U.S.R. Decreto n. 4064

IL RETTORE

VISTO lo Statuto dell'Ateneo;

VISTA la legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi, e sue successive modifiche ed integrazioni;

VISTA il d.P.R. 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

VISTO il D. Lgs. n. 165 del 30 marzo 2001, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

VISTO il D.Lgs. n. 10 del 23 gennaio 2002 che detta norme di attuazione della Direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;

VISTO il D.Lgs. n. 196 del 30 giugno 2003, recante il codice in materia di protezione dei dati personali;

VISTO il D.Lgs. n. 82 del 7.3.2005 che disciplina il "*Codice dell'amministrazione digitale"*;

VISTO il D.Lgs. n. 159 del 4.4.2006 recante disposizioni integrative e correttive al decreto legislativo 7.3.2005, n. 82;

VISTA la delibera n. 3 del 24.10.2006 con la quale il Senato Accademico ha approvato il *Regolamento di Ateneo in materia di firma digitale;*

DECRETA

E' emanato il *Regolamento di Ateneo in materia di firma digitale* e l'allegato 1 che ne costituisce parte integrante.

Il Regolamento entra in vigore il giorno successivo a quello della sua pubblicazione all'Albo Ufficiale dell'Università.

Napoli, 31 ottobre 2006

IL RETTORE
Guido TROMBETTI

ADP

Regolamento di Ateneo in materia di firma digitale

1
Oggetto e finalità del Regolamento

1. Il presente regolamento disciplina le modalità di gestione e di utilizzo della firma digitale nell'ambito della Università degli Studi di Napoli Federico II - da questo punto in avanti denominata “Ateneo” - nel rispetto del quadro normativo stabilito dalle seguenti fonti legislative: Direttiva 13 dicembre 1999 n. 1999/93/CE; D.P.R 28 dicembre 2000, n. 445; D. Lgs. 7 marzo 2005, n. 82 e successive modifiche, di seguito denominato “Codice”.

2. Le norme che seguono definiscono:
   - l’organizzazione interna del servizio di assegnazione, sospensione e revoca dei certificati da utilizzare per la sottoscrizione in forma elettronica dei documenti informatici di cui al successivo art. 2.
   - le regole e l’ambito di applicabilità della sottoscrizione dei documenti informatici con firma digitale.

2
Documenti informatici e firma digitale

1. L’Ateneo, in linea con la normativa vigente e con gli indirizzi strategici in materia di *e-government,* avvalendosi delle proprie infrastrutture tecnico-organizzative per la informatizzazione dei processi amministrativi e per il miglioramento dei servizi, promuove la produzione e la circolazione al suo interno e verso l’esterno di documenti informatici, al fine di semplificare le procedure, riducendo i tempi e i costi dell’azione amministrativa.

2. Il documento informatico sottoscritto con firma digitale, purché formato nel rispetto delle regole tecniche sancite dalla normativa vigente, soddisfa il requisito legale della forma scritta e ha valore ed efficacia probatoria, opponibile ai terzi, di piena prova della provenienza delle dichiarazioni, fino a querela di falso intentata dal sottoscrittore, ai sensi dell’art. 20, comma 2 e dell’art. 21, comma 2, del Codice.

3. Ai sensi dell’art. 34, comma1, lettera b) del Codice, l’Ateneo si avvale del servizio di firma digitale erogato da un Ente accreditato presso il CNIPA ed iscritto all’elenco dei certificatori pubblici. I contratti di fornitura del servizio saranno stipulati nel rispetto della legislazione vigente in materia e delle norme del presente Regolamento.

4. Il documento informatico ricevuto da un ente o soggetto esterno o spedito dall’Ateneo ad un ente o soggetto esterno, ai sensi dell’art. 53, comma 5, del D.P.R. 445/2000, deve essere protocollato mediante il sistema del protocollo informatico ed includere (art. 55, comma 4, del D.P.R. 445/2000) la segnatura di protocollo che può contenere tutte le informazioni di registrazione del documento. Inoltre, se l’invio è verso un’altra amministrazione pubblica, il documento informatico deve essere obbligatoriamente sottoscritto con firma digitale.

5. La trasmissione dei documenti informatici sottoscritti con firma digitale deve essere eseguita mediante PEC (Posta Elettronica Certificata) in tutti i casi in cui sia necessario disporre di ricevute, opponibili ai terzi, di invio e di avvenuta consegna, oppure sia necessario scambiare informazioni e documenti con soggetti che hanno avanzato esplicita richiesta di utilizzare tale modalità.

3
Definizioni

1. In conformità con il Codice ed ai fini del presente Regolamento si intende per:

a) *certificato elettronico*: l'attestato elettronico che collega i dati utilizzati per verificare la firma elettronica all'identità del titolare;
b) *certificato qualificato, di seguito denominato "certificato":* il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
c) *certificatore accreditato, di seguito denominato "Certificatore"*: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime, che è in possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ed è accreditato presso il CNIPA, ai sensi dell'art. 29 del Codice;
d) *chiave privata*: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico; la chiave è custodita su un dispositivo sicuro di firma, il cui uso è possibile previa immissione di un codice di sblocco (PIN);
e) *chiave pubblica*: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche; l'elenco delle chiavi pubbliche rilasciate e valide è pubblicato a cura del certificatore che ha emesso il certificato;
f) *documento informatico*: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
g) *firma elettronica*: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
h) *firma elettronica qualificata*: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;
i) *firma digitale*: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

j) *titolare*: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
k) *validazione temporale*: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

4
Soggetti interessati

1. Agiscono nel processo di assegnazione e gestione dei dispositivi di firma digitale:

   a. l'Ateneo che, in qualità di "terzo interessato", richiede il rilascio del certificato a favore del titolare, fornisce informazioni e certificazioni per ciò che attiene alle deleghe, al ruolo e alle funzioni istituzionali dei dipendenti eventualmente da riportare sul certificato ed ha la facoltà, ai sensi dell'art. 36, comma 1, lettera c) del Codice, di richiedere la sospensione o la revoca del certificato;

   b. il Certificatore, nella duplice funzione di responsabile del rilascio, della pubblicazione e della tenuta del certificato, nonché di responsabile della identificazione della persona che fa richiesta della certificazione;

   c. il titolare, inteso come il dipendente dell'Ateneo o il soggetto al quale, per disposizione del Rettore o del Direttore Amministrativo, adottata anche in ragione del ruolo istituzionale e della funzione di cui egli è investito, sia assegnato il certificato per la firma digitale;

   d. gli incaricati del servizio di firma digitale, d'ora in avanti denominati incaricati_firma, individuati e nominati dal Direttore Amministrativo e responsabili, su delega del Certificatore, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati e della consegna di dispositivi e codici per l'utilizzo del servizio di firma digitale.

5
Obblighi e responsabilità del Certificatore

1. Le responsabilità del Certificatore sono sancite dall'art. 30, comma 1 del Codice.

2. Nel rispetto del disposto dell'art. 32, comma 3 del Codice, ai fini del presente Regolamento, sono obblighi cui impegnare il Certificatore nei contratti di fornitura quelli di seguito specificati:

   a. identificazione della persona a cui rilasciare il certificato, restando il Certificatore responsabile di detta identificazione anche quando effettuata materialmente da terzi, su delega del Certificatore medesimo;

   b. attivazione della procedura per il rilascio del certificato;

c. attivazione della procedura per la revoca o la sospensione del certificato;

d. rilascio, pubblicazione e tenuta del certificato nel rispetto delle regole tecniche di cui all'art. 71 del Codice e nel rispetto della normativa in materia di tutela della privacy;

e. conformità delle informazioni contenute nel certificato a quelle previste nell'art. 28 comma 1 del Codice, ad esclusione dell'uso dello pseudonimo;

f. impostazione dell'informazione relativa al nome dell'organizzazione di cui fa parte il titolare con la denominazione "Università degli Studi di Napoli Federico II";

g. accettazione delle comunicazioni riguardanti il modificarsi o il venir meno delle informazioni inserite nel certificato, ai sensi del citato art. 28 del Codice, richieste esclusivamente dall'Ateneo;

h. tempestiva pubblicazione della revoca e della sospensione del certificato, con riferimento ai casi di cui al successivo art. 8;

i. tenuta della registrazione di tutte le informazioni relative al certificato dal momento della sua emissione per un periodo di almeno venti anni.

6
Obblighi del titolare

1. Il titolare del certificato di firma digitale è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che egli utilizzerà solo personalmente e per ragioni istituzionali.

2. Il titolare è tenuto ad informare immediatamente gli incaricati_firma di ogni circostanza che, ai sensi del successivo art. 8, renda necessaria o comunque opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnati; deve altresì informare tempestivamente gli incaricati_firma di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

3. Al rispetto dei suddetti obblighi e delle modalità di utilizzo della firma digitale stabilite dalla normativa vigente il titolare si impegna con dichiarazione scritta resa agli incaricati_firma, su modulo all'uopo predisposto, all'atto della consegna dei dispositivi di firma.

7
Compiti e responsabilità degli incaricati_firma

1. Gli incaricati_firma provvedono a:
   a. gestire e aggiornare gli elenchi dei titolari di certificato;
   b. svolgere l'attività istruttoria interna necessaria affinché il Certificatore soddisfi le richieste di assegnazione, di revoca o di sospensione dei certificati, comprensiva degli adempimenti, per conto dell'Ateneo, per la tutela dei dati personali dei titolari dei certificati, ai sensi del D.Lgs. 196/2003;
   c. fornire istruzioni ai titolari sul corretto utilizzo del servizio di firma digitale.

Gli incaricati_firma sono inoltre formalmente delegati dal Certificatore a svolgere i seguenti adempimenti:

a. identificare le persone fisiche all'atto della registrazione, in ottemperanza a quanto disposto dalla normativa vigente in materia di tutela dei dati personali;
b. consegnare a ciascun titolare il dispositivo sicuro di firma ed i codici riservati.

2. I compiti degli incaricati_firma sono descritti analiticamente nel *"Manuale d'uso del servizio di firma digitale"* che la Direzione Amministrativa dell'Ateneo, a seguito di stipula di contratto di fornitura di certificati, predispone di concerto con il Certificatore, in linea con il manuale di gestione del servizio dovuto dal Certificatore medesimo. In detto manuale d'uso interno sono descritte nel dettaglio le modalità operative di erogazione e di fruizione del servizio di firma digitale, coerentemente con l'elenco delle principali fasi procedimentali riportato nell'allegato 1, che è parte integrante del presente regolamento.

3. I contratti di fornitura di certificati devono prevedere espressamente la delega dal Certificatore agli incaricati_firma.

8
Revoca e sospensione

1. La revoca di un certificato determina la cessazione anticipata della sua validità e può intervenire su iniziativa del Certificatore, del titolare oppure dell'Ateneo.

2. La revoca deve essere richiesta dall'Ateneo, quale terzo interessato, al Certificatore tutte le volte che ricorra almeno una delle seguenti cause:

   a) cessazione del rapporto di lavoro del dipendente per qualunque causa;
   b) venir meno, per qualunque causa, dei requisiti di ruolo, qualifica o funzioni istituzionali che ne motivavano l'assegnazione;
   c) perdita di possesso del dispositivo sicuro di firma;
   d) sospetta falsificazione o abusi.

3. La sospensione di un certificato determina l'interruzione temporanea della sua validità e può intervenire su iniziativa del Certificatore, del titolare oppure dell'Ateneo.

4. La sospensione deve essere richiesta dall'Ateneo, quale terzo interessato, al Certificatore tutte le volte che ricorra almeno una delle seguenti cause:

   a) richiesta di revoca da parte degli interessati motivata dalla possibile, ma non certa, compromissione della chiave privata;
   b) sospetta perdita di segretezza del codice di sblocco del dispositivo sicuro di firma;
   c) qualunque causa che determini il temporaneo venir meno di uno o più requisiti che ne motivavano l'assegnazione, ivi compresa la sospensione dal servizio del dipendente che ne è titolare.

5. Ai sensi e per gli effetti dell'art. 36, comma 3, del Codice, la revoca o la sospensione del certificato, qualunque ne sia la causa, hanno effetto dal momento della pubblicazione della lista, rispettivamente, dei certificati revocati o sospesi che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

9
L'uso della sottoscrizione con firma digitale in Ateneo

1. Nell'ambito delle attività didattico-scientifiche, tecniche ed amministrative dell'Ateneo, i documenti da inviare all'esterno o all'interno dell'Ateneo possono essere in forma cartacea ovvero informatica. I documenti informatici, per soddisfare il requisito legale della forma scritta, devono essere obbligatoriamente sottoscritti con firma digitale.

2. I documenti informatici prima di essere sottoscritti con firma digitale devono essere registrati in formato "pdf" e devono riportare in calce, in chiaro, il ruolo, il nome ed il cognome del sottoscrittore e la data.

3. Per quanto attiene alla obbligatorietà del protocollo informatico ed alla necessità di utilizzo della Posta Elettronica Certificata, si rinvia a quanto disciplinato dal precedente art. 2.

10
Trattamento dei dati personali

1. Ai sensi del "Regolamento di attuazione del codice in materia di protezione dei dati personali", emanato con D.R. n. 5073 del 30.12.2005, l'Ateneo è il titolare, per il perseguimento dei propri fini istituzionali, tra gli altri, del trattamento dei dati personali connesso alla gestione dei certificati.

2. L'Ateneo, in qualità di terzo interessato richiedente i certificati, ai sensi di quanto disposto nell'art. 28 del Codice, tratta i dati personali degli interessati, secondo i principi di liceità, pertinenza, non eccedenza e necessità, comunicandoli al Certificatore, previa consegna dell'informativa agli interessati, per consentire i successivi adempimenti.

11
Entrata in vigore

1. Il presente regolamento entra in vigore il giorno successivo a quello della sua pubblicazione all'Albo ufficiale dell'Università.

Napoli, lì 31 ottobre 2006

IL RETTORE
Guido TROMBETTI

Allegato 1 al *"Regolamento di Ateneo in materia di firma digitale"*

Si riportano nel seguito, in sintesi, le principali fasi procedimentali che, in conformità con il quadro normativo vigente, il *"Manuale d'uso del servizio di firma digitale"* di cui all'art. 7 del presente Regolamento, dovrà in ogni caso prevedere per la gestione dei certificati.

Atti preparatori per la assegnazione di certificati

- **individuazione dei titolari**: il Rettore o il Direttore Amministrativo, a seconda delle rispettive competenze, dispone la richiesta per il primo rilascio, il rinnovo, la sospensione o la revoca dei certificati per la firma digitale;
- **predisposizione del modulo di registrazione e stampa delle condizioni generali della fornitura:** acquisito il provvedimento di cui sopra, gli incaricati_firma predispongono il modulo di registrazione e la stampa delle condizioni generali della fornitura e del consenso al trattamento dei dati personali connessi all'erogazione del servizio di gestione della firma digitale.

Atti preparatori per il rinnovo di certificati

- **individuazione certificati in scadenza:** gli incaricati_firma individuano, con frequenza mensile, i certificati la cui data di scadenza è compresa entro i trenta giorni solari successivi e, verificata la non sussistenza di condizioni per la sospensione o la revoca degli stessi, richiedono alla Direzione Amministrativa autorizzazione formale per il rinnovo dei certificati;
- **richiesta di rinnovo:** ottenuta l'autorizzazione, le operazioni da effettuare sono le stesse di quelle in precedenza riportate per l'assegnazione.

Identificazione e registrazione nel caso di assegnazione o di rinnovo del certificato

- **identificazione dell'interessato**: gli incaricati_firma identificano il richiedente mediante il controllo di un valido documento di riconoscimento esibito dal richiedente stesso;
- **richiesta di registrazione:** l'interessato riceve dagli incaricati_firma l'informativa riguardante il trattamento dei dati personali effettuato dall'Ateneo e quindi, alla presenza di un incaricato_firma (che controfirma), sottoscrive:
    a. il consenso per il trattamento dei suoi dati personali da parte del Certificatore,
    b. la richiesta di registrazione.

  Tali documenti sono trasmessi dagli incaricati_firma al Certificatore, secondo le modalità concordate con il Certificatore medesimo;
- **registrazione:** gli incaricati_firma provvedono, secondo le modalità e le regole tecniche stabilite dal Certificatore, alla registrazione che consente l'avvio della successiva fase di generazione delle chiavi e di emissione del certificato da parte del Certificatore;

- **chiusura registrazione**: gli incaricati_firma consegnano all'interessato il codice di registrazione, una copia del modulo di registrazione ed una copia delle condizioni generali del servizio. L'interessato deve attestare, firmando un apposito modulo, di aver ricevuto la suddetta documentazione;
- **ricezione del dispositivo sicuro di firma**: nel caso in cui la richiesta di emissione/rinnovo sia approvata dal Certificatore, gli incaricati_firma ricevono dal Certificatore il kit per l'apposizione della firma digitale costituito da: il dispositivo sicuro di firma (smart card o token USB) e, in busta chiusa, il codice segreto di attivazione del dispositivo stesso (pin), quello di sblocco del dispositivo (puk) e, se è il caso, il lettore di smart card;
- **consegna del dispositivo sicuro di firma**: gli incaricati_firma consegnano al titolare del certificato il kit per l'apposizione della firma digitale. Il titolare sottoscrive quindi una dichiarazione in cui attesta l'integrità della busta contenente il pin, e sottoscrive altresì la dichiarazione di responsabilità di cui al comma 3 dell'art. 6 del Regolamento. Gli incaricati_firma assistono il titolare dei certificati di firma nelle operazioni di verifica di funzionamento del kit ricevuto, provvedendo così ad una prima fase di addestramento;
- **gestione del rigetto della richiesta di emissione o rinnovo:** se il Certificatore, motivandone per iscritto le ragioni, rigetta la richiesta, gli incaricati_firma riesaminano gli atti istruttori e provvedono a perfezionare eventuali vizi di forma o di procedura. Nel caso in cui le motivazioni addotte dal Certificatore siano di altra natura, gli incaricati_firma provvedono ad informare la Direzione Amministrativa affinché siano adottate le misure del caso.

Sospensione o revoca del certificato

- **sospensione e revoca per la perdita dei requisiti:** l'Ateneo, in qualità di terzo interessato da cui provengono i poteri del titolare del certificato, avvalendosi degli incaricati_firma per l'istruttoria dei provvedimenti, ha la facoltà di far sospendere oppure revocare i certificati nei casi previsti dall'art. 8 del presente Regolamento. In tali casi, ricevuto il decreto di sospensione o revoca dal Rettore o dal Direttore Amministrativo, a seconda delle rispettive competenze, gli incaricati_firma utilizzano le modalità operative e tecniche stabilite dal Certificatore per la revoca o la sospensione di certificati; contestualmente, informano il titolare del certificato dell'avvenuto inoltro della richiesta e concordano con lui i termini per la restituzione, se prevista, dei dispositivi ricevuti in consegna;
- **sospensione e revoca richiesta dal titolare:** nei casi previsti dagli artt. 6 e 8 del presente Regolamento, il titolare del certificato presenta agli incaricati_firma motivata istanza, rivolta al Rettore o al Direttore Amministrativo, a seconda delle rispettive competenze, per la sospensione o revoca del proprio certificato. Qualora la richiesta sia accolta, gli incaricati_firma curano l'istruttoria dei relativi provvedimenti, con le procedure di cui al punto precedente e supportano il titolare per tutti i successivi adempimenti nei confronti del Certificatore.

Napoli, lì 31 ottobre 2006

IL RETTORE
GUIDO TROMBETTI