



INFRASTRUTTURA SCAMBIO FLUSSI

Manuale gestione accreditamento credenziali A2A (U4F)

Versione 1.0

1. Scopo del documento

Il documento descrive:

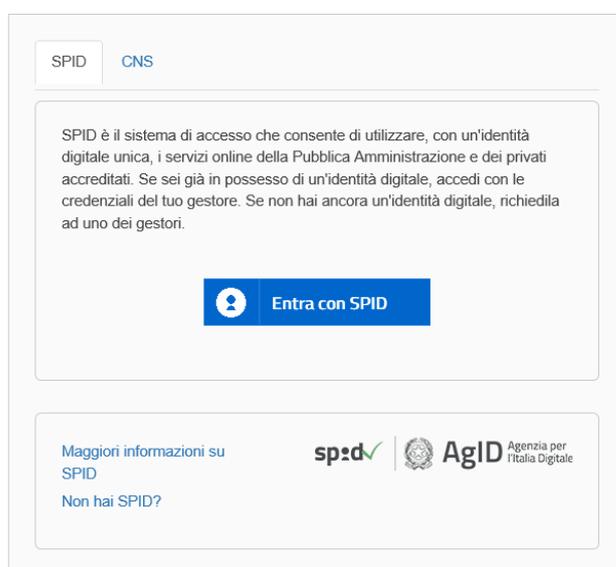
- le modalità di gestione delle credenziali A2A (Application to Application) necessarie per autenticarsi sull'infrastruttura scambio flussi **U4F**;
- le caratteristiche dei certificati digitali per l'autenticazione, la crittografia dei dati.

2. Gestione credenziali

2.1. Accesso tramite CNS / SPID

Per accedere alla procedura di gestione delle credenziali applicative è necessario che l'utente sia in possesso di una **CNS**¹ personale (ovvero di un proprio account **SPID**² livello 3) in corso di validità.

Autenticazione



SPID CNS

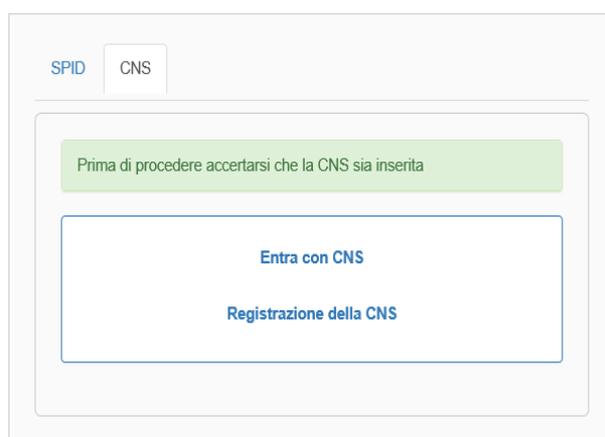
SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila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

¹ Carta Nazionale dei Servizi - <https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi>

² Sistema Pubblico di Identità Digitale - <https://www.spid.gov.it/>

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 valorizzando i parametri di sicurezza (password, domanda e risposta segreta per il recupero dell'identità)³.

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 nei vari ambienti elaborativi:

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

2.2.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 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.

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

Le informazioni obbligatorie da introdurre sono:

³ 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 (https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/accreditamento-cr/Manuale_accREDITamento_e_credenziali_versione_1.pdf).

- **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 shows a web interface for managing application credentials. At the top, there's a blue header with the title 'Credenziali applicative' and a '+ 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, with a message 'Non ci sono dati disponibili!'. A modal window titled 'Nuova credenziale' is open, containing the following fields:

- Descrizione:** A text input field containing 'Credenziali per procedura EBD\$ 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.ct'. Below it is a 'Scegli file' button and the text 'Nessun file selezionato'.

At the bottom of the modal, there 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'Italia⁴.

⁴ <https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/accreditamento-cr/>

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
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 ⁵
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
R08	Cifratura	Cryptographic Message Syntax (CMS) – IETF RFC 3852		07/2004

⁵ <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”