Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

spid
Sistema Pubblico
di Identità Digitale

Procedura per la migrazione assistita verso Identità SPID

Definizioni e acronimi

SP-Ap	Service Provider – Account/Identità Pregresse Il soggetto che richiede la migrazione assistita dei propri account
IDP	Identity Provider SPID Soggetto SPID su cui viene trasferito l'account dell'utente del SP
Utente	Soggetto che richiede il rilascio dell'Identità digitale tramite il SP

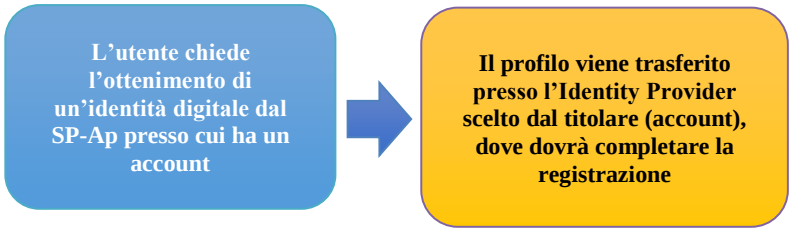
Versioni del documento

Revisione	***Descrizione modifiche***	***Data***
Release 1.0	Prima emissione	febbraio 2018

1.0 Procedura assistita

Il presente processo si applica alle identità di un fornitore di servizi per le quali non è possibile fornire tutte le garanzie necessarie all'ottenimento di una identità SPID, in particolare il riconoscimento *de visu*, e pertanto non ricadono nella fattispecie delle cosiddette identità pregresse.
Lo scopo principale del presente processo è facilitare la migrazione da identità *legacy*.

1.1 Processo di trasferimento dell'identità dal PAP all'IDP



Il processo di creazione di una Identità SPID si realizza attraverso l'iniziativa del titolare delle credenziali (utente) che richiede al proprio Fornitore di Servizi (SP), attraverso una apposita funzionalità, di conferire i dati del proprio account al Gestore di Identità (IDP), dove completerà la procedura di registrazione seguendo la procedura standard.

L'interazione è svolta tra 3 soggetti:

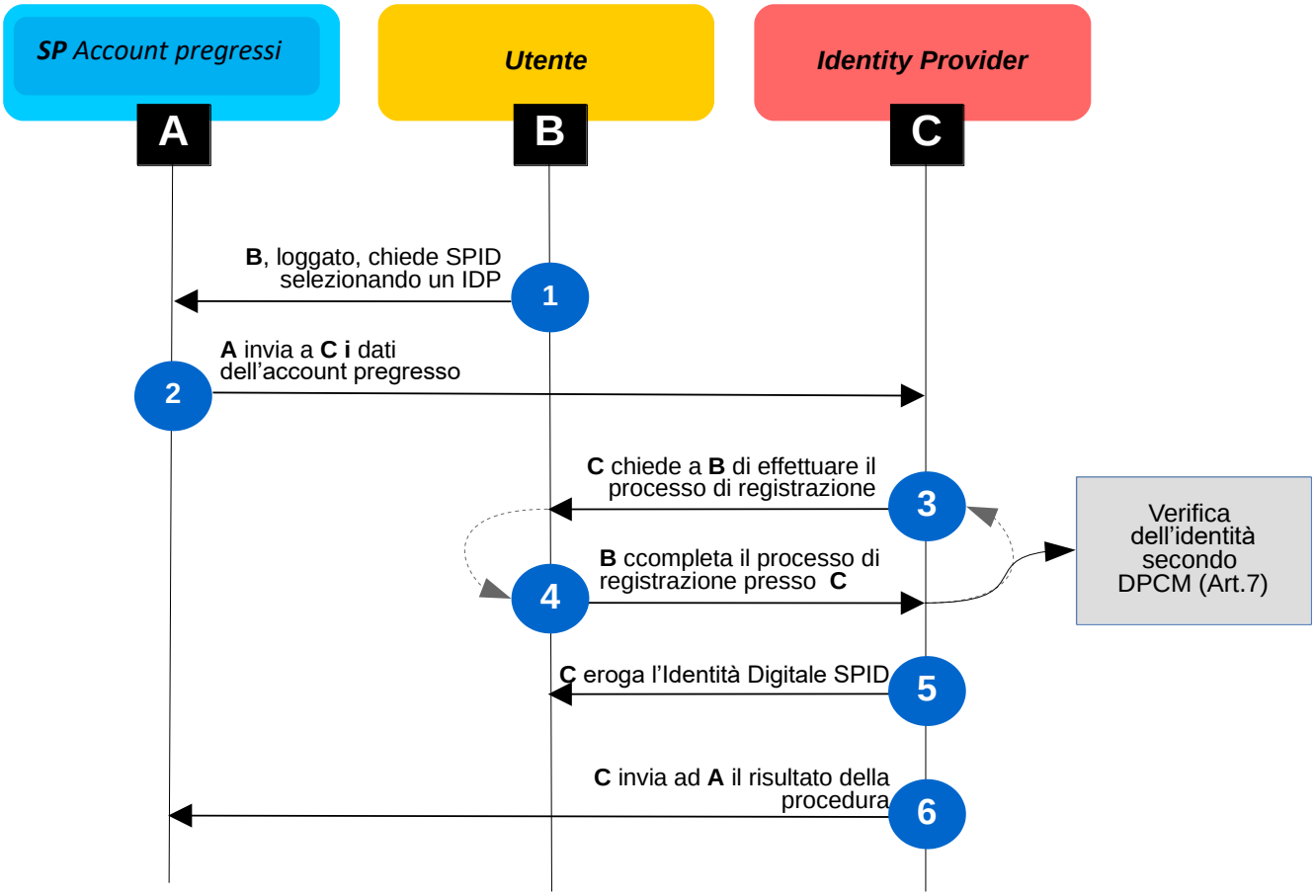
- **Provider Account pregressi (PAp)**: soggetto che ha richiesto la migrazione assistita dei propri account
- **Identity Provider (IDP)**: soggetto che eroga le identità e su cui viene trasferito l'account dell'utente del SP
- **Utente**: soggetto che richiede l'ottenimento dell'Identità Digitale tramite il SP

1.1.1 Identificazione del titolare

Sarà necessario che l'utente sia autenticato sul SP, l'asserzione generata dovrà essere firmata e i dati criptati dal SP.

1.2 Processo di richiesta identità SPID

Lo scenario prevede che l'utente, obbligatoriamente autenticato, possa essere reindirizzato su sua richiesta verso un IDP, dove la maschera di registrazione sarà precompilata con i dati forniti dal SP-Ap. L'utente può effettuare la procedura di richiesta dell'identità digitale singolarmente per uno o più IDP tra quelli elencati sul SP. Sul SP dovranno risultare disponibili solo gli IDP accreditati da AgID come IDP Spid al momento della richiesta dell'identità digitale da parte dell'utente e che avranno aderito allo specifico programma di migrazione ed autorizzati da AgID.



#	Soggetto	Azione	Note
1	***Utente***	L'utente, loggato sul SP, chiede l'erogazione dell'identità digitale scegliendo l'IDP con cui ottenerla	Il pulsante da mostrare è specificato al par. 1.2.4 L'utente dovrà essere autenticato come indicato al par. 1.2.1
2	***SP-Ap***	L'SP invia una *response* con i dati del soggetto richiedente l'Identità Digitale SPID	Come indicato al par. 1.2.5.1
3	***IDP***	L'IDP richiederà all'Utente ulteriori informazioni e attività al fine di completare la registrazione ed erogare l'Identità Digitale	
4	***Utente***		
5	***IDP***	L'IDP eroga l'Identità Digitale all'Utente	

1.2.3 Metadata

AgID concorda con il SP e il/gli IDP la pubblicazione del metadata riportante, come informazioni, i dati come da *schema xsd* e documentazione allegata.

- **Allegato 1: metadata riuso identità**
  - **spid-idpreuse-metadata/spid-idpreuse-metadata.xsd**
  - **spid-idpreuse-metadata/spid-idpreuse-metadata.html**

1.2.4 Bottone "Ottieni SPID"

Il bottone "Ottieni SPID" verrà fornito da AgID assieme alla pubblicazione del metadata specifico della procedura.

1.2.5 Asserzioni

Le asserzioni per lo scambio delle informazioni sono:

- ✓ **Response: schema *response* riuso identità (saml-schema-protocol-2.0.xsd)**
- ✓ **Result: schema *result* riuso identità (spid-idreusenotverified-result.xsd)**

1.2.5.1 Response

Si conforma a quanto definito dalle Regole Tecniche SPID relativamente a Response (sintassi, schema e regole di processamento e sicurezza) in quanto contenente i valori attributi, divenendo, di fatto, un modello "IDP Initiated" (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html par. 5.1.4)

Gli SP dovranno fare una POST della respone all'endpoint specificato nel metadata (idpResponseEndpoint). I dati dovranno essere criptati come da specifiche SAML 2.0 (http://docs.oasis-open.org/security/saml/Post2.0/sstc-

saml-metadata-algsupport-v1.0-cs01.html) e W3C XMLEnc (http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/).

La response potrà contenere solo i dati come definito da tabella attributi SPID.

Le informazioni che, obbligatoriamente, il SP-Ap deve fornire sono:

- Codice Fiscale
- Cognome
- Nome

Tutti i dati potranno essere modificati.

- **Allegato 2: response riuso identità**
  - **spid-idpreuse-response/saml-schema-protocol-2.0.xsd**
  - **spid-idpreuse-response/saml-schema-protocol-2.0.html**

1.2.5.2 Result

Result è l'asserzione che restituisce al SP-Ap l'esito dell'erogazione dell'Identità Digitale all'utente.

Valgono tutti i messaggi di errore definiti da SPID, con, in aggiunta, gli errori specifici per l'attività di recupero identità pregresse.

- ✓ **Allegato 3: result riuso identità**
  - **spid-idreuseverified-result/spid-idreuseverified-result.xsd**
  - **spid-idreuseverified-result/spid-idreusenotverified-result.html**

1.2.6 Altre informazioni

La firma delle asserzioni sia lato SP-Ap che lato IDP dovrà essere apposta con la chiave del certificato pubblico definito nel metadata di configurazione di cui al par. 1.2.3.

Prima della messa in produzione SP-Ap e IDP dovranno testare la procedura mettendo a disposizione ambienti per i processi di competenza.