“MANUALE OPERATIVO ALLA CLIENTELA”
PER GLI ADEMPIMENTI VERSO DI ESSA PRESCRITTI IN MATERIA DI FIRMA ELETTRONICA AVANZATA

(Documento [1] predisposto ai sensi del DPCM 22.2.2013 [2])

[1] Aggiornato al 27/10/2014

[2] DPCM 22 febbraio 2013, Regole Tecniche in materia di generazione, apposizione, e verifica delle firme elettroniche avanzate, qualificate e digitali

Note di Redazione

[<rif. articolo, comma, lettera>] **:** *riferimenti al DPCM*

[# rif. tabella>] **:** *riferimenti alla tabella di analisi del DPCM*

Contenuti

1. INFORMAZIONI GENERALI 5

1.1 NATURA GIURIDICA DELLA FIRMA ELETTRONICA 5
1.2 FINALITA' DELLA FIRMA ELETTRONICA AVANZATA (FEA) 5
1.3 AMBITO DI UTILIZZO: CON CHI E QUANDO E' POSSIBILE UTILIZZARE LA FEA 5
1.4 AFFIDABILITA' DELLA SOLUZIONE 6
1.5 COPERTURA ASSICURATIVA 6
1.6 COME FUNZIONA IL SERVIZIO DI FEA 6

2. LA DICHIARAZIONE/CONTRATTO DI ACCETTAZIONE ALL'USO DELLA FEA 7

3. LA SOTTOSCRIZIONE CON FEA 8

3.1 IL PROCESSO DI SOTTOSCRIZIONE 8
3.2 COME OTTENERE UNA COPIA DI UN DOCUMENTO INFORMATICO SOTTOSCRITTO 9
3.3 COSA SI TROVA NELLA COPIA DI UN DOCUMENTO INFORMATICO SOTTOSCRITTO 9

4. CARATTERISTICHE DEL SISTEMA FEA 11

4.1 IL SOGGETTO CHE EROGA LA SOLUZIONE 11
4.2 IL FIRMATARIO 11
4.2.1 Identificazione del firmatario *11*
4.2.2 Controllo esclusivo della firma da parte del firmatario *12*
4.3 LA FIRMA 13
4.3.1 Connessione univoca della firma al firmatario *14*
4.3.2 Connessione univoca della firma al documento sottoscritto *14*
4.4 IL DOCUMENTO INFORMATICO 15
4.4.1 Conservazione del documento informatico sottoscritto *15*

ALLEGATI/APPENDICI 16

A – PRINCIPALI RIFERIMENTI NORMATIVI SULLA FIRMA ELETTRONICA 16

Glossario di Acronimi e Termini

DPCM	Decreto del Presidente del Consiglio dei Ministri della Repubblica Italiana
CERTIFICATO DIGITALE	Documento crittografico contenente i dati identificativi dell'intestatario e la sua chiave pubblica firmato dall'autorita' di certificazione che attesta tali dati effettuando l'identificazione del soggetto
CHIAVI	Coppia di elementi (chiave privata o secret key e chiave pubblica o public key) costituitivi di un sistema di crittografia asimmetrica (Infrastruttura a Chiave Pubblica o PKI) entrambi univocamente associati a ciascun attore. Di tale coppia univoca di chiavi, solo la chiave privata e' personale e segreta (nel caso specifico e' quella usata per la firma)
FEA	Firma Elettronica Avanzata
PIN	Personal Identification Number
OTP	One Time Password
SSCD	Secure Signature-Creation Device
HSM	Hardware Security Module
LTANS	Long-Term Archive and Notary Services
RSA	Iniziali di Rivest, Shamir, Adleman
ETSI	European Telecommunications Standards Institute

1. INFORMAZIONI GENERALI

1.1 Natura Giuridica della Firma Elettronica

[DPCM 22 febbraio 2013, Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali]

Il Gruppo BNL S.p.A. ha introdotto la tecnologia della firma elettronica per mezzo della quale e' possibile firmare documenti bancari, o autorizzare transazioni, in formato elettronico ed eliminare cosi' il ricorso alla carta oltre che velocizzare l'esecuzione dei propri processi e semplificare l'operativita' al Cliente.
I documenti e/o le transazioni che con tale modalita' vengono sottoscritti o autorizzati dal Cliente, sono documenti informatici che sul piano giuridico hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa.

1.2 Finalita' della Firma Elettronica Avanzata (FEA)

[art.55, comma 2]
[# 0.2]

Oltre alla firma elettronica e alla firma digitale BNL ha recentemente introdotto ulteriori servizi innovativi basati sulla tecnologia della Firma Elettronica Avanzata (FEA) avendo l'obiettivo, limitatamente ai rapporti commerciali ed operativi con essa intrattenuti, di estendere gradualmente, e per quanto possibile, l'utilizzo della sottoscrizione elettronica a tutta la propria clientela, coprendo tutte le esigenze e situazioni che ne dovessero richiedere l'uso nell'ambito dello svolgimento dei propri processi di vendita ed operativi.

1.3 Ambito di Utilizzo: con chi e quando e' possibile utilizzare la FEA

[art.55, comma 2]
[# 0.2]

Il servizio di firma elettronica avanzata, nelle attuali implementazioni, consente al cliente di manifestare il consenso o sottoscrivere contratti/documenti che riguardano i rapporti con la Banca o le societa' cui la Banca colloca/distribuisce prodotti/servizi, ossia, solo a titolo di esempio:

- i contratti, per cui e' prevista la FEA, che egli intende stipulare con la propria banca
- i contratti, per cui e' prevista la FEA, che egli intende stipulare con le societa' di cui la Banca colloca/distribuisce prodotti/servizi
- le operazioni, per cui e' prevista la FEA, connesse ai rapporti che egli intrattiene con la Banca o con le altre societa' o enti (nei casi previsti).

1.4 Affidabilita' della Soluzione

[art.55, comma 1], [art.59 comma 1, 2]
[# 0.1], [# 2.18, 2.19]

Tutte le soluzioni scelte e le implementazioni adottate da BNL possiedono i requisiti informatici e giuridici cosi' come previsti e definiti dalla Direttiva Europea e dalla normativa nazionale in materia.
Per maggiori dettagli sulla base normativa che regola la firma elettronica si rimanda ai riferimenti riportati in allegato.

1.5 Copertura Assicurativa

[art.57 comma 2, 3]
[# 2.16, 2.17>]

BNL ha stipulato, in conformita' alla normativa vigente, polizza assicurativa con primaria Compagnia assicuratrice a tutela dei danni eventualmente derivanti/causati da problemi tecnici riconducibili all'utilizzo della FEA.

1.6 Come Funziona il Servizio di FEA

[art.57 comma 1, lettera d (sintesi)]
[# 2.11>]

- il Cliente e' riconosciuto e identificato
- il Cliente acconsente ad utilizzare il servizio di FEA
- la Banca provvede ad abilitare il servizio
- la Banca richiede al Cliente, laddove previsto, di sottoscrivere un contratto/documento
- il Cliente, presa visione del contratto/documento da sottoscrivere, manifesta la volonta' di firmare utilizzando gli strumenti di cui e' dotato e dei quali ha esclusivo controllo e disponibilita'
- i sistemi di Banca, previa verifica e autenticazione positiva del Cliente e della sua richiesta di cui al punto precedente, provvedono ad eseguire la sottoscrizione con FEA tramite la sua chiave privata custodita nel dispositivo sicuro di firma

2. LA DICHIARAZIONE/CONTRATTO DI ACCETTAZIONE ALL'USO DELLA FEA

[art.57 comma 1, lettera a], [art.57 comma 1, lettera h]
[# 2.2, 2.3, 2.4], [# 2.15]

L'utilizzo della firma elettronica con valore di Firma Elettronica Avanzata avviene solo dopo che il Cliente, opportunamente e preliminarmente riconosciuto, in conformita' a quanto prescritto dalla normativa, abbia manifestato la sua volonta' di accettare, con un'apposita dichiarazione/contratto di autorizzazione, l'utilizzo di tale strumento.
In tale dichiarazione/contratto, rilasciato al Cliente successivamente alla sua sottoscrizione, sono riportati nel dettaglio i termini e le condizioni di uso del servizio ivi compresa qualsiasi sua eventuale limitazione.

Il Cliente puo' chiedere in ogni momento, gratuitamente, una copia della suddetta dichiarazione/contratto di accettazione. Questa richiesta puo' essere fatta, per iscritto, a una qualunque filiale della Banca del Gruppo BNL.
Il Cliente, nei casi in cui la procedura lo preveda, puo' reperire una copia del suddetto contratto all'interno del proprio Home Banking (ove attivato dallo stesso cliente).

Il Cliente puo' anche richiedere, nelle modalita' previste, supporto al servizio di help desk (800.900.900) per eventuali informazioni relative al servizio di Firma Elettronica Avanzata.

3. LA SOTTOSCRIZIONE CON FEA

[art.57, comma 1, lettera e => descrizione procedurale]

3.1 Il Processo di Sottoscrizione

[art.56, comma 1, lettera a, c, g]
[# 1.1, 1.3, 1.7]

Nei casi in cui il Cliente intendesse utilizzare il servizio di FEA, ove operativamente previsto, il processo applicativo della Banca provvedera' a:

- produrre il documento informatico da sottoscrivere
- sottoporre tale documento, per visione e controllo, al Cliente
- richiedere al Cliente di effettuarne la sottoscrizione con FEA mediante l'utilizzo delle sue personali credenziali di identificazione fornitegli da BNL e dei mezzi/strumenti in esclusivo-personale possesso e disponibilita' del Cliente stesso, quali ad esempio:

  a. PIN [1] e OTP [2] (tramite hardware token e/o mobile token per la produzione del valore dell'OTP)

  b. firma autografa apposta personalmente dal Cliente su supporto informatico costituito da tablet/tavoletta mediante apposita penna in grado di acquisire (senza conservazione) i dati comportamentali [3] rilevabili dal segno rappresentante la sua firma

Conseguentemente all'esecuzione delle operazioni di cui sopra, con le quali il Cliente manifesta la sua volonta' di sottoscrizione, i sistemi e l'infrastruttura di Banca, provvederanno a:

- acquisire i dati
- effettuare le verifiche di autenticazione.
- solo e soltanto in caso di esito positivo, eseguire il processo di sottoscrizione:

- firmando con la chiave del Cliente protetta e custodita in un dispositivo sicuro di firma
- mettendo a disposizione il documento informatico sottoscritto dando notifica dell'esito finale

In sintesi, in un contesto sicuro e in modo verificabile e certo, il processo precedentemente descritto, implementa i passi di:

[1] Personal Identification Number

[2] Password (One Time Password) crittograficamente generata, utilizzabile una singola volta per una singola operazione

[3] Ritmo, pressione, velocità, accelerazione, movimento, etc. Tali dati non vengono direttamente conservati dalla Banca ma sono tradotti in codici alfanumerici che restano riconducibili al Cliente senza peraltro poter, tramite essi, riprodurre i dati biometrici originali

i. identificazione del Cliente
ii. presa visione da parte del Cliente del documento informatico da sottoscrivere
iii. richiesta al Cliente di sottoscrivere con FEA quel documento informatico
iv. sottoscrizione con FEA eseguita dal Cliente, con gli strumenti personali che sono nella sua esclusiva disponibilita', in quel momento, di quel documento informatico
v. messa a disposizione del documento informatico sottoscritto con FEA dando notifica dell'esito di esecuzione della sottoscrizione medesima

3.2 Come Ottenere una Copia di un Documento Informatico Sottoscritto

[art.57, comma 1, lettere c, d]
[# 2.10, 2.11]

Il Cliente puo' richiedere copia dei documenti da lui sottoscritti e, in particolare, nel caso abbia firmato un contratto, deve ricevere un esemplare del contratto avente tutti i requisiti stabiliti dalla legge.
Nel caso in questione, essendo i documenti di cui trattasi, dei documenti informatici, ogni copia eventualmente prodotta e rilasciata risulta essere identica e conforme al documento originale e, rispetto al quale, vengono mantenute, parimenti inalterate, tutte le stesse caratteristiche presenti nel documento di origine.
Cio' premesso, e' nella facolta' del Cliente richiedere "copia" elettronica dei documenti informatici sottoscritti, conservati dalla Banca nei termini di tempo previsti dalla legge.

3.3 Cosa si Trova nella Copia di un Documento Informatico Sottoscritto

[art.56 comma 1, lettere b, d, e, f]
[# 1.2, 1.4, 1.5, 1.6]

A seguito della sottoscrizione con FEA, l'originario documento informatico viene trasformato, nel caso specifico e in modo conforme ai formati standard previsti, in un documento firmato elettronicamente.
Scorrendo e leggendo il testo del documento informatico sottoscritto con FEA, risulteranno visibili, in appositi spazi all'interno del layout del documento sottoscritto, delle immagini aventi lo scopo di riportare e rappresentare, in termini puramente "grafici", alcuni dei dati specifici ottenuti e risultanti dalla corrispondente ed eseguita operazione di FEA effettuata sul documento medesimo.
Qualora il Cliente voglia visualizzare e conoscere il/i firmatario/i che ha/hanno sottoscritto digitalmente il documento informatico (riferibile allo stesso Cliente) e a quali parti di esso corrisponda ciascuna sottoscrizione con FEA, e' necessario che egli apra la specifica sezione, o voce di menu', riguardante le "firme elettroniche", resa a tal fine disponibile dalla/e applicazione/i

di visualizzazione.
In estrema sintesi i dati visualizzati conterranno:

- le informazioni relative a ciascun firmatario presente
- le parti del documento informatico corrispondenti a ciascuna firma apposta
- le informazioni del/i soggetto/i firmatario/i in forma di certificato digitale che associa l'identita' digitale del firmatario/i.

I documenti informatici cosi' sottoscritti assumono la forma e le caratteristiche atte a deteminare e garantire la riconducibilita' al sottoscrittore (verifiche di integrita' del documento e di identita' del/i sottoscrittore/i) assicurandone, anche, come meglio dettagliato in seguito, la loro autonoma verificabilita'.

4. CARATTERISTICHE DEL SISTEMA FEA

[art.57 comma 1, lettera e => descrizione tecnica (art.56, comma 1, lettere a, b, c, d, e, f, g, h)]

4.1 Il Soggetto che Eroga La Soluzione

[art.55 comma 2, lettera a], [art.56 comma 1, lettera f]
[# 0.2], [# 1.6]

Il soggetto erogatore del servizio di FEA e' BNL che lo svolge solo ed esclusivamente nell'ambito dei rapporti intrattenuti fra i Clienti e la Banca o, comunque, nei casi e situazioni descritte in maggior dettaglio al precedente paragrafo 1.3.

4.2 Il Firmatario

[art.56 comma 1, lettera a], [art.57 comma 1, lettera a]
[# 1.1], [# 2.1]

I soggetti che possono sottoscrivere con FEA i documenti informatici sono il Cliente e, per quanto riguarda la Banca, laddove previsto, i funzionari ai quali risulti assegnato, in quel momento, l'esercizio di quel ruolo-funzione operativa.

4.2.1 Identificazione del firmatario

[art.56 comma 1, lettera a], [art.57 comma 1, lettera a], [art.57 comma 1, lettera h]
[# 1.1], [# 2.4], [2.15]

Ciascun Cliente, secondo quanto previsto dalla normativa bancaria (con particolare riferimento anche alla normativa in tema di antiriciclaggio), viene sottoposto alla procedura di riconoscimento/identificazione [4] e gli vengono, quindi, consegnati i mezzi/strumenti di uso strettamente personale per poter assolvere pienamente all'operativita' richiesta e prevista dai servizi di cui potra' fruire ed in assenza dei quali la sua operativita' risulterebbe in sostanza inibita.

Inoltre, per essere abilitato al servizio di FEA, il Cliente deve aver sottoscritto, contestualmente o meno alle operazioni precedenti, la dichiarazione/contratto di autorizzazione all'uso della FEA.

Espletate con successo tutte le precedenti operazioni, il certificato digitale [5] viene generato e associato ad una chiave pubblica unica del Cliente mentre la corrispondente chiave privata viene tenuta memorizzata e custodita in un dispositivo sicuro di firma (denominato con l'acronimo SSCD [6]) implementato, nel caso specifico di Banca, tramite HSM [7]). I certificati digitali e le chiavi,

---

4 Procedura equipollente e conforme alle normative vigenti previste per le autorita' di registrazione

5 Certificato X.509 attestante l'identita' digitale del Cliente e l'associazione alla sua persona fisica

6 Secure Signature-Creation Device, dispositivo definito e previsto dalla normativa, atto a garantire i piu' elevati standard di sicurezza per la firma digitale

7 Hardware Security Module, denominato commercialmente HSM. Tali prodotti implementano elevati

pubblica e privata, pertanto, non sono rialsciate fisicamente al Cliente; esse, previa autenticazione del Cliente, vengono attivate e movimentate all'interno dei sistemi Banca.
Solo da questo momento risulta operativamente abilitato l'uso della FEA per il Cliente e solo da allora, tramite i mezzi di identificazione direttamente ed esclusivamente controllati dal Cliente stesso, risulta possibile effettuare la sottoscrizione di documenti informatici con FEA.

4.2.2 Controllo esclusivo della firma da parte del firmatario

[art.56 comma 1, lettera c]
[# 1.3]

Ogni qualvolta al Cliente viene richiesto di firmare un documento informatico con FEA, nell'ambito dei rapporti contrattuali della Banca, egli, qualora lo voglia sottoscrivere, potra' farlo, sotto il suo esclusivo controllo e volonta' e, a seconda dei diversi contesti applicativi e operativi, operando, e conformando la sua azione, nel seguente modo:

a. imputando, insieme alle sue credenziali personali (username e pin), l'OTP prodotto in quel momento dal suo hardware/mobile token

b. facendo, in quel momento, nello spazio apposito visualizzato sullo schermo del tablet e con la contestuale presenza di un operatore di Banca, il segno della sua firma autografa mediante un apposito pennino capace di rilevare i relativi valori comportamentali

I suddetti dati ed eventi, acquisiti dai sistemi e dall'infrastruttura di banca su canali sicuri e cifrati, in conformita' con quanto prescritto dalla normativa vigente in materia, hanno le seguenti caratteristiche:

- assicurano l'autenticazione del Cliente, in quanto soltanto a lui riconducibili
- attestano l'esercizio del controllo esclusivo del Cliente, essendo egli l'unico soggetto ad averli potuti fornire in virtu' del fatto che sono forniti/prodotti/generati da quegli strumenti di uso strettamente personale che sono stati a lui esclusivamente associati-consegnati e risultano, quindi, nel suo esclusivo possesso, controllo e disponibilita'
- garantiscono l'esercizio della manifestazione della volonta' del Cliente in quanto i suddetti dati hanno valori diversi per ciascuna operazione di firma e sono strettamente e singolarmente (individualmente) collegati ad ogni singolo documento firmato

profili di sicurezza in conformità dei quali sono obbligati a dotarsi delle corrispondenti certificazioni internazionali cosi' come previsto e prescritto dalla normativa in materia

Nella fattispecie, infatti, in virtu' delle verifiche di correttezza e di autenticazione, e' possibile associare documenti firmati, identita' del Cliente e ogni singola operazione di firma relativa all'evento di sottoscrizione, risultando essere, i valori assunti da tali dati, unici e distintivi, per quanto sopra detto, di ciascuna manifestazione di volonta'.

Conseguentemente, solo e soltanto in caso di esito positivo delle suddette verifiche di correttezza e di autenticazione effettuabili ed effettuate sui dati acquisiti, verra' effettivamente autorizzata ed eseguita la firma con la chiave privata di quel Cliente protetta e custodita nel dispositivo sicuro di firma.

In conformita' e a completamento dei requisiti di assessment e di sicurezza, in ordine a garantire trasparenza, tracciabilita' e ricostruibilita' (auditing) di ogni singola istanza dei processi di sottoscrizione, i sistemi e l'infrastruttura di Banca provvedono, contestualmente a quanto sopra descritto, a tracciare su un log, conforme allo standard LTANS [8] e reso opponibile a terzi, la cronologia degli eventi e del corrispondente insieme di valori caratterizzanti ciascuna operazione di sottoscrizione avvenuta.

4.3 La firma

[art.56, comma 1, lettera h]
[# 1.8]

La firma del documento informatico attraverso il dispositivo sicuro di firma (HSM) dove sono protette e custodite le chiavi private ed il cui utilizzo ed esecuzione vengono automaticamente autorizzati e "sbloccati" solo in caso di positivo esito delle verifiche precedentemente descritte, e' realizzata ed implementata in modo conforme a quanto avviene per la firma digitale, ovvero:

- viene calcolata, dal documento in input oggetto della sottoscrizione, la sua impronta informatica [9] tramite un algoritmo standard conforme alla normativa [10] che assicura e garantisce che l'output ottenuto abbia la caratteristica di essere una rappresentazione univoca del documento informatico su cui l'impronta stessa e' stata calcolata.

---

[8] Long-Term Archive and Notary Services, standards relativi ai servizi di trust nell'ambito dell'archiviazione a lungo termine

[9] L' ''impronta informatica'' di un file e' definita come la sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione di una funzione di calcolo, detta funzione di hash, che consente di identificare in modo preciso il file stesso, e tale per cui:

- uno stesso file cui è applicata la stessa funzione di hash genera sempre la medesima impronta e pertanto la stringa ottenuta in output è univoca per ogni file e ne è un identificatore
- dall'impronta informatica non è possibile risalire al contenuto del documento informatico che l'ha generata, ma essa consente di verificare se il documento originario è stato modificato.

[10] Nella fattispecie, algoritmo SHA-256

- le operazioni di calcolo crittografico vengono eseguite e assicurate all'interno del dispositivo sicuro di firma (HSM)

4.3.1 Connessione univoca della firma al firmatario

[art.56 comma 1, lettera b]
[# 1.2]

Analogamente, la connessione della firma al firmatario e' garantita secondo le stesse modalita' tecnico-tecnologiche utilizzate dalle normative relative alla firma digitale.
L'implementazione della FEA da parte di BNL, infatti, e' basata sull'utilizzo di coppie di chiavi asimmetriche [11], ovvero:

- la chiave (parte privata), protetta e custodita in un dispositivo sicuro di firma:
  - e' associata univocamente all'identita' del Cliente
  - e' usata per firmare un documento informatico (ovvero cifrarne l'impronta)
  - ogni suo utilizzo, richiede l'autorizzazione la quale deve essere data ogni volta e puo' essere fornita solo dal suo titolare (Cliente)

- la parte pubblica della chiave, contenuta nel certificato digitale:
  - e' associata univocamente all'identita' dello stesso Cliente
  - puo' essere utilizzata da chiunque per effettuare le operazioni tecniche di verifica del documento informatico firmato digitalmente dal Cliente cui corrisponde quel certificato digitale

4.3.2 Connessione univoca della firma al documento sottoscritto

[art.56 comma 1, lettera h]
[# 1.8]

Il documento informatico sottoscritto con FEA e' un documento, o oggetto documentale, unico.
A seguito dell'apposizione della firma, il documento informatico da sottoscrivere viene trasformato dalla operazione di firma in modo conforme ai formati standard previsti per i documenti firmati digitalmente, al cui interno sono stati introdotti, e inseparabilmente contenuti, i certificati di tutti i sottoscrittori.
I documenti informatici cosi' firmati e formati godono della proprieta' di poter essere verificati in qualsiasi momento tramite l'applicazione, su quel documento informatico, di procedure ed algoritmi crittografici standard.

[11] Public Key Infrastructure con algoritmo RSA, algoritmo crittografico che prende il nome dalle iniziali dei ricercatori che lo hanno inventato: Ronald Rivest, Adi Shamir, Leonard Adleman

4.4 Il Documento Informatico

[art.56 comma 1, lettere d, e, g]
[# 1.4, 1.5, 1.7]

Il documento informatico da sottoscrivere e' prodotto in modo da assicurare la conformita' a quanto prescritto dalla normativa per l'oggetto della sottoscrizione riguardo, cioe', all'assenza di elementi atti a modificarne nel tempo dati in esso originariamente contenuti al momento della sua produzione.

Del documento, da sottoscrivere o sottoscritto con FEA, in quanto prodotto in conformita' degli standard specificati da ETSI [12] secondo la normativa italiana ed europea, e' inoltre assicurato il mantenimento della loro leggibilita' e validita' nel tempo tramite apposizione e, ove necessario, rinnovo di marche temporali [13].

4.4.1 Conservazione del documento informatico sottoscritto

[art.57 comma 1, lettera b]
[# 2.5, 2.6, 2.7, 2.8, 2.9]

La conservazione a norma e' un processo che permette di custodire nel tempo i documenti informatici, sottoscritti o meno, che devono essere archiviati.

Esso garantisce, nel lungo termine, ovvero dall'inizio della conservazione e per tutto il tempo di custodia previsto e richiesto, il mantenimento continuo ed ininterrotto delle caratteristiche di validita' originarie di ciascun oggetto messo in conservazione assicurandone, insieme alla reperibilita' e riesibizione per tutta la durata del periodo di archiviazione/conservazione, anche il rispetto delle norme sul trattamento dei dati.

I documenti informatici sottoscritti con FEA, e qualsiasi altro documento e informazione o registrazione anche di assessment, vengono custoditi da BNL in un proprio sistema di conservazione conforme alla normativa vigente.

Nella fattispecie alla fine del processo di sottoscrizione con FEA, i sistemi e l'infrastruttura di Banca provvedono a imbustare i documenti informatici suddetti, nonche' le informazioni o registrazioni teste' menzionate, nel formato conforme agli standard di archiviazione a lungo termine e ad applicare una marca temporale emessa da una Autorita' di Certificazione terza al fine di “sigillare” con data certa l'inizio della loro messa in archiviazione e conseguente conservazione.

---

[12] European Telecommunications Standards Institute

[13] Una marca temporale (timestamp) è una sequenza di caratteri che rappresentano, secondo un formato standard, una data e/o un orario che accerti e certifichi l'effettivo avvenimento di un certo evento

ALLEGATI/APPENDICI

[art.57 comma 1, lettere d, g, h]
[# 2.11, 2.14, 2.15]

A – Principali Riferimenti Normativi sulla Firma Elettronica

- Direttiva Europea 99
- DPCM 22 febbraio 2013