UNIVERSITÀ
DEGLI STUDI
DI PALERMO

LINEE GUIDA SULLA

GESTIONE DOCUMENTALE

Indice

LINEE GUIDA SULLA GESTIONE DOCUMENTALE

• Premessa

Scopo di questo documento è di fornire alcuni chiarimenti ed indicazioni utili per consentire la corretta formazione, gestione e sottoscrizione di documenti nativamente digitali, nonché contribuire all'eliminazione di fraintendimenti e approcci che tutt'ora causano la produzione di documenti analogici e anomale ibridazioni.

I *documenti* prodotti dalla pubblica amministrazione sono gli elementi che compongono il procedimento amministrativo, e che ne marcano l'iter procedurale, dettagliandone tempi, azioni e attori, fino alla emanazione del provvedimento finale.

L'efficacia di un provvedimento della PA dipende inevitabilmente dalla validità degli atti che ad esso hanno condotto, che devono essere "perfezionati" per mezzo di adeguata sottoscrizione. Ai sensi del *Regolamento UE n° 910/2014 - eIDAS*, lo strumento utilizzato per la sottoscrizione deve offrire garanzie di autenticità, integrità e non ripudio. In questo senso, la firma digitale (o *firma elettronica qualificata*, FEQ), essendo connessa unicamente al firmatario e consentendo l'identificazione certa di chi ha "*firmato un documento*", risponde pienamente ai requisiti previsti. Ogni documento, se firmato digitalmente, è valido *erga omnes,* fino a prova di falso a seguito di querela.

Dal punto di vista formale e gestionale, **gli atti di una pubblica amministrazione, insieme alla piattaforma informatica** attraverso la quale se ne garantiscono la produzione, la valenza probatoria, la conservazione, la pubblicazione, la consultazione e la trasmissione, **compongono il suo sistema documentale e archivistico**.

Il concetto di "sottoscrizione" di un *atto* (dal latino *agere*, agire) non va limitato all'ambito documentale, ma piuttosto esteso a tutte le *azioni*[1] che quotidianamente compiamo sulle piattaforme informatiche e per mezzo degli strumenti utilizzati nella gestione amministrativa.

[1] A titolo di esempio, di seguito un elenco non esaustivo di "azioni" che è possibile "sottoscrivere": autorizzare (qualcuno a far qualcosa), affermare, negare, autenticare, attestare (dichiarare che qualcosa è vero, è falso), accettare, rifiutare, rigettare, chiedere, informare, comunicare, prendere visione, ricevere, disporre, ordinare, certificare, aderire (essere d'accordo su una dichiarazione di altri)

- **Obblighi, vincoli e presupposti normativi**

Obbligatorietà del formato digitale nativo per i documenti

Con il DPCM 13 novembre 2014 sono state definitivamente formulate le regole per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, alle quali le pubbliche amministrazioni devono attenersi. L'obbligo in argomento viene chiaramente sancito all'art. 9, c. 2, dove si stabilisce che gli originali dei documenti vanno realizzati attraverso gli strumenti informatici.

Accessibilità dei documenti

Per accessibilità si intende la capacità dei sistemi informatici di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari. Con il termine "accessibile" si intende un documento che può essere fruito da tutti, comprese quindi quelle persone che presentano disabilità nell'utilizzo degli strumenti informatici e che usufruiscono di tecnologie assistive per la lettura dei contenuti, conosciute come strumenti di sintesi vocale *"text-to-speech"* (*Screen Readers*).

Il formato digitale più idoneo per soddisfare l'esigenza di disporre di documenti accessibili online è il PDF accessibile[2]*.* La creazione di un PDF accessibile parte dalla formazione di un documento originario utilizzando un software di videoscrittura[3]*, convertito successivamente in PDF.* Per questo motivo, **non rispondono ai criteri di accessibilità i PDF derivanti da scansioni di documenti cartacei**. Tali documenti, che al loro interno non contengono testo, ma immagini che rappresentano testo, non sono leggibili attraverso i software di *text reading* e rappresentano la barriera più grande in termini di accessibilità.

Utilizzo di formati "aperti"

Al fine di garantire accesso a lungo termine ai dati senza barriere legali o tecniche, le amministrazioni pubbliche ed i governi sono diventati progressivamente consapevoli dei formati aperti come questioni che riguardano le politiche pubbliche. In tal senso si muovono le indicazioni che prevedono che i formati impiegati per i documenti debbano seguire quelli definiti come standard internazionali. La Commissione Europea ha sottoscritto lo standard *OpenDocument*, nel quale sono definiti i formati di file per lo scambio di documenti[4]. OpenDocument (già uno standard secondo OASIS - organismo indipendente riconosciuto per gli standard) è stato sottoposto alla ISO (*International Organization for Standardization*) per la standardizzazione, che lo ha approvato e accettato il 1º maggio 2006 (ISO 26300). Ci si attende che presto l'Unione Europea stabilisca l'uso di OpenDocument come standard comune per i documenti

[2] AGID - Guida pratica per la creazione di un documento accessibile
https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/guida_pratica_creazione_word_accessibile_2.pdf
[3] AGID - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici - 2.1.1 - Formazione del documento informatico: *"a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2"* - https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico.pdf
[4] Le estensioni per i file più comuni descritte nello standard *OpenDocument* sono .odt (documenti di testo), .ods (fogli di calcolo), .odp (presentazioni), .odg (grafica) e .odb (database).

di produttività da ufficio per gli stati membri.

Trasparenza dell'azione della pubblica amministrazione

L'accessibilità dei documenti rientra negli obblighi previsti dal d.lgs. 14 marzo 2013, n. 33 e le sue successive modificazioni (cd. *decreto trasparenza*), che ha riordinato la normativa esistente – anche innovandola – fornendo così una disciplina unitaria della trasparenza amministrativa.

Tutela degli archivi delle pubbliche amministrazioni

Il ***Codice dei beni culturali e del paesaggio*** (decreto legislativo 22 gennaio 2004, n. 42), definisce ***beni culturali*** gli archivi degli enti e degli istituti pubblici (art. 10, comma2-b) sottomettendoli altresì a vincolo di tutela (art. 13, comma 2), senza la necessità di una esplicita dichiarazione d'interesse storico. Una corretta gestione di tutte le fasi del documento (acquisizione, formazione, classificazione, conservazione, scarto ecc.) non è soltanto funzionale al procedimento amministrativo e all'accessibilità di lungo termine dei dati, ma è un obbligo normativo posto a salvaguardia del patrimonio archivistico italiano.

• La sottoscrizione con firma digitale

Il corretto utilizzo delle credenziali per l'identificazione dei soggetti e della sottoscrizione di atti è immediatamente richiamato nel CAD all'art. 32 (*"Obblighi del titolare e del prestatore di servizi di firma elettronica qualificata"*) che recita *"Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;* ***è altresì tenuto ad utilizzare personalmente il dispositivo di firma****"*.

In tal senso, riteniamo indispensabile sgombrare il campo da un malinteso che è spesso alla base della violazione del divieto di cessione a terzi delle credenziali e dei dispositivi di firma. Per giustificare tale deroga, infatti, viene impropriamente invocato l'istituto della *delega*, nel quale il soggetto delegato, in virtù di apposito provvedimento, viene legittimato al compimento di atti o all'esercizio di funzioni di competenza del delegante. Comunque venga definito (disposizione, ordine di servizio, delega) il provvedimento deve essere conferito per atto scritto, non essendo ammessa una mera delega orale, e deve indicare espressamente il nome e la qualificazione del delegato. In tale istituto **il delegato firma in proprio per conto del delegante**, e consente al cittadino/utente di comprendere quale sia il soggetto legittimato al compimento e/o a porre la firma sugli atti, e quindi di individuare i soggetti con i quali confrontarsi e dialogare nel contraddittorio.

Diversamente, con la cessione (anche temporanea o occasionale) del dispositivo di firma e delle credenziali ad esso associate viene lesa la pubblica fede e si configura un falso in atto pubblico, le cui conseguenze ricadono sia sul cedente che sull'utilizzatore.

Per ulteriori approfondimenti, in ordine alla gravità e alla rilevanza penale e amministrativa della violazione di tali obblighi, si invita a consultare l'*appendice* al presente documento.

- **La sottoscrizione nella posta elettronica**

Ogni soggetto che ha un rapporto definito e istituzionalizzato con l'Ateneo dispone di un indirizzo di posta elettronica nel formato nome.cognome@*(subdominio.)*unipa.it, che può utilizzare grazie alla coppia di credenziali (username e password) attribuite dai sistemi. Tale attribuzione è subordinata a una serie di procedure contrattuali che prevedono una fase preliminare di identificazione certa del soggetto, e che fanno sì che **le credenziali siano connesse unicamente al loro titolare**. Pertanto, pur non avendo le stesse caratteristiche tecnologiche di un documento firmato con FEQ, in termini di valenza probatoria una e-mail inviata da **un indirizzo personale istituzionale** può intendersi sottoscritta con **firma elettronica** semplice (c.d. *firma debole).*

Ricordiamo che la *firma elettronica* è definita nel regolamento UE 910/2014 (eIDAS) come *i dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*; tale firma ha il valore stabilito nel CAD nell'articolo 20, comma 1-bis. In tal senso **l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità**. In altre parole, non c'è nulla di predefinito, ma decide il giudice caso per caso, in base al suo libero convincimento.

Nel caso di un messaggio di e-mail, **si intende sottoscritto dal mittente (con *firma debole*) il corpo del messaggio e gli allegati che non siano a loro volta sottoscritti (digitalmente) da altri soggetti**. Se lo scopo della comunicazione è la trasmissione di atti o provvedimenti dei quali il mittente non è autore, tali allegati si intenderanno validamente sottoscritti soltanto se firmati digitalmente. In caso contrario, il mittente è responsabile del contenuto del messaggio e della natura degli allegati.

Gli indirizzi e-mail assegnati agli uffici, tipicamente nel formato *nomestruttura@(subdominio.)*unipa.it, non hanno le stesse caratteristiche di validazione del mittente: **non sono infatti riconducibili univocamente ad un soggetto**, in quanto di norma utilizzati da più operatori afferenti alla stessa struttura, e quindi **un messaggio proveniente da tale indirizzo non può intendersi in alcun modo validamente sottoscritto.** Di conseguenza, assume ancora maggiore importanza la necessità che l'informazione trasmessa (gli atti o i provvedimenti allegati) siano firmati digitalmente dagli autori.

- **La sottoscrizione in Titulus e su altre piattaforme informatiche**

Analogamente a quanto accade per tutte le piattaforme software (irisweb, Ugov, portale didattica) adottate presso l'Ateneo, anche l'accesso a Titulus è subordinato al possesso di credenziali di autenticazione. È necessario precisare che **in Titulus con il termine "documento" si intende un oggetto complesso, composto dall'insieme dei metadati relativi alla registrazione** (data, oggetto, classificazione, RPA, mittente, destinatario, annotazioni, ecc.) **e dei file ad essa associati.** Ogni operazione svolta in Titulus, analogamente alle altre piattaforme, debitamente registrata dal sistema, si intende validamente sottoscritta per il mezzo delle credenziali utilizzate per l'accesso. Stante però la struttura composita del *documento* in Titulus, la sottoscrizione di una singola azione non implica la sua estensione automatica a tutto il contenuto, e a maggior ragione dei file associati.

In particolare, va chiarito che **l'apposizione di una "annotazione" è un'azione pertinente al procedimento, non al file associato**. Le annotazioni rappresentano passaggi procedurali, temporalmente marcati dal sistema, nei quali è possibile identificare con certezza il sottoscrittore.

Ad esempio, si può certamente utilizzare una annotazione per esprimere l'approvazione (o il diniego) per l'avanzamento allo step procedurale successivo; al contrario, non va in alcun modo utilizzata per comunicazioni più o meno formali tra gli operatori.

Le annotazioni non hanno comunque alcun effetto nella sottoscrizione dei file associati che, se non firmati digitalmente, rimangono nella responsabilità dell'operatore che li ha caricati, e la cui valenza probatoria è confinata all'interno della piattaforma di gestione archivistica e documentale. Infine, è importante comprendere che le annotazioni hanno visibilità soltanto all'interno della AOO dove il procedimento si è sviluppato.

- **Linee guida e indicazioni operative**

- In ottemperanza delle vigenti norme, ed in armonia con l'evoluzione della PA verso il digitale nativo, questa Amministrazione deve inderogabilmente provvedere ad eliminare tutte le residue anomalie del procedimento amministrativo che conducono alla produzione di documenti in formato analogico o ibrido. In particolare, i bandi e le procedure di reclutamento del personale docente devono obbligatoriamente prevedere non solo l'elezione di un domicilio digitale da parte dei partecipanti, ma anche la disponibilità di adeguati dispositivi di identificazione e sottoscrizione digitale.
- La mancanza di firma digitale da parte del sottoscrittore esterno non può essere motivo di deroga al divieto di formazione di documenti analogici da parte della pubblica amministrazione. Per ovviare a tale eventualità, l'Amministrazione dovrà dotarsi, ad esempio, di dispositivi per l'acquisizione della firma grafometrica o di pacchetti di firme digitali *one-shot*, per consentire la sottoscrizione digitale in presenza. Qualunque sia il sistema adottato, la sottoscrizione potrà avvenire solo dopo che sia stata verificata ed accertata l'identità del sottoscrittore.
- L'uso della firma digitale per sottoscrivere un file non è mai sbagliato. Possono esserci dei casi nei quali tale operazione sia esuberante rispetto alle reali necessità, ma non per questo si tratta di un errore. Inoltre, la firma digitale conferisce validità al file anche al di fuori del contesto nel quale è stato prodotto. Diversamente, ad esempio, un documento estrapolato dal suo gestore documentale può non offrire sufficienti garanzie di autenticità e veridicità.
- Tutti documenti vanno prodotti utilizzando formati di tipo aperto ed accessibile, specialmente se oggetto di pubblicazione o diffusione. Per la loro redazione è quindi consigliabile affidarsi ai formati *OpenDocument* e all'uso di strumenti software che ne consentano la produzione, il salvataggio e la lettura.
- Nell'eventualità di pubblicazione, dai documenti vanno oscurati tutti i dati eccedenti le finalità previste, nonché i dati personali o sensibili.
- La conformità della copia informatica del documento all'originale analogico è attestata dal responsabile del procedimento, in conformità a quanto disposto agli articoli 22 e 23-bis del CAD. La questione è affrontata nel dettaglio in un'apposita sezione di questo stesso testo.
- In Titulus, il *documento* (non il file) è sottoscritto dall'operatore con le proprie credenziali. Ugualmente sottoscritte sono le annotazioni, che riportano inoltre la marcatura temporale apposta dal sistema.
- Le annotazioni in Titulus vanno utilizzate per scandire e rappresentare i passi procedurali del processo, e non per comunicazioni "al volo" tra gli operatori. Poiché attinenti al procedimento, e non al documento, le annotazioni non sostituiscono la sottoscrizione digitale del file.
- Per quanto appena detto, quando il documento viene inviato a destinatari esterni all'Ateneo, i *file ad esso associati* devono essere firmati digitalmente. Le annotazioni sono infatti visibili solo ai soggetti competenti all'interno dell'AOO di partenza. I documenti inviati all'esterno dell'Amministrazione, o che per la loro natura devono avere una opponibilità a

terzi, non possono mai essere firmati con la locuzione *"F.to [Nome Cognome]"*, in quanto verrebbe meno la loro validità.

- Tutti i documenti con estensione PDF possono essere firmati in modalità PAdES, che consente la normale visualizzazione del documento e l'apposizione di firme multiple in successione. Pur nell'ambito dei formati previsti ed accettati dalla normativa vigente, l'Ateneo di Palermo predilige e incoraggia l'uso di questo formato per la sottoscrizione digitale di tutti i documenti di tipo PDF.
- Tutti i file di altro tipo (fogli elettronici, documenti testuali editabili, audio, video, archivi vari...) per essere sottoscritti richiedono la firma in formato CAdES. Il file generato (con estensione p7m) sarà un archivio compresso contenente tutti i file originali (tra i quali possono essere presenti anche file PDF).
- L'uso dei formati documentali PAdES e CAdES è necessario per consentire il corretto assolvimento degli obblighi di versamento in conservazione.
- Poiché i sensi della normativa *"le pubbliche amministrazioni (...) formano gli originali dei propri documenti attraverso gli strumenti informatici"* [5], non è consentita alcuna conversione del documento da digitale ad analogico o viceversa. Stampare su carta un documento, per poi apporvi una firma olografa ed effettuarne la scansione per utilizzarlo all'interno dei sistemi di Ateneo è deprecato e non ne costituisce una valida sottoscrizione. L'acquisizione per immagine di un documento cartaceo (proveniente dall'esterno) rappresenta una *copia informatica di un documento analogico*[6] e non è sostitutiva dell'originale. In tal senso, pur se in presenza di una eventuale attestazione di conformità, l'originale sottostà ai vincoli previsti dalla normativa per gli archivi pubblici, e alle regole previste per lo scarto.
- Per gli stessi motivi, è fortemente deprecata la produzione di documenti ibridi, che è fonte di caos e che genera anomalie e misinterpretazioni sui sistemi. Se una *copia informatica di un documento analogico sottoscritto olograficamente* dovesse essere successivamente sottoposta a sottoscrizione con firme digitali, solo queste ultime avrebbero valenza probatoria, mentre quella olografa manterrebbe il proprio valore sul documento cartaceo originale. Ci troveremmo quindi di fronte a *due distinti documenti originali*, ciascuno con un proprio set di sottoscrizioni non coincidenti per soggetti, modalità e tempi.
- A margine, è da chiarire che l'apposizione di firme olografe o di loro riproduzioni su documenti informatici (sebbene assolutamente consentita) è del tutto ridondante ed ininfluente rispetto alla sottoscrizione digitale, e va quindi intesa come mero arricchimento grafico. Analogamente a quanto avviene per loghi e sigilli, il suo eventuale inserimento deve comunque essere fatto precedentemente o contestualmente alla sottoscrizione digitale, in modo da evitare di danneggiare ed invalidare la firma o di marcare il documento come modificato dopo la firma.

[5] DPCM 13 novembre 2014, art. 9, c. 2
[6] art. 22 CAD

- **Documenti analogici, copie informatiche e attestazione di conformità**

Dato ormai per acquisito che la modalità formazione del documento all'interno dell'amministrazione pubblica sia di tipo *digitale nativo*, è necessario individuare le modalità di gestione dei **documenti analogici che a questa pervengono dall'esterno**, e che devono essere acquisiti per confluire sul sistema documentale. Tale può anche essere il caso di documenti originariamente creati in formato digitale dall'amministrazione, ma che un soggetto esterno ha riprodotto su supporto cartaceo e sottoscritto olograficamente, come tuttora spesso avviene per alcuni contratti o convenzioni che sfuggono alle presenti indicazioni operative .

La gestione di tali documenti prevede quindi una loro conversione in formato digitale (scansione), definita dal CAD come "copia informatica di documento analogico", che *sic et simpliciter* non è in grado di sostituire l'originale[7]. Infatti, come già diffusamente evidenziato in questo testo, il file ottenuto non acquisisce le caratteristiche attribuibili alla firma olografa presente sul documento originale, risultando in una copia non sottoscritta e disconoscibile in caso di contraddittorio. Di conseguenza, ove il documento fosse destinato ad essere firmato digitalmente da ulteriori sottoscrittori, come nel caso di un contratto, il documento risulterebbe mancante della firma originale, e non sarebbe quindi perfezionato ed efficace.

E' quindi necessario che alla copia informatica venga riconosciuta una *"corrispondenza di forma e contenuto con l'originale analogico"*[8]. A tale scopo, il CAD richiede una *"attestazione di conformità previo raffronto dei documenti o attraverso certificazione di processo*[9]*"*. Per le caratteristiche di complessità previste dalla applicazione di quest'ultima, è certamente più immediato predisporre una procedura di attestazione tramite raffronto.

A tale riguardo, le linee guida di AGID (cap. 2.5) specificano che *"**l'attestazione** di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, **può essere inserita nel documento informatico contenente la copia informatica** o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. **Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato**".*

In considerazione di ciò, dopo che preliminarmente l'Amministrazione avrà individuato e nominato i soggetti ai quali attribuire il potere e il diritto di attestare la conformità, dotandoli di firma digitale, di seguito si suggerisce la procedura da seguire.

- Il funzionario incaricato verifica che la scansione corrisponda effettivamente all'originale analogico (ad esempio controlla che siano state acquisite tutte le pagine e che queste siano leggibili nella loro interezza, ecc.)
- Se l'esito è positivo, compila il documento di attestazione *(vedi Allegato 1 al presente documento)* seguendo le indicazioni scritte in rosso, e lo salva in formato PDF

---

[7] CAD art. 22 c. 4: "*Le copie formate ai sensi dei commi 1, 1-bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico,* e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5".

[8] CAD art. 22 c. 1-bis: "La *copia per immagine su supporto informatico di un documento analogico* è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, *previo raffronto dei documenti o attraverso certificazione di processo* nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia."

[9] ibidem

- Quindi unisce in un unico file in formato PDF[10] i documenti ottenuti dalla scansione del documento originale e dal salvataggio del documento descritto al punto precedente
- Procede a firmare digitalmente il documento informatico ottenuto
- Infine, allega il documento firmato digitalmente alla registrazione di protocollo, inserendo eventualmente una annotazione del tipo *"Copia informatica conforme all'originale analogico allegata in data gg/mm/aaaa"*.

[10] Tra i molti software che consentono l'unione di più documenti in un unico file, si suggerisce di utilizzare la versione basic di PDFsam (https://pdfsam.org/download-pdfsam-basic/) software gratuito, *open-source* e *cross-platform*, che offre molte altre funzionalità utili per la manipolazione di file PDF. Per ovvi motivi di tutela delle informazioni, si sconsiglia invece l'uso di utility di elaborazione on-line, che richiedono l'esportazione dei documenti da elaborare verso server di terze parti.

- **Esempi, domande e risposte**

Come verifico se un file è firmato digitalmente?

Se si tratta di un file con estensione PDF (quindi in formato PAdES), puoi utilizzare lo stesso programma con il quale lo visualizzi (*Acrobat Reader* o qualunque pdf reader di recente rilascio), oppure un software per la firma digitale come *Go Sign Desktop*. Quest'ultimo tipo di software è invece la scelta esclusiva se il file ha estensione P7M, ed è quindi firmato in modalità CAdES.

Devo firmare digitalmente un file PDF e includere anche una tabella in formato Excel, quale formato di firma posso utilizzare?

Poiché il formato PAdES si applica solo ai file di tipo PDF, dovrai necessariamente utilizzare il formato CAdES: il risultato sarà un file con estensione p7m che conterrà al suo interno i due file.

Devo inviare ad un destinatario esterno all'ateneo un documento protocollato su Titulus. È sufficiente l'annotazione del dirigente come firma?

Assolutamente no. Le annotazioni non sostituiscono in alcun modo la sottoscrizione del documento e non vengono rese disponibili ai destinatari esterni, poiché sono attinenti alla procedura e non al documento. Titulus in questo caso può soltanto certificare la provenienza del messaggio dal sistema di protocollo dell'Ateneo (attraverso la PEC associata alla AOO mittente), ma il documento risulterà privo di sottoscrizione. L'allegato dovrà necessariamente essere firmato digitalmente prima dell'invio ai destinatari.

Mi è stato assegnato (in qualità di RPA o CC) un documento di Titulus, ma ritengo non sia di mia competenza. Penso di inserire un'annotazione per comunicare l'errore al protocollo.

Non è la scelta corretta. L'annotazione non va utilizzata in sostituzione di altri mezzi di comunicazione (e-mail, telefono, Teams...), ben più adatti al caso in argomento, ma per di più non modifica in alcun modo l'attribuzione data al documento. Piuttosto, è possibile rigettare il documento (se si è RPA) o rimuoversi dai CC, per mezzo dei pulsanti a ciò dedicati, e contattare diversamente l'operatore per segnalargli il disguido.

Ho redatto un documento con Word, che ho poi stampato su carta: posso effettuarne la scansione per firmarlo digitalmente?

Sebbene sia un'operazione possibile in quanto il risultato sarà comunque un file validamente firmato, si tratta di una procedura inutilmente ridondante (perché non esportare il file in formato PDF e firmarlo digitalmente?), formalmente deprecata ai sensi della normativa che regola la formazione dei documenti presso le pubbliche amministrazioni, che costituisce uno spreco di risorse e il cui prodotto spesso genera errori in Titulus. Inoltre, i file così creati hanno dimensioni di gran lunga superiori e di solito impediscono l'indicizzazione del contenuto e la ricerca di testo al suo interno.

L'immagine della firma che appare sul documento firmato digitalmente è firma autografa?

No. L'immagine della firma è un artificio tecnico utilizzato in un documento in formato PDF (firma PAdES) per creare un *effetto analogico* sul documento informatico firmato digitalmente. Legalmente non presenta aspetti negativi, in quanto gli strumenti di verifica della firma digitale non sono influenzati dall'inserimento contestuale di questa immagine della firma. D'altra parte, questa funzionalità è fuorviante perché crea un'ambigua similitudine tra il cartaceo e il digitale, favorendo la mentalità analogica rispetto a quella digitale, che è diversa e tale deve essere nel modo meno equivoco possibile.

Devo protocollare un messaggio di posta elettronica pervenuto all'indirizzo istituzionale personale/di struttura. Posso stamparlo in PDF e caricarlo su Titulus?

No. Come già detto, un messaggio e-mail è un documento sottoscritto con *firma elettronica*. La sua stampa in formato PDF viola il requisito di integrità del documento[11], in quanto tale operazione elimina dal messaggio tutte le informazioni riguardanti il trasporto (data, ora, indirizzo del mittente, percorso del messaggio, ecc.) utili alla valutazione in fase di giudizio, rendendo di fatto non più valida la firma. Inoltre, la stampa non tiene in considerazione la presenza di eventuali allegati, o al più riproduce quelli visibili come immagine. Per la corretta registrazione sul sistema di protocollo, il messaggio va quindi estratto dal client di posta nel suo formato nativo. Il metodo di estrazione del messaggio dipende dal client utilizzato. Il risultato sarà un singolo file (solitamente con estensione *.eml*, più raramente *.msg*) che conterrà il corpo del messaggio, tutti gli eventuali allegati e manterrà inalterate le altre informazioni che lo corredano.

Il responsabile del procedimento, nelle trasmissioni di documenti alla firma del DG e del Rettore, deve apporre l'annotazione "F.to il Responsabile del procedimento"?

Questa domanda è frutto di un fraintendimento. L'uso della locuzione "*F.to*" o qualunque riferimento alla "firma" nelle annotazioni non fa altro che creare confusione. Se è richiesta una firma sul documento, il documento va firmato digitalmente. Diversamente, l'annotazione NON COSTITUISCE NE' SOSTITUISCE IN ALCUN MODO LA SOTTOSCRIZIONE DEL DOCUMENTO. E' una manifestazione di volontà e di instradamento che agisce sul flusso procedurale, e che contribuisce (oppure osta) al suo avanzamento. Con riferimento al caso indicato, una annotazione significativamente e funzionalmente corretta potrebbe essere *"Nella qualità di responsabile del procedimento, lo scrivente approva [dà il proprio assenso, nega il consenso, sconsiglia/restituisce per i seguenti motivi, ecc.]*".

È in uso la modalità di firma tramite la locuzione "F.to Nome e Cognome" (apposta da un soggetto diverso), in calce al documento con la seguente annotazione riportata nella correlata protocollazione: "la presente nota è da intendersi firmata"

Molto più che deprecabile, tale modalità potrebbe facilmente rientrare tra le fattispecie di reato previste dal codice penale per il **falso in atto pubblico** (art. 483) o la **sostituzione di**

[11] art. 20 CAD, comma 1-bis

persona (art. 494). Ancora una volta, si ribadisce che non si tratta in alcun modo di una valida sottoscrizione del documento, ed è totalmente priva di valore l'annotazione, che risulta autoreferenziale e risibilmente tautologica.

Ho ricevuto una mail dall'indirizzo di struttura della segreteria di un dipartimento. Il messaggio non è sottoscritto, ma trasmette in allegato una richiesta su carta intestata del dipartimento, in formato PDF, che riporta inoltre le firme grafiche del direttore e del RAD. Come devo comportarmi?

Questo è in pratica un compendio degli errori da evitare nella redazione di documenti e nell'invio di comunicazioni per una pubblica amministrazione. Nessuna delle parti di questo esempio contiene una sottoscrizione valida: il messaggio, proveniente da un indirizzo di email le cui credenziali sono condivise tra più utenti, non consente di riconoscerne l'autore né fornisce indicazioni utili alla sua individuazione, ma al massimo permette di circoscrivere il novero degli ipotetici mittenti. Le firme grafiche non costituiscono in alcun modo una valida sottoscrizione del documento, potendo essere facilmente copiate da un altro documento come elementi grafici, esattamente come può dirsi per la "carta intestata". Di conseguenza, l'intera comunicazione risulta *non firmata* e può essere legittimamente considerata priva di valore.

Appendice

Obblighi relativi al corretto utilizzo della firma elettronica qualificata, delle credenziali personali e sanzioni derivanti dalla loro inosservanza

DLgs n. 82/2005 Codice dell'amministrazione digitale -
Art. 32 - Obblighi del titolare e del prestatore di servizi di firma elettronica qualificata
1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad ***utilizzare personalmente il dispositivo di firma.***

C.P. - Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici.
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

C.P. - Art. 491-bis. Documenti informatici
Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.

C.P. - Art. 493. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.
Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio, relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

C.P. - Art. 494. Sostituzione di persona.
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno.

Cassazione penale, sez. V, sent 27/08/2013, 35543 e 10/3/2009, 16328:
(...) sul piano oggettivo, ai fini della sussistenza del reato di falso in scrittura privata (art. 485 c.p.), il consenso o l'acquiescenza della persona di cui sia falsificata la firma, non svolge alcun rilievo, in quanto la tutela penale ha per oggetto non solo l'interesse della persona offesa, apparente firmataria del documento, ma anche la fede pubblica, la quale è compromessa nel momento in cui l'agente faccia uso della scrittura contraffatta per procurare a sé un vantaggio o per arrecare ad altri un danno; pertanto anche l'erroneo convincimento sull'effetto scriminante del consenso costituisce una inescusabile ignoranza della legge penale. Sul piano soggettivo, nel delitto in questione, per l'integrazione del dolo specifico non occorre il perseguimento di finalità illecite, poiché l'oggetto di esso è costituito dal fine di trarre un vantaggio di qualsiasi natura, legittimo od illegittimo.

Cass.Pen. Sez.V, Sent. 5/7/1990
(...) posto che il verbale di ricezione di dichiarazione di appello da parte del cancelliere costituisce un atto pubblico facente fede fino a querela di falso, sussiste il reato di falso in atto pubblico anche qualora tale verbale sia stato redatto e sottoscritto da un coadiutore giudiziario col consenso del cancelliere (...)

Cass. Pen., sez. V, 12/7/2011, 32856 e Cass. Pen., sez. V, 12/5/2011, 24917
In tema di falsità ideologica in atto pubblico (art. 483 c.p.), ai fini della sussistenza dell'elemento soggettivo è sufficiente il dolo generico, e cioè la volontarietà e la consapevolezza della falsa attestazione, mentre non è richiesto l'animus nocendi nè l'animus decipiendi, con la conseguenza che il delitto sussiste non solo quando la falsità sia compiuta senza l'intenzione di nuocere ma anche quando la sua commissione sia accompagnata dalla convinzione di non produrre alcun danno

Allegato

Modulo per l'attestazione della conformità della copia informatica di originale analogico

Università degli Studi di Palermo

Copia informatica di documento analogico
Dichiarazione di conformità all'originale

Si attesta che **il presente documento è copia informatica conforme al documento analogico originale**, ai sensi degli artt. 22 e 23-ter del D.Lgs 82/2005 e successive modifiche. **Il documento cartaceo originale è assunto agli archivi di questa Amministrazione e ivi conservato.**

Qui di seguito i dati del documento analogico originale e di colui che ne attesta la conformità.

Dati del documento analogico originale:	
Nome e cognome del firmatario:	*indicare nome e cognome di colui che ha firmato il documento originale*
Data in cui è stata apposta la firma:	*indicare la data e l'ora in cui il documento originale è stato firmato*
Numero dei fogli del documento analogico originale:	*indicare il numero di fogli di cui è composto il documento originale*
Luogo fisico in cui è conservato il documento analogico originale:	*indicare dove è conservato il documento originale (ad esempio "in archivio corrente presso questo ufficio" o "in archivio di deposito")*
Stato del documento:	*indicare, a seconda del caso, la frase "Documento emesso da questo ufficio" oppure "Documento depositato presso questo ufficio"*

Dati relativi a colui che attesta la conformità della copia informatica al documento analogico originale:	
Nome e cognome:	*indicare nome e cognome di colui che sta attestando la conformità della copia*
Qualifica:	*indicare la categoria e l'ufficio di appartenenza di colui che sta attestando la conformità della copia*

Documento firmato digitalmente ai sensi della normativa vigente