

La firma digitale in Ateneo: Organizzazione del CDRL e linee guida per l'utilizzo della firma

Università degli Studi di Napoli Federico II

C.S.I. – Centro di Ateneo per i Servizi Informativi

Area tecnica eGovernment

Data ultimo aggiornamento: 21.7.2014

→

Il valore e la validità della firma digitale

- Ai sensi del CAD, il Codice dell'Amministrazione Digitale, il documento informatico sottoscritto con firma digitale:
 - soddisfa il requisito legale della forma scritta,
 - ha efficacia giuridico-probatoria.
- La firma digitale garantisce l'identificabilità dell'autore, l'integrità, l'immodificabilità del documento e il non ripudio del documento informatico sottoscritto.
- L'utilizzo del dispositivo di firma si presuppone riconducibile al titolare, salvo che questi dia prova contraria.
- L' Ateneo, in qualità di "terzo interessato", si avvale dei servizi offerti dal certificatore accreditato ARUBAPEC SpA.



La firma digitale - Generalità

- La firma digitale è basata su un procedimento di "crittografia asimmetrica" che fa uso di una coppia di chiavi: <u>una privata</u> (utilizzata per firmare) ed <u>una pubblica</u> (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 servizio firma digitale dell'Ateneo (1/2)

- L'Ateneo, in qualità di "terzo interessato", si avvale dei servizi offerti dal certificatore accreditato ARUBAPEC SpA.
- Il servizio si basa sulla organizzazione di una "Registration Authority" interna, denominata "Centro di Registrazione Locale (CDRL) ", costituita da amministrativi dell'Ateneo all'uopo nominati dal Rettore su indicazione dei Direttori di Dipartimento e quindi delegati dal Certificatore.
- I dispositivi sicuri di firma, contenenti la chiave crittografica di sottoscrizione ed il certificato del titolare, sono **SIM** all'interno di lettori di tipo "**token USB**".
- I certificati qualificati sono assegnati ai responsabili di struttura, ai docenti e ricercatori, ai dirigenti e capi ufficio o ad altri soggetti, secondo le indicazioni fornite dal Rettore e dal Direttore Generale.



Il servizio firma digitale dell'Ateneo (2/2)

- Il Regolamento di Ateneo (DR 4064 del 31.10.2006) in materia di Firma Digitale, definisce:
 - ✓ Regole per l'assegnazione, la sospensione e la revoca dei certificati da parte dell'Ateneo,
 - ✓ Compiti e responsabilità dell'Ateneo (nella figura della propria «Registration Authority» interna, nel seguito, «CDRL») nei confronti del Certificatore, e dei Titolari di certificato qualificato,
 - ✓ Diritti dell'Ateneo, in qualità di "terzo interessato" e adempimenti dei Titolari,
 - ✓ Regole per la sottoscrizione e la tenuta dei documenti amministrativi digitali



Il Centro Di Registrazione Locale (CDRL) UNINA (1/2)



Responsabile della gestione dei rapporti per lo svolgimento delle attività contrattuali: Il Direttore Tecnico dell'Area eGovernment del CSI

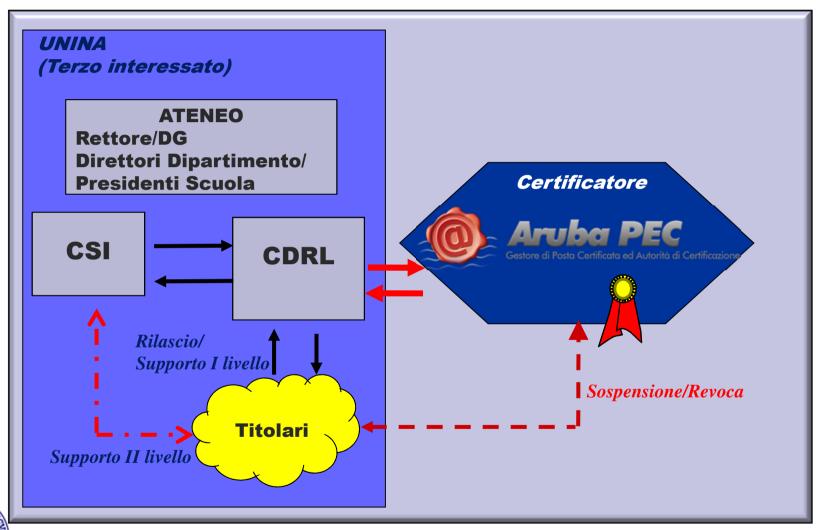
Operatori di Registrazione, preposti all'identificazione, registrazione dei titolari, emissione certificati e consegna dei kit: incaricati presso URP

Incaricati di Registrazione, preposti all'identificazione, registrazione dei titolari e consegna dei kit: incaricati presso dipartimenti o scuole

Direttore di Dipartimento/ Presidente di Scuola: compiti di vigilanza e garanzia del corretto operato dell'IR



Il Centro Di Registrazione Locale (CDRL) UNINA (2/2)





Il Centro Di Registrazione Locale (CDRL) (3/3)



CSI

 Responsabile CDRL, nella persona del Presidente

Amministrazione Centrale

 Operatori di Registrazione (ODR):

Dipartimenti e Scuole

 Incaricati di Registrazione (IR):

COORDINAMENTO CDRL

- RUP fornitura RDO97213
- Sviluppo sistemi per la gestione della firma digitale
- Sviluppo di applicazioni basate sulla firma digitale
- Supporto tecnico agli utenti

- Emissione certificati
- Supporto agli utenti
- Registrazione titolari e consegna kit
- Supporto agli utenti



L'emissione dei certificati in modalità «bulk»





La fase di registrazione e di consegna dei kit di firma (1/2)

- Gli IR presso ciascun dipartimento/scuola hanno a disposizione l'elenco dei titolari di firma;
- 2. Per ciascun titolare, all'atto della consegna, associano a ciascuna scheda contenente la SIM personalizzata la busta contenente: la scheda di registrazione, una copia del contratto e la busta oscurata con PIN/PUK;
- 3. La scheda di registrazione contenuta nella busta viene completata con gli estremi del documento di riconoscimento del titolare e sottoscritta dal titolare (4 firme: 3 per formule accettazione, 1 per attestazione consegna) e dall'IR;
- 4. Viene effettuata una fotocopia del documento di identità, del tesserino con il CF e della scheda di registrazione;
- 5. Se il documento di identità è una CIE, non è necessario allegare copia del documento;
- 6. E' ammissibile la patente emessa dalla Prefettura o dalla MCTC;
- 7. La copia della scheda di registrazione viene consegnata al titolare insieme al contratto, al box con il token e alla busta oscurata;
- 8. Le schede di registrazione sono inviate, a mezzo corriere, alla Arubapec.



La fase di registrazione e di consegna dei kit di firma (2/2)



Completamento modulo di registrazione e fotocopie D.I. e tesserino fiscale

Sottoscrizione del modulo da parte del titolare e dell'IR Consegna al titolare della copia del modulo di registrazione, del contratto, del kit e della busta con le credenziali

Trasmissione alla
ARUBAPEC delle schede di registrazione con fotocopie documenti



Le condizioni generali del contratto

- Definizione dei quattro ruoli: CA, Terzo interessato (Università), Committente (CSI), Utente;
- Contratto non a titolo oneroso tra CA e Utente;
- Il riferimento è all'accordo tra CA e CSI (RDO 97213) per la fornitura di 3200 kit di firme e relativi servizi;
- La durata dei certificati è pari a 6 anni, rinnovabili di ulteriori 6 anni;
- Un certificato può essere revocato:
 - Su indicazione dell'Ateneo,
 - Su richiesta del titolare,
 - Per volontà della CA;
- In ogni caso, viene informata anche la struttura di partenza;
- Foro competente: Napoli.



La consegna della documentazione alla ARUBA PEC

- A conclusione della consegna dei kit ai titolari del proprio dipartimento, ciascun IR:
 - predispone e sottopone alla firma del Responsabile della propria struttura la lettera di trasmissione, completa dell'elenco dei nominativi dei docenti;
 - Acquisisce l'immagine dei contratti e dei relativi documenti di identità e CF;
 - Richiede la registrazione della lettera con allegato il file contenente le immagini dei contratti. La registrazione è indirizzata, in cc, anche al CSI.
- L'indirizzo ARUBA PEC per la spedizione, a mezzo corriere, di tutta la documentazione cartacea in originale, è:

Aruba PEC c/o Visal Srl Archivio CDRL Via Don Milani, 5 52010 Soci (AR)



Il sito Praxis per l'eGovernment

Indirizzo: http://www.praxis.unina.it/





La sospensione/revoca dei certificati (1/2)

CA

 Comunica l'avvenuta revoca all'l'interessato e al CDRL. Il CDRL informa la struttura di afferenza.

Titolare

 Comunica la richiesta di revoca/sospensione alla CA e informa il CDRL e la propria struttura di afferenza. In ogni caso, la richiesta viene notificata al CDRL anche dalla CA. Il CDRL si attiva per la eventuale ri-emissione del certificato.

CDRL

• Procede su indicazione dell'Ateneo (ad es, nel caso di conclusione del rapporto di lavoro) e ne dà comunicazione anche alla struttura di afferenza del titolare.



La sospensione/revoca dei certificati (2/2)

- Istruzioni disponibili all'indirizzo:
 http://www.praxis.unina.it/firma-digitale-Sospensione-Revoca
 - Modalità per il Titolare di richiesta sospensione/revoca:
 - Richiesta scritta su apposito modulo ARUBAPEC firmata dal Titolare e inviata per mail o fax alla ArubaPEC, eventualmente anticipata telefonicamente;
 - On line, mediante collegamento al sito ArubaPEC https://lcm.arubapec.it/lcm/.
- In ogni caso, l'interessato informa il CDRL, per il tramite dell'IR di riferimento, dell'avvenuta richiesta di sospensione del certificato.



Caratteristiche della Unina Key

- E' il nuovo dispositivo **USB** di Firma digitale scelto dall'Università degli Studi di Napoli "Federico II".
- Non necessita di installazione hardware o software (driver e/o applicazioni).
- E' un dispositivo portatile facile da utilizzare su qualunque PC (desktop, laptop).
- Integra una Smart Card in formato SIM (analoga a quella del telefono cellulare), un lettore di Smart Card ed una memoria Flash di capacità pari a 4 Gbyte.
- Contiene, oltre al certificato per la firma digitale, anche un certificato elettronico di autenticazione.
- L'aggiornamento del software sulla Unina Key avviene in modo automatico.
- Il rinnovo del certificato è eseguito dal titolare stesso, via web.



La gestione del certificato di firma

- Il PIN e il PUK possono essere modificati dal Titolare.
- 5 tentativi (ripetuti) di immissione PIN errato, bloccano la carta. Per lo sblocco, va utilizzato il PUK.
- 5 tentativi (ripetuti) di immissione PUK errato, bloccano la carta in modo definitivo.
- Il Titolare deve sospendere/revocare il proprio certificato di firma in caso di smarrimento, furto, sospetta manomissione del dispositivo.
- La CA o il CDRL possono richiedere la sospensione o la revoca di certificati nei casi di cui all'art. 17 delle Condizioni Generali di Contratto.



I prerequisiti

Sistemi Operativi supportati

- MS Win XP, MS Vista, MS Win 7, MS Win 8 (32 e 64 bit)
- MS Server 2003 MS Server 2008 (32 e 64 bit)
- Mac OS X Tiger Mac OS Leopard Mac OS Snow Leopard MAC OS Lion – Mac OS Mavericks
- UBUNTU

Java

Le versioni Java compatibili sono la 1.6 e versioni successive

Browser

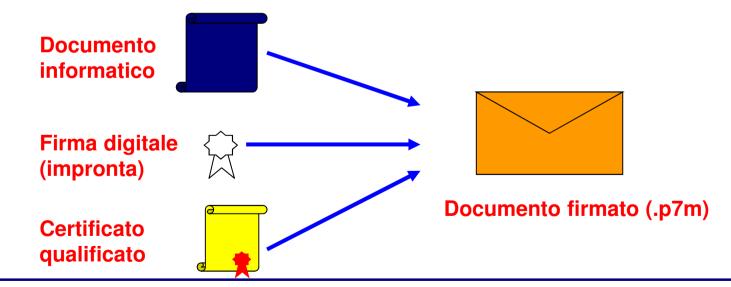
- Explorer
- Chrome (su MAC solo con Java 7)
- Mozilla-Firefox
- Safari



La struttura di un documento firmato digitalmente

Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il file firmato, cioè la busta, contiene al suo interno:

- il documento informatico nel formato originale,
- la firma digitale calcolata sull'impronta del documento,
- il certificato qualificato del sottoscrittore.



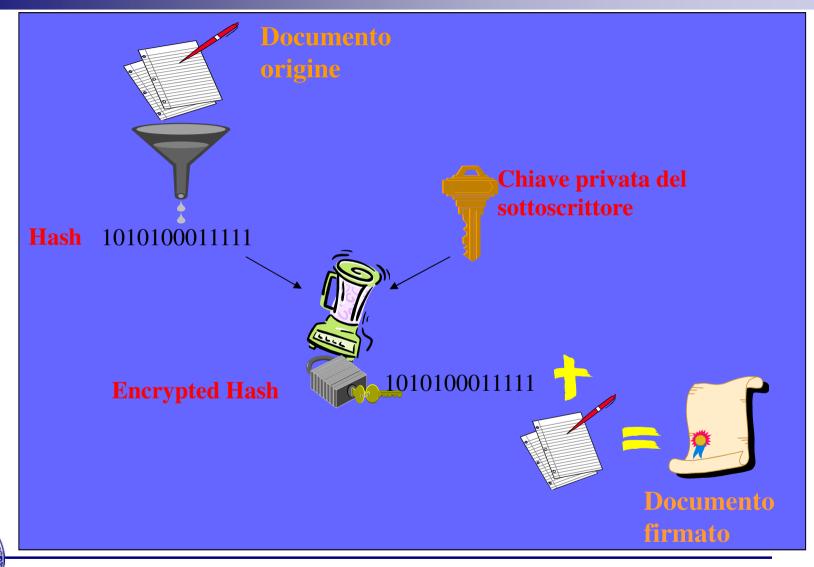


Il processo di apposizione della firma digitale (1/2)



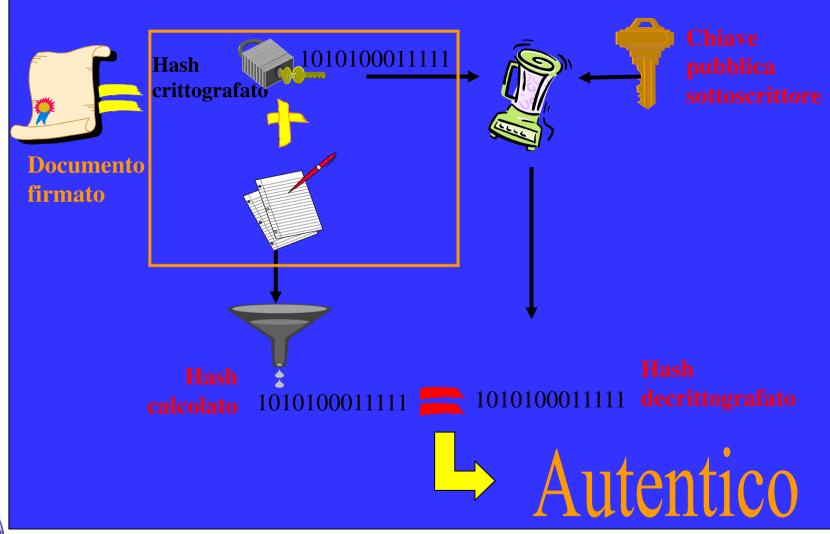


Il processo di apposizione della firma digitale (2/2)





Il processo di verifica della firma digitale (2/2)

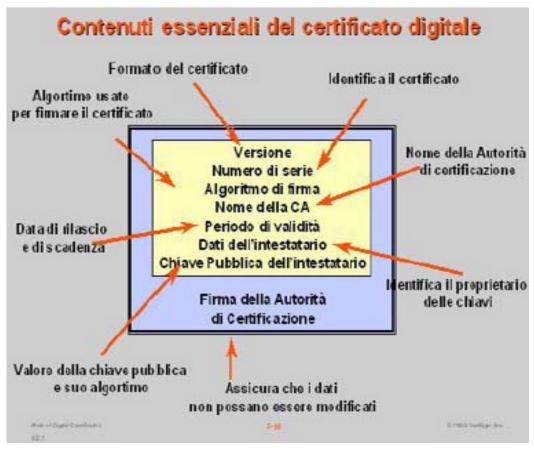




Il certificato qualificato

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

pubblica:





Come verificare la firma digitale

- La verifica di autenticità e di integrità del file firmato può essere eseguita:
 - con un qualunque strumento di verifica di libera e gratuita disponibilità quale, ad esempio, DigitaSign reader, Dike, etc.
 - utilizzando la funzionalità «Verifica» disponibile sulla UNINAKEY.





Il certificato per l'autenticazione ai servizi in rete

- A bordo delle SIM è presente anche un certificato «CNS like» per l'autenticazione dei titolari ai servizi informatici dell'Ateneo.
- Il dispositivo è compatibile con quelli previsti dall'art. 64 comma 2 del Codice per l'Amministrazione Digitale (CAD) per l'accesso ai servizi in rete della PA e contiene, tra gli altri dati, i codice fiscale del titolare della carta e la denominazione dell'Università quale terzo interessato.
- Ai sensi dell'art. 65 del CAD, le istanze e le dichiarazioni presentate dagli interessati per via telematica siano valide ed equivalenti alle istanze e dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento se i richiedenti si autenticano al sistema informativo dell'Ateneo utilizzando tale certificato digitale di autenticazione.



La gestione dei documenti digitali

Formazione (O.A. o sistemi istituzionali) Sottoscrizione con firma digitale

Registrazione nell'archivio digitale dell'Ateneo

Archiviazione e conservazione



Le due modalità per l'apposizione della firma

CASO A

I documenti informatici "gestionali", creati cioè da procedure istituzionali, sono firmati digitalmente dall'utente mediante il sistema di firma digitale centralizzato (Confirma). Esempi: Verbale digitale di esame, Mandato di pagamento elettronico, etc.

CASO B

I documenti informatici ^(*) "locali" sono firmati digitalmente mediante un'applicazione software (es: Aruba key o DigitalSign), eseguita sulla postazione dell'utente. Esempi: Decreti, Verbali del Consiglio di Dipartimento, RdO MEPA, AVCP, PRIN, etc.



(*) **Documento informatico:** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Caso A: firma dei documenti gestionali

- Va verificata la preventiva installazione Java.
- Va eseguito, preventivamente e solo una volta, l'import del certificato contenuto nel dispositivo Aruba Key.



■ Per gli utenti MAC: la password richiesta per l'import del certificato è quello di login al sistema.



Caso A: l'applet di firma CONFIRMA

■ All'atto della richiesta di apposizione firma, viene avviato il processo di firma e compare, quindi, la finestra dell'applet:



■ Il docente, dopo aver selezionato la funzionalità «firma digitale», dovrà solo apporre il proprio PIN.



Caso B: Firmare un file con Unina Key

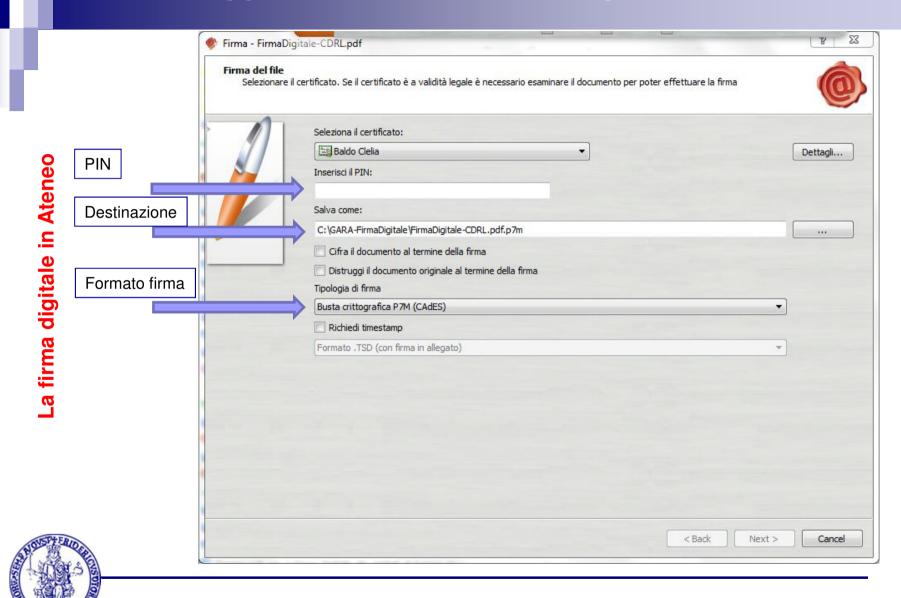
- Con Unina KEY è possibile apporre la firma digitale anche su intere cartelle di file (contenenti anche file già firmati digitalmente).
- E' sufficiente selezionare il file o la cartella e trascinare quanto selezionato sul pulsante "Firma".



- Il documento deve essere, salvo casi eccezionali, in formato pdf.
- Il formato del file firmato deve essere il «Cades» (estensione p7m).



Caso B: l'apposizione della Firma digitale



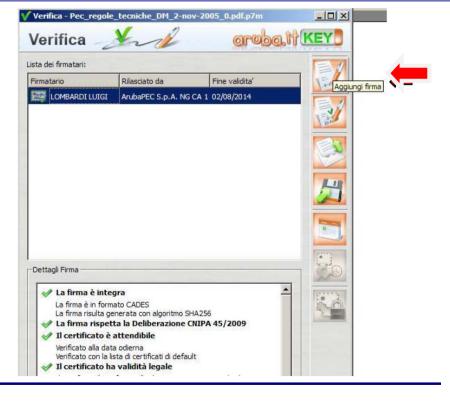
Caso B: firma multipla di tipo parallelo

Se il file è già firmato digitalmente, la funzione da utilizzare è quella di

firma multipla:

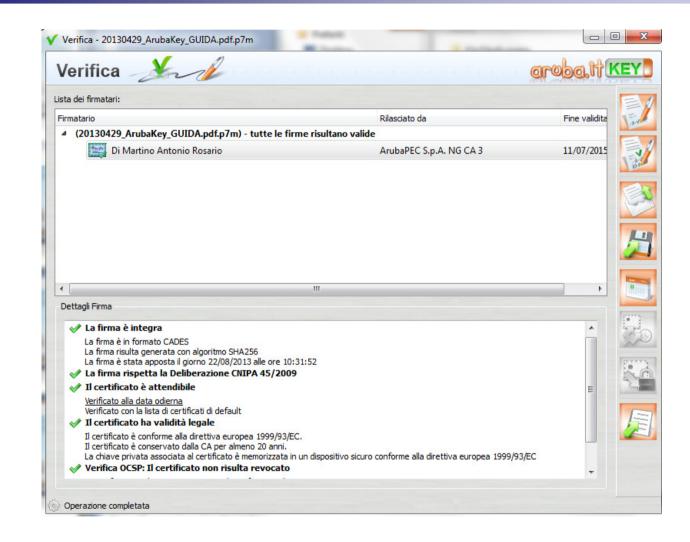


Nella schermata che appare va quindi selezionato il pulsante «Aggiungi firma» che consente di apporre una firma parallela.





Caso B: la verifica di un file firmato digitalmente





L'inoltro di segnalazioni al CSI

 In caso di malfunzionamento del sistema di firma digitale o richiesta di supporto tecnico relativamente all'uso della firma digitale, è possibile inviare una segnalazione al CSI tramite il sistema CERDI

Ticket:



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

GESTIONE CERTIFICATI DI FIRMA DIGITALE

http://www.cerdi.unina.it







Informazioni utili

- Guide, Procedure Operative e Modulistica si trovano all'indirizzo www.praxis.unina.it, sezione Firma Digitale.
- Supporto Tecnico: CSI-Area tecnica eGovernment (egov@unina.it).



