Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SPID
Sistema Pubblico di Identità Digitale

Umberto Rosini
rosini@agid.gov.it

SPID… solo un problema di password?

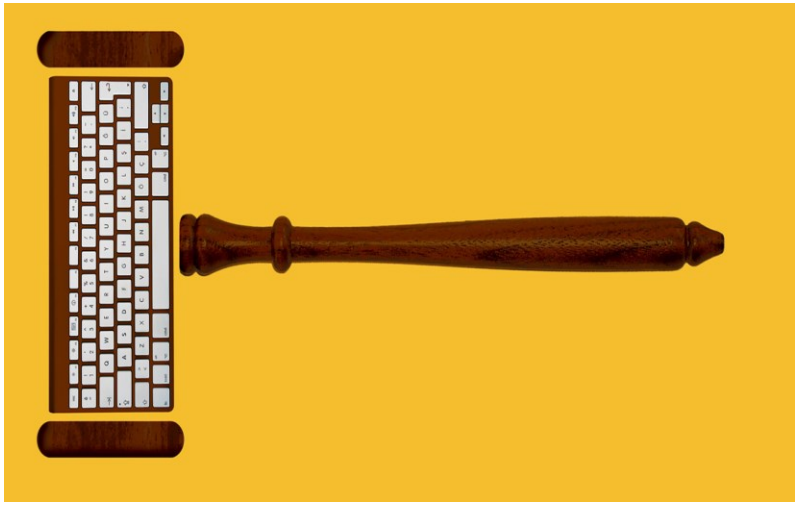
Umberto Rosini - rosini@agid.gov.it

Agenzia per l’Italia Digitale
Presidenza del Consiglio dei Ministri

SPID… DPCM 24 Ottobre 2014

“per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia Digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese”

DPCM 24 ottobre 2014

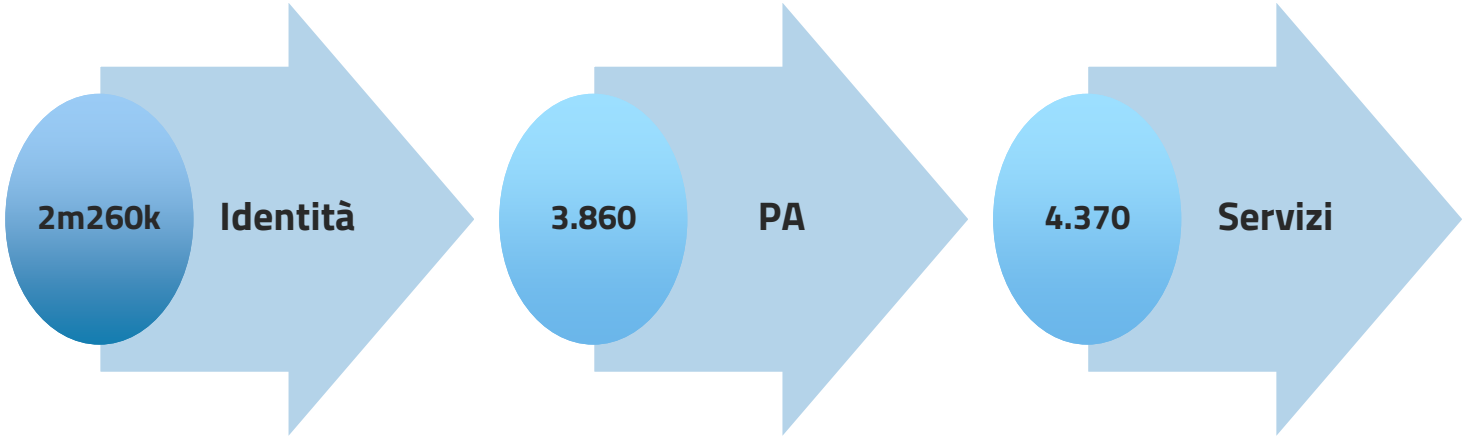


Umberto Rosini - rosini@agid.gov.it

Agenzia per l’Italia Digitale
Presidenza del Consiglio dei Ministri

SPID... cos'è?

SPID, il Sistema Pubblico di Identità Digitale, è la soluzione che ti permette di accedere a tutti i servizi online della Pubblica Amministrazione e dei privati con un'unica Identità Digitale verificata e garantita.



Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

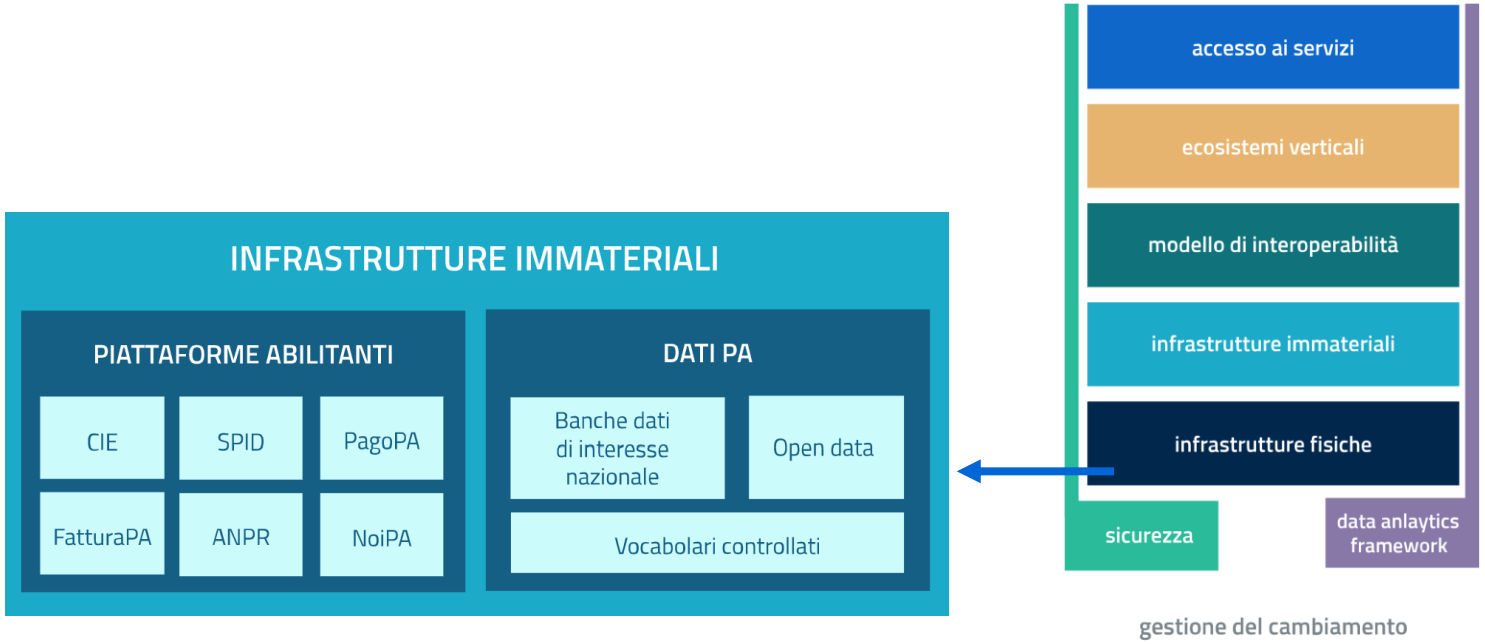
Sistemi di autenticazione servizi PA

- SPID
- CIE
- CNS

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

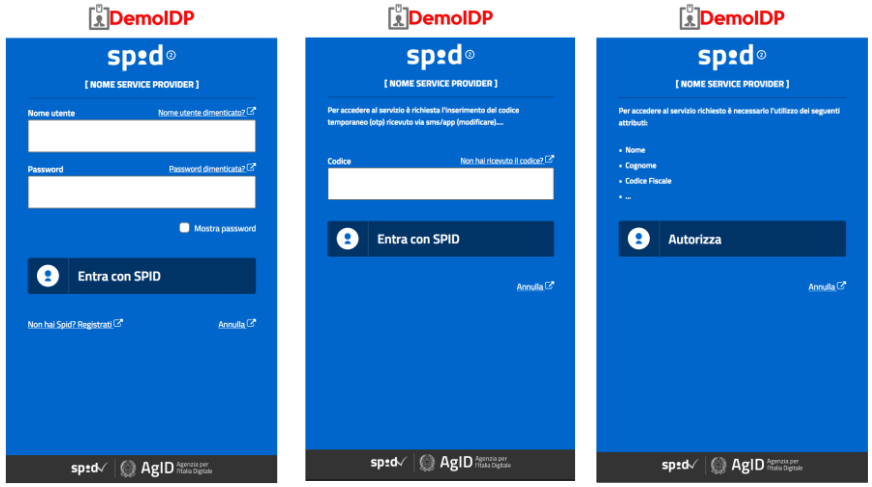
Piano triennale



Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Flusso SPID

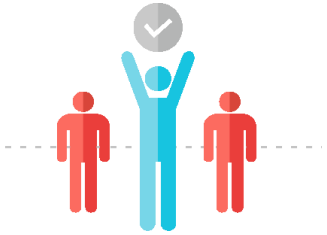


Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SAML

SAML 2 profilo "Web Browser SSO"



Identity Provider

Attribute Authority

Service Provider

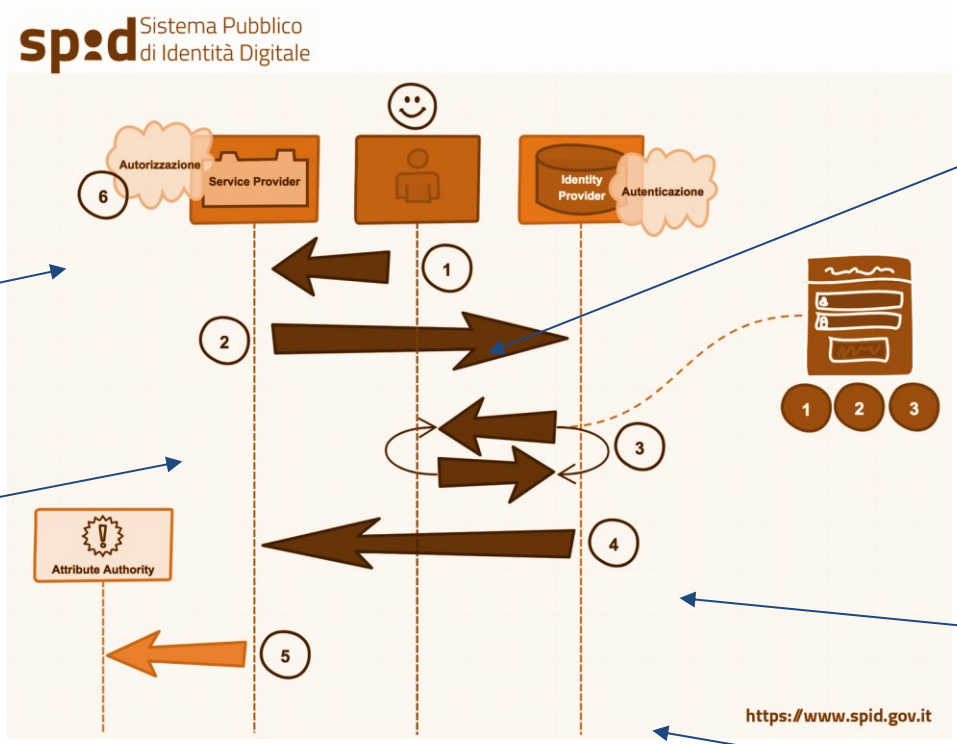
ISO/IEC 29115:2013
Entity authentication assurance framework

Ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SAML



L'SP con i dati provenienti dall'IDP ed eventuali ulteriori di un' Attribute Authority provvede ad autorizzare l'utente nel servizio richiesto

L'utente richiede l'accesso ad un servizio che necessita autenticazione

L'SP invia una request all'Identity Provider

L'IDP richiede le credenziali, secondo il livello SPID stabilito, all'utente

L'SP eventualmente chiederà ulteriori attributi ad un' Attribute Authority

L'IDP invia una response all'SP

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Le risorse OpenSource

Risorse open source a disposizione degli sviluppatori in Developers Italia:

github.com/italia

- **gateway completi:**
  - spid-sp-playbook
  - spid-sp-sapspid
  - spid-sp-simplesamlphp
- **plugin per CMS:**
  - spid-concrete5
  - spid-drupal-module
  - spid-joomla-plugin
  - spid-laravel
  - spid-liferay
  - spid-limesurvey-plugin
  - spid-magento-ext
  - spid-wordpress
- **plugin per web framework**
  - spid-django
  - spid-passport
  - spid-rails
  - spid-perl-dancer2
  - spid-spring
  - spid-symfony-bundle
- **librerie generiche**
  - spid-android-sdk
  - spid-dotnet-sdk
  - spid-ios-sdk
  - spid-perl

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

eIDAS

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Evoluzioni del Sistema Pubblico di Identità Digitale

- ***SPID Smart Button***
- ***OpenID Connect***
- ***Docs Italia***
- ***Riscrittura di attributi***
- ***Attribute Authority***
- ***Statistiche***
- ***OnBoarding***
- ***Nuove convenzioni e soggetti aggregatori***
- ***Perfezionamento flussi e operazioni dispositive***
- ***Ambiente di test***

Umberto Rosini - rosini@agid.gov.it

Smart Button

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

OpenID Connect

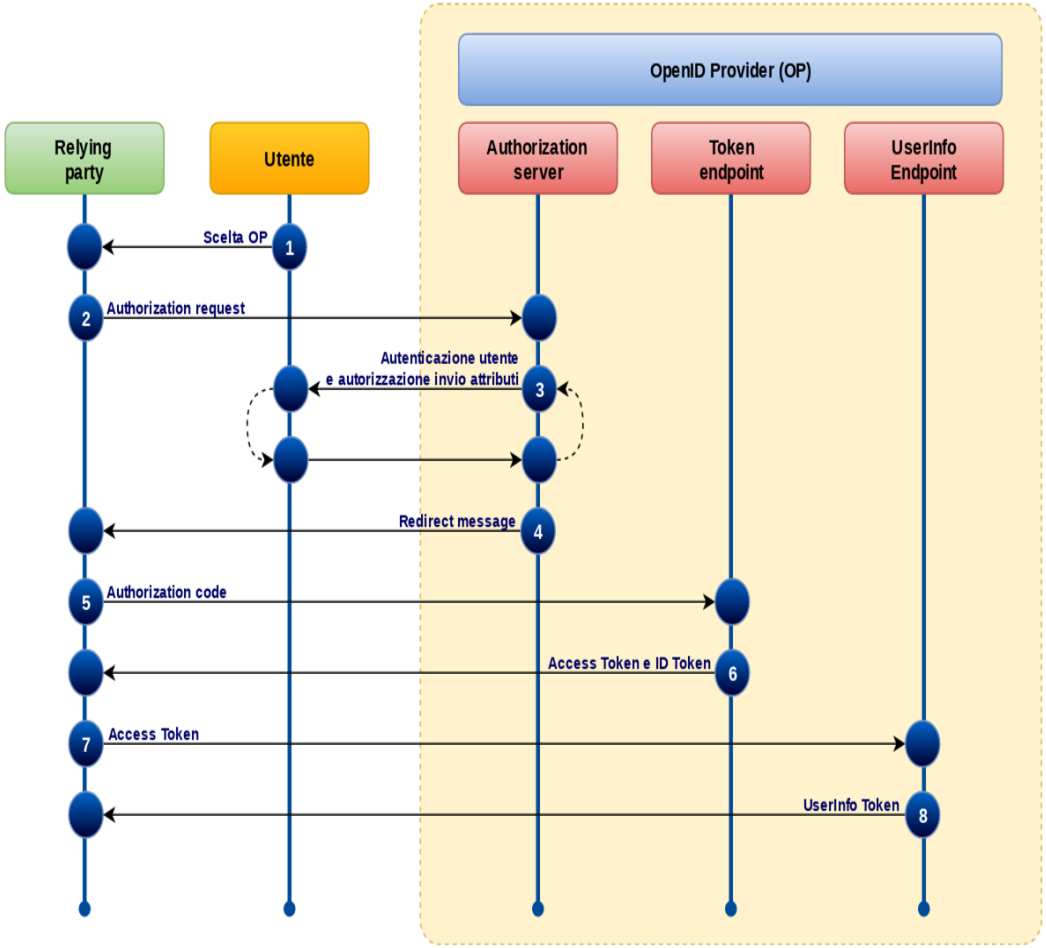
OpenID Connect è un layer di identità basato su JSON / REST che si posiziona sopra al protocollo OAuth 2.0. La sua filosofia di design è "rendi semplici le cose semplici e rendi possibili le cose complicate".
OpenID Connect non si occupa solo di autenticazione ma può essere anche utilizzato per autorizzazione, delega e API access management. SPID OpenID Connect si basa sul profilo iGOV.

I suoi punti di forza sono:

- facilità di integrazione;
- abilità di integrare applicazioni su diverse piattaforme, single-page app, web, backend, mobile, IoT;
- permette integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile;
- risolve diverse problematiche di sicurezza riscontrate in OAuth 2.0
- è utilizzato da tutti i servizi social e anche di pagamento.

Umberto Rosini - rosini@agid.gov.it

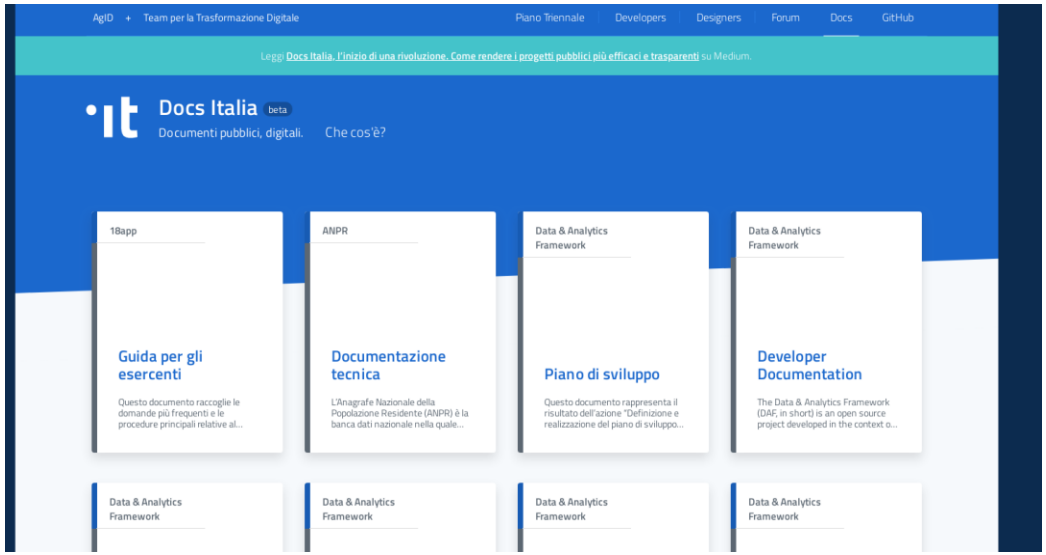
OpenID Connect



Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Docs Italia

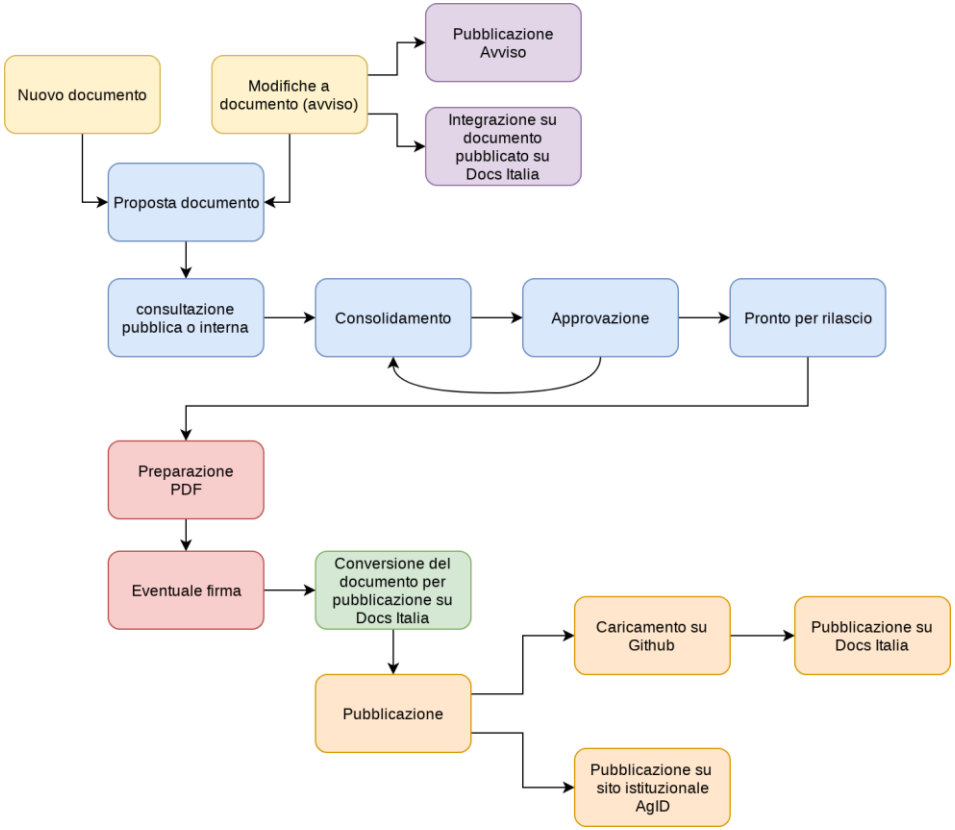


- **https://docs.italia.it**
- **Versione web regole tecniche**
- **Guide semplificate**
- **Documenti in consultazione pubblica**

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Docs Italia



Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Attributi

Attributo	Identificatore[1]	Tipo[2]	Note
Codice identificativo	*spidCode*	*xs:string*	Il codice identificativo è assegnato dal gestore dell'identità digitale, deve essere univoco in ambito SPID. Il formato è il seguente: *<codice Identificativo> = <cod_IdP><nr. univoco>* Dove: • *<cod_IdP>*: è un codice composto da 4 lettere univocamente assegnato al gestore delle identità; • *<nr.univoco>*: è una stringa alfanumerica composta da 10 caratteri che il gestore delle identità genera in maniera univoca nell'ambito del proprio dominio. (Es. "*ABCD123456789A*")
Nome	*name*	*xs:string*	Stringa composta da una sequenza di una o più sottostringhe non vuote con carattere iniziale in maiuscolo intervallate da uno (solo) spazio (Es. "*Francesca*" , "*Giovanni Mario*")
Cognome	*familyName*	*xs:string*	Stringa composta da una sequenza di una o più sottostringhe non vuote con carattere iniziale in maiuscolo intervallate da uno (solo) spazio (Es."*Rossi*", "*Bianchi Verdi*")
Luogo di nascita	*placeOfBirth*	*xs:string*	Stringa corrispondente al codice catastale (Codice Belfiore) del Comune o della nazione estera di nascita. (Es. "*F205*" per la citta di Milano)
Provincia di nascita	*countyOfBirth*	*xs:string*	Stringa corrispondente alla sigla della provincia di nascita (Es. "*MI*" per provincia di Milano)
Data di nascita	*dateOfBirth*	*xs:date*	Secondo specifica *xs:date* nel formato "*YYYY-MM-DD*" dove • *YYYY* indica l'anno utilizzando 4 cifre; • *MM* indica il mese in (due) cifre; • *DD* indica il giorno in (due) cifre; (Es. "*2002-09-24*")
Sesso	*gender*	*xs:string*	Valori ammessi: • "*F*" per sesso femminile • "*M*" per sesso maschile
Ragione o denominazione sociale	*companyName*	*xs:string*	Stringa composta da una sequenza di sottostringhe non vuote intervallate da uno (solo) spazio. In maiuscolo le sottostringhe corrispondenti a nomi . (Es. "*Agenzia per l'Italia Digitale*")
Sede legale	*registeredOffice*	*xs:string*	Stringa composta da una sequenza di sottostringhe non vuote intervallate da uno (solo) spazio rappresentanti: • Tipologia(via, viale, piazza …); • Indirizzo; • Nr.civico; • CAP; • Luogo; • Provincia; (Es. "*via Listz 21 00144 Roma*")
Codice fiscale	*fiscalNumber*	*xs:string*	Per il formato si faccia riferimento alla codifica dell'attributo CF per i certificati, proposta nell'ambito del Draft ETSI EN 319 412-1, che nel caso specifico prevede la seguente composizione: *TINIT-<CodiceFiscale>*
Partita IVA	*ivaCode*	*xs:string*	Per il formato si faccia riferimento alla codifica dell'attributo Partita IVA per i certificati, proposta nell'ambito del Draft ETSI EN 319 412-1, che nel caso specifico prevede la seguente composizione: *VATIT-<PartitaIVA>*
Documento d'identità	*idCard*	*xs:string*	Stringa composta dalla sequenza di sottostringhe (non vuote) concatenate nell'ordine sotto riportato e intervallate da uno (solo) spazio: • *<tipo di documento> xs:string*: valori ammessi: *cartaIdentita, passaporto, patenteGuida, patenteNautica, librettoPensione, patentinoImpTermici, portoArmi, tesseraRiconoscimento*; • *<numero di documento> xs:string*, Numero del documendo; • *<ente emettitore> xs:string*; stringa ottenuta dalla concatenazione dei termini costituenti la denominazione dell'ente a meno di congiunzioni, articoli e preposizioni. Es. regioneLazio (Regione Lazio); provinciaCatania (Provincia di Catania); prefetturaRoma (Prefettura di Roma); MinisteroEconomiaFinanze (Ministero dell'Economia e delle Finanze); • *<data emissione> xs:date*; data di rilascio del documento; • *<data scadenza> xs:date*; data di scadenza del documento;

Umberto Rosini - rosini@agid.gov.it

Attributi

Tabella attributi secondari

Attributo	Identificatore[3]	Tipo[4]	Note
Numero di telefono mobile	*mobilePhone*	*xs:string*	Stringa numerica senza spazi intermedi (Es. " *34912345678*")
Indirizzo di posta elettronica	*email*	*xs:string*	Formato standard indirizzo di posta elettronica
Domicilio fisico	*address*	*xs:string*	Stringa composta da una sequenza di sottostringhe non vuote intervallate da uno (solo) spazio rappresentanti: • Tipologia(via, viale, piazza …); • Indirizzo; • Nr.civico; • CAP; • Luogo; • Provincia;
Data di scadenza identità	*expirationDate*	*xs:date*	Secondo specifica *xs:date*
Domicilio digitale	*digitalAddress*	*xs:string*	Indirizzo casella PEC

Prefisso	XML Namespace
xs	*http://www.w3.org/2001/XMLSchemainstance*

Umberto Rosini - rosini@agid.gov.it

Riscrittura attributi

Domicilio fisico	*physicalDomicile*	**<tipologia-toponimo>_<toponimo>_<numero>_<cap>_<nazione>_<codice-comune>_<nome-comune>_<sigla-provincia>** La tipologia-toponimo fa riferimento al vocabolario controllato (cfr...) Il comune è corrispondente al codice catastale (Codice Belfiore) del Comune se Italiano o il geonameId se Estero (geonames.org) La nazione riporterà il codice ISO 3166-1 alpha-2 della nazione del comune Esempio *Sede legale italiana:* • via_strada test_10/A_CAP_IT_H501 *Sede legale estera:* • street_test_99_CAP_US_5128638 Rif:http://api.geonames.org/get?geonameId=5128638&username=demo&style=full Rif:http://download.geonames.org/export/dump/ * Per i comuni si fa riferimento all'archivio storico dei comuni presente sul sito ANPR (https://www.anpr.interno.it/portale)

Umberto Rosini - rosini@agid.gov.it

Riscrittura attributi

2.1 Persone fisiche (uso personale)

Attributo	Identificatore	Tipologia	Obbligatorietà
Codice identificativo	*spidCode*	Primario	Si
Nome	*name*	Primario	Si
Cognome	*familyName*	Primario	Si
Luogo di nascita	*placeOfBirth*	Primario	Si
Codice fiscale	*fiscalNumber*	Primario	Si
Data di nascita	*dateOfBirth*	Primario	Si
Sesso	*gender*	Primario	Si
Documento di identità	*idCard*	Primario	Si
Numero di telefono mobile	*phoneNumber*	Secondario	Si
Indirizzo di posta elettronica	*email*	Secondario	Si
Indirizzo PEC	*pec*	Secondario	No
Domicilio fisico	*physicalDomicile*	Secondario	Si
Domicilio digitale	*digitalDomicile*	Secondario	No
Tipologia di identità	*identityType*	Secondario	Si
Sottotipologia di identità	*identityPurpose*	Secondario	Si

2.2 Persone fisiche (uso professionale)

Attributo	Identificatore	Tipologia	Obbligatorietà
Codice identificativo	*spidCode*	Primario	Si
Nome	*name*	Primario	Si
Cognome	*familyName*	Primario	Si
Luogo di nascita	*placeOfBirth*	Primario	Si
Codice fiscale	*fiscalNumber*	Primario	Si
Partita IVA	*vatNumber*	Primario	No
Data di nascita	*dateOfBirth*	Primario	Si
Sesso	*gender*	Primario	Si
Documento di identità	*idCard*	Primario	Si
Numero di telefono mobile	*phoneNumber*	Secondario	Si
Indirizzo di posta elettronica	*email*	Secondario	Si
Indirizzo PEC	*pec*	Secondario	No
Domicilio fisico	*physicalDomicile*	Secondario	Si
Domicilio digitale	*digitalDomicile*	Secondario	No
Tipologia di identità	*identityType*	Secondario	Si
Sottotipologia di identità	*identityPurpose*	Secondario	Si

Umberto Rosini - rosini@agid.gov.it

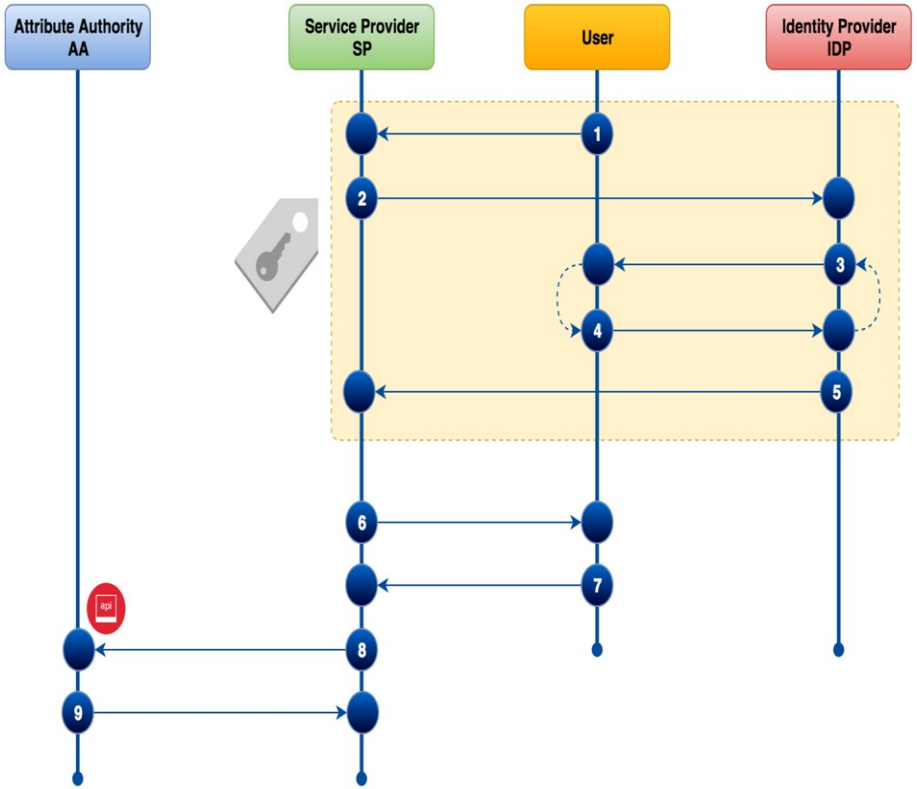
Riscrittura attributi

2.3 Persone giuridiche

Attributo	Identificatore	Tipologia	Obbligatorietà
Codice identificativo	*spidCode*	Primario	Si
Ragione o denominazione sociale	*companyName*	Primario	Si
Sede legale	*registeredOffice*	Primario	Si
Partita IVA	*vatNumber*	Primario	Si
Codice fiscale persona giuridica	*legalPersonFiscalNumber*	Secondario	Si
Nome persona collegata	*linkedPersonName*	Secondario	Si
Cognome persona collegata	*linkedPersonFamilyName*	Secondario	Si
Codice fiscale persona collegata	*linkedPersonFiscalNumber*	Secondario	Si
Email	*email*	Secondario	Si
Numero di telefono mobile persona collegata	*phoneNumber*	Secondario	Si
Indirizzo di posta elettronica persona giuridica	*legalPersonEmail*	Secondario	Si
Indirizzo PEC persona giuridica	*pec*	Secondario	Si
Ambiti o limitazioni di utilizzo	*areaLimitationsUse*	Secondario	No
Tipologia di identità	*identityType*	Secondario	Si

@ SMAU Padova // 23-01-18
Umberto Rosini - rosini@agid.gov.it

Attribute Authority



- API Standard
- two-way authentication
- whitelist

Umberto Rosini - rosini@agid.gov.it

Statistiche

- per ottenere **statistiche di business** (**IdP, SP, AA**)
  - le statistiche sono raccolte per conoscere lo stato di avanzamento del sistema, elaborare documentazione, essere a supporto di organi di stampa e cittadini attraverso il rilascio in forma di dato aperto;

- per **monitorare** *in tempo reale* le diverse componenti del sistema (**IdP, SP, AA**)
  - i dati e le informazioni di monitoraggio sono raccolte per controllare in tempo reale o comunque non superiore a intervalli di un giorno, aspetti del sistema riguardanti il funzionamento dello stesso;

- per **vigilare** sul rispetto di quanto stabilito in convenzione (**IdP**)
  - I dati e le informazioni riguardanti la vigilanza riguardano il rispetto formale di quanto convenuto in sede di accreditamento e convenzione;

Umberto Rosini - rosini@agid.gov.it

Convenzioni

- **Service provider pubblici**
- **Service provider privati**

Umberto Rosini - rosini@agid.gov.it
Umberto Rosini - rosini@agid.gov.it

Soggetti aggregatori

Aggregatore può essere un soggetto pubblico o privato che offre un servizio implementato a SPID o un sistema di Access Management a Pubbliche Amministrazioni.

Convenzione:
https://bit.ly/2pxdM0I

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Perfezionamento flussi e operazioni dispositive

1. SPID Livello 1 (LoA2)

Livello Servizio 1	Livello Servizio 2	Flusso di autenticazione	Note
1	1	Nessuna ulteriore autenticazione richiesta	Single Sign On
1	2	Richiesto OTP	
1	3	Richiesta autenticazione di 3 livello (specifica per IDP)	

2. SPID Livello 2 (LoA3)

Livello Servizio 1	Livello Servizio 2	Flusso di autenticazione	Note
2	1	Nessuna ulteriore autenticazione richiesta	Single Sign On
2	2	Richiesto OTP	
2	3	Richiesta autenticazione di 3 livello (specifica per IDP)	

3. SPID Livello 3 (LoA3)

Livello Servizio 1	Livello Servizio 2	Flusso di autenticazione	Note
3	1	Nessuna ulteriore autenticazione richiesta	Single Sign On
3	2	Richiesto OTP	
3	3	Richiesta autenticazione di 3 livello (specifica per IDP)	

Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Perfezionamento flussi e operazioni dispositive

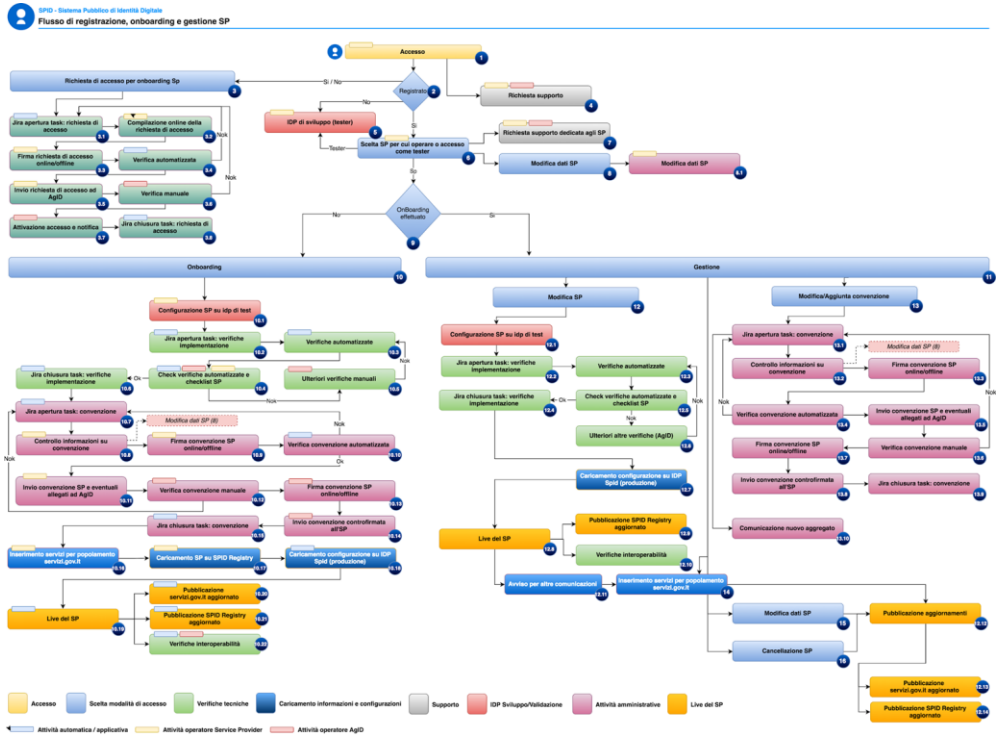
4. SPID Operazioni dispositive all'interno dello stesso servizio

L'operazione dispositiva è un'attività che si applica ad azioni effettuate all'interno dello stesso servizio in cui ha acceduto l'utente.
Prevede la chiamata all'IDP con un livello maggiore o uguale a quello utilizzato per accedere (eccetto per il livello 1 per cui si applica il single sign on).

Livello iniziale	Livello dispositivo	Flusso di autenticazione	Note
1	2	Richiesto OTP	
1	3	Richiesta autenticazione di 3 livello (specifica per IDP)	
2	2	Richiesto OTP	
2	3	Richiesta autenticazione di 3 livello (specifica per IDP)	
3	3	Richiesta autenticazione di 3 livello (specifica per IDP)	

Umberto Rosini - rosini@agid.gov.it

Onboarding

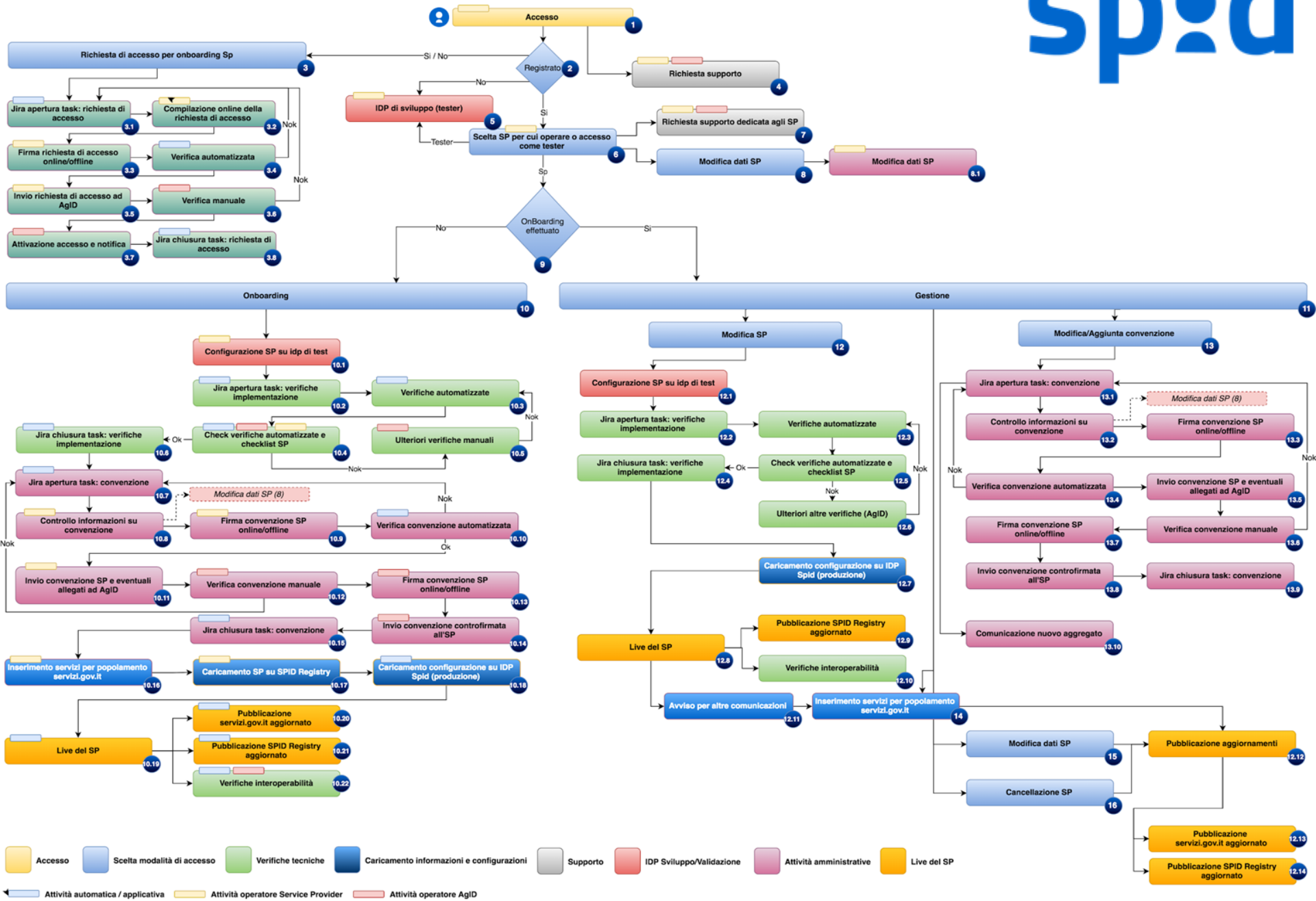


Umberto Rosini - rosini@agid.gov.it

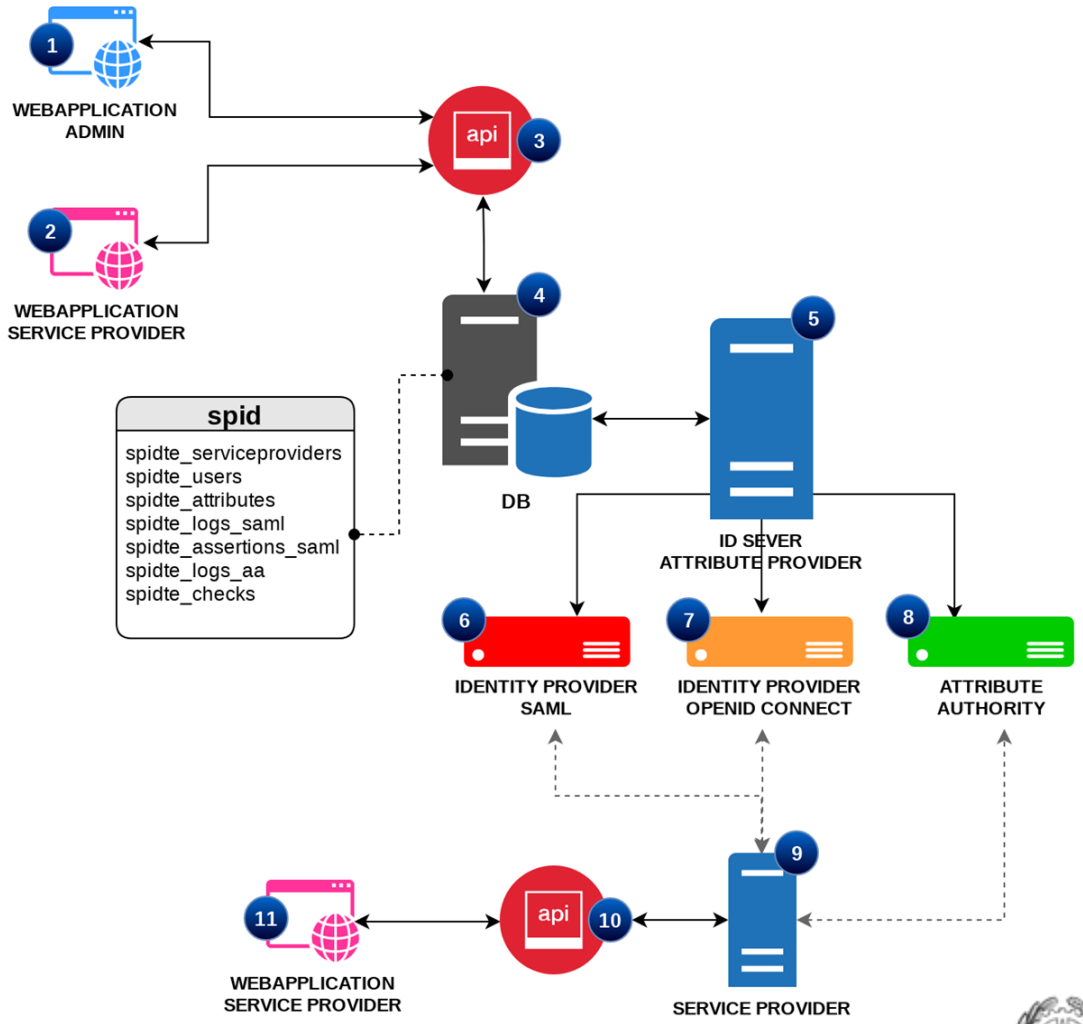
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SPID - Sistema Pubblico di Identità Digitale

Flusso di registrazione, onboarding e gestione SP

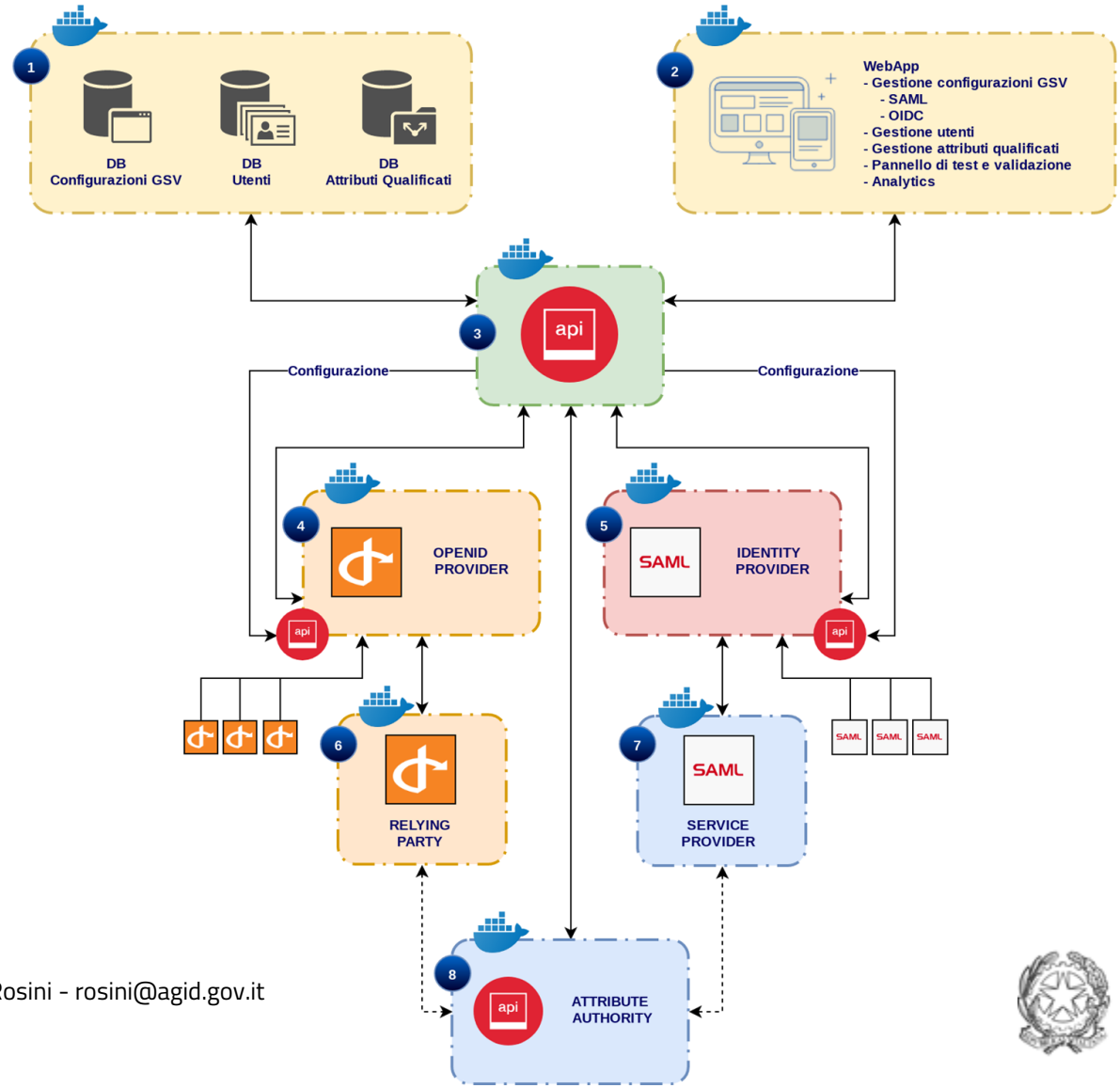


Ambiente di test



Umberto Rosini - rosini@agid.gov.it

Ambiente di test



Umberto Rosini - rosini@agid.gov.it

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

sp:d

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

www.agid.gov.it | www.spid.gov.it

Umberto Rosini
rosini@agid.gov.it
@umbr0s