Manuale di accreditamento e di gestione delle credenziali

Scambio dei dati via Internet per le segnalazioni di Anagrafe Soggetti, Centrale dei Rischi, AnaCredit e MMSR

Versione 1.1

luglio 2019

Storia del documento

Versione	Data	Descrizione modifiche
1.0	giu-18	Include le istruzioni precedentemente descritte nel manuale *Gestione delle credenziali application to application (A2A)* v 1.2
1.1	lug-19	Include le istruzioni per l'accreditamento e la gestione delle credenziali per le *survey* MMSR

INDICE

I. Scopo del documento

il documento descrive:

- il processo di accreditamento al servizio di trasferimento dati via *Internet* con la Banca d'Italia per l'invio delle segnalazioni di Centrale dei rischi, Anagrafe dei Soggetti, AnaCredit e Money Market Statistical Reporting (MMSR).

- le modalità di gestione della credenziale Application To Application (A2A) necessarie per autenticarsi verso i sistemi informatici che erogano il servizio

- le caratteristiche dei certificati per l'autentificazione, la crittografia e la firma dei dati.

II.Accreditamento al servizio di trasferimento dati

1. Ambiente di esercizio

Per accedere al servizio di trasferimento dati su *Internet* ciascun segnalante deve dotarsi di una propria credenziale applicativa a cui saranno associati i certificati di per l'autenticazione e crittografia dei dati.
La stessa credenziale applicativa (con i relativi certificati) è valida per il colloquio con la Centrale dei rischi, l'Anagrafe dei Soggetti, AnaCredit e MMSR.

La credenziale identifica univocamente l'intermediario e resta attiva per il tutto il tempo in cui l'intermediario scambierà informazioni con la Banca d'Italia.

Nel caso in cui un centro servizi svolga operazioni di scambio informazioni per conto di più segnalanti, dovrà utilizzare una credenziale differente per ogni segnalante.

Una volta concluso il processo di accreditamento e avviato il colloquio con la Banca d'Italia **non è possibile sostituire la credenziale**.
Invece è possibile sostituire in qualunque momento i certificati associati alla credenziale e la persona o le persone incaricate di gestirli (cfr. cap. IV).

Anche nel caso in cui l'intermediario avesse affidato la gestione delle proprie credenziali a un centro servizi e volesse riassumerne la gestione o incaricare un'altra società **non deve cambiare credenziale né ripetere l'accreditamento**, ma è sufficiente che venga delegato il nuovo gestore (manager) della credenziale. (cfr. par. IV. 5).

Il processo di accreditamento prevede due *step*:

1) registrazione della credenziale.

Un operatore incaricato dall'intermediario, dopo essersi registrato al sito della Banca d'Italia con la propria CNS, registra una **credenziale applicativa A2A**;

L'applicazione WEB dedicata alla gestione delle credenziali in ambiente di esercizio è disponibile al seguente indirizzo internet (URL): **https:// mft.bancaditalia.it/.**

Ad ogni credenziale deve essere associato almeno un certificato digitale di autenticazione e di crittografia, quest'ultimo necessario alla Banca d'Italia per cifrare le comunicazioni con la chiave pubblica del ricevente, il medesimo certificato può essere utilizzato per entrambe le funzioni.
Le modalità per registrare e gestire la credenziale sono descritte nel capitolo IV.

2) accreditamento della credenziale

L'intermediario comunica alla Banca d'Italia l'identificativo della credenziale utilizzando un apposito modulo[1] che dovrà essere compilato e firmato digitalmente dal legale rappresentante dell'intermediario e inviato a res@pec.bancaditalia.it da una casella di posta elettronica certificata (PEC).
Le istruzioni per l'invio e la compilazione del modulo sono descritte nel capitolo V.

La Banca d'Italia ricevuto il modulo accredita l'intermediario allo scambio dati via Internet e invia la notifica dell'avvenuto accreditamento all'indirizzo mail indicato nel modulo.

Attenzione: Prima di inviare le segnalazioni l'intermediario deve assicurarsi di aver ricevuto la mail di conferma. Si suggerisce anche di verificare la corretta configurazione della credenziale mediante un test di canale.

2. Ambiente di collaudo

Per accedere all'ambiente di collaudo o certificazione è necessario registrare un'apposita credenziale, non è possibile utilizzare quella registrata in ambiente di esercizio o produzione. Comunque è possibile, anzi è consigliato, associare alla credenziale di collaudo i medesimi certificati associati alla credenziale di esercizio.

Il processo di accreditamento per l'ambiente di collaudo è identico a quello descritto per l'ambiente di esercizio.

[1] Il modulo è pubblicato sul sito internet della Banca d'Italia.

L’applicazione WEB dedicata alla gestione delle credenziali dell’ambiente di collaudo è disponibile al seguente indirizzo internet (URL): **https://certmft.bancaditalia.it/**

III. Certificati e standard crittografici

1. Riepilogo certificati digitali in uso

Obiettivo	Certificato richiesto
Autenticazione	Certificato applicativo di autenticazione rilasciato da certificatore appartenente alla lista dei certificatori riconosciuta dai *browser* più comuni
Firma dei dati in ingresso a Banca d'Italia	Certificato rilasciato da certificatore accreditato AGID per il rilascio di certificati per utilizzo con dispositivo sicuro per l'apposizione della firma digitale
Cifratura dati in ingresso a Banca d'Italia	Certificato di chiave pubblica di Banca d'Italia, emesso da CA Banca d'Italia e messo a disposizione sul sito internet della Banca d'Italia
Firma dei dati in uscita da Banca d'Italia	Firma non qualificata mediante certificati emessi da CA Banca d'Italia
Cifratura dati in uscita da Banca d'Italia	Certificato di chiave pubblica di cifratura della controparte

2. Standard di riferimento

Rif.	Requisito	Standard di riferimento	Ver.	Data
R01	Firma digitale	XAdES Specifications – ETSI TS 101 903	1.4.2	**12/2010**
R02		CAdES Specifications – ETSI TS 101 733	2.2.1	**04/2013**
R03		Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – IETF RFC 5280	N/A	**05/2008**
R04		OCSP – IETF RFC 6960	N/A	**06/2013**
R05		Electronic Signatures and Infrastructures; Signature verification procedures and policies – ETSI TS 102 853	1.1.1	**07/2012**
R06		XAdES Baseline profiles – ETSI TS 103 171	2.1.1	**03/2012**
R07		CAdES Baseline profiles – ETSI TS 103 173	2.2.1	**04/2013**
R08	Cifratura	Cryptographic Message Syntax (CMS) – IETF RFC 3852		**07/2004**

IV. Gestione credenziali *application to application* (A2A)

1. Registrazione utente con Carta Nazionale dei Servizi (CNS)

Per accedere alla procedura di gestione delle credenziali applicative è necessario essere in possesso di una CNS in corso di validità.
Solo la prima volta è necessario registrare la propria identità registrando i dati della CNS, completando il profilo utente con i dati anagrafici e valorizzando i parametri di sicurezza (password, domanda e risposta segreta per recupero identità).

Di seguito le URL dell'applicazione WEB dedicata alla gestione delle credenziali:

AMBIENTE ELABORATIIVO	**Indirizzo Internet (URL)**
COLLAUDO (alias certificazione)	https://certmft.bancaditalia.it/
PRODUZIONE (alias esercizio)	https:// mft.bancaditalia.it/

NOTA: non è consentito l'utilizzo di "CNS LIKE", è previsto il solo utilizzo di CNS (o "CNS Full") rilasciate da CA presenti sull'**elenco pubblico dei certificatori che emettono certificati CNS** (Trusted LIST ITALIANA). Tale lista include tutti i certificati afferenti le autorità di certificazione che rilasciano certificati anche **per le Carte Nazionali dei Servizi**[2]**.**

L'utente digita la URL dell'applicazione e viene ridiretto sul menu di scelta delle azioni relative all'autenticazione e alla **gestione delle credenziali utente** CNS e credenziali A2A. All'utente è richiesto di inserire la propria CNS nell'apposito lettore e scegliere la prima opzione:

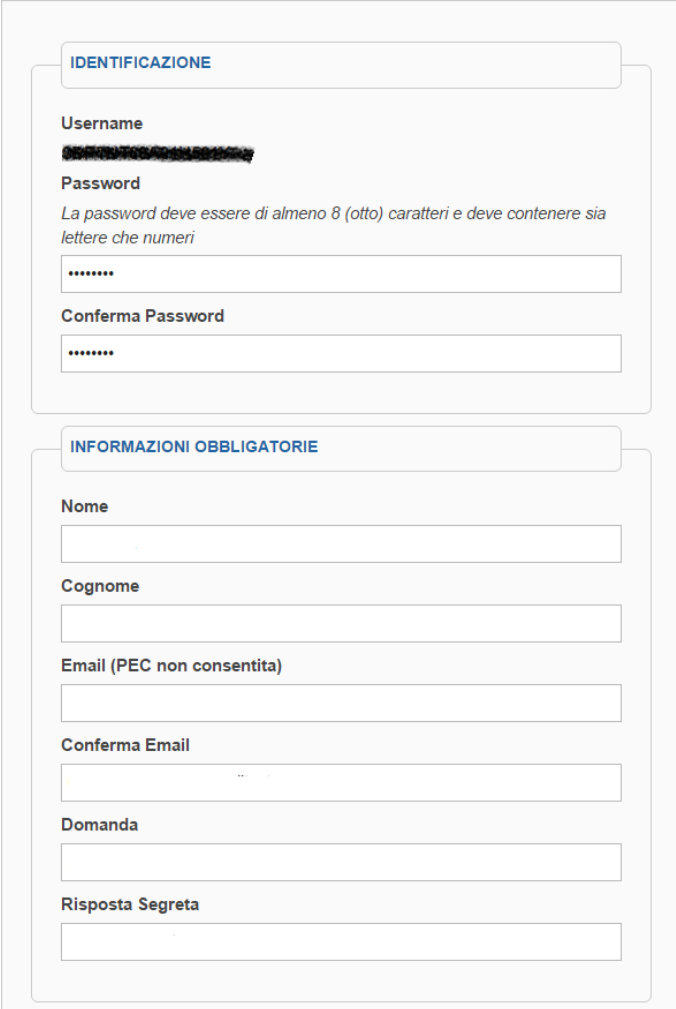
[2] Per i dettagli tecnici e normativi si rimanda al sito AGID:
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/carta-nazionale-servizi
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/certificati

All'attivazione del link l'utente è ridiretto sull'applicazione di registrazione dei dati di identificazione, i parametri richiesti sono tutti obbligatori e hanno l'obiettivo di generare un profilo utente con i dati necessari alla sua identificazione.

La ***username*** è valorizzata automaticamente con il **CODICE FISCALE** che è estratto dal campo ***subject*** del certificato di autenticazione presente sulla CNS. La *username* potrà essere utilizzata successivamente come credenziale di autenticazione sulle applicazioni internet esposte dalla Banca d'Italia che richiedano solo la coppia di credenziali *username* e *password.*

Gli altri parametri, tutti **obbligatori**, sono:

- ***Password***: deve essere di almeno 8 (otto) caratteri e deve contenere sia lettere che numeri;
- **Nome**;
- **Cognome**;
- **Email**: deve essere fornita un'email valida ai fini della validazione della nuova utenza. L'indirizzo email non deve essere già presente sui sistemi di identificazione della Banca d'Italia in quanto potrà essere utilizzato per identificare l'utente nei workflow di recupero credenziali;
- **Domanda** e **risposta segreta**: campi di testo ad immissione libera, sono necessari per il recupero completo delle credenziali.

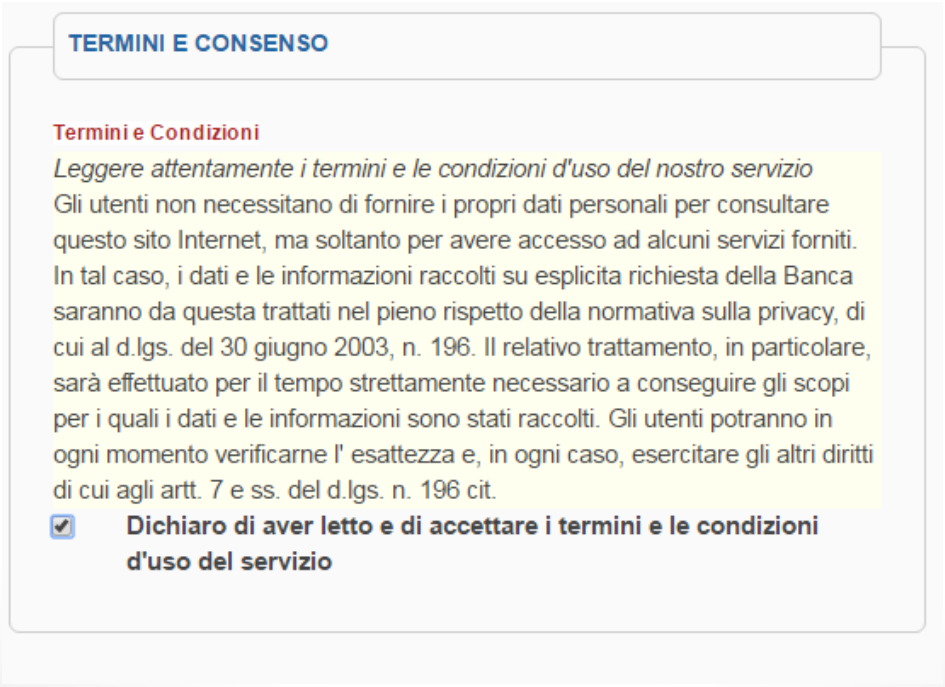


Successivamente l'utente potrà inserire altri parametri **opzionali**:

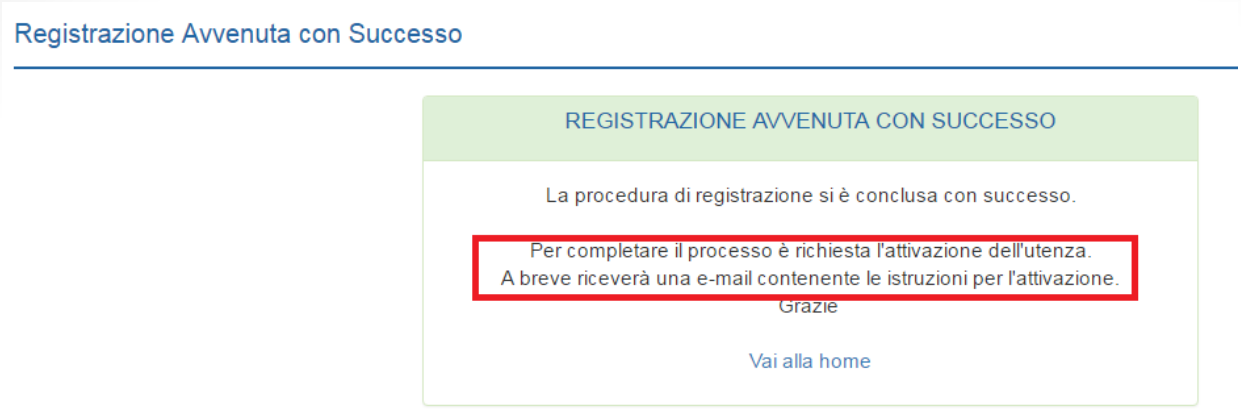
- **Numero** di **telefono cellulare**: potrà essere utilizzato come presidio di sicurezza aggiuntivo in alcune fasi di riconoscimento per il tramite di invio di SMS contenenti codici di sicurezza utilizzabili una sola volta, i cosiddetti OTP (OneTime Password).
- **Certificato di cifratura personale**: In tale contesto l'utente **potrà** fornire un certificato x509 di cifratura **personale** che sarà utilizzato solo per cifrare messaggi diretti alla persona fisica identificata dal codice fiscale presente sulla CNS. **Tale certificato non deve essere confuso con il certificato di cifratura associato alla credenziale applicativa (A2A) illustrata nel seguito del documento**. Il certificato di cifratura personale potrà essere sottoposto **in uno dei seguenti formati:**
    - DER - formato binario
    - PEM - formato base64

  Nel caso in cui il certificato sia firmato da una o più CA intermedie, i certificati di quest'ultime non dovranno essere incluse nel *file* caricato.

Al termine l'utente **dovrà** accettare i termini e le condizioni d'uso del servizio.



Successivamente alla conferma all'utente è mostrata la seguente schermata:

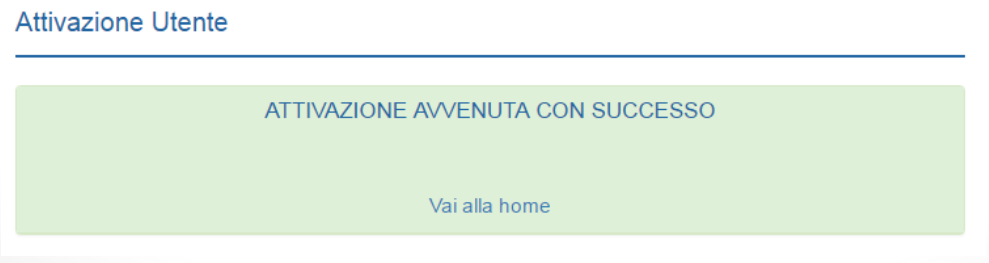


Quindi il sistema invia una email all'indirizzo indicato in fase di registrazione**.**

Al fine di completare e validare l'iscrizione l'utente dovrà seguire le istruzioni contenute nella stessa email entro 72 ore.

Di seguito un **esempio** di e-mail inviata dal sistema di registrazione

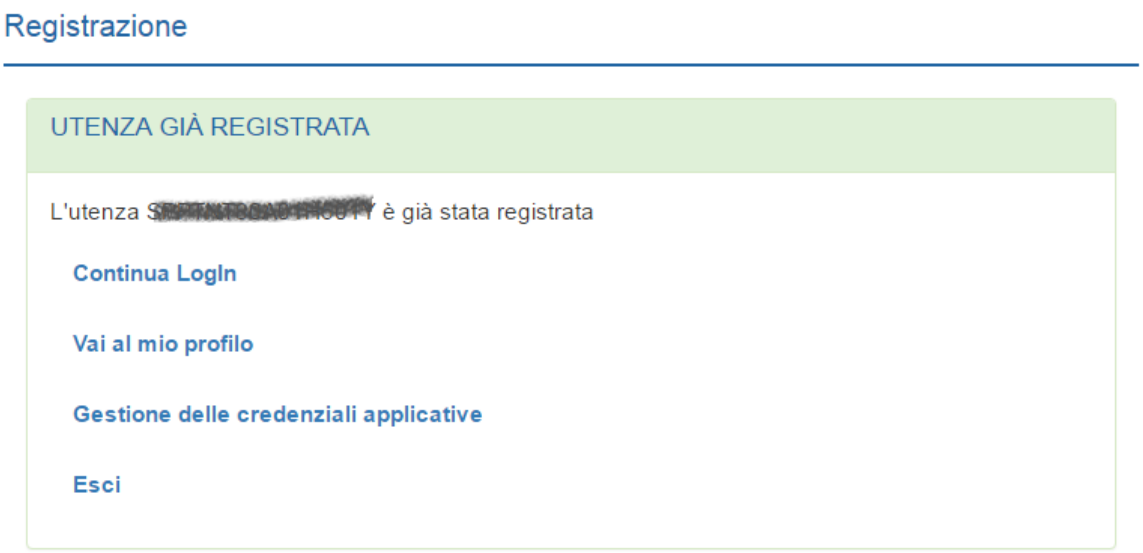
Cliccando il link l'utente sarà ridiretto su una pagina web che attesterà il completamento dell'attivazione:



Trascorse 72 ore dall'iscrizione, se non confermato, il profilo utente sarà cancellato definitivamente dagli archivi del sistema di autenticazione e sarà necessario procedere con una nuova procedura di registrazione, anche utilizzando gli stessi dati.
In caso di conferma positiva, entro le 72 ore, l'utente è abilitato e può procedere con la creazione delle credenziali A2A.

L'utente **che abbia già registrato la propria CNS** scegliendo l'opzione:

otterrà dal sistema il seguente messaggio e potrà scegliere tra la funzione di gestione del proprio profilo o accedere direttamente alla gestione delle credenziali applicative.



NOTA : Non è possibile utilizzare un indirizzo e-mail già utilizzato in precedenza per registrare altre credenziali.

Qualora non fosse possibile utilizzare un altro indirizzo email o un alias dello stesso, è possibile richiedere la cancellazione delle vecchie credenziali inviando un'email all'indirizzo del *Service Desk* (autoregistrazione@bancaditalia.it)

2. Registrazione credenziali applicative

Per registrare una credenziale A2A, dopo aver eseguito la registrazione della CNS, l'utente deve selezionare il menù "Gestione delle credenziali applicative".

Tale selezione indirizza l'utente sul menu di scelta delle azioni relative alla **gestione delle credenziali A2A**. Ogni utente può registrare un numero illimitato di credenziali A2A, delle quali diviene "manager".

Ogni credenziale deve disporre di almeno un certificato digitale (x509) tra quello con le finalità di autenticazione A2A e quello utilizzabile per la cifratura dei messaggi inviati dalla Banca d'Italia alla controparte (quest'ultima detiene la chiave privata di cifratura).

Per creare una nuova credenziale A2A cliccare sulla voce "Nuova credenziale".

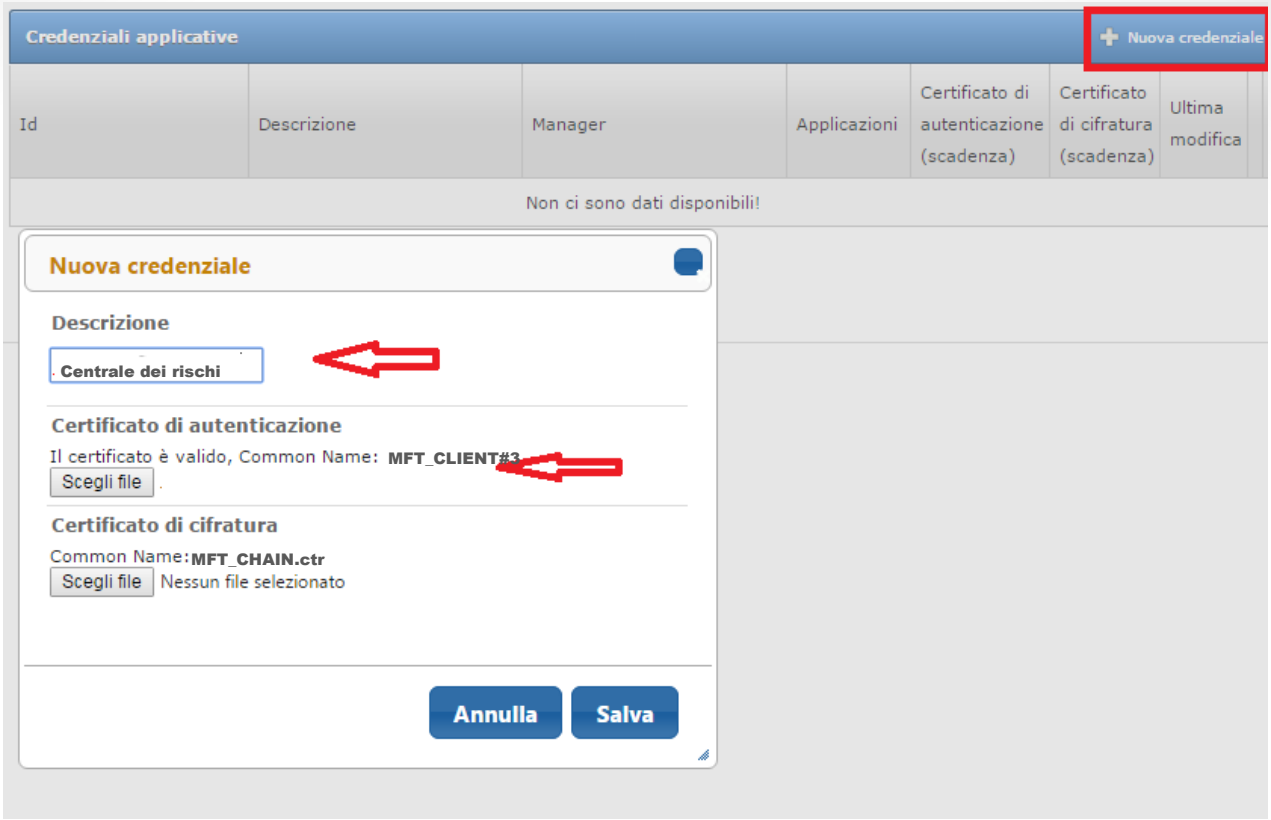
Le informazioni obbligatorie sono:

- ***Descrizione****: campo di testo libero. Immettere una descrizione dell'intermediario per cui tale credenziale viene creata; ciò potrà successivamente facilitare un eventuale troubleshooting sul sistema;*
- ***Uno o entrambi i certificati x509 di autenticazione e cifratura.***
  I certificati X509 potranno essere sottoposti **in uno dei seguenti formati:**

    - DER - formato binario
    - PEM - formato base64

  Nel caso in cui il certificato sia firmato da una o più CA intermedie, i certificati delle CA intermedie o radice **non devono** essere incluse nel *file* caricato.

  Una volta completata l'immissione delle informazioni richieste, **il sistema genera automaticamente un ID che identifica univocamente la credenziale applicativa.**



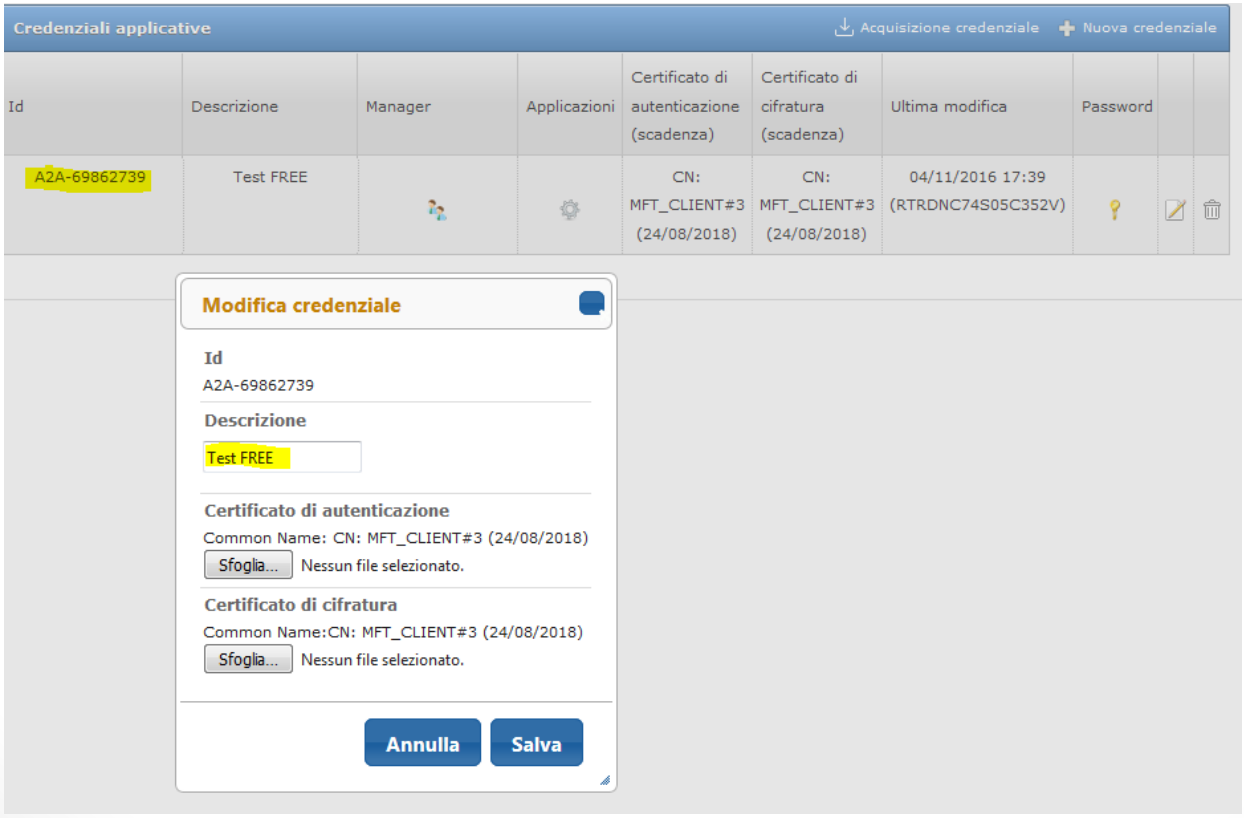
L'identificativo univoco associato alla credenziale A2A che si sta creando non potrà essere scelto dall'utente ma verrà generato automaticamente dal sistema una volta completata l'immissione delle informazioni richieste e sarà del tipo "A2A-XXXXXXX", così come mostrato nell'esempio illustrato nella figura seguente.

3. Gestione della credenziale A2A

Modifica della Credenziale

I manager possono in ogni momento variare la descrizione e sostituire i certificati di autenticazione e cifratura della credenziale A2A in loro possesso, utilizzando l'icona evidenziata in giallo nel menu riportato nella figura seguente e che rappresenta il menu di gestione delle credenziali A2A.

Selezionando l'icona di modifica, mediante il popup illustrato nella figura seguente è possibile modificare la descrizione o sostituire i certificati precedentemente caricati sul sistema.



Cancellazione della credenziale

Un manager può in qualunque momento cancellare una credenziale.

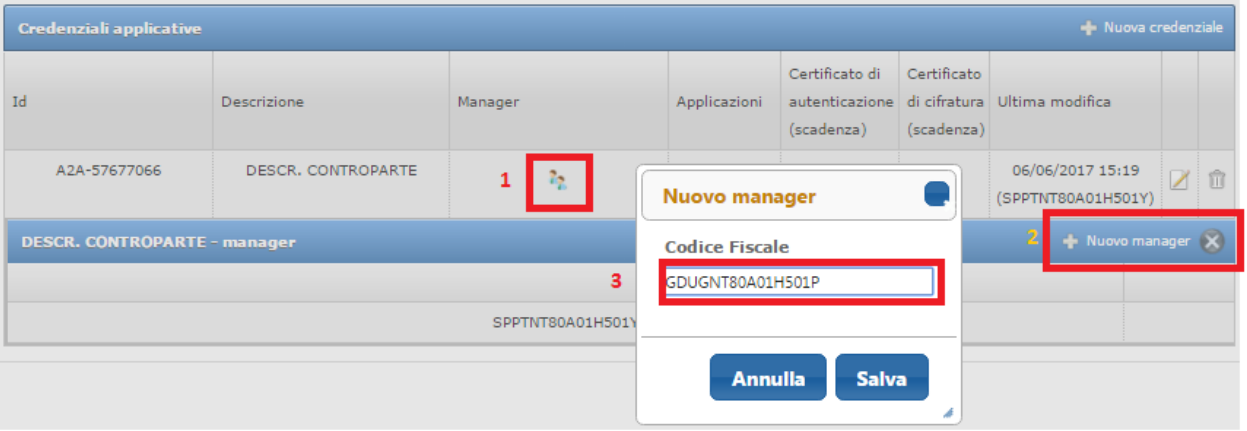
> **Attenzione: l'eliminazione non può essere annullata.** Non è possibile riutilizzare lo stesso codice identificativo (ID) di una credenziale cancellata, pertanto le **credenziali accreditate**[3] **non devono essere cancellate** .

La cancellazione può essere effettuata direttamente nella maschera di gestione delle credenziali applicative come mostrato nella figura seguente:

[3] Cioè le credenziali già comunicate alla Banca d'Italia e per le quali il processo di accreditamento si è concluso positivamente.

Gestione del manager della credenziale

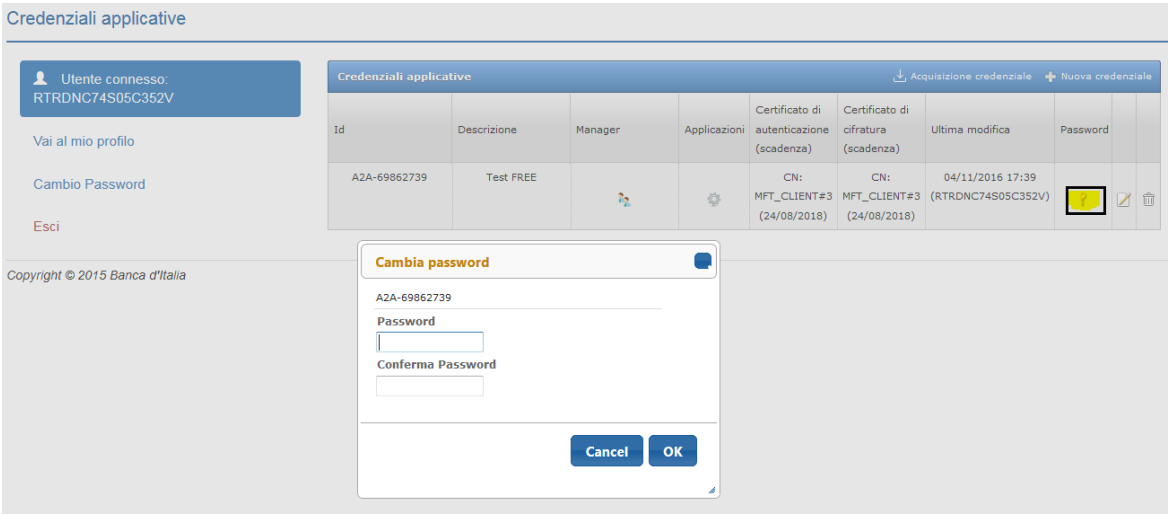
Una credenziale A2A può essere gestita da un numero illimitato di manager.
È possibile visualizzare **l'elenco dei manager** di una credenziale cliccando sull'icona evidenziata nella figura seguente.



Uno qualunque dei manager può delegare la gestione della credenziale ad altri manager inserendo il **codice fiscale** dei nuovi manager.

La delega di gestione non è esclusiva, tutti i manager possono operare sulle proprie credenziali sfruttando tutte le funzionalità associate.

Un qualunque manager può eliminare un altro manager dalla gestione della credenziale, tale operazione non ha effetto sulle altre credenziali applicative ad esso associate e non ha effetto sulla credenziale associata alla CNS del manager eliminato.

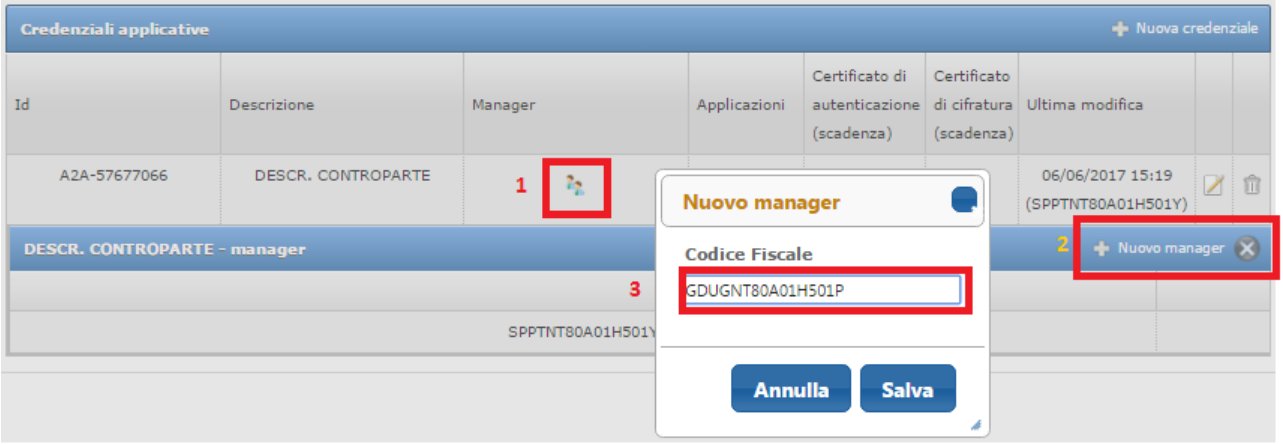


Al fine di evitare possibili difficoltà nella gestione della credenziale applicativa (a causa di operazioni straordinarie o sostituzione dei fornitori) **si suggerisce di associare almeno due manager alla stessa, di cui almeno uno dipendente dell'intermediario segnalante**.

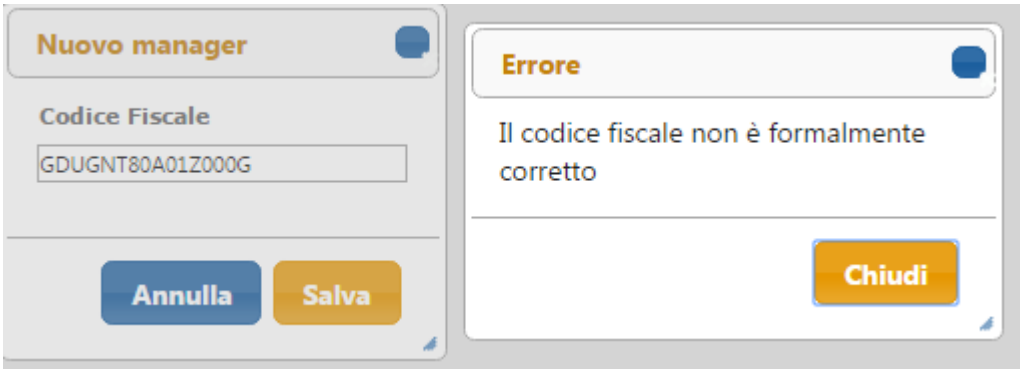
Delega della credenziale

Una credenziale può essere gestita da più manager.

Il meccanismo di delega si basa sulla comunicazione al sistema del CODICE FISCALE del nuovo manager attraverso l'interfaccia di gestione della credenziale, come mostrato nella figura sottostante:

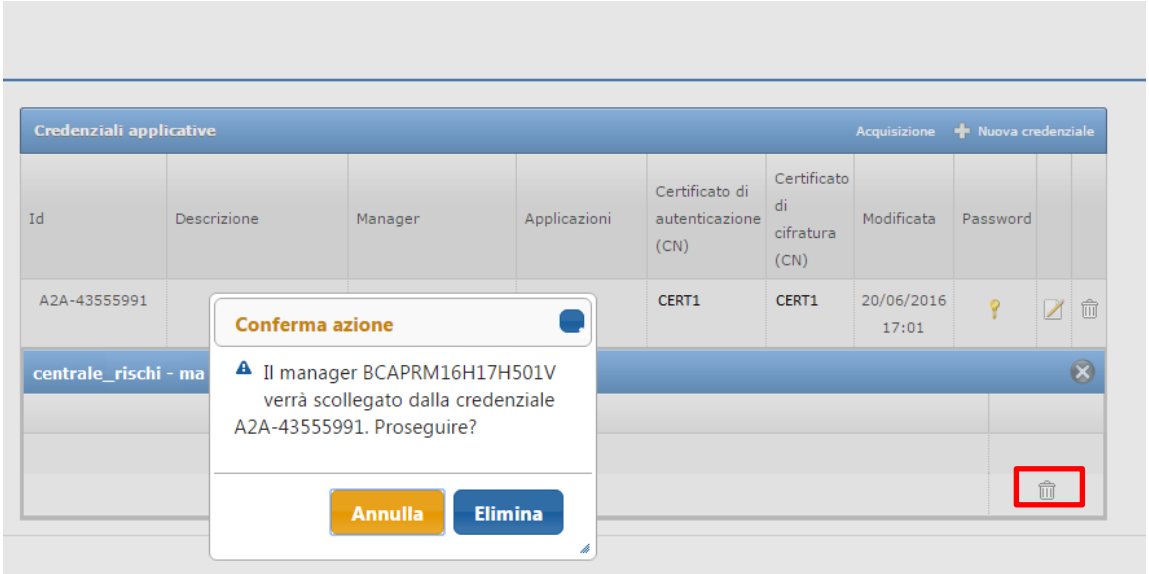


NOTA: L'aggiunta del codice fiscale di un manager può essere condotto a termine ancor prima della sua iscrizione; il sistema **verifica solo la correttezza formale** del codice fiscale inserito:



Cancellazione di un manager

Il nuovo manager può gestire anche gli altri manager, eventualmente scollegando i manager non più delegati.



NOTA: una credenziale non può rimanere "orfana" e ogni manager può, rispetto alla singola credenziale gestita, eliminare tutti gli altri manager della stessa con l'esclusione di sé stesso.

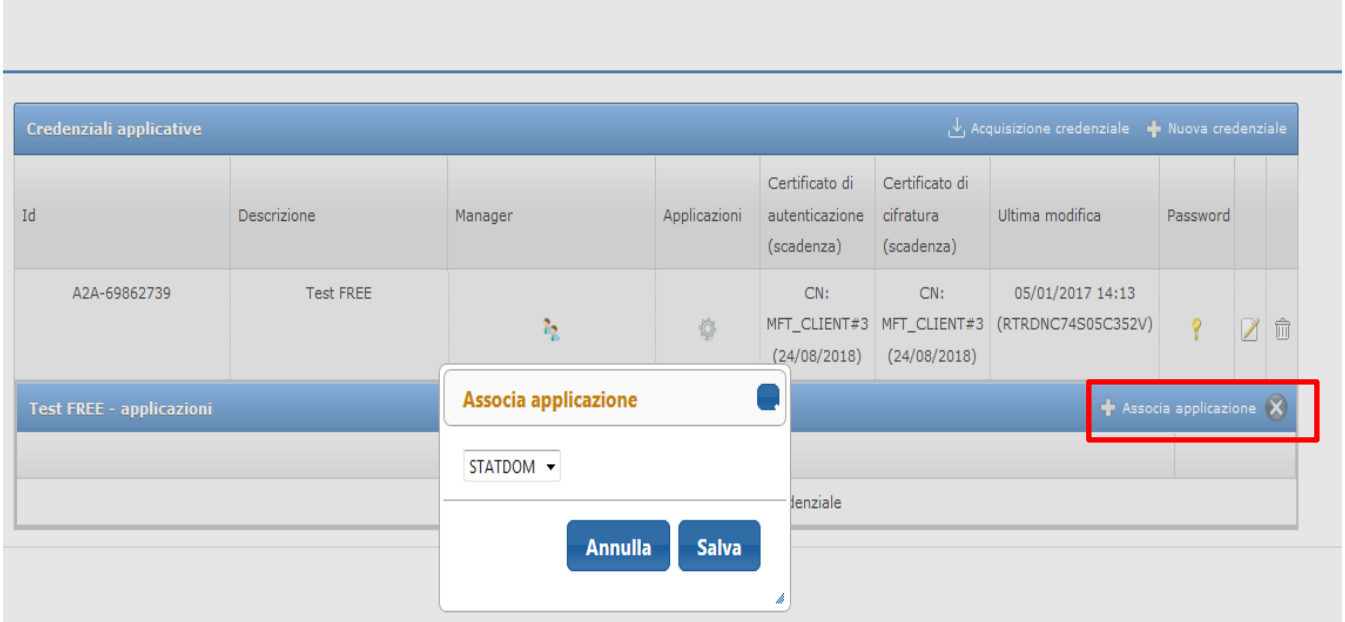
Alla conferma dell'azione il manager selezionato sarà scollegato dalla credenziale applicativa. Tale azione non influisce sullo status dell'utente che viene scollegato dalla credenziale che rimane manager di tutte le altre credenziali a lui associate.

In caso di necessità di cancellazione e/o modifica urgente o massiva è tuttavia possibile richiedere il supporto gestionale da parte del *Service Desk* (autoregistrazione@bancaditalia.it), in particolare in caso di incidenti di sicurezza.

Abilitazione all'applicazione della credenziale.

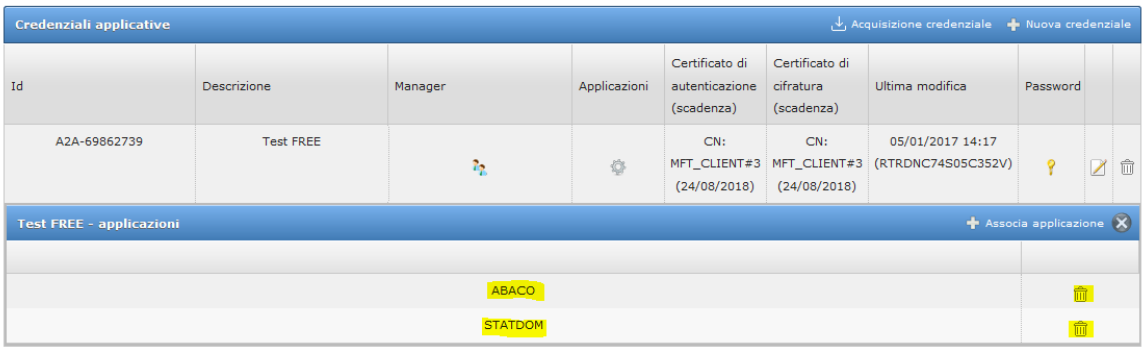
Ogni credenziale permette di fare riferimento ad un certificato di autenticazione e/o di cifratura per una o più applicazioni esposte su Internet dalla Banca.

Al momento della creazione la credenziale viene memorizzata ma non abilitata ad alcuna applicazione, tale azione deve essere espressamente richiamata da un utente manager della stessa credenziale. Al fine di permettere l'abilitazione sui sistemi di autenticazione è necessario cliccare sull'azione "+ Associa applicazione" .



Tale azione permetterà l'associazione ad una delle applicazioni. Per lo scambio di flussi con la **Centrale Rischi**, l'**Anagrafe dei soggetti**, **AnaCredit e Money Market Statistical reporting (MMSR[4])** è necessario associare la credenziale all'applicazione '**STATDOM**'.

Una credenziale può essere associata a diverse applicazioni:



[4] La survey a supporto della rilevazione MMSR sono 4 (MMNS, MMSE, MMOS, MMFX).

Un manager può associare e disassociare in qualsiasi momento una credenziale da una qualunque applicazione. La **disabilitazione** è ottenuta attraverso la funzione “cestino”.

V. Istruzioni per la compilazione e l'invio del modulo per l'accreditamento

Il modulo per l'accreditamento va inviato se l'intermediario non è ancora accreditato al servizio di scambio dati via *Internet* e **deve essere compilato digitalmente in tutte le sue parti.**

Per l'ambiente di esercizio e di collaudo sono previsti due moduli identici, ma distinti.

È richiesta la firma digitale del legale rappresentante da apporre direttamente all'interno del modulo ovvero per il tramite della firma del file (in questo caso il campo interno al modulo non deve essere compilato e occorre produrre un file con estensione .pdf.p7m).

Nel modulo sono richieste le seguenti informazioni:

denominazione e codice ABI dell'intermediario. il codice ABI deve essere completo di contro codice ed in formato numerico senza eventuali zeri a sinistra e senza punti, spazi o qualsiasi altro carattere non numerico.

identificativo della credenziale applicativa a cui sono associati i certificati digitali di autenticazione e crittografia per lo scambio di dati via Internet con la Banca d'Italia

indirizzo mail dove si vuole ricevere comunicazioni relative allo scambio dati via *Internet* e informazioni sull'aggiornamento della documentazione tecnica.
Data la rilevanza delle informazioni che vi transiteranno e la necessità di garantire una stabilità nel tempo si suggerisce di indicare l'indirizzo mail di una casella funzionale. Se l'indirizzo che si vuole fornire è una PEC si prega di verificare che lo sia abilitato alla ricezione di posta non certificata.
Si prega di prestare particolarmente attenzione alla compilazione di tale indirizzo in quanto sarà utilizzato per notificare la conferma di avvenuto accreditamento, per inviare i messaggi di sistema e comunicate le novità che riguardano lo scambio dei dati via *Internet*.
Qualunque variazione all'indirizzo indicato dovrà essere prontamente comunicata via PEC utilizzando il medesimo modulo**.**

nome, cognome e codice fiscale di una delle persone incaricate di gestire la credenziale (Manager).

numero di telefono e *indirizzo e-mail* dell'ufficio da contattare per problematiche riguardanti l'accreditamento al servizio di scambio dati via Internet.

Una volta compilato, il modulo va inviato via PEC all'indirizzo res@pec.bancaditalia.it, indicando nell'oggetto "Scambio dati via *Internet* - richiesta di accreditamento" e l'ambiente (collaudo o esercizio) per cui si chiede l'accreditamento.
Richieste di chiarimento inerenti l'accreditamento possono essere inoltrate alla casella di posta elettronica **RDVI.HELPDESK@bancaditalia.it.**

FAQ

1. Non riesco a confermare la registrazione iniziale.

È possibile che siano trascorse più di 72 ore e quindi è necessario ripetere la procedura di registrazione.

In alcuni casi particolari, pur non essendo trascorse le 72 ore, è possibile che l'attivazione non vada a buon fine a causa del comportamento di alcuni client e-mail che modificano il link inviato dall'applicazione rendendolo invalido. In questo caso, il processo di registrazione può essere completato copiando il testo dell'indirizzo mediante la funzionalità di copia e quindi incollandolo direttamente nella barra indirizzi del browser.

2. Non ho ricevuto la e-mail di conferma registrazione.

Accertarsi che la propria casella postale non abbia superato i limiti di utilizzo consentiti, ovvero che l'e-mail non sia stata intercettata da sistemi automatici di anti-spam o anti-phishing. In tal caso, controllare nella cartella posta indesiderata della vostra casella. Accertarsi di non aver utilizzato un indirizzo di posta elettronica certificata (PEC).

3. Non sono sicuro di aver inserito l'indirizzo e-mail corretto.

Attendere 72 ore e ripetere la registrazione con l'indirizzo corretto.

4. Cosa è una credenziale A2A?

La credenziale A2A è un codice alfanumerico nella forma A2A-<123456789>, a tale codice identificativo è possibile associare:

- Certificato X509 di autenticazione: necessario per mutua autenticazione SSL tra gli applicativi delle controparti e i sistemi applicativi.

- Certificato di cifratura: utilizzato dal sistema per cifrare i flussi di risposta verso le controparti.

- Uno o più manager della credenziale: i manager si distinguono per codice fiscale e sono persone fisiche identificate con la CNS.

- Uno o più contesti applicativi, ogni credenziale può essere utilizzata su uno o più applicazioni esposte sul canale Internet.

5. **Numero e tipologia dei certificati – Quali e quanti certificati digitali sono necessari?**

Sono necessari tre certificati: di identificazione, di firma e di crittografia. Per l'identificazione e la crittografia può essere usato un certificato unico.

Ad una credenziale devono essere associati il certificato o i certificati di identificazione e di crittografia.

Lo stesso certificato può essere associato a due credenziali solo in ambienti diversi (collaudo e produzione). Si consiglia l'utilizzo dei medesimi certificati (identificazione, firma e crittografia) sia per l'ambiente di collaudo sia per quello di produzione.

6. **Credenziali di collaudo (alias certificazione) e produzione, come si distinguono?**

Esiste un'interfaccia per l'ambiente di collaudo e una pe l'ambiente di produzione, con assegnazione separata delle credenziali tra i due ambienti.

Le controparti otterranno credenziali A2A (applicative) che Il sistema assegnerà attraverso l'interfaccia di gestione, la forma delle credenziali sarà del tipo A2A-1234567.

Sarà cura degli intermediari utilizzare la credenziale corretta sull'ambiente corrispondente

7. **Centri servizi - Nel caso in cui un centro servizi svolga operazioni di scambio per conto di più segnalanti, può utilizzare una sola credenziale?**

No, Per lo scambio di informazioni con la Centrale dei rischi dovrà utilizzare una credenziale differente per ogni segnalante, con i propri certificati.

8. **Gestione dei certificati digitali - È ammessa la gestione via software dei certificati per la protezione del canale, oppure risulta obbligatorio l'utilizzo di apparati HW (i cosiddetti HSM)?**

Solo i certificati di firma devono essere conservati su dispositivi sicuri per l'apposizione della firma del tipo SmartCard (CNS). I certificati utilizzati per l'autenticazione del canale sono di norma oggetti su file protetti da opportuni SW (Keystore). La responsabilità della gestione della sicurezza ricade interamente sul possessore del certificato associato alla credenziale.

9. Formato dei certificati digitali - Che tipo di certificati sono i file con estensione ".pem"? Si fa sempre riferimento al certificato di cifratura e di autenticazione?

Il formato PEM è il formato più comunemente utilizzato dalle Certification Authorities per emettere i certificati. Altre estensioni convenzionali possono essere .crt e .cer.I PEM sono file ASCII con codifica Base64 e contengono "-----BEGIN CERTIFICATE-----" all'inizio e "-----END CERTIFICATE-----" alla fine. Possono essere in formato PEM sia certificati server, che certificati intermedi e chiavi private.

(cfr. https://it.wikipedia.org/wiki/X.509 , https://www.ietf.org/rfc/rfc5280.txt)

10. Acquisto dei certificati digitali - L'acquisizione dei certificati per l'autenticazione e la cifratura dei dati vanno richiesti presso un'azienda accreditata dall'Agenzia per l'Italia Digitale AGID?

No, la normativa vigente (EIDAS-AGID) impone vincoli solo sui certificati digitali utilizzabili per Firma Digitale Qualificata, Marca Temporale e CNS (identificazione persona fisica).

I certificati di autenticazione e cifratura applicativa (flussi A2A) possono essere rilasciati da una qualunque Certification Autority (CA) il cui certificato ROOT sia presente nel CA_BUNDLE della fondazione Mozilla e consultabile al link: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/

11. Cifratura - Il certificato di cifratura dovrebbe contenere una chiave AES generata dal segnalante e protetta con una chiave pubblica, questa chiave pubblica è della Banca d'Italia?

No, l'eventuale utilizzo di CSR (certificate signing request) per la generazione di certificati X509 fa parte del metodo scelto dalla Certification Autority (CA) di riferimento della controparte; ciò detto non si entra nel merito di come sono generati/approvvigionati i certificati di autenticazione e cifratura.

12. Il sistema di cifratura prevede una chiave AES. Come viene cifrata la chiave AES ?

La Banca d'Italia utilizza la chiave simmetrica AES per cifrare i dati che inoltra al segnalante, la chiave di cifratura AES viene a sua volta cifrata con la chiave pubblica del destinatario in modo che il solo il destinatario la possa aprire usando la sua chiave privata. ***Lo standard di riferimento per la cifratura è la RFC3852.***

13. La CNS può essere di tipologia LIKE od obbligatoriamente FULL?

Non è consentito l'utilizzo di "CNS LIKE", è previsto il solo utilizzo di CNS (o "CNS Full") rilasciate da CA presenti sull'elenco pubblico dei certificatori che emettono certificati CNS (Trusted LIST ITALIANA). Tale lista include tutti i certificati afferenti le autorità di certificazione che rilasciano certificati anche per le Carte Nazionali dei Servizi.

Per i dettagli tecnici e normativi si rimanda al sito AGID:

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/carta-nazionale-servizi
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/certificati