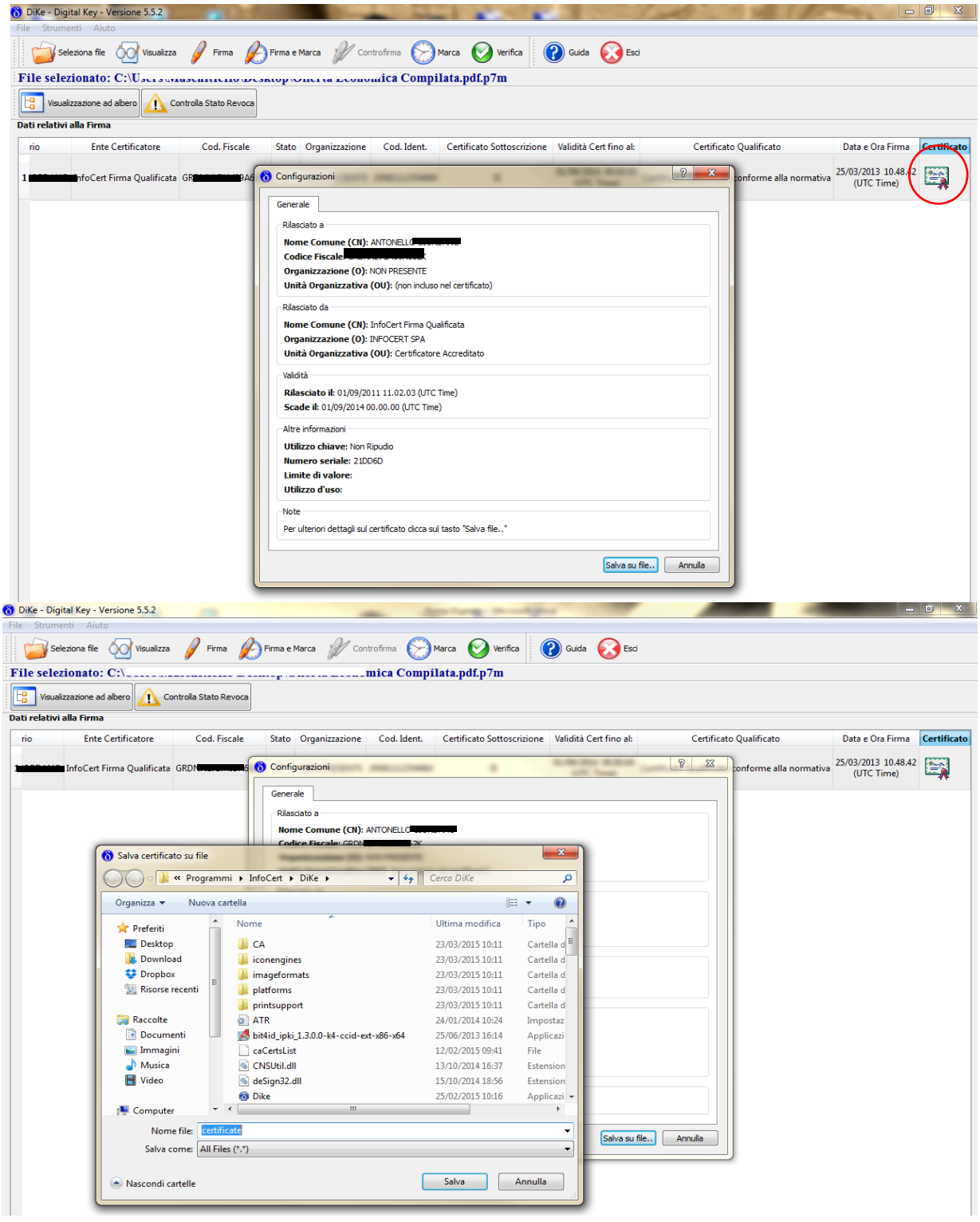
Uno sguardo infine non deve mancare alla validità del certificato di firma e allo stato di revoca dello stesso. Il controllo della revoca del certificato è effettuabile cliccando sul tasto "Controllo Stato Revoca" come segue in figura:



Si può avere ad esempio la revoca del certificato di firma qualora siamo in presenza della perdita dei requisiti morali da parte del soggetto come ad es. la condanna in giudizio.



Qualora volessimo, potremmo salvare il certificato di firma del firmatario, nei nostri documenti ai fini archivistici. Per far ciò cliccare sull'icona del certificato, presente nell'ultima colonna, in corrispondenza della riga riguardante il firmatario d'interesse e scaricare lo stesso come segue:



E' utile tener presente che con Dike oltre a poter controllare un documento firmato digitalmente possiamo anche visualizzare lo stesso cliccando sul comando visualizza come mostrato in figura: