



Agenzia per l'Italia Digitale

*Presidenza del Consiglio dei Ministri*

**spid**

Sistema Pubblico  
di Identità Digitale

**Procedura per la richiesta di rilascio  
di Identità SPID da Identità pregressa**





## Definizioni e acronimi

<b>SP-IP</b>	Provider delle Identità pregresse  Il soggetto che richiede la migrazione delle proprie Identità pregresse su SPID
<b>IDP</b>	Identity Provider SPID  Soggetto SPID su cui viene trasferito l'account dell'utente del SP
<b>Fonte autorevole</b>	Qualsiasi fonte ufficiale sulla quale si possa fare affidamento per l'ottenimento di dati, informazioni e/o elementi di prova esatti da utilizzare per verificare l'identità. Fonti autorevoli sono individuate dalle convenzioni di cui all'art. 4 del DPCM 24 ottobre 2014

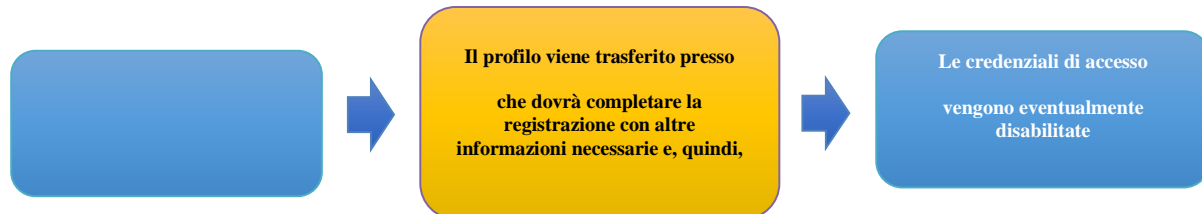
## Versioni del documento

<i>Revisione</i>	<i>Descrizione modifiche</i>	<i>Data</i>
Release 1.0	Prima emissione	febbraio 2018





## 1.2 Procedura per il



La procedura per il

**Provider delle Identità Pregresse (SP-IP):** soggetto che ha richiesto il riconoscimento delle identità pregresse

**Identity Provider (IDP)**

SP

**Utente**

to il

riconoscimento delle identità pregresse.

### 1.2.1 Identificazione elettronica del titolare

di cui è responsabile il SP.

livello di sicurezza almeno analogo al livello SPID 2 (LoA3). Tale identificazione elettronica dovrà essere eseguita

(response ref. 1.2.5.1) da parte dello stesso.

a identificazione elettronica operata

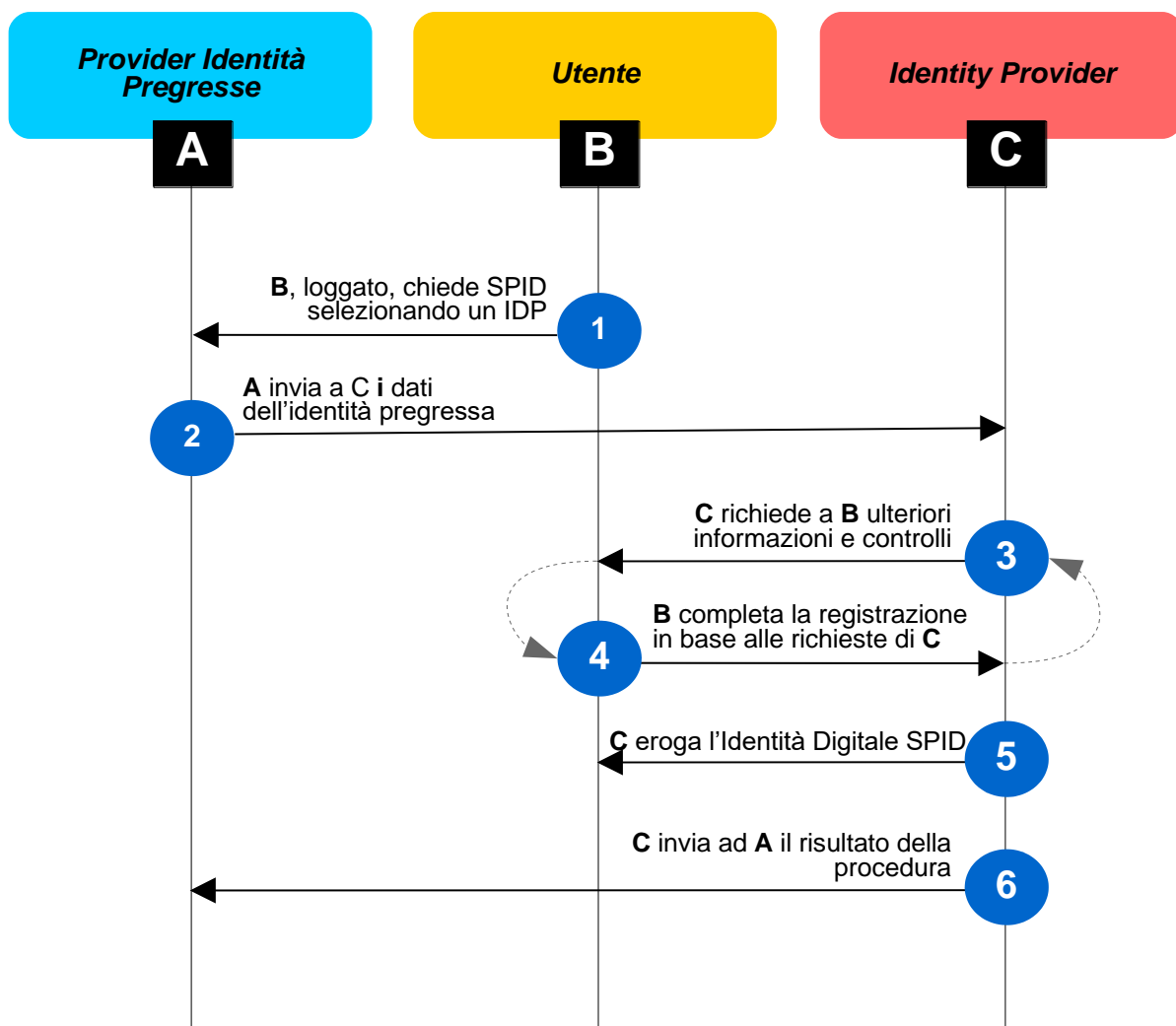
previste dalle Modalità Attuative del sistema SPID.



### 1.2.2 Procedura per la richiesta identità SPID da identità pregressa

Lo scenario prevede che l'utente, richiedendo l'identità digitale tramite il SP-IP che ha richiesto il riconoscimento delle identità pregresse, possa richiedere che venga rediretto verso l'IDP scelto ed effettui una procedura semplificata per l'ottenimento dell'Identità Digitale. Gli utenti che scelgono di effettuare tale richiesta, dovranno obbligatoriamente essere autenticati sul servizio del SP con un livello equivalente al livello SPID 2 (LoA3).

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.





#	Soggetto	Azione	Note
1	<b>Utente</b>	L'utente, loggato sul sistema del 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	<b>SP-IP</b>	L'SP-IP invia una response con i dati del soggetto richiedente l'Identità Digitale SPID	Come indicato al par. 1.2.5.1
3	<b>IDP</b>	L'IDP potrà richiedere all'Utente ulteriori informazioni e passaggi al fine di completare la registrazione ed erogare l'Identità Digitale	
4	<b>Utente</b>		
5	<b>IDP</b>	L'IDP eroga l'Identità Digitale all'Utente	
6	<b>IDP</b>	L'IDP comunica al SP-IP l'esito della richiesta	Come indicato al par. 1.2.5.2

### 1.2.3 Metadata

AgID concorda con il SP e il/gli IDP la pubblicazione del metadata riportante, come informazioni, i dati come da 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-idreuseverified-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 response 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-alsupport-v1.0-cs01.html](http://www.w3.org/2001/04/xmlenc#aes256-cbc)) e W3C XMLEnc (<http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>).

<http://www.w3.org/2001/04/xmlenc#aes256-cbc>

[http://www.w3.org/2001/04/xmlenc#rsa-1\\_5](http://www.w3.org/2001/04/xmlenc#rsa-1_5)

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

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

- Codice Fiscale
- Cognome
- Nome

Il codice fiscale non potrà essere modificato, mentre è lasciata facoltà all'IDP se consentire all'utente di modificare il proprio nome e cognome ed eventuali altri dati ricevuti dal SP, a condizione che la loro correttezza sia riscontrata su una fonte autorevole.

- ✓ **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 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.

Gli IDP dovranno fare una POST della result all'endpoint specificato nel metadata (pipResultEndpoint). I dati dovranno essere criptati come da specifiche SAML 2.0 (<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-alsupport-v1.0-cs01.html>) e W3C XMLEnc (<http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>).

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

#### 1.2.6 Altre informazioni

La firma delle asserzioni sia lato SP 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 e IDP dovranno testare la procedura mettendo a disposizione ambienti per i processi di competenza.