

Servizi per l'e-government nell'università Federico II

Alcune informazioni utili per i titolari di Kit di firma digitale ARUBAKEY/UNINAKEY

COME SI RICHIEDE UN KIT PER LA FIRMA DIGITALE

Per poter richiedere il proprio certificato di firma è necessario presentarsi presso l'Ufficio URP per consentire il riconoscimento "de visu" e consegnare agli Incaricati Firma del Centro di Registrazione Locale dell'Università, la seguente documentazione:

1. **Il modulo di registrazione**, disponibile sul sito Praxis all'indirizzo <http://www.praxis.unina.it/firma-digitale-richiesta>, da compilarsi in ogni sua parte **all'atto della consegna** (se ne consiglia comunque la compilazione presso l'URP).
2. **Copia FRONTE/RETRO di un documento d'identità**, in corso di validità (passaporto, carta d'identità, patente auto). Nel caso in cui la residenza riportata del documento d'identità non coincida con l'attuale residenza indicata nella sezione "Dati del richiedente" contenuta nel modulo di richiesta, allegare certificato di cambio di residenza oppure relativa autocertificazione.
3. **Copia del codice fiscale** (riportato anche sulla tessera sanitaria e sulla carta d'identità elettronica)

RECAPITI DEGLI INCARICATI FIRMA

Dott. Gennaro Mocerino, CapoUfficio U.R.P., Responsabile Adempimenti Firma Digitale	081 2537216
Dott. Giuseppe De Biase	081 2537269
Dott. Nicola Marti	081 2537225
Dott. Antonio Scannapiecoro (presso l'UPDR, Palazzo degli Uffici, IV piano, Via G.C. Cortese, 29)	081 2537747

E-mail: firma.digitale@unina.it

Sede: Ufficio Relazioni con il Pubblico (fax **081 2537390**) – **Corso Umberto I (Sede rettorato), IV piano**

SUPPORTO PER UTILIZZO FIRMA DIGITALE - RIFERIMENTI CSI

- Documentazione e modulistica disponibile sul sito eGovernment: <http://www.praxis.unina.it>
- Direttore tecnico area eGovernment: dott.ssa Clelia Baldo (tel. **081.2537019**; e-mail cbaldo@unina.it)
- Per attivazione nuovi servizi basati su firma digitale, e-mail area tecnica eGovernment: egov@unina.it
- Per supporto ed assistenza, inviare una segnalazione al CSI mediante l'applicazione al seguente indirizzo: <http://www.cerdi.unina.it/Ticket>

INFORMAZIONI DI CARATTERE GENERALE

1. I certificati digitali (di firma digitale e di autenticazione) contenuti nella chiavetta ARUBAKEY/UNINAKEY hanno **validità pari a sei anni**. E' cura dell'interessato richiederne, prima della scadenza, il **rinnovo** (per ulteriori 6 anni) seguendo le indicazioni disponibili sul sito <http://www.praxis.unina.it>.
2. Le guide all'utilizzo del dispositivo (per Windows e per MAC) sono reperibili all'indirizzo: <http://www.praxis.unina.it/firma-digitale-guide-manuali>.
3. Le chiavette sono pre-installate per ambiente **Windows** e **MAC**. Gli utenti, prima di usare il token di firma, sono pregati di seguire le istruzioni contenute nel manuale "**ArubaKey-Installazione**", pubblicato all'indirizzo di cui al punto 2.
4. Il **PIN** fornito nella busta oscurata può essere modificato dal Titolare, mediante l'utilizzo del comando "Gestione Carta" – "**Cambio PIN**" disponibile tra le applicazioni installate sul dispositivo ARUBAKEY, come riportato nel manuale "**Guida rapida ARUBAKEY**" pubblicato all'indirizzo di cui al punto 2.
5. Quando si utilizza la chiave di firma, se il PC è in rete, viene effettuato - in automatico - l'**aggiornamento** del software di firma. Tale operazione può richiedere anche alcuni minuti.
6. Per produrre un file con estensione **".p7m"**, assicurarsi, prima di apporre una firma digitale, di aver selezionato come "**Tipologia di firma**" il formato "**Busta crittografica p7m (Cades)**". In caso contrario, se il file da firmare è .pdf, il software appone la firma in formato pdf.