



EVOLUZIONE BANCA DATI SINISTRI

INFRASTRUTTURA SCAMBIO FLUSSI

Manuale gestione accreditamento credenziali A2A

Versione 1.1

1. Scopo del documento

Il documento descrive:

- il processo di accreditamento alla procedura EBDS
- le modalità di gestione delle credenziali A2A (Application to Application) necessarie per autenticarsi all'interno dei sistemi informatici che erogano il servizio
- le caratteristiche dei certificati digitali per l'autenticazione, la crittografia e la firma dei dati.

2. Il processo di accreditamento alla procedura EBDS

2.1. Ambiente di esercizio

Per accedere ai servizi A2A messi a disposizione dalla procedura EBDS, l'impresa assicuratrice deve dotarsi di una propria **credenziale applicativa** a cui poi vanno contestualmente associati certificati digitali di proprietà validi per l'autenticazione, la firma e la cifratura dei dati.

La credenziale A2A identificherà univocamente l'impresa e resterà attiva per tutto il tempo in cui la stessa scambierà informazioni con IVASS/Banca d'Italia.

Il processo di accreditamento prevede due step:

1. Registrazione della credenziale A2A

Un incaricato dell'impresa mediante propria CNS ovvero credenziale SPID professionale/personale di livello 3 accede alla procedura Web di esercizio di *self-registration* e registra una **credenziale applicativa**.

Ad ogni credenziale deve quindi essere associato un certificato digitale di autenticazione ed uno di firma/cifratura, quest'ultimo necessario ad EBDS per cifrare le comunicazioni con la chiave pubblica del ricevente.

Il medesimo certificato potrà comunque essere utilizzato per entrambe le funzioni.

Le modalità per registrare e gestire la credenziale applicativa sono descritte più avanti in questo documento.

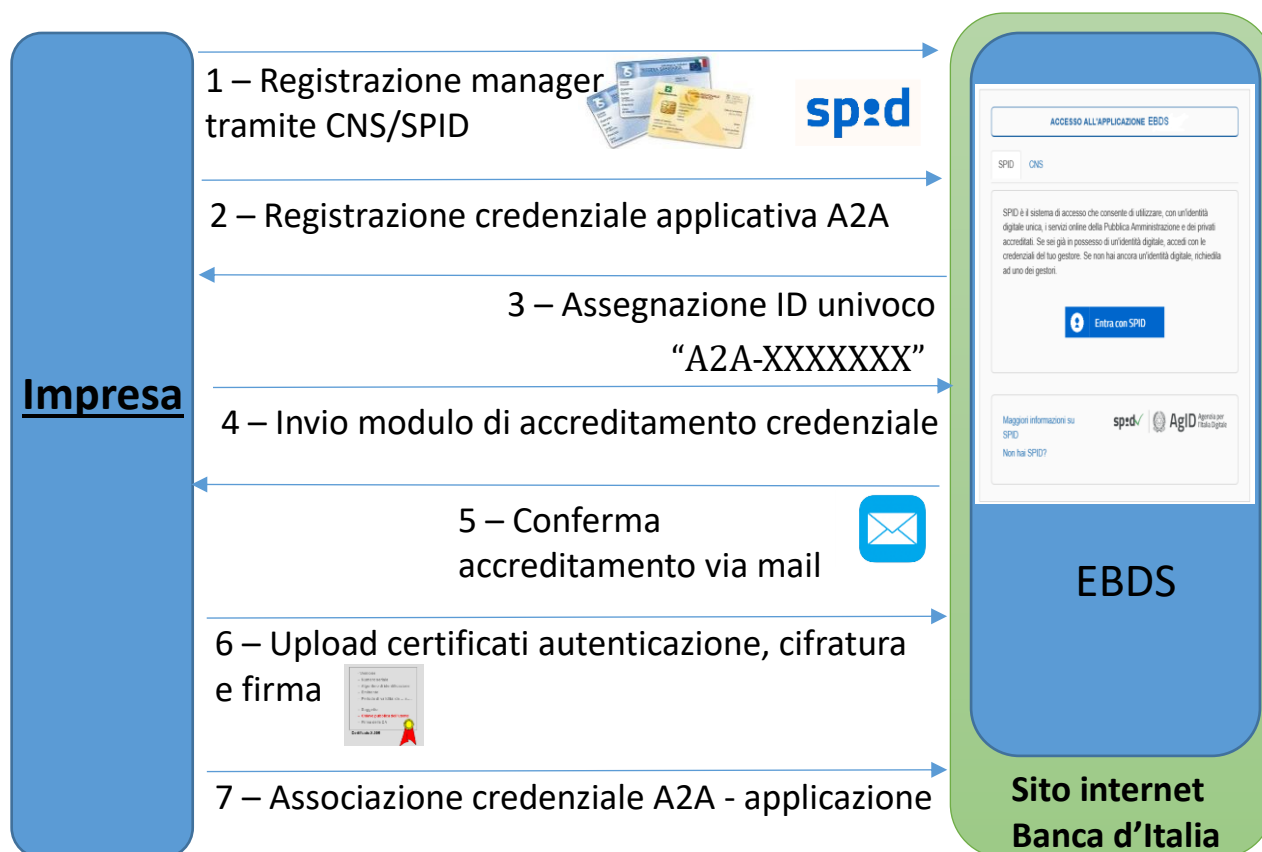
2. Accreditamento della credenziale A2A

L'impresa (il referente antifrode o un amministratore con delega di rappresentanza) **comunica con una PEC¹ a IVASS** l'identificativo della credenziale applicativa e il codice compagnia da associare alla stessa, richiedendo l'abilitazione allo scambio dati.

IVASS, ricevuta la richiesta ed effettuati i controlli di rito, accredita l'impresa allo scambio dati via Internet e invia la notifica dell'avvenuto accreditamento.

ATTENZIONE: Prima di iniziare ad inviare le segnalazioni sui sinistri ad EBDS, l'impresa deve assicurarsi di aver ricevuto conferma di accreditamento. Si suggerisce anche di verificare previamente la corretta configurazione della propria credenziale applicativa mediante un test di canale.

¹ studi.gestionedati@pec.ivass.it



Per ulteriori approfondimenti si rimanda alla sezione FAQ del documento "Manuale di accreditamento e di gestione delle credenziali" scaricabile dal sito internet di Banca D'Italia.

2.2. Ambiente di collaudo

Per accedere all'ambiente di collaudo è necessario registrare un'apposita credenziale: non è dunque possibile utilizzare quella registrata in ambiente di esercizio ma è comunque possibile - anzi consigliato - associare a questa credenziale di collaudo i medesimi certificati associati a quella di esercizio. Il processo di accreditamento per l'ambiente di collaudo è identico a quello descritto per l'ambiente di esercizio.

3. Certificati e standard crittografici

3.1. 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 ²
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

3.2. 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

² <https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/doc-tecnica-cr/index.html> Nella sezione “Certificati digitali – cifratura” -> “Certificato di cifratura Banca d'Italia - utilizzato a partire dal 28 maggio 2021”

4. Gestione credenziali

4.1. Accesso tramite CNS / SPID

Per accedere alla procedura di gestione delle credenziali applicative è necessario che l'utente sia in possesso di una *CNS*³ personale (ovvero di un proprio account *SPID*⁴ livello 3) in corso di validità.

Autenticazione



SPID CNS

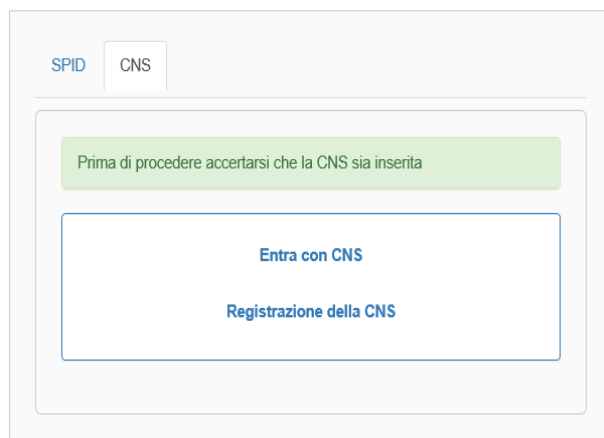
SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila ad uno dei gestori.

 **Entra con SPID**

Maggiori informazioni su SPID
Non hai SPID?

spid ✓  **AgID** Agenzia per l'Italia Digitale

Autenticazione



SPID **CNS**

Prima di procedere accertarsi che la CNS sia inserita

Entra con CNS

[Registrazione della CNS](#)

Nel caso si optasse per l'accesso tramite CNS, solo la prima volta è necessario registrare la CNS completando il profilo utente con i dati anagrafici e

³ Carta Nazionale dei Servizi - <https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi>

⁴ Sistema Pubblico di Identità Digitale - <https://www.spid.gov.it/>

valorizzando i parametri di sicurezza (password, domanda e risposta segreta per il recupero dell'identità)⁵.

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.

Di seguito un riepilogo degli URL delle applicazioni WEB dedicate alle gestioni delle credenziali per la procedura EBDS nei vari ambienti elaborativi:

AMBIENTE ELABORATIVO	Indirizzo Internet (URL)
COLLAUDO	https://certscambioflussi-registration.bancaditalia.it
ESERCIZIO	https://scambioflussi-registration.bancaditalia.it

4.2. Registrazione della credenziale applicativa

Per registrare una credenziale A2A, dopo aver eseguito l'accesso l'utente deve selezionare la voce di menu "Gestione delle credenziali applicative".



Tale selezione indirizza l'utente all'interno del 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 un certificato digitale (x509) con finalità di autenticazione A2A e di un certificato per la firma digitale e la cifratura (mediante chiave pubblica) dei messaggi inviati da IVASS/Banca d'Italia all'impresa (quest'ultima detiene la chiave privata per la decifratura).

Tali certificati possono anche coincidere.

⁵ Per la registrazione della CNS, fare riferimento al cap. IV – par. 1 del "Manuale di accreditamento e di gestione delle credenziali" scaricabile dal sito internet di Banca D'Italia.

Per creare una nuova credenziale A2A cliccare sulla voce “Nuova credenziale”.

Le informazioni obbligatorie da introdurre sono:

- **Descrizione:** campo di testo libero. Si consiglia di immettere una descrizione dell'impresa assicurativa 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.**

The screenshot displays the 'Credenziali applicative' (Application Credentials) management interface. At the top right, a red box highlights the '+ Nuova credenziale' button. Below the header is a table with columns: Id, Descrizione, Manager, Applicazioni, Certificato di autenticazione (scadenza), Certificato di cifratura (scadenza), and Ultima modifica. The table is currently empty, showing the message 'Non ci sono dati disponibili!'. A modal window titled 'Nuova credenziale' is open, containing the following fields:

- Descrizione:** A text input field with the placeholder text 'Credenziale per procedura "EBDS: Impresa assicurativa: XXXX"'. A red arrow points to this field.
- Certificato di autenticazione:** A section with the text 'Il certificato è valido, Common Name: EBD\$ CLIENT\$'. Below it is a 'Scegli file' button. A red arrow points to the 'Common Name' text.
- Certificato di cifratura:** A section with the text 'Common Name: EBD\$ CHAIN.cer'. Below it is a 'Scegli file' button and the text 'Nessun file selezionato'.

At the bottom of the modal are two buttons: 'Annulla' and 'Salva'.

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.

Credenziali applicative								
Acquisizione credenziale Nuova credenziale								
Id	Descrizione	Manager	Applicazioni	Certificato di autenticazione (scadenza)	Certificato di cifratura (scadenza)	Ultima modifica	Password	
A2A-69862739	Test FREE			CN: MFT_CLIENT#3 (24/08/2018)	CN: MFT_CLIENT#3 (24/08/2018)	04/11/2016 17:39 (RTRDNC74S05C352V)		 

NOTA: Per quanto concerne la gestione della credenziale A2A (modifica e cancellazione della credenziale, gestione del manager, delega della credenziale, cancellazione di un manager, abilitazione e disabilitazione della credenziale all'applicazione) fare riferimento alla cap. IV – par. 3 del “Manuale di accreditamento e di gestione delle credenziali – versione 1” scaricabile dal sito internet della Banca D'Italia.