UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA
Ufficio Processi Documentali
Registration Authority d'Ateneo
Direzione Generale
Settore Gestione Documentale

IL RETTORE

VISTO il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE a far data dal 1° luglio 2016;

VISTO il DPR 28 dicembre 2000, n. 445 recante norme in materia di "Disposizioni legislative in materia di documentazione amministrativa";

VISTO il D.Lgs 30 dicembre 2010, n. 235, recante norme in materia di "Modifiche ed integrazioni al D.Lgs 7 marzo 2005, n. 82, del Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69" ed in particolare gli artt. dal 24 al 37;

VISTO il D.Lgs 30 giugno 2003, n. 196, e successive modificazioni, recante Codice in materia di protezione dei dati personali;

VISTO il DL 9 febbraio 2012, n. 5, convertito in L. 4 aprile 2012, n. 35 recante norme in materia di "Dematerializzazione di procedure in materia di università, in particolare l'art. 48 Sezione II";

VISTO il DPCM 22 febbraio 2013, recante norme in materia delle "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali";

VISTE le Linee Guida del novembre 2014 per la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma elettronica – art. 35, comma 5 del "Codice dell'Amministrazione Digitale";

VISTO il DPCM 5 febbraio 2015 - Proroga del termine per completare il piano di migrazione di cui all'articolo 4 del DPCM 19 luglio 2012 di «Definizione dei termini di validita' delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma» - recante modifiche al DPCM 19 luglio 2012;

VISTO il Regolamento Didattico dell'Università degli Studi di Milano-Bicocca, emanato con D.R. 0025752 del 17 settembre 2013, in particolare l'art. 23, recante norme in materia di "Verifiche del profitto";

VISTO il Regolamento degli Studenti dell'Università degli Studi di Milano-Bicocca, modificato con DR nr. 0045651 del 9 settembre 2015, in particolare l'art. 14, recante norme in materia di "Verifiche del profitto";

VISTO il "Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Università degli Studi di Milano-Bicocca", adottato con Decreto del D.G. 0055325 del 18 dicembre 2014;

TENUTO CONTO della partecipazione dell'Ateneo al progetto CT4University-Università Digitale, con particolare riferimento alla stesura delle Linee Guida per la verbalizzazione e la registrazione degli esiti degli esami di profitto e di laurea sostenuti dagli studenti universitari esclusivamente con modalità informatiche, a decorrere dall'A.A. 2011/2012;

CONSIDERATO CHE la firma digitale apposta sui verbali on-line è finalizzata a perseguire obiettivi di semplificazione del procedimento, efficienza ed economicità, con il principale scopo di ridurre al massimo i tempi di aggiornamento delle carriere degli studenti e favorire la più ampia dematerializzazione documentale;

TENUTO CONTO CHE l'Ateneo sottoscrive con firma digitale i seguenti documenti: Contratti in forma pubblica amministrativa, Convenzioni, Verbali d'esame, Ordinativi informatici, Ordini MePA ai sensi dell'Allegato n. 17 del "Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Università degli Studi di Milano-Bicocca;

TENUTO CONTO CHE l'Ateneo, utilizza i seguenti dispositivi di firma: HSM (Hardware Security Module) insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche; Smart Card, il cui utilizzo dei dispositivi di firma è disciplinato nella Sezione II del presente Regolamento;

PRESO ATTO della Delibera con la quale il Consiglio di Amministrazione, nella seduta del 24/05/2016, ha approvato il "REGOLAMENTO SULLA FIRMA DIGITALE";

DECRETA

L'emanazione del Regolamento sulla Firma Digitale (con dispositivi HSM e SMART CARD).

REGOLAMENTO SULLA FIRMA DIGITALE

Sezione I

Art. 1
OGGETTO E FINALITÀ

1. Il presente Regolamento disciplina le modalità di rilascio, gestione e utilizzo della firma digitale nell'ambito dell'Università degli Studi di Milano-Bicocca (d'ora in poi denominata Ateneo), nel rispetto delle fonti legislative e regolamentari vigenti.
2. Il Regolamento disciplina in particolare:
   a) l'attivazione, sospensione e revoca dei certificati, rilasciati da certificatori accreditati, da utilizzare per la sottoscrizione in forma elettronica dei documenti informatici;
   b) le regole e l'ambito di applicabilità della sottoscrizione dei documenti elettronici con firma digitale secondo quanto indicato nel paragrafo 2.5 del "Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Università degli Studi di Milano-Bicocca".
3. L'Ateneo, ottemperando alla normativa vigente e agli 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 elettronici, al fine di semplificare le procedure, ridurre i tempi e i costi dell'azione amministrativa anche attraverso una riorganizzazione dei flussi documentali e una piena implementazione con il sistema del protocollo informatico.

Art. 2
IL DOCUMENTO INFORMATICO E IL SUO VALORE LEGALE

1. La firma digitale è lo strumento per la sottoscrizione dei documenti informatici di valore e validità giuridica.
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 ed 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 dell'Amministrazione Digitale (d'ora in avanti CAD).
3. L'efficacia probatoria del documento informatico sottoscritto, con firma digitale ha l'efficacia prevista dall'art. 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare del certificato, salvo che questi dia prova contraria.

Il documento sottoscritto con la firma digitale ha le seguenti caratteristiche:
- dal punto di vista del valore legale, soddisfa il requisito della forma scritta;
- garantisce l'autenticità del documento informatico, in quanto viene resa certa l'identità del sottoscrittore;
- assicura l'integrità del documento sottoscritto, cioè la sicurezza che il documento informatico non sia stato manomesso dopo la sua sottoscrizione;
- garantisce il non ripudio della firma, in quanto l'utilizzo del dispositivo di firma digitale si presume riconducibile al titolare del dispositivo stesso.1. L'art. 1 del CAD definisce il

documento informatico la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

4. L'apposizione ad un documento informatico di una firma digitale basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione, ovvero non produce nessun effetto giuridico.

Art. 3
DEFINIZIONI

1. Ai fini del Regolamento, ed in conformità al CAD, si intendono per:
   a) **Certificato qualificato**: 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;
   b) **Certificatore - Certification Authority (CA)**: 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 di sicurezza ed è accreditato presso AgID ai sensi dell'art. 29 del CAD;
   c) **Dispositivo di firma**: l'insieme degli strumenti che consentono la sottoscrizione con firma digitale dei documenti informatici, come indicato nel successivo art. 5;
   d) **Documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
   e) **Firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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;
   f) **Registration Authority** di Ateneo (RA): incaricata dell'identificazione dei Titolari ai fini del rilascio dei certificati digitali ai sensi dell'art. 55 comma 2, lettera a) del DPCM 22.02.13 per il personale dell'Ateneo – le cui funzioni sono svolte dagli Incaricati all'identificazione e dal Primo Incaricato;
   g) **Titolare**: la persona fisica cui è attribuito il certificato di firma digitale e che ha accesso ai dispositivi per la creazione della firma elettronica.
   h) **Marca Temporale**: servizio offerto da una CA, che permette di associare una validazione temporale (data e ora certe, legalmente valide e opponibili a terzi) ad un documento informatico (art. 20, comma 3 del CAD) al momento della sua creazione, trasmissione o archiviazione. L'apposizione di una Marca Temporale ad un documento firmato digitalmente fornisce la prova dell'esistenza del documento al momento della generazione della marca stessa e ne garantisce, quindi, la validità nel tempo.

Art. 4
FORMATI DI FIRMA DIGITALE

1. L'Ateneo, nel rispetto degli standard europei, individua tre tipi di sottoscrizione digitale per produrre file firmati digitalmente:
   a) Cades, genera un file con estensione .p7m;
   b) Pades, genera un file con estensione .pdf;
   c) Xades, genera un file con estensione .XML.

I dispositivi attivi in Ateneo utilizzano il formato Cades.

Art. 5
DISPOSITIVI DI FIRMA

1. L'Ateneo, utilizza i seguenti dispositivi di firma:
   a) HSM (Hardware Security Module) insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche;
   b) Smart Card. L'utilizzo dei dispositivi di firma con Smart Card è disciplinato nella Sezione II del presente Regolamento;
   c) dispositivi per l'utilizzo della firma elettronica avanzata.

Art. 6
SOGGETTI COINVOLTI

1. Operano nel processo di attivazione e gestione del certificato digitale i seguenti soggetti:
   a) l'**Ateneo,** in qualità di terzo interessato, richiede il certificato a favore del Titolare, provvede a fornire informazioni per ciò che attiene al ruolo e alle funzioni istituzionali del personale a cui possono essere assegnati i certificati di firma digitale, individua e nomina gli Incaricati dell'Identificazione, ha inoltre la facoltà, ai sensi dell'art. 36, comma 1 lettera c) del CAD, di richiedere la revoca o la sospensione del certificato;
   b) il **Titolare** al quale è assegnato il certificato di firma digitale;
   c) gli **Incaricati dell'Identificazione** tra cui il **Primo Incaricato** (d'ora in poi denominati Incaricati) nominati dal Rettore e responsabili, su delega della CA, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati; all'interno dell'Ateneo sono individuati gli Incaricati come indicato nella Guida Operativa Firme Digitali (d'ora in avanti Guida Operativa), rinvenibile sul sito d'Ateneo alla pagina personale e che fa parte integrante del presente Regolamento;
   d) il **Referente tecnico** appositamente individuato che supporta gli Incaricati nelle attività di funzionalità del Sistema di generazione dei certificati di firma;
   e) la **CA** - Certification Authority, soggetto che si occupa della gestione del servizio di firma digitale nel rispetto di quanto disposto dall'art. 32, comma 3 del CAD.

Art. 7
OBBLIGHI DEL TITOLARE

1. Il Titolare del certificato di firma digitale è tenuto:
   a) ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma che utilizzerà personalmente;
   b) a conservare con la massima diligenza e riservatezza i propri codici personali al fine di evitarne l'uso fraudolento da parte di terzi;
   c) a comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione al servizio di certificazione e ad informare anticipatamente gli Incaricati dell'eventuale variazione del rapporto contrattuale con l'Ateneo e di tutti i dati richiesti per l'emissione del certificato, compilando l'apposito Modulo 1 - allegato al Regolamento;
   d) ad informare anticipatamente gli Incaricati di ogni circostanza che renda necessaria o, comunque, opportuna la revoca o la sospensione del certificato; deve altresì informare tempestivamente gli Incaricati di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente alla CA.

2. Sono previste spese amministrative nei casi citati nel paragrafo "Revoca di un certificato" di firma digitale HSM riportato nella Guida Operativa che fa parte integrante del presente Regolamento.

Art. 8
COMPITI E RESPONSABILITÀ DEGLI INCARICATI

1. Gli Incaricati provvedono a:
   a) verificare con certezza l'identità del Titolare secondo le modalità descritte nella Guida Operativa;
   b) rilasciare al Titolare il certificato qualificato attraverso l'utilizzo dell'apposito sistema informatico fornito dalla CA, seguendo le istruzioni operative previste dal Manuale Operativo della CA;
   c) informare il Titolare riguardo agli obblighi assunti in merito alla protezione della segretezza delle chiavi private e al trattamento dei dati personali;
   d) fornire istruzioni al Titolare sul corretto utilizzo del servizio di firma digitale;
   e) supportare il Titolare nelle ipotesi di revoca, sospensione o annullamento della sospensione delle firme attivate presso la RA di Ateneo e comunicare le operazioni effettuate agli Incaricati di firma;
   f) raccogliere le comunicazioni di rilascio/rinnovo, sospensione e/o revoca e conservarle con modalità sicure;
   g) individuare mensilmente i certificati la cui data di scadenza è compresa entro i trenta giorni solari successivi e, verificata la non sussistenza di condizioni per la loro sospensione o revoca, richiedere l'autorizzazione formale per il rinnovo degli stessi;
   h) compilare l'elenco dei Titolari di certificati da rinnovare, tenuto conto dell'esistenza dei presupposti giuridici ed inviare l'elenco al Primo Incaricato;
   i) conservare le buste fornite dalla CA e contenenti i codici personali, in luogo sicuro e protetto, avendone accesso esclusivo;
   j) rispettare le misure minime di sicurezza previste per il trattamento dei dati personali dal D.Lgs. 196/2003;
   k) rispettare le necessarie procedure di sicurezza nell'esercizio delle proprie funzioni.

Art. 9
COMPITI E RESPONSABILITÁ DEL PRIMO INCARICATO

1. Il Primo Incaricato, oltre ai compiti definiti dall'art. 8:
   a) procede all'identificazione degli eventuali nuovi Incaricati;
   b) gestisce le eventuali emissioni di certificati in sostituzione degli Incaricati;
   c) revoca e/o sospende i certificati qualificati;
   d) coordina le attività degli altri Incaricati;
   e) monitora lo stato di avanzamento dei processi di cui ai punti precedenti
   f) monitora le attività di rinnovo dei certificati;
   g) invia l'elenco dei certificati da rinnovare alla CA;
   h) provvede ad aggiornate i dati variati dei titolari comunicandoli alla CA.

Art. 10
COMPITI E RESPONSABILITÀ DEL REFERENTE TECNICO

1. Il Referente tecnico:
   a) supporta gli Incaricati raccogliendo tutte le richieste e le segnalazioni di anomalie da trasmettere al Referente del servizio di CA;

b) monitora lo stato di avanzamento del processo al precedente punto.

Art. 11
USO DELLA SOTTOSCRIZIONE CON FIRMA DIGITALE IN ATENEO

1. L'Ateneo, in ottemperanza alle prescrizioni normative, nell'ambito delle attività didattico-scientifiche, tecniche ed amministrative, utilizza la firma digitale per le seguenti finalità:
   a) sottoscrizione delle registrazioni on line degli esami di profitto;
   b) sottoscrizione di contratti e convenzioni nell'ambito dell'attività istituzionale dell'Ateneo;
   c) sottoscrizione di documenti amministrativo-contabili nell'ambito di procedure d'acquisto di forniture e servizi.
2. Ulteriori obblighi potranno essere previsti al fine dell'adeguamento a future disposizioni normative e secondo quanto previsto dal "Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi dell'Università degli Studi di Milano-Bicocca".

Art. 12
PROCEDURA DI AUTORIZZAZIONE, IDENTIFICAZIONE E REGISTRAZIONE DELL' UTENTE TITOLARE

1. Gli Incaricati provvedono all'autorizzazione, identificazione e registrazione del richiedente il certificato di firma, secondo la procedura descritta nella Guida Operativa.

Art. 13
CAUSE DI REVOCA E DI SOSPENSIONE

1. La revoca di un certificato determina l'immediata e definitiva cessazione della sua validità, indipendentemente dalla data di scadenza del certificato stesso e non influisce sulla validità del certificato e delle firme apposte con esso nel periodo precedente la revoca). Le cause di revoca e sospensione sono riportate nella Guida Operativa.

Art. 14
PROCEDURA DI SOSPENSIONE E DI REVOCA

1. Le procedure di sospensione e di revoca sono descritte in ogni fase nella Guida Operativa.

Art. 15
RINNOVO

1. Il certificato di firma digitale ha una durata di 3 anni e può essere rinnovato.
2. La procedura di rinnovo è descritta nella Guida Operativa.

Sezione II

Art. 16
DISPOSITIVO DI FIRMA CON SMART CARD

1. Le firme digitali con dispositivo di firma **Smart Card** sono rilasciate da una CA (ai sensi dell'articolo 29 del CAD), che per l'Ateneo è InfoCert S.p.A e possono essere richieste solo in casi **eccezionali e motivati**, valutati di volta in volta, su autorizzazione del Rettore.
2. La Smart Card è una tessera dotata di microchip (apparato elettronico incorporato), programmabile solo all'origine e in grado di contenere informazioni in modo sicuro. Mediante apposito lettore collegabile al computer, ed un software di verifica della firma in grado di interagire con il dispositivo e di gestire il dispositivo stesso, consente di apporre la propria di firma digitale. La Smart Card non permette la sottoscrizione multipla di più documenti.
Indicazioni più dettagliate sono rinvenibili nel Manuale Operativo della CA e nella Guida Operativa allegata al presente Regolamento.

Art. 17
UFFICIO PREPOSTO AL RILASCIO E PROCEDURA

1. L'ufficio preposto al rilascio della firma digitale mediante dispositivo Smart Card è l'**Ufficio Processi Documentali.**
2. L'Ufficio, nel processo di attivazione e gestione dei certificati di firma, opera attraverso gli **Incaricati,** i quali terranno direttamente i rapporti sia con la CA sia con il Richiedente-Titolare.
3. L'Ufficio opera d'intesa con il responsabile dello sportello bancario dell'Istituto cassiere.

Sezione III

Art. 18
TRATTAMENTO DEI DATI PERSONALI

1. L'Ateneo è Titolare, per il perseguimento dei propri fini istituzionali, del trattamento dei dati personali connesso alla gestione dei certificati; in qualità di terzo interessato richiedente i certificati tratta i dati personali degli interessati secondo principi di liceità, pertinenza, non eccedenza e necessità, comunicandoli alla CA per consentire i successivi adempimenti.

Art. 19
NORME DI RINVIO

1. Per tutto quanto non espressamente previsto dal Regolamento si rinvia alle disposizioni legislative e regolamentari in materia.
2. Ai certificati di firma con Smart Card si applicano per quanto compatibili le norme del presente Regolamento e si rinvia alla Guida Operativa per le procedure di gestione.

Art. 20
ENTRATA IN VIGORE

1. Il Regolamento è pubblicato all'Albo on-line ed entrerà in vigore il giorno successivo alla pubblicazione.

IL RETTORE

Prof.ssa Maria Cristina Messa