



L'e-Government dell'ateneo Federico II

Napoli, 23 marzo 2010

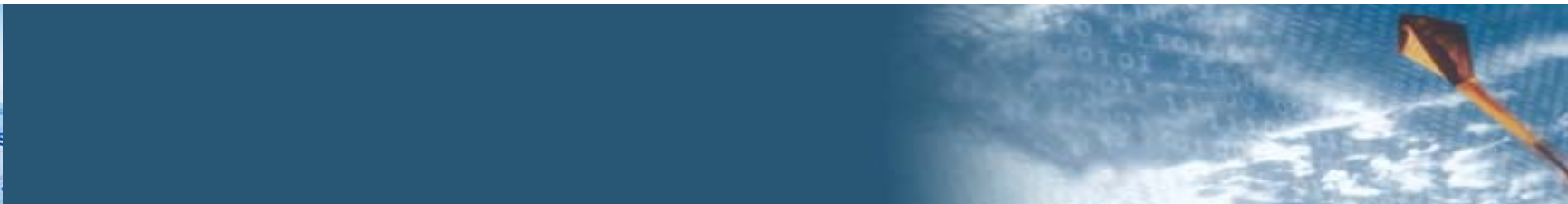
CSI - Area Tecnica e-Government



Clelia Baldo



Linee guida per la
Gestione digitale dei verbali di
Consiglio di Facoltà e di Giunta



I PARTE

Definizioni, cenni normativi e concetti generali sulla firma digitale



L'e-Government di Ateneo ed il sistema PRAXIS



è l'insieme delle soluzioni tecnico-organizzative per **l'e-Government dell'Università degli Studi di Napoli Federico II**, in linea con la normativa vigente e con le direttive strategiche governative in materia di amministrazione digitale.

Indirizzo del sito dell'eGovernment di Ateneo:
<http://www.praxis.unina.it>





Il Documento Informatico

- Le politiche di e-Government mirano alla dematerializzazione dei documenti cartacei, mediante la progressiva introduzione dei documenti informatici.
- Il “**documento informatico**” è definito come “rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”.
- Il 1° gennaio 2006 è entrato in vigore il D.lgs n.82/2005, denominato **Codice dell’Amministrazione Digitale (CAD)**, strumentazione normativa coordinata con l’impianto giuridico vigente in materia di: formazione, gestione, riproduzione, conservazione, trasmissione ed accessibilità dei documenti informatici.





Il Codice dell'amministrazione digitale e la firma digitale

- Il documento informatico sottoscritto con **firma digitale**
 - ✓ soddisfa il requisito legale della forma scritta,
 - ✓ ha efficacia giuridico-probatoria.

- La firma digitale garantisce l'**autenticità** e l'**integrità** del documento informatico sottoscritto. Inoltre, l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria (**non ripudio**).

- L'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.





La firma digitale - Generalità

- La firma digitale è basata su un procedimento di “crittografia asimmetrica” che fa uso di una **coppia di chiavi**: una privata (utilizzata per firmare) ed una pubblica (utilizzata per le operazioni di verifica della firma).
- La corrispondenza tra le chiavi di firma ed il sottoscrittore è garantita da una terza parte fidata, il **certificatore qualificato**.
- Il certificatore (qualificato) genera e consegna a ciascun titolare un **dispositivo sicuro di firma** contenente: la coppia di chiavi assieme ad un **certificato qualificato di firma** che consente l’associazione della persona con la sua chiave pubblica.
- Il certificatore (qualificato) gestisce l’**identificazione e la registrazione** certa del richiedente, nonchè la **sospensione** temporanea della validità o la **revoca** definitiva del certificato qualificato.



Il processo di firma digitale

Calcola il valore dell'impronta del documento informatico

Cifra il valore dell'impronta calcolata utilizzando la chiave privata del sottoscrittore

Aggiunge al documento originale la firma digitale ed il certificato qualificato del sottoscrittore

DOCUMENTO INFORMATICO FIRMATO

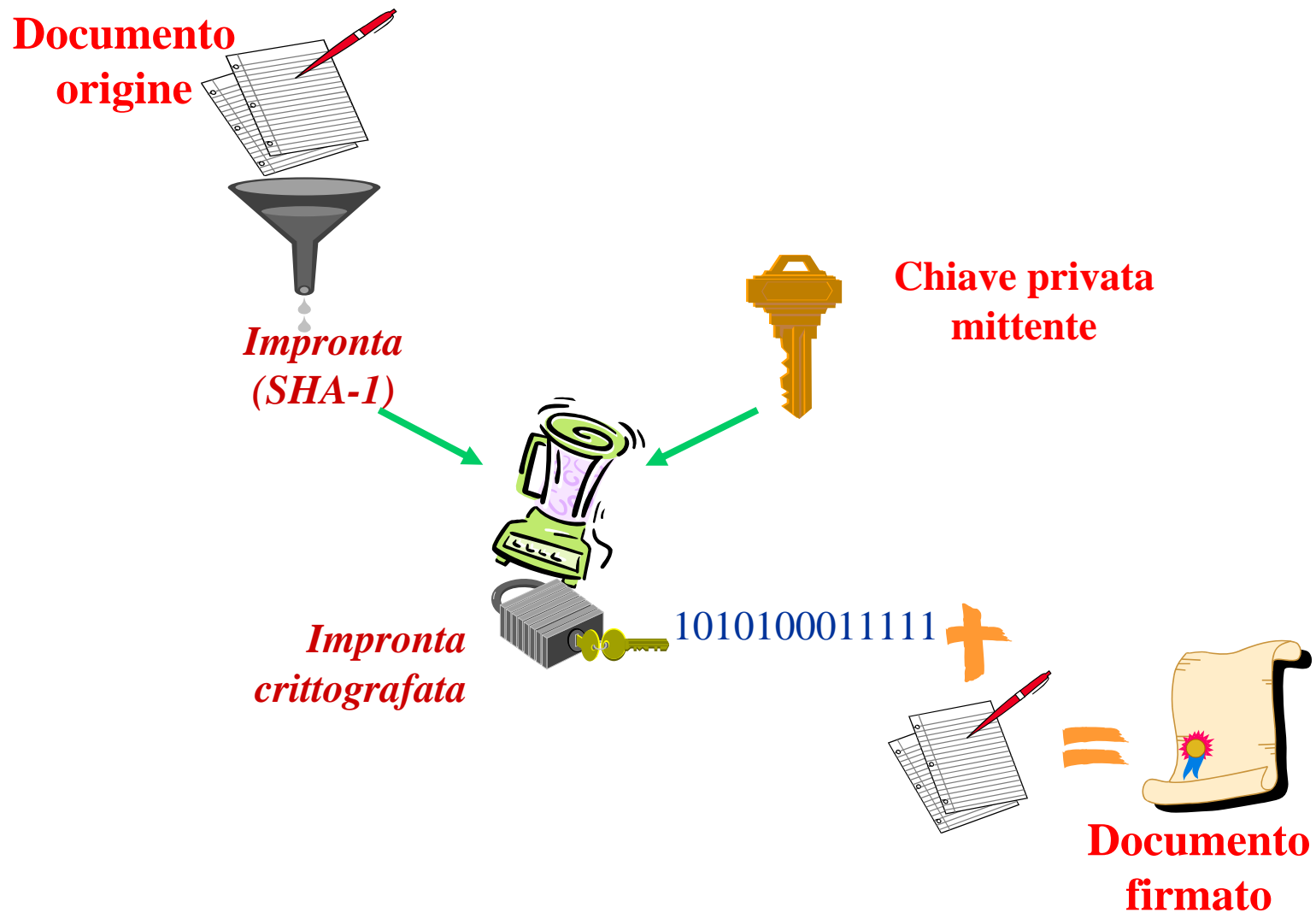


Il processo di firma digitale (1/2)

- **A** redige un documento informatico;
- Il documento è sottoposto ad “hashing”, con la generazione di un'impronta di lunghezza fissa (SHA-1 è l' algoritmo di hash usato);
- L'impronta viene crittografata con la chiave privata di **A** ed allegata al documento;
- Il documento origine e la sua impronta cifrata arrivano a **B**.



Il processo di firma digitale (2/2)



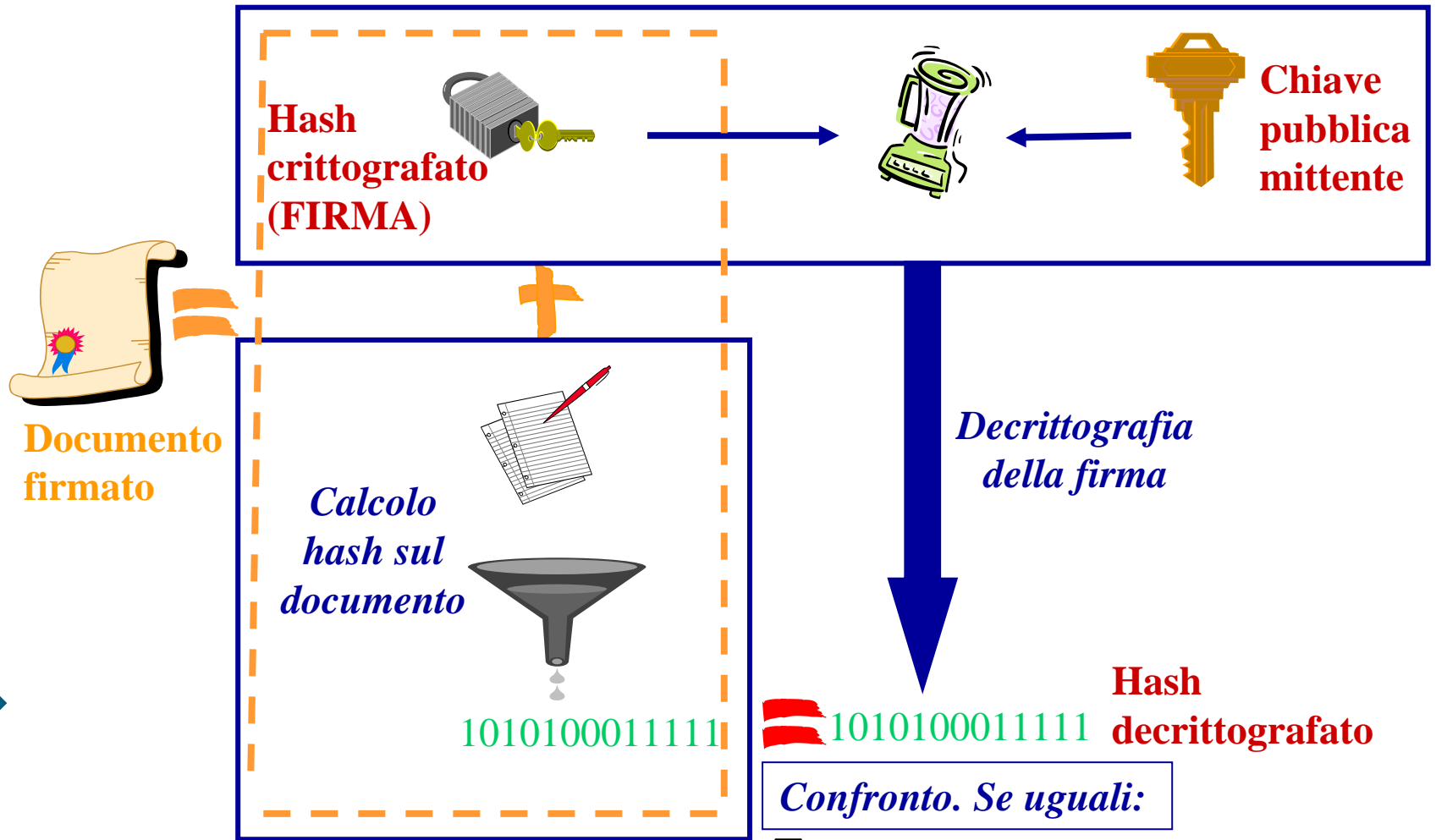


La verifica della firma digitale (1/2)

1. **B** riapplica l'hashing sul documento ed ottiene una nuova impronta;
2. **B** decifra l'impronta ricevuta con la chiave pubblica di **A**;
3. **B** confronta le due impronte: se sono uguali la firma è autentica e il messaggio non è stato modificato;
4. Se sono diverse, manca l'autenticazione o manca l'integrità.



La verifica della firma digitale (2/2)



Autentico ed integro



Il certificato qualificato

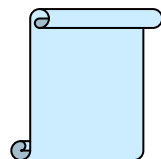
- Il certificato di firma è un documento elettronico che, oltre a contenere i dati essenziali del titolare, ne contiene la chiave pubblica:



Il formato di firma

- Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il file firmato, ossia la busta crittografica, contiene al suo interno:
 - il documento informatico nel formato originale,
 - la firma digitale ad esso associata (l'impronta crittografata con la chiave privata del o dei sottoscrittori),
 - il certificato qualificato del sottoscrittore (oppure, nel caso di più sottoscrittori, il certificato di ciascuno).

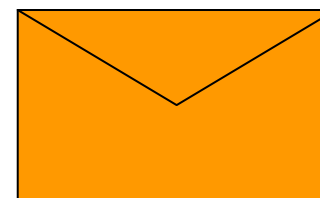
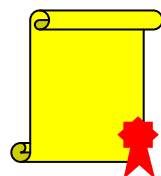
Documento informatico



Firma digitale (impronta crittografata)



Certificato qualificato



Documento firmato (.p7m)



Come apporre la firma digitale su un documento informatico

- Il titolare deve apporre in chiaro, nel documento, il proprio ruolo, il nome, il cognome e la data di sottoscrizione.
- Il titolare deve trasformare il documento informatico in formato pdf, eventualmente adoperando strumenti di tipo "open source", scaricabili anche dal sito <http://www.praxis.unina.it>.
- Per firmare il documento, è sufficiente eseguire l'applicazione **DigitalSign** (o equivalente, qualora si utilizzi una diversa CA), il cui CD di installazione è contenuto nel kit di firma.
- Il file firmato digitalmente può essere nuovamente sottoposto al processo di firma, consentendo la generazione di un documento a "firma congiunta", oppure "controfirmato". In ogni caso, il file generato presenta una sola estensione: ".p7m"
- Il file ".p7m" ottenuto può quindi, in generale, essere: conservato su supporto magnetico, oppure trasmesso mediante strumenti telematici (Posta Elettronica o Posta Elettronica Certificata), oppure allegato ad una registrazione di protocollo.





Come verificare la firma digitale su un documento informatico

- La verifica di autenticità e di integrità del file firmato può essere eseguita con un qualunque strumento di verifica, tra cui il prodotto DigitalSign reader che può essere scaricato dal sito <http://www.praxis.unina.it>.
- In tal caso, saranno evidenziate a video, in chiaro, le informazioni riguardanti tutti i sottoscrittori del documento contenute nei loro certificati qualificati di firma.
- Un documento firmato e protocollato potrà altresì essere verificato direttamente con le funzionalità offerte, in modo integrato, dal sistema di **Protocollo Informatico**.





Informazioni sull'utilizzo della firma presso Unina

- Le istruzioni per l'utilizzo e la custodia del dispositivo sicuro di firma sono contenuti nel **"Manuale d'uso del servizio di firma digitale"**.
- Per maggiori dettagli sulle politiche dell'Ateneo in materia di utilizzo della Firma Digitale, si può fare riferimento al **Regolamento d'Ateneo** emanato con D.R. 4064 del 31.10.2006.
- Ulteriori informazioni, manuali, presentazioni, prodotti per download e link utili sono disponibili sul sito dell'eGovernment di Ateneo all'indirizzo:

<http://www.praxis.unina.it>





II PARTE

La gestione digitale dei verbali di Consiglio di Facoltà e di Giunta

Il processo di formazione dei verbali



Presidente di Facoltà e
Segretario

Redazione del verbale in formato
immodificabile e produzione del
documento in formato .pdf

Sottoscrizione congiunta con firma
digitale del verbale e degli allegati
da parte del Presidente e del Segretario.



Presidenza di Facoltà

Registrazione di protocollo dei
documenti firmati (.p7m) , con
assegnazione all'Ufficio Organi
Collegiali



Ufficio Organi Collegiali

Accesso alla propria "lista di lavoro"
e presa in carico del documento



La gestione informatica dei verbali (1/3)

- I verbali (di CdF e di Giunta) devono essere sottoscritti con firma digitale, a firma congiunta, dal Preside e dal Segretario.
- Il documento firmato digitalmente deve inoltre essere protocollato, in modo tale da risultare a data certa ed essere inoltre reso immediatamente disponibile all'Ufficio Organi Collegiali (che va riportato come destinatario unico della registrazione di protocollo).
- Non è più necessario allegare anche la nota di trasmissione del verbale stesso.
- In fase di redazione dei verbali si raccomanda di:
 1. utilizzare una nomenclatura standard e condivisa per la denominazione dei verbali (ad es: CDF-Fac-GGMMAAAA-v1.pdf), dove "fac" è l'identificativo breve di ciascuna Facoltà;
 2. inserire il codice identificativo del verbale su ciascuna pagina del documento stesso.





La gestione informatica dei verbali (2/3)

- A fronte di eventuali **successive modifiche** del verbale, va prodotto un nuovo file (cambiando il numero della versione del documento), nuovamente firmato digitalmente e, se la modifica non avviene nell'ambito della stessa giornata, riprotocollato. E' comunque opportuno riportare nelle note di registrazione un riepilogo delle variazioni rispetto alla precedente versione del documento.
- Se al verbale sono associati anche uno o più **documenti allegati**, vanno eseguiti i seguenti passi:
 1. Creazione di una cartella contenente tutti gli oggetti in formato **".pdf"** (singolarmente sottoscritti con firma digitale dal Preside e dal Segretario);
 2. Protocollazione del verbale come file primario ed inserimento di ciascun allegato nella registrazione di protocollo;
 3. Impostazione dell'Ufficio Organi Collegiali quale destinatario esclusivo della registrazione di protocollo.





La gestione informatica dei verbali (3/3)

- La Segreteria di Presidenza **conserva** gli allegati (cartacei) in versione originale.
- La **voce di classificazione** da adoperare in fase di registrazione di protocollo del verbale è la II-20 per il verbale di CdF, II-21 per il verbale di Giunta.
- Sia la Presidenza che l'Ufficio Organi Collegiali mantengono la **visibilità** sui documenti protocollati e possono effettuare, in qualunque momento, il salvataggio in locale, sul proprio PC, del file associato alla registrazione.
- I documenti associati alla registrazione (sia il verbale che gli allegati) sono in formato crittografico (.p7m): l'utente può quindi controllarne, tramite Protocollo Informatico, le informazioni aggiornate sulla **autenticità ed integrità** e le stesse informazioni relative al momento della registrazione.
- I documenti sono consultabili, oltre che in formato ".p7m" (in tal caso bisogna disporre di un programma di lettura idoneo), anche in formato ".pdf".





Un caso particolare

- Nel caso in cui il Preside o il Segretario debbano allontanarsi dall'aula, il verbale dovrà essere firmato anche dai soggetti chiamati a sostituire, temporaneamente, il Preside o il Segretario.
- In tal caso, nel testo del verbale dovrà essere chiaramente indicato, in corrispondenza dei punti discussi in assenza del Preside o del Segretario, il nominativo del sostituto.
- In calce al verbale, saranno quindi riportate le seguenti informazioni:
 - ✓ la dicitura "il presente documento è firmato digitalmente, per le parti di specifica competenza, da:"
 - ✓ a seguire, i nominativi, a stampa, dei firmatari: Preside, Segretario e sostituto/i
- Il verbale sarà quindi firmato digitalmente, a firme congiunte, da tutti i sottoscrittori.



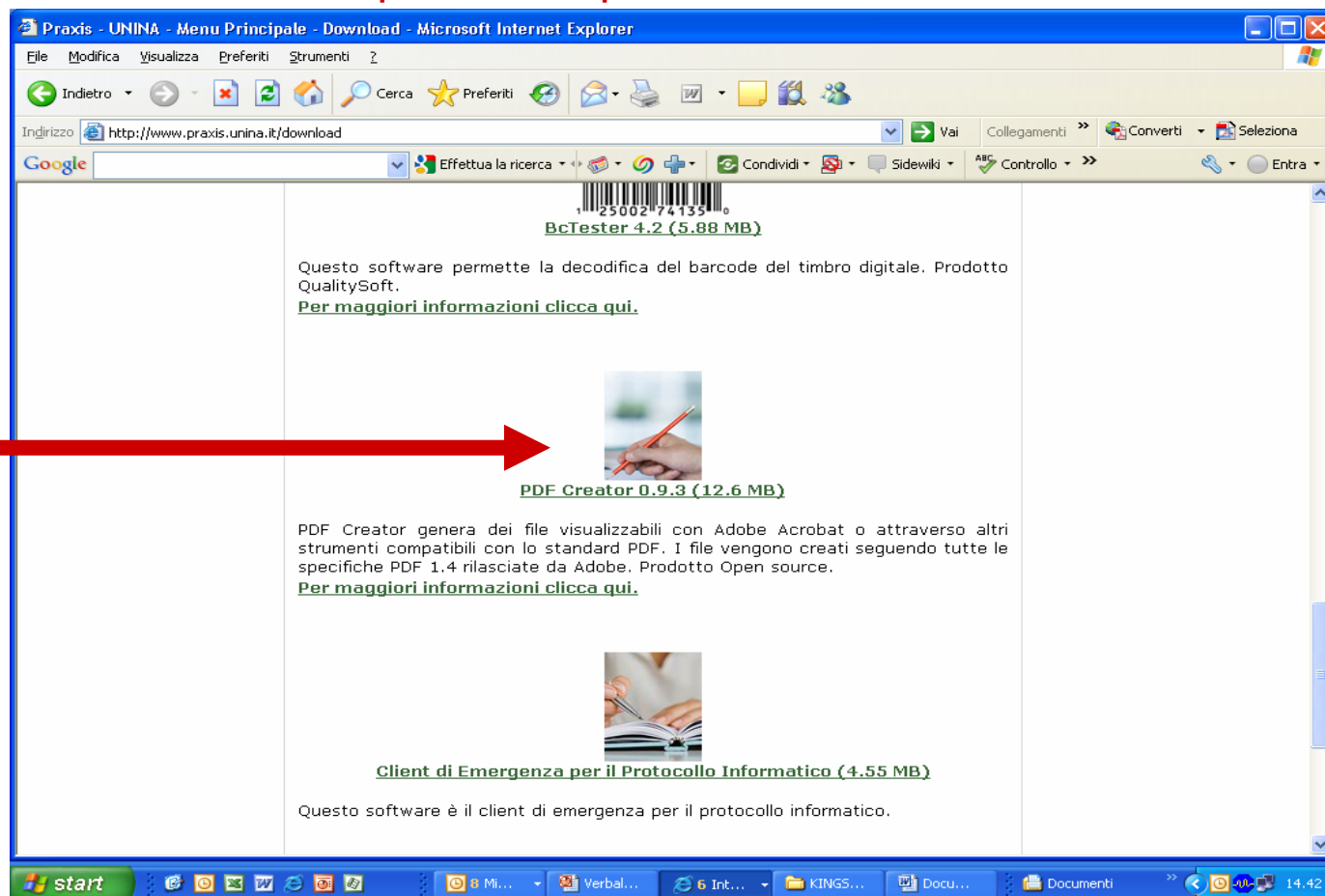


III PARTE

Mini-guida operativa

La creazione dei documenti da firmare

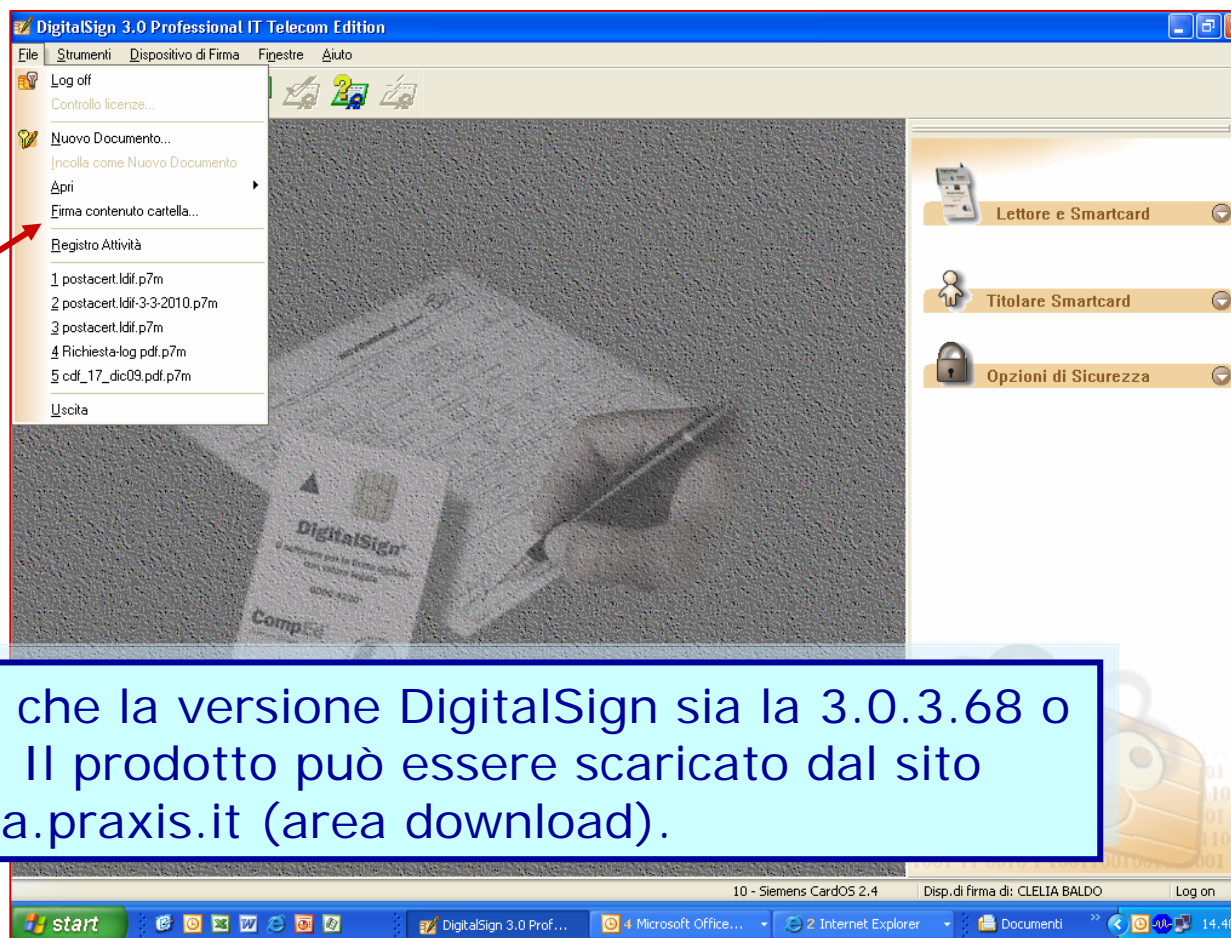
- Utilizzare prodotti per la creazione pdf. Eventualmente, è disponibile il link al prodotto Open Source "PDF Creator" all'indirizzo: <http://www.praxis.unina.it/download>



La firma digitale dei documenti (1/2)

- Utilizzare il prodotto Digital Sign Professional fornito con il kit di firma, inserendo il dispositivo di firma nella porta USB del PC.

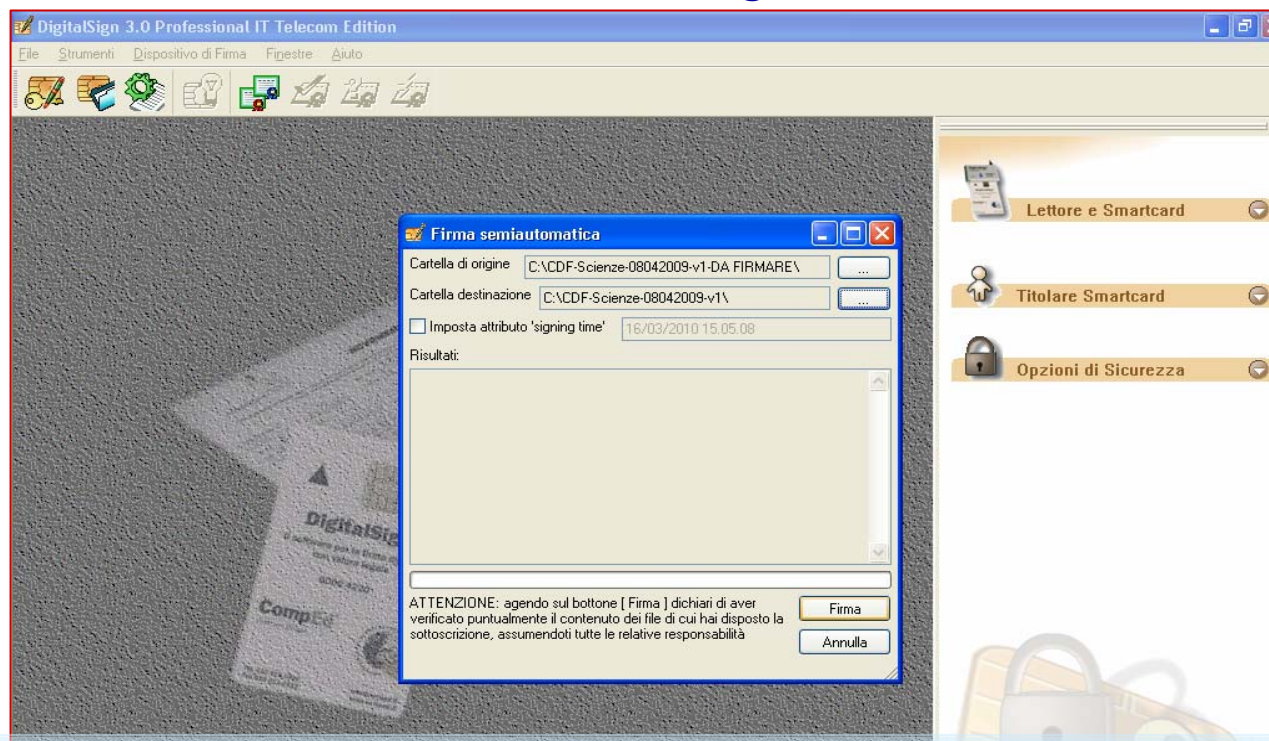
Dalla voce di menu "File" selezionare la voce "Firma contenuto cartella"



Accertarsi che la versione DigitalSign sia la 3.0.3.68 o superiore. Il prodotto può essere scaricato dal sito www.unina.praxis.it (area download).

La firma digitale dei documenti (2/2)

- Selezionare le cartelle di origine (file non firmati) e quella di arrivo (che conterrà tutti i file origine firmati)



La procedura sarà eseguita da ciascun sottoscrittore. Il secondo firmatario utilizzerà come cartella di origine quella contenente i documenti firmati dal primo firmatario.

La registrazione di protocollo (1/2)

- Il verbale dovrà essere registrato come file primario
- Gli allegati dovranno invece essere registrati nella sezione "Allegati"

primario

allegati

La procedura sarà eseguita da ciascun sottoscrittore. Il secondo firmatario utilizzerà come cartella di origine quella contenente i documenti firmati dal primo firmatario.

La registrazione di protocollo (1/2)

- Il verbale dovrà essere registrato come file primario
- Gli allegati dovranno invece essere registrati nella sezione "Allegati"

primario

allegati

**Gli allegati potranno essere molteplici.
L'organizzazione dei documenti nei file allegato va valutata caso per caso dalla Facoltà ed eventualmente condivisa con l'Ufficio Organi Collegiali.**



La registrazione di protocollo (2/2)

- E' possibile visualizzare l'esito del controllo di autenticità ed integrità dei documenti all'atto della registrazione di protocollo ed al momento della richiesta.
- I documenti possono essere riprodotti in formato "pdf" mediante la funzione del "timbro crittografico" che riproduce, sia in formato crittografico che in chiaro, la segnatura di protocollo dei documenti.
- Le eventuali modifiche ai documenti registrati – sia il primario che gli allegati – sono storicizzate, con indicazione di: data, ora, postazione che ha effettuato l'operazione e precedente versione del documento.





Documenti tecnici di riferimento

- Sul sito www.praxis.unina.it sono disponibili i seguenti manuali e guide operative:

Sezione Firma Digitale

- Manuale d'uso della Firma Digitale
- Configurazione del livello di sicurezza in DigitalSign

Sezione Protocollo Informatico

- Guida operativa al Protocollo Informatico
- Guida all'utilizzo del Timbro Digitale





Area download

- Sul sito www.praxis.unina.it, in area “Download”, sono inoltre disponibili i seguenti prodotti:
 - DigitalSign Professional (per i sottoscrittori), oppure Reader, per coloro che devono solo visualizzare i documenti firmati
 - PDFCreator per la generazione di file formato pdf
 - Analizzatore timbro crittografico per leggere in chiaro il codice apposto sui documenti protocollati





Riferimenti

Ambito	Riferimento
Procedimento amministrativo	Ufficio Organi Collegiali <i>email: organcoll@unina.it</i>
Utilizzo degli strumenti firma digitale e protocollo informatico	C.S.I. – Area tecnica eGovernment <i>email: egov@unina.it</i>
Supporto per la firma digitale	Incaricati_firma <i>email: firma.digitale@unina.it</i> <i>tel: 081.25 37747, 37048, 37743</i> <i>fax: 081.2537390</i>
Supporto operativo ed help desk	C.S.I. – Contact Center <i>email: www.contactcenter@unina.it</i> <i>PEC: www.contactcenter@pec.unina.it</i> <i>tel: 081.676799</i>

