

**IAM - Onboarding Applicativi e modalità di autenticazione**

Versione Gennaio 2025

Tabella 1 – Tabella delle Versioni

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIONI** | | | |
| **DATA** | **VERSIONE** | **DESCRIZIONE** | **CAP/SEZ. MODIFICATI** |
| 27/08/2024 | 1.0 | Prima versione del documento | Tutti |
| 20/09/2024 | 2.0 | Autenticazione tramite eIDAS  Linee Guida | Accreditamento  Autenticazione  Autenticazione Utenze personali  Autenticazione tramite eIDAS  Linee Guida |
| 31/01/2025 | 3.0 | Revisione Documento | Riorganizzazione Documento |

**Indice**

[1. Introduzione al documento 5](#_Toc196726574)

[1.1. Scopo e campo di applicazione 5](#_Toc196726575)

[1.2. Acronomi e Glossario 5](#_Toc196726576)

[2. Accreditamento 6](#_Toc196726577)

[3. Autenticazione 7](#_Toc196726578)

[3.1. Autenticazione M2M 8](#_Toc196726579)

[3.2. Autenticazione M2W 9](#_Toc196726580)

[3.3. Autenticazione Utenze Personali 11](#_Toc196726581)

[3.3.1. Autenticazione tramite username e password 12](#_Toc196726582)

[3.3.2. Autenticazione tramite SPID 14](#_Toc196726583)

[3.3.3. Autenticazione tramite CIE 17](#_Toc196726584)

[3.3.4. Autenticazione tramite eIDAS 18](#_Toc196726585)

[4. Endpoint Esposti 20](#_Toc196726586)

[4.1. Ambiente di Collaudo 20](#_Toc196726587)

[4.2. Ambiente di Produzione 20](#_Toc196726588)

[5. WSO2 API 22](#_Toc196726589)

[5.1. Creazione ed Eliminazione Utenti 22](#_Toc196726590)

[6. Implementazione Protocollo OpenID 25](#_Toc196726591)

[7. Linee Guida 26](#_Toc196726592)

[8. Allegati 27](#_Toc196726593)

**Indice delle tabelle**

[Tabella 1 – Tabella delle Versioni 2](#_Toc196726594)

[Tabella 2 – Acronomi e Glossario 5](#_Toc196726595)

[Tabella 3 – Campi JWT 7](#_Toc196726596)

[Tabella 4 – Tenant di Collaudo e Produzione 9](#_Toc196726597)

[Tabella 5 – Tenant di Collaudo e Produzione 11](#_Toc196726598)

[Tabella 6 – Endpoint Esposti 20](#_Toc196726599)

[Tabella 7 – Endpoint Ambiente di Collaudo 20](#_Toc196726600)

[Tabella 8 – Endpoint Ambiente di Produzione 21](#_Toc196726601)

[Tabella 9 – Allegati 27](#_Toc196726602)

**Indice delle figure**

[Figura 1 – Modulo Richiesta Accreditamento 6](#_Toc196726603)

[Figura 2 – JWT Access Token 7](#_Toc196726604)

[Figura 3 – Autenticazione M2M 8](#_Toc196726605)

[Figura 4 – Autenticazione M2W 9](#_Toc196726606)

[Figura 5 – Autenticazione Utenze Personali 12](#_Toc196726607)

[Figura 6 – Modalità di Autenticazione 12](#_Toc196726608)

[Figura 7 – Autenticazione tramite username e password 13](#_Toc196726609)

[Figura 8 – Maschere di Autenticazione utente tramite username e password 13](#_Toc196726610)

[Figura 9 – Autenticazione tramite SPID 14](#_Toc196726611)

[Figura 10 – Maschere di Autenticazione utente tramite SPID 16](#_Toc196726612)

[Figura 11 – Maschere di Autenticazione utente tramite CIE 17](#_Toc196726613)

[Figura 12 – Maschere di Autenticazione utente tramite eIDAS 18](#_Toc196726614)

[Figura 13 – Creazione ed Eliminazione Utenti 23](#_Toc196726615)

# Introduzione al documento

Il presente documento descrive le specifiche per l’onboarding di una applicazione nel perimetro di IAM ECOMiC, implementato attraverso il software WSO2 Identity Server (WSO2 IS).

## Scopo e campo di applicazione

Scopo del documento è descrivere i passaggi tecnici necessari all’accreditamento (onboarding) di una applicazione in uno dei tenant attualmente definiti: ISPC, ICAR, ICCU ed al successivo utilizzo dello IAM da parte dell’applicazione accreditata.

## Acronomi e Glossario

Tabella 2 – Acronomi e Glossario

|  |  |
| --- | --- |
| DEFINIZIONE/ ACRONIMO | DESCRIZIONE |
| IAM | Identity and Access Management |
| IdP | Identity Provider |
| JWT | JSON Web Token |
| M2M | Machine to Machine |
| M2W | Machine to Widget |
| OIDC | OpenID Connect |
| SP | Service Provider |

# Accreditamento

L’integrazione tra applicazione e IAM prevede che l’applicazione si identifichi attraverso l’uso di una coppia client\_id/client\_secret.

Tale coppia di chiavi viene rilasciata dal sistema IAM centrale a valle di una richiesta di accreditamento (onboarding) dell’applicazione (SP - Service Provider) all’interno della lista dei SP supportati dallo IAM stesso.

Al fine di accreditare una o *n* nuove applicazioni tra i SP supportati dallo IAM centrale, il richiedente dovrà compilare il file Excel “Allegato 6A - IAM\_Modulo di accreditamento nuove applicazioni\_202501” disponibile come allegato tecnico a tale documento (Cfr. capitolo: “[Allegati](#_Allegati)”) e inviarlo al seguente indirizzo e-mail: [ipac.info@cultura.gov.it](mailto:ipac.info@cultura.gov.it).

Il referente dell’applicazione richiedente l’accreditamento, dovrà indicare nel file excel le seguenti informazioni:

* Nome dell’Application SP e relative Modalità di Autenticazione richieste
* Nome del relativo Tenant di Collaudo e Produzione con le relative URL di Callback ed eventuale Logout, nonché la necessità di gestire gli utenti nello UserStore

Figura 1 – Modulo Richiesta Accreditamento

Immagine che contiene testo, schermata, numero, Parallelo

Il contenuto generato dall'IA potrebbe non essere corretto.

Al termine della lavorazione dell’onboarding, il referente dell’applicazione richiedente riceverà comunicazione delle coppie client\_id/client\_secret da poter utilizzare per le autenticazioni degli utenti e delle applicazioni.

# Autenticazione

Lo IAM genera access token di tipo “JWT”, ovvero un token di lunghezza contenuta che di fatto è codificato in base64. Con questo token viene effettuata una richiesta network al server di autorizzazione per ricevere le informazioni di autorizzazione associate al token.

Di seguito, un esempio di un jwt token decodificato di una utenza SPID:

Figura 2 – JWT Access Token

Immagine che contiene testo, schermata, documento, Carattere

Descrizione generata automaticamente

Tabella 3 – Campi JWT

|  |  |
| --- | --- |
| CAMPO JWT | DESCRIZIONE |
| Sub | Soggetto dell’utenza in SPID e CIE il codice fiscale |
| given\_name | Nome |
| family\_name | Cognome |
| fiscalNumber | Codice Fiscale |
| email | Email del utente (n.b. CIEID non ha email) |

Sono attualmente disponibili le seguenti modalità di autenticazione:

* M2M – Machine to Machine
* M2W – Machine to Widget
* Utenze personali:
  + Username/password (lo username può essere anche una e-mail)
  + SPID
  + CIE
  + eIDAS

## Autenticazione M2M

L’autenticazione sullo IAM prevede un interfacciamento via OIDC e l’invio da parte dell’applicazione di client ID e client secret.

Di seguito viene riportato il sequence diagram della fase di autenticazione M2M:

Figura 3 – Autenticazione M2M

Immagine che contiene testo, schermata, diagramma, Rettangolo

Descrizione generata automaticamente

Di seguito si riporta una Curl di esempio relativa ad una chiamata M2M; l’applicativo dovrà conoscere il suo client\_id e client\_secret per staccare il token:

*curl -L 'https://identity.cloud.sbn.it/oauth2/token' -H 'Content-Type: application/x-www-form-urlencoded' -d 'grant\_type=client\_credentials'-d 'scope=openid profile' -d 'client\_id=YYYYYYYYYYYYYY' -d 'client\_secret=XXXXXXXXXXXXXXX'*

Come risposta ritornerà un json senza id\_token:

*{"access\_token":"Access token in formato jwt","scope":"openid profile","token\_type":"Bearer","expires\_in":3600}*

## Autenticazione M2W

Il sistema IAM mette a disposizione le informazioni pubbliche esposte dall’endpoint standard well-known (<https://identity.cloud.sbn.it/t/nome_TENANT/oauth2/oidcdiscovery/.well-known/openid-configuration>), dove nome\_TENANT è uno dei seguenti valori:

Tabella 4 – Tenant di Collaudo e Produzione

|  |  |
| --- | --- |
| AMBIENTE | TENANT |
| COLLAUDO | coll.ispc.it |
| coll.icar.it |
| coll.cloud.sbn.it |
| PRODUZIONE | ispc.it |
| icar.it |
| iccu.it |

e assume che la verifica dei token abilitanti per il flusso M2W sia effettuata lato client.

Al fine di agevolare la verifica dei token, il sistema IAM ECOMiC espone un’API specifica.

Tale API accetta in input il token da verificare e, all’interno della sua risposta, fornisce informazioni in merito alla effettiva validità e durata residua.

Di seguito viene riportato il sequence diagram della fase di autenticazione M2W:

Figura 4 – Autenticazione M2W

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Di seguito viene riportato un esempio di un tracciato di una autenticazione di un portale web:

1. Per prima cosa il portale web manda una richiesta di authorize allo IAM inserendo nelle query paramenters le seguenti informazioni:

* **scope**= openid email profile
* **response\_type**= code
* **redirect\_uri**= <https://alphabetica.it/c/portal/login/openidconnect>
* **state**= OzNZ1tBIwm45icwO9vN6u3OUHQatvAugsPMgCHMGXIg
* **nonce**= WIoVgwhQc64F9jS-zSKYXjLEqq2EkBPq3G3oYzikXP0
* **client\_id**= YYYYYYYYYYYYYY

1. Si riporta come esempio la seguente url:

<https://identity.cloud.sbn.it/oauth2/authorize?scope=openid> email profile&response\_type=code&redirect\_uri= <https://alphabetica.it/c/portal/login/openidconnect&state=OzNZ1tBIwm45icwO9vN6u3OUHQatvAugsPMgCHMGXIg&nonce=WIoVgwhQc64F9jS-zSKYXjLEqq2EkBPq3G3oYzikXP0&client_id=YYYYYYYYYYYYYY>

1. Una volta autenticato, il sistema rimanda all’applicativo, come è stato richiesto dal parametro redirect\_uri, e aggiunge nel query param un code, ad esempio:

<https://alphabetica.it/c/portal/login/openidconnect?code=66b2f737-b5d2-3f5f-a95d-b597c3068674&state=5439054390klgfdlk>

L’applicativo manderà in breve termine la richiesta per staccare il token come nel seguente esempio:

*curl -L 'https://identity.cloud.sbn.it/oauth2/token' -H 'Content-Type: application/x-www-form-urlencoded' -d 'grant\_type=authorization\_code' -d 'code=66b2f737-b5d2-3f5f-a95d-b597c3068674' -d 'redirect\_uri=https://alphabetica.it/c/portal/login/openidconnect' -d 'client\_id=YYYYYYYYYYYYYY' -d 'client\_secret=XXXXXXXXXXXXXXX'*

Come risposta si avrà un json con il seguente formato:

*{"access\_token":"Access token in formato jwt","refresh\_token":"e2313f42-0f7f-36dc-bdaf-c7c23253d1dd","scope":"openid profile","id\_token":"ID token in formato jwt","token\_type":"Bearer","expires\_in":3600}*

Si fornisce come allegato a tale documento un *tracciato record di esempio di autenticazione M2W* il cui metodo di login utilizzato è tramite SPID Demo in ambiente di Collaudo - la stessa logica delle chiamate è utilizzata per le altre tipologie di login: CIE/eIDAS/Utenze Nominali - (“Allegato 6B - IAM\_

Tracciato record di esempio Autenticazione M2W\_202501” - Cfr. capitolo: “[Allegati](#_Allegati)”).

## Autenticazione Utenze Personali

L’integrazione tra applicazione e IAM prevede che l’utente effettui il login direttamente sulla pagina messa a disposizione dallo IAM centrale.

L’applicazione può accedere a tale pagina attraverso una chiamata HTTPS con metodo GET all’indirizzo (produzione):

**https://identity.cloud.sbn.it/oauth2/authorize**

Tale richiesta deve essere corredata dalle seguenti informazioni:

* **client\_id/secret**: credenziali rilasciate in fase di accreditamento
* **redirect\_uri**: indirizzo verso cui essere ridirezionati ad autenticazione ultimata
* **issuer**: <https://identity-collaudo.cloud.sbn.it/t/nome_TENANT/oauth2/oidcdiscovery>
* dove ***nome\_TENANT*** è uno dei seguenti valori:

Tabella 5 – Tenant di Collaudo e Produzione

|  |  |
| --- | --- |
| AMBIENTE | TENANT |
| COLLAUDO | coll.ispc.it |
| coll.icar.it |
| coll.cloud.sbn.it |
| PRODUZIONE | ispc.it |
| icar.it |
| iccu.it |

* **scope**: in accordo con il tipo di insieme di dati da recuperare (es. ‘openid’)

Per l’autenticazione dell’utente, sarà possibile integrare nella GUI dell’applicativo la pagina di Login offerta dallo IAM stesso.

A valle dell’autenticazione l’applicativo riceverà in risposta un json analogo al seguente:

*{"access\_token":"Access token in formato jwt","refresh\_token":"e2313f42-0f7f-36dc-bdaf-c7c23253d1dd","scope":"openid profile","token\_type":"Bearer","expires\_in":3600}*

Di seguito il generico sequence diagram della fase di autenticazione:

Figura 5 – Autenticazione Utenze Personali

Immagine che contiene testo, schermata, quadrato, diagramma

Descrizione generata automaticamente

L’utente può autenticarsi tramite le seguenti modalità:

* username/password (ministeriali e non)
* SPID
* CIE
* eIDAS

Figura 6 – Modalità di Autenticazione

Immagine che contiene testo, schermata, Carattere, Marchio

Descrizione generata automaticamente

### Autenticazione tramite username e password

Di seguito il sequence diagram che descrive l’interazione tra un’applicazione che voglia utilizzare il sistema IAM in oggetto e WSO2 stesso, nel caso di autenticazione tramite username e password:

Figura 7 – Autenticazione tramite username e password

Immagine che contiene testo, schermata, diagramma, Rettangolo

Descrizione generata automaticamente

Di seguito vengono riportate le maschere di riferimento in cui l’utente dovrà inserire le proprie credenziali (username e password) per accedere all’applicazione di riferimento:

Figura 8 – Maschere di Autenticazione utente tramite username e password

Immagine che contiene testo, schermata, Carattere, design

Il contenuto generato dall'IA potrebbe non essere corretto.

### Autenticazione tramite SPID

Di seguito il sequence diagram che descrive l’interazione tra una applicazione che voglia utilizzare il sistema IAM in oggetto e WSO2 stesso, nel caso di autenticazione tramite SPID (per motivi di semplicità la componente Satosa non è esplicitata):

Figura 9 – Autenticazione tramite SPID

Immagine che contiene testo, schermata, diagramma, design

Descrizione generata automaticamente

Le informazioni riportate in fase di autenticazione sono:

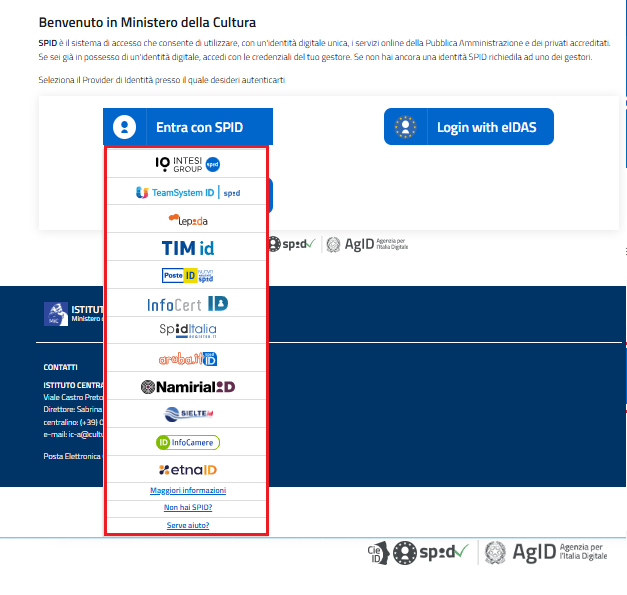
* **given\_name** - Nome
* **family\_name** - Cognome
* **fiscalNumber** - Codice fiscale
* **email** - E-mail come registrata nell’utenza SPID
* **authMethod** – metodo di autenticazione (“SPID”)

Di seguito vengono riportate le maschere principali di riferimento che l’utente dovrà selezionare per accedere all’applicazione di riferimento tramite SPID:

Figura 10 – Maschere di Autenticazione utente tramite SPID







### Autenticazione tramite CIE

L’autenticazione tramite CIE segue un flusso analogo a quello dell’autenticazione tramite SPID, ma le informazioni restituite dal provider del servizio sono le seguenti:

* **given\_name** - Nome
* **family\_name** - Cognome
* **fiscalNumber** - Codice fiscale
* **authMethod** – metodo di autenticazione (“SPID”)

Di seguito vengono riportate le maschere principali di riferimento che l’utente dovrà selezionare per accedere all’applicazione di riferimento tramite CIE:

Figura 11 – Maschere di Autenticazione utente tramite CIE

Immagine che contiene testo, schermata, Carattere, Marchio

Il contenuto generato dall'IA potrebbe non essere corretto.



Immagine che contiene testo, schermata, Pagina Web, Sito Web

Il contenuto generato dall'IA potrebbe non essere corretto.

### Autenticazione tramite eIDAS

L’autenticazione tramite eIDAS segue un flusso analogo a quello dell’autenticazione tramite SPID, ma le informazioni restituite dal provider del servizio sono le seguenti:

* **PersonIdentifier** - Codice identificativo univoco
* **FirstName** - Nome
* **FamilyName** - Cognome
* **DateOfBirth** - Data di nascita

Di seguito vengono riportate le maschere principali che l’utente dovrà selezionare per accedere all’applicazione di riferimento tramite eIDAS:

Figura 12 – Maschere di Autenticazione utente tramite eIDAS

Immagine che contiene testo, schermata, Carattere, Marchio

Il contenuto generato dall'IA potrebbe non essere corretto.



Immagine che contiene testo, elettronica, schermata, software

Il contenuto generato dall'IA potrebbe non essere corretto.

Si ricorda che l’utilizzo di tale modalità di autenticazione è dedicato ai cittadini europei che vogliano accedere ai servizi online degli Stati membri tramite la propria identità nazionale. Pertanto, tra le Country selezionabili non risulta essere presente la nazionalità italiana.

# Endpoint Esposti

La procedura di autenticazione (login e logout) prevede l’accesso ai seguenti endpoint:

Tabella 6 – Endpoint Esposti

|  |  |  |
| --- | --- | --- |
| AMBIENTE | TENANT | DESCRIZIONE |
| https://<HOST>/oauth2/authorize | GET | Endpoint da raggiungere per ottenere l’authorization code |
| https://<HOST>/oauth2/token | POST | Endpoint da raggiungere per ottenere l’access\_token e l’id\_token |
| https://<HOST>/oidc/logout | POST | Endpoint da raggiungere per effettuare il logout, fornendo i seguenti parametri:   * id\_token\_hint (obbligatorio) * post\_logout\_redirect\_uri (opzionale) * state (opzionale)   (senza authorization nell'header) |

## Ambiente di Collaudo

Endpoint dell’ambiente di collaudo:

Tabella 7 – Endpoint Ambiente di Collaudo

|  |  |
| --- | --- |
| UTILIZZO | END POINT |
| Identity Provider Entity ID: | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |
| Authorization Endpoint | https://identity-collaudo.cloud.sbn.it:443/oauth2/authorize |
| Token Endpoint | https://identity-collaudo.cloud.sbn.it:443/oauth2/token |
| Token Revocation Endpoint | https://identity-collaudo.cloud.sbn.it:443/oauth2/revoke |
| Token Introspection Endpoint | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/introspect |
| User Info Endpoint | https://identity-collaudo.cloud.sbn.it:443/oauth2/userinfo |
| Session IFrame Endpoint | https://identity-collaudo.cloud.sbn.it:443/oidc/checksession |
| Logout Endpoint | https://identity-collaudo.cloud.sbn.it:443/oidc/logout |
| Discovery Endpoint | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |
| Dynamic Client Registration Endpoint | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/api/identity/oauth2/dcr/v1.1/register |
| JWKS Endpoint | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/jwks |
| Discovery Endpoint | https://identity-collaudo.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |

ove ***nome\_TENANT*** è uno dei seguenti valori:

**[coll.ispc.it |coll.icar.it |coll.cloud.sbn.it]**

## Ambiente di Produzione

Endpoint dell’ambiente di produzione:

Tabella 8 – Endpoint Ambiente di Produzione

|  |  |
| --- | --- |
| UTILIZZO | END POINT |
| Identity Provider Entity ID: | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |
| Authorization Endpoint | https://identity.cloud.sbn.it:443/oauth2/authorize |
| Token Endpoint | https://identity.cloud.sbn.it:443/oauth2/token |
| Token Revocation Endpoint | https://identity.cloud.sbn.it:443/oauth2/revoke |
| Token Introspection Endpoint | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/introspect |
| User Info Endpoint | https://identity.cloud.sbn.it:443/oauth2/userinfo |
| Session IFrame Endpoint | https://identity.cloud.sbn.it:443/oidc/checksession |
| Logout Endpoint | https://identity.cloud.sbn.it:443/oidc/logout |
| Web finger Endpoint | https://identity.cloud.sbn.it:443/.well-known/webfinger |
| Discovery Endpoint | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |
| Dynamic Client Registration Endpoint | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/api/identity/oauth2/dcr/v1.1/register |
| JWKS Endpoint | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/jwks |
| Discovery Endpoint | https://identity.cloud.sbn.it:443/t/***nome\_TENANT***/oauth2/oidcdiscovery |

dove ***nome\_TENANT*** è uno dei seguenti valori:

**[ispc.it |icar.it |iccu.it]**

# WSO2 API

Le API esposte da WSO2 utili ad accedere ai servizi di gestione utente sono documentate al seguente link: <https://is.docs.wso2.com/en/6.1.0/apis/scim2-rest-apis/>

Al fine di autenticarsi per poter utilizzare il suddetto set di API, è necessario avere apposite credenziali (username e password).

Tali credenziali possono essere richieste in fase di onboarding, qualora l’applicativo avesse la necessità di gestire utente su WSO2 (database locale del IdP).

L’autenticazione avverrà utilizzando uno schema Basic Authentication con encoding di username e password in base64.

Lo username segue la naming convention:

*api\_<Nome Application SP>@<tenant>*

Esempio per l’applicativo “SBNCLOUD”: [api\_SBNCLOUD@iccu.it](mailto:api_SBNCLOUD@iccu.it)

La password sarà fornita in fase di on-boarding.

Le operazioni permesse sono: lettura di risorse e creazione/eliminazione di utenze.

## Creazione ed Eliminazione Utenti

La responsabilità della corretta creazione ed eliminazione di una utenza da parte di un applicativo all’interno dello user store di WSO2 è a totale carico dell’applicativo stesso.

Poiché più applicazioni, all’interno dello stesso tenant, possono essere accedute dallo stesso utente e poiché WSO2 non ha indicazione alcuna su quali applicazioni profilino i diversi utenti della sua base dati, si è ritenuto opportuno implementare una gestione logica di questa informazione anche all’interno di WSO2 attraverso il protocollo che segue.

In fase di onboarding, per ogni applicazione che ha necessità di creare autonomamente delle utenze in WSO2, verrà creato un gruppo all’interno dello IAM attraverso la risorsa ‘group’ di WSO2 stesso – il nome del gruppo sarà una stringa con formato app\_group\_<Nome Application SP>.

Ogni qual volta che una applicazione andrà a creare una utenza in WSO2, dovrà agganciare tale utente al proprio gruppo. Se l’utente già esiste in WSO2, è responsabilità dell’applicazione associare l’utente già esistente al proprio gruppo. Questa operazione può essere fatta attraverso lo stesso set di API SCIM2.

Ogni qual volta una applicazione volesse eliminare un utente dalla base dati di WSO2, dovrà prima eliminare l’associazione dell’utente stesso dal proprio gruppo (e solo da quello) e successivamente eliminare l’utente stesso da WSO2 se e solo se non dovessero risultare altri gruppi (applicazioni) cui l’utente è associato. Questo garantisce che un utente sia fisicamente eliminato dallo user store di WSO2 solo se non è associato ad alcun gruppo.

Questo protocollo assicura che non ci sia nessun utente nello user store che non sia associato ad almeno un gruppo. Eventuali utenti migrati nello user store da applicazioni preesistenti devono essere associati all’applicazione di provenienza attraverso opportuni batch di bonifica (se la migrazione è già avvenuta) o attraverso gli stessi batch di migrazione iniziale (migrazione massiva iniziale).

Nel dettaglio, si riportano le principali API necessarie ad effettuare la logica sopra descritta:

1. Recupero della lista di gruppi cui l’utente è associato:

**GET /Users/{id}** -> su base {id} dell’utente, ritorna un json contenente la lista dei gruppi cui l’utente appartiene nel campo “Resources/groups”

1. Aggiunta di un utente ad un gruppo:

**PATCH /Groups/{id}** -> su base {id} del gruppo cui si vuole associare l’utente, è necessario fornire un json contenente l’operazione specifica che si vuole eseguire, in questo caso “Operations/op” con valore “add”. Il campo “value/members” ospiterà la lista di utenti da aggiungere in base al loro specifico {id}

1. Rimozione di un utente ad un gruppo:

**PATCH /Groups/{id}** -> su base {id} del gruppo cui si vuole associare l’utente, è necessario fornire un json contenente l’operazione specifica che si vuole eseguire, in questo caso “Operations/op” con valore “remove”. Il campo “value/members” ospiterà la lista di utenti da aggiungere in base al loro specifico {id}

Figura 13 – Creazione ed Eliminazione Utenti

Immagine che contiene testo, schermata, Parallelo, Carattere

Descrizione generata automaticamente

# Implementazione Protocollo OpenID

A titolo di esempio, l’applicazione SBNCloud (SP) del tenant ICCU (sviluppata in ANGULAR) utilizza la seguente libreria per implementare l’autorizzazione e l’accesso con OpenID:

<https://github.com/manfredsteyer/angular-oauth2-oidc>

Può comunque essere utilizzata, qualsiasi altra libreria compatibile con il protocollo per la gestione dell’iter.

L’applicativo ha responsabilità di scegliere quale libreria Oauth2/Oidc basta che rispetti lo standard.

# Linee Guida

Possono emergere degli scenari di business in cui un applicativo permette ad un utente non autenticato di effettuare una serie di operazioni sulle proprie risorse (ricerca, selezione, consultazione, etc.), ma poi richiede all'utente stesso di autenticarsi prima di usufruire della risorsa o di modificarla.

In questi scenari, in cui si prevede una fase di autenticazione durante lo svolgimento del caso d'uso, si può rendere necessario adottare una soluzione che permetta all’utente di tornare alla pagina di interesse a valle della fase di autenticazione, senza perdere in tal modo lo stato delle operazioni pregresse.

Qualora richiesta, tale funzionalità è da gestirsi a livello applicativo, in quanto lo IAM non ha la possibilità di ricevere e restituire informazioni applicative specifiche durante la fase di autenticazione.

Sarà quindi l'applicativo a dover gestire la storicizzazione di tutte le informazioni necessarie al corretto ripristino dello use case (ad esempio ultima pagina visionata, ultima risorsa selezionata con specifico id) in modo da fornire all'utente finale una esperienza di navigazione più fluida.

Tali informazioni dovranno pertanto essere recuperate e valutate dopo la fase di autenticazione, nel momento in cui il controllo del flusso torna all'applicativo stesso ovvero nella pagina specificata come callback URL del flusso di autenticazione.

# Allegati

Si riportano di seguito una serie di documenti rilevanti[[1]](#footnote-1), a supporto e completamento del corrente.

Tabella 9 – Allegati

|  |  |  |  |
| --- | --- | --- | --- |
| ID | TITOLO ALLEGATO | TIPOLOGIA DEL DOCUMENTO | DESCRIZIONE |
| 1 | Allegato 6A - IAM\_ Modulo di accreditamento nuove applicazioni\_202501 | Tecnico | Modulo di accreditamento (onboarding) nuove applicazioni (SP-Service Provider) |
| 2 | Allegato 6B - IAM\_  Tracciato record di esempio Autenticazione M2W\_202501 | Tecnico | Esempio di tracciato record di Autenticazione M2W |

1. La documentazione è consultabile sul sito I.PaC al seguente indirizzo: [Documenti di progetto](https://ipac.cultura.gov.it/category/documenti-di-progetto/) [↑](#footnote-ref-1)